OceanStor Pacific Series 8.2.1

SFS Usage Guide

Issue	01
Date	2024-07-31

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

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

Trademarks and Permissions

and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://e.huawei.com

Security Declaration

Product Lifecycle

Huawei's regulations on product lifecycle are subject to the *Product End of Life Policy.* For details about this policy, visit the following web page:
https://support.huawei.com/ecolumnsweb/en/warranty-policy

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Initial Digital Certificate

The Initial digital certificates on Huawei devices are subject to the *Rights and Responsibilities of Initial Digital Certificates on Huawei Devices.* For details about this document, visit the following web page:
https://support.huawei.com/enterprise/en/bulletins-service/ENEWS2000015789

Huawei Enterprise End User License Agreement

This agreement is the end user license agreement between you (an individual, company, or any other entity) and Huawei for the use of the Huawei Software. Your use of the Huawei Software will be deemed as your acceptance of the terms mentioned in this agreement. For details about this agreement, visit the following web page:
https://e.huawei.com/en/about/eula

Lifecycle of Product Documentation

Huawei after-sales user documentation is subject to the *Product Documentation Lifecycle Policy.* For details about this policy, visit the following web page:
https://support.huawei.com/enterprise/en/bulletins-website/ENEWS2000017761

About This Document

Purpose

This document describes how to plan, install, configure, and maintain the OceanStor Pacific series storage system.

Intended Audience

This document is intended for:

- Technical support engineers
- Operation and maintenance (O&M) personnel

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Copyright © Huawei Technologies Co., Ltd.

Change History

Issue	Date	Description
01	2024-07-31	This issue is the first official release.

 Copyright © Huawei Technologies Co., Ltd.

Contents

About This Document iii
1 Before You Start 1
2 Introduction 2
3 Network Planning 3
3.1 Before You Start 3
3.2 Planning of OceanStor Pacific 9550/OceanStor Pacific 9950/OceanStor Pacific 9546/OceanStor Pacific 9350/OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node) 4
3.2.1 File Service (DPC Scenario) 4
3.2.1.1 Overview 4
3.2.1.2 Networking Scenarios 5
3.2.1.3 Network Requirements 6
3.2.1.4 Network Solution 7
3.2.1.5 Planning Ports for Nodes 12
3.2.1.5.1 OceanStor Pacific 9550 12
3.2.1.5.2 OceanStor Pacific 9950 13
3.2.1.5.3 OceanStor Pacific 9546 14
3.2.1.6 Network Example 17
3.2.1.6.1 Network Example for OceanStor Pacific 9550/OceanStor Pacific 9546 17
3.2.1.6.2 Network Example for OceanStor Pacific 9950 22
3.2.2 File Service (Standard Protocol Scenario) 27
3.2.2.1 Overview 27
3.2.2.2 Networking Scenarios 28
3.2.2.3 Network Requirements 30
3.2.2.4 Network Solution 31
3.2.2.5 Planning Ports for Nodes 36
3.2.2.5.1 OceanStor Pacific 9550 and OceanStor Pacific 9350 36
3.2.2.5.2 OceanStor Pacific 9546 37
3.2.2.5.3 OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node) 40
3.2.2.6 Network Example 41
3.2.2.6.1 Network Example for OceanStor Pacific 9550/OceanStor Pacific 9546/OceanStor Pacific 9350/OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node) 41
3.2.3 File/Object Service (DPC and Standard Protocol Hybrid Scenario) 47
3.2.3.1 Overview 47

 Copyright © Huawei Technologies Co., Ltd.

3.2.3.2 Networking Scenarios....47
3.2.3.3 Network Requirements....50
3.2.3.4 Network Solution....51
3.2.3.5 Planning Ports for Nodes....55
3.2.3.5.1 OceanStor Pacific 9550....55
3.2.3.5.2 OceanStor Pacific 9546 (Two CPUs per Node)....56
3.2.3.6 Network Example....59
3.3 Planning of OceanStor Pacific 9520/OceanStor Pacific 9540/OceanStor Pacific 9920/OceanStor Pacific 9340....59
3.3.1 File Service (DPC Scenario)....59
3.3.1.1 Overview....59
3.3.1.2 Networking Scenarios....60
3.3.1.3 Network Requirements....62
3.3.1.4 Network Solution....62
3.3.1.5 Planning Ports for Nodes....66
3.3.1.5.1 OceanStor Pacific 9540 Kunpeng-based....66
3.3.1.5.2 OceanStor Pacific 9920 Kunpeng-based (SAS SSD)....67
3.3.1.5.3 OceanStor Pacific 9920 Kunpeng-based (Palm-sized NVMe SSD)....68
3.3.1.6 Network Example....68
3.3.2 File Service (Standard Protocol Scenario)....74
3.3.2.1 Overview....74
3.3.2.2 Networking Scenarios....75
3.3.2.3 Network Requirements....80
3.3.2.4 Network Solution....81
3.3.2.5 Planning Ports for Nodes....85
3.3.2.5.1 OceanStor Pacific 9540 Kunpeng-based and OceanStor Pacific 9340 Kunpeng-based....85
3.3.2.5.2 OceanStor Pacific 9520 Kunpeng-based 12-Slot....87
3.3.2.5.3 OceanStor Pacific 9920 Kunpeng-based (SAS SSD)....88
3.3.2.5.4 OceanStor Pacific 9920 Kunpeng-based (Palm-sized NVMe SSD)....89
3.3.2.5.5 OceanStor Pacific 9520 Kunpeng-based 14-Slot....90
3.3.2.6 Network Example....91
3.3.3 File/Object Service (DPC and Standard Protocol Hybrid Scenario)....96
3.3.3.1 Overview....96
3.3.3.2 Networking Scenarios....97
3.3.3.3 Network Requirements....100
3.3.3.4 Network Solution....100
3.3.3.5 Planning Ports for Nodes....103
3.3.3.5.1 OceanStor Pacific 9540 Kunpeng-based....103
3.3.3.6 Network Example....105
3.4 LLD Planning and Implementation....105
3.4.1 Manually Filling out the Deployment File Template....105
4 Hardware Installation....108

 Copyright © Huawei Technologies Co., Ltd.

5 Installing Software 109
5.1 Before You Start 109
5.2 Installation Overview 110
5.3 Installation PC Requirements 110
5.4 Installing Software 111
5.4.1 Installing the File Service (Standard Protocol Scenario) 111
5.4.1.1 Node Requirements 111
5.4.1.2 Installation Process 112
5.4.1.3 Preparing for Installation 113
5.4.1.3.1 Preparing Documents and Tools 113
5.4.1.3.2 Obtaining Software Packages 115
5.4.1.4 Configuring Switches 120
5.4.1.4.1 Switch Configuration Requirements and Configuration Data 120
5.4.1.4.2 Configuring GE External Management Switches 121
5.4.1.4.3 Configuring 10GE/25GE Service Switches (Applicable to CE6865) 122
5.4.1.5 Installation Procedure (Applicable to LLD-based Configuration) 124
5.4.1.5.1 Initializing Nodes Using SmartKit 124
5.4.1.5.1.1 Preparing the Deployment File Template and SmartKit 124
5.4.1.5.1.2 Configuring iBMC IP Addresses for Nodes 126
1. Configuring iBMC IP Addresses for Nodes in Batches 126
2. Configuring an iBMC IP Address for a Single Node 137
5.4.1.5.1.3 Checking Version Mappings 142
5.4.1.5.1.4 (Optional) Upgrading Firmware 147
5.4.1.5.1.5 (Optional) Installing the OS 153
5.4.1.5.1.6 Initializing Networks 157
5.4.1.5.1.7 (Optional) Upgrading Drivers 160
5.4.1.5.2 Installing OceanStor Pacific Series Software 167
5.4.1.6 Installation Procedure (Applicable to Wizard-based Configuration) 170
5.4.1.6.1 Configuring iBMC IP Addresses for Nodes 170
5.4.1.6.2 Checking Storage Nodes Before Installation 174
5.4.1.6.2.1 Checking Whether a RAID Controller Card Is Used (Applicable to Kunpeng-based Devices) 174
5.4.1.6.2.2 OceanStor Pacific 9550, 9546, 9350, and 9346 175
1. Checking the Node Firmware Version 175
2. Checking the OS Version 175
3. Checking BIOS Settings 176
4. Checking the Device Firmware and Driver Versions 177
5. Checking the Hi1822V120 NIC Mode 178
5.4.1.6.2.3 OceanStor Pacific 9540 Kunpeng-based Without a RAID Controller Card, 9520 Kunpeng-based Without a RAID Controller Card, 9920 Kunpeng-based Without a RAID Controller Card, and 9340 Kunpeng-based Without a RAID Controller Card 179
1. OceanStor Pacific 9520 Kunpeng-based 14-Slot Without a RAID Controller Card and 9920 Kunpeng-based (Palm-sized NVMe SSD) Without a RAID Controller Card 179
1. Checking the Node Firmware Version 179

 Copyright © Huawei Technologies Co., Ltd.

2. Checking the OS Version 179
3. Checking BIOS Settings 180
4. Checking the Device Firmware and Driver Versions 181
2. Other Kunpeng-based Models Without a RAID Controller Card 181
1. Checking the Node Firmware Version 182
2. Checking the OS Version 182
3. Checking BIOS Settings 183
4. Checking the Device Firmware and Driver Versions 184
5. Checking the Hi1822V120 NIC Mode 185
6. Checking the Compatibility of a Disk Backplane 186
5.4.1.6.2.4 OceanStor Pacific 9540 Kunpeng-based with a RAID Controller Card, 9520 Kunpeng-based with a RAID Controller Card, and 9340 Kunpeng-based with a RAID Controller Card 187
1. Checking the Node Firmware Version 188
2. Checking the OS Version 188
3. Checking the Cache Policy of a System Disk 189
4. Checking the JBOD Function 191
5. Checking BIOS Settings 191
6. Checking the Device Firmware and Driver Versions 193
7. Checking the Hi1822V120 NIC Mode 193
8. Checking the Compatibility of a Disk Backplane 195
5.4.1.6.3 Configuring the Management Network of a Node 196
5.4.1.6.3.1 Configuration Requirements 196
5.4.1.6.3.2 Configuring a Physical Port IP Address 196
5.4.1.6.3.3 Configuring a Bond Port IP Address 198
5.4.1.6.3.4 Configuring a Physical Port IP Address and a VLAN 202
5.4.1.6.3.5 Configuring a Bond Port IP Address and a VLAN 204
5.4.1.6.4 Installing OceanStor Pacific Series Software 207
5.4.1.6.4.1 Installing Management Nodes (Applicable to OceanStor Pacific 9550, 9546, 9540, 9520, and 9920) 207
5.4.1.6.4.2 Installing Management Nodes (Applicable to OceanStor Pacific 9350, 9346, and 9340) 217
5.4.1.6.4.3 Adding Storage Nodes 228
5.4.1.6.4.4 Configuring the Storage Network (When Front- and Back-End Storage Networks Are Shared and Use RoCE and Multiple IP Addresses for Networking) 234
5.4.1.6.4.5 Configuring the Storage Network (When Front- and Back-End Storage Networks Are Shared and Use TCP for Networking) 238
5.4.1.6.4.6 Installing Storage Nodes 241
5.4.1.6.4.7 Creating a Control Cluster (Applicable to OceanStor Pacific 9550 and 9350) 241
5.4.1.6.4.8 Creating a Control Cluster (Applicable to OceanStor Pacific 9540, 9520, 9920, 9340, 9546, and 9346) 243
5.4.1.7 Obtaining and Loading a License 245
5.4.1.8 Performing an Upgrade Using a Preset Hot Patch 245
5.4.2 Installing the File Service (DPC Scenario) 246
5.4.2.1 Node Requirements 246
5.4.2.2 DPC Node Configuration Description 246

 Copyright © Huawei Technologies Co., Ltd.

5.4.2.3 Installation Process 251
5.4.2.4 Preparing for Installation 254
5.4.2.4.1 Preparing Documents and Tools 254
5.4.2.4.2 Obtaining Software Packages 255
5.4.2.5 Configuring Switches 260
5.4.2.5.1 Switch Configuration Requirements and Installation Data 260
5.4.2.5.2 Configuring GE External Management Switches 261
5.4.2.5.3 Configuring 25GE External Management Switches (Applicable to CE6865) 262
5.4.2.5.4 Configuring 100GE External Management Switches (Applicable to CE8850) 263
5.4.2.6 Installation Procedure (Applicable to LLD-based Configuration) 265
5.4.2.6.1 Initializing Nodes Using SmartKit 265
5.4.2.6.1.1 Preparing the Deployment File Template and SmartKit 265
5.4.2.6.1.2 Configuring iBMC IP Addresses for Nodes 267
1. Configuring iBMC IP Addresses for Nodes in Batches 267
2. Configuring an iBMC IP Address for a Single Node 278
5.4.2.6.1.3 Checking Version Mappings 283
5.4.2.6.1.4 (Optional) Upgrading Firmware 288
5.4.2.6.1.5 (Optional) Installing the OS 294
5.4.2.6.1.6 Initializing Networks 298
5.4.2.6.1.7 (Optional) Upgrading Drivers 301
5.4.2.6.2 Installing OceanStor Pacific Series Software 308
5.4.2.7 Installation Procedure (Applicable to Wizard-based Configuration) 311
5.4.2.7.1 Configuring the Management IP Address of a Data Cluster Module (Applicable to OceanStor Pacific 9950) 311
5.4.2.7.2 Configuring iBMC IP Addresses for Nodes 313
5.4.2.7.3 Checking Storage Nodes Before Installation 317
5.4.2.7.3.1 Checking Whether a RAID Controller Card Is Used (Applicable to Kunpeng-based Devices) 317
5.4.2.7.3.2 OceanStor Pacific 9950, 9550, and 9546 318
1. Checking the Node Firmware Version 318
2. Checking the OS Version 318
3. Checking BIOS Settings 319
4. Checking the Device Firmware and Driver Versions 320
5. Checking the Hi1822V120 NIC Mode 321
5.4.2.7.3.3 OceanStor Pacific 9540 Kunpeng-based Without a RAID Controller Card and 9920 Kunpeng-based Without a RAID Controller Card 322
1. OceanStor Pacific 9920 Kunpeng-based (Palm-sized NVMe SSD) Without a RAID Controller Card 322
1. Checking the Node Firmware Version 322
2. Checking the OS Version 322
3. Checking BIOS Settings 323
4. Checking the Device Firmware and Driver Versions 324
2. Other Kunpeng-based Models Without a RAID Controller Card 324
1. Checking the Node Firmware Version 324
2. Checking the OS Version 325

 Copyright © Huawei Technologies Co., Ltd.

3. Checking BIOS Settings....326
4. Checking the Device Firmware and Driver Versions....327
5. Checking the Hi1822V120 NIC Mode....328
6. Checking the Compatibility of a Disk Backplane....329
5.4.2.7.3.4 OceanStor Pacific 9540 Kunpeng-based with a RAID Controller Card....330
1. Checking the Node Firmware Version....330
2. Checking the OS Version....331
3. Checking the Cache Policy of a System Disk....332
4. Checking the JBOD Function....334
5. Checking BIOS Settings....334
6. Checking the Device Firmware and Driver Versions....336
7. Checking the Hi1822V120 NIC Mode....336
8. Checking the Compatibility of a Disk Backplane....338
5.4.2.7.4 Configuring the Management Network of a Node....339
5.4.2.7.4.1 Configuration Requirements....339
5.4.2.7.4.2 Configuring a Physical Port IP Address....339
5.4.2.7.4.3 Configuring a Bond Port IP Address....341
5.4.2.7.4.4 Configuring a Physical Port IP Address and a VLAN....344
5.4.2.7.4.5 Configuring a Bond Port IP Address and a VLAN....347
5.4.2.7.5 Installing OceanStor Pacific Series Software....349
5.4.2.7.5.1 Installing Management Nodes (Applicable to OceanStor Pacific 9950, 9550, 9546, 9540, and 9920)....350
5.4.2.7.5.2 Adding Storage Nodes....359
5.4.2.7.5.3 Configuring the Storage Network (When Front- and Back-End Storage Networks Are Shared and Use RoCE and Multiple IP Addresses for Networking)....366
5.4.2.7.5.4 Installing Storage Nodes....370
5.4.2.7.5.5 Creating a Control Cluster (Applicable to OceanStor Pacific 9950 and 9550)....370
5.4.2.7.5.6 Creating a Control Cluster (Applicable to OceanStor Pacific 9540, 9520, 9920, and 9546)....372
5.4.2.8 Obtaining and Loading a License....374
5.4.2.9 Configuring the System Time (Applicable to the Huawei Cloud Stack Online Scenario)....374
5.4.2.10 Adding Data Cluster Modules (Applicable to OceanStor Pacific 9950)....375
5.4.2.11 (Optional) Installing an MPI Framework....377
5.4.2.12 Performing an Upgrade Using a Preset Hot Patch....377
5.4.3 Installing the File/Object Service (DPC and Standard Protocol Hybrid Scenario)....378
5.5 Appendix....379
5.5.1 Logging In to a Node....379
5.5.1.1 Logging In to a Node Using PuTTY (Network Port Mode)....379
5.5.1.2 Using PuTTY to Log In to a Node in Key Pair Authentication Mode....380
5.5.1.3 Logging In to a Node Using a KVM....383
5.5.2 Switch-Related Operations....384
5.5.2.1 Logging In to a Switch....384
5.5.2.2 Configuring Flow Control for a Switch....386
5.5.2.2.1 DSCP Flow Control Algorithm....386

 Copyright © Huawei Technologies Co., Ltd.

5.5.2.2.1.1 Configuring Flow Control for a Switch (Recommended Configuration of AI Fabric) 387
5.5.2.2.1.2 Configuring Flow Control for a Switch 404
5.5.2.2.2 PCP Flow Control Algorithm 417
5.5.2.2.2.1 Configuring Flow Control for a Switch (Recommended Configuration of AI Fabric) 417
5.5.2.2.2.2 Configuring Flow Control for a Switch (CE6857E/CE6857F/FM6857E/CE6865/CE6865E/CE8850) 441
5.5.2.2.2.3 Configuring Flow Control for a Switch (CE6866/CE8851) 462
5.5.2.3 Configuring ACL Rules for Switches 466
5.5.2.3.1 Using a Script 467
5.5.2.3.2 Using Switch Commands 469
5.5.2.4 Querying the ACL Rule Configuration of a Switch 473
5.5.3 Checking the cloud_vpc.ini File 476
5.5.4 Enabling JBOD (Applicable to OceanStor Pacific 9540 Kunpeng-based, 9520 Kunpeng-based, 9920 Kunpeng-based, and 9340 Kunpeng-based) 476
5.5.5 Configuring BIOS 477
5.5.5.1 Configuring BIOS (Applicable to OceanStor Pacific 9950, 9550, 9546, 9350, and 9346) 477
5.5.5.2 Configuring BIOS (Applicable to OceanStor Pacific 9540 Kunpeng-based, 9520 Kunpeng-based, 9920 Kunpeng-based, and 9340 Kunpeng-based) 479
5.5.5.2.1 Configuring BIOS (Applicable to OceanStor Pacific 9520 Kunpeng-based 14-Slot and 9920 Kunpeng-based (Palm-sized NVMe SSD)) 479
5.5.5.2.2 Configuring BIOS (Applicable to Other Kunpeng-based Devices) 481
5.5.6 Installing OSs for Storage Nodes 487
5.5.6.1 Installing an OS (Applicable to OceanStor Pacific 9950, 9550, 9546, 9350, and 9346) 487
5.5.6.2 Installing an OS (Applicable to OceanStor Pacific 9520 Kunpeng-based Without a RAID Controller Card, 9540 Kunpeng-based Without a RAID Controller Card, 9920 Kunpeng-based Without a RAID Controller Card, and 9340 Kunpeng-based Without a RAID Controller Card) 493
5.5.6.2.1 Installing an OS (Applicable to OceanStor Pacific 9520 Kunpeng-based 14-Slot Without a RAID Controller Card and 9920 Kunpeng-based (Palm-sized NVMe SSD) Without a RAID Controller Card) 493
5.5.6.2.2 Installing an OS (Applicable to Other Kunpeng-based Models Without a RAID Controller Card) 499
5.5.6.3 Installing an OS (Applicable to OceanStor Pacific 9520 Kunpeng-based with a RAID Controller Card, 9540 Kunpeng-based with a RAID Controller Card, 9920 Kunpeng-based with a RAID Controller Card, and 9340 Kunpeng-based with a RAID Controller Card) 505
5.5.6.4 Installing a Third-Party OS 505
5.5.7 Installing the OS Dependency Package 507
5.5.8 Weak Password Dictionary 512
5.5.9 Adding a Port 513
5.5.10 Configuring a Static Route 515
5.5.10.1 Configuring a Static Route for a Physical Port 515
5.5.10.2 Configuring a Static Route for a Bond Port 516
5.5.10.3 Configuring a Static Route for a VLAN Port 516
5.5.11 Querying a Static Route 517
5.5.11.1 Querying the Static Routes of a Physical Port 517
5.5.11.2 Querying the Static Routes of a Bond Port 518
5.5.11.3 Querying the Static Routes of a VLAN Port 519

 Copyright © Huawei Technologies Co., Ltd.

5.5.12 Deleting a Static Route....519
5.5.12.1 Deleting a Static Route from a Physical Port....519
5.5.12.2 Deleting a Static Route from a Bond Port....520
5.5.12.3 Deleting a Static Route from a VLAN Port....520
5.5.13 Configuring a Policy-Based Route....520
5.5.13.1 Configuring a Policy-based Route for a Physical Port....520
5.5.13.2 Configuring a Policy-based Route for a Bond Port....521
5.5.13.3 Configuring a Policy-based Route for a VLAN Port....522
5.5.14 Querying a Policy-Based Route....523
5.5.14.1 Querying the Policy-based Routes of a VLAN Port....523
5.5.15 Deleting a Policy-based Route....524
5.5.15.1 Deleting a Policy-based Route from a VLAN Port....524
5.5.16 Configuring the Storage Network IP Address by Modifying the Configuration File....524
5.5.16.1 Configuring the Storage Network (TCP/IP)....524
5.5.16.2 Configuring the Storage Network (RoCE and Multiple IP Addresses)....530
5.5.17 Configuring a Temporary IP Address....535
5.5.18 Formatting an NVMe SSD....535
5.5.19 Uninstalling OceanStor Pacific Series Software....536
5.5.20 Installing the iBMA Component....538
5.5.21 Identifying the Installation Mode....540
5.5.22 Importing the OS Certificate of a DPC Node....540
5.5.23 Obtaining the Node Installation Resource Package....550
5.5.24 FAQs....552
5.5.24.1 Failed to Install the Scale-Out Storage OS Using the 3108 or 3416 RAID Controller Card....552
5.5.24.2 How Do I Solve the Problem That the Number of PFC-enabled Queues Exceeds the Upper Limit?....553
5.5.25 Other Operations....554
5.5.25.1 Uploading Files to a Node Using FileZilla....554
5.5.25.2 Importing Environmental Variables....555
5.5.25.3 Installing LFTP....556
5.5.25.4 Modifying the Management Node Network....557
5.5.25.5 Obtaining the Compatibility Information Using Huawei Storage Interoperability Navigator....558
5.5.25.6 Configuring Switch Ports in a Batch....558
5.5.25.7 Changing the System Time of a Node....559

6 Basic Service Configuration....560

6.1 Before You Start....560
6.2 Installation Overview....561
6.3 Installation PC Requirements....561
6.4 Configuring Basic Services....562
6.4.1 Configuring Basic File Services (Standard Protocol Scenario)....562
6.4.1.1 Configuring Basic Services (Standard Protocol Scenario-NFS Share)....562
6.4.1.1.1 Configuration Process....562

 Copyright © Huawei Technologies Co., Ltd.

6.4.1.1.2 Creating a Converged Storage Pool....563
6.4.1.1.3 Enabling the File Service on a Node....571
6.4.1.1.4 (Optional) Enabling the SmartTier Feature....573
6.4.1.1.5 Adding a VXLAN....573
6.4.1.1.6 Using SmartKit to Perform Deployment Inspection....574
6.4.1.2 Configuring Basic Services (Standard Protocol Scenario-CIFS Share)....584
6.4.1.2.1 Configuration Process....584
6.4.1.2.2 Creating a Converged Storage Pool....585
6.4.1.2.3 Enabling the File Service on a Node....593
6.4.1.2.4 (Optional) Enabling the SmartTier Feature....595
6.4.1.2.5 Adding a VXLAN....595
6.4.1.2.6 Creating a Local Authentication User (Applicable to Non-Domain Environments)....596
6.4.1.2.7 Using SmartKit to Perform Deployment Inspection....599
6.4.2 Configuring Basic File Services (DPC Scenario)....609
6.4.2.1 Configuration Process....609
6.4.2.2 Configuring the DPC Node Storage Network IP Address by Modifying the Configuration File....610
6.4.2.3 Creating a Converged Storage Pool....610
6.4.2.4 Enabling the File Service on a Node....619
6.4.2.5 (Optional) Enabling the SmartTier Feature....621
6.4.2.6 Installing DPC....621
6.4.2.6.1 Checking the Connectivity Between the Internal Management Networks of a Management Node and a DPC Node Before Installation....621
6.4.2.6.2 Creating DPC....622
6.4.2.6.3 Configuring the Storage Network....627
6.4.2.7 Performance Tuning....632
6.4.2.7.1 Scenario 1....632
6.4.2.7.2 Scenario 2....632
6.4.2.7.3 Scenario 3....636
6.4.2.7.4 Scenario 4....637
6.4.2.8 Using SmartKit to Perform Deployment Inspection....638
6.4.2.9 Appendix....649
6.4.2.9.1 Configuring a Static Route....649
6.4.2.9.1.1 Configuring a Static Route for a Physical Port....649
6.4.2.9.1.2 Configuring a Static Route for a Bond Port....650
6.4.2.9.1.3 Configuring a Static Route for a VLAN Port....651
6.4.2.9.2 Importing the OS Certificate of a DPC Node....652
6.4.2.9.3 Installing the OS Dependency Package....662
6.4.3 Configuring Basic Object Services....667
6.4.3.1 Creating a Converged Storage Pool....668
6.4.3.2 Enabling the Object Service on a Node....676
6.4.3.3 (Optional) Enabling the SmartTier Feature....678
6.4.3.4 Adding a VXLAN....678
6.4.3.5 Using SmartKit to Perform Deployment Inspection....679

 Copyright © Huawei Technologies Co., Ltd.

6.5 Managing Basic Services 689
6.5.1 Managing a Converged Storage Pool 690
6.5.1.1 Viewing Storage Pool Information 690
6.5.1.2 Modifying a Storage Pool 692
6.5.1.3 Modifying a Disk Pool 693
6.5.1.4 Deleting a Storage Pool 694
6.5.2 Managing Certificates 697
6.5.2.1 Viewing Certificates 697
6.5.2.2 Viewing Built-In CA Certificates 699
6.5.2.3 Exporting a Certificate Signing Request (CSR) File 701
6.5.2.4 Using Built-In CA to Issue Digital Certificates 702
6.5.2.5 Exporting Issued Digital Certificates 704
6.5.2.6 Exporting a Built-In CA Certificate 704
6.5.2.7 Importing and Activating a Certificate 704
6.5.2.8 Modifying a Certificate 707
6.5.2.9 Deleting an Issued Digital Certificate 708
6.5.2.10 Auto Certificate Issuing 708
6.5.2.11 Replacing the HyperMetro Arbitration Security Certificate 709
6.5.2.12 Deleting the CA Certificate of 714
6.5.3 Managing DPC Nodes 715
6.5.3.1 Viewing Nodes 715
6.5.3.2 Enabling FSA 715
6.5.3.3 Disabling FSA 716
6.5.3.4 Deleting DPC 716
6.5.4 Removing a Node 717
6.5.5 Viewing VXLAN Information 718
6.5.5.1 Viewing VXLAN Information 720
6.5.5.2 Removing a VXLAN 721
6.5.6 Managing the External Key Service 721
6.5.7 Setting Per-Second Performance Monitoring for Converged Services 724
6.5.8 Adding a Node for an Enabled Service 725
6.5.9 Deleting a Subnet 726
7 Maintenance and Fault Management 727

 Copyright © Huawei Technologies Co., Ltd.

1 Before You Start

Instructions on Using the Security Sandbox

- Enabling the security sandbox function can improve system security and prevent untrusted users or attackers from logging in to the storage operating system (OS) through SSH to perform malicious operations. When the OceanStor Pacific Series 8.2.1RC1 software or later is installed for the first time, the security sandbox is automatically enabled on the added storage nodes.
- After the security sandbox is enabled, users can only use the **cli_portal** command after logging in to the OS. The **cli_portal** command can be used to run the CLI, **minisystem**, and **diagnose** (only for FSA nodes) commands. All commands or scripts that are directly executed on the OS cannot be executed, including common **ls**, **rm**, and **cat** commands, as shown in the following figure:

  ```
  FSMA:cliportal> cat /etc/passwd
  Error : Command 'cat' does not exist or has an incorrect format.
  Try 'help' for more information.
  ```

- Before executing OS commands, disable the security sandbox by referring to **Routine Management** > **Managing a Cluster System** > **Managing Hardware Information** > **Disabling Security Sandbox** in *OceanStor Pacific Series 8.2.1 Administrator Guide*. After the OS commands are executed, enable the security sandbox by referring to **Routine Management** > **Managing a Cluster System** > **Managing Hardware Information** > **Enabling Security Sandbox** in *OceanStor Pacific Series 8.2.1 Administrator Guide*.

  NOTE

  - You can also run the **closesandbox** command on the cli_portal to disable the security sandbox.
  - The security sandbox supports only the standard storage OS. Other non-standard OSs do not support the security sandbox function.
  - After the security sandbox function is disabled, the system is no longer protected by any security sandbox.
  - After the security sandbox is disabled, you need to restart the session for the setting to take effect. After the security sandbox is disabled, you can enable it as required.
  - The security sandbox is applicable to OceanStor Pacific series 8.1.3 and later versions.

 Copyright © Huawei Technologies Co., Ltd.

2 Introduction

Huawei Cloud Stack is a cloud solution provided by Huawei Cloud for government and enterprise customers and delivered on customers' premises. It consists of the Huawei Cloud Stack (HCS) and Huawei Cloud Stack Online (HCSO) solutions. Scalable File Service (SFS) provides customers with on-demand, scalable, high-performance, and large-capacity file storage in the HCS or HCSO scenario. OceanStor Pacific series scale-out storage can interconnect with SFS on Huawei Cloud to provide scale-out storage capabilities for SFS.

- SFS supports the following devices: OceanStor Pacific 9550, OceanStor Pacific 9950, OceanStor Pacific 9546, OceanStor Pacific 9350, OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node), OceanStor Pacific 9520 Kunpeng-based, OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9920 Kunpeng-based, and OceanStor Pacific 9340 Kunpeng-based.
- SFS supports file and object services.

 Copyright © Huawei Technologies Co., Ltd.

3 Network Planning

3.1 Before You Start

3.2 Planning of OceanStor Pacific 9550/OceanStor Pacific 9950/OceanStor Pacific 9546/OceanStor Pacific 9350/OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node)

3.3 Planning of OceanStor Pacific 9520/OceanStor Pacific 9540/OceanStor Pacific 9920/OceanStor Pacific 9340

3.4 LLD Planning and Implementation

3.1 Before You Start

Instructions on Using the Security Sandbox

- Enabling the security sandbox function can improve system security and prevent untrusted users or attackers from logging in to the storage operating system (OS) through SSH to perform malicious operations. When the OceanStor Pacific Series 8.2.1RC1 software or later is installed for the first time, the security sandbox is automatically enabled on the added storage nodes.
- After the security sandbox is enabled, users can only use the **cli_portal** command after logging in to the OS. The **cli_portal** command can be used to run the CLI, **minisystem**, and **diagnose** (only for FSA nodes) commands. All commands or scripts that are directly executed on the OS cannot be executed, including common **ls**, **rm**, and **cat** commands, as shown in the following figure:

  ```
  FSMA:cliportal> cat /etc/passwd
  Error : Command 'cat' does not exist or has an incorrect format.
  Try 'help' for more information.
  ```

- Before executing OS commands, disable the security sandbox by referring to **Routine Management** > **Managing a Cluster System** > **Managing Hardware Information** > **Disabling Security Sandbox** in *OceanStor Pacific Series 8.2.1 Administrator Guide*. After the OS commands are executed, enable the security sandbox by referring to **Routine Management** > **Managing a Cluster System** > **Managing Hardware Information** >

 Copyright © Huawei Technologies Co., Ltd.

Enabling Security Sandbox in *OceanStor Pacific Series 8.2.1 Administrator Guide*.

NOTE

- You can also run the **closesandbox** command on the cli_portal to disable the security sandbox.
- The security sandbox supports only the standard storage OS. Other non-standard OSs do not support the security sandbox function.
- After the security sandbox function is disabled, the system is no longer protected by any security sandbox.
- After the security sandbox is disabled, you need to restart the session for the setting to take effect. After the security sandbox is disabled, you can enable it as required.
- The security sandbox is applicable to OceanStor Pacific series 8.1.3 and later versions.

3.2 Planning of OceanStor Pacific 9550/OceanStor Pacific 9950/OceanStor Pacific 9546/OceanStor Pacific 9350/OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node)

3.2.1 File Service (DPC Scenario)

3.2.1.1 Overview

Network Introduction

The following networks are involved for OceanStor Pacific series in the DPC scenario:

- BMC network

  The BMC network connects to Mgmt ports of nodes to enable remote device management.
- Management network
  - The external management network is used by users to access DeviceManager and the CLI, and for communication between storage nodes and external HCS/HCSO O&M systems.
  - The internal management network is used for management data communication between the management and storage nodes.
- Control network
  - Transmits control messages in the system.
  - Adopts a floating IP address that floats among storage network ports on nodes.
- Storage network

  In the DPC scenario, the front-end storage network and back-end storage network are shared for data communication between storage nodes and between DPC and OSD.

 Copyright © Huawei Technologies Co., Ltd.

3.2.1.2 Networking Scenarios

Table 3-1 shows the DPC networking scenarios supported by OceanStor Pacific 9550, OceanStor Pacific 9950, and OceanStor Pacific 9546.

Table 3-1 Networking scenarios

Device Name	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example
OceanStor Pacific 9550	3.2.1.5.1 OceanStor Pacific 9550	25GE (LOM) or GE (LOM)	CE6865 (25GE) or switch that supports GE	100GE RoCE (CX5)	CE8850
OceanStor Pacific 9950	3.2.1.5.2 OceanStor Pacific 9950	100GE (LOM) or GE (LOM)	CE8850 (100GE) or switch that supports GE	100GE RoCE (customized CX6 NIC)	CE8850
OceanStor Pacific 9546	3.2.1.5.3 OceanStor Pacific 9546	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850
Tiering scenario: OceanStor Pacific 9550 + OceanStor Pacific 9950	3.2.1.5.1 OceanStor Pacific 9550	25GE (LOM) or GE (LOM)	CE6865 (25GE) or switch that supports GE	100GE RoCE (CX5)	CE8850
	3.2.1.5.2 OceanStor Pacific 9950	100GE (LOM) or GE (LOM)	CE8850 (100GE) or switch that supports GE	100GE RoCE (customized CX6 NIC)	CE8850
Tiering scenario: OceanStor Pacific 9950 + OceanStor Pacific 9546	3.2.1.5.2 OceanStor Pacific 9950	100GE (LOM) or GE (LOM)	CE8850 (100GE) or switch that supports GE	100GE RoCE (customized CX6 NIC)	CE8850
	3.2.1.5.3 OceanStor Pacific 9546	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850

Copyright © Huawei Technologies Co., Ltd.

Device Name	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example
Tiering scenario: OceanStor Pacific 9546 + OceanStor Pacific 9550	3.2.1.5.3 OceanStor Pacific 9546	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850
	3.2.1.5.1 OceanStor Pacific 9550	25GE (LOM) or GE (LOM)	CE6865 (25GE) or switch that supports GE	100GE RoCE (CX5)	CE8850

3.2.1.3 Network Requirements

Table 3-2 describes the specific network requirements in the DPC scenario.

Table 3-2 Network requirements

Network Type	Network Requirements
BMC network	• A BMC network can be a GE network. • The number of BMC network ports on each storage node can be one or two.
Storage network	• The RoCE protocol and 100GE network are supported, and only multiple IP addresses can be configured. **NOTE** When the storage network does not use the bond network, each port on the storage network can be bonded to one IP address. • The storage networks of all nodes use the same VLAN ID.
Control network	If the storage network uses multiple IP addresses, select a port on the storage network to configure one floating IP address for the control network. The control network and the storage network can be in the same subnet (recommended) or different subnets. If they use the same VLAN ID and are in the same subnet, they must use different IP address segments.

Copyright © Huawei Technologies Co., Ltd.

Network Type	Network Requirements
External management network	• Supports the TCP/IP protocol. • Networking mode: 1. OceanStor Pacific 9550: When the 25GE network is used, the number of network ports can be one or two. Two management network ports can be bonded only in bond4 mode. When the GE network is used, the number of network ports can be only one and bond is not supported. 2. OceanStor Pacific 9950: When the 100GE network is used, the number of network ports can be one or two. Two management network ports can be bonded only in bond4 mode. When the GE network is used, the number of network ports can be one or two. Two management network ports can be bonded only in bond1 mode. 3. OceanStor Pacific 9546: The number of network ports can be one or two. Two management network ports can be bonded only in bond1 mode.
Internal management network	It is integrated with the storage network, and the two networks share ports and IP addresses.

NOTICE

All networks support only IPv4 addresses.

3.2.1.4 Network Solution

This network solution applies to high-performance computing (HPC) scenarios.

Figure 3-1 shows the network solution.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-1 Network solution

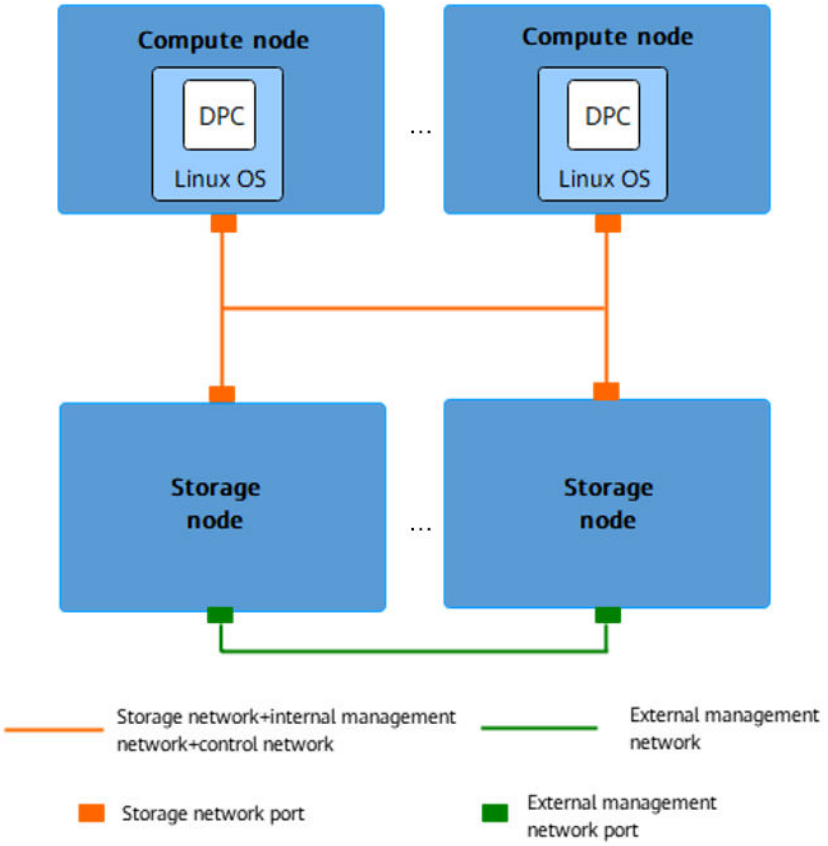


Figure 3-2 shows the physical network.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-2 Physical network

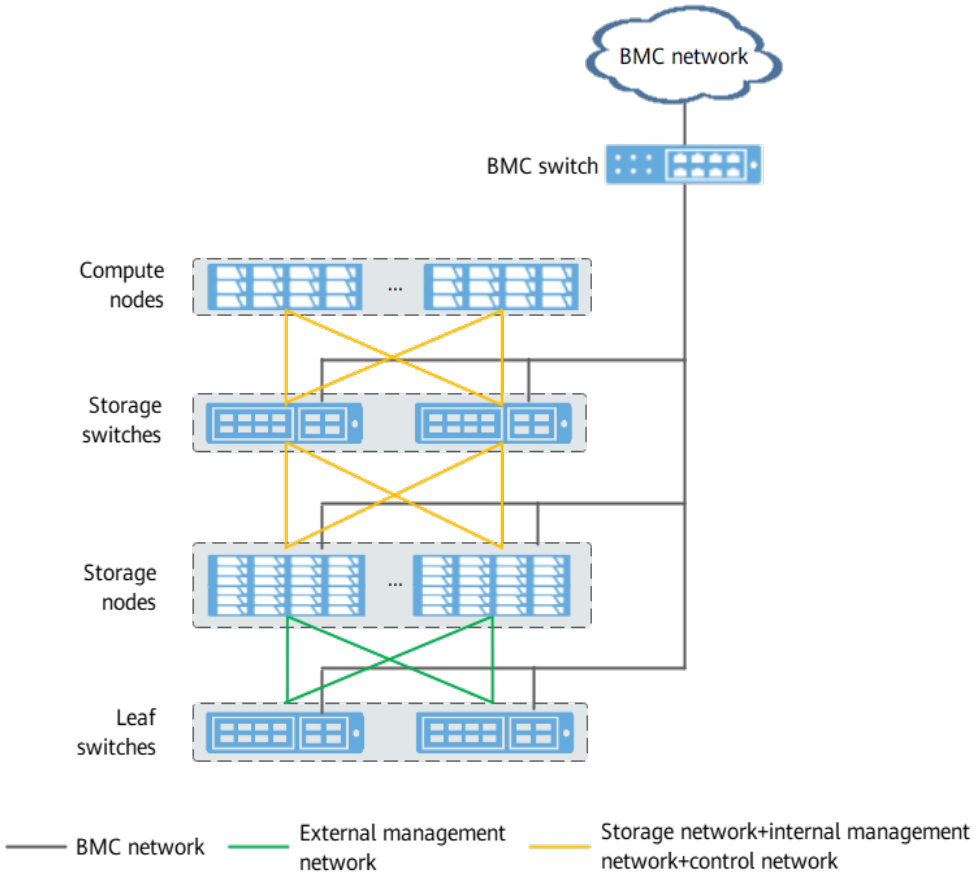


Table 3-3 describes the network requirements and IP address planning.

Table 3-3 Network requirements and IP address planning

Device Type	Requirements	IP Address Planning
Compute node	The storage network of a compute node must be able to communicate with the storage network of a storage node through a distributed gateway.	Planned and allocated by the HCS/HCSO network in a unified manner.

 Copyright © Huawei Technologies Co., Ltd.

Device Type	Requirements	IP Address Planning
Storage/ Management node (the first two storage nodes are also management nodes)	Internal management network: shares network ports and IP addresses with the storage network. External management network: 1. OceanStor Pacific 9550: When the 25GE network is used, each storage node provides two management network ports to connect to the external management network (One or two network ports can be used. When two network ports are used, only bond4 is supported.). When the GE network is used, each storage node provides one management network port to connect to the external management network. 2. OceanStor Pacific 9950: When the 100GE network is used, each storage node provides two management network ports to connect to the external management network (One or two network ports can be used. When two network ports are used, only bond4 is supported.). When the GE network is used, eight storage nodes share two management network ports to connect to the external management network. 3. OceanStor Pacific 9546: Each storage node provides two management network ports to connect to the external management network (One or two network ports can be used. When two network ports	• Configure one floating IP address for the external management network of each cluster for cluster management. • Configure one floating IP address for the internal management network of each cluster. • Configure one management IP address for the external management network on each storage node. • Configure two management IP addresses for the internal management network (same as the IP addresses of the storage network) on each storage node.

 Copyright © Huawei Technologies Co., Ltd.

Device Type	Requirements	IP Address Planning
	are used, only bond1 is supported.). **NOTE** • The external management network is used by users to access DeviceManager and the CLI, and for communication between storage nodes and external HCS/HCSO O&M systems. • The internal management network is used for management data communication between the management and storage nodes. • The IP addresses of the external and internal management networks must be in different network segments.	
	Storage network: Two ports are provided for accessing the storage network using multiple IP addresses.	Planned and allocated by the HCS/HCSO network in a unified manner. **NOTE** If you plan to expand capacity, you are advised to reserve storage network IP addresses for nodes that will be added.
	Control network: If any port on the storage network is used, the control network IP address automatically floats on the storage network ports.	The control network IP address and the storage network IP address cannot be in the same network segment but must be in the same subnet. Example: Storage network IP address: 192.168.1.1/16-192.168.128.255/16 Control network IP address: 192.168.129.1/16-192.168.255.255/16
	BMC network: One port is provided for accessing the BMC network.	Configure one IP address for the BMC network.

 Copyright © Huawei Technologies Co., Ltd.

Device Type	Requirements	IP Address Planning
Storage switch	• Provided by the HCS/HCSO network. • The flow control priority is 32 and the queue is 4. • The oversubscription ratio is 1:1.	Planned and allocated by the HCS/HCSO network in a unified manner.
Leaf switch	• One management network port is provided for accessing the management network. • Switches must be de-stacked.	Configure one management network IP address for each switch.

3.2.1.5 Planning Ports for Nodes

3.2.1.5.1 OceanStor Pacific 9550

Figure 3-3 shows an example of planning ports for a storage node.

Figure 3-3 Example of planning ports for a storage node (using 2-port NICs)

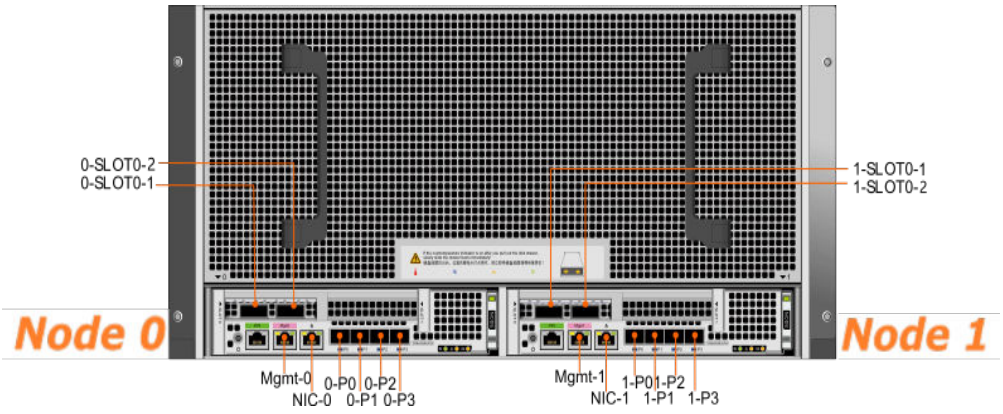


Table 3-4 describes the ports on node *X* (either node between the two nodes in the preceding figure) when the storage network is 100GE RoCE.

Copyright © Huawei Technologies Co., Ltd.

Table 3-4 Port usage

Port Name	Port Type	Access Network	Description
X-SLOT0-1 and *X*-SLOT0-2	100GE	Storage network/ Control network/ Internal management network	The ports connect to the storage switches. **NOTICE** When the storage network uses the RoCE protocol, connect storage ports to switches as follows: • Connect *X*-SLOT0-1 to switch A. • Connect *X*-SLOT0-2 to switch B.
X-P0 and *X*-P1, or NIC-*X*	25GE (*X*-P0 and *X*-P1) or GE (NIC-*X*)	External management network	The ports connect to the leaf switches.
Mgmt-*X*	GE	BMC network	The port connects to the BMC switch.

3.2.1.5.2 OceanStor Pacific 9950

Figure 3-4 shows an example of planning ports for a storage node.

Figure 3-4 Example of planning ports for a storage node

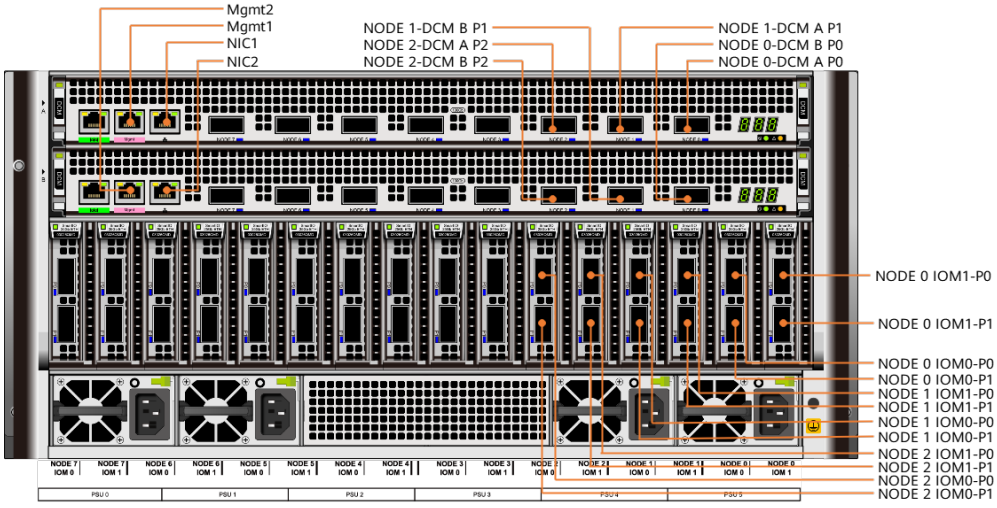


Table 3-5 describes the ports on node *X* (any node among the three nodes in **Figure 3-4**) when the storage network is 100GE RoCE.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-5 Port usage

Port Name	Port Type	Access Network	Description
NODE *X* IOM1-P0 and NODE *X* IOM0-P0	100GE	Storage network/ Control network/ Internal management network	The ports connect to the storage switches.
NODE *X*-DCM A P*X* and NODE *X*-DCM B P*X* or NIC1 and NIC2	100GE (NODE *X*-DCM A P*X* and NODE *X*-DCM B P*X*) or GE (NIC1 and NIC2)	External management network	The ports connect to the leaf switches. **NOTE** NIC1 and NIC2 are aggregated uplink ports of the eight nodes.
Mgmt1 and Mgmt2	GE	BMC network	The ports connect to the BMC switch.

3.2.1.5.3 OceanStor Pacific 9546

- Planning ports for OceanStor Pacific 9546 (One Node per Chassis, Two CPUs per Node):

  Figure 3-5 OceanStor Pacific 9546 (One Node per Chassis, Two CPUs per Node)

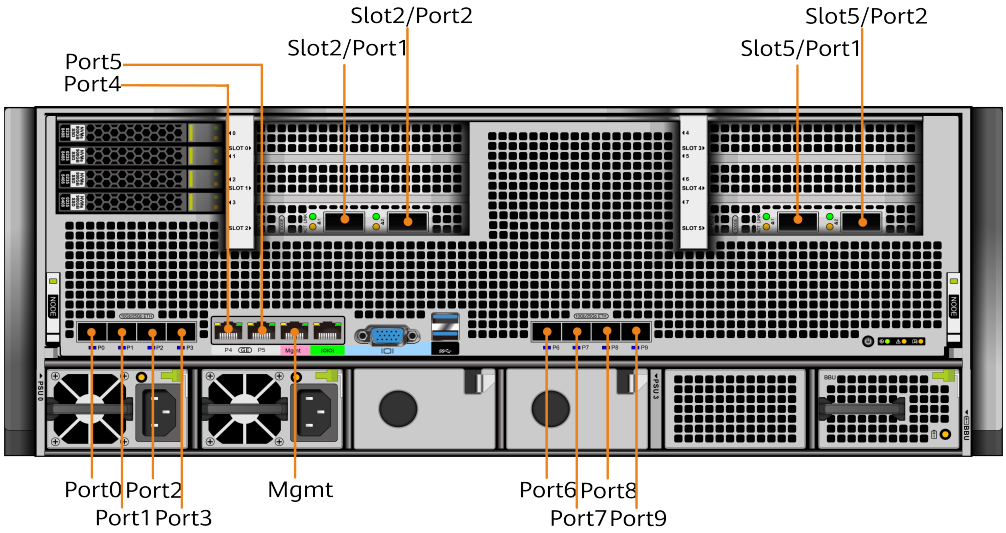
  

  Table 3-6 describes the ports on a node when the storage network is 100GE RoCE.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-6 Port usage

Port Name	Port Type	Access Network	Description
Slot2/Port1 and Slot2/Port2	100GE	Storage network/Control network/Internal management network	The ports connect to the storage switches.
Port4 and Port5	GE	External management network	The ports connect to the leaf switches.
Mgmt	GE	BMC network	The port connects to the BMC switch.

- Planning ports for OceanStor Pacific 9546 (Two Nodes per Chassis, Two CPUs per Node):

Figure 3-6 OceanStor Pacific 9546 (Two Nodes per Chassis, Two CPUs per Node)

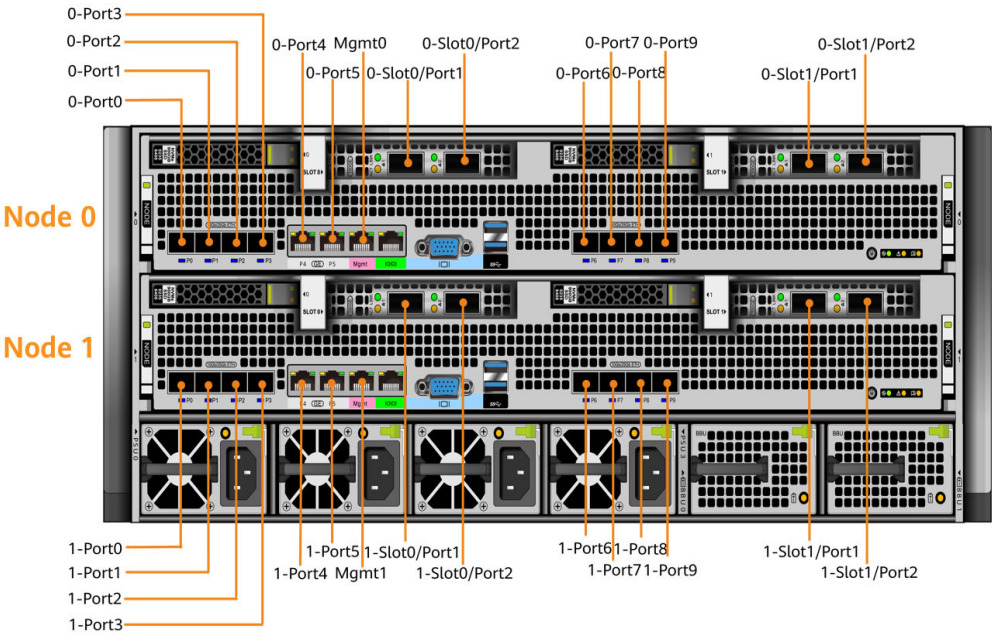


Table 3-7 describes the ports on node *X* (either node between the two nodes in Figure 3-6) when the storage network is 100GE RoCE.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-7 Port usage

Port Name	Port Type	Access Network	Description
X-Slot0/Port1 and *X*-Slot0/Port2	100GE	Storage network/Control network/Internal management network	The ports connect to the storage switches.
X-Port4 and *X*-Port5	GE	External management network	The ports connect to the leaf switches.
Mgmt*X*	GE	BMC network	The port connects to the BMC switch.

- Planning ports for OceanStor Pacific 9546 (Two Nodes per Chassis, One CPU per Node):

Figure 3-7 Example of planning ports for OceanStor Pacific 9546 (Two Nodes per Chassis, One CPU per Node)

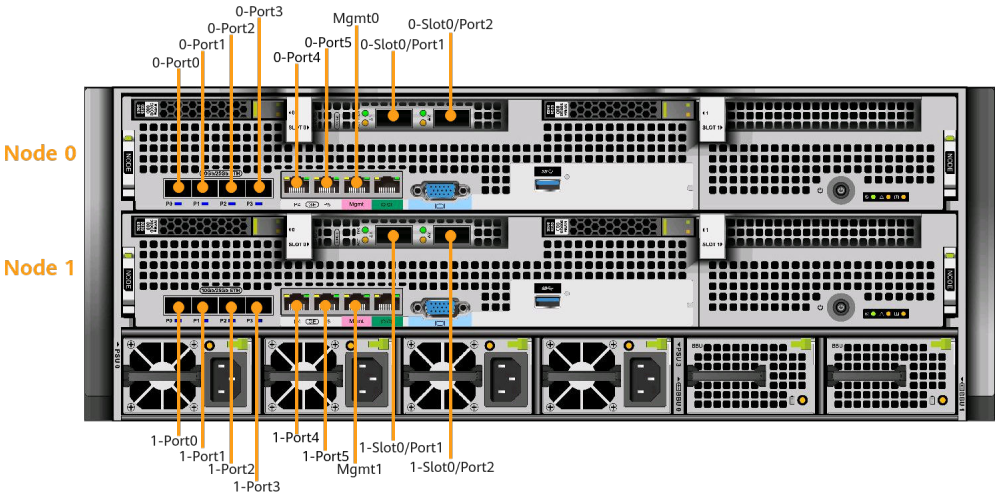


Table 3-8 describes the ports on node *X* (either node between the two nodes in Figure 3-7) when the storage network is 100GE RoCE.

Table 3-8 Port usage

Port Name	Port Type	Access Network	Description
X-Slot0/Port1 and *X*-Slot0/Port2	100GE	Storage network/Control network/Internal management network	The ports connect to the storage switches.

 Copyright © Huawei Technologies Co., Ltd.

Port Name	Port Type	Access Network	Description
X-Port4 and *X*-Port5	GE	External management network	The ports connect to the leaf switches.
Mgmt*X*	GE	BMC network	The port connects to the BMC switch.

3.2.1.6 Network Example

3.2.1.6.1 Network Example for OceanStor Pacific 9550/OceanStor Pacific 9546

The number of IP addresses required by each network is as follows:

- Number of management network IP addresses = Number of storage switches + Number of leaf switches + Number of BMC switches + Number of management switches + Number of compute nodes + Number of storage nodes (excluding the storage nodes deployed on the same servers as the management nodes) + Number of management nodes x 2 + 2
- Number of BMC network IP addresses = Number of compute nodes + Number of storage nodes
- Number of storage network IP addresses = Number of compute nodes (bond) + Number of storage nodes x 3

This section describes the network IP address planning when two compute nodes, four storage nodes (management nodes are deployed on the same servers as the storage nodes), two storage switches, two leaf switches, one management switch, and one BMC switch are deployed.

NOTE

Each OceanStor Pacific 9550/OceanStor Pacific 9546 device has two storage nodes.

Management Network

Table 3-9 describes the IP address planning for the management network.

Table 3-9 IP address planning for the management network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Floating management IP address for the external management network	Logical management port	10.110.100.100	255.255.255.0	10.110.100.1

Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Floating management IP address for the internal management network	Logical management port	172.16.0.12	255.255.255.0	10.110.100.1
Management network IP address for compute node 1	Determined by users	192.168.0.11 (shared with a storage network IP address)	255.255.255.0	192.168.0.1
Management network IP address for compute node 2	Determined by users	192.168.0.12 (shared with a storage network IP address)	255.255.255.0	192.168.0.1
Internal management network IP address for storage node 1 (management node 1)	Shared with a storage network port	172.16.0.13 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
Internal management network IP address for storage node 2 (management node 2)	Shared with a storage network port	172.16.0.15 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
Management network IP address for storage node 3	Shared with a storage network port	172.16.0.17 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
Management network IP address for storage node 4	Shared with a storage network port	172.16.0.19 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
External management network IP address for storage node 1 (management node 1)	OceanStor Pacific 9550: shared *X*-P0 and *X*-P1 OceanStor Pacific 9546: shared Port4 and Port5	10.110.100.106	255.255.255.0	10.110.100.1

 Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
External management network IP address for storage node 2 (management node 2)	OceanStor Pacific 9550: shared *X*-P0 and *X*-P1 OceanStor Pacific 9546: shared Port4 and Port5	10.110.100.107	255.255.255.0	10.110.100.1
Management network IP address for the BMC switch	MEth0/0/0	10.110.100.110	255.255.255.0	10.110.100.1
Management network IP address for the management switch	MEth0/0/0	10.110.100.112	255.255.255.0	10.110.100.1
Management network IP address for storage switch 1	MEth0/0/0	10.110.100.113	255.255.255.0	10.110.100.1
Management network IP address for storage switch 2	MEth0/0/0	10.110.100.114	255.255.255.0	10.110.100.1
Management network IP address for leaf switch 1	MEth0/0/0	10.110.100.115	255.255.255.0	10.110.100.1
Management network IP address for leaf switch 2	MEth0/0/0	10.110.100.116	255.255.255.0	10.110.100.1

BMC Network

Table 3-10 describes the IP address planning for the BMC network.

Copyright © Huawei Technologies Co., Ltd.

Table 3-10 IP address planning for the BMC network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
BMC network IP address for compute node 1	Determined by users	10.110.100.11	255.255.255.0	10.110.100.1
BMC network IP address for compute node 2	Determined by users	10.110.100.12	255.255.255.0	10.110.100.1
BMC network IP address for storage node 1	Mgmt	10.110.100.13	255.255.255.0	10.110.100.1
BMC network IP address for storage node 2	Mgmt	10.110.100.14	255.255.255.0	10.110.100.1
BMC network IP address for storage node 3	Mgmt	10.110.100.15	255.255.255.0	10.110.100.1
BMC network IP address for storage node 4	Mgmt	10.110.100.16	255.255.255.0	10.110.100.1

Storage Network

Table 3-11 describes the IP address planning for the storage network.

Table 3-11 IP address planning for the storage network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Storage network IP address for compute node 1 (bond is used as an example)	Determined by users	192.168.0.11	255.255.255.0	192.168.0.1

Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Storage network IP address for compute node 2 (bond is used as an example)	Determined by users	192.168.0.12	255.255.255.0	192.168.0.1
Storage network IP addresses for storage node 1	Storage network ports providing multiple IP addresses	172.16.0.13	255.255.255.0	172.16.0.1
		172.16.0.14	255.255.255.0	172.16.0.1
Storage network IP addresses for storage node 2	Storage network ports providing multiple IP addresses	172.16.0.15	255.255.255.0	172.16.0.1
		172.16.0.16	255.255.255.0	172.16.0.1
Storage network IP addresses for storage node 3	Storage network ports providing multiple IP addresses	172.16.0.17	255.255.255.0	172.16.0.1
		172.16.0.18	255.255.255.0	172.16.0.1
Storage network IP addresses for storage node 4	Storage network ports providing multiple IP addresses	172.16.0.19	255.255.255.0	172.16.0.1
		172.16.0.20	255.255.255.0	172.16.0.1
Control network IP address for storage node 1	Storage network ports providing multiple IP addresses	172.16.0.129	255.255.255.0	172.16.0.1
Control network IP address for storage node 2	Storage network ports providing multiple IP addresses	172.16.0.130	255.255.255.0	172.16.0.1
Control network IP address for storage node 3	Storage network ports providing multiple IP addresses	172.16.0.131	255.255.255.0	172.16.0.1

 Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Control network IP address for storage node 4	Storage network ports providing multiple IP addresses	172.16.0.132	255.255.255.0	172.16.0.1

3.2.1.6.2 Network Example for OceanStor Pacific 9950

The number of IP addresses required by each network is as follows:

- Number of management network IP addresses = Number of storage switches + Number of leaf switches + Number of BMC switches + Number of management switches + Number of compute nodes + Number of storage nodes (excluding the storage nodes deployed on the same servers as the management nodes) + Number of management nodes x 2 + Number of data cluster modules + 2
- Number of BMC network IP addresses = Number of compute nodes + Number of storage nodes
- Number of storage network IP addresses = Number of compute nodes (bond) + Number of storage nodes x 3

This section describes a network IP address planning example when two compute nodes, four storage nodes (housed in one OceanStor Pacific 9950 device), two management nodes (deployed on the same servers as storage nodes), two storage switches, two leaf switches, one management switch, and one BMC switch are deployed.

NOTE

Each OceanStor Pacific 9950 device has eight storage nodes and two data cluster modules.

Management Network

Table 3-12 describes the IP address planning for the management network.

Table 3-12 IP address planning for the management network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Floating management IP address for the external management network	Logical management port	10.110.100.100	255.255.255.0	10.110.100.1

Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Floating management IP address for the internal management network	Logical management port	172.16.0.12	255.255.255.0	172.16.0.1
Management network IP address for compute node 1	Determined by users	192.168.0.11 (shared with a storage network IP address)	255.255.255.0	192.168.0.1
Management network IP address for compute node 2	Determined by users	192.168.0.12 (shared with a storage network IP address)	255.255.255.0	192.168.0.1
Internal management network IP address for storage node 1 (management node 1)	Shared with a storage network port	172.16.0.13 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
Internal management network IP address for storage node 2 (management node 2)	Shared with a storage network port	172.16.0.15 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
Management network IP address for storage node 3	Shared with a storage network port	172.16.0.17 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
Management network IP address for storage node 4	Shared with a storage network port	172.16.0.19 (shared with a storage network IP address)	255.255.255.0	172.16.0.1

 Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
External management network IP address for storage node 1 (management node 1)	Shared NIC1-1 and NIC1-2	10.110.100.106	255.255.255.0	10.110.100.1
External management network IP address for storage node 2 (management node 2)	Shared NIC1-1 and NIC1-2	10.110.100.107	255.255.255.0	10.110.100.1
Management network IP address for the BMC switch	MEth0/0/0	10.110.100.110	255.255.255.0	10.110.100.1
Management network IP address for the management switch	MEth0/0/0	10.110.100.112	255.255.255.0	10.110.100.1
Management network IP address for storage switch 1	MEth0/0/0	10.110.100.113	255.255.255.0	10.110.100.1
Management network IP address for storage switch 2	MEth0/0/0	10.110.100.114	255.255.255.0	10.110.100.1
Management network IP address for leaf switch 1	MEth0/0/0	10.110.100.115	255.255.255.0	10.110.100.1
Management network IP address for leaf switch 2	MEth0/0/0	10.110.100.116	255.255.255.0	10.110.100.1

 Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Management network IP address for data cluster module 1	Shared NIC1-1 and NIC1-2	10.110.100.117	255.255.255.0	10.110.100.1
Management network IP address for data cluster module 2	Shared NIC1-1 and NIC1-2	10.110.100.118	255.255.255.0	10.110.100.1

BMC Network

Table 3-13 describes the IP address planning for the BMC network.

Table 3-13 IP address planning for the BMC network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
BMC network IP address for compute node 1	Determined by users	10.110.100.11	255.255.255.0	10.110.100.1
BMC network IP address for compute node 2	Determined by users	10.110.100.12	255.255.255.0	10.110.100.1
BMC network IP address for storage node 1	Shared Mgmt1 and Mgmt2	10.110.100.13	255.255.255.0	10.110.100.1
BMC network IP address for storage node 2	Shared Mgmt1 and Mgmt2	10.110.100.14	255.255.255.0	10.110.100.1
BMC network IP address for storage node 3	Shared Mgmt1 and Mgmt2	10.110.100.15	255.255.255.0	10.110.100.1
BMC network IP address for storage node 4	Shared Mgmt1 and Mgmt2	10.110.100.16	255.255.255.0	10.110.100.1

Copyright © Huawei Technologies Co., Ltd.

Storage Network

Table 3-14 describes the IP address planning for the storage network.

Table 3-14 IP address planning for the storage network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Storage network IP address for compute node 1 (bond is used as an example)	Determined by users	192.168.0.11	255.255.255.0	192.168.0.1
Storage network IP address for compute node 2 (bond is used as an example)	Determined by users	192.168.0.12	255.255.255.0	192.168.0.1
Storage network IP addresses for storage node 1	Storage network ports providing multiple IP addresses	172.16.0.13	255.255.255.0	172.16.0.1
		172.16.0.14	255.255.255.0	172.16.0.1
Storage network IP addresses for storage node 2	Storage network ports providing multiple IP addresses	172.16.0.15	255.255.255.0	172.16.0.1
		172.16.0.16	255.255.255.0	172.16.0.1
Storage network IP addresses for storage node 3	Storage network ports providing multiple IP addresses	172.16.0.17	255.255.255.0	172.16.0.1
		172.16.0.18	255.255.255.0	172.16.0.1
Storage network IP addresses for storage node 4	Storage network ports providing multiple IP addresses	172.16.0.19	255.255.255.0	172.16.0.1
		172.16.0.20	255.255.255.0	172.16.0.1

Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Control network IP address for storage node 1	Storage network ports providing multiple IP addresses	172.16.0.129	255.255.255.0	172.16.0.1
Control network IP address for storage node 2	Storage network ports providing multiple IP addresses	172.16.0.130	255.255.255.0	172.16.0.1
Control network IP address for storage node 3	Storage network ports providing multiple IP addresses	172.16.0.131	255.255.255.0	172.16.0.1
Control network IP address for storage node 4	Storage network ports providing multiple IP addresses	172.16.0.132	255.255.255.0	172.16.0.1

3.2.2 File Service (Standard Protocol Scenario)

3.2.2.1 Overview

Network Introduction

The following networks are involved for OceanStor Pacific series in the standard protocol scenario:

- BMC network

  The BMC network connects to Mgmt ports of nodes to enable remote device management.
- Management network
  - The external management network is used by users to access DeviceManager and the CLI, and for communication between storage nodes and external HCS/HCSO O&M systems.
  - The internal management network is used for management data communication between the management and storage nodes.
- Control network
  - Transmits control messages in the system.
  - Adopts a floating IP address that floats among storage network ports on nodes.

 Copyright © Huawei Technologies Co., Ltd.

- Storage network

  The front-end storage network and back-end storage network are shared for data communication between storage nodes and between DPC and OSD.

- Service network

  Enables data communication between storage nodes and users' service network and supports NFS/CIFS interface protocol.

3.2.2.2 Networking Scenarios

Table 3-15 shows the standard protocol (NFS/CIFS) networking scenarios supported by OceanStor Pacific 9550, OceanStor Pacific 9546, OceanStor Pacific 9350, and OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node).

Select a service type based on the actual service scenario to achieve optimal system performance. The options are **General** and **Intelligent video and image**.

- **General**: applies to high-performance computing (HPC) scenarios (such as meteorology, genetics, and oil industries) and big data analysis scenarios (such as 5G log retention and analysis), providing the file, object, and HDFS storage services for upper-layer applications.
- **Intelligent video and image**: applies to video and image storage industries, including video stream and checkpoint image storage scenarios.

Table 3-15 Networking scenarios

Device Name	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example	Service Network (NIC Example)	Service Switch Example
OceanStor Pacific 9550	OceanStor Pacific 9550	GE (LOM)	Switch that supports GE	25GE RoCE (LOM)	CE6865	10GE/ 25GE TCP (Hi1822)	CE6865
				25GE TCP (LOM)	CE6865	10GE/ 25GE TCP (Hi1822)	CE6865
OceanStor Pacific 9350	OceanStor Pacific 9350	GE (LOM)	Switch that supports GE	25GE RoCE (LOM)	CE6865	10GE/ 25GE TCP (Hi1822)	CE6865
				25GE TCP (LOM)	CE6865	10GE/ 25GE TCP (Hi1822)	CE6865

Copyright © Huawei Technologies Co., Ltd.

Device Name	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example	Service Network (NIC Example)	Service Switch Example
OceanStor Pacific 9546	3.2.2.5.2 OceanStor Pacific 9546	GE (LOM)	Switch that supports GE	25GE RoCE (LOM)	CE6865	10GE/25GE TCP (Hi1822 V120)	CE6865
				25GE TCP (LOM)	CE6865	10GE/25GE TCP (Hi1822 V120)	CE6865
				10GE RoCE (LOM)	CE6865	10GE TCP (Hi1822 V120)	CE6865
				10GE TCP (LOM)	CE6865	10GE TCP (Hi1822 V120)	CE6865
OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node)	3.2.2.5.3 OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node)	GE (LOM)	Switch that supports GE	25GE RoCE (LOM)	CE6865	10GE/25GE TCP (Hi1822 V120)	CE6865
				25GE TCP (LOM)	CE6865	10GE/25GE TCP (Hi1822 V120)	CE6865
Tiering scenario: OceanStor Pacific 9546 + OceanStor Pacific 9550	3.2.2.5.2 OceanStor Pacific 9546	GE (LOM)	Switch that supports GE	25GE RoCE (LOM)	CE6865	10GE/25GE TCP (Hi1822)	CE6865

Copyright © Huawei Technologies Co., Ltd.

Device Name	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example	Service Network (NIC Example)	Service Switch Example
	OceanStor Pacific 9550	GE (LOM)	Switch that supports GE	25GE RoCE (LOM)	CE6865	10GE/ 25GE TCP (Hi1822)	CE6865
Tiering scenario: OceanStor Pacific 9546 + OceanStor Pacific 9550	3.2.2.5.2 OceanStor Pacific 9546	GE (LOM)	Switch that supports GE	25GE TCP (LOM)	CE6865	10GE/ 25GE TCP (Hi1822)	CE6865
	OceanStor Pacific 9550	GE (LOM)	Switch that supports GE	25GE TCP (LOM)	CE6865	10GE/ 25GE TCP (Hi1822)	CE6865

NOTE

- If the 10GE network uses 25GE NICs, optical modules must be configured. The rate of the storage optical modules must be the same as that of the switch optical modules.
- OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node) and OceanStor Pacific 9350 are used in the intelligent video and image scenario.
- The Hi1822 and Hi1822V120 NICs have four ports (when the Hi1822V120 NIC is used, only the four-port NIC is used). Only the first two ports of the NICs are used.

3.2.2.3 Network Requirements

In the standard protocol scenario, front- and back-end storage networks are shared. **Table 3-16** describes the specific network requirements.

Table 3-16 Network requirements

Network Type	Network Requirements
BMC network	• A BMC network can be a GE network. • The number of BMC network ports on each storage node can be one or two.
Service network	The TCP/IP protocol is supported. It supports 10GE/25GE networks and allows you to configure only bond4.

Copyright © Huawei Technologies Co., Ltd.

Network Type	Network Requirements
Storage network	• The RoCE protocol is supported. RoCE supports the 10GE (OceanStor Pacific 9546) and 25GE (OceanStor Pacific 9550/OceanStor Pacific 9546/OceanStor Pacific 9350/ OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node)) networks, and only multiple IP addresses can be configured. **NOTE** When the storage network does not use the bond network, each port on the storage network can be bonded to one IP address. • The TCP/IP protocol is supported. TCP/IP supports the 10GE (OceanStor Pacific 9546) and 25GE (OceanStor Pacific 9550/OceanStor Pacific 9546/OceanStor Pacific 9350/OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node)) networks, and only bond4 can be configured. • The storage networks of all nodes use the same VLAN ID.
Control network	If the storage network uses multiple IP addresses, select a port on the storage network to configure one floating IP address for the control network. The control network and the storage network can be in the same subnet (recommended) or different subnets. If they are in the same subnet, they must use different IP address segments.
External management network	• Supports the TCP/IP protocol. • Networking mode: 1. OceanStor Pacific 9550/OceanStor Pacific 9350: The number of network ports can be only one and bond is not supported. 2. OceanStor Pacific 9546/OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node): The number of network ports can be one or two. Two management network ports can be bonded only in bond1 mode.
Internal management network	It is integrated with the storage network, and the two networks share ports and IP addresses.

NOTICE

All networks support only IPv4 addresses.

3.2.2.4 Network Solution

Figure 3-8 shows the network solution.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-8 Network solution

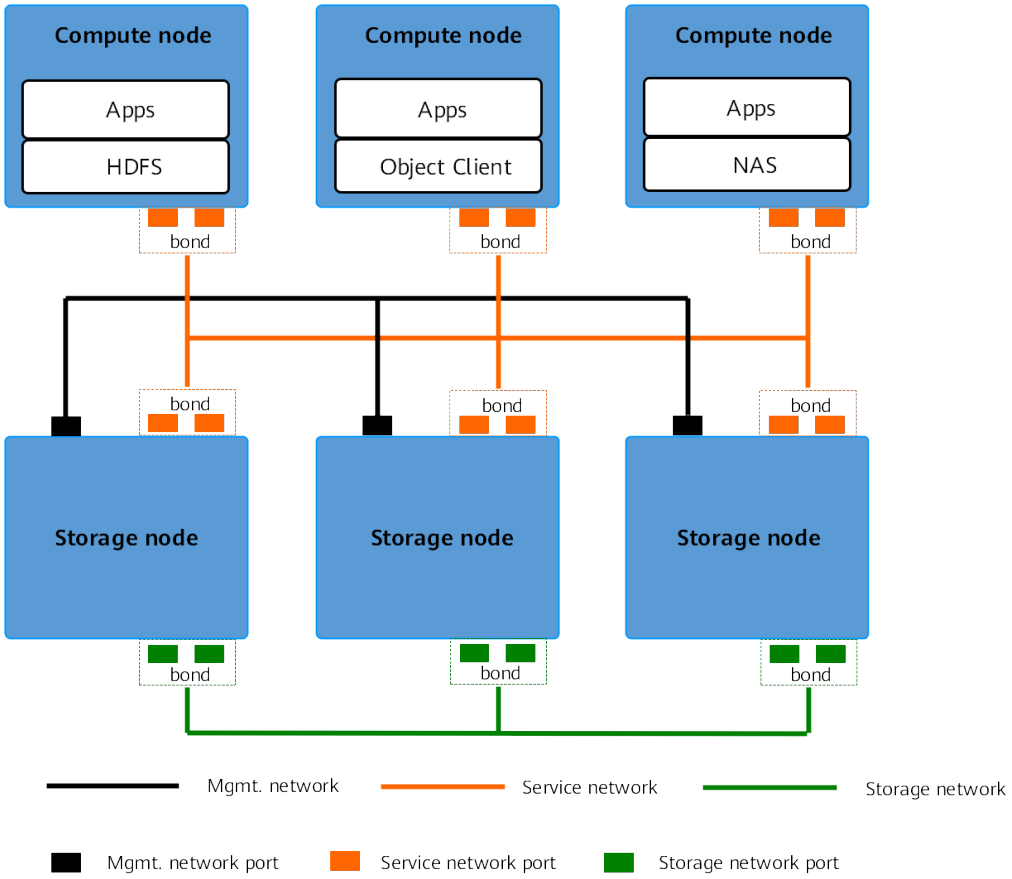


Figure 3-9 shows the physical network.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-9 Physical network

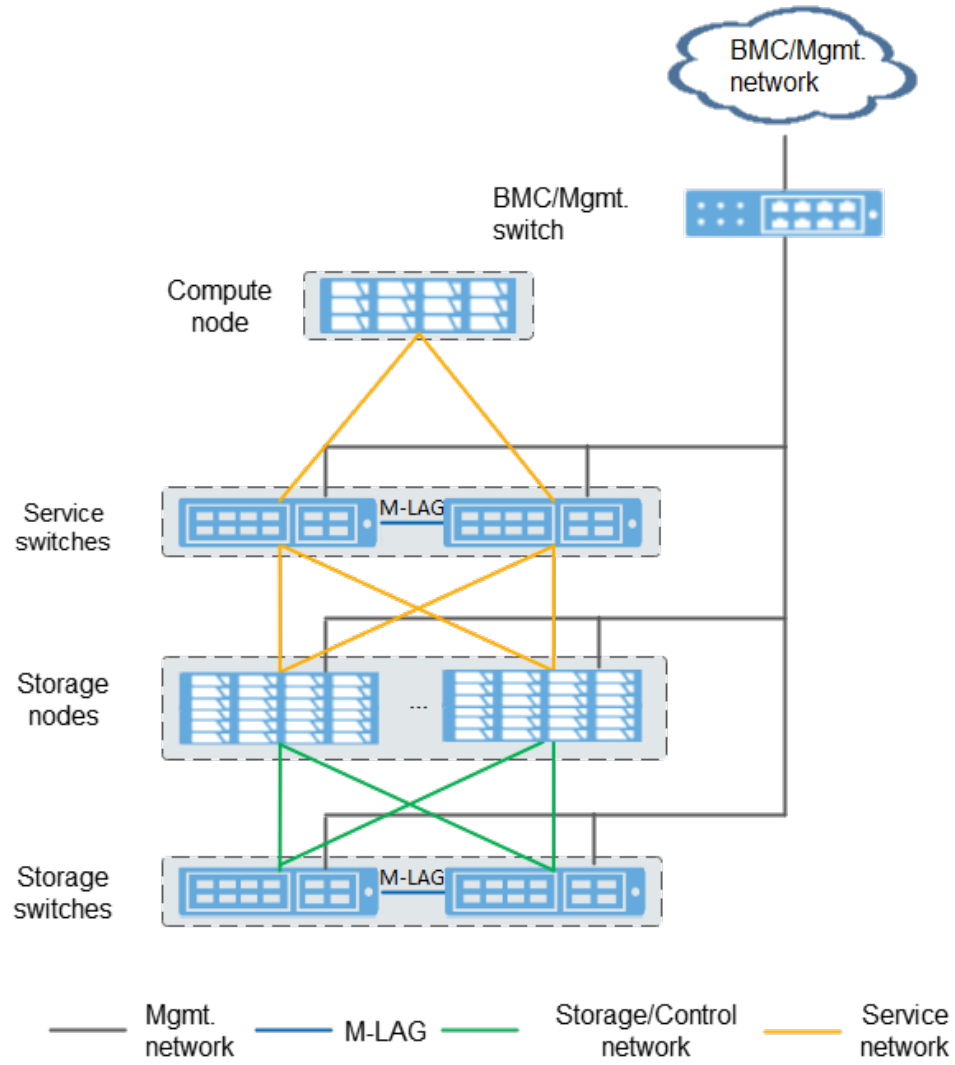


Table 3-17 describes the network requirements and IP address planning.

Table 3-17 Network requirements and IP address planning

Device Type	Requirements	IP Address Planning
Compute node	The storage network of a compute node must be able to communicate with the storage network of a storage node through a distributed gateway.	Planned and allocated by the HCS/HCSO network in a unified manner.

 Copyright © Huawei Technologies Co., Ltd.

Device Type	Requirements	IP Address Planning
Storage/ Management node (the first two storage nodes are also management nodes)	Internal management network: shares network ports and IP addresses with the storage network. External management network: 1. OceanStor Pacific 9550/ OceanStor Pacific 9350: Each storage node provides one management network port to connect to the external management network. 2. OceanStor Pacific 9546/ OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node): Each storage node provides two management network ports to connect to the external management network (One or two network ports can be used. When two network ports are used, only bond1 is supported.). **NOTE** • The external management network is used by users to access DeviceManager and the CLI, and for communication between storage nodes and external HCS/HCSO O&M systems. • The internal management network is used for management data communication between the management and storage nodes. • The IP addresses of the external and internal management networks must be in different network segments.	• Configure one floating IP address for the external management network of each cluster for cluster management. • Configure one floating IP address for the internal management network of each cluster. • Configure one management IP address for the external management network on each storage node. • Configure two management IP addresses for the internal management network (same as the IP addresses of the storage network) on each storage node.

 Copyright © Huawei Technologies Co., Ltd.

Device Type	Requirements	IP Address Planning
	Storage network: Provides two ports to connect to the storage network using multiple IP addresses (RoCE) or bond4 (TCP).	Planned and allocated by the HCS/HCSO network in a unified manner. **NOTE** If you plan to expand capacity, you are advised to reserve storage network IP addresses for nodes that will be added.
	Control network (when the storage network uses the RoCE protocol or multiple IP addresses for networking): If any port on the storage network is used, the control network IP address automatically floats on the storage network ports.	The control network IP address and the storage network IP address cannot be in the same network segment but must be in the same subnet.
	Service network: Two ports are provided to form bond4 for accessing the service network. **NOTE** • The Hi1822 and Hi1822V120 NICs have four ports (when the Hi1822V120 NIC is used, only the four-port NIC is used). Only the first two ports of the NICs are used.	Configure one VTEP IP address for establishing a VXLAN tunnel with compute nodes (ECS).
	BMC network: One port is provided for accessing the BMC network.	Configure one IP address for the BMC network.
Storage switch	• Provided by the HCS/HCSO network. • The flow control priority is 32 and the queue is 4. • The oversubscription ratio is 1:1.	Planned and allocated by the HCS/HCSO network in a unified manner.

 Copyright © Huawei Technologies Co., Ltd.

Device Type	Requirements	IP Address Planning
Leaf switch	• One management network port is provided for accessing the management network. • Switches must be de-stacked.	Configure one management network IP address for each switch. **NOTE** In the standard protocol scenario, if the uplink traffic to leaf switches contains both service network traffic and management network traffic, the uplink bandwidth needs to be calculated based on the number of nodes.

3.2.2.5 Planning Ports for Nodes

3.2.2.5.1 OceanStor Pacific 9550 and OceanStor Pacific 9350

Figure 3-10 shows an example of planning ports for a storage node.

Figure 3-10 Example of planning ports for a storage node (using 4-port NICs)

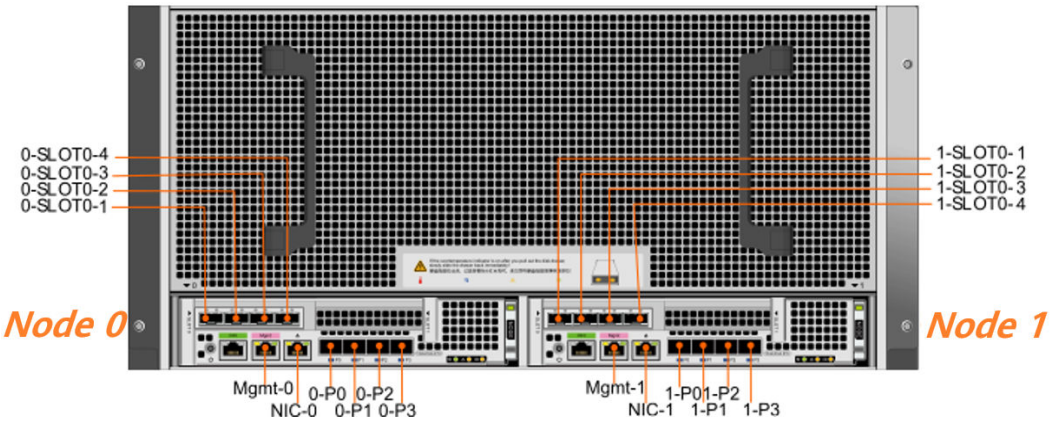


Table 3-18 describes the ports on node *X* (either node between the two nodes in **Figure 3-10**) when the service network is 10GE or 25GE and the storage network is 25GE.

Table 3-18 Port usage

Port Name	Port Type	Access Network	Description
X-SLOT0-1 and *X*-SLOT0-2	10GE or 25GE	Service network	The ports connect to the service switches.

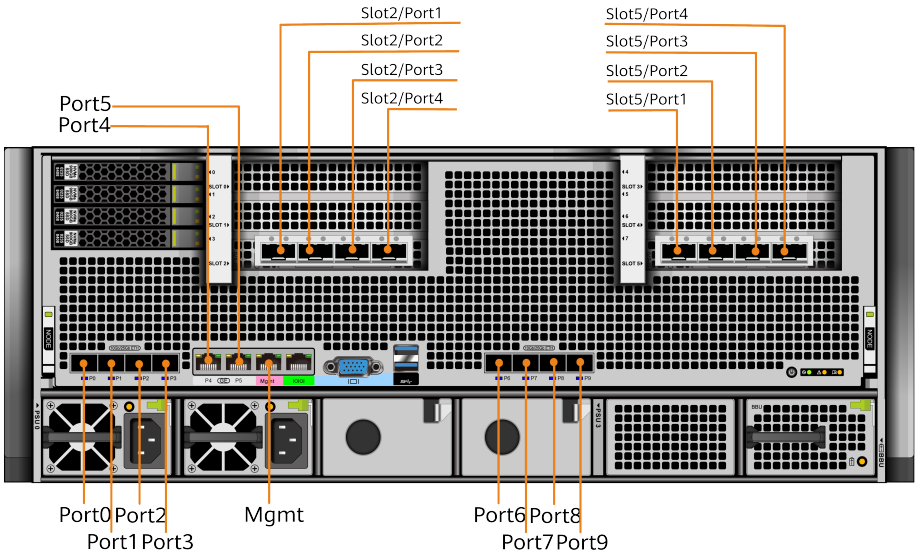
Copyright © Huawei Technologies Co., Ltd.

Port Name	Port Type	Access Network	Description
X-P0 and *X*-P1	25GE	Storage network/ Control network/ Internal management network	The ports connect to the storage switches. **NOTICE** When the storage network uses the RoCE protocol, connect storage ports to switches as follows: • Connect *X*-P0 to switch A. • Connect *X*-P1 to switch B.
NIC-*X*	GE	External management network	The ports connect to the leaf switches.
Mgmt-X	GE	BMC network	The port connects to the BMC switch.

3.2.2.5.2 OceanStor Pacific 9546

- Planning ports for OceanStor Pacific 9546 (One Node per Chassis, Two CPUs per Node):

  Figure 3-11 Example of planning ports for OceanStor Pacific 9546 (One Node per Chassis, Two CPUs per Node)



 Copyright © Huawei Technologies Co., Ltd.

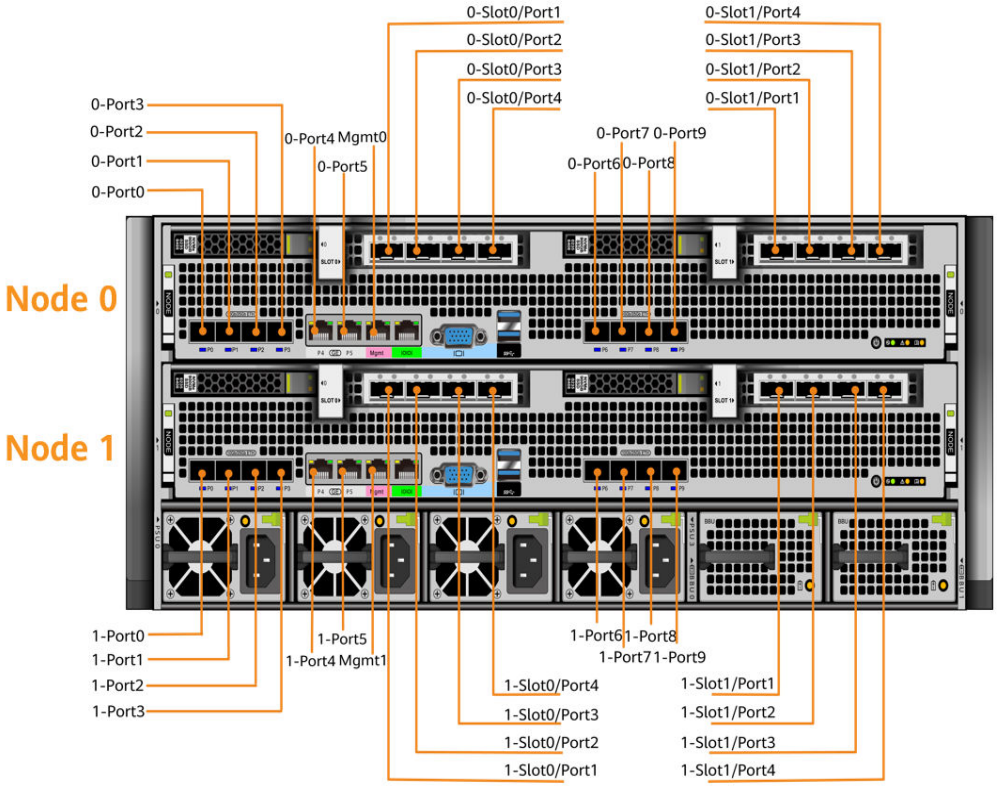
Table 3-19 describes the ports on a node when the storage network is 25GE.

Table 3-19 Port usage

Port Name	Port Type	Access Network	Description
Slot2/Port1 and Slot2/Port2	10GE or 25GE	Service network	The ports connect to the service switches.
Port0 and Port1	25GE	Storage network/Control network/Internal management network	The ports connect to the storage switches.
Port4 and Port5	GE	External management network	The ports connect to the leaf switches.
Mgmt	GE	BMC network	The port connects to the BMC switch.

- Planning ports for OceanStor Pacific 9546 (Two Nodes per Chassis, Two CPUs per Node):

Figure 3-12 Example of planning ports for OceanStor Pacific 9546 (Two Nodes per Chassis, Two CPUs per Node)



 Copyright © Huawei Technologies Co., Ltd.

Table 3-20 describes the ports on node *X* (either node between the two nodes in **Figure 3-12**) when the storage network is 10GE or 25GE.

Table 3-20 Port usage

Port Name	Port Type	Access Network	Description
X-Slot0/Port1 and *X*-Slot0/Port2	10GE or 25GE	Service network	The ports connect to the service switches.
X-Port0 and *X*-Port1	10GE or 25GE	Storage network/Control network/Internal management network	The ports connect to the storage switches.
X-Port4 and *X*-Port5	GE	External management network	The ports connect to the leaf switches.
Mgmt*X*	GE	BMC network	The port connects to the BMC switch.

- Planning ports for OceanStor Pacific 9546 (Two Nodes per Chassis, One CPU per Node):

Figure 3-13 Example of planning ports for OceanStor Pacific 9546 (Two Nodes per Chassis, One CPU per Node)

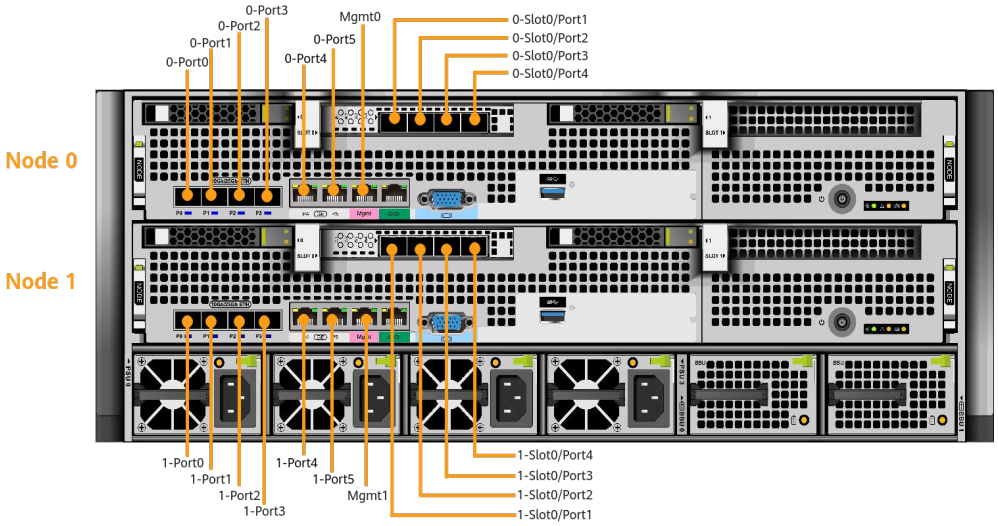


Table 3-21 describes the ports on node *X* (either node between the two nodes in **Figure 3-13**) when the storage network is 10GE or 25GE.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-21 Port usage

Port Name	Port Type	Access Network	Description
X-Slot0/Port1 and *X*-Slot0/Port2	10GE or 25GE	Service network	The ports connect to the service switches.
X-Port0 and *X*-Port1	10GE or 25GE	Storage network/Control network/Internal management network	The ports connect to the storage switches.
X-Port4 and *X*-Port5	GE	External management network	The ports connect to the leaf switches.
Mgmt*X*	GE	BMC network	The port connects to the BMC switch.

3.2.2.5.3 OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node)

Figure 3-14 OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node)

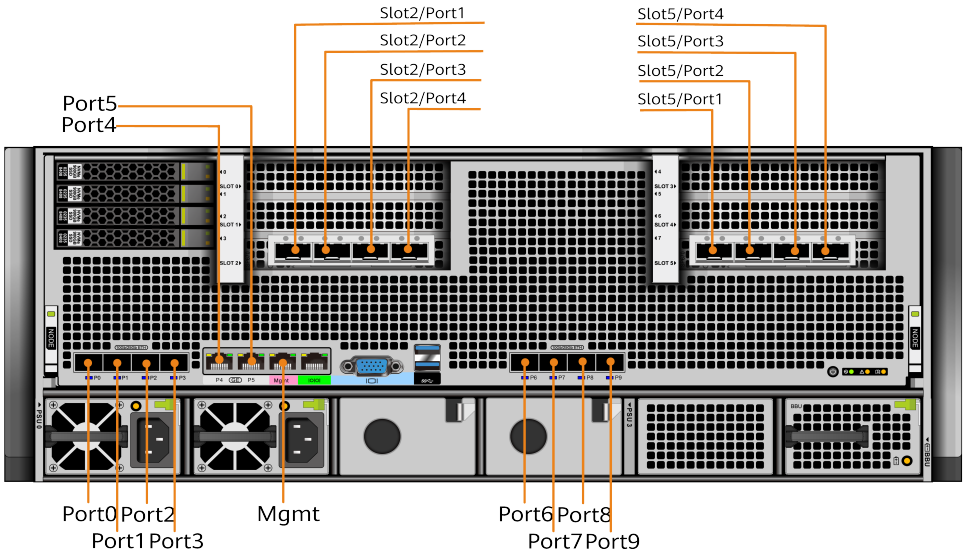


Table 3-22 describes the ports on a node when the storage network is 25GE.

Copyright © Huawei Technologies Co., Ltd.

Table 3-22 Port usage

Port Name	Port Type	Access Network	Description
Slot2/Port1 and Slot2/Port2	10GE or 25GE	Service network	The ports connect to the service switches.
Port0 and Port1	25GE	Storage network/ Control network/ Internal management network	The ports connect to the storage switches.
Port4 and Port5	GE	External management network	The ports connect to the leaf switches.
Mgmt	GE	BMC network	The port connects to the BMC switch.

3.2.2.6 Network Example

3.2.2.6.1 Network Example for OceanStor Pacific 9550/OceanStor Pacific 9546/ OceanStor Pacific 9350/OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node)

The number of IP addresses required by each network is as follows:

- Number of management network IP addresses = Number of service switches + Number of storage switches + Number of leaf switches + Number of BMC switches + Number of management switches + Number of storage nodes (excluding the storage nodes deployed on the same servers as the management nodes) + Number of management nodes x 2 + 2
- Number of BMC network IP addresses = Number of storage nodes
- Number of storage network IP addresses = Number of storage nodes x 3
- Number of file service network IP addresses (bond network) = Number of storage nodes x Number of access zones + Number of subnets

This section describes the network IP address planning when four storage nodes (management nodes are deployed on the same servers as the storage nodes), two storage switches, two service switches, two leaf switches, one management switch, and one BMC switch are deployed.

NOTE

Each OceanStor Pacific 9550/OceanStor Pacific 9546/OceanStor Pacific 9350 device has two storage nodes.

Management Network

Table 3-23 describes the IP address planning for the management network.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-23 IP address planning for the management network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Floating management IP address for the external management network	Logical management port	10.110.100.100	255.255.255.0	10.110.100.1
Floating management IP address for the internal management network	Logical management port	172.16.0.12	255.255.255.0	10.110.100.1
Internal management network IP address for storage node 1 (management node 1)	Shared with a storage network port	172.16.0.13 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
Internal management network IP address for storage node 2 (management node 2)	Shared with a storage network port	172.16.0.15 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
Management network IP address for storage node 3	Shared with a storage network port	172.16.0.17 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
Management network IP address for storage node 4	Shared with a storage network port	172.16.0.19 (shared with a storage network IP address)	255.255.255.0	172.16.0.1

 Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
External management network IP address for storage node 1 (management node 1)	OceanStor Pacific 9550: NIC-*X* OceanStor Pacific 9546: shared Port4	10.110.100.106	255.255.255.0	10.110.100.1
External management network IP address for storage node 2 (management node 2)	OceanStor Pacific 9550: NIC-*X* OceanStor Pacific 9546: shared Port4	10.110.100.107	255.255.255.0	10.110.100.1
Management network IP address for the BMC switch	MEth0/0/0	10.110.100.110	255.255.255.0	10.110.100.1
Management network IP address for the management switch	MEth0/0/0	10.110.100.112	255.255.255.0	10.110.100.1
Management network IP address for storage switch 1	MEth0/0/0	10.110.100.113	255.255.255.0	10.110.100.1
Management network IP address for storage switch 2	MEth0/0/0	10.110.100.114	255.255.255.0	10.110.100.1
Management network IP address for leaf switch 1	MEth0/0/0	10.110.100.115	255.255.255.0	10.110.100.1
Management network IP address for leaf switch 2	MEth0/0/0	10.110.100.116	255.255.255.0	10.110.100.1

 Copyright © Huawei Technologies Co., Ltd.

BMC Network

Table 3-24 describes the IP address planning for the BMC network.

Table 3-24 IP address planning for the BMC network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
BMC network IP address for storage node 1	Mgmt	10.110.100.13	255.255.255.0	10.110.100.1
BMC network IP address for storage node 2	Mgmt	10.110.100.14	255.255.255.0	10.110.100.1
BMC network IP address for storage node 3	Mgmt	10.110.100.15	255.255.255.0	10.110.100.1
BMC network IP address for storage node 4	Mgmt	10.110.100.16	255.255.255.0	10.110.100.1

Storage Network

Table 3-25 describes the IP address planning for the storage network.

Table 3-25 IP address planning for the storage network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Storage network IP addresses for storage node 1	Storage network ports providing multiple IP addresses	172.16.0.13	255.255.255.0	172.16.0.1
		172.16.0.14	255.255.255.0	172.16.0.1
Storage network IP addresses for storage node 2	Storage network ports providing multiple IP addresses	172.16.0.15	255.255.255.0	172.16.0.1
		172.16.0.16	255.255.255.0	172.16.0.1

Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Storage network IP addresses for storage node 3	Storage network ports providing multiple IP addresses	172.16.0.17	255.255.255.0	172.16.0.1
		172.16.0.18	255.255.255.0	172.16.0.1
Storage network IP addresses for storage node 4	Storage network ports providing multiple IP addresses	172.16.0.19	255.255.255.0	172.16.0.1
		172.16.0.20	255.255.255.0	172.16.0.1
Control network IP address for storage node 1	Storage network ports providing multiple IP addresses	172.16.0.129	255.255.255.0	172.16.0.1
Control network IP address for storage node 2	Storage network ports providing multiple IP addresses	172.16.0.130	255.255.255.0	172.16.0.1
Control network IP address for storage node 3	Storage network ports providing multiple IP addresses	172.16.0.131	255.255.255.0	172.16.0.1
Control network IP address for storage node 4	Storage network ports providing multiple IP addresses	172.16.0.132	255.255.255.0	172.16.0.1

File Service Network

Table 3-26 describes the IP address planning for the file service network. One access zone and one subnet are used as an example.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-26 IP address planning for the file service network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
IP address of the general DNS service in the subnet	Service bond port of a node	192.168.100.10	255.255.255.0	192.168.100.1
Access zone IP address pool	Bond port	192.168.100.11 to 192.168.100.16 **NOTE** • Number of IP addresses in the access zone IP address pool = Number of storage nodes x *N* (*N* indicates the number of access zones). For example, if one access zone is configured, the number of IP addresses in the IP address pool is six. • The service network IP addresses can be inconsecutive. This example uses consecutive IP addresses.	255.255.255.0	192.168.100.1

 Copyright © Huawei Technologies Co., Ltd.

3.2.3 File/Object Service (DPC and Standard Protocol Hybrid Scenario)

3.2.3.1 Overview

Network Introduction

The following networks are involved for OceanStor Pacific series in the DPC and standard protocol hybrid scenario:

- BMC network

  The BMC network connects to Mgmt ports of nodes to enable remote device management.
- Management network
  - The external management network is used by users to access DeviceManager and the CLI, and for communication between storage nodes and external HCS/HCSO O&M systems.
  - The internal management network is used for management data communication between the management and storage nodes.
- Control network
  - Transmits control messages in the system.
  - Adopts a floating IP address that floats among storage network ports on nodes.
- Storage network

  The front-end storage network and back-end storage network are shared for data communication between storage nodes and between DPC and OSD.
- Service network

  Enables data communication between storage nodes and users' service network and supports NFS/CIFS/object interface protocol.

3.2.3.2 Networking Scenarios

Table 3-27 shows the DPC and standard protocol hybrid networking scenarios supported by OceanStor Pacific 9550, OceanStor Pacific 9950, and OceanStor Pacific 9546 (Two CPUs per Node).

Copyright © Huawei Technologies Co., Ltd.

Table 3-27 Networking scenarios

Device Name	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example	Service Network (NIC Example)	Service Switch Example
OceanStor Pacific 9550	**3.2.3.5.1 OceanStor Pacific 9550**	25GE (LOM) or GE (LOM)	CE6865 (25GE) or switch that supports GE	100GE RoCE (CX5)	CE8850	25GE TCP (Hi1822)	CE6865
OceanStor Pacific 9546 (Two CPUs per Node)	**3.2.3.5.2 OceanStor Pacific 9546 (Two CPUs per Node)**	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850	25GE TCP (Hi1822V120)	CE6865
Tiering scenario: OceanStor Pacific 9550 + OceanStor Pacific 9950	**3.2.1.5.1 OceanStor Pacific 9550**	25GE (LOM) or GE (LOM)	CE6865 (25GE) or switch that supports GE	100GE RoCE (CX5)	CE8850	25GE TCP (Hi1822)	CE6865
	3.2.1.5.2 OceanStor Pacific 9950	100GE (LOM) or GE (LOM)	CE8850 (100GE) or switch that supports GE	100GE RoCE (customized CX6 NIC)	CE8850	Not connected to the service network	Not connected to the service network

Copyright © Huawei Technologies Co., Ltd.

Device Name	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example	Service Network (NIC Example)	Service Switch Example
Tiering scenario: OceanStor Pacific 9950 + OceanStor Pacific 9546 (Two CPUs per Node)	3.2.1.5.2 OceanStor Pacific 9950	100GE (LOM) or GE (LOM)	CE8850 (100GE) or switch that supports GE	100GE RoCE (customized CX6 NIC)	CE8850	Not connected to the service network	Not connected to the service network
	3.2.3.5.2 OceanStor Pacific 9546 (Two CPUs per Node)	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850	25GE TCP (Hi1822V120)	CE6865
Tiering scenario: OceanStor Pacific 9546 + OceanStor Pacific 9550	3.2.3.5.2 OceanStor Pacific 9546 (Two CPUs per Node)	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850	25GE TCP (Hi1822V120)	CE6865
	3.2.1.5.1 OceanStor Pacific 9550	25GE (LOM) or GE (LOM)	CE6865 (25GE) or switch that supports GE	100GE RoCE (CX5)	CE8850	25GE TCP (Hi1822)	CE6865

NOTE

The Hi1822 and Hi1822V120 NICs have four ports (when the Hi1822V120 NIC is used, only the four-port NIC is used). Only the first two ports of the NICs are used.

Copyright © Huawei Technologies Co., Ltd.

3.2.3.3 Network Requirements

Table 3-28 describes the specific network requirements in the DPC and standard protocol hybrid scenario.

Table 3-28 Network requirements

Network Type	Network Requirements
BMC network	• A BMC network can be a GE network. • The number of BMC network ports on each storage node can be one or two.
Service network	The TCP/IP protocol is supported. It supports 25GE networks and allows you to configure only bond4.
Storage network	• The RoCE protocol and 100GE network are supported, and only multiple IP addresses can be configured. **NOTE** When the storage network does not use the bond network, each port on the storage network can be bonded to one IP address. • The storage networks of all nodes use the same VLAN ID.
Control network	If the storage network uses multiple IP addresses, select a port on the storage network to configure one floating IP address for the control network. The control network and the storage network can be in the same subnet (recommended) or different subnets. If they are in the same subnet, they must use different IP address segments.
External management network	• Supports the TCP/IP protocol. • Networking mode: 1. OceanStor Pacific 9550: When the 25GE network is used, the number of network ports can be one or two. Two management network ports can be bonded only in bond4 mode. When the GE network is used, the number of network ports can be only one and bond is not supported. 2. OceanStor Pacific 9950: When the 100GE network is used, the number of network ports can be one or two. Two management network ports can be bonded only in bond4 mode. When the GE network is used, the number of network ports can be one or two. Two management network ports can be bonded only in bond1 mode. 3. OceanStor Pacific 9546 (Two CPUs per Node): The number of network ports can be one or two. Two management network ports can be bonded only in bond1 mode.

Copyright © Huawei Technologies Co., Ltd.

Network Type	Network Requirements
Internal management network	It is integrated with the storage network.

NOTICE

All networks support only IPv4 addresses.

3.2.3.4 Network Solution

Figure 3-15 shows the network solution.

Figure 3-15 Network solution

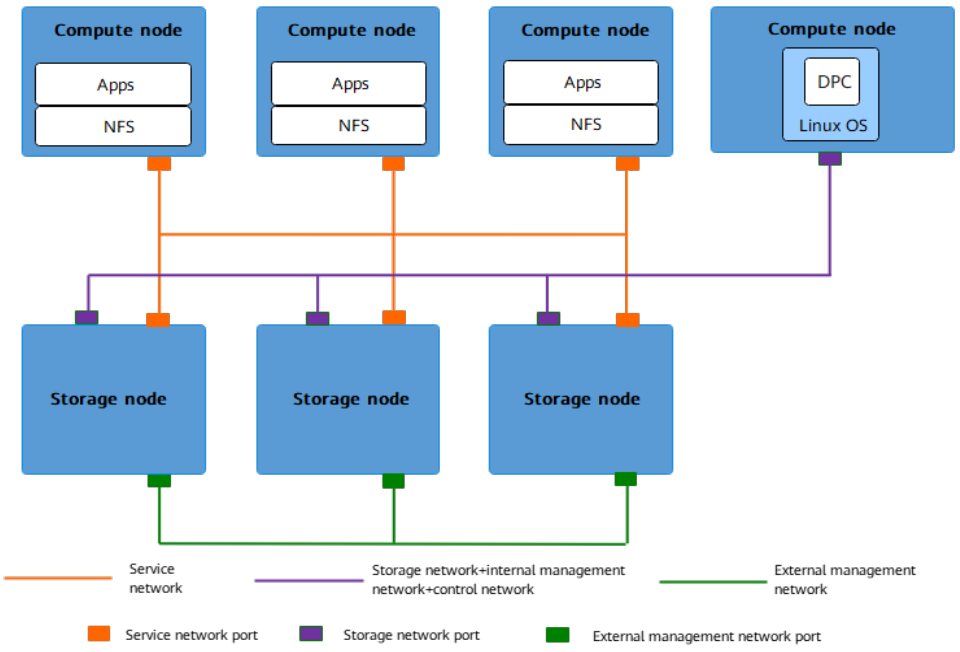


Figure 3-16 shows the physical network.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-16 Physical network

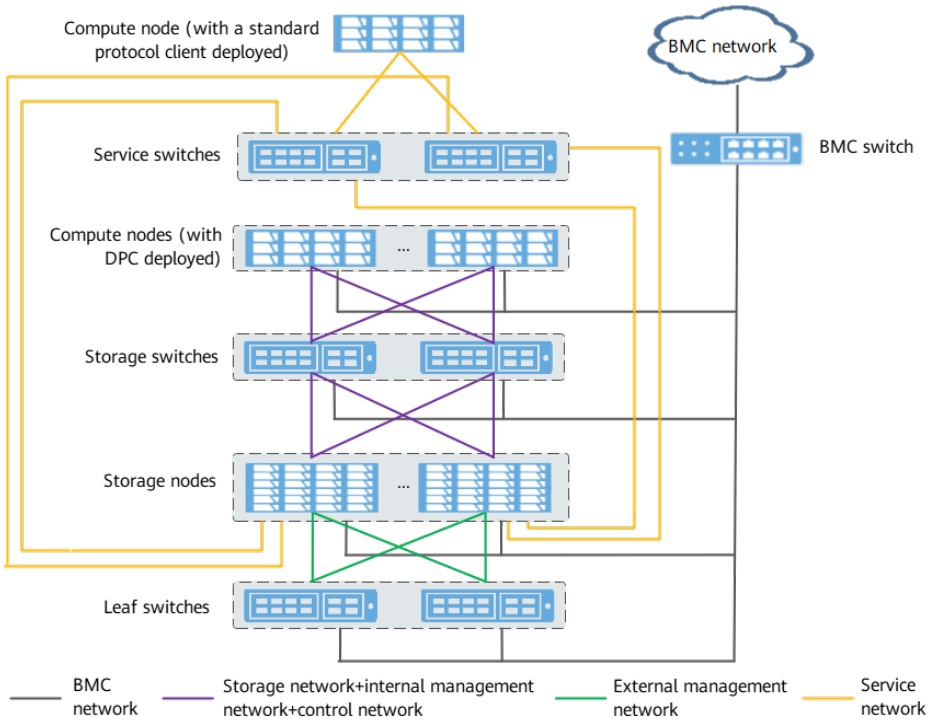


Table 3-29 describes the network requirements and IP address planning.

Table 3-29 Network requirements and IP address planning

Device Type	Requirements	IP Address Planning
Compute node	The storage network of a compute node must be able to communicate with the storage network of a storage node through a distributed gateway.	Planned and allocated by the HCS/HCSO network in a unified manner.

 Copyright © Huawei Technologies Co., Ltd.

Device Type	Requirements	IP Address Planning
Storage/ Management node (the first two storage nodes are also management nodes)	Internal management network: shares network ports and IP addresses with the storage network. External management network: 1. OceanStor Pacific 9550: When the 25GE network is used, each storage node provides two management network ports to connect to the external management network (One or two network ports can be used. When two network ports are used, only bond4 is supported.). When the GE network is used, each storage node provides one management network port to connect to the external management network. 2. OceanStor Pacific 9950: When the 100GE network is used, each storage node provides two management network ports to connect to the external management network (One or two network ports can be used. When two network ports are used, only bond4 is supported.). When the GE network is used, eight storage nodes share two management network ports to connect to the external management network. 3. OceanStor Pacific 9546 (Two CPUs per Node): Each storage node provides two management network ports to connect to the external management network (One or two network ports can be used. When two network ports	• Configure one floating IP address for the external management network of each cluster for cluster management. • Configure one floating IP address for the internal management network of each cluster. • Configure one management IP address for the external management network on each storage node. • Configure two management IP addresses for the internal management network (same as the IP addresses of the storage network) on each storage node.

 Copyright © Huawei Technologies Co., Ltd.

Device Type	Requirements	IP Address Planning
	are used, only bond1 is supported.). **NOTE** • The external management network is used by users to access DeviceManager and the CLI, and for communication between storage nodes and external HCS/HCSO O&M systems. • The internal management network is used for management data communication between the management and storage nodes. • The IP addresses of the external and internal management networks must be in different network segments.	
	Storage network: Two ports are provided for accessing the storage network using multiple IP addresses.	Planned and allocated by the HCS/HCSO network in a unified manner. **NOTE** If you plan to expand capacity, you are advised to reserve storage network IP addresses for nodes that will be added.
	Control network: If any port on the storage network is used, the control network IP address automatically floats on the storage network ports.	The control network IP address and the storage network IP address cannot be in the same network segment but must be in the same subnet.
	Service network: Two ports are provided to form bond4 for accessing the service network. **NOTE** • The Hi1822 and Hi1822V120 NICs have four ports (when the Hi1822V120 NIC is used, only the four-port NIC is used). Only the first two ports of the NICs are used.	Configure one VTEP IP address for establishing a VXLAN tunnel with compute nodes (ECS).
	BMC network: One port is provided for accessing the BMC network.	Configure one IP address for the BMC network.

 Copyright © Huawei Technologies Co., Ltd.

Device Type	Requirements	IP Address Planning
Storage switch	• Provided by the HCS/HCSO network. • The flow control priority is 32 and the queue is 4. • The oversubscription ratio is 1:1.	Planned and allocated by the HCS/HCSO network in a unified manner.
Leaf switch	• One management network port is provided for accessing the management network. • Switches must be de-stacked.	Configure one management network IP address for each switch. **NOTE** In the DPC and standard protocol hybrid scenario, if the uplink traffic to leaf switches contains both service network traffic and management network traffic, the uplink bandwidth needs to be calculated based on the number of nodes.

3.2.3.5 Planning Ports for Nodes

3.2.3.5.1 OceanStor Pacific 9550

Figure 3-17 shows an example of planning ports for a storage node.

Figure 3-17 Example of planning ports for a storage node

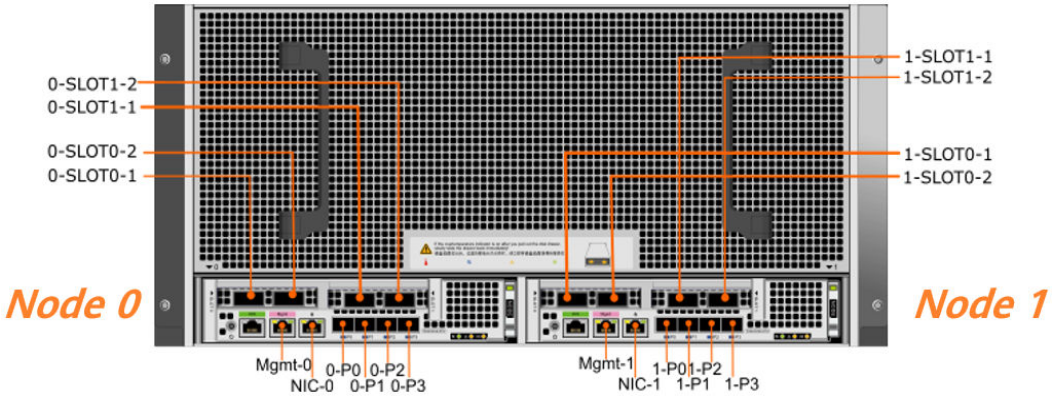


Table 3-30 describes the ports on node *X* (either node between the two nodes in Figure 3-17) when the service network is 25GE and the storage network is 100GE RoCE.

 Copyright © Huawei Technologies Co., Ltd.

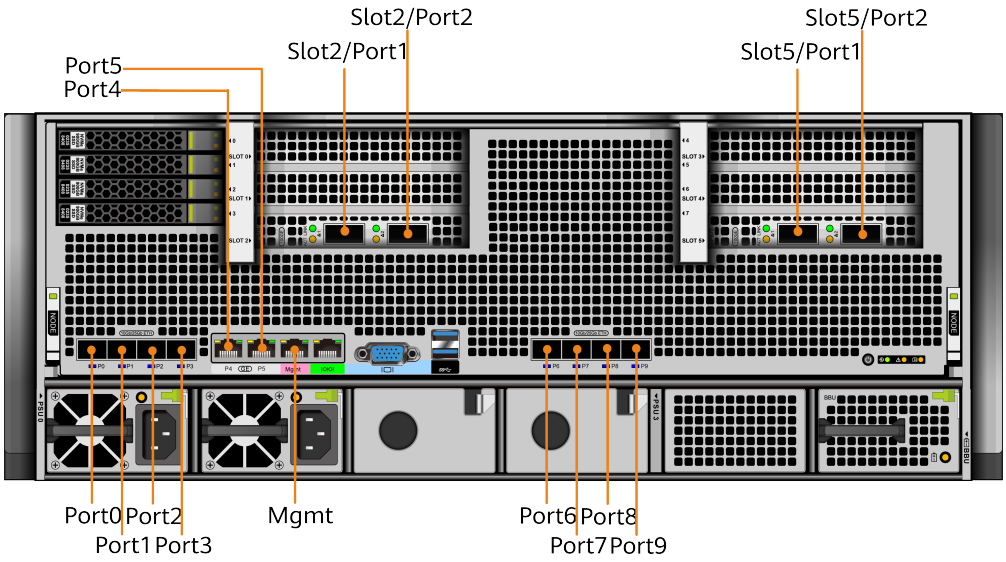
Table 3-30 Port usage

Port Name	Port Type	Access Network	Description
X-SLOT1-0 and *X*-SLOT1-1	25GE	Service network	The ports connect to the service switches.
X-SLOT0-0 and *X*-SLOT0-1	100GE	Storage network/ Control network/ Internal management network	The ports connect to the storage switches.
X-P0 and *X*-P1, or NIC-*X*	25GE (*X*-P0 and *X*-P1) or GE (NIC-*X*)	External management network	The ports connect to the leaf switches.
Mgmt-*X*	GE	BMC network	The port connects to the BMC switch.

3.2.3.5.2 OceanStor Pacific 9546 (Two CPUs per Node)

- Planning ports for OceanStor Pacific 9546 (One Node per Chassis, Two CPUs per Node):

  Figure 3-18 OceanStor Pacific 9546 (One Node per Chassis, Two CPUs per Node) (using 2-port NICs)



 Copyright © Huawei Technologies Co., Ltd.

Figure 3-19 OceanStor Pacific 9546 (One Node per Chassis, Two CPUs per Node) (using 4-port NICs)

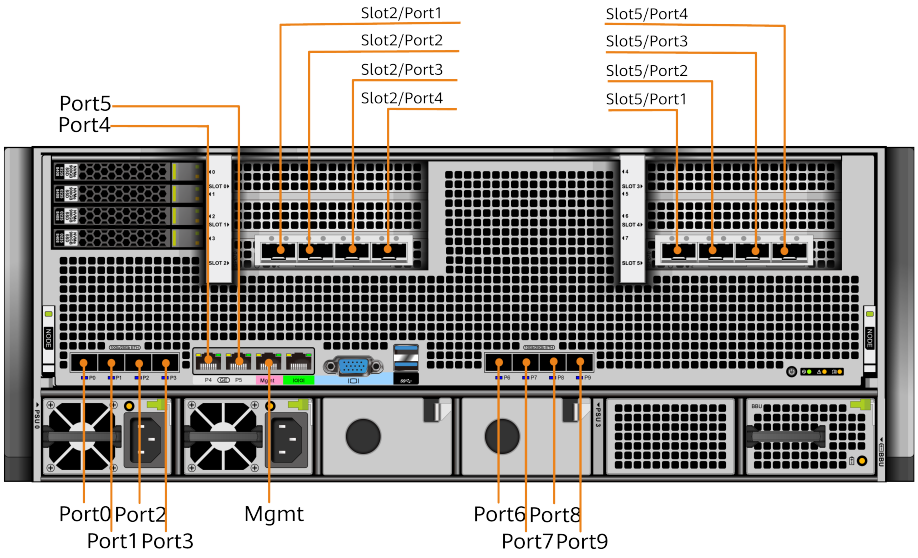


Table 3-31 describes the ports on a node when the service network is 25GE and the storage network is 100GE RoCE.

Table 3-31 Port usage

Port Name	Port Type	Access Network	Description
Slot5/Port1 and Slot5/Port2	25GE	Service network	The ports connect to the service switches.
Slot2/Port1 and Slot2/Port2	100GE	Storage network/Control network/Internal management network	The ports connect to the storage switches.
Port4 and Port5	GE	External management network	The ports connect to the leaf switches.
Mgmt	GE	BMC network	The port connects to the BMC switch.

- Planning ports for OceanStor Pacific 9546 (Two Nodes per Chassis, Two CPUs per Node):

Copyright © Huawei Technologies Co., Ltd.

Figure 3-20 OceanStor Pacific 9546 (Two Nodes per Chassis, Two CPUs per Node) (using 2-port NICs)

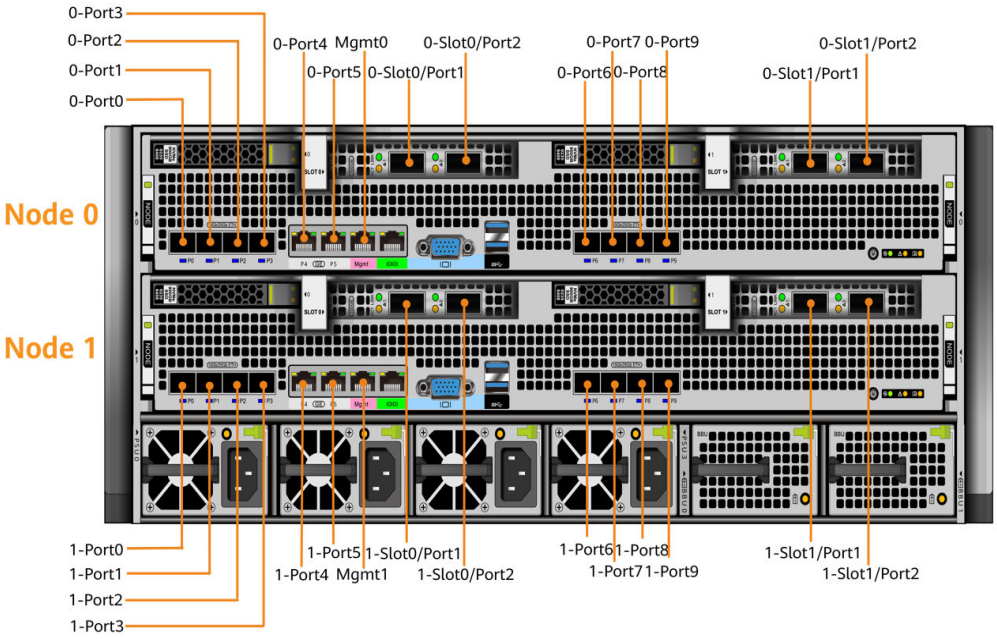


Figure 3-21 OceanStor Pacific 9546 (Two Nodes per Chassis, Two CPUs per Node) (using 4-port NICs)

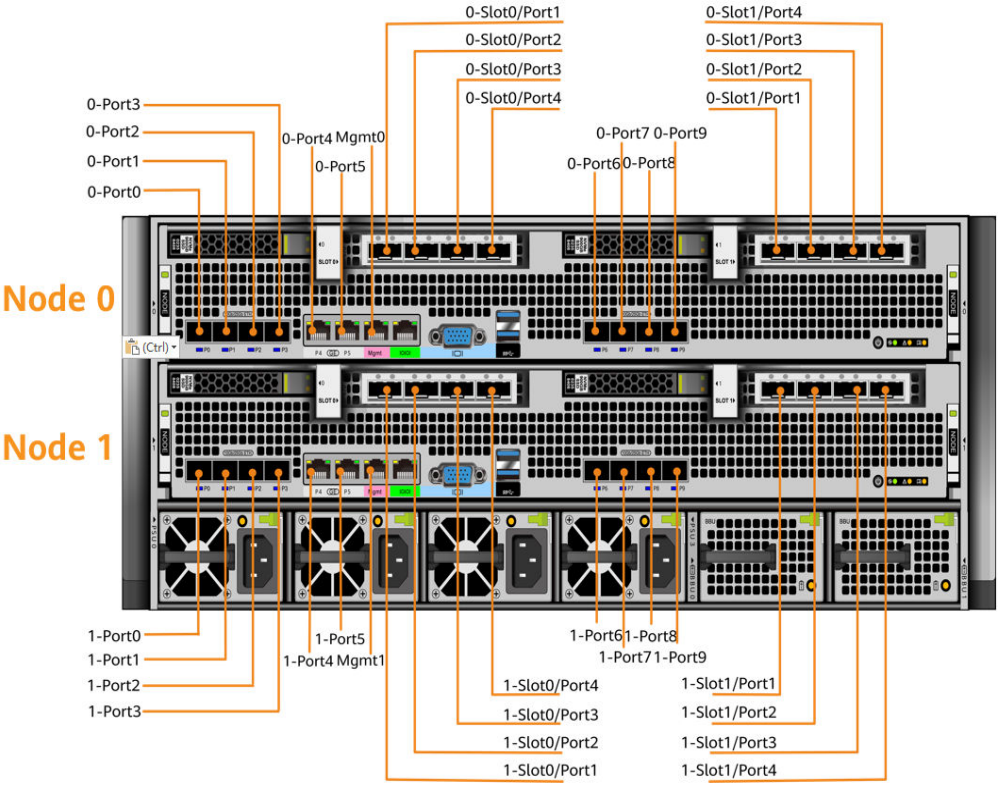


Table 3-32 describes the ports on node *X* (either node between the two nodes in Figure 3-20 or Figure 3-21) when the service network is 25GE and the storage network is 100GE.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-32 Port usage

Port Name	Port Type	Access Network	Description
X-Slot1/Port1 and *X*-Slot1/Port2	25GE	Service network	The ports connect to the service switches.
X-Slot0/Port1 and *X*-Slot0/Port2	100GE	Storage network/Control network/Internal management network	The ports connect to the storage switches.
X-Port4 and *X*-Port5	GE	External management network	The ports connect to the leaf switches.
Mgmt*X*	GE	BMC network	The port connects to the BMC switch.

3.2.3.6 Network Example

This section uses seven nodes (one compute node that uses standard protocols, two compute nodes that use DPC, and four storage nodes) as an example to describe the IP address planning.

For details about the networking of the two compute nodes that use DPC and the four storage nodes, see **3.2.1.6 Network Example**.

In addition, the number of service IP addresses planned for each of the four storage nodes is as follows:

Number of service network IP addresses (bond network) = Number of storage nodes x Number of access zones + Number of subnets

3.3 Planning of OceanStor Pacific 9520/OceanStor Pacific 9540/OceanStor Pacific 9920/OceanStor Pacific 9340

3.3.1 File Service (DPC Scenario)

3.3.1.1 Overview

Network Introduction

The following networks are involved for OceanStor Pacific series in the DPC scenario:

Copyright © Huawei Technologies Co., Ltd.

- BMC network

  The BMC network connects to Mgmt ports of nodes to enable remote device management.

- Management network
  - The external management network is used by users to access DeviceManager and the CLI, and for communication between storage nodes and external HCS/HCSO O&M systems.
  - The internal management network is used for management data communication between the management and storage nodes.
- Control network
  - Transmits control messages in the system.
  - Adopts a floating IP address that floats among storage network ports on nodes.
- Storage network

  In the DPC scenario, the front-end storage network and back-end storage network are shared for data communication between storage nodes and between DPC and OSD.

3.3.1.2 Networking Scenarios

Table 3-33 shows the DPC networking scenarios (interconnection with HCS/HCSO) supported by OceanStor Pacific 9540 Kunpeng-based and OceanStor Pacific 9920 Kunpeng-based.

Table 3-33 Networking scenarios

Device Name	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example
OceanStor Pacific 9540 Kunpeng-based	3.3.1.5.1 OceanStor Pacific 9540 Kunpeng-based	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850
OceanStor Pacific 9920 Kunpeng-based (SAS SSD)	3.3.1.5.2 OceanStor Pacific 9920 Kunpeng-based (SAS SSD)	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850

Copyright © Huawei Technologies Co., Ltd.

Device Name	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example
OceanStor Pacific 9920 Kunpeng-based (palm-sized NVMe SSD)	3.3.1.5.3 OceanStor Pacific 9920 Kunpeng-based (Palm-sized NVMe SSD)	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850
Tiering scenario: OceanStor Pacific 9540 Kunpeng-based + OceanStor Pacific 9920 Kunpeng-based	3.3.1.5.1 OceanStor Pacific 9540 Kunpeng-based	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850
	3.3.1.5.2 OceanStor Pacific 9920 Kunpeng-based (SAS SSD)	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850
Tiering scenario: OceanStor Pacific 9920 Kunpeng-based + OceanStor Pacific 9546	3.3.1.5.2 OceanStor Pacific 9920 Kunpeng-based (SAS SSD)	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850
	3.2.1.5.3 OceanStor Pacific 9546	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850

Copyright © Huawei Technologies Co., Ltd.

3.3.1.3 Network Requirements

Table 3-34 describes the specific network requirements in the DPC scenario.

Table 3-34 Network requirements

Network Type	Network Requirements
BMC network	• A BMC network can be a GE network. • The number of BMC network ports on each storage node can be one or two.
Storage network	• The RoCE protocol and 100GE network are supported, and only multiple IP addresses can be configured. **NOTE** When the storage network does not use the bond network, each port on the storage network can be bonded to one IP address. • The storage networks of all nodes use the same VLAN ID.
Control network	If the storage network uses multiple IP addresses, select a port on the storage network to configure one floating IP address for the control network. The control network and the storage network can be in the same subnet (recommended) or different subnets. If they are in the same subnet, they must use different IP address segments.
External management network	The TCP/IP protocol is supported. The number of network ports can be one or two. You are advised to bond two network ports in bond1 mode.
Internal management network	It is integrated with the storage network, and the two networks share ports and IP addresses.

NOTICE

All networks support only IPv4 addresses.

3.3.1.4 Network Solution

Figure 3-22 shows the network solution.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-22 Network solution

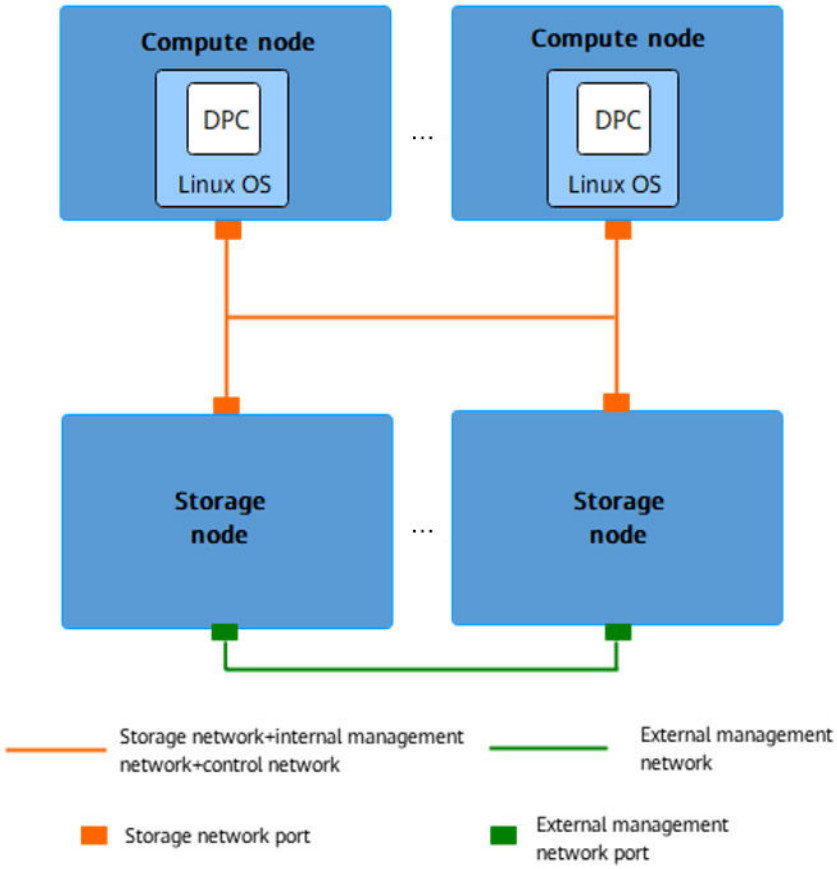


Figure 3-23 shows the physical network.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-23 Physical network

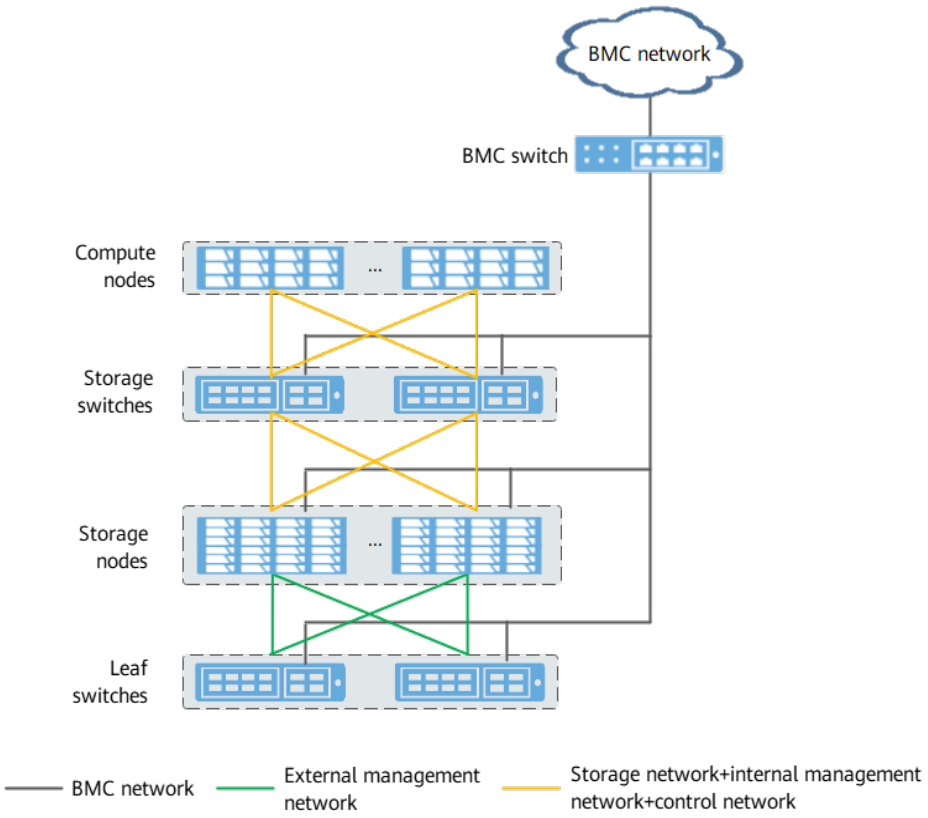


Table 3-35 describes the network requirements and IP address planning.

Table 3-35 Network requirements and IP address planning

Device Type	Requirements	IP Address Planning
Compute node	The storage network of a compute node must be able to communicate with the storage network of a storage node through a distributed gateway.	Planned and allocated by the HCS/HCSO network in a unified manner.

 Copyright © Huawei Technologies Co., Ltd.

Device Type	Requirements	IP Address Planning
Storage/ Management node (the first two storage nodes are also management nodes)	Internal management network: shares network ports and IP addresses with the storage network. External management network: Each storage node provides two management network ports to connect to the external management network (One or two network ports can be used. When two network ports are used, you are advised to bond them in bond1 mode.). **NOTE** • The external management network is used by users to access DeviceManager and the CLI, and for communication between storage nodes and external HCS/HCSO O&M systems. • The internal management network is used for management data communication between the management and storage nodes. • The IP addresses of the external and internal management networks must be in different network segments.	• Configure one floating IP address for the external management network of each cluster for cluster management. • Configure one floating IP address for the internal management network of each cluster. • Configure one management IP address for the external management network on each storage node. • Configure two management IP addresses for the internal management network (same as the IP addresses of the storage network) on each storage node.
	Storage network: Two ports are provided for accessing the storage network using multiple IP addresses.	Planned and allocated by the HCS/HCSO network in a unified manner. **NOTE** If you plan to expand capacity, you are advised to reserve storage network IP addresses for nodes that will be added.
	Control network: If any port on the storage network is used, the control network IP address automatically floats on the storage network ports.	The control network IP address and the storage network IP address cannot be in the same network segment but must be in the same subnet.

 Copyright © Huawei Technologies Co., Ltd.

Device Type	Requirements	IP Address Planning
	BMC network: One port is provided for accessing the BMC network.	Configure one IP address for the BMC network.
Storage switch	• Provided by the HCS/HCSO network. • The flow control priority is 32 and the queue is 4. • The oversubscription ratio is 1:1.	Planned and allocated by the HCS/HCSO network in a unified manner.
Leaf switch	• One management network port is provided for accessing the management network. • Switches must be de-stacked.	Configure one management network IP address for each switch.

3.3.1.5 Planning Ports for Nodes

3.3.1.5.1 OceanStor Pacific 9540 Kunpeng-based

Figure 3-24 shows an example of planning ports for a storage node.

Figure 3-24 Example of planning ports for a storage node

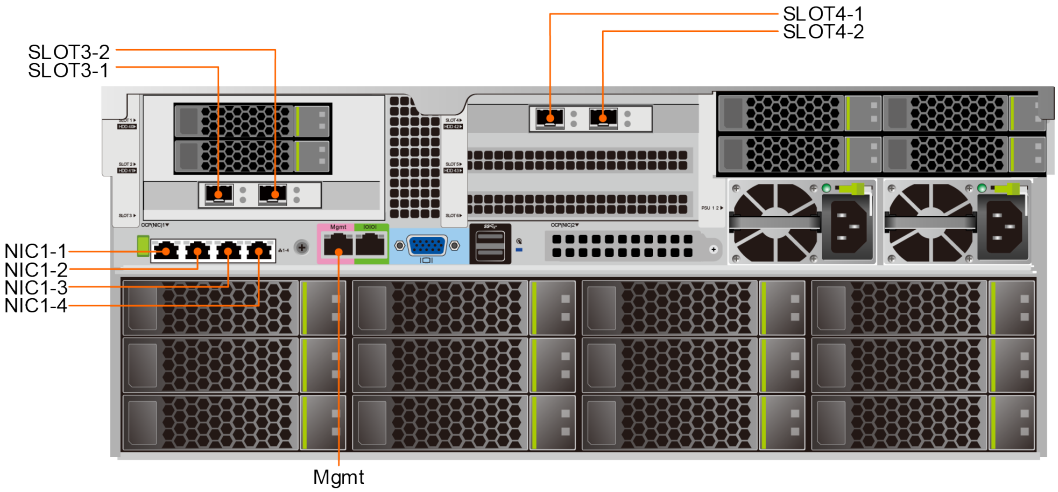


Table 3-36 describes the ports on a node when the storage network is 100GE RoCE.

Copyright © Huawei Technologies Co., Ltd.

Table 3-36 Port usage

Port Name	Port Type	Access Network	Description
SLOT4-1 and SLOT4-2	100GE	Storage network/ Control network/ Internal management network	The ports connect to the storage switches.
NIC1-1 and NIC1-2	GE	External management network	The ports connect to the leaf switches.
Mgmt	GE	BMC network	The port connects to the BMC switch.

3.3.1.5.2 OceanStor Pacific 9920 Kunpeng-based (SAS SSD)

Figure 3-25 shows an example of planning ports for a storage node.

Figure 3-25 Example of planning ports for a storage node

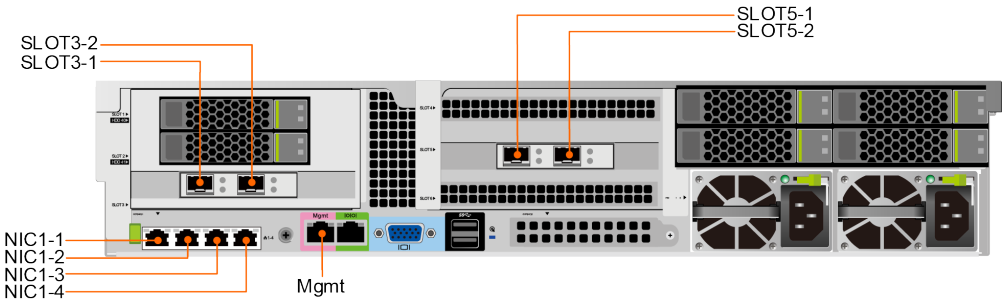


Table 3-37 describes the ports on a node when the storage network is 100GE RoCE.

Table 3-37 Port usage

Port Name	Port Type	Access Network	Description
SLOT5-1 and SLOT5-2	100GE	Storage network/ Control network/ Internal management network	The ports connect to the storage switches.
NIC1-1 and NIC1-2	GE	External management network	The ports connect to the leaf switches.

 Copyright © Huawei Technologies Co., Ltd.

Port Name	Port Type	Access Network	Description
Mgmt	GE	BMC network	The port connects to the BMC switch.

3.3.1.5.3 OceanStor Pacific 9920 Kunpeng-based (Palm-sized NVMe SSD)

Figure 3-26 shows an example of planning ports for a storage node.

Figure 3-26 Example of planning ports for a storage node

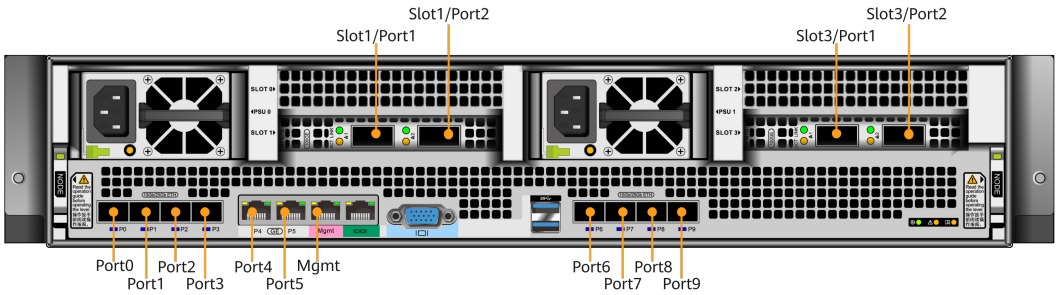


Table 3-38 describes the ports on a node when the storage network is 100GE RoCE.

Table 3-38 Port usage

Port Name	Port Type	Access Network	Description
Slot1/Port1 and Slot3/Port1	100GE	Storage network	The ports connect to the storage switches.
Port4 and Port5	GE	Management network	The ports connect to the management switch.
Mgmt	GE	BMC network	The port connects to the BMC switch.

3.3.1.6 Network Example

The number of IP addresses required by each network is as follows:

- Number of management network IP addresses = Number of storage switches + Number of leaf switches + Number of BMC switches + Number of management switches + Number of storage nodes x 2 + 2

Copyright © Huawei Technologies Co., Ltd.

- Number of BMC network IP addresses = Number of compute nodes + Number of storage nodes
- Number of storage network IP addresses = Number of compute nodes (bond) + Number of storage nodes x 3

This section describes the network IP address planning when two compute nodes, four storage nodes (management nodes are deployed on the same servers as the storage nodes), two storage switches, two leaf switches, one management switch, and one BMC switch are deployed.

Management Network

Table 3-39 describes the IP address planning for the management network.

Table 3-39 IP address planning for the management network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Floating management IP address for the external management network	Logical management port	10.110.100.100	255.255.255.0	10.110.100.1
Floating management IP address for the internal management network	Logical management port	172.16.0.12	255.255.255.0	172.16.0.1
Internal management network IP address for compute node 1	Determined by users	192.168.0.11 (shared with a storage network IP address)	255.255.255.0	192.168.0.1
Internal management network IP address for compute node 2	Determined by users	192.168.0.12 (shared with a storage network IP address)	255.255.255.0	192.168.0.1
Internal management network IP address for storage node 1	Shared with a storage network port	172.16.0.13 (shared with a storage network IP address)	255.255.255.0	172.16.0.1

 Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Internal management network IP address for storage node 2	Shared with a storage network port	172.16.0.15 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
Internal management network IP address for storage node 3	Shared with a storage network port	172.16.0.17 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
Internal management network IP address for storage node 4	Shared with a storage network port	172.16.0.19 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
External management network IP address for compute node 1	Determined by users	10.110.100.104	255.255.255.0	10.110.100.1
External management network IP address for compute node 2	Determined by users	10.110.100.105	255.255.255.0	10.110.100.1
External management network IP address for storage node 1	NIC1-1 port	10.110.100.106	255.255.255.0	10.110.100.1
External management network IP address for storage node 2	NIC1-1 port	10.110.100.107	255.255.255.0	10.110.100.1

 Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
External management network IP address for storage node 3	NIC1-1 port	10.110.100.108	255.255.255.0	10.110.100.1
External management network IP address for storage node 4	NIC1-1 port	10.110.100.109	255.255.255.0	10.110.100.1
Management network IP address for the BMC switch	MEth0/0/0	10.110.100.110	255.255.255.0	10.110.100.1
Management network IP address for the management switch	MEth0/0/0	10.110.100.111	255.255.255.0	10.110.100.1
Management network IP address for storage switch 1	MEth0/0/0	10.110.100.112	255.255.255.0	10.110.100.1
Management network IP address for storage switch 2	MEth0/0/0	10.110.100.113	255.255.255.0	10.110.100.1
Management network IP address for leaf switch 1	MEth0/0/0	10.110.100.114	255.255.255.0	10.110.100.1
Management network IP address for leaf switch 2	MEth0/0/0	10.110.100.115	255.255.255.0	10.110.100.1

 Copyright © Huawei Technologies Co., Ltd.

BMC Network

Table 3-40 describes the IP address planning for the BMC network.

Table 3-40 IP address planning for the BMC network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
BMC network IP address for compute node 1	Determined by users	10.120.100.11	255.255.255.0	10.120.100.1
BMC network IP address for compute node 2	Determined by users	10.120.100.12	255.255.255.0	10.120.100.1
BMC network IP address for storage node 1	Mgmt	10.120.100.13	255.255.255.0	10.120.100.1
BMC network IP address for storage node 2	Mgmt	10.120.100.14	255.255.255.0	10.120.100.1
BMC network IP address for storage node 3	Mgmt	10.120.100.15	255.255.255.0	10.120.100.1
BMC network IP address for storage node 4	Mgmt	10.120.100.16	255.255.255.0	10.120.100.1

Storage Network

Table 3-41 describes the IP address planning for the storage network.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-41 IP address planning for the storage network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Storage network IP address for compute node 1 (bond is used as an example)	Determined by users	192.168.0.11	255.255.255.0	192.168.0.1
Storage network IP address for compute node 2 (bond is used as an example)	Determined by users	192.168.0.12	255.255.255.0	192.168.0.1
Storage network IP addresses for storage node 1	Storage network ports providing multiple IP addresses	172.16.0.13	255.255.255.0	172.16.0.1
		172.16.0.14	255.255.255.0	172.16.0.1
Storage network IP addresses for storage node 2	Storage network ports providing multiple IP addresses	172.16.0.15	255.255.255.0	172.16.0.1
		172.16.0.16	255.255.255.0	172.16.0.1
Storage network IP addresses for storage node 3	Storage network ports providing multiple IP addresses	172.16.0.17	255.255.255.0	172.16.0.1
		172.16.0.18	255.255.255.0	172.16.0.1
Storage network IP addresses for storage node 4	Storage network ports providing multiple IP addresses	172.16.0.19	255.255.255.0	172.16.0.1
		172.16.0.20	255.255.255.0	172.16.0.1
Control network IP address for storage node 1	Storage network ports providing multiple IP addresses	172.16.0.129	255.255.255.0	172.16.0.1

 Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Control network IP address for storage node 2	Storage network ports providing multiple IP addresses	172.16.0.130	255.255.255.0	172.16.0.1
Control network IP address for storage node 3	Storage network ports providing multiple IP addresses	172.16.0.131	255.255.255.0	172.16.0.1
Control network IP address for storage node 4	Storage network ports providing multiple IP addresses	172.16.0.132	255.255.255.0	172.16.0.1

3.3.2 File Service (Standard Protocol Scenario)

3.3.2.1 Overview

Network Introduction

The following networks are involved for OceanStor Pacific series in the standard protocol scenario:

- BMC network

  The BMC network connects to Mgmt ports of nodes to enable remote device management.
- Management network
  - The external management network is used by users to access DeviceManager and the CLI, and for communication between storage nodes and external HCS/HCSO O&M systems.
  - The internal management network is used for management data communication between the management and storage nodes.
- Control network
  - Transmits control messages in the system.
  - Adopts a floating IP address that floats among storage network ports on nodes.
- Storage network

  The front-end storage network and back-end storage network are shared for data communication between storage nodes and between DPC and OSD.
- Service network

 Copyright © Huawei Technologies Co., Ltd.

Enables data communication between storage nodes and users' service network and supports NFS/CIFS interface protocol.

3.3.2.2 Networking Scenarios

Table 3-42 shows the standard protocol (NFS/CIFS) networking scenarios supported by OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9920 Kunpeng-based, OceanStor Pacific 9520 Kunpeng-based, and OceanStor Pacific 9340 Kunpeng-based.

Table 3-42 Networking scenarios

Device Name (Supported Protocols)	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example	Service Network (NIC Example)	Service Switch Example
OceanStor Pacific 9540 Kunpeng-based or OceanStor Pacific 9340 Kunpeng-based	3.3.2.5.1 OceanStor Pacific 9540 Kunpeng-based and OceanStor Pacific 9340 Kunpeng-based	GE (LOM)	Switch that supports GE	25GE RoCE (CX4)	CE6865	10GE/25GE TCP (Hi1822V120)	CE6865
				25GE TCP (CX4)	CE6865	10GE/25GE TCP (Hi1822V120)	CE6865
				10GE RoCE (CX4)	CE6865	10GE TCP (Hi1822V120)	CE6865
				10GE TCP (CX4)	CE6855/CE6857/CE6881/CE6865	10GE TCP (Hi1822V120)	CE6865
OceanStor Pacific 9520 Kunpeng-based 12-slot	3.3.2.5.2 OceanStor Pacific 9520 Kunpeng-based 12-Slot	GE (LOM)	Switch that supports GE	25GE RoCE (CX4)	CE6865	10GE/25GE TCP (Hi1822V120)	CE6865
				10GE TCP (CX4)	CE6855/CE6857/CE6881/CE6865	10GE TCP (Hi1822V120)	CE6865

Copyright © Huawei Technologies Co., Ltd.

Device Name (Supported Protocols)	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example	Service Network (NIC Example)	Service Switch Example
				10GE RoCE (CX4)	CE6857/ CE6865	10GE TCP (Hi1822V120)	CE6865
OceanStor Pacific 9520 Kunpeng-based 14-slot	3.3.2.5.5 OceanStor Pacific 9520 Kunpeng-based 14-Slot	GE (LOM)	Switch that supports GE	25GE RoCE (LOM)	CE6865	10GE/ 25GE TCP (Hi1822V120)	CE6865
				25GE TCP (LOM)	CE6865	25GE TCP (Hi1822V120)	CE6865
				10GE RoCE (LOM)	CE6865	10GE TCP (Hi1822V120)	CE6865
				10GE TCP (LOM)	CE6865	10GE TCP (Hi1822V120)	CE6865
OceanStor Pacific 9920 Kunpeng-based (SAS SSD)	3.3.2.5.3 OceanStor Pacific 9920 Kunpeng-based (SAS SSD)	GE (LOM)	Switch that supports GE	25GE RoCE (CX4)	CE6865	25GE TCP (Hi1822V120)	CE6865
		GE (LOM)	Switch that supports GE	25GE TCP (CX4)	CE6865	25GE TCP (Hi1822V120)	CE6865

Copyright © Huawei Technologies Co., Ltd.

Device Name (Supported Protocols)	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example	Service Network (NIC Example)	Service Switch Example
OceanStor Pacific 9920 Kunpeng-based (palm-sized NVMe SSD)	3.3.2.5.4 OceanStor Pacific 9920 Kunpeng-based (Palm-sized NVMe SSD)	GE (LOM)	Switch that supports GE	25GE RoCE (LOM)	CE6865	10GE/25GE TCP (Hi1822V120)	CE6865
		GE (LOM)	Switch that supports GE	25GE TCP (LOM)	CE6865	25GE TCP (Hi1822V120)	CE6865
		GE (LOM)	Switch that supports GE	10GE TCP (LOM)	CE6857	10GE TCP (Hi1822V120)	CE6857
Tiering scenario: OceanStor Pacific 9540 Kunpeng-based + OceanStor Pacific 9920 Kunpeng-based (SAS SSD)	3.3.2.5.1 OceanStor Pacific 9540 Kunpeng-based and OceanStor Pacific 9340 Kunpeng-based	GE (LOM)	Switch that supports GE	25GE RoCE (CX4)	CE6865	10GE/25GE TCP (Hi1822V120)	CE6865
	3.3.2.5.3 OceanStor Pacific 9920 Kunpeng-based (SAS SSD)	GE (LOM)	Switch that supports GE	25GE RoCE (CX4)	CE6865	10GE/25GE TCP (Hi1822V120)	CE6865

Copyright © Huawei Technologies Co., Ltd.

Device Name (Supported Protocols)	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example	Service Network (NIC Example)	Service Switch Example
Tiering scenario: OceanStor Pacific 9920 Kunpeng-based (SAS SSD) + OceanStor Pacific 9546 (Two CPUs per Node)	3.3.2.5.3 OceanStor Pacific 9920 Kunpeng-based (SAS SSD)	GE (LOM)	Switch that supports GE	25GE RoCE (CX4)	CE6865	25GE TCP (Hi1822V120)	CE6865
	3.2.2.5.2 OceanStor Pacific 9546	GE (LOM)	Switch that supports GE	25GE RoCE (CX4)	CE6865	25GE TCP (Hi1822V120)	CE6865
Tiering scenario: OceanStor Pacific 9920 Kunpeng-based (SAS SSD) + OceanStor Pacific 9546	3.3.2.5.3 OceanStor Pacific 9920 Kunpeng-based (SAS SSD)	GE (LOM)	Switch that supports GE	25GE TCP (CX4)	CE6865	25GE TCP (Hi1822V120)	CE6865
	3.2.2.5.2 OceanStor Pacific 9546	GE (LOM)	Switch that supports GE	25GE TCP (LOM)	CE6865	25GE TCP (Hi1822V120)	CE6865

Copyright © Huawei Technologies Co., Ltd.

Device Name (Supported Protocols)	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example	Service Network (NIC Example)	Service Switch Example
Tiering scenario: OceanStor Pacific 9920 Kunpeng-based (palm-sized NVMe SSD) + OceanStor Pacific 9546	3.3.2.5.4 OceanStor Pacific 9920 Kunpeng-based (Palm-sized NVMe SSD)	GE (LOM)	Switch that supports GE	25GE RoCE (LOM)	CE6865	25GE TCP (Hi1822V120)	CE6865
	3.2.2.5.2 OceanStor Pacific 9546	GE (LOM)	Switch that supports GE	25GE RoCE (LOM)	CE6865	25GE TCP (Hi1822V120)	CE6865
Tiering scenario: OceanStor Pacific 9920 Kunpeng-based (palm-sized NVMe SSD) + OceanStor Pacific 9546	3.3.2.5.4 OceanStor Pacific 9920 Kunpeng-based (Palm-sized NVMe SSD)	GE (LOM)	Switch that supports GE	100GE TCP (CX5)	CE8850	25GE TCP (Hi1822V120)	CE6865
	3.2.2.5.2 OceanStor Pacific 9546	GE (LOM)	Switch that supports GE	25GE TCP (LOM)	CE6865	25GE TCP (Hi1822V120)	CE6865

Copyright © Huawei Technologies Co., Ltd.

Device Name (Supported Protocols)	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example	Service Network (NIC Example)	Service Switch Example
Tiering scenario: OceanStor Pacific 9920 Kunpeng-based (palm-sized NVMe SSD) + OceanStor Pacific 9546 (Two CPUs per Node)	3.3.2.5.4 OceanStor Pacific 9920 Kunpeng-based (Palm-sized NVMe SSD)	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850	100GE RoCE (sharing network ports with the storage network)	CE8850
	3.2.2.5.2 OceanStor Pacific 9546	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850	25GE TCP (Hi1822V120)	CE6865

NOTE

- If the 10GE network uses 25GE NICs, optical modules must be configured. The rate of the storage optical modules must be the same as that of the switch optical modules.
- OceanStor Pacific 9340 Kunpeng-based is recommended in the intelligent video and image scenario.
- The Hi1822 and Hi1822V120 NICs have four ports (when the Hi1822V120 NIC is used, only the four-port NIC is used). Only the first two ports of the NICs are used.

3.3.2.3 Network Requirements

This section describes the network requirements in the standard protocol scenario, as shown in **Table 3-43**.

Table 3-43 Network requirements

Network Type	Network Requirements
BMC network	• A BMC network can be a GE network. • The number of BMC network ports on each storage node can be one or two.

Copyright © Huawei Technologies Co., Ltd.

Network Type	Network Requirements
Service network	The TCP/IP protocol is supported. It supports 10GE/25GE networks and allows you to configure only bond4.
Storage network	• The RoCE protocol is supported. RoCE supports 10GE (OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9520 Kunpeng-based, and OceanStor Pacific 9340 Kunpeng-based) and 25GE (OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9920 Kunpeng-based, OceanStor Pacific 9520 Kunpeng-based, and OceanStor Pacific 9340 Kunpeng-based) networks, and only multiple IP addresses can be configured. **NOTE** When the storage network does not use the bond network, each port on the storage network can be bonded to one IP address. • The TCP/IP protocol is supported. TCP/IP supports 10GE/25GE networks and allows you to configure only bond4. • The storage networks of all nodes use the same VLAN ID.
Control network	If the storage network uses multiple IP addresses, select a port on the storage network to configure one floating IP address for the control network. The control network and the storage network can be in the same subnet (recommended) or different subnets. If they are in the same subnet, they must use different IP address segments.
External management network	The TCP/IP protocol is supported. The number of network ports can be one or two. You are advised to bond two network ports in bond1 mode.
Internal management network	It is integrated with the storage network, and the two networks share ports and IP addresses.

NOTICE

All networks support only IPv4 addresses.

3.3.2.4 Network Solution

Figure 3-27 shows the network solution.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-27 Network solution

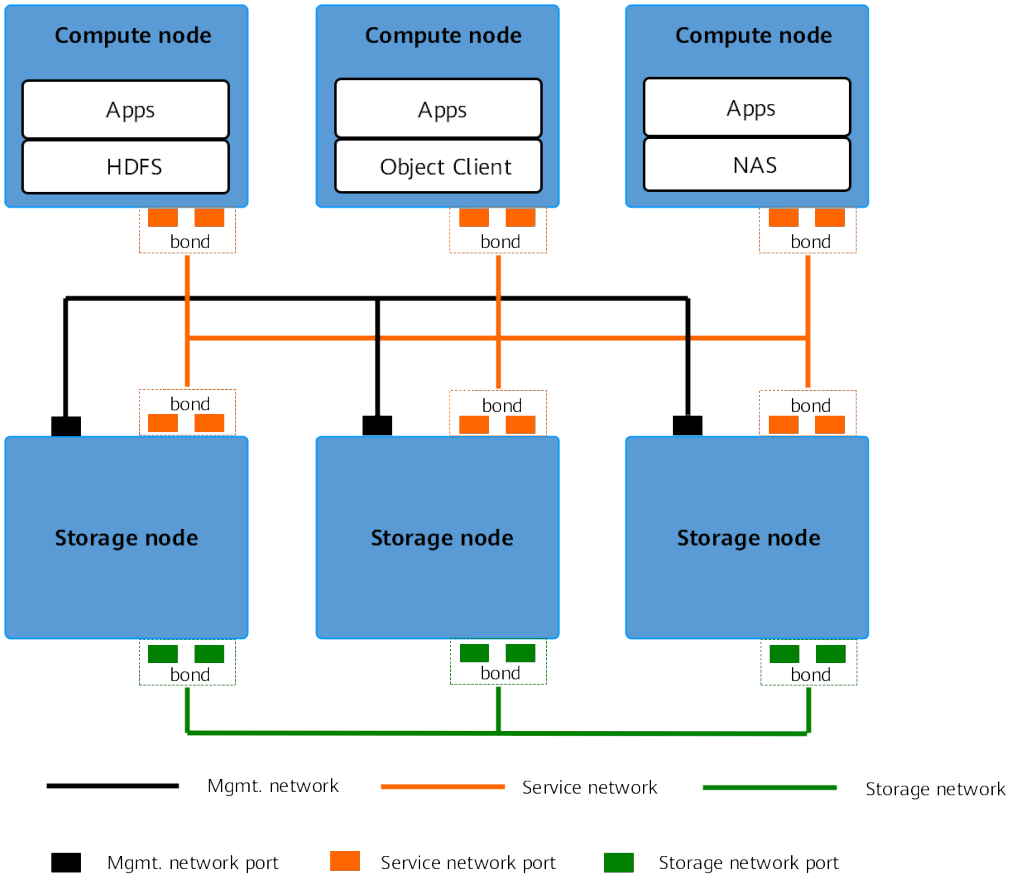


Figure 3-28 shows the physical network.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-28 Physical network

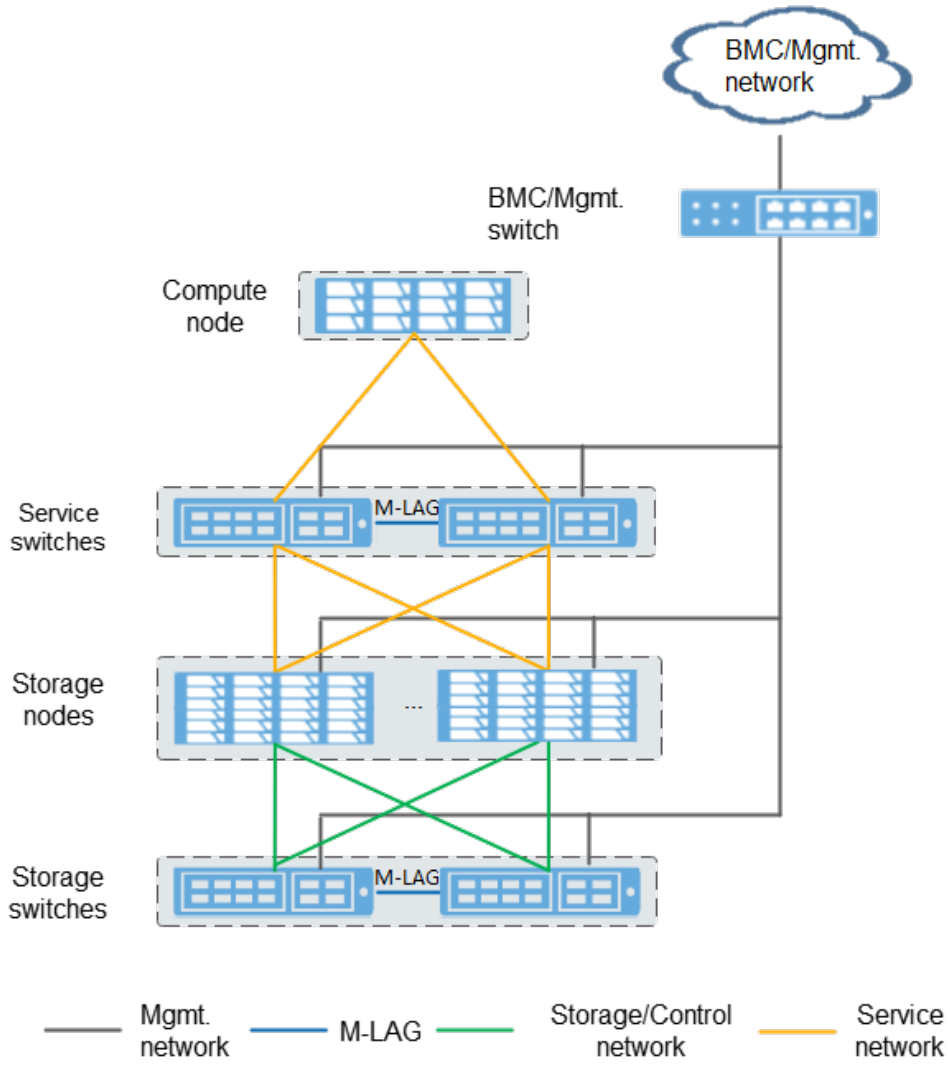


Table 3-44 describes the network requirements and IP address planning.

Table 3-44 Network requirements and IP address planning

Device Type	Requirements	IP Address Planning
Compute node	The storage network of a compute node must be able to communicate with the storage network of a storage node through a distributed gateway.	Planned and allocated by the HCS/HCSO network in a unified manner.

 Copyright © Huawei Technologies Co., Ltd.

Device Type	Requirements	IP Address Planning
Storage/ Management node (the first two storage nodes are also management nodes)	Internal management network: shares network ports and IP addresses with the storage network. External management network: Each storage node provides two management network ports to connect to the external management network (One or two network ports can be used. When two network ports are used, you are advised to bond them in bond1 mode.). **NOTE** • The external management network is used by users to access DeviceManager and the CLI, and for communication between storage nodes and external HCS/HCSO O&M systems. • The internal management network is used for management data communication between the management and storage nodes. • The IP addresses of the external and internal management networks must be in different network segments.	• Configure one floating IP address for the external management network of each cluster for cluster management. • Configure one floating IP address for the internal management network of each cluster. • Configure one management IP address for the external management network on each storage node. • Configure two management IP addresses for the internal management network (same as the IP addresses of the storage network) on each storage node.
	Storage network: Provides two ports to connect to the storage network using multiple IP addresses (RoCE) or bond4 (TCP).	Planned and allocated by the HCS/HCSO network in a unified manner. **NOTE** If you plan to expand capacity, you are advised to reserve storage network IP addresses for nodes that will be added.
	Control network (when the storage network uses the RoCE protocol or multiple IP addresses for networking): If any port on the storage network is used, the control network IP address automatically floats on the storage network ports.	The control network IP address and the storage network IP address cannot be in the same network segment but must be in the same subnet.

 Copyright © Huawei Technologies Co., Ltd.

Device Type	Requirements	IP Address Planning
	Service network: Two ports are provided to form bond4 for accessing the service network. **NOTE** • The Hi1822 and Hi1822V120 NICs have four ports (when the Hi1822V120 NIC is used, only the four-port NIC is used). Only the first two ports of the NICs are used.	Configure one VTEP IP address for establishing a VXLAN tunnel with compute nodes (ECS).
	BMC network: One port is provided for accessing the BMC network.	Configure one IP address for the BMC network.
Storage switch	• Provided by the HCS/HCSO network. • The flow control priority is 32 and the queue is 4. • The oversubscription ratio is 1:1.	Planned and allocated by the HCS/HCSO network in a unified manner.
Leaf switch	• One management network port is provided for accessing the management network. • Switches must be de-stacked.	Configure one management network IP address for each switch. **NOTE** In the standard protocol scenario, if the uplink traffic to leaf switches contains both service network traffic and management network traffic, the uplink bandwidth needs to be calculated based on the number of nodes.

3.3.2.5 Planning Ports for Nodes

3.3.2.5.1 OceanStor Pacific 9540 Kunpeng-based and OceanStor Pacific 9340 Kunpeng-based

Figure 3-29 and **Figure 3-30** show examples of planning ports for a storage node.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-29 Example of planning ports for a storage node (using 2-port NICs)

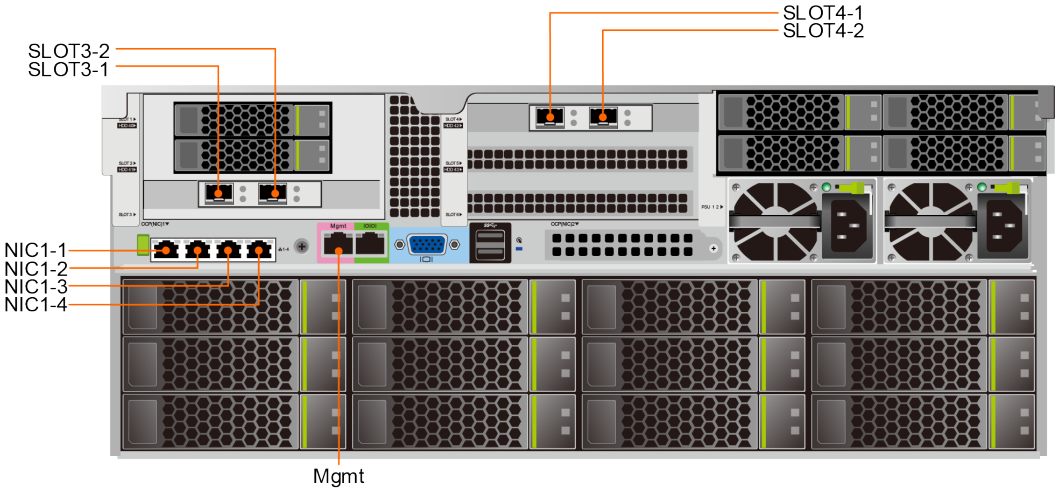


Figure 3-30 Example of planning ports for a storage node (using 4-port NICs)

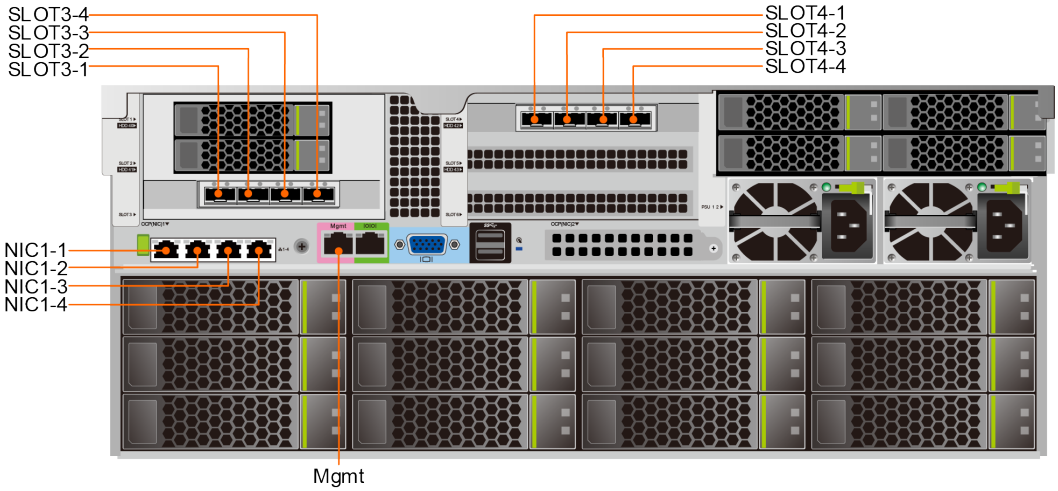


Table 3-45 describes the ports on a node when the service network is 10GE or 25GE and the storage network is 10GE or 25GE.

Table 3-45 Port usage

Port Name	Port Type	Access Network	Description
SLOT3-1 and SLOT3-2	10GE or 25GE	Service network	The ports connect to the service switches.
SLOT4-1 and SLOT4-2	10GE or 25GE	Storage network/ Control network/ Internal management network	The ports connect to the storage switches.

 Copyright © Huawei Technologies Co., Ltd.

Port Name	Port Type	Access Network	Description
NIC1-1 and NIC1-2	GE	External management network	The ports connect to the leaf switches.
Mgmt	GE	BMC network	The port connects to the BMC switch.

3.3.2.5.2 OceanStor Pacific 9520 Kunpeng-based 12-Slot

Figure 3-31 and Figure 3-32 show examples of planning ports for a storage node.

Figure 3-31 Example of planning ports for a storage node (using 2-port NICs)

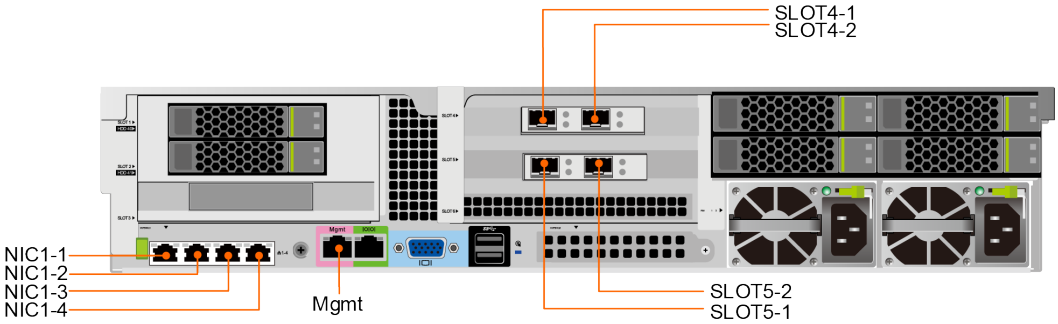


Figure 3-32 Example of planning ports for a storage node (using 4-port NICs)

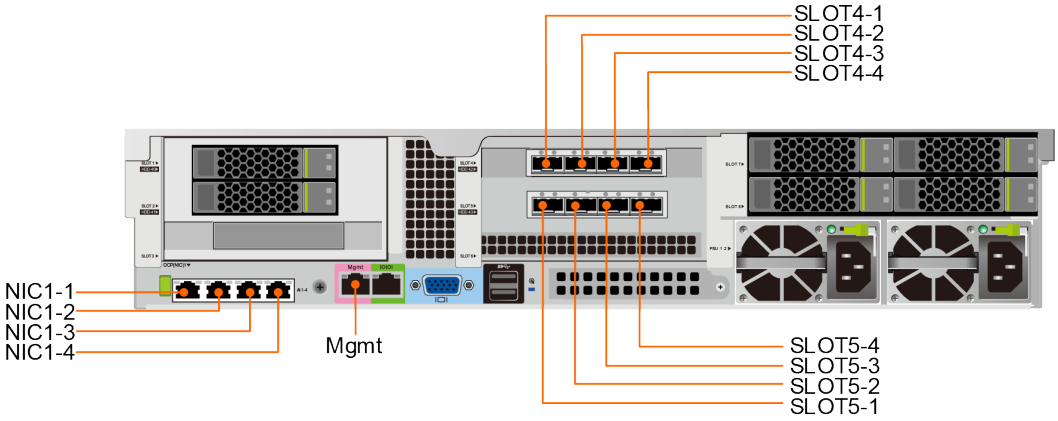


Table 3-46 describes the ports on a node when the service network is 10GE or 25GE and the storage network is 10GE or 25GE.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-46 Port usage

Port Name	Port Type	Access Network	Description
SLOT5-1 and SLOT5-2	10GE or 25GE	Service network	The ports connect to the service switches.
SLOT4-1 and SLOT4-2	10GE or 25GE	Storage network/ Control network/ Internal management network	The ports connect to the storage switches.
NIC1-1 and NIC1-2	GE	External management network	The ports connect to the leaf switches.
Mgmt	GE	BMC network	The port connects to the BMC switch.

3.3.2.5.3 OceanStor Pacific 9920 Kunpeng-based (SAS SSD)

Figure 3-33 and Figure 3-34 show examples of planning ports for a storage node.

Figure 3-33 Example of planning ports for a storage node (using 2-port NICs)

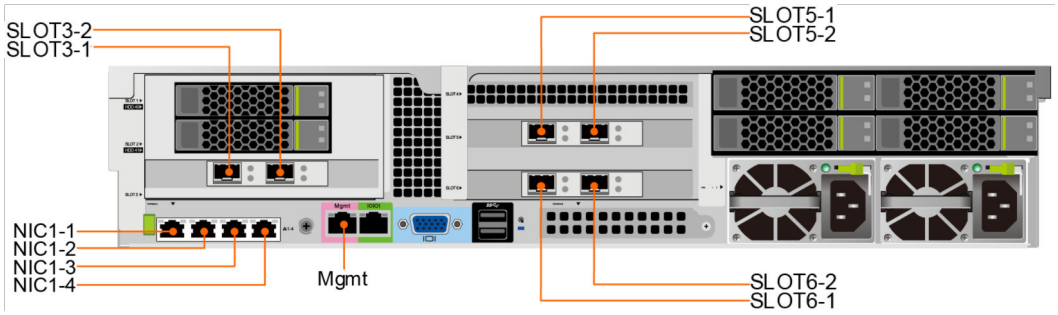
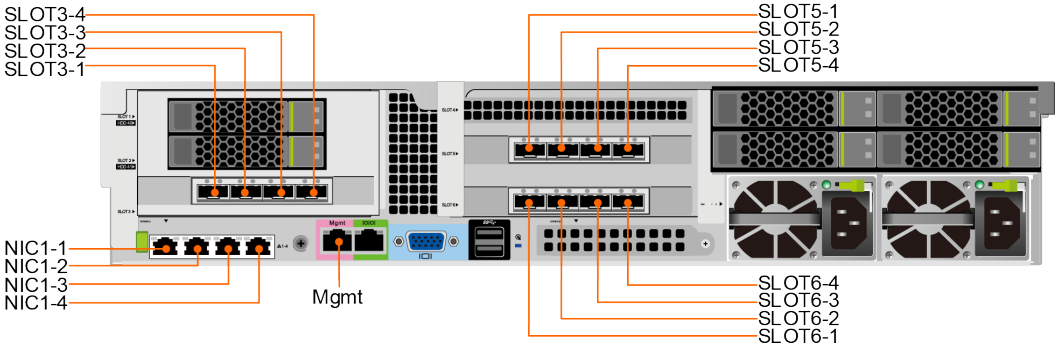


Figure 3-34 Example of planning ports for a storage node (using 4-port NICs)



 Copyright © Huawei Technologies Co., Ltd.

Table 3-47 describes the ports on a node when the service network is 10GE or 25GE and the storage network is 25GE RoCE.

Table 3-47 Port usage

Port Name	Port Type	Access Network	Description
SLOT3-1 and SLOT3-2	10GE or 25GE	Service network	The ports connect to the service switches.
SLOT5-1 and SLOT5-2	25GE	Storage network	The ports connect to the storage switches.
NIC1-1 and NIC1-2	GE	External management network	The ports connect to the leaf switches.
Mgmt	GE	BMC network	The port connects to the BMC switch.

3.3.2.5.4 OceanStor Pacific 9920 Kunpeng-based (Palm-sized NVMe SSD)

Figure 3-35 shows an example of planning ports for a storage node.

Figure 3-35 Example of planning ports for a storage node

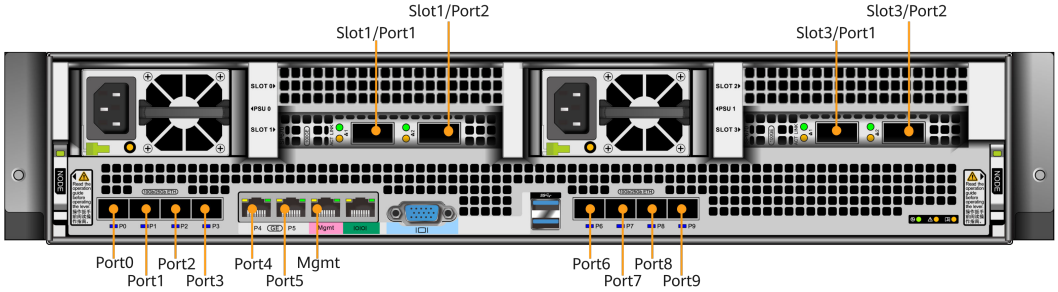


Table 3-48 describes the ports on a node when the storage network is 25GE RoCE and the service network is 25GE TCP.

Table 3-48 Port usage

Port Name	Port Type	Access Network	Description
Port0 and Port1	25GE	Storage network	The ports connect to the storage switches.

Copyright © Huawei Technologies Co., Ltd.

Port Name	Port Type	Access Network	Description
Slot1/Port1 and Slot1/Port2	25GE	Service network	The ports connect to the service switches.
Port4 and Port5	GE	Management network	The ports connect to the management switch.
Mgmt	GE	BMC network	The port connects to the BMC switch.

3.3.2.5.5 OceanStor Pacific 9520 Kunpeng-based 14-Slot

Figure 3-36 shows an example of planning ports for a storage node.

Figure 3-36 Example of planning ports for a storage node

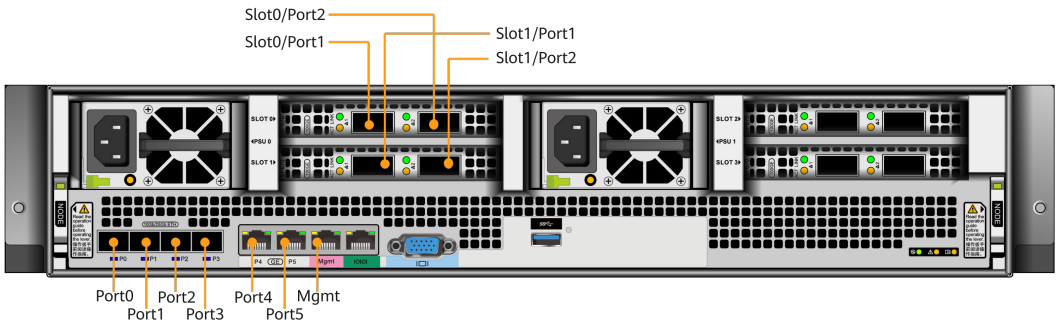


Table 3-49 describes the port usage when the storage network is 10GE TCP, 25GE TCP, or 25GE RoCE and the service network is 10GE TCP or 25GE TCP.

Table 3-49 Port usage

Port Name	Port Type	Access Network	Description
Slot0/Port1 and Slot0/Port2	10GE or 25GE	Service network	The ports connect to the service switches.
Port0 and Port1	10GE or 25GE	Storage network	The ports connect to the storage switches.
Port4 and Port5	GE	Management network	The ports connect to the management switch.

Copyright © Huawei Technologies Co., Ltd.

Port Name	Port Type	Access Network	Description
Mgmt	GE	BMC network	The port connects to the BMC switch.

3.3.2.6 Network Example

The number of IP addresses required by each network is as follows:

- Number of management network IP addresses = Number of service switches + Number of storage switches + Number of leaf switches + Number of BMC switches + Number of management switches + Number of storage nodes (excluding the storage nodes deployed on the same servers as the management nodes) + Number of management nodes x 2 + 2
- Number of BMC network IP addresses = Number of storage nodes
- Number of storage network IP addresses = Number of storage nodes x 3
- Number of file service network IP addresses (bond network) = Number of storage nodes x Number of access zones + Number of subnets

This section describes the network IP address planning when four storage nodes (management nodes are deployed on the same servers as the storage nodes), two storage switches, two service switches, two leaf switches, one management switch, and one BMC switch are deployed.

Management Network

Table 3-50 describes the IP address planning for the management network.

Table 3-50 IP address planning for the management network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Floating management IP address for the external management network	Logical management port	10.110.100.100	255.255.255.0	10.110.100.1
Floating management IP address for the internal management network	Logical management port	172.16.0.12	255.255.255.0	172.16.0.1

Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Internal management network IP address for storage node 1 (management node 1)	Shared with a storage network port	172.16.0.13 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
Internal management network IP address for storage node 2 (management node 2)	Shared with a storage network port	172.16.0.15 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
Management network IP address for storage node 3	Shared with a storage network port	172.16.0.17 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
Management network IP address for storage node 4	Shared with a storage network port	172.16.0.19 (shared with a storage network IP address)	255.255.255.0	172.16.0.1
External management network IP address for storage node 1 (management node 1)	NIC1-1 port	10.110.100.106	255.255.255.0	10.110.100.1
External management network IP address for storage node 2 (management node 2)	NIC1-1 port	10.110.100.107	255.255.255.0	10.110.100.1

 Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Management network IP address for the BMC switch	MEth0/0/0	10.110.100.110	255.255.255.0	10.110.100.1
Management network IP address for the management switch	MEth0/0/0	10.110.100.111	255.255.255.0	10.110.100.1
Management network IP address for storage switch 1	MEth0/0/0	10.110.100.112	255.255.255.0	10.110.100.1
Management network IP address for storage switch 2	MEth0/0/0	10.110.100.113	255.255.255.0	10.110.100.1
Management network IP address for leaf switch 1	MEth0/0/0	10.110.100.114	255.255.255.0	10.110.100.1
Management network IP address for leaf switch 2	MEth0/0/0	10.110.100.115	255.255.255.0	10.110.100.1

BMC Network

Table 3-51 describes the IP address planning for the BMC network.

Table 3-51 IP address planning for the BMC network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
BMC network IP address for storage node 1	Mgmt	10.120.100.13	255.255.255.0	10.120.100.1

Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
BMC network IP address for storage node 2	Mgmt	10.120.100.14	255.255.255.0	10.120.100.1
BMC network IP address for storage node 3	Mgmt	10.120.100.15	255.255.255.0	10.120.100.1
BMC network IP address for storage node 4	Mgmt	10.120.100.16	255.255.255.0	10.120.100.1

Storage Network

Table 3-52 describes the IP address planning for the storage network.

Table 3-52 IP address planning for the storage network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Storage network IP addresses for storage node 1	Storage network ports providing multiple IP addresses	172.16.0.13	255.255.255.0	172.16.0.1
		172.16.0.14	255.255.255.0	172.16.0.1
Storage network IP addresses for storage node 2	Storage network ports providing multiple IP addresses	172.16.0.15	255.255.255.0	172.16.0.1
		172.16.0.16	255.255.255.0	172.16.0.1
Storage network IP addresses for storage node 3	Storage network ports providing multiple IP addresses	172.16.0.17	255.255.255.0	172.16.0.1
		172.16.0.18	255.255.255.0	172.16.0.1
Storage network IP addresses for storage node 4	Storage network ports providing multiple IP addresses	172.16.0.19	255.255.255.0	172.16.0.1
		172.16.0.20	255.255.255.0	172.16.0.1

Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Control network IP address for storage node 1	Storage network ports providing multiple IP addresses	172.16.0.129	255.255.255.0	172.16.0.1
Control network IP address for storage node 2	Storage network ports providing multiple IP addresses	172.16.0.130	255.255.255.0	172.16.0.1
Control network IP address for storage node 3	Storage network ports providing multiple IP addresses	172.16.0.131	255.255.255.0	172.16.0.1
Control network IP address for storage node 4	Storage network ports providing multiple IP addresses	172.16.0.132	255.255.255.0	172.16.0.1

File Service Network

Table 3-53 describes the IP address planning for the file service network. One access zone and one subnet are used as an example.

Table 3-53 IP address planning for the file service network

IP Address Name	Port	IP Address	Subnet Mask	Gateway
IP address of the general DNS service in the subnet	Service bond port of a node	192.168.100.10	255.255.255.0	192.168.100.1

Copyright © Huawei Technologies Co., Ltd.

IP Address Name	Port	IP Address	Subnet Mask	Gateway
Access zone IP address pool	Bond port	192.168.100.11 to 192.168.100.16 **NOTE** • Number of IP addresses in the access zone IP address pool = Number of storage nodes x *N* (*N* indicates the number of access zones). For example, if one access zone is configured, the number of IP addresses in the IP address pool is six. • The service network IP addresses can be inconsecutive. This example uses consecutive IP addresses.	255.255.255.0	192.168.100.1

3.3.3 File/Object Service (DPC and Standard Protocol Hybrid Scenario)

3.3.3.1 Overview

Network Introduction

The following networks are involved for OceanStor Pacific series in the DPC and standard protocol hybrid scenario:

- BMC network

  The BMC network connects to Mgmt ports of nodes to enable remote device management.
- Management network
  - The external management network is used by users to access DeviceManager and the CLI, and for communication between storage nodes and external HCS/HCSO O&M systems.
  - The internal management network is used for management data communication between the management and storage nodes.
- Control network
  - Transmits control messages in the system.
  - Adopts a floating IP address that floats among storage network ports on nodes.
- Storage network

 Copyright © Huawei Technologies Co., Ltd.

The front-end storage network and back-end storage network are shared for data communication between storage nodes and between DPC and OSD.

- Service network

  Enables data communication between storage nodes and users' service network and supports NFS/CIFS/object interface protocol.

3.3.3.2 Networking Scenarios

Table 3-54 shows the DPC and standard protocol hybrid networking scenarios supported by OceanStor Pacific 9540 Kunpeng-based and OceanStor Pacific 9920 Kunpeng-based.

Table 3-54 Networking scenarios

Device Name	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example	Service Network (NIC Example)	Service Switch Example
OceanStor Pacific 9540 Kunpeng-based	3.3.3.5.1 OceanStor Pacific 9540 Kunpeng-based	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850	25GE (Hi1822V120)	CE6865
Tiering scenario: OceanStor Pacific 9540 Kunpeng-based + OceanStor Pacific 9920 Kunpeng-based (SAS SSD)	3.3.3.5.1 OceanStor Pacific 9540 Kunpeng-based	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850	25GE (Hi1822V120)	CE6865
	3.3.1.5.2 OceanStor Pacific 9920 Kunpeng-based (SAS SSD)	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850	Not connected to the service network	Not connected to the service network

Copyright © Huawei Technologies Co., Ltd.

Device Name	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example	Service Network (NIC Example)	Service Switch Example
Tiering scenario: OceanStor Pacific 9920 Kunpeng-based (SAS SSD) + OceanStor Pacific 9546 (Two CPUs per Node)	3.3.1.5.2 OceanStor Pacific 9920 Kunpeng-based (SAS SSD)	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850	Not connected to the service network	Not connected to the service network
	3.2.3.5.2 OceanStor Pacific 9546 (Two CPUs per Node)	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850	25GE (Hi1822V120)	CE6865
Tiering scenario: OceanStor Pacific 9920 Kunpeng-based (palm-sized NVMe SSD) + OceanStor Pacific 9546	3.3.1.5.3 OceanStor Pacific 9920 Kunpeng-based (Palm-sized NVMe SSD)	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850	Not connected to the service network	Not connected to the service network

Copyright © Huawei Technologies Co., Ltd.

Device Name	Port Planning	External Management Network (NIC Example)	Leaf Switch Example	Storage Network (NIC Example)	Storage Switch Example	Service Network (NIC Example)	Service Switch Example
	3.2.3.5.2 OceanStor Pacific 9546 (Two CPUs per Node)	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850	25GE (Hi1822V120)	CE6865
Tiering scenario: OceanStor Pacific 9920 Kunpeng-based (palm-sized NVMe SSD) + OceanStor Pacific 9546 (Two CPUs per Node)	3.3.1.5.3 OceanStor Pacific 9920 Kunpeng-based (Palm-sized NVMe SSD)	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850	100GE RoCE (sharing network ports with the storage network)	CE8850
	3.2.3.5.2 OceanStor Pacific 9546 (Two CPUs per Node)	GE (LOM)	Switch that supports GE	100GE RoCE (CX5)	CE8850	25GE TCP (sharing network ports with the storage network)	CE6865

NOTE

The Hi1822 and Hi1822V120 NICs have four ports (when the Hi1822V120 NIC is used, only the four-port NIC is used). Only the first two ports of the NICs are used.

Copyright © Huawei Technologies Co., Ltd.

3.3.3.3 Network Requirements

This section describes the network requirements in the DPC and standard protocol hybrid scenario, as shown in **Table 3-55**.

Table 3-55 Network requirements

Network Type	Network Requirements
BMC network	• A BMC network can be a GE network. • The number of BMC network ports on each storage node can be one or two.
Service network	The TCP/IP protocol is supported. It supports 25GE networks and allows you to configure only bond4.
Storage network	• The RoCE protocol and 100GE network are supported, and only multiple IP addresses can be configured. **NOTE** When the storage network does not use the bond network, each port on the storage network can be bonded to one IP address. • The storage networks of all nodes use the same VLAN ID.
Control network	If the storage network uses multiple IP addresses, select a port on the storage network to configure one floating IP address for the control network. The control network and the storage network can be in the same subnet (recommended) or different subnets. If they are in the same subnet, they must use different IP address segments.
External management network	The TCP/IP protocol is supported. The number of network ports can be one or two. You are advised to bond two network ports in bond1 mode.
Internal management network	It is integrated with the storage network, and the two networks share ports and IP addresses.

NOTICE

All networks support only IPv4 addresses.

3.3.3.4 Network Solution

Figure 3-37 shows the network solution.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-37 Network solution

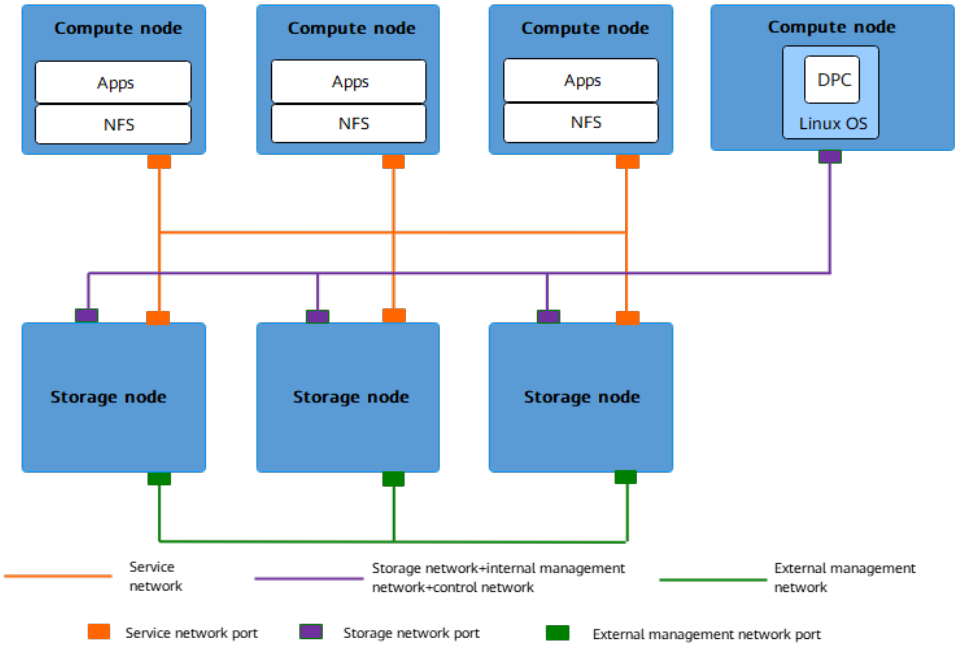
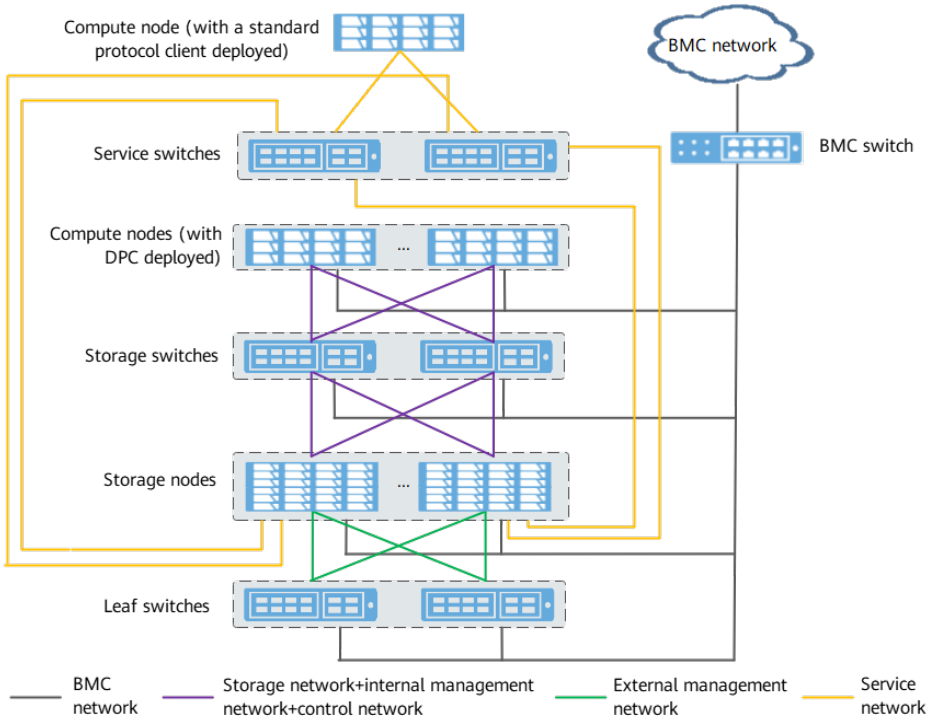


Figure 3-38 shows the physical network.

Figure 3-38 Physical network



 Copyright © Huawei Technologies Co., Ltd.

Table 3-56 describes the network requirements and IP address planning.

Table 3-56 Network requirements and IP address planning

Device Type	Requirements	IP Address Planning
Compute node	The storage network of a compute node must be able to communicate with the storage network of a storage node through a distributed gateway.	Planned and allocated by the HCS/HCSO network in a unified manner.
Storage/ Management node (the first two storage nodes are also management nodes)	Internal management network: shares network ports and IP addresses with the storage network. External management network: Each storage node provides two management network ports to connect to the external management network (One or two network ports can be used. When two network ports are used, you are advised to bond them in bond1 mode.). **NOTE** • The external management network is used by users to access DeviceManager and the CLI, and for communication between storage nodes and external HCS/HCSO O&M systems. • The internal management network is used for management data communication between the management and storage nodes. • The IP addresses of the external and internal management networks must be in different network segments.	• Configure one floating IP address for the external management network of each cluster for cluster management. • Configure one floating IP address for the internal management network of each cluster. • Configure one management IP address for the external management network on each storage node. • Configure two management IP addresses for the internal management network (same as the IP addresses of the storage network) on each storage node.
	Storage network: Two ports are provided for accessing the storage network using multiple IP addresses.	Planned and allocated by the HCS/HCSO network in a unified manner. **NOTE** If you plan to expand capacity, you are advised to reserve storage network IP addresses for nodes that will be added.

 Copyright © Huawei Technologies Co., Ltd.

Device Type	Requirements	IP Address Planning
	Control network: If any port on the storage network is used, the control network IP address automatically floats on the storage network ports.	The control network IP address and the storage network IP address cannot be in the same network segment but must be in the same subnet.
	Service network: Two ports are provided to form bond4 for accessing the service network. **NOTE** • The Hi1822 and Hi1822V120 NICs have four ports (when the Hi1822V120 NIC is used, only the four-port NIC is used). Only the first two ports of the NICs are used.	Configure one VTEP IP address for establishing a VXLAN tunnel with compute nodes (ECS).
	BMC network: One port is provided for accessing the BMC network.	Configure one IP address for the BMC network.
Storage switch	• Provided by the HCS/HCSO network. • The flow control priority is 32 and the queue is 4. • The oversubscription ratio is 1:1.	Planned and allocated by the HCS/HCSO network in a unified manner.
Leaf switch	• One management network port is provided for accessing the management network. • Switches must be de-stacked.	Configure one management network IP address for each switch. **NOTE** In the DPC and standard protocol hybrid scenario, if the uplink traffic to leaf switches contains both service network traffic and management network traffic, the uplink bandwidth needs to be calculated based on the number of nodes.

3.3.3.5 Planning Ports for Nodes

3.3.3.5.1 OceanStor Pacific 9540 Kunpeng-based

Figure 3-39 and **Figure 3-40** show examples of planning ports for a storage node.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-39 Example of planning ports for a storage node (using 2-port NICs)

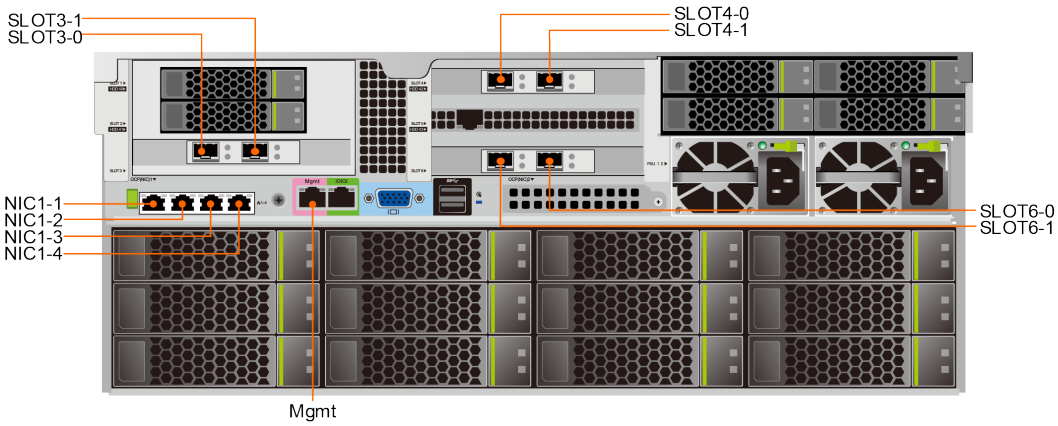


Figure 3-40 Example of planning ports for a storage node (using 4-port NICs)

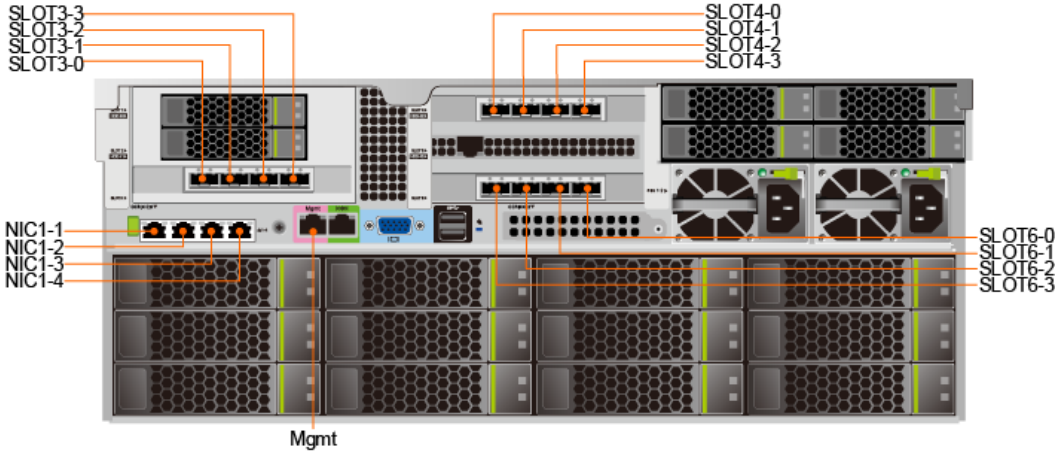


Table 3-57 describes the ports on a node when the service network is 25GE and the storage network is 100GE RoCE.

Table 3-57 Port usage

Port Name	Port Type	Access Network	Description
SLOT3-0 and SLOT3-1	25GE	Service network	The ports connect to the service switches.
SLOT4-0 and SLOT4-1	100GE	Storage network/ Control network/ Internal management network	The ports connect to the storage switches.
NIC1-1 and NIC1-2	GE	External management network	The ports connect to the leaf switches.

 Copyright © Huawei Technologies Co., Ltd.

Port Name	Port Type	Access Network	Description
Mgmt	GE	BMC network	The port connects to the BMC switch.

3.3.3.6 Network Example

This section uses seven nodes (one compute node that uses standard protocols, two compute nodes that use DPC, and four storage nodes) as an example to describe the IP address planning.

For details about the networking of the two compute nodes that use DPC and the four storage nodes, see **3.3.1.6 Network Example**.

In addition, the number of service IP addresses planned for each of the four storage nodes is as follows:

- Number of service network IP addresses (bond network) = Number of storage nodes x Number of access zones + Number of subnets

3.4 LLD Planning and Implementation

3.4.1 Manually Filling out the Deployment File Template

This section describes how to obtain and manually fill out the deployment file template for use during system deployment.

Prerequisites

- You have planned system deployment parameters and IP addresses.
- SmartKit that matches the storage system version has been installed on the installation PC.

  You can log in to Huawei technical support website (**https://support.huawei.com/enterprise/**), enter the product model of the storage system in the search box, and select the suggested path to go to the documentation page of the product model. Search for and download the version mapping table of the storage system version to obtain the SmartKit version that matches the product model. Then choose **Support** > **Tools** > **Enterprise Data Center** > **SmartKit** and download the SmartKit tool of the required version.

Procedure

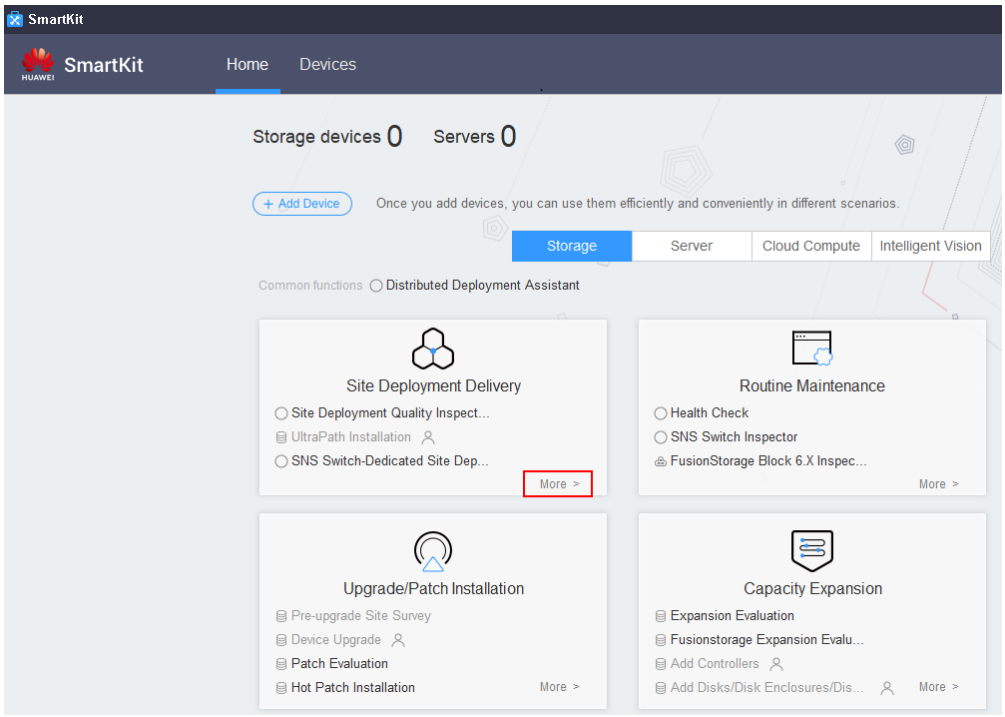
Step 1 Log in to Huawei technical support website (**https://support.huawei.com/enterprise/**) and enter **SmartKit** in the search box to find the user guide of the desired version. Then install and run SmartKit by referring to sections "Installing SmartKit" and "Running SmartKit".

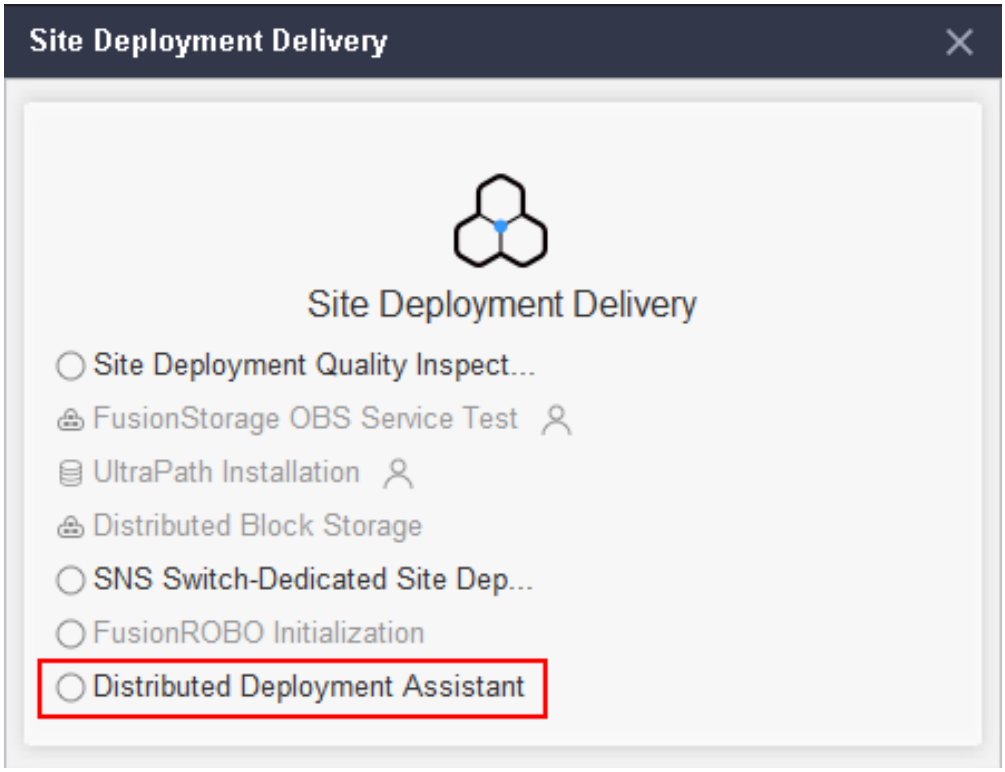
Step 2 Install the Distributed Deployment Assistant tool by referring to section "Installing Functions" in the SmartKit user guide. Online installation is recommended. If you

 Copyright © Huawei Technologies Co., Ltd.

adopt offline installation, log in to Huawei technical support website (**https://support.huawei.com/enterprise/**) and enter **DistributedDeployHelper.zip** in the search box to obtain the offline installation package of Distributed Deployment Assistant.

Step 3 After installing the Distributed Deployment Assistant, go to the **Home** page of SmartKit, choose **Site Deployment Delivery** > **More**, and select **Distributed Deployment Assistant** in the dialog box that is displayed.





 Copyright © Huawei Technologies Co., Ltd.

Step 4 Start the Distributed Deployment Assistant, click **Deployment File Template** and complete the node, network, and cluster planning.

----End

 Copyright © Huawei Technologies Co., Ltd.

4 Hardware Installation

For details about hardware installation, see *OceanStor Pacific Series 8.2.1 Hardware Installation Guide*.

 Copyright © Huawei Technologies Co., Ltd.

5 Installing Software

5.1 Before You Start
5.2 Installation Overview
5.3 Installation PC Requirements
5.4 Installing Software
5.5 Appendix

5.1 Before You Start

Instructions on Using the Security Sandbox

- Enabling the security sandbox function can improve system security and prevent untrusted users or attackers from logging in to the storage operating system (OS) through SSH to perform malicious operations. When the OceanStor Pacific Series 8.2.1RC1 software or later is installed for the first time, the security sandbox is automatically enabled on the added storage nodes.
- After the security sandbox is enabled, users can only use the **cli_portal** command after logging in to the OS. The **cli_portal** command can be used to run the CLI, **minisystem**, and **diagnose** (only for FSA nodes) commands. All commands or scripts that are directly executed on the OS cannot be executed, including common **ls**, **rm**, and **cat** commands, as shown in the following figure:

```
FSMA:cliportal> cat /etc/passwd
Error : Command 'cat' does not exist or has an incorrect format.
Try 'help' for more information.
```

- Before executing OS commands, disable the security sandbox by referring to **Routine Management** > **Managing a Cluster System** > **Managing Hardware Information** > **Disabling Security Sandbox** in *OceanStor Pacific Series 8.2.1 Administrator Guide*. After the OS commands are executed, enable the security sandbox by referring to **Routine Management** > **Managing a Cluster System** > **Managing Hardware Information** > **Enabling Security Sandbox** in *OceanStor Pacific Series 8.2.1 Administrator Guide*.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- You can also run the **closesandbox** command on the cli_portal to disable the security sandbox.
- The security sandbox supports only the standard storage OS. Other non-standard OSs do not support the security sandbox function.
- After the security sandbox function is disabled, the system is no longer protected by any security sandbox.
- After the security sandbox is disabled, you need to restart the session for the setting to take effect. After the security sandbox is disabled, you can enable it as required.
- The security sandbox is applicable to OceanStor Pacific series 8.1.3 and later versions.

5.2 Installation Overview

This chapter describes the key points of the installation solution, helping you quickly understand how to install OceanStor Pacific series software.

Select the desired installation process in the following sections according to the scenario of the file service to be installed (standard protocol scenario, DPC scenario, or DPC and standard protocol hybrid scenario) and the installation mode (LLD-based or wizard-based configuration mode). During software installation, configure management and service switches first (service switches are not required in the DPC scenario). Then configure or install other software:

- In LLD-based configuration mode, you need to prepare an LLD configuration file, import the LLD configuration file to SmartKit to initialize nodes, and import the LLD configuration file to DeviceManager Client to complete one-click installation.
- In wizard-based configuration mode, you need to check the OS, firmware, and drivers of each storage node, configure networks for each node, use the DeviceManager Client tool to install all management nodes, and then use the management nodes to install storage nodes.

  NOTE

  The OS and related firmware and drivers have been installed before the delivery of OceanStor Pacific series. If the versions of the OS and related firmware and drivers are the same as those in the version mapping, you do not need to install them separately and you can use the DeviceManager Client tool to install OceanStor Pacific series software. If the versions of the OS and related firmware and drivers are different from those in the version mapping, reinstall the OS and related firmware and drivers on each node.

5.3 Installation PC Requirements

OceanStor-Pacific_8.2.1RC1_DeviceManagerClient.zip is run on the installation PC and used to install and deploy OceanStor Pacific series software. **Table 5-1** lists the requirements.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-1 Installation PC requirements

Item	Requirements
OS	For details about DeviceManager Client's requirements for the OS and browser, visit **Huawei Storage Interoperability Navigator**.
Browser	
Available capacity of the disk where DeviceManager Client is installed	8 GB or more
Memory	1 GB or more
OS time	Set the value to the current time zone and time.
PuTTY	Indicates a cross-platform remote access tool, used to access each node in the Windows OS during software installation.
FileZilla	Indicates a cross-platform file transfer tool, used to transfer files between Windows and Linux OSs.

5.4 Installing Software

5.4.1 Installing the File Service (Standard Protocol Scenario)

5.4.1.1 Node Requirements

Requirements on Node OS Time

The OS time of all nodes must be the same as the local time.

Management Node Deployment Requirements

Management nodes can be deployed only in active/standby mode, and the active and standby management nodes must use the same platform architecture (Kunpeng or x86).

Requirements for Compute and Storage Nodes

In RoCE networking scenarios, the lldpad service must be disabled. Otherwise, nodes will be isolated and services will be interrupted.

Log in to a node as user **fsadmin**, run the **su - root** command to switch to user **root**, and run the following command to disable the lldpad service:

```
systemctl stop lldpad.service
```

 Copyright © Huawei Technologies Co., Ltd.

5.4.1.2 Installation Process

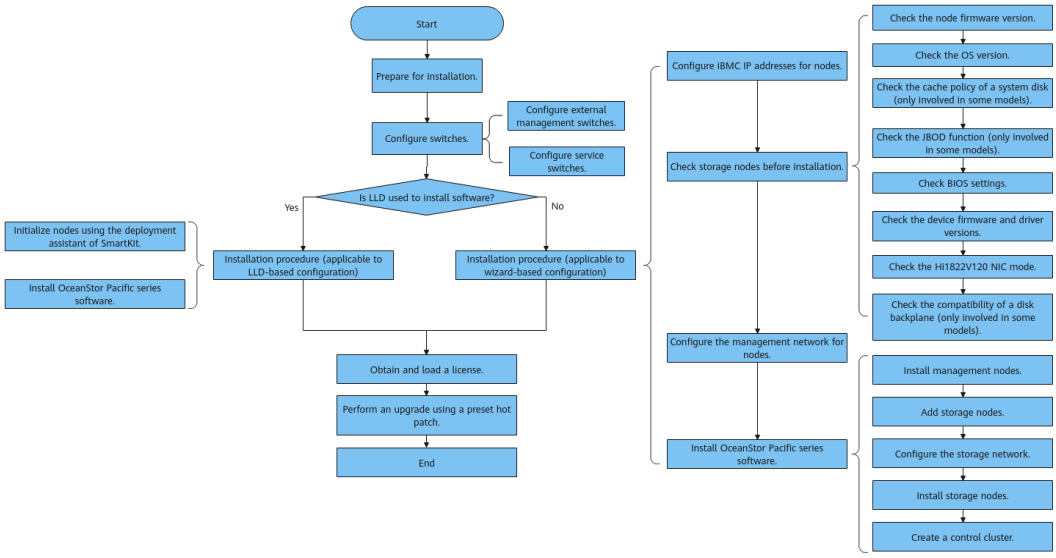
Software installation in the standard protocol scenario includes software installation and deployment on management nodes and storage nodes. A management node and a storage node are deployed on the same server.

The software can be installed in LLD-based or wizard-based configuration mode. The LLD-based configuration mode is recommended. **Figure 5-1** shows the installation process of the two modes.

NOTE

- In LLD-based configuration mode, use the LLDesigner tool to plan nodes, networks, and clusters, export the deployment configuration file, and use the deployment assistant of SmartKit to initialize the nodes based on the deployment configuration file. Node initialization includes: configuring iBMC IP addresses of nodes, checking storage nodes before installation, and configuring management and storage networks for nodes. Then use DeviceManager Client to install the OceanStor Pacific series software in LLD-based configuration mode.
- In wizard-based configuration mode, manually add nodes, configure networks, and create a control cluster on DeviceManager for OceanStor Pacific series software installation.

Figure 5-1 Installation process (standard protocol scenario)



During the OceanStor Pacific series installation process, you need to configure IP addresses and related components for nodes of each role. **Table 5-2** describes the network configuration of each hardware type.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-2 Network configurations

Hardware Type	Network to Be Configured	Deployment Requirements on Nodes
OceanStor Pacific 9550/OceanStor Pacific 9546/ OceanStor Pacific 9520/OceanStor Pacific 9540/ OceanStor Pacific 9920/OceanStor Pacific 9350/ OceanStor Pacific 9346/OceanStor Pacific 9340	• External management network **NOTE** • Network protocol: TCP • Networking mode: 1. OceanStor Pacific 9550/ OceanStor Pacific 9350: The number of network ports can be only one and bond is not supported. 2. OceanStor Pacific 9546/ OceanStor Pacific 9346: The number of network ports can be one or two. Two management network ports can be bonded only in bond1 mode. 3. OceanStor Pacific 9520/ OceanStor Pacific 9540/ OceanStor Pacific 9920/ OceanStor Pacific 9340: The number of network ports can be one or two. You are advised to bond two network ports in bond1 mode. • Storage network (front- and back-end shared) **NOTE** Network protocol/Networking mode: RoCE/multi-IP or TCP/ bond4 (recommended) • Shared internal management network and storage network	• OceanStor Pacific 9540/OceanStor Pacific 9520/ OceanStor Pacific 9920/OceanStor Pacific 9340/ OceanStor Pacific 9546 (One Node per Chassis, Two CPUs per Node)/ OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node): ≥ 3 • OceanStor Pacific 9550/OceanStor Pacific 9350/ OceanStor Pacific 9546 (Two Nodes per Chassis): ≥ 4

5.4.1.3 Preparing for Installation

5.4.1.3.1 Preparing Documents and Tools

Documents

Table 5-3 describes how to obtain documents.

Copyright © Huawei Technologies Co., Ltd.

Table 5-3 Obtaining documents

Name	How to Obtain
OceanStor Pacific Series 8.2.1RC1 Version Mapping	This document defines the version numbers of the storage software, node firmware, NIC driver and firmware, RAID controller card driver and firmware used with OceanStor Pacific series, and the addresses for obtaining them. For enterprise users, log in to **https://support.huawei.com/enterprise**. For carrier users, log in to **https://support.huawei.com**. Enter **OceanStor Pacific** in the search box and click the suggested path to enter the product page. Search for and download the document of the desired version.
OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)	For enterprise users, log in to **https://support.huawei.com/enterprise**. For carrier users, log in to **https://support.huawei.com**. Enter the document name in the search box and click the search button. Search for and download the document of the desired version.
OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide	
CE6800 series switch documents	For enterprise users, log in to **https://support.huawei.com/enterprise**. For carrier users, log in to **https://support.huawei.com**. Enter **CloudEngine 58&68&78&88&98** in the search box and click the suggested path to enter the product page. Search for and download the document of the desired version.
CE8800 series switch documents	
CE9800 series switch documents	
CE16800 series switch documents	For enterprise users, log in to **https://support.huawei.com/enterprise**. For carrier users, log in to **https://support.huawei.com**. Enter **CloudEngine 12800&16800** in the search box and click the suggested path to enter the product page. Search for and download the document of the desired version.
ES3000 V5 NVMe PCIe SSD User Guide	For enterprise users, log in to **https://support.huawei.com/enterprise**. For carrier users, log in to **https://support.huawei.com**. Enter **ES3000 V5** in the search box and click the suggested path to enter the product page. Search for and download the document of the desired version.

 Copyright © Huawei Technologies Co., Ltd.

Tools

Table 5-4 lists the required tools.

Table 5-4 Tools

Item	Description
One network cable	Connects an installation PC to a storage node or switch.
One console cable	Connects switches. One end of the console cable is an RJ-45 port, and the other end is a DB-9 port (connecting to an installation PC). If the installation PC has no serial port, prepare a USB-to-serial cable.

5.4.1.3.2 Obtaining Software Packages

Table 5-5 and Table 5-6 describe how to obtain the OceanStor Pacific series software package, device firmware, and drivers.

NOTE

The version of the obtained software package is subject to *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

Copyright © Huawei Technologies Co., Ltd.

Table 5-5 Obtaining the OceanStor Pacific series software package

Type	Name	Description	How to Obtain
Software package	**OceanStor-Pacific_8.2.1RC1.tar.gz**	OceanStor Pacific series software package, including all components of OceanStor Pacific series	• You can obtain the OceanStor Pacific series software package, deployment tool, tool set, OS software package, and data pilot service package from Huawei official website. For enterprise users, log in to **https://support.huawei.com/enterprise**. For carrier users, log in to **https://support.huawei.com**. In the search box, enter **OceanStor Pacific** and click the suggested path to enter the corresponding product page. For enterprise users, click **Software Download**. For carrier users, click **Software**. Then, search for and download the software package of the desired version and its ***.asc** digital certificate file. • For details about other compatible OSs, visit **Huawei Storage Interoperability Navigator**. You need to prepare the OS installation package by yourself.
	OceanStor-Pacific_8.2.1RC1_DeviceManagerClient.zip	OceanStor Pacific series deployment tool, used for installing the OceanStor Pacific series software For details about supported OS and browser versions, visit **Huawei Storage Interoperability Navigator**.	
	• OS software package applicable to Kunpeng-based nodes: **OceanStor-Pacific**_8.2.1RC1_**OS***xxx*.**SP***xx*_**aarch64.tgz** • OS software package applicable to x86-based nodes: **OceanStor-Pacific**_8.2.1RC1_**OS***xxx*.**SP***xx*_**x86-64.tgz**	Storage node OS software package. For details about the package name, see *OceanStor Pacific Series 8.2.1RC1 Version Mapping*. If the version of the storage node OS software package does not meet the requirements in the version mapping, you need to reinstall the OS software package.	
	OceanStor-Pacific_8.2.1RC1_Tools.tar.gz	OceanStor Pacific series tool set, used to install the dependency packages of third-party OSs	

 Copyright © Huawei Technologies Co., Ltd.

Type	Name	Description	How to Obtain
	OceanStor-Pacific_8.2.1RC1_Value-addedService.tar.gz	Data pilot service package, used to configure the SmartIndexing function	

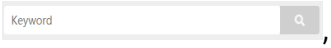
 Copyright © Huawei Technologies Co., Ltd.

Type	Name	Description	How to Obtain
Software digital signature validation tool	PGP Verify	To prevent a software package from being maliciously tampered with during transmission or storage, download the corresponding digital signature file for integrity verification when downloading the software package. After the software package is downloaded, verify its PGP digital signature according to *OpenPGP Signature Verification Guide*. If the software package fails the verification, do not use the software package, and contact Huawei technical support engineers. Before a software package is used in installation or upgrade, its digital signature also needs to be verified according to *OpenPGP Signature Verification Guide* to ensure that the software	For carrier users: **https://support.huawei.com/carrier/digitalSignatureAction** For enterprise users: **https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054**

 Copyright © Huawei Technologies Co., Ltd.

Type	Name	Description	How to Obtain
		package is not tampered with.	

Table 5-6 Device drivers and firmware

Type	Description	How to Obtain
Half-palm NVMe SSD, NVMe SSD card, NVMe SSD, and HDD drivers, firmware, and tools	For details about the firmware, driver, and tool versions used with the hardware, see *OceanStor Pacific Series 8.2.1RC1 Version Mapping*. If the device driver, firmware, and tool versions are earlier than those required in the version mapping, you need to upgrade them. If the device driver, firmware, and tool versions are later than those required in the version mapping, you need to reinstall them.	For details about the firmware, driver, and tool package names used with the hardware and how to obtain the packages, see *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.
IB and RoCE NIC drivers and firmware		
RAID controller card firmware and driver		
CLI tools of some RAID controller cards	For some RAID controller cards, a CLI tool needs to be installed for disk configuration and management. Query the models of the RAID controller cards where a CLI tool needs to be installed, as well as the name and version of the CLI tool from **Huawei Storage Interoperability Navigator**.	Obtain the CLI tool from the official website of the RAID controller card manufacturer. You can obtain the CLI tool as follows: 1. Log in to the official website of the RAID controller card manufacturer. 2. Enter the tool name in search box  , click the search icon, click **Management Software and Tools**, and then click the name of the tool to be downloaded in the **Title** column.

 Copyright © Huawei Technologies Co., Ltd.

Type	Description	How to Obtain
Node firmware	For details about the firmware version used with the node, see *OceanStor Pacific Series 8.2.1RC1 Version Mapping*. If the node firmware version does not meet the requirements in the version mapping, you need to upgrade the firmware.	For details about the firmware package name used with the node and how to obtain the package, see *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

5.4.1.4 Configuring Switches

5.4.1.4.1 Switch Configuration Requirements and Configuration Data

Table 5-7 lists the switch configuration requirements.

Table 5-7 Switch configuration requirements

Type	Configuration Requirements
External management switch	Use the non-stacking mode. A VLAN needs to be configured for TCP/IP.
Service switch	

Table 5-8 describes the parameters used in the subsequent configuration commands. Replace the parameters according to the actual situation.

Table 5-8 Configuration data

Type	Sub-type	Parameter	Remarks
External management switch	External management plane VLAN	manage-vlan	In the port parameters, a letter indicates only a digit. The actual port prevails.
	External management plane gateway	manage-ip	
	Subnet mask	Subnet mask or prefix	
	External management ports	*1/0/e* to *1/0/n*	

Copyright © Huawei Technologies Co., Ltd.

Type	Sub-type	Parameter	Remarks
	Uplink Eth-Trunk	up-eth	
	Uplink ports	1/0/*c* to 1/0/*d*	
Service switch	Service plane VLAN	front-vlan	
	Service plane gateway	front-ip	
	Subnet mask	Subnet mask or prefix	
	Service ports	1/0/*a* to 1/0/*b*	
	Uplink ports	1/0/*x* to 1/0/*y*	
	Service Eth-Trunk	service-eth1 to service-eth*n*	
	Uplink Eth-Trunk	up-eth	

5.4.1.4.2 Configuring GE External Management Switches

Context

Replace the italic parameters in the commands based on the site requirements. For details about the parameters, see **5.4.1.4.1 Switch Configuration Requirements and Configuration Data**.

Procedure

Step 1 Log in to a switch. For details, see **5.5.2.1 Logging In to a Switch**.

Step 2 Configure a management network VLAN.

```
<HUAWEI> system-view
[~HUAWEI] vlan manage-vlan
[*HUAWEI-Vlanmanage-vlan] description management
[*HUAWEI-Vlanmanage-vlan] commit
[*HUAWEI-Vlanmanage-vlan] quit
```

Step 3 Configure a management network gateway.

NOTE

If the gateway has been configured, skip this step.

```
[*HUAWEI] interface vlanif manage-vlan
[*HUAWEI-Vlanmanage-vlan] ip address manage-ip Subnet mask
[*HUAWEI-Vlanmanage-vlan] commit
[*HUAWEI-Vlanmanage-vlan] quit
```

Step 4 Add the management ports on the switch to the port group.

 Copyright © Huawei Technologies Co., Ltd.

```
[~HUAWEI] port-group 1
[~HUAWEI-port-group1] group-member ge 1/0/e to ge 1/0/n
[*HUAWEI-port-group1] port link-type trunk
[*HUAWEI-port-group1] port trunk pvid vlan manage-vlan  #Run this command only when no VLAN is configured for the management network ports of nodes.
[*HUAWEI-port-group1] undo port trunk allow-pass vlan 1
[*HUAWEI-port-group1] port trunk allow-pass vlan manage-vlan
[*HUAWEI-port-group1] commit
[~HUAWEI-port-group1] quit
[~HUAWEI]quit
<HUAWEI> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: Y
```

Step 5 (Optional) Configure uplink ports. Uplink ports must be configured only when the switch is connected to an upper-level switch.

```
[~HUAWEI] interface eth-trunk up-eth     # Configure the ports to work in trunk mode.
[*HUAWEI-Eth-Trunkup-eth] port link-type trunk
[*HUAWEI-Eth-Trunkup-eth] undo port trunk allow-pass vlan 1
[*HUAWEI-Eth-Trunkup-eth] port trunk allow-pass vlan manage-vlan
[*HUAWEI-Eth-Trunkup-eth] trunkport interface-type 1/0/c to 1/0/d
[*HUAWEI-Eth-Trunkup-eth] commit
[~HUAWEI-Eth-Trunkup-eth] quit
[~HUAWEI]quit
<HUAWEI> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: Y
```

Step 6 Run the **display current-configuration** command to check the related configuration in sequence.

----End

5.4.1.4.3 Configuring 10GE/25GE Service Switches (Applicable to CE6865)

Context

Replace the italic parameters in the commands based on the site requirements. For details about the parameters, see **5.4.1.4.1 Switch Configuration Requirements and Configuration Data**.

Procedure

NOTE

- This section uses V200R021C00 as an example. If you encounter compatibility issues when running commands for other versions, see the product documentation of the desired switch version. For enterprise users, **click here**. For carrier users, **click here**.
- Replace the contents in italic based on site requirements.

Step 1 Log in to a switch. For details, see **5.5.2.1 Logging In to a Switch**.

Step 2 Configure the IP address of the management network port on a switch.

To configure an IPv4 address, run the following commands:

```
<HUAWEI> system-view
[~HUAWEI] interface meth 0/0/0
[~HUAWEI-MEth0/0/0] ip address Management IP address of the switch Subnet mask
[*HUAWEI-MEth0/0/0] commit
[~HUAWEI-MEth0/0/0] quit
Warning: The current configuration will be written to the device. Continue? [Y/N]: Y
```

Step 3 Configure a VLAN for the service network.

```
[~HUAWEI] vlan front-vlan
[*HUAWEI-Vlanfront-vlan] description SFS_STorage_SFS_TOR
```

```
[*HUAWEI-Vlanfront-vlan] commit
[~HUAWEI-Vlanfront-vlan] quit
```

Step 4 Configure a gateway for the service network.

```
[~HUAWEI] interface vlanif front-vlan
[*HUAWEI-Vlanfront-vlan] ip address front-ip Subnet mask
[*HUAWEI-Vlanfront-vlan] arp timeout 60
[*HUAWEI-Vlanfront-vlan] arp proxy anyway enable
[*HUAWEI-Vlanfront-vlan] mac-address 0000-5e00-0101 #The virtual MAC address range is 0000-5e00-0101 to 0000-5e00-01fe. 0000-5e00-0101 is recommended.
[*HUAWEI-Vlanfront-vlan] arp delete trigger link-down enable
[*HUAWEI-Vlanfront-vlan] arp direct-route enable
[*HUAWEI-Vlanfront-vlan] arp direct-route preference 1
[*HUAWEI-Vlanfront-vlan] commit
[~HUAWEI-Vlanfront-vlan] quit
```

Step 5 Configure Ethernet link aggregation on the service management network and add ports to it.

```
[~HUAWEI] interface eth-trunk service-eth1
[*HUAWEI-Eth-Trunkservice-eth1] mode lacp-dynamic
[*HUAWEI-Eth-Trunkservice-eth1] lacp timeout fast
[*HUAWEI-Eth-Trunkservice-eth1] lacp port-id-extension enable
[*HUAWEI-Eth-Trunkservice-eth1] trunkport 25ge 1/0/a    #Determine the port based on the NIC type and the number of bonded network ports.
[*HUAWEI-Eth-Trunkservice-eth1] commit
[~HUAWEI-Eth-Trunkservice-eth1] quit
...#Repeat the preceding operations to add other Eth-Trunk interfaces.
[~HUAWEI] interface eth-trunk service-ethn
[*HUAWEI-Eth-Trunkservice-ethn] mode lacp-dynamic
[*HUAWEI-Eth-Trunkservice-ethn] lacp timeout fast
[*HUAWEI-Eth-Trunkservice-ethn] lacp port-id-extension enable
 [*HUAWEI-Eth-Trunkservice-ethn] trunkport 25ge 1/0/b    #Determine the port based on the NIC type and the number of bonded network ports.
[*HUAWEI-Eth-Trunkservice-ethn] commit
[~HUAWEI-Eth-Trunkservice-ethn] quit
```

Step 6 Add the VLANs planned for the service network to each group of ports.

```
[~HUAWEI] interface eth-trunk service-eth1 /*service-eth is the Ethernet link aggregation port.*/
[*HUAWEI-Eth-Trunkservice-eth1] port link-type trunk
[*HUAWEI-Eth-Trunkservice-eth1] undo port trunk allow-pass vlan 1
[*HUAWEI-Eth-Trunkservice-eth1] port trunk allow-pass vlan front-vlan /*front-vlan is the VLAN ID.*/
[*HUAWEI-Eth-Trunkservice-eth1] commit
[~HUAWEI-Eth-Trunkservice-eth1] quit
...#Repeat the preceding operations to add a VLAN to each group of interfaces.
[~HUAWEI] interface eth-trunk service-ethn   /*service-eth is the Ethernet link aggregation port.*/
[*HUAWEI-Eth-Trunkservice-ethn] port link-type trunk
[*HUAWEI-Eth-Trunkservice-ethn] undo port trunk allow-pass vlan 1
[*HUAWEI-Eth-Trunkservice-ethn] port trunk allow-pass vlan front-vlan /*front-vlan is the VLAN ID.*/
[*HUAWEI-Eth-Trunkservice-ethn] commit
[~HUAWEI-Eth-Trunkservice-ethn] quit
```

Step 7 (Optional) Configure uplink ports. Uplink ports must be configured only when the switch is connected to an upper-level switch.

```
[~HUAWEI] interface eth-trunk up-eth
[*HUAWEI-Eth-Trunkup-eth] undo portswitch
[*HUAWEI-Eth-Trunkup-eth] mode lacp-static
[*HUAWEI-Eth-Trunkup-eth] ip address Management IP address of the uplink switch Subnet mask
[*HUAWEI-Eth-Trunkup-eth] trunkport 100ge 1/0/x to 1/0/y
[*HUAWEI-Eth-Trunkup-eth] commit
[~HUAWEI-Eth-Trunkup-eth] quit
[~HUAWEI] quit
<HUAWEI> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: Y
```

Step 8 Run the **display current-configuration** command to check the related configuration in sequence.

----End

 Copyright © Huawei Technologies Co., Ltd.

5.4.1.5 Installation Procedure (Applicable to LLD-based Configuration)

5.4.1.5.1 Initializing Nodes Using SmartKit

5.4.1.5.1.1 Preparing the Deployment File Template and SmartKit

Context

This section describes how to prepare the LLD configuration file, download and install the SmartKit tool, and go to the main page of the tool for initializing nodes.

Procedure

Step 1 Obtain the deployment file template. If you have obtained it, skip this step.

Use LLDesigner to prepare the deployment file template. For details, see section "LLD Planning and Implementation" in *OceanStor Pacific Series 8.2.1 Network Planning Guide (SFS)*.

Step 2 Download and install SmartKit.

- For enterprise users: Log in to **https://support.huawei.com/enterprise**, enter **SmartKit** in the search box, and select **Distributed Storage > Tools and Platform > SmartKit** from the suggested paths. The SmartKit page is displayed.
  a. On the SmartKit page, click **Software Download**, and select and download SmartKit of the latest version according to the publication date.
  b. On the SmartKit page, click **Documentation**, find *SmartKit User Guide* of the desired version, and install and run SmartKit respectively by following the instructions provided in sections "Installing SmartKit" and "Running SmartKit".
- For carrier users: Log in to **https://support.huawei.com**, enter **SmartKit** in the search box, and select **Carrier IT > Data Storage > Storage Common > SmartKit** from the suggested paths. The SmartKit page is displayed.
  a. On the SmartKit page, click **Software**, and select and download SmartKit of the latest version according to the release date.
  b. On the SmartKit page, click **Product Documentation**, find *SmartKit User Guide* of the desired version, and install and run SmartKit respectively by following the instructions provided in sections "Installing SmartKit" and "Running SmartKit".

Step 3 Install the Scale-Out Storage Deployment Delivery tool by referring to section "Installing Functions" in *SmartKit User Guide*.

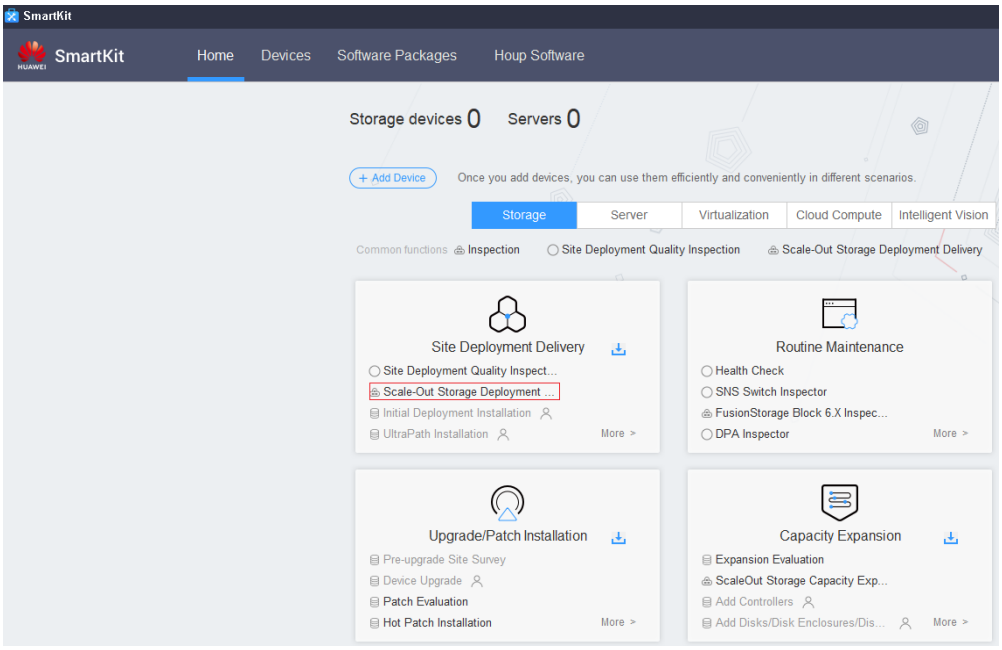
Step 4 Go to the **Site Deployment Delivery** page.

NOTE

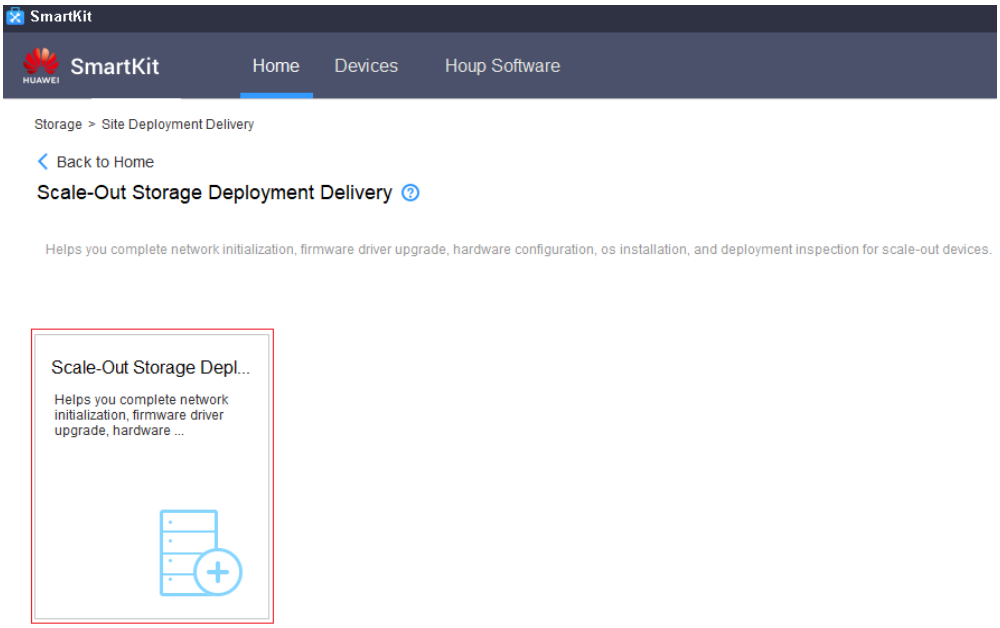
The GUI of SmartKit may vary with the version.

1. On the home page of SmartKit, choose **Site Deployment Delivery** > **Scale-Out Storage Deployment Delivery**. The **Scale-Out Storage Deployment Delivery** page is displayed.

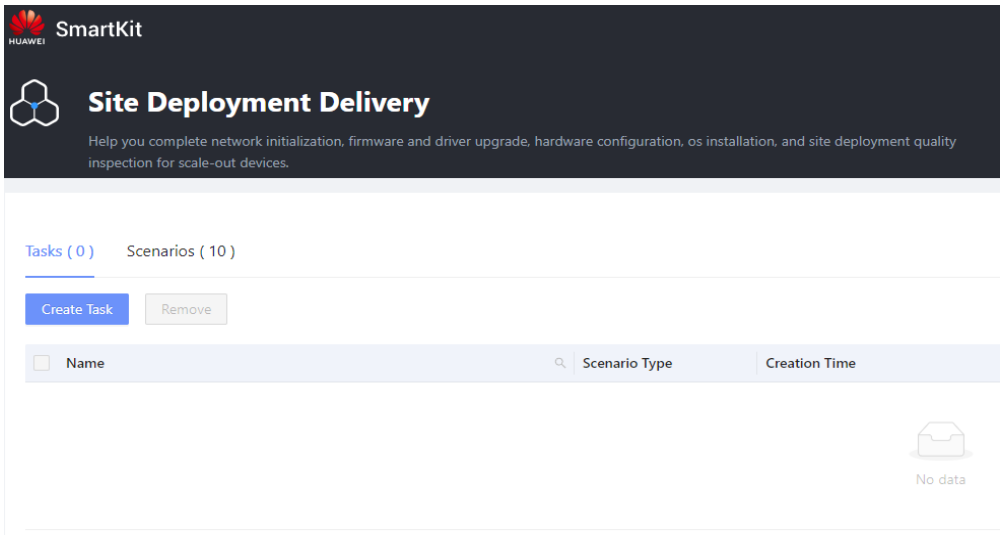
 Copyright © Huawei Technologies Co., Ltd.



2. On the **Scale-Out Storage Deployment Delivery** page, click **Scale-Out Storage Deployment Delivery**. The **Site Deployment Delivery** page is displayed.



 Copyright © Huawei Technologies Co., Ltd.



----End

5.4.1.5.1.2 Configuring iBMC IP Addresses for Nodes

?.1. Configuring iBMC IP Addresses for Nodes in Batches

Context

This section describes how to use SmartKit to batch configure iBMC IP addresses for nodes by node SN or chassis SN.

If the node name is specified when the LLD configuration file is prepared, the node name will be automatically configured when an iBMC IP address is configured. If an OceanStor Pacific 9950 device exists, you also need to configure the management IP addresses of its data cluster modules and the system will automatically change the passwords of the data cluster modules.

NOTE

The GUI of SmartKit may vary with the version.

Prerequisites

- If the storage software has been installed on the nodes to be deployed, uninstall the storage software by referring to **5.5.19 Uninstalling OceanStor Pacific Series Software**, clear the network and route information configured on the nodes, and then initialize the nodes using SmartKit.
- When using LLDesigner to prepare an LLD configuration file, you need to enter the node SN or enclosure SN.

Procedure

- If no OceanStor Pacific 9950 device exists in the cluster, configure iBMC IP addresses by referring to **Scenario 1**.
- If an OceanStor Pacific 9950 device exists in the cluster:

  Data cluster modules provide the back-end network switching function for OceanStor Pacific 9950 scale-out storage clusters. A data cluster module

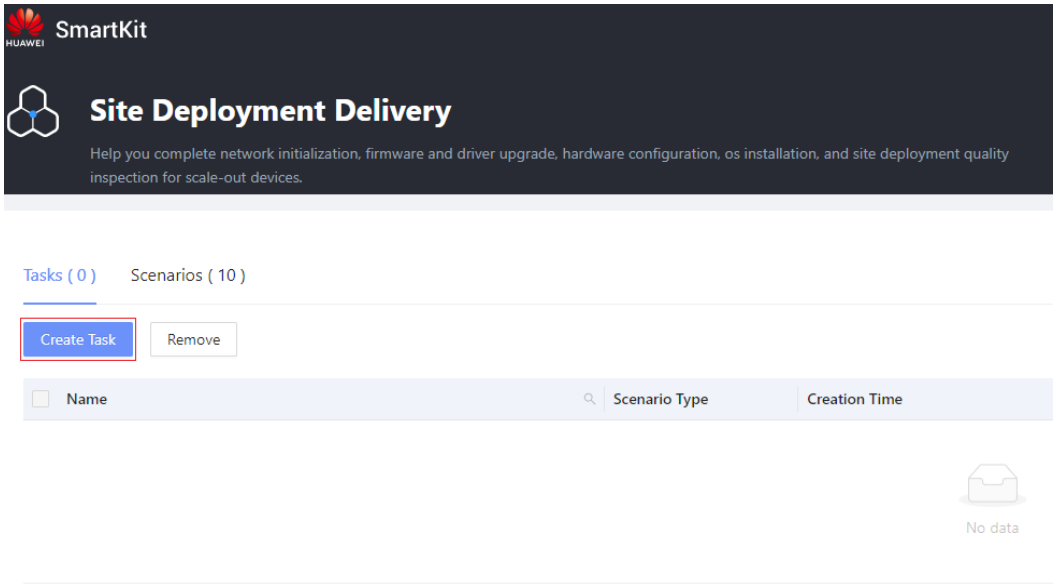
 Copyright © Huawei Technologies Co., Ltd.

connects to a storage device and detects the hardware of the storage device. When it detects a risk, it reports an alarm. You can view alarms reported by the data cluster module on DeviceManager. Management IP addresses must be configured for the data cluster modules on the OceanStor Pacific 9950 device, and the management IP addresses of the data cluster modules must be able to communicate with the management network.

- If the management network can communicate with the iBMC network, you only need to connect the installation PC to the iBMC switch, and configure the management IP addresses and iBMC IP addresses of the data cluster modules at the same time. For details, see **Scenario 1**.
- If the management network cannot communicate with the iBMC network, you need to connect the installation PC to the management switch and iBMC switch, and configure the management IP addresses and iBMC IP addresses of the data cluster modules separately. For details, see **Scenario 2**.

Scenario 1

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.



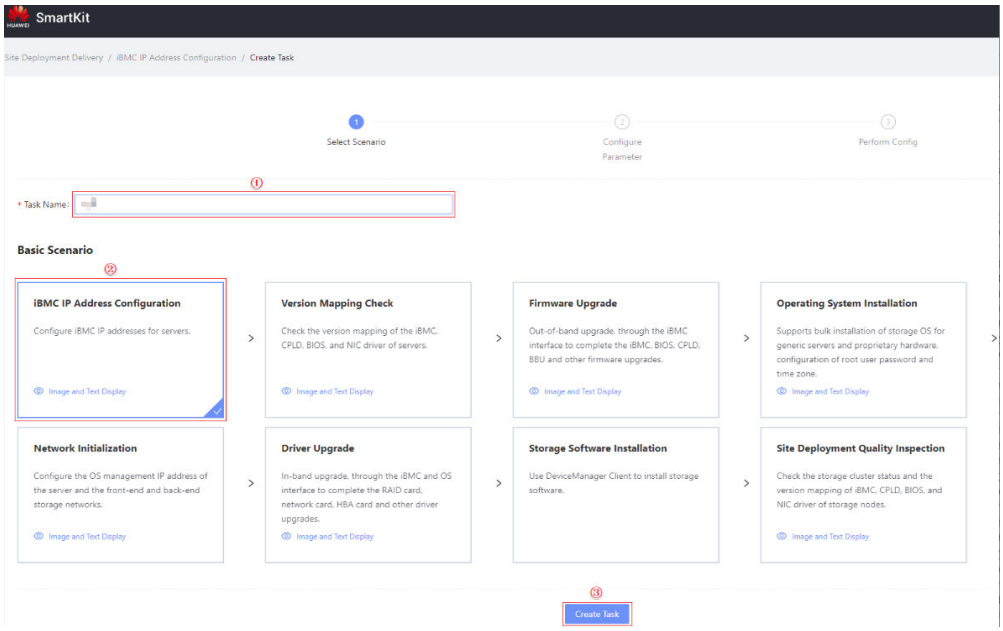
Step 2 Select an iBMC IP address configuration scenario.

1. Set **Task Name**, select **iBMC IP Address Configuration**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).

 Copyright © Huawei Technologies Co., Ltd.



2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

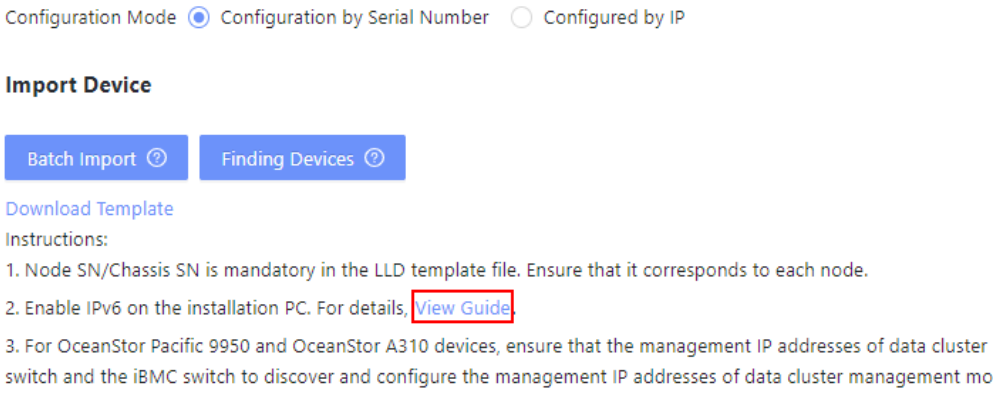
   NOTE

   If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

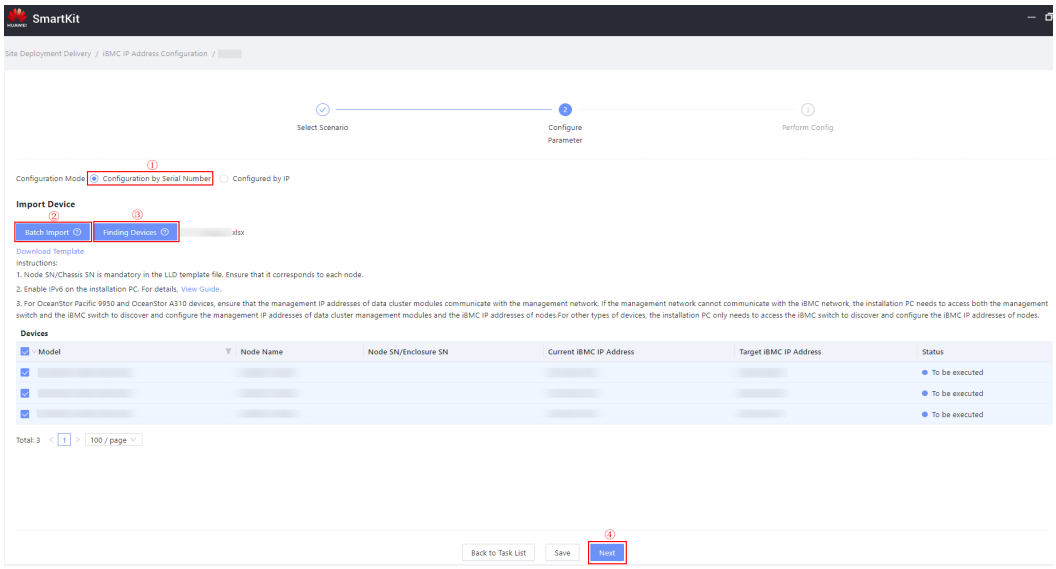
Step 3 Configure parameters.

NOTE

- The installation PC must be connected to an iBMC switch.
- The IPv6 function must be enabled on the installation PC. For details, click **View Guide** under **Usage Notes** in the following figure.



 Copyright © Huawei Technologies Co., Ltd.



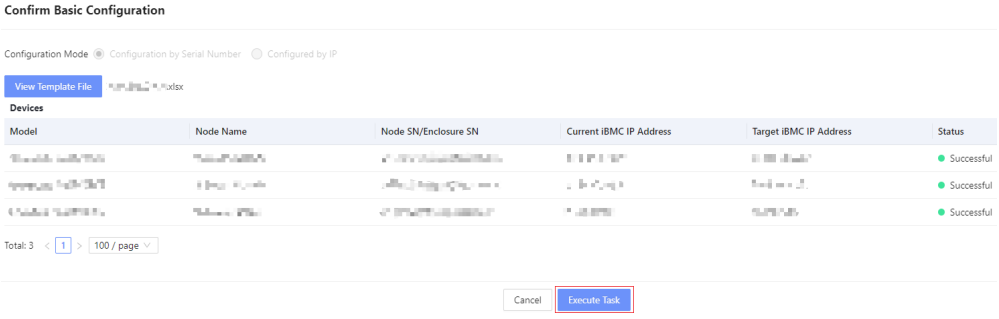
1. Set **Configuration Mode** to **Configuration by Serial Number**.
2. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.
3. Click **Finding Devices**. The system will discover the current iBMC IP addresses of the nodes by SN. After the discovery is complete, view the discovery result in the **Status** column.

   NOTE

   - If the discovery is successful, the system will update the current iBMC IP addresses of the discovered nodes to the **Current iBMC IP Address** column.
   - If the discovery fails, click **View Guide** under **Usage Notes**, rectify the fault according to the guide, and click **Finding Devices** again.
4. Click **Next**.

Step 4 Perform the configuration.

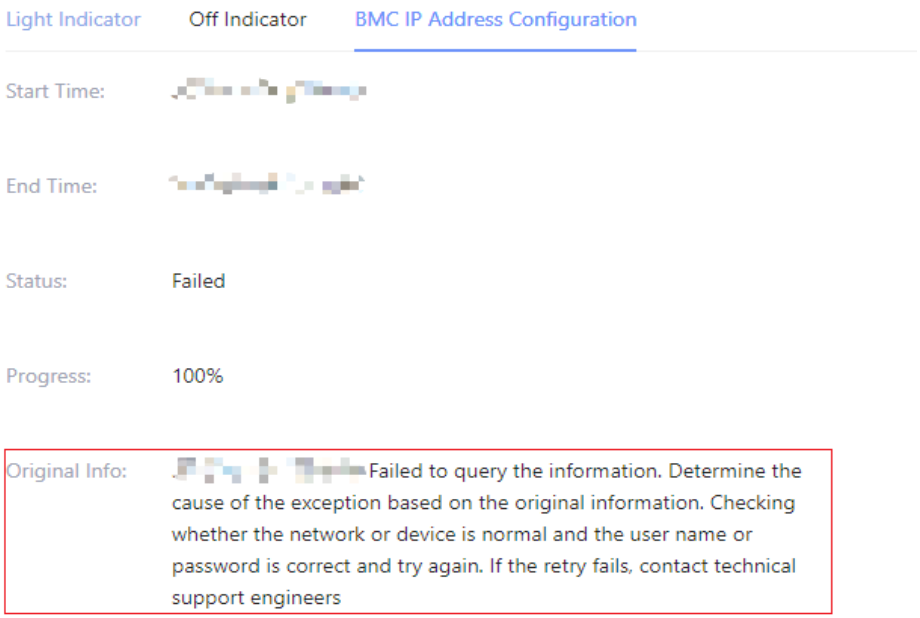
1. Click **View Template File**. The imported LLD configuration file will be automatically opened. Confirm the information to be configured. After confirming that the information is correct, click **Execute Task**.



2. After the configuration is complete, view the configuration results of all nodes in the **Configuration Status** column.

   If **Config failed** is displayed in the **Configuration Status** column, click **Details** in the **Operation** column. Click the **BMC IP Address Configuration** tab, and rectify the fault based on the information in **Original Info**. The following is an example:

 Copyright © Huawei Technologies Co., Ltd.

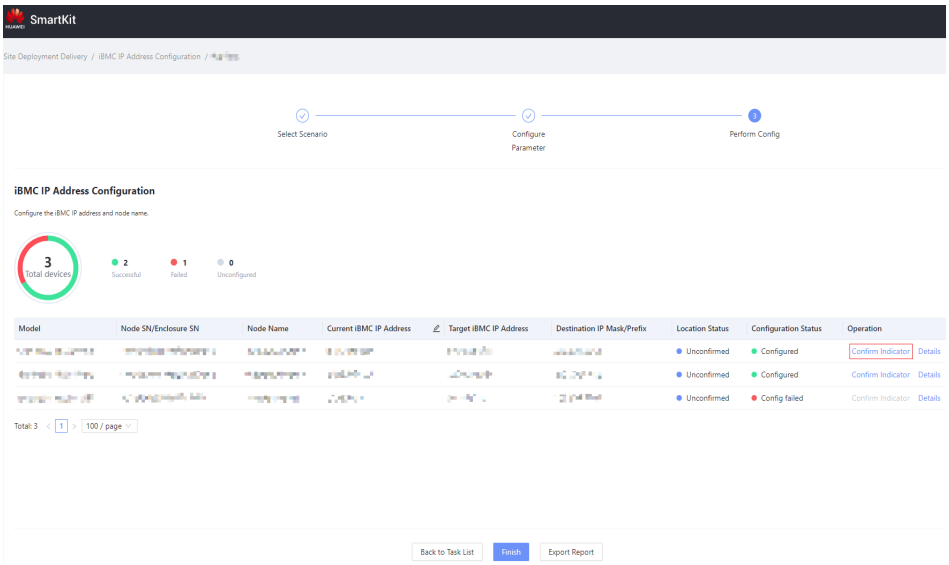


NOTE

You can also click **Export Report** in the lower part to collect and view the configuration results of all nodes.

3. Confirm indicators.

   Click **Confirm Indicator** in the **Operation** column corresponding to each IP address.



 Copyright © Huawei Technologies Co., Ltd.

NOTE

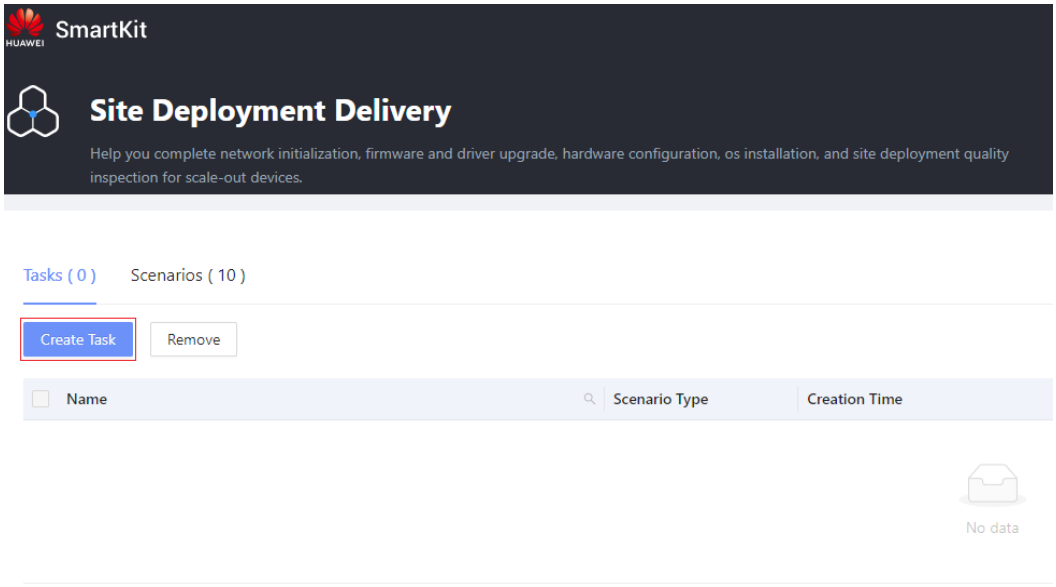
- For details about the positions of device location indicators, see **Appendix** > **Indicators and Buttons** in *OceanStor Pacific Series 8.2.1 Hardware Installation Guide*.
- If the location indicator of the corresponding device is on, the configuration is successful. In the **Confirm Indicator** dialog box that is displayed, click **Correct**. The location indicator will be automatically turned off.
- If the location indicator status is not as expected, re-plan the iBMC IP addresses and configure them from the beginning. If the fault persists, contact Huawei technical support engineers.

4. Click **Finish**.

----End

Scenario 2

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.



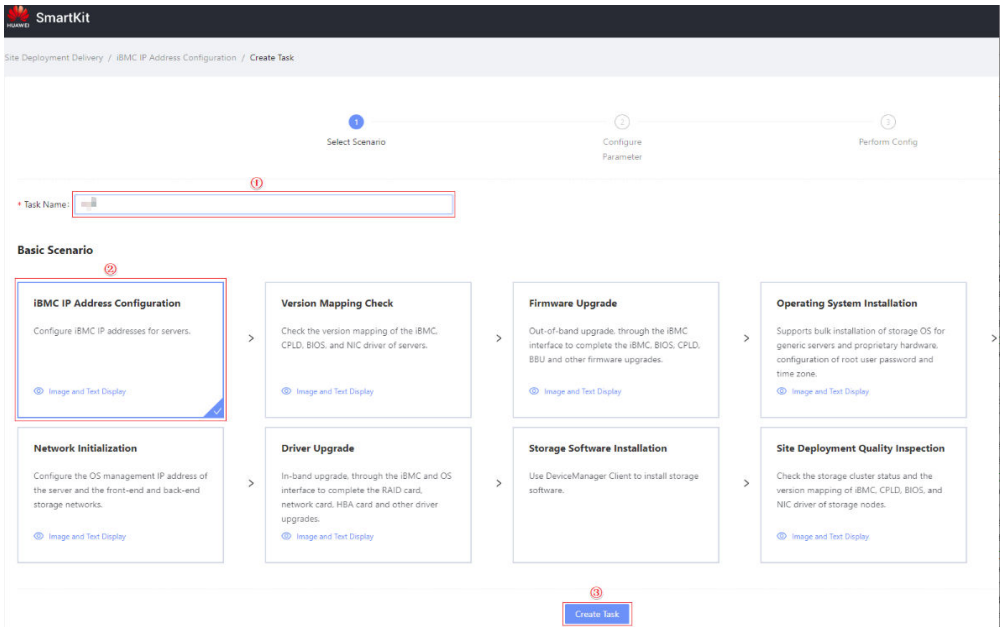
Step 2 Select an iBMC IP address configuration scenario.

1. Set **Task Name**, select **iBMC IP Address Configuration**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).

 Copyright © Huawei Technologies Co., Ltd.



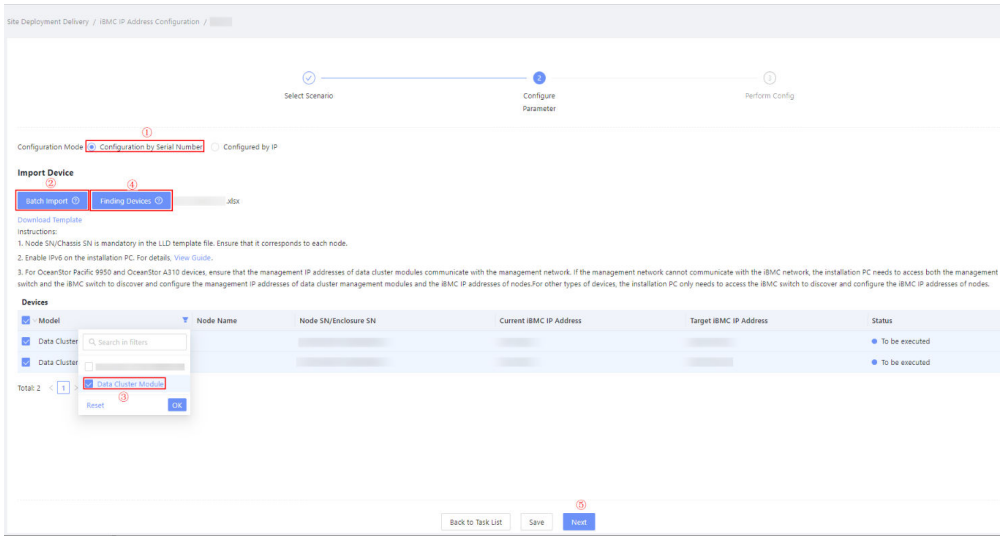
2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

   NOTE

   If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

Step 3 Configure management IP addresses for data cluster modules.

1. Connect the installation PC to the management switch.
2. Configure parameters.



   a. Set **Configuration Mode** to **Configuration by Serial Number**.
   b. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.
   c. In the **Model** drop-down list, select **Data Cluster Module** (that is, select all data cluster modules).

 Copyright © Huawei Technologies Co., Ltd.

d. Click **Finding Devices**. The system will discover the current management IP addresses of the data cluster modules by SN. After the discovery is complete, view the discovery result in the **Status** column.

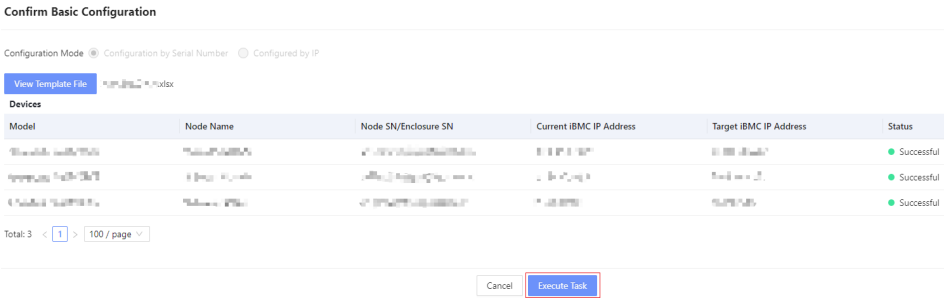
NOTE

- If the discovery is successful, the system will update the current management IP addresses of the discovered data cluster modules to the **Current iBMC IP Address** column.
- If the discovery fails, click **View Guide** under **Usage Notes**, rectify the fault according to the guide, and click **Finding Devices** again.

e. Click **Next**.

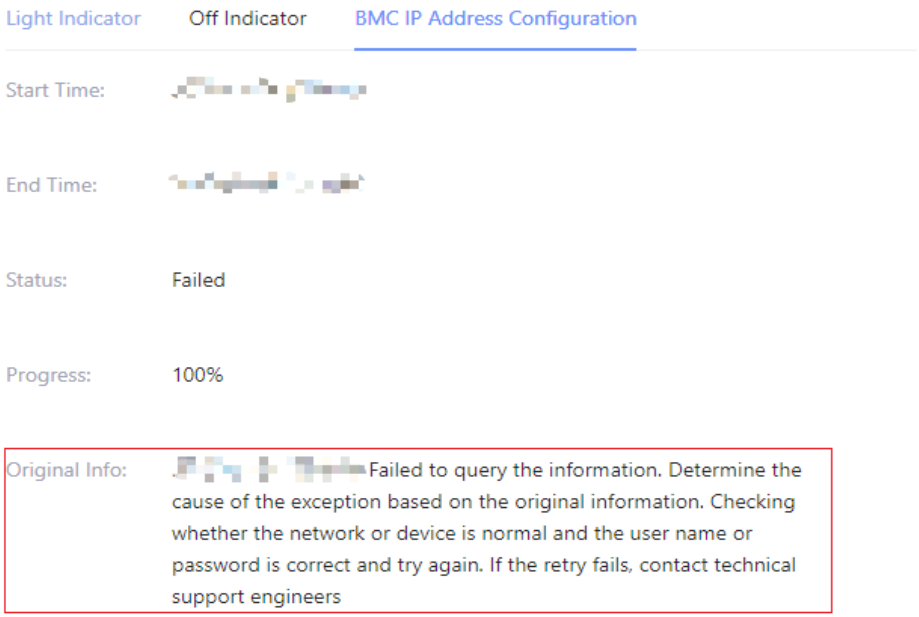
3. Execute the task.

a. Click **View Template File**. The imported LLD configuration file will be automatically opened. Confirm the information to be configured. After confirming that the information is correct, click **Execute Task**.



b. After the configuration is complete, view the configuration results of all nodes in the **Configuration Status** column.

If **Config failed** is displayed in the **Configuration Status** column, click **Details** in the **Operation** column. Click the **BMC IP Address Configuration** tab, and rectify the fault based on the information in **Original Info**. The following is an example:

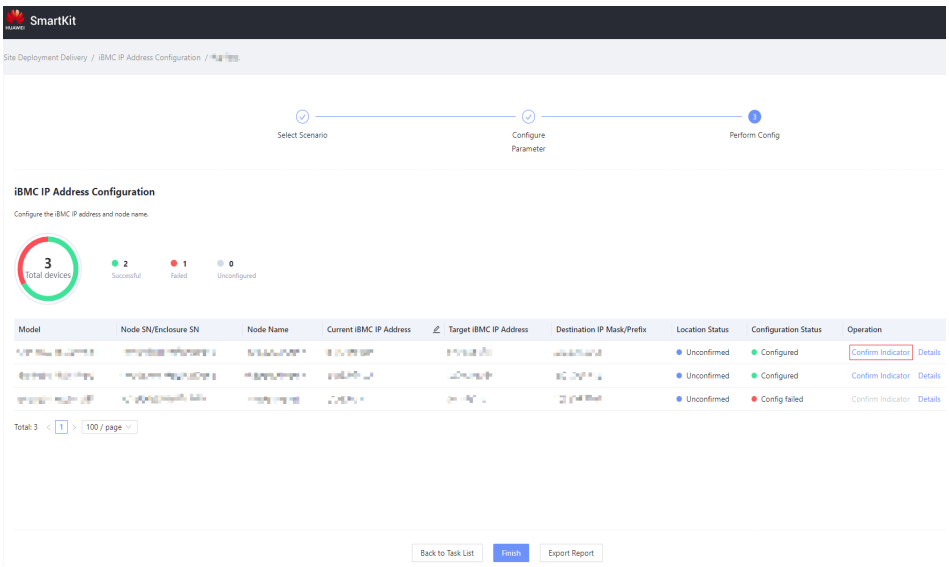


 Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> You can also click **Export Report** in the lower part to collect and view the configuration results of all nodes.

4. Confirm indicators.

   Click **Confirm Indicator** in the **Operation** column corresponding to each IP address.



> **NOTE**
>
> - For details about the positions of device location indicators, see **Appendix** > **Indicators and Buttons** in *OceanStor Pacific Series 8.2.1 Hardware Installation Guide*.
> - If the location indicator of the corresponding device is on, the configuration is successful. In the **Confirm Indicator** dialog box that is displayed, click **Correct**. The location indicator will be automatically turned off.
> - If the location indicator status is not as expected, re-plan the iBMC IP addresses and configure them from the beginning. If the fault persists, contact Huawei technical support engineers.

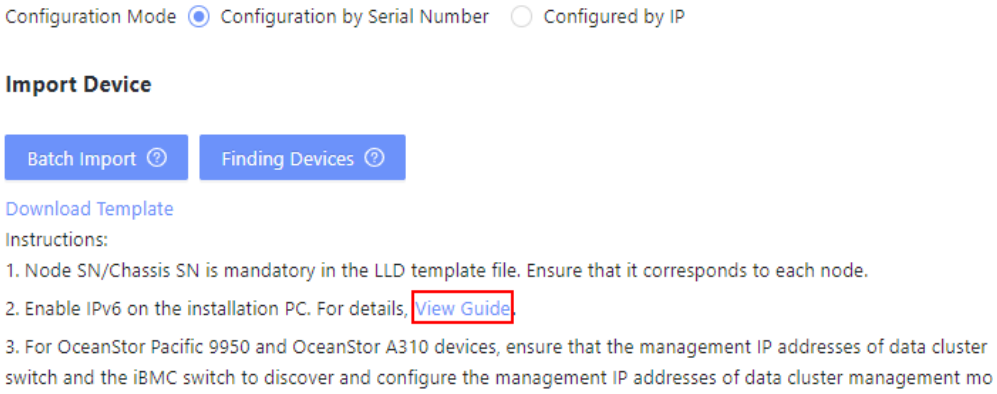
Step 4 Configure iBMC IP addresses for nodes.

1. Connect the installation PC to the iBMC switch.

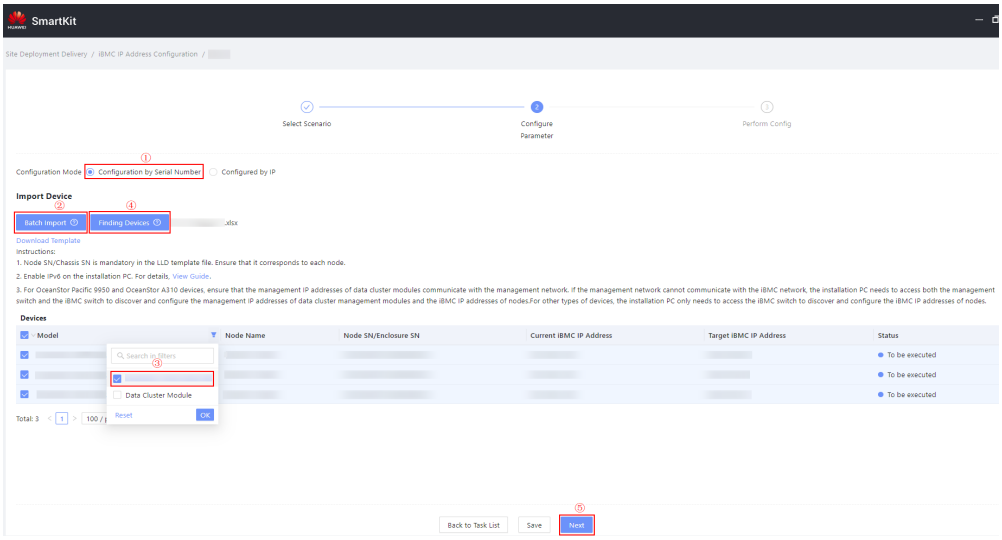
 Copyright © Huawei Technologies Co., Ltd.

NOTE

The IPv6 function must be enabled on the installation PC. For details, click **View Guide** under **Usage Notes** in the following figure.



2. Configure parameters.



a. Set **Configuration Mode** to **Configuration by Serial Number**.

b. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.

c. In the **Model** drop-down list, select the device models of all nodes for which iBMC IP addresses are to be configured.

d. Click **Finding Devices**. The system will discover the current iBMC IP addresses of the nodes by SN. After the discovery is complete, view the discovery result in the **Status** column.

NOTE

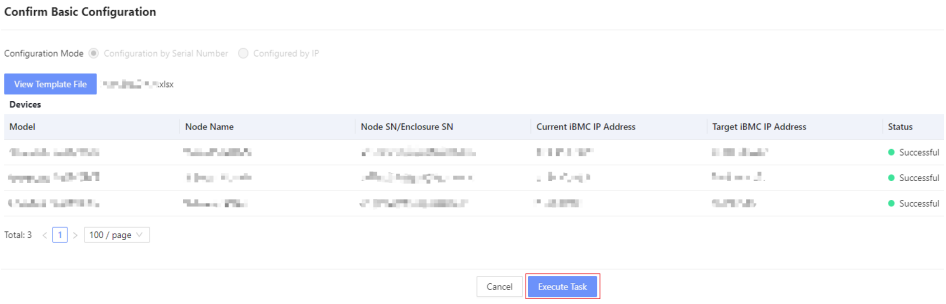
- If the discovery is successful, the system will update the current iBMC IP addresses of the discovered nodes to the **Current iBMC IP Address** column.
- If the discovery fails, click **View Guide** under **Usage Notes**, rectify the fault according to the guide, and click **Finding Devices** again.

e. Click **Next**.

 Copyright © Huawei Technologies Co., Ltd.

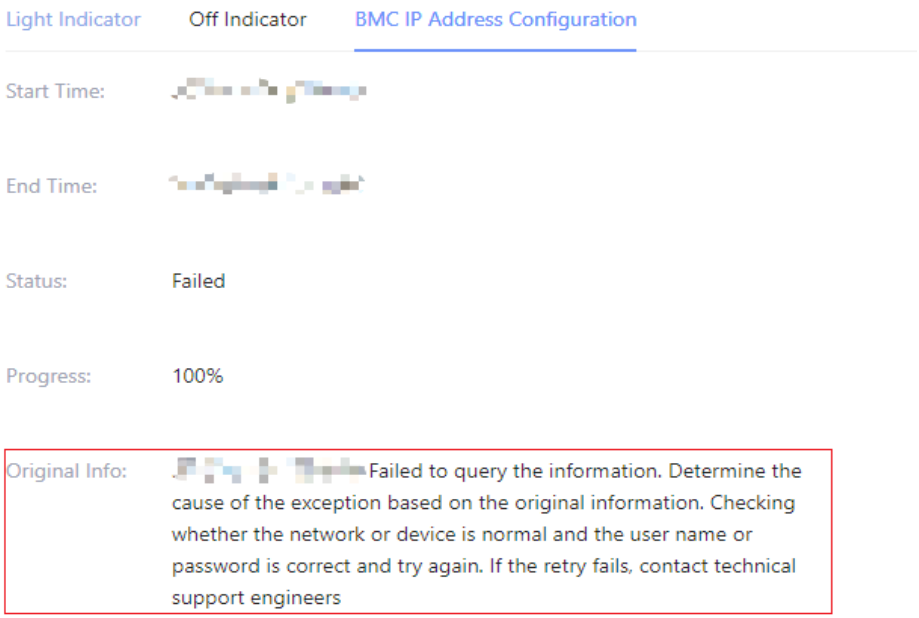
3. Execute the task.

   a. Click **View Template File**. The imported LLD configuration file will be automatically opened. Confirm the information to be configured. After confirming that the information is correct, click **Execute Task**.



   b. After the configuration is complete, view the configuration results of all nodes in the **Configuration Status** column.

      If **Config failed** is displayed in the **Configuration Status** column, click **Details** in the **Operation** column. Click the **BMC IP Address Configuration** tab, and rectify the fault based on the information in **Original Info**. The following is an example:



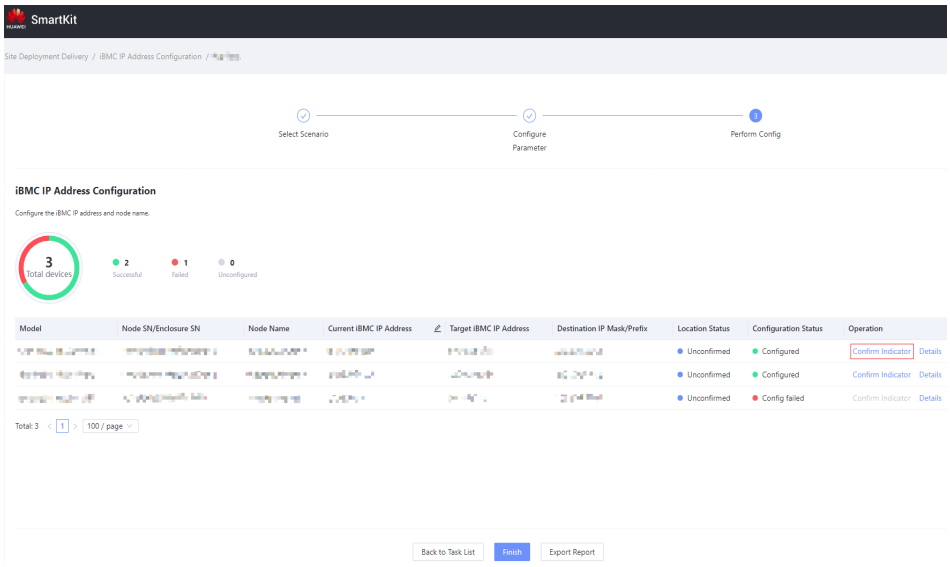
   NOTE

   You can also click **Export Report** in the lower part to collect and view the configuration results of all nodes.

4. Confirm indicators.

   Click **Confirm Indicator** in the **Operation** column corresponding to each IP address.

 Copyright © Huawei Technologies Co., Ltd.



NOTE

- For details about the positions of device location indicators, see **Appendix** > **Indicators and Buttons** in *OceanStor Pacific Series 8.2.1 Hardware Installation Guide*.
- If the location indicator of the corresponding device is on, the configuration is successful. In the **Confirm Indicator** dialog box that is displayed, click **Correct**. The location indicator will be automatically turned off.
- If the location indicator status is not as expected, re-plan the iBMC IP addresses and configure them from the beginning. If the fault persists, contact Huawei technical support engineers.

----End

?.2. Configuring an iBMC IP Address for a Single Node

Context

This section describes how to use SmartKit to configure the target iBMC IP address using the default iBMC IP address of a node. This method can configure an iBMC IP address for only one node at a time.

If the node name is specified when the LLD configuration file is prepared, the node name will be automatically configured when an iBMC IP address is configured. If an OceanStor Pacific 9950 device exists, you also need to configure the management IP addresses of its data cluster modules and the system will automatically change the passwords of the data cluster modules.

NOTE

The GUI of SmartKit may vary with the version.

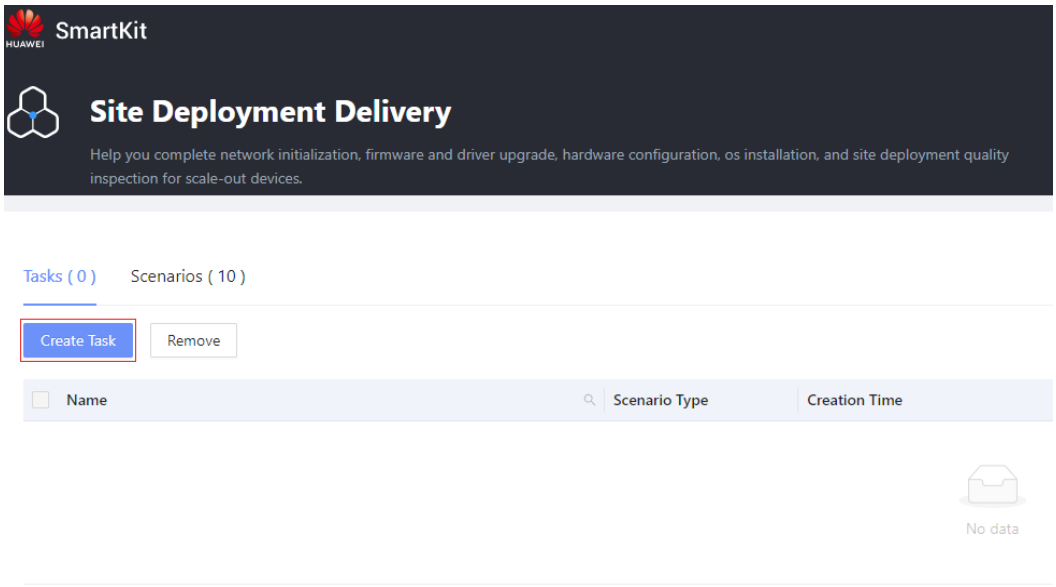
Prerequisites

If the storage software has been installed on the nodes to be deployed, uninstall the storage software by referring to **5.5.19 Uninstalling OceanStor Pacific Series Software**, clear the network and route information configured on the nodes, and then initialize the nodes using SmartKit.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.

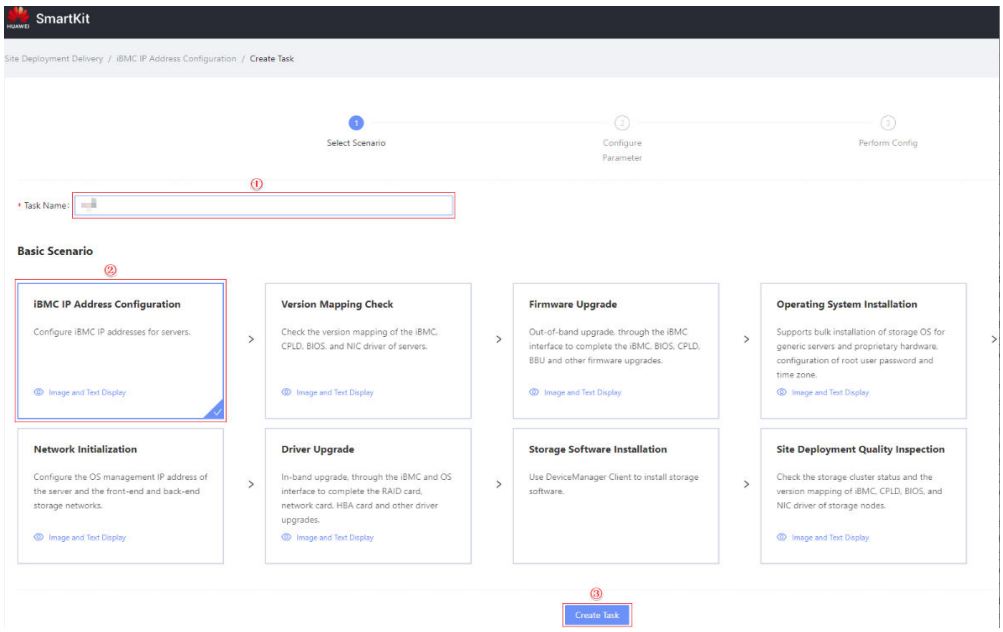


Step 2 Select an iBMC IP address configuration scenario.

1. Set **Task Name**, select **iBMC IP Address Configuration**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).



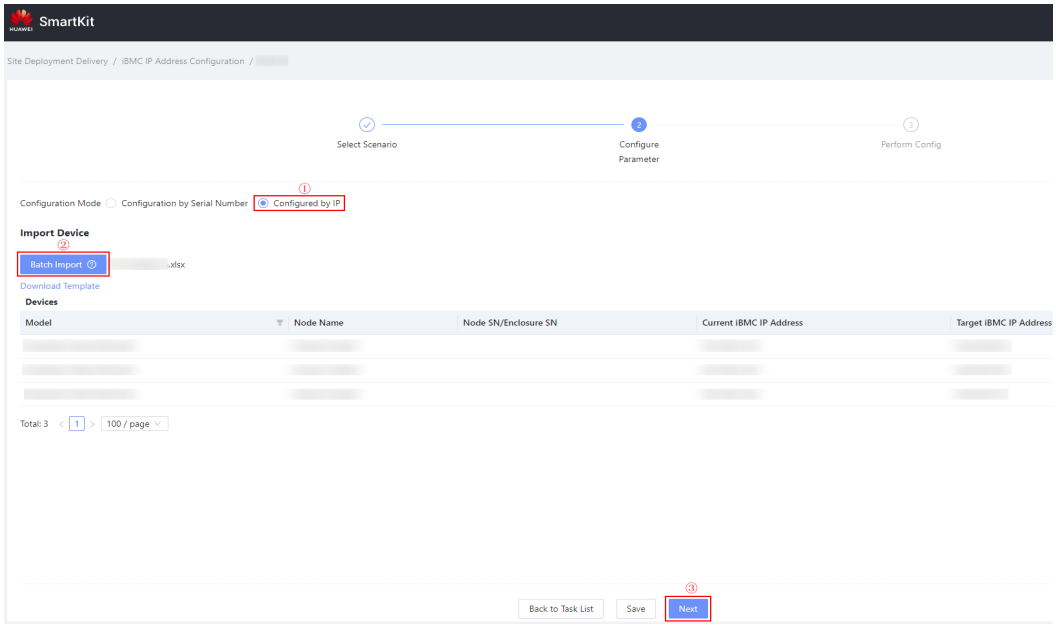
2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

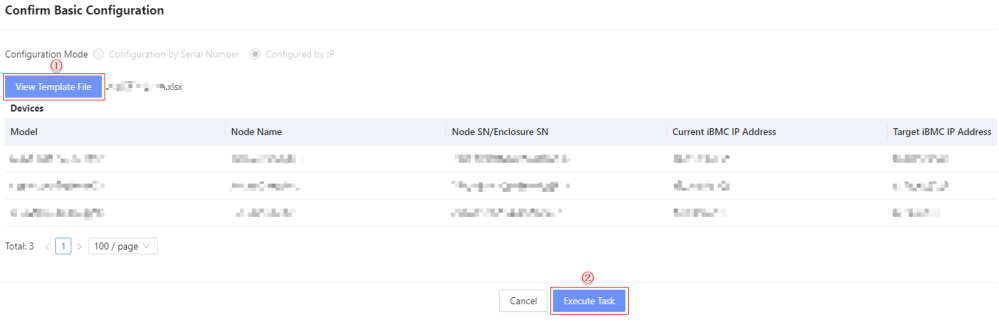
Step 3 Configure parameters.



1. Set **Configuration Mode** to **Configured by IP**.
2. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.
3. Click **Next**.

Step 4 Perform the configuration.

1. Click **View Template File**. The imported LLD configuration file will be automatically opened. Confirm the information to be configured. After confirming that the information is correct, click **Execute Task**.



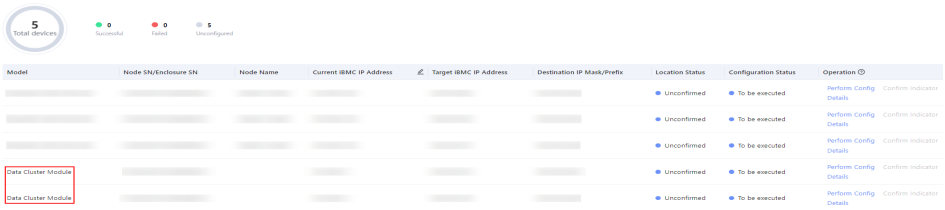
2. Configure iBMC IP addresses.

   Only one IP address can be configured at a time. To configure a single IP address, perform the following steps:

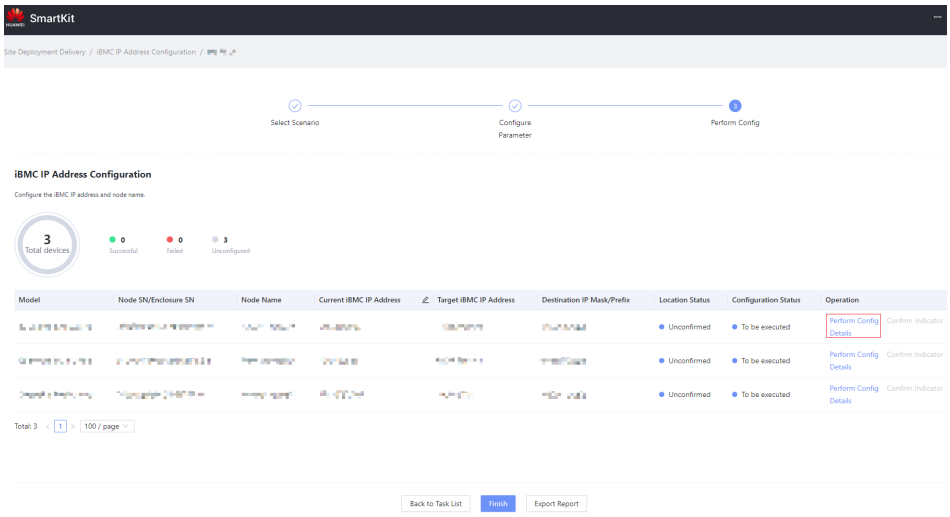
 Copyright © Huawei Technologies Co., Ltd.

NOTE

If an OceanStor Pacific 9950 device exists, management IP addresses must be configured for its data cluster modules. The configuration information about the data cluster modules (whose **Model** is **Data Cluster Module**) is displayed.



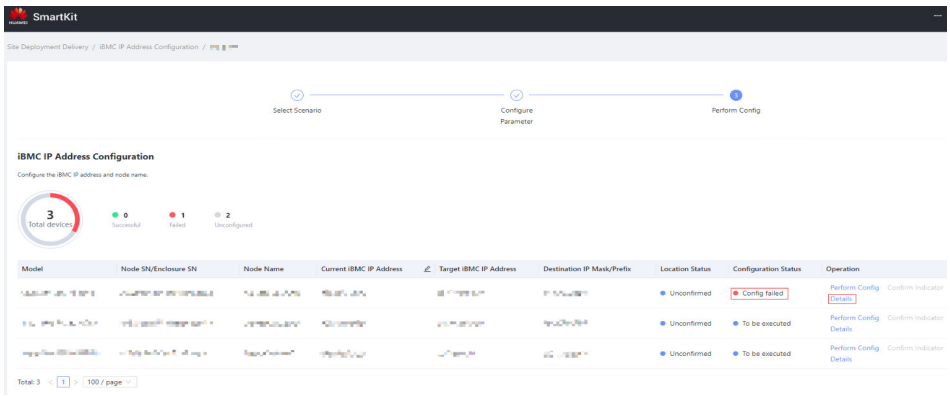
a. Click **Perform Config** in the **Operation** column of the node to be configured.



NOTE

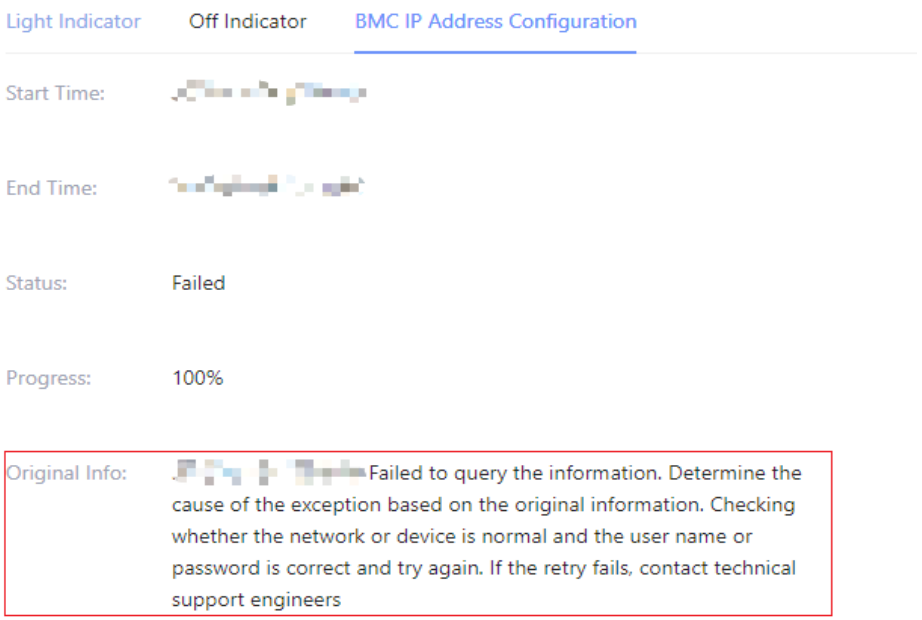
Before the configuration, the IP address of the installation PC must be in the same subnet as the default IP address. You can view the default IP address in the **Current iBMC IP Address** column. The default mask is 255.255.255.0.

b. After the configuration is complete, view the configuration result of the node in the **Configuration Status** column.



If **Config failed** is displayed in the **Configuration Status** column, click **Details** in the **Operation** column. Click the **BMC IP Address Configuration** tab, and rectify the fault based on the information in **Original Info**. The following is an example:

 Copyright © Huawei Technologies Co., Ltd.



NOTE

You can also click **Export Report** in the lower part to collect and view the configuration results of all IP addresses.

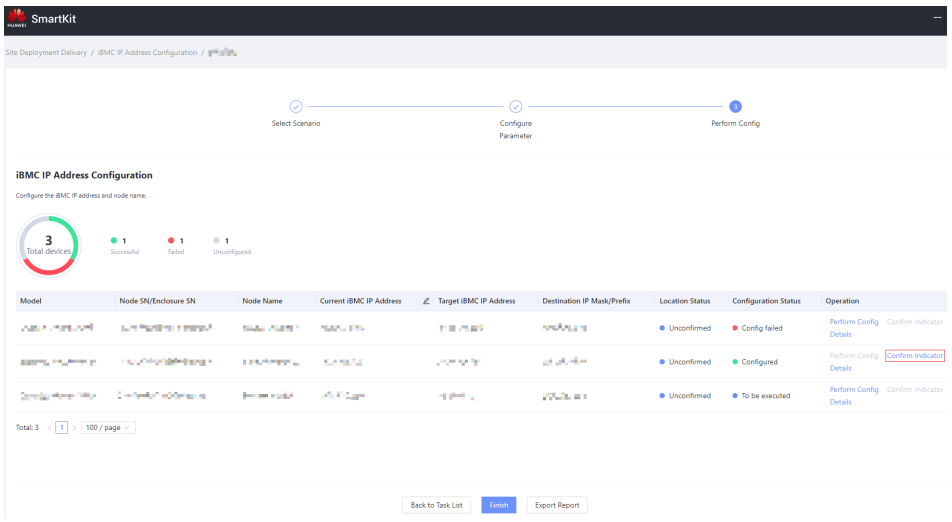
3. Confirm indicators.

NOTE

If an OceanStor Pacific 9950 device exists, the management IP addresses of the data cluster modules must be able to communicate with the management network. If the management network cannot communicate with the iBMC network, you need to connect the installation PC to the management switch and iBMC switch, and check the configuration results for the management IP addresses and iBMC IP addresses of the data cluster modules separately.

a. Connect the installation PC to the corresponding switch and configure the installation PC to be in the same subnet as **Target iBMC IP Address**.

b. Click **Confirm Indicator** in the **Operation** column corresponding to each IP address.



 Copyright © Huawei Technologies Co., Ltd.

NOTE

- For details about the positions of device location indicators, see **Appendix** > **Indicators and Buttons** in *OceanStor Pacific Series 8.2.1 Hardware Installation Guide*.
- If the location indicator of the corresponding device is on, the configuration is successful. In the **Confirm Indicator** dialog box that is displayed, click **Correct**. The location indicator will be automatically turned off.
- If the location indicator status is not as expected, re-plan the iBMC IP addresses and configure them from the beginning. If the fault persists, contact Huawei technical support engineers.

4. After confirming that the information is correct, click **Finish**.

----End

5.4.1.5.1.3 Checking Version Mappings

Context

This section describes how to use SmartKit to check the version mapping of a node, such as the OS, firmware, and driver.

NOTE

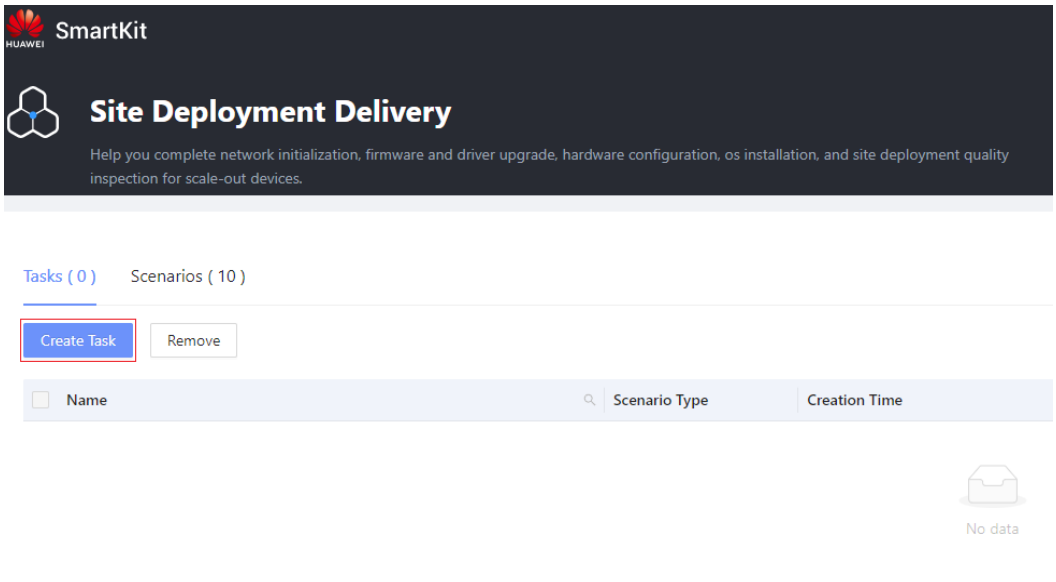
The GUI of SmartKit may vary with the version.

Prerequisites

The installation PC communicates properly with the newly configured iBMC network of a node.

Procedure

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.



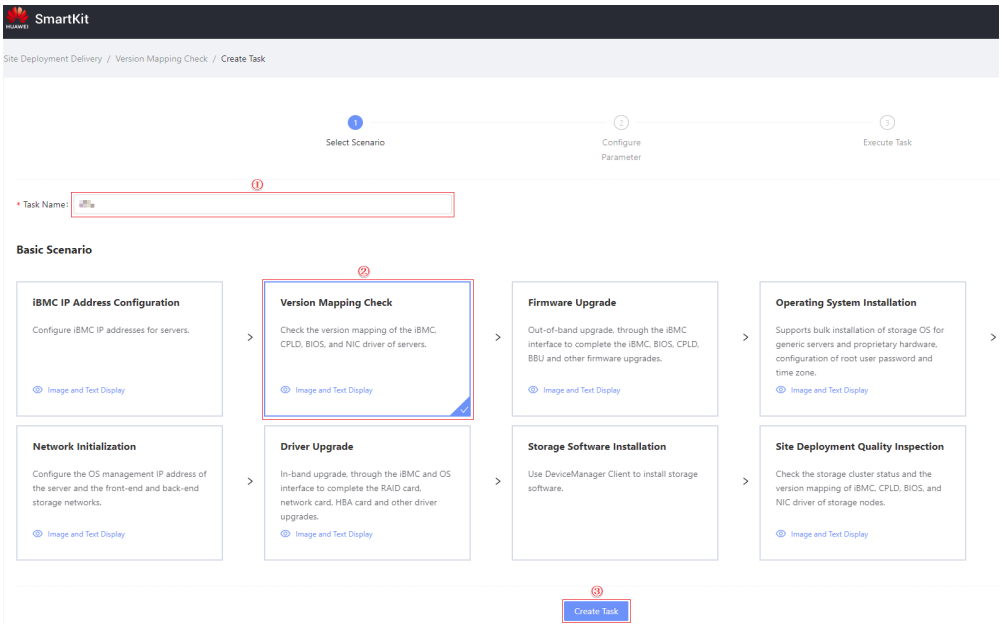
 Copyright © Huawei Technologies Co., Ltd.

Step 2 Select a scenario.

1. Set **Task Name**, select **Version Mapping Check**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).

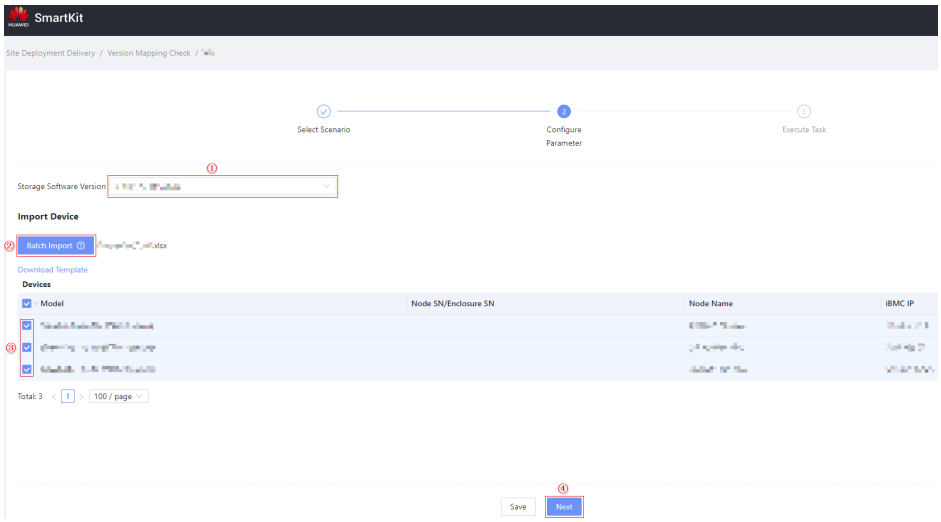


2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

   NOTE

   If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

Step 3 Configure parameters.

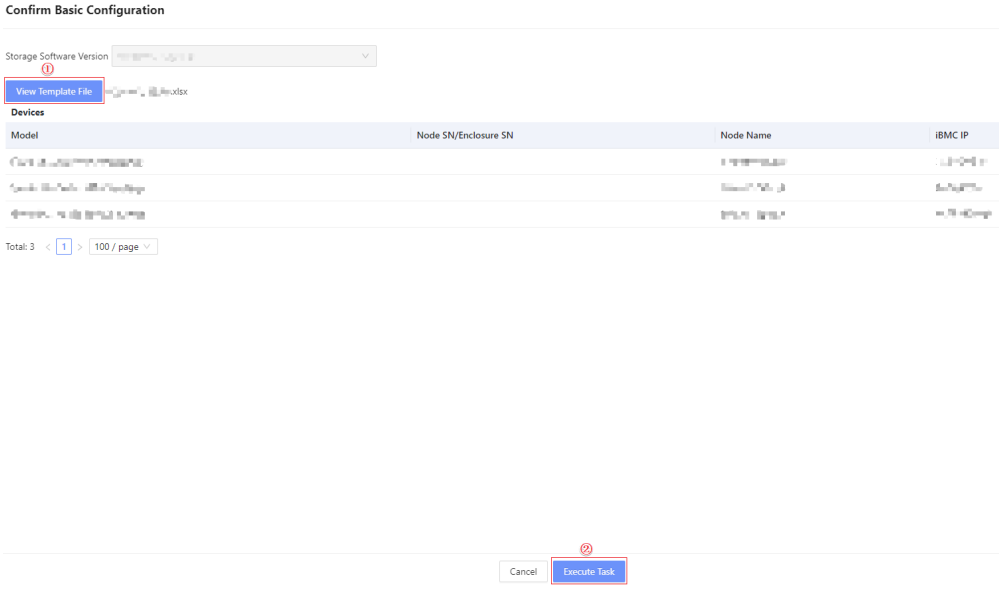


 Copyright © Huawei Technologies Co., Ltd.

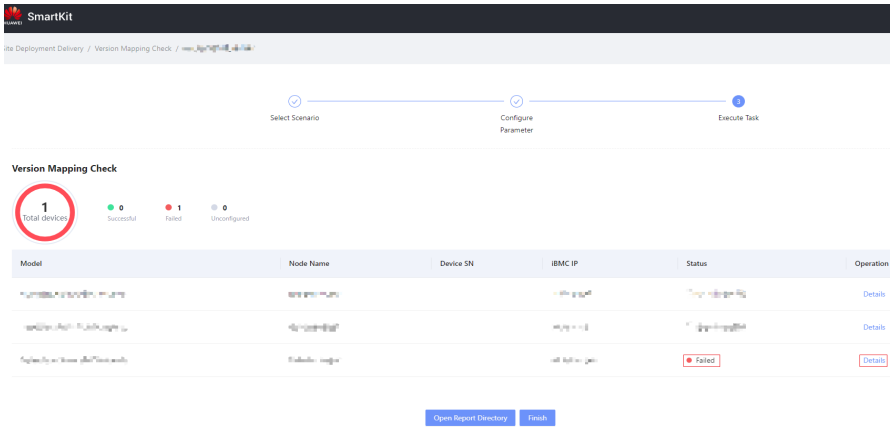
1. Set **Storage Software Version**.
2. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.
3. In **Devices**, select the nodes for which you want to check version mapping.
4. Click **Next**.

Step 4 Execute the task.

1. Click **View Template File**. The imported LLD configuration file will be automatically opened. Confirm the information to be configured. After confirming that the information is correct, click **Execute Task**.



2. After the task is complete, check whether **Successfully** is displayed in the **Status** column of each node.
   - If yes, click **Finish**.
   - If no, perform the following steps for each failed node (after the troubleshooting is complete, click **Finish**):
     i. Click **Details** in the **Operation** column of the node.



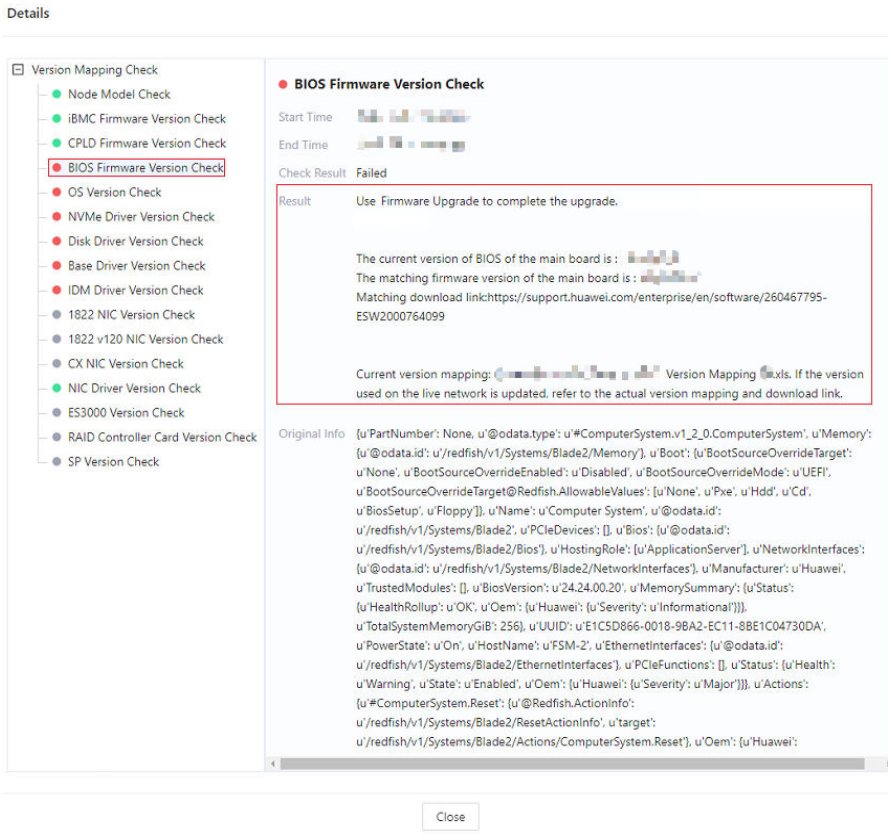
 Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> You can also click **Open Report Directory** in the lower part to collect and view the check results of all nodes.

ii. On the **Details** page, click each failed check item (marked in red) on the left and perform troubleshooting according to the description in **Result**. The following are examples:

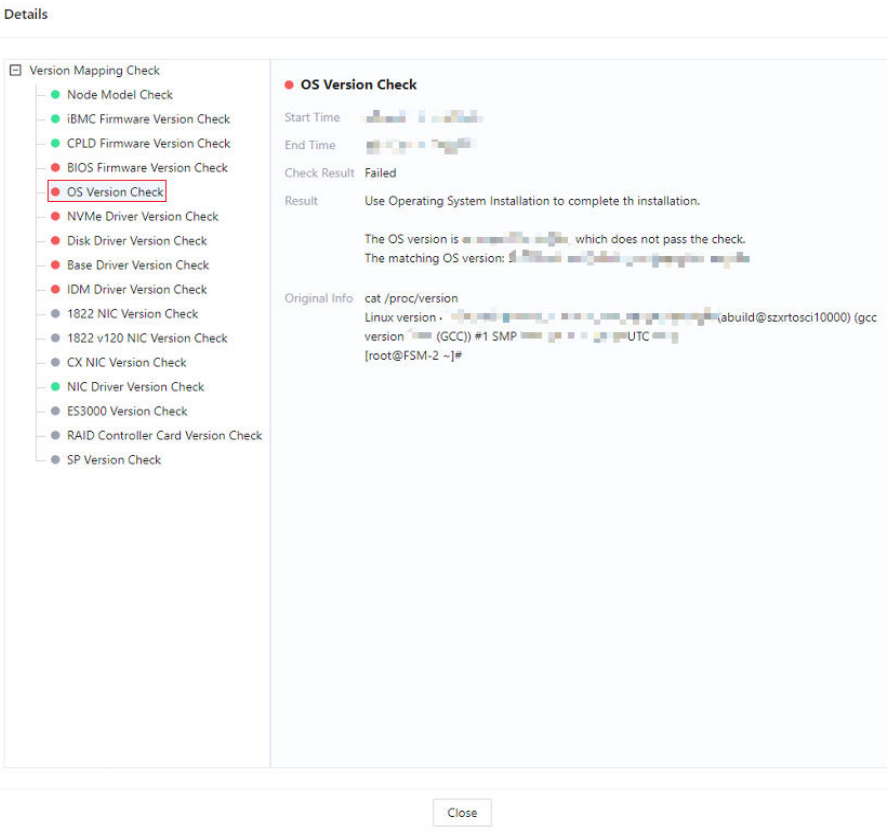
> **NOTE**
>
> - The check items on the left of the **Details** page are displayed in the operation sequence. Handle the failed check items from top to bottom.
> - For a check item that fails, the link for downloading the related software package is displayed in **Result**. You can click the link to download the software package. If the download link is not provided, obtain the related software package by referring to **5.4.1.3.2 Obtaining Software Packages**.

Firmware:

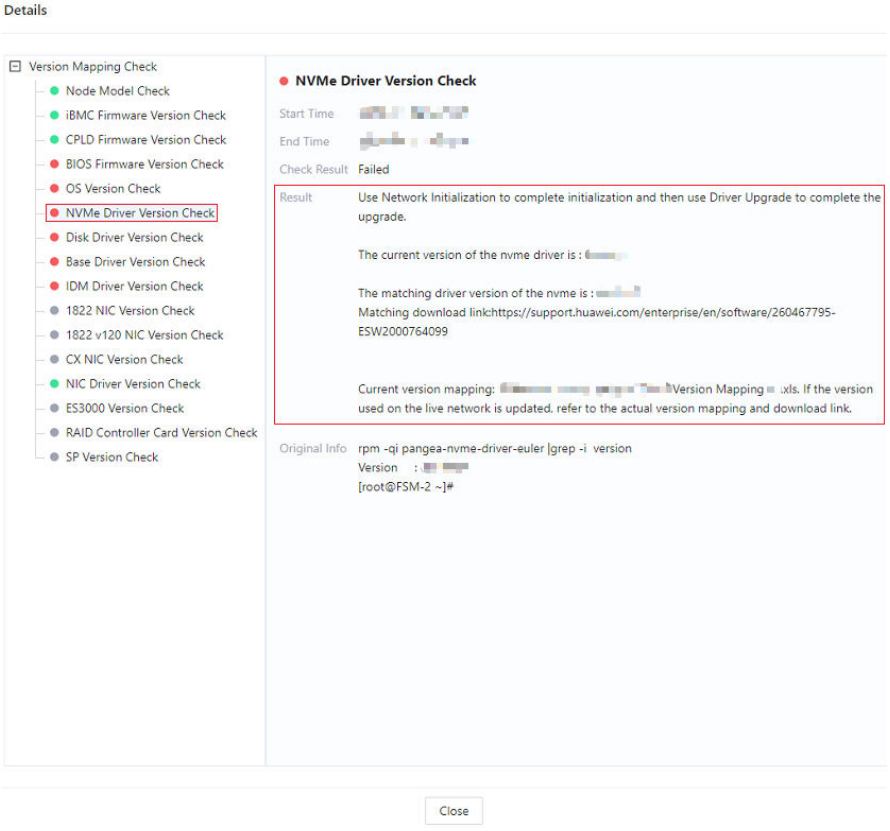


OS:

 Copyright © Huawei Technologies Co., Ltd.



Driver:



 Copyright © Huawei Technologies Co., Ltd.

----End

5.4.1.5.1.4 (Optional) Upgrading Firmware

Context

This section describes how to upgrade firmware on SmartKit.

NOTE

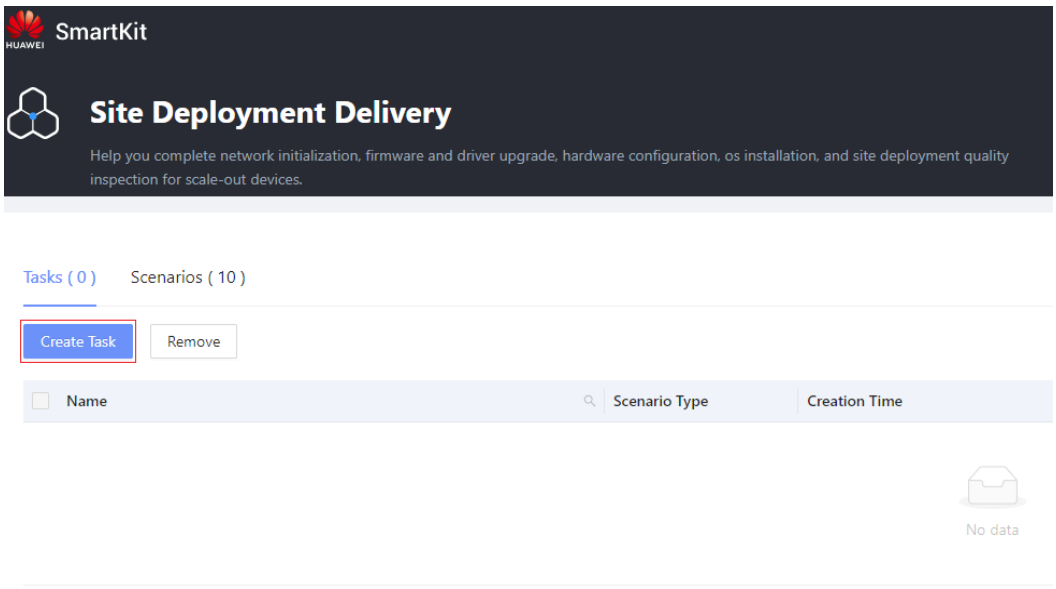
The GUI of SmartKit may vary with the version.

Prerequisites

- You have determined that firmware needs to be upgraded according to the check results in **Checking Version Mappings** and downloaded the corresponding firmware package.
- The installation PC communicates properly with the newly configured iBMC network of a node.

Procedure

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.



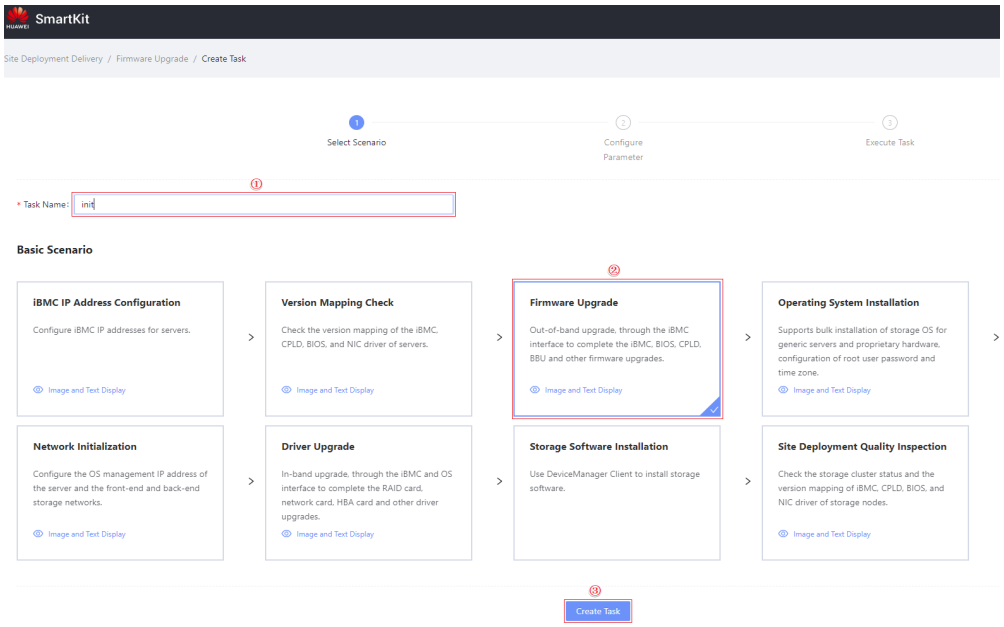
Step 2 Select a scenario.

1. Set **Task Name**, select **Firmware Upgrade**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).

 Copyright © Huawei Technologies Co., Ltd.

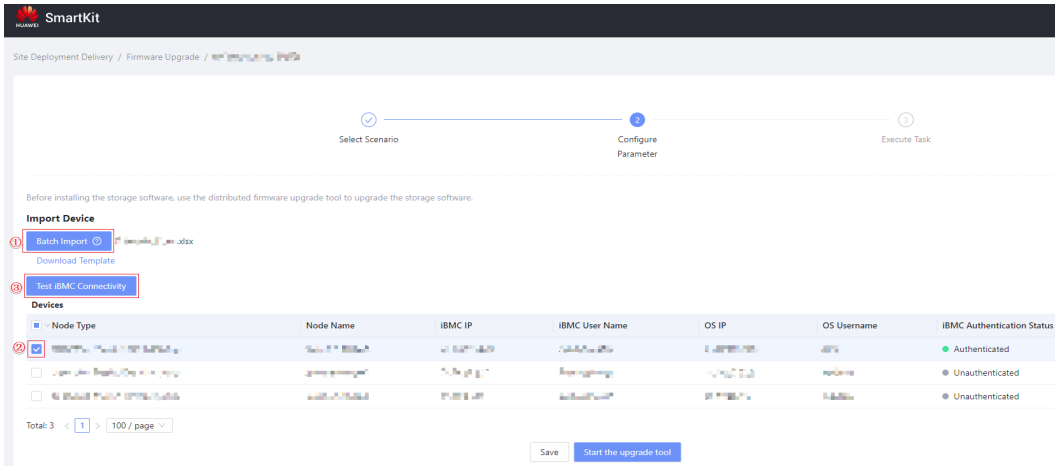


2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

   NOTE

   If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

Step 3 Configure parameters.



1. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.
2. In **Devices**, select a node whose firmware needs to be upgraded.
3. Click **Test iBMC Connectivity** for authentication.

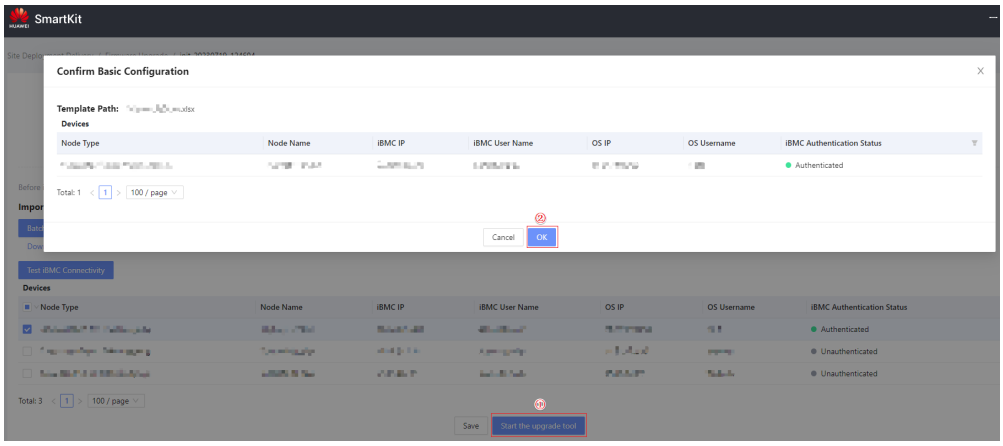
   NOTE

   If authentication failure is displayed in the **iBMC Authentication Status** column of a node, rectify the fault according to the description in .

Step 4 Execute the task.

 Copyright © Huawei Technologies Co., Ltd.

1. Click **Start the upgrade tool**. A dialog box is displayed for you to confirm the configuration information. After confirming that the information is correct, click **OK**. The firmware upgrade page is displayed.

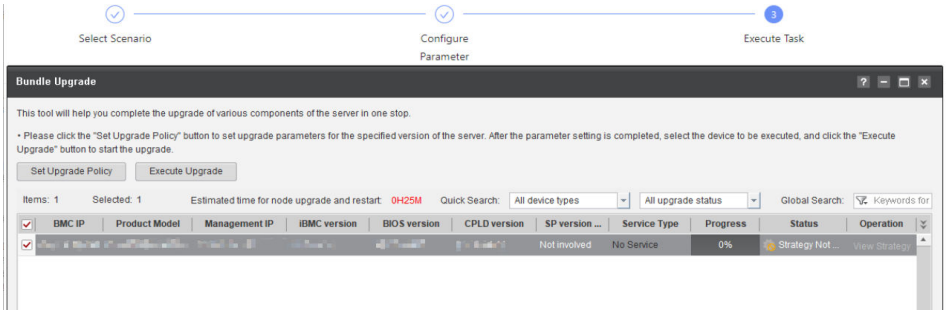


2. Set the upgrade policy.

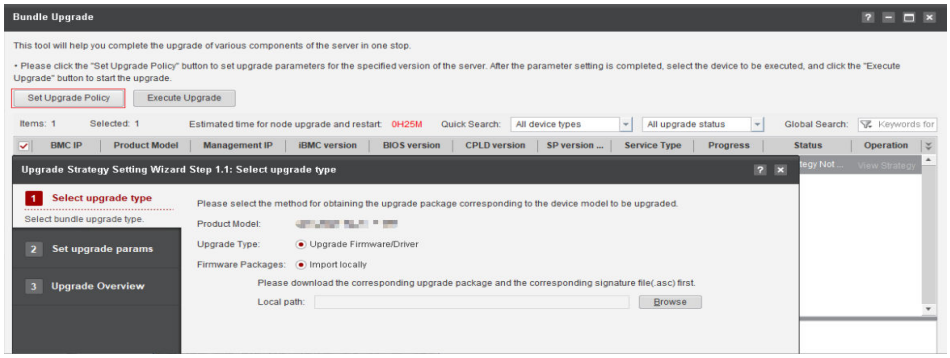
   a. Select the devices to be upgraded.

   NOTE

   Devices of different models need to be upgraded in different batches. Select devices of the same model to set the upgrade policy.



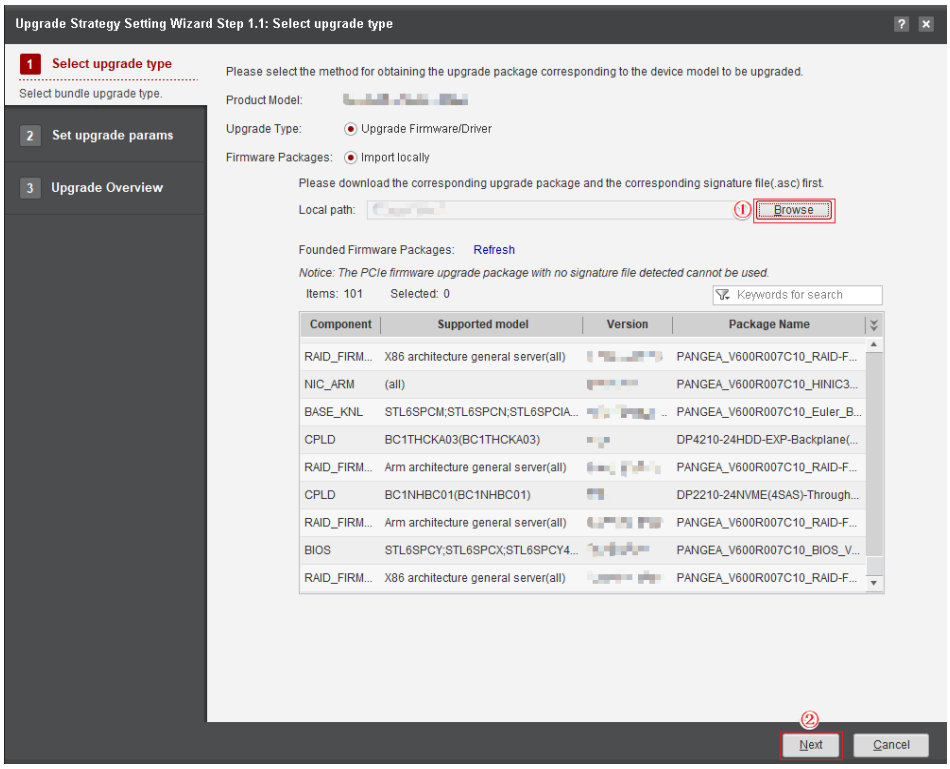
   b. Click **Set Upgrade Policy**. The **Upgrade Strategy Setting Wizard** dialog box is displayed.



   c. Import the firmware upgrade package.

   Click **Browse**, select the path for storing the firmware upgrade package, and click **Next**.

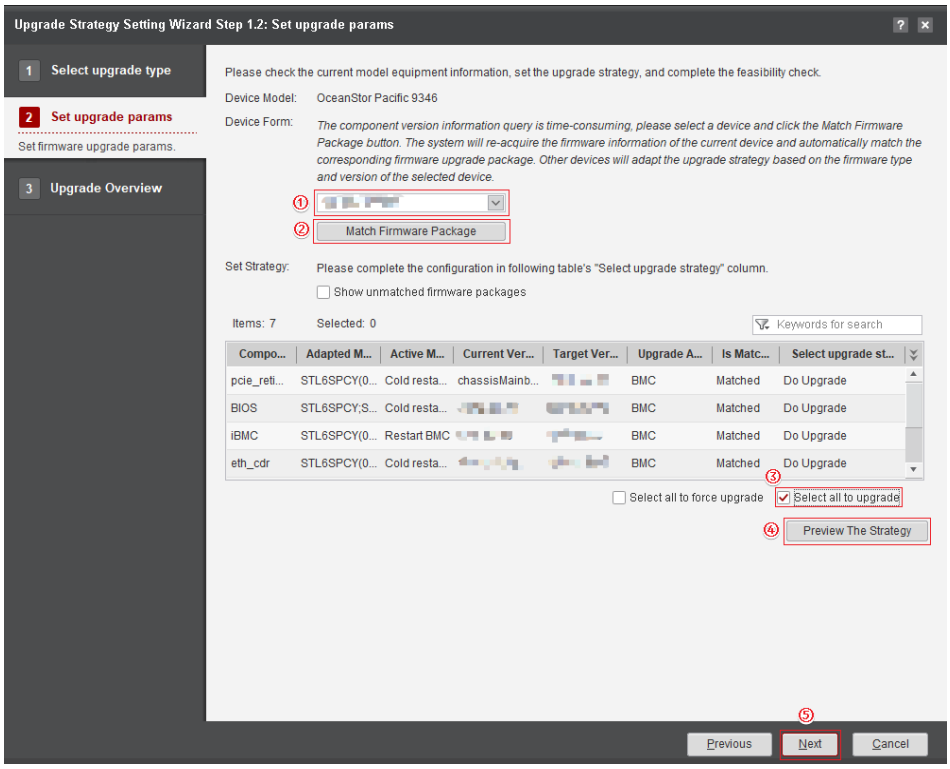
 Copyright © Huawei Technologies Co., Ltd.



NOTE

You are advised not to store other files in the path for storing the firmware upgrade package. Otherwise, the parsing efficiency of the tool will be affected.

d. Set parameters.



i. Select any node as the device form.

ii. Click **Match Firmware Package**. The matched firmware information will be displayed.

iii. Select the firmware to be upgraded. Based on the check result in **Checking Version Mappings**, select **Do Upgrade** in the **Select upgrade strategy** column for the firmware whose current version is earlier than the target version.

NOTE

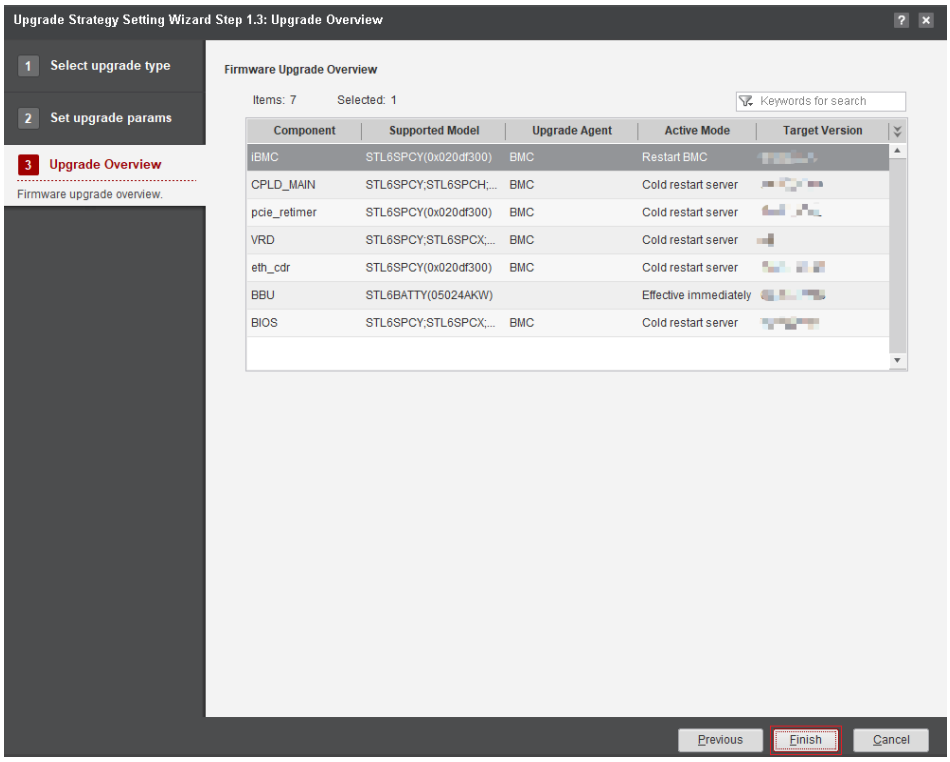
Select all to force upgrade: In special scenarios, if the current firmware version is later than the target version, select this option. This option forcibly upgrades all firmware to the target version.

iv. (Optional) Click **Preview The Strategy**. The **Upgrade Strategy Preview** dialog box is displayed.

In the **Upgrade strategy** area, check that the upgrade policy to be executed in the **Expected Result** column is correct and click **OK**.

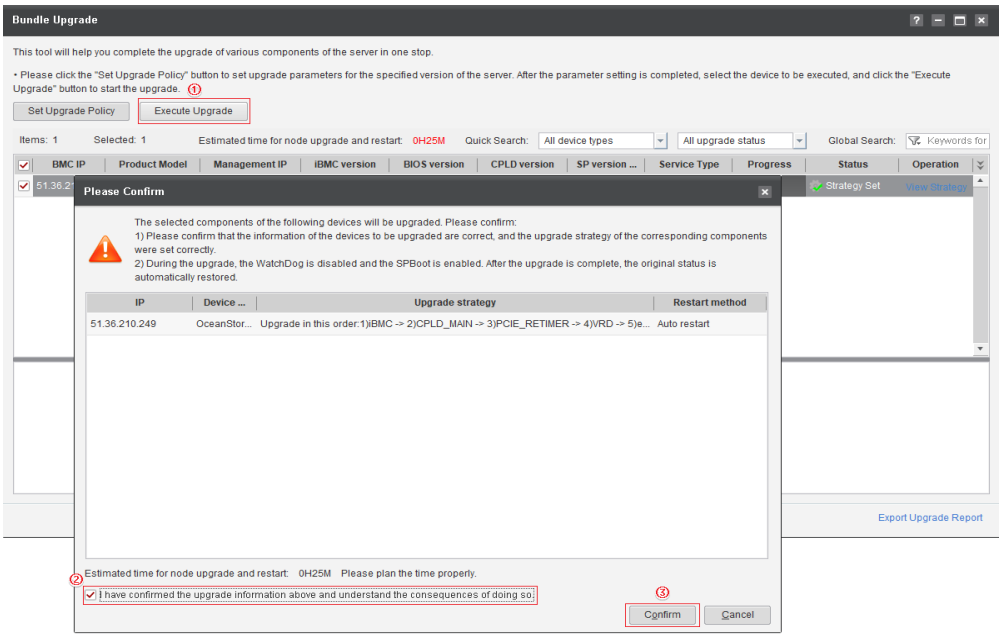
v. Click **Next**.

e. View the basic information about the firmware upgrade and click **Finish**.

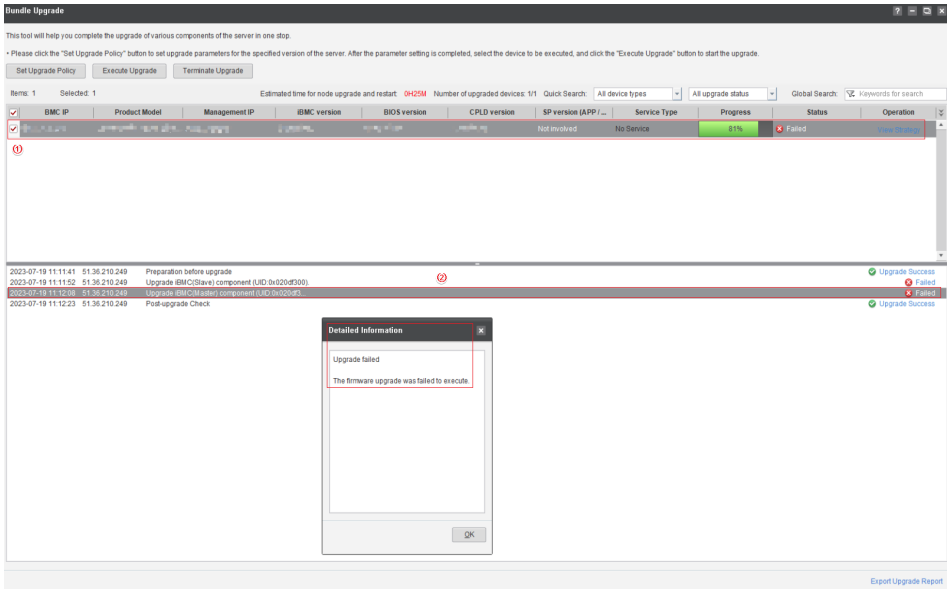


3. Click **Execute Upgrade**. A confirmation dialog box is displayed. After confirming the information, select **I have confirmed...** and click **Confirm**.

 Copyright © Huawei Technologies Co., Ltd.



4. After the upgrade is complete, check whether **Upgrade Success** is displayed in the **Status** column of all nodes.
   - If yes, click ✕ in the upper right corner of the dialog box to end the upgrade process.
   - If no, perform the following steps for each failed node (after the troubleshooting is complete, click ✕ in the upper right corner of the dialog box):



   i. Select the failed node. The upgrade details are displayed in the lower part.
   ii. In the details area, locate the failed steps and click them one by one. Then perform troubleshooting according to the description in the displayed **Detailed Information** dialog box.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

You can also click **Export Upgrade Report** in the lower right corner to collect and view the upgrade results of all nodes.

----End

5.4.1.5.1.5 (Optional) Installing the OS

Context

This section describes how to install the OS on SmartKit.

NOTE

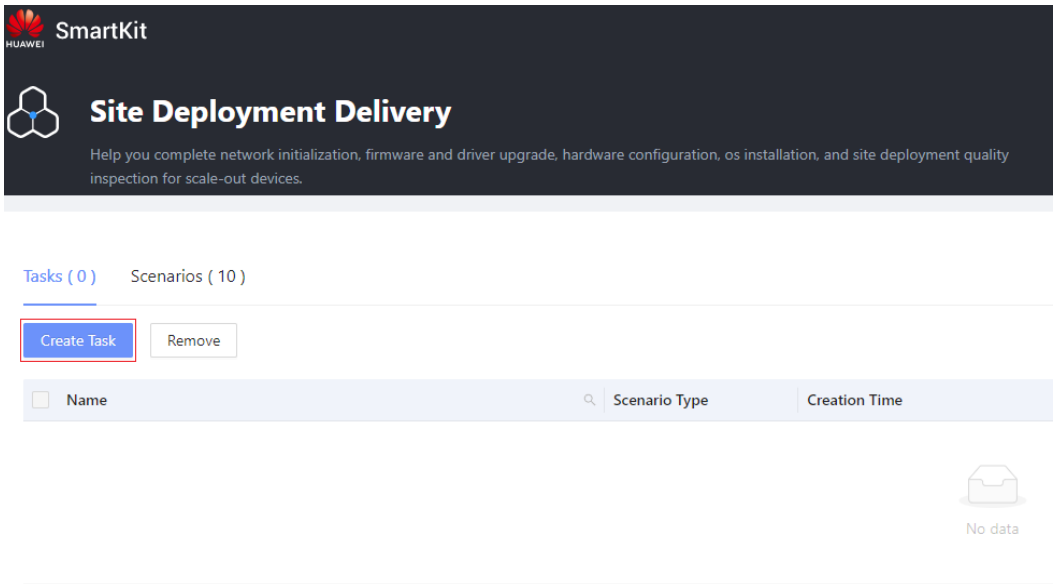
The GUI of SmartKit may vary with the version.

Prerequisites

- You have determined that the OS needs to be installed according to the check results in **Checking Version Mappings** and downloaded the OS image file.
- The installation PC communicates properly with the newly configured iBMC network of a node.

Procedure

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.



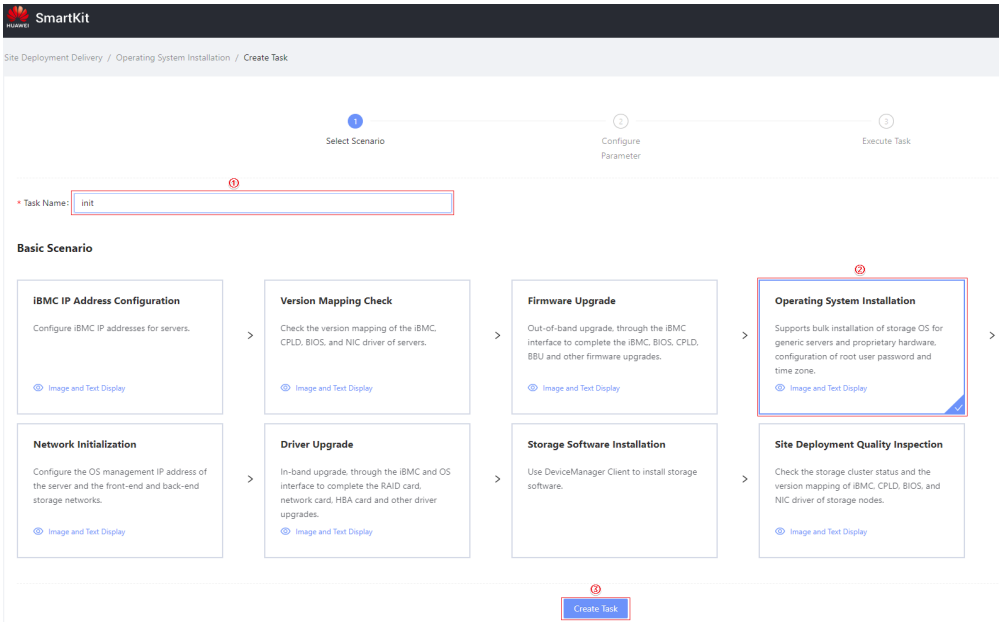
Step 2 Select a scenario.

1. Set **Task Name**, select **Operating System Installation**, and click **Create Task**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).

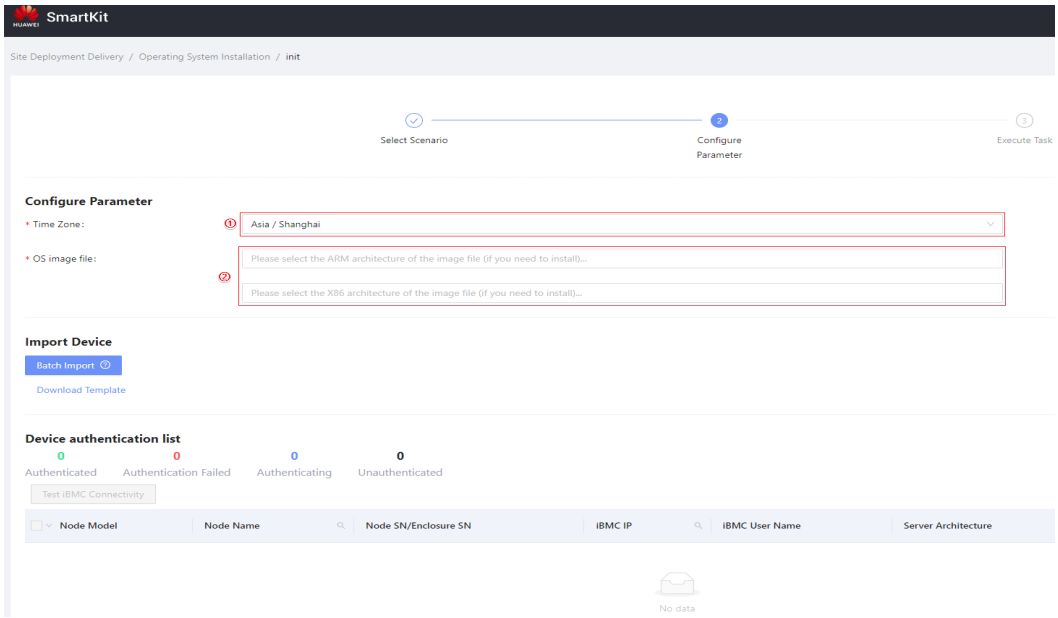


2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

NOTE

If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

Step 3 Configure parameters.



1. In the **Time Zone** drop-down list, select a time zone as required.

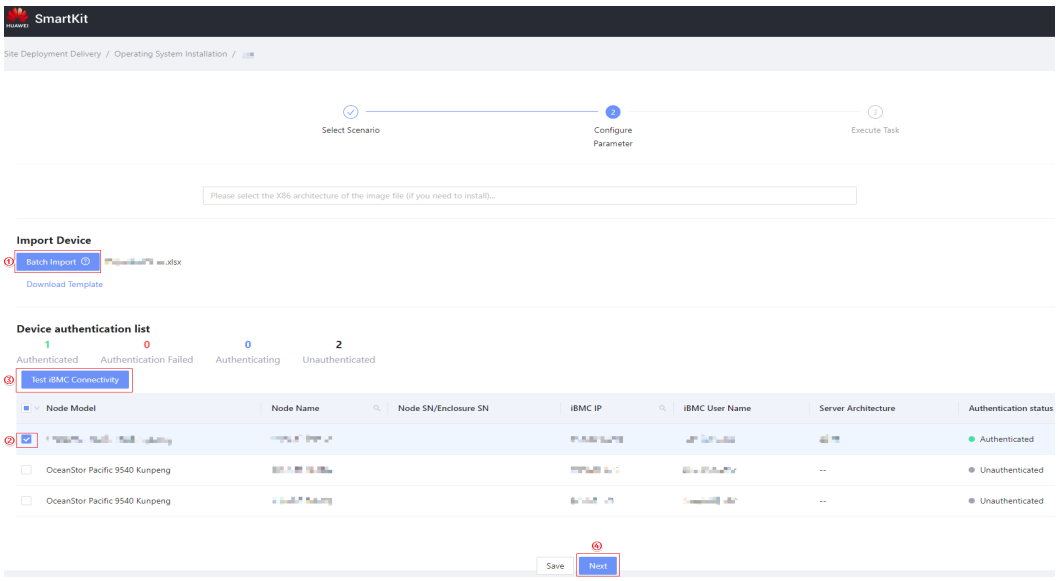
 Copyright © Huawei Technologies Co., Ltd.

2. In the **OS image file** text box, select the path for storing the image file according to the architecture of the nodes where the OS is to be installed.

   NOTE

   - Image files of the Arm and x86 architectures can be uploaded. If only one node architecture is involved, upload only the OS image file of the architecture. If two node architectures are involved, upload the OS image files of the two architectures.
   - If you are uncertain about the node architecture, see the **Server Architecture** column after the iBMC authentication is complete in **Step 4.2**.

Step 4 Import and authenticate devices.



1. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.
2. In **Device authentication list**, select a node where the OS is to be installed and click **Test iBMC Connectivity** for authentication.

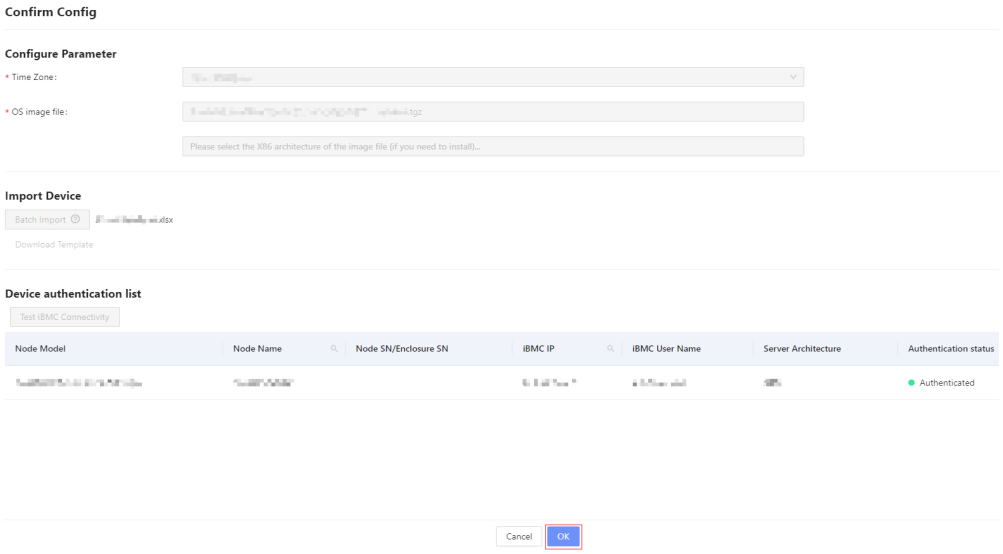
   NOTE

   If authentication failure is displayed in the **Authentication status** column of a node, rectify the fault according to the description in .
3. After the authentication is complete, click **Next**.

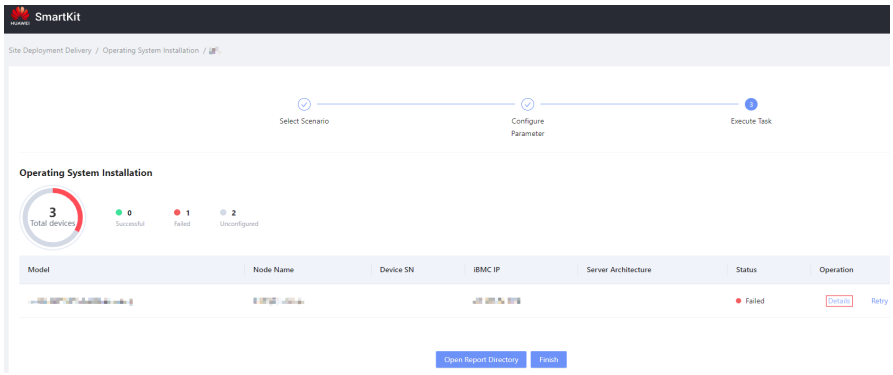
Step 5 Execute the task.

1. After confirming that the basic configuration information is correct, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

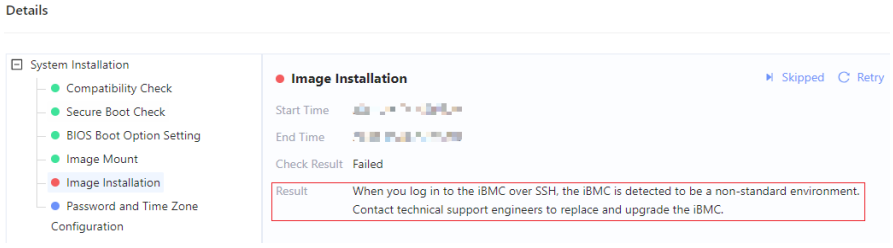


2. After the task is complete, check whether **Successfully** is displayed in the **Status** column of each node.
   - If yes, click **Finish**.
   - If no, perform the following steps for each failed node (after the troubleshooting is complete, click **Finish**):
     i. Click **Details** in the **Operation** column of the node.



> **NOTE**
>
> You can also click **Open Report Directory** in the lower part to collect and view the installation results of all nodes.

     ii. On the **Details** page, click each failed item (marked in red) on the left and perform troubleshooting according to the description in **Result**. The following is an example:



----End

 Copyright © Huawei Technologies Co., Ltd.

5.4.1.5.1.6 Initializing Networks

Context

This section describes how to initialize networks on SmartKit, including configuring the management IP addresses of all nodes and front-end and back-end storage IP addresses of storage nodes.

NOTE

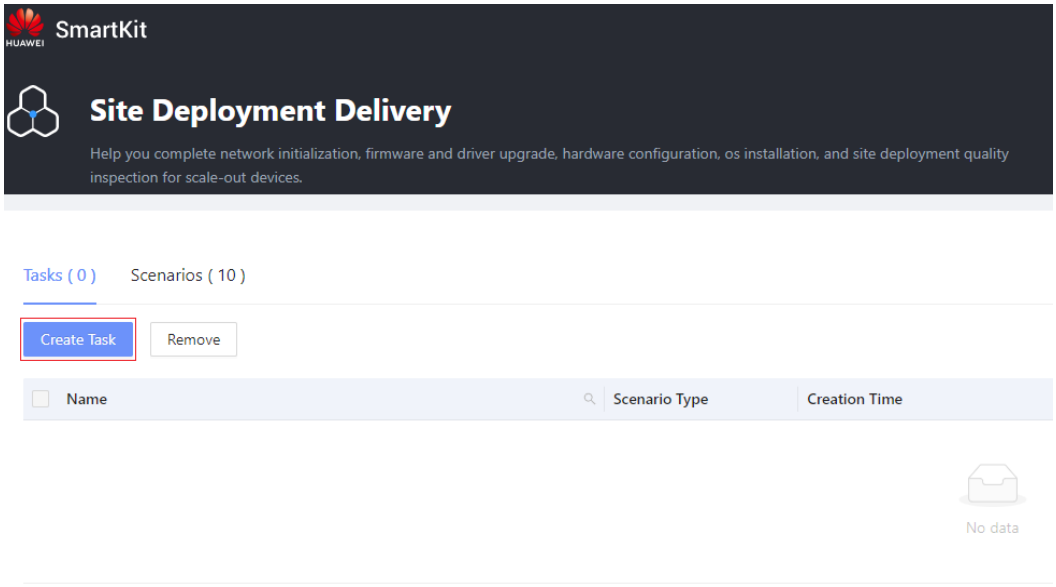
The GUI of SmartKit may vary with the version.

Prerequisites

- The installation PC communicates properly with the newly configured iBMC network of a node.

Procedure

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.



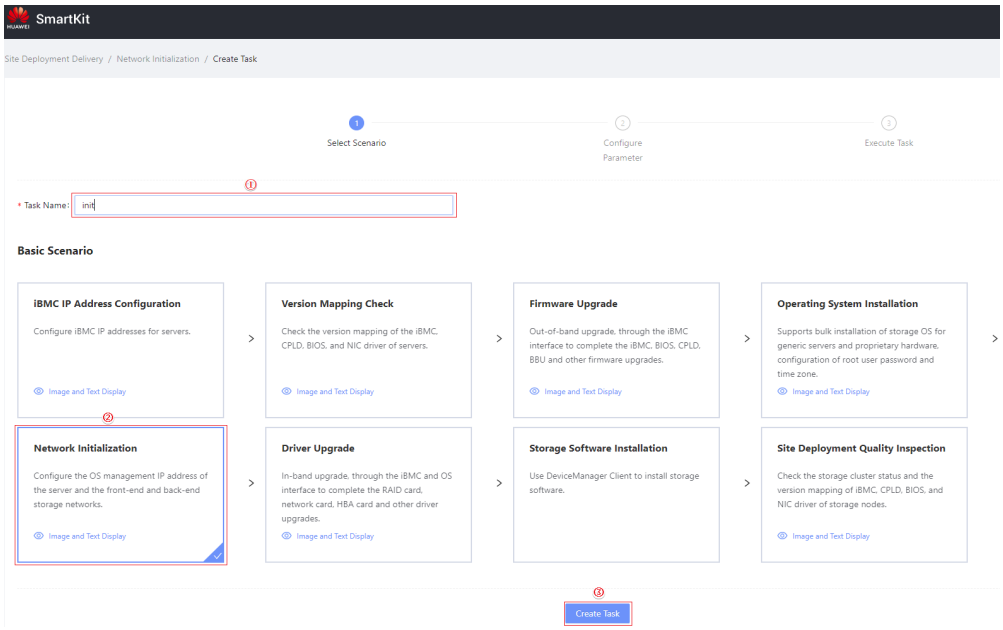
Step 2 Select a scenario.

1. Set **Task Name**, select **Network Initialization**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).

 Copyright © Huawei Technologies Co., Ltd.

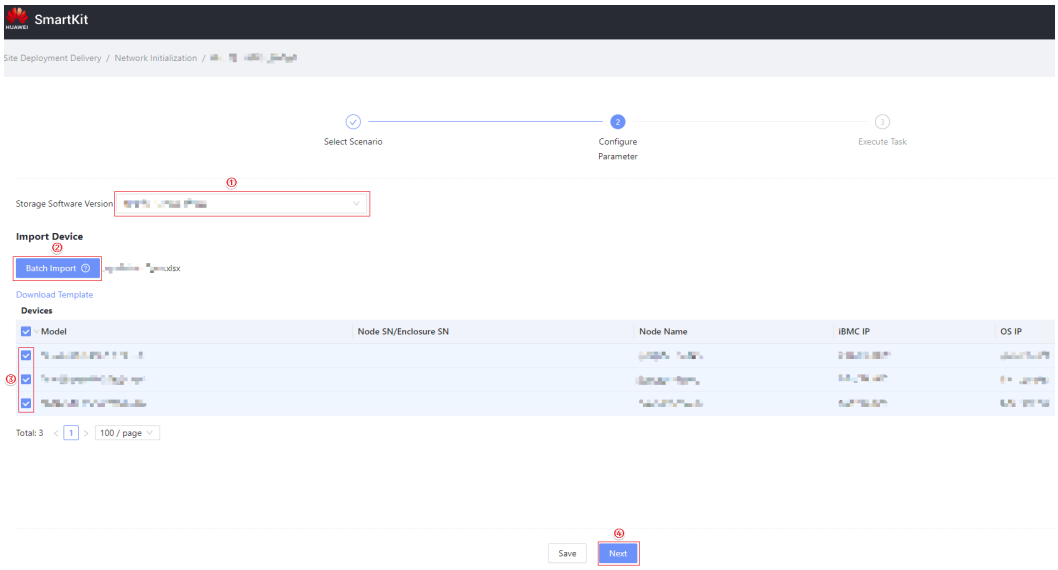


2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

   NOTE

   If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

Step 3 Configure parameters.

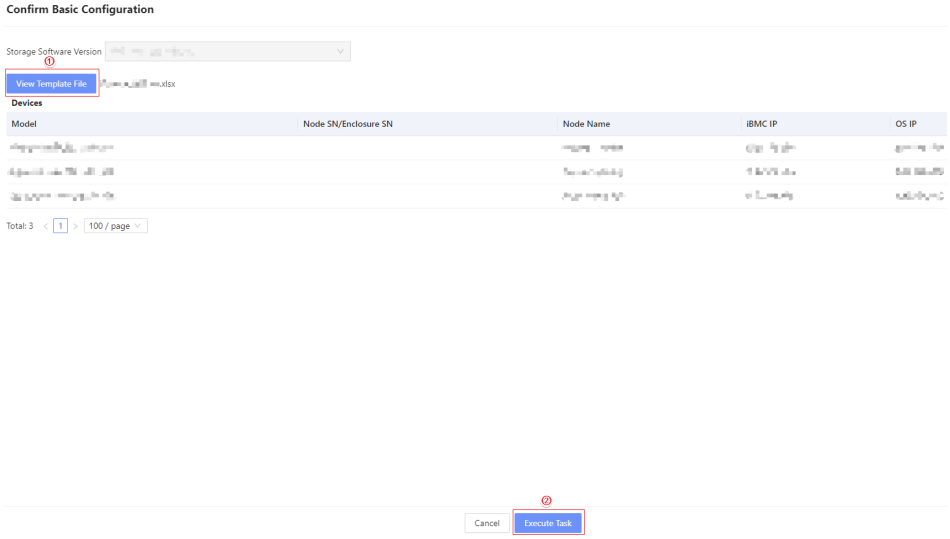


1. Set **Storage Software Version**.
2. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.
3. In **Devices**, select the nodes for which you want to initialize networks.
4. Click **Next**.

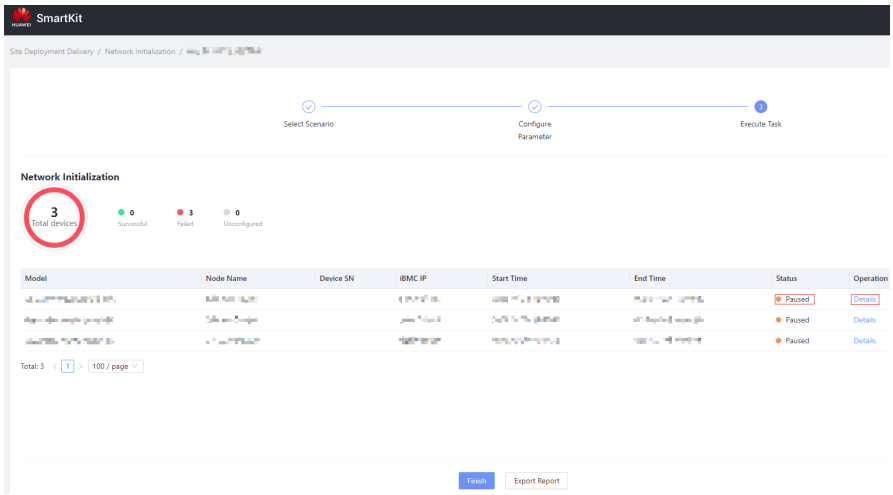
Step 4 Execute the task.

 Copyright © Huawei Technologies Co., Ltd.

1. Click **View Template File**. The imported LLD configuration file will be automatically opened. Confirm the information to be configured. After confirming that the information is correct, click **Execute Task**.

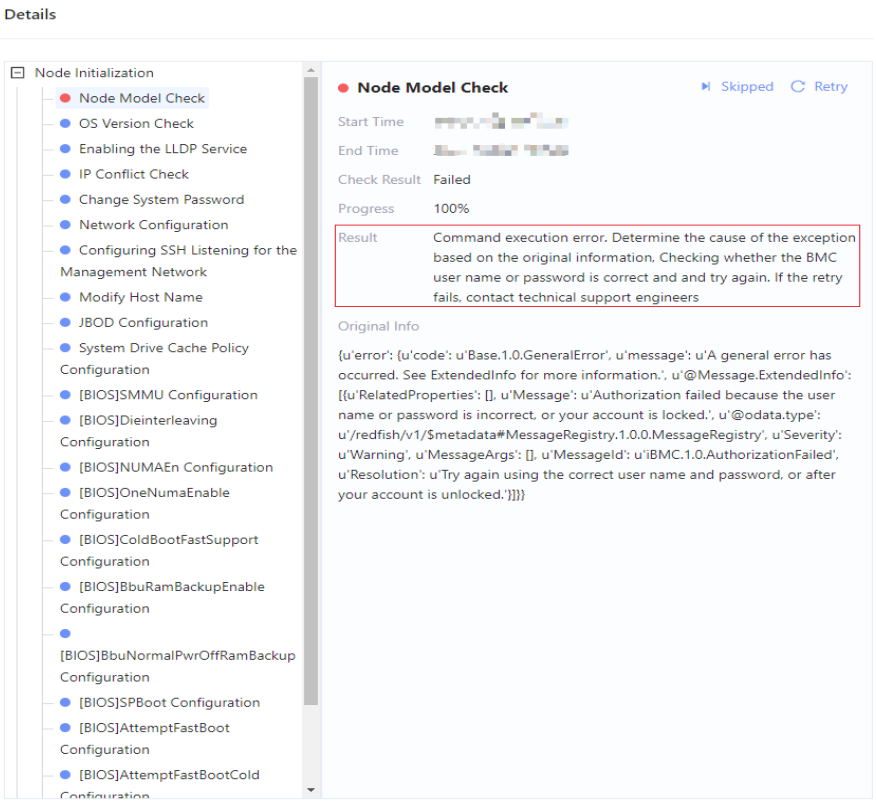


2. After the task is complete, check whether **Successfully** is displayed in the **Status** column of each node.
   - If yes, click **Finish**.
   - If no, perform the following steps for each failed node (after the troubleshooting is complete, click **Finish**):
     i. Click **Details** in the **Operation** column of the node.



     ii. On the **Details** page, click each failed item (marked in red) on the left and perform troubleshooting according to the description in **Result**. The following is an example:

 Copyright © Huawei Technologies Co., Ltd.



NOTE

You can also click **Export Report** in the lower part to collect and view the configuration results of all nodes.

----End

5.4.1.5.1.7 (Optional) Upgrading Drivers

Context

This section describes how to upgrade drivers on SmartKit.

NOTE

The GUI of SmartKit may vary with the version.

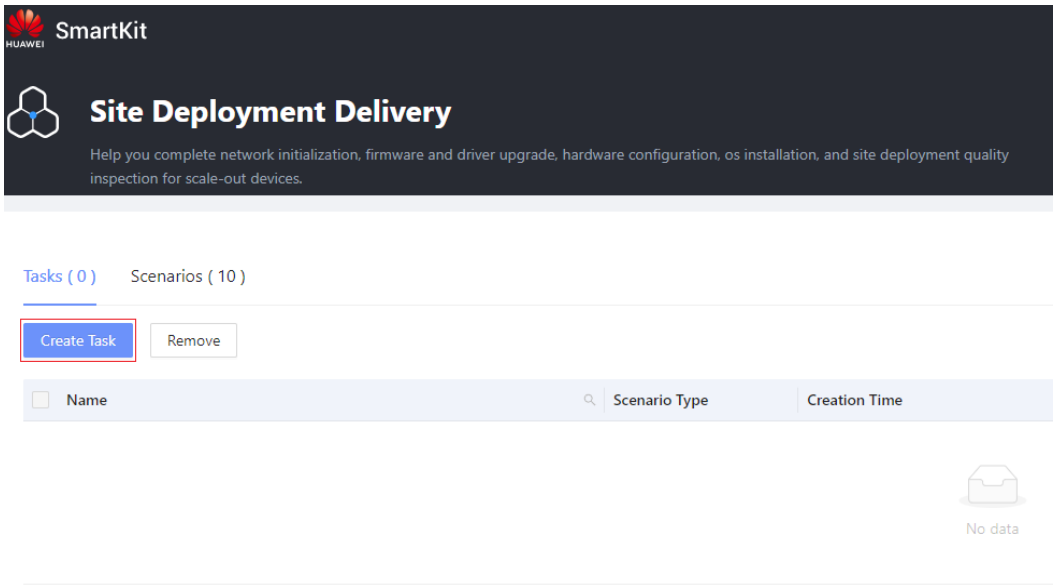
Prerequisites

- You have determined that a driver needs to be upgraded according to the check results in **Checking Version Mappings** and downloaded the corresponding driver package.
- The installation PC communicates properly with the management network of a node.
- The installation PC communicates properly with the newly configured iBMC network of a node.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.

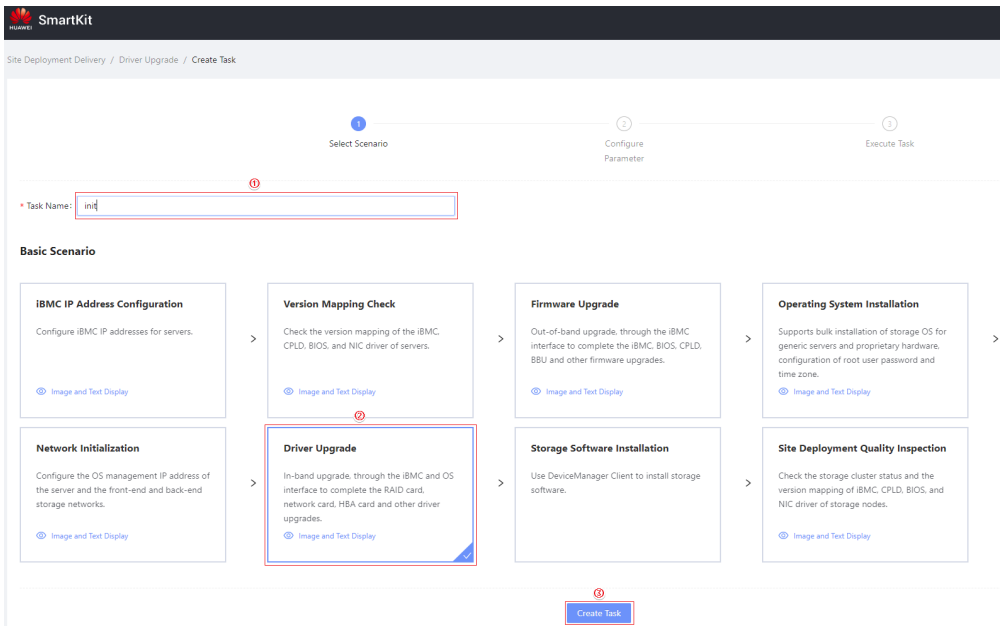


Step 2 Select a scenario.

1. Set **Task Name**, select **Driver Upgrade**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).



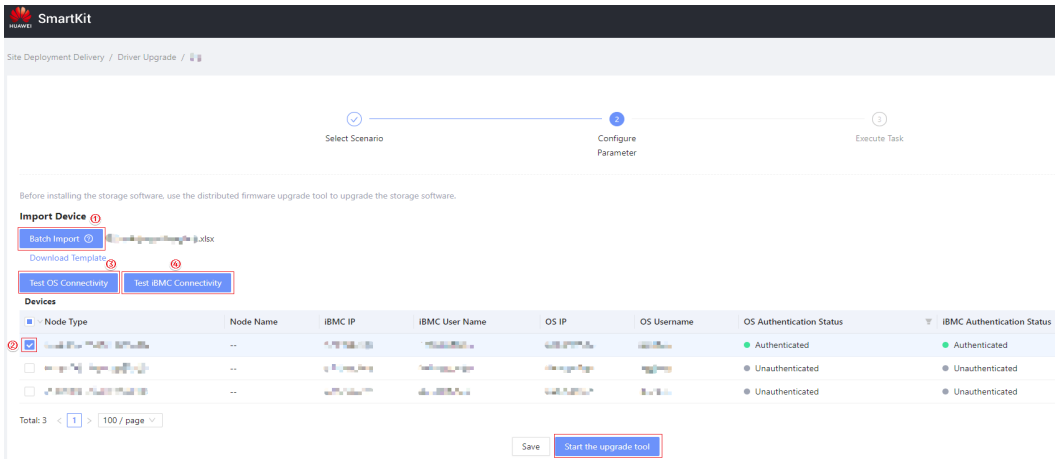
2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

Step 3 Configure parameters.



1. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.
2. In **Devices**, select a node whose driver needs to be upgraded.
3. Click **Test OS Connectivity** to perform OS authentication.

   NOTE

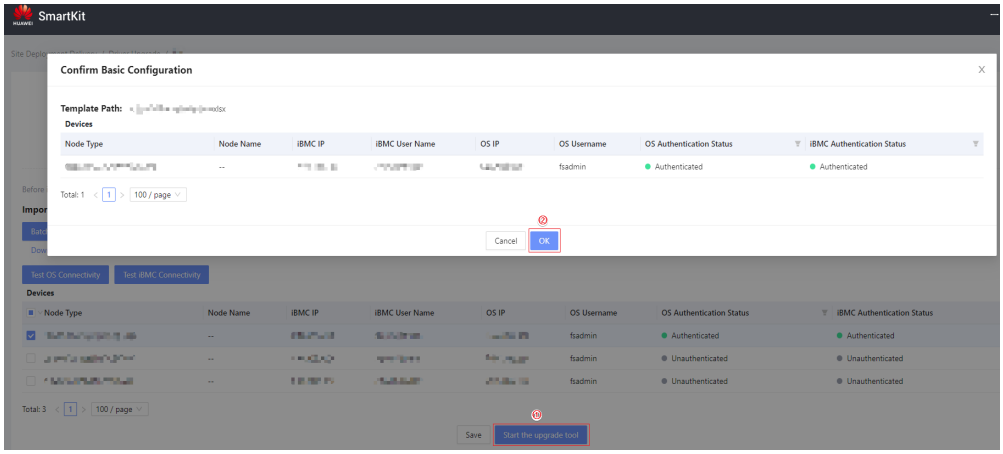
   If authentication failure is displayed in the **OS Authentication Status** column, rectify the fault according to the description in .
4. Click **Test iBMC Connectivity** to perform iBMC authentication.

   NOTE

   If authentication failure is displayed in the **iBMC Authentication Status** column, rectify the fault according to the description in .

Step 4 Execute the task.

1. Click **Start the upgrade tool**. A dialog box is displayed for you to confirm the configuration information. After confirming that the information is correct, click **OK**. The driver upgrade page is displayed.



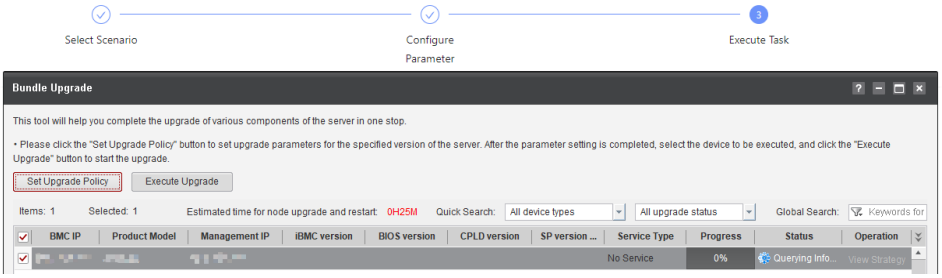
 Copyright © Huawei Technologies Co., Ltd.

2. Set the upgrade policy.

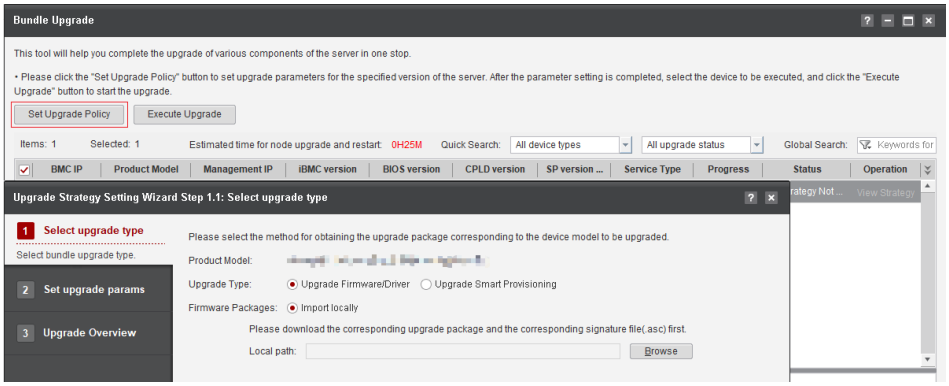
   a. Select the devices to be upgraded.

   NOTE

   Devices of different models need to be upgraded in different batches. Select devices of the same model to set the upgrade policy.



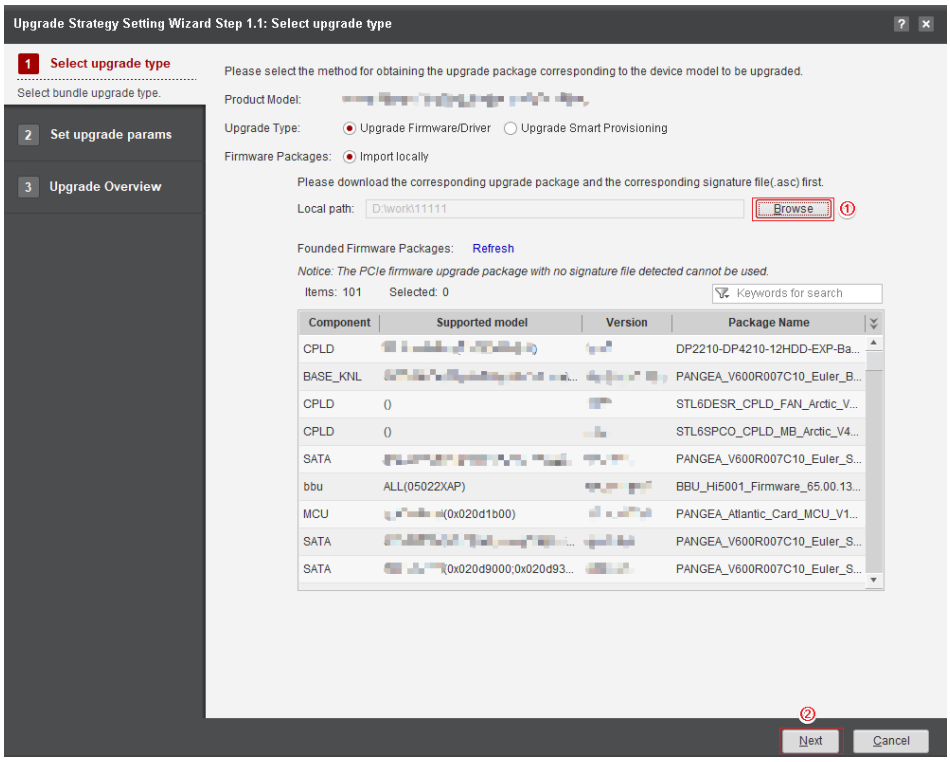
   b. Click **Set Upgrade Policy**. The **Upgrade Strategy Setting Wizard** dialog box is displayed.



   c. Import the driver upgrade package.

   Click **Browse**, select the path for storing the driver upgrade package, and click **Next**.

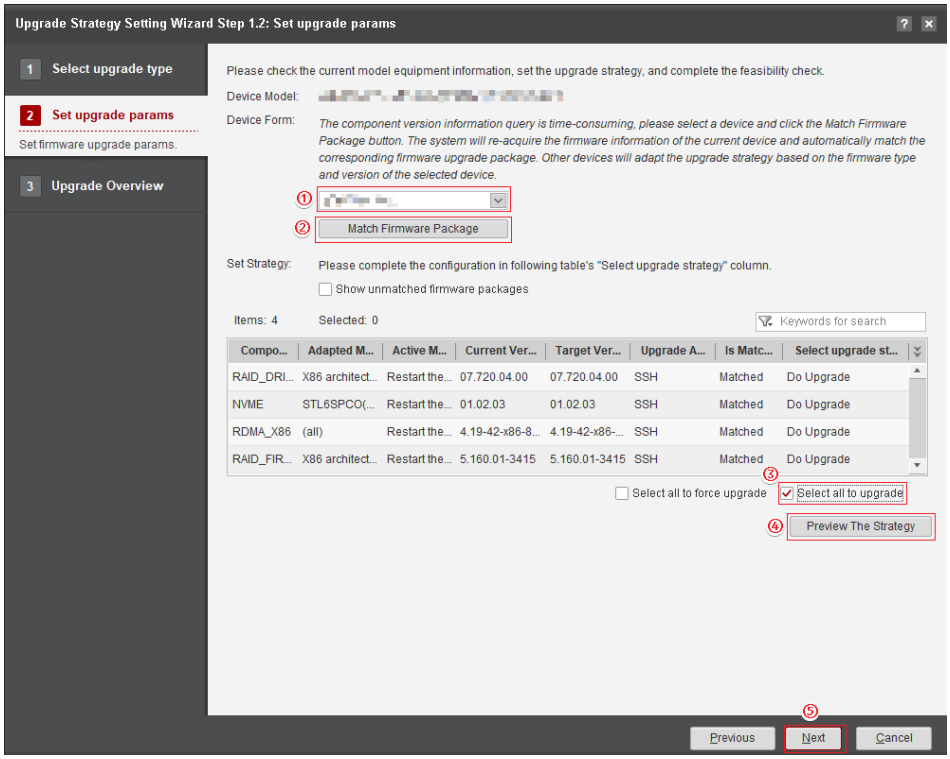
 Copyright © Huawei Technologies Co., Ltd.



NOTE

You are not advised to store other files in the path for storing the driver upgrade package. Otherwise, the parsing efficiency of the tool will be affected.

d. Set parameters.



i. Select any node as the device form.

ii. Click **Match Firmware Package**. The matched driver information will be displayed.

iii. Select the drivers to be upgraded. Based on the check result in **Checking Version Mappings**, select **Do Upgrade** in the **Select upgrade strategy** column for the drivers whose current version is earlier than the target version.

NOTE

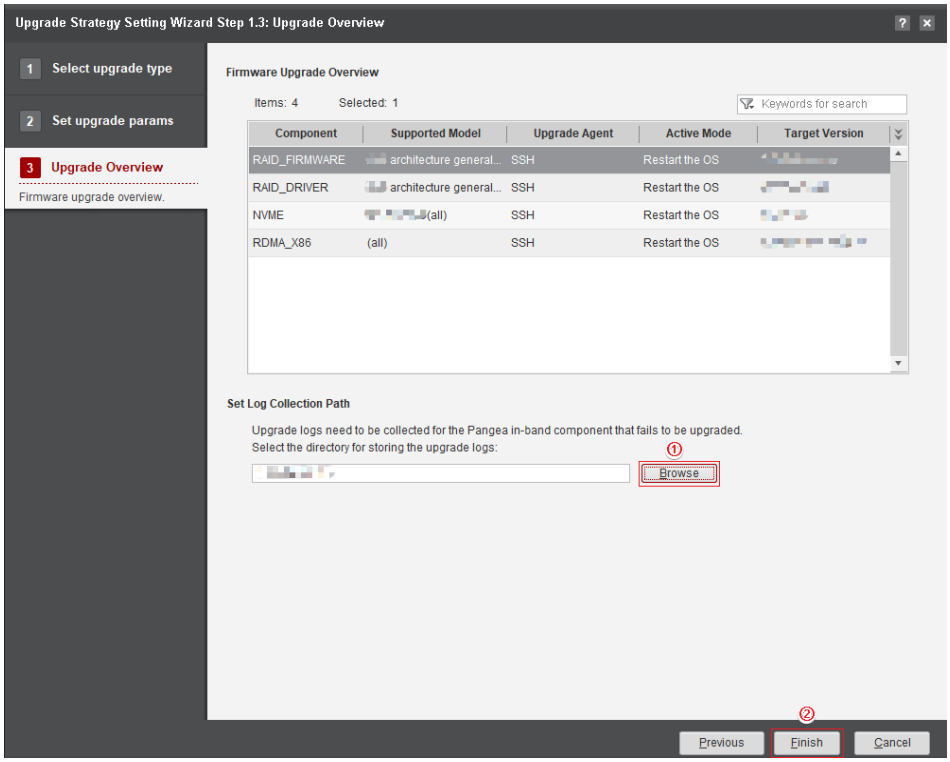
Select all to force upgrade: In special scenarios, if the current driver version is later than the target version, select this option. This option forcibly upgrades all drivers to the target version.

iv. (Optional) Click **Preview The Strategy**. The **Upgrade Strategy Preview** dialog box is displayed.

In the **Upgrade strategy** area, check that the upgrade policy to be executed in the **Expected Result** column is correct and click **OK**.

v. Click **Next**.

e. View the basic information about the driver upgrade.



i. (Optional) Click **Browse** to set the log collection path.

ii. Click **Finish**.

3. Click **Execute Upgrade**. A confirmation dialog box is displayed. After confirming the information, select **I have confirmed...** and click **Confirm**.

 Copyright © Huawei Technologies Co., Ltd.

4. After the upgrade is complete, check whether **Upgrade Success** is displayed in the **Status** column of all nodes.

   – If yes, click in the upper right corner of the dialog box to end the upgrade process.

   – If no, perform the following steps for each failed node (after the troubleshooting is complete, click in the upper right corner of the dialog box):

      i. Select the failed node. The upgrade details are displayed in the lower part.

      ii. In the details area, locate the failed steps and click them one by one. Then perform troubleshooting according to the description in the displayed **Detailed Information** dialog box.

Copyright © Huawei Technologies Co., Ltd.

NOTE

You can also click **Export Upgrade Report** in the lower right corner to collect and view the upgrade results of all nodes.

----End

5.4.1.5.2 Installing OceanStor Pacific Series Software

Scenarios

Use DeviceManager to install the OceanStor Pacific series software in LLD-based configuration mode.

Prerequisites

- The OS of the installation PC meets the compatibility requirements. For details, see the **DeviceManager-Client** requirements in **Huawei Storage Interoperability Navigator**.
- The network connection between the installation PC and all nodes is normal.
- The command prompt for user **root** is **#**.
- For OceanStor Pacific 9550/OceanStor Pacific 9350 devices, you must select all disks to create a storage pool.

Procedure

Step 1 Check the **cloud_vpc.ini** file. Perform the following operations on each storage node:

1. Use SSH to log in to a storage node as user **fsadmin**. To obtain the default user password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. After the password is changed, log in to the node again.
2. Run the **su - root** command to switch to user **root**.
3. Check the **cloud_vpc.ini** file by referring to **5.5.3 Checking the cloud_vpc.ini File**.

Step 2 Decompress **OceanStor-Pacific_8.2.1RC1_DeviceManagerClient.zip** on the installation PC, and double-click **run.bat** in the decompression directory. The browser automatically opens DeviceManager Client.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

The OS time of management nodes must be the same. Otherwise, change the time to be the same by referring to **5.5.25.7 Changing the System Time of a Node**.

During the installation, do not close the **OceanStor-Pacific_devicemanager-client** window.

The decompression directory of the software package cannot contain spaces or brackets.

DeviceManager Client cannot be opened using a shared path.

If the browser does not automatically open, open the browser manually and enter **https://127.0.0.1:***port* in the address box. The value of *port* is the character string in the **OceanStor-Pacific_devicemanager-client** window. For example, in **Starting ProtocolHandler ["https-jsse-nio-127.0.0.1-8088"]**, the port number is **8088**.

If multiple clusters need to be installed, close the **OceanStor-Pacific_devicemanager-client** window after one cluster is installed, and then open the **OceanStor-Pacific_devicemanager-client** window again to install the next cluster.

Step 3 The browser may display a message indicating that the security certificate of the website is incorrect. You can ignore the security warning message as prompted if the IP address is correct.

Take Google Chrome as an example. On the security prompt page, click **Advanced** and select **Proceed to** *XXX.XXX.XXX.XXX* **(unsafe)**. The OceanStor Pacific series installation page is displayed.

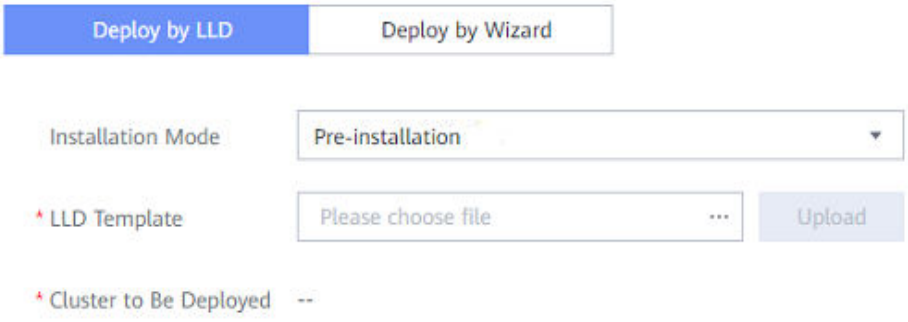
Step 4 Select **Deploy by LLD**.

Step 5 Use the LLD template to install and deploy the OceanStor Pacific series software. Two installation modes are supported: **Pre-installation** and **Regular installation**.

NOTE

- **Pre-installation**: The basic service package has been installed on the nodes and you do not need to upload the software package.
- **Regular installation**: The basic service package is not installed on the nodes and you need to upload the software package.

1. Identify the installation mode. For details, see **5.5.21 Identifying the Installation Mode**.
2. Perform the following operations depending on the installation mode.
   - Pre-installation:



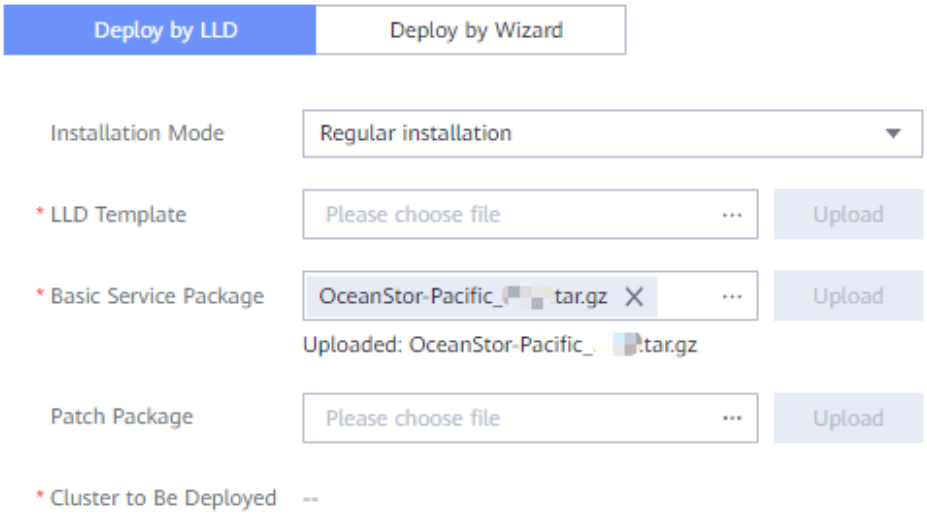
 Copyright © Huawei Technologies Co., Ltd.

i. Click ... next to **LLD Template**, select the configured LLD configuration file, and click **Upload**.

ii. **Cluster to Be Deployed** indicates the cluster name set in the LLD configuration file.

iii. Click **Deploy** to start installation and deployment of the OceanStor Pacific series software.

– Regular installation:



i. Click ... next to **LLD Template**, select the configured LLD configuration file, and click **Upload**.

ii. Upload software packages. After the upload is successful, the system displays the software package names.

1) Click ... next to **Basic Service Package**, select basic service package **OceanStor-Pacific_8.2.1RC1.tar.gz**, and click **Upload**. After the package is uploaded successfully, the system displays the package name.

2) (Optional) If a patch needs to be installed, click ... next to **Patch Package**, select patch package **OceanStor-Pacific_8.2.1RC1.SPH*XXX***, and click **Upload**.

iii. **Cluster to Be Deployed** indicates the cluster name set in the LLD configuration file.

iv. Click **Deploy** to start installation and deployment of the OceanStor Pacific series software.

Step 6 The system automatically starts to deploy the cluster.

Step 7 After the deployment is complete, ping the management, storage, or control IP addresses of other nodes from a node to ensure that the network communication between nodes is normal.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

To run the **ping** command, you need to enter the minisystem view first as follows:

1. Use an SSH tool to log in to a node as user **fsadmin** and enter the cliportal view. To obtain the default user password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. After the password is changed, log in to the node again. If the default password has been changed, use the new password to log in.
2. Run the **minisystem** command and enter the password of user **root** as prompted to go to the minisystem view.

Step 8 Load a license by referring to **5.4.2.8 Obtaining and Loading a License** so that the system can obtain a new validity period and service authorization.

----End

Follow-up Procedure

- On the installation PC, double-click the **shutdown.bat** script in the decompression directory of **OceanStor-Pacific_8.2.1RC1_DeviceManagerClient.zip** to close the DeviceManager Client window. If the window cannot exit normally, click in the upper right corner to close it.
- If the RoCE network is configured, you need to configure RoCE flow control on switches. For details, see **5.5.2.2 Configuring Flow Control for a Switch**. If you have configured RoCE flow control, skip this operation.
- If the RoCE network is configured, you need to configure ACL rules for switches. For details, see **5.5.2.3 Configuring ACL Rules for Switches**. If you have configured them, skip this operation.
- If parameter settings are incorrect after the software is installed, uninstall the OceanStor Pacific series software and reinstall it. For details about how to uninstall the OceanStor Pacific series software, see **5.5.19 Uninstalling OceanStor Pacific Series Software**.
- After the installation and deployment are complete, you can use the management IP addresses of DeviceManager and nodes to remotely log in to management and storage nodes.
- Update default accounts in time. For details, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*.
- Update security certificates in time. For details, see section "Security Certificate Management" in *OceanStor Pacific Series 8.2.1 Security Configuration Guide*.

5.4.1.6 Installation Procedure (Applicable to Wizard-based Configuration)

5.4.1.6.1 Configuring iBMC IP Addresses for Nodes

Scenarios

iBMC is a remote management system. It monitors and manages hardware in a highly reliable manner.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

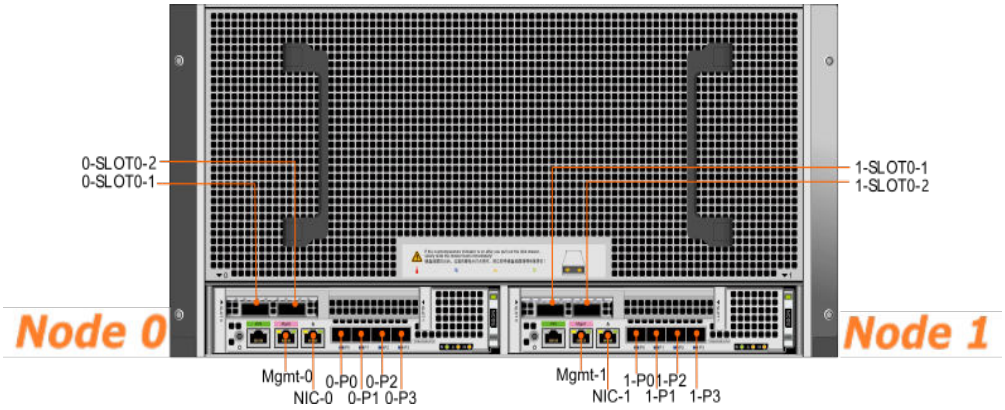
Step 1 Obtain the default IP addresses of iBMC management network ports.

NOTE

The IP address of the installation PC must be in the same network segment as the default iBMC IP address. The default iBMC masks of all devices are 255.255.255.0.

- The default iBMC IP address of OceanStor Pacific 9340/OceanStor Pacific 9540/OceanStor Pacific 9520/OceanStor Pacific 9920 is 192.168.2.100.
- An OceanStor Pacific 9550/OceanStor Pacific 9350 device has two nodes, whose iBMC network ports are Mgmt-0 and Mgmt-1 respectively. The default iBMC IP address corresponding to the Mgmt-0 port is 192.168.2.101, and the default iBMC IP address corresponding to the Mgmt-1 port is 192.168.2.102. **Figure 5-2** shows the iBMC network ports of OceanStor Pacific 9550/ OceanStor Pacific 9350.

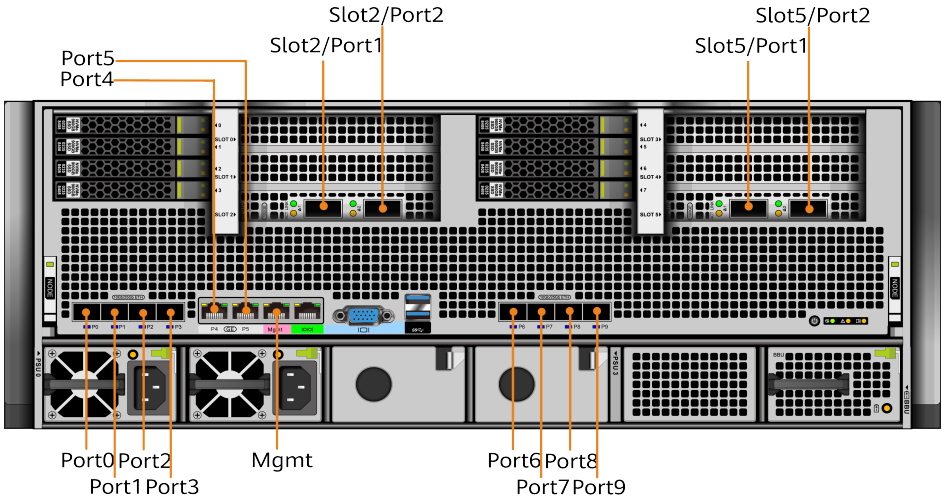
Figure 5-2 Example of planning ports for a storage node (using 2-port NICs)



- OceanStor Pacific 9546/OceanStor Pacific 9346
  - The iBMC network port of OceanStor Pacific 9546 (One Node per Chassis, Two CPUs per Node)OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node) is the Mgmt port, and its default IP address is 192.168.2.102. **Figure 5-3** shows the iBMC network port of OceanStor Pacific 9546 (One Node per Chassis, Two CPUs per Node)/OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node)..

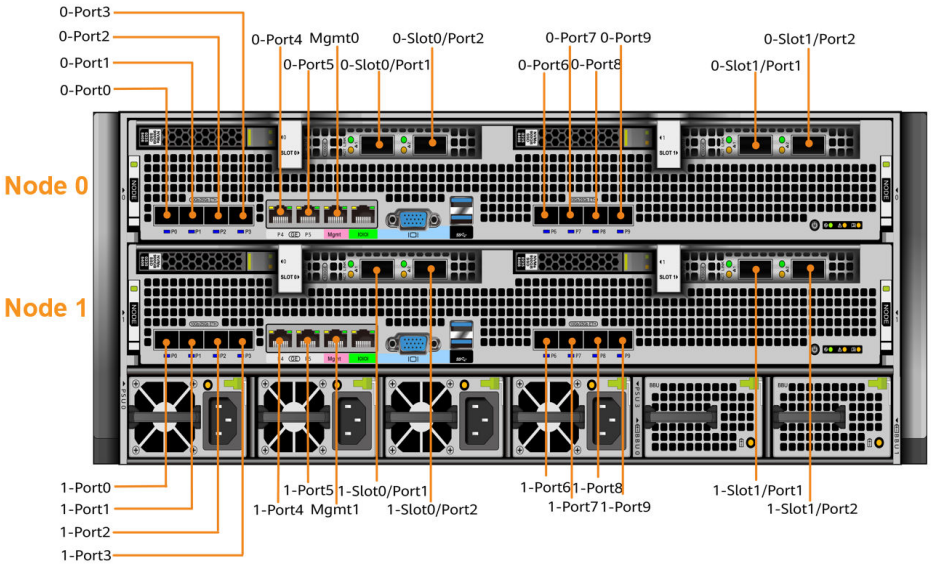
 Copyright © Huawei Technologies Co., Ltd.

Figure 5-3 Example of planning ports for a node with two CPUs



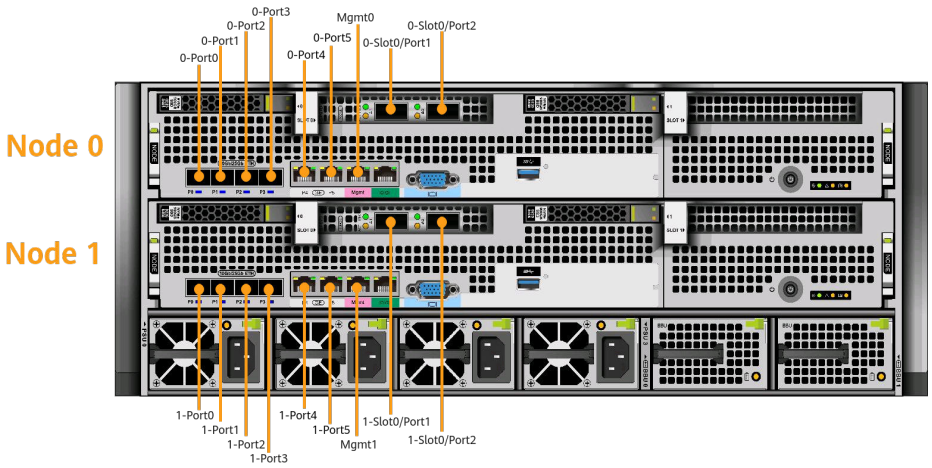
– An OceanStor Pacific 9546 (Two Nodes per Chassis) device has two nodes, whose iBMC network ports are Mgmt0 and Mgmt1 respectively. The default iBMC IP address corresponding to the Mgmt0 port is 192.168.2.101, and the default iBMC IP address corresponding to the Mgmt1 port is 192.168.2.102. **Figure 5-4** shows the iBMC network ports of OceanStor Pacific 9546 (Two Nodes per Chassis, Two CPUs per Node), and **Figure 5-5** shows the iBMC network ports of OceanStor Pacific 9546 (Two Nodes per Chassis, One CPU per Node).

Figure 5-4 Example of planning ports for a node with two CPUs



 Copyright © Huawei Technologies Co., Ltd.

Figure 5-5 Example of planning ports for a node with one CPU



Step 2 In the address box of a browser, enter **https://***Default IP address of the iBMC management network port* and enter the user name and password to log in to the iBMC system of a node. The default user name is **Administrator**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

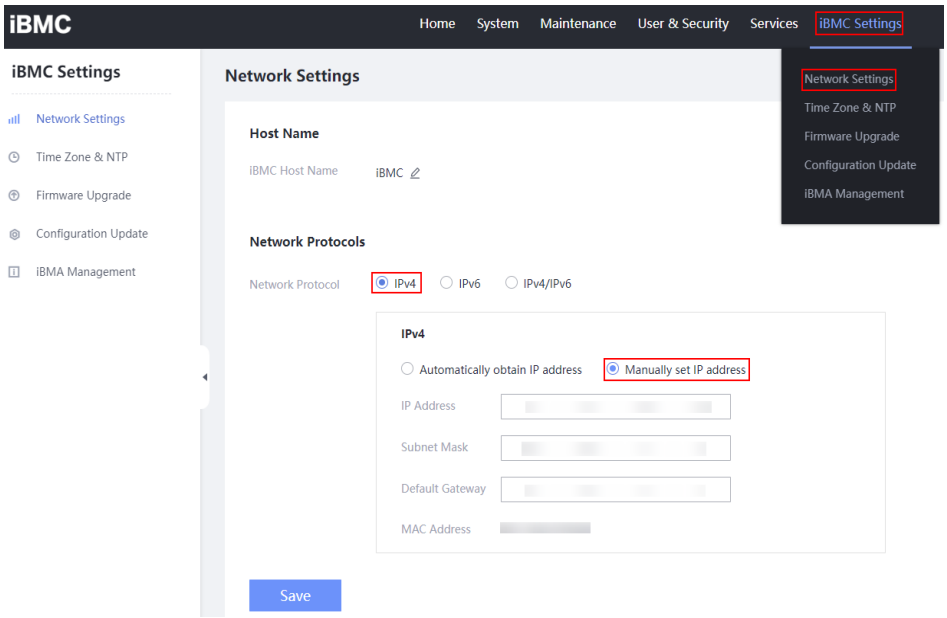
Step 3 Configure iBMC IP addresses.

1. Choose **iBMC Settings** > **Network Settings**.

   NOTE

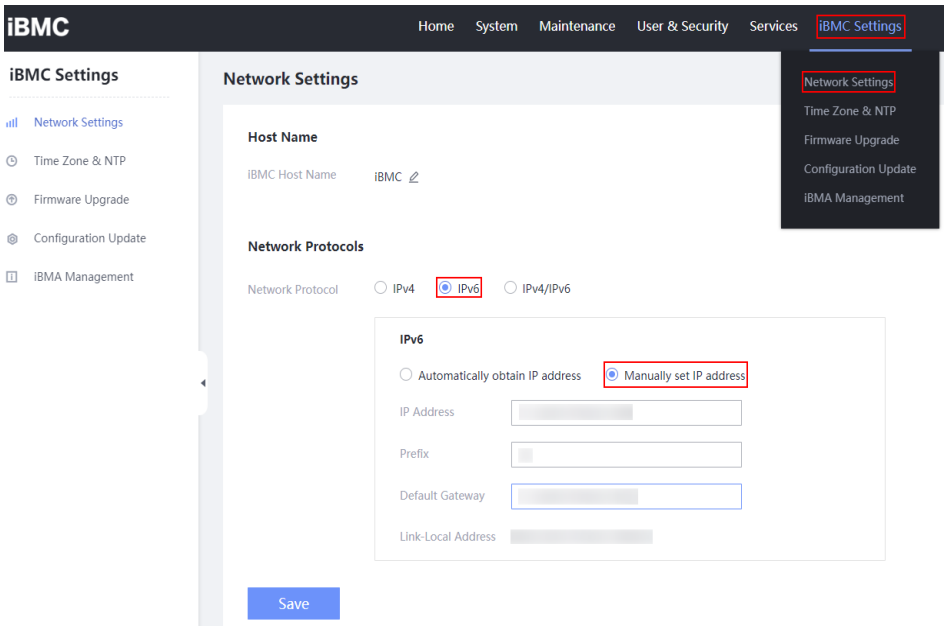
   For details about the support for IPv4 and IPv6, see section "Network Requirements" of the desired scenario in *OceanStor Pacific Series 8.2.1 Network Planning Guide (SFS)*.

   - When configuring IPv4 addresses, select **IPv4** and **Manually set IP address**, and set **IP Address**, **Subnet Mask**, and **Default Gateway** in sequence.



   - When configuring IPv6 addresses, select **IPv6** and **Manually set IP address**, and set **IP Address**, **Prefix**, and **Default Gateway** in sequence.

 Copyright © Huawei Technologies Co., Ltd.



2. Click **Save**. After the modification is successful, the system displays a success message.

----End

5.4.1.6.2 Checking Storage Nodes Before Installation

5.4.1.6.2.1 Checking Whether a RAID Controller Card Is Used (Applicable to Kunpeng-based Devices)

Procedure

Step 1 Log in to the iBMC system.

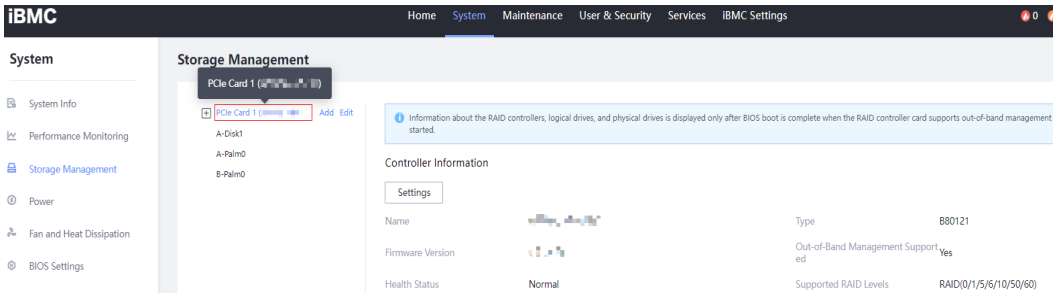
Enter the new iBMC IP address in the address box of a browser and enter the user name and password to log in to the iBMC system of a node. The default user name is **Administrator**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

- **https://***iBMC IPv4 address*
- **https://[***iBMC IPv6 address***]**

Step 2 Choose **System** > **Storage Management**. If **PCIe Card** *Slot number* **(***RAID controller card model***)** or **RAID Card***Slot number* is displayed, a RAID controller card is used.

An example is provided as follows:

 Copyright © Huawei Technologies Co., Ltd.



----End

5.4.1.6.2.2 OceanStor Pacific 9550, 9546, 9350, and 9346

?.1. Checking the Node Firmware Version

Procedure

Step 1 Log in to the iBMC system.

Enter the new iBMC IP address in the address box of a browser and enter the user name and password to log in to the iBMC system of a node. The default user name is **Administrator**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

https://*iBMC IPv4 address*

Step 2 Go to the **Home** page. Check whether **iBMC Firmware Version** and **BIOS Firmware Version** of the node meet the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

Step 3 Choose **iBMC Settings** > **Firmware Upgrade** > **Version Info**. Check whether **CPLD Version** meets the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

Step 4 If the requirements are not met, upgrade the firmware to the target version by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*.

----End

?.2. Checking the OS Version

Procedure

Step 1 Go to the **Home** page of iBMC. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 2 Open the virtual KVM interface, and enter user name **root** to log in to the OS of the storage node. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

Step 3 Run the following command to check whether the OS version meets the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

 Copyright © Huawei Technologies Co., Ltd.

```
cat /proc/version
```

- If the requirements are met, perform the following operations in sequence:
  a. Check the **cloud_vpc.ini** file by referring to **5.5.3 Checking the cloud_vpc.ini File**.
  b. Go to **Checking BIOS Settings**.
- If the requirements are not met, perform the following operations in sequence:
  a. Set BIOS parameters by referring to **5.5.5.1 Configuring BIOS (Applicable to OceanStor Pacific 9950, 9550, 9546, 9350, and 9346)**.
  b. Install an OS that meets the requirements by referring to **5.5.6.1 Installing an OS (Applicable to OceanStor Pacific 9950, 9550, 9546, 9350, and 9346)**.
  c. Upgrade the NIC and disk firmware and drivers by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*.
  d. Check the Hi1822V120 NIC mode by referring to **Checking the Hi1822V120 NIC Mode**.
  e. Check the **cloud_vpc.ini** file by referring to **5.5.3 Checking the cloud_vpc.ini File**.
  f. Configure networks by referring to **5.4.1.6.3 Configuring the Management Network of a Node**.

----End

?.3. Checking BIOS Settings

Procedure

Step 1 Log in to the iBMC system.

Step 2 Choose **iBMC Settings** > **Configuration Update** > **Export Configuration**.

Step 3 Click **Export**.

Step 4 Query the following information in the exported configuration file:

- Check whether the value of **BbuBackForCpuOff** is **Enable**.
- Check whether the value of **OneNumaEnable** is **Enable**.
- For OceanStor Pacific 9950, check whether the value of **BbuNvSize** is **32G**.
- For OceanStor Pacific 9550, check whether the value of **BbuNvSize** is **16G**.
- For OceanStor Pacific 9546, check whether the value of **BbuNvSize** is **16G**.
- For OceanStor Pacific 9350, check whether the value of **BbuNvSize** is **16G**.
- For OceanStor Pacific 9346, check whether the value of **BbuNvSize** is **16G**.
- Check whether the value of **BbuUceEnhance** is **Enable**.

NOTICE

Ensure that the value of **OneNumaEnable** in the configuration file is the same as the preceding value.

 Copyright © Huawei Technologies Co., Ltd.

If the queried values are different from the preceding values, set the parameters by referring to **5.5.5.1 Configuring BIOS (Applicable to OceanStor Pacific 9950, 9550, 9546, 9350, and 9346)**.

----End

?.4. Checking the Device Firmware and Driver Versions

Procedure

Step 1 Log in to the iBMC system.

NOTE

An OceanStor Pacific 9950 device has eight nodes. You need to log in to the iBMC of each node and perform the following operations.

An OceanStor Pacific 9550/OceanStor Pacific 9350 device has two nodes. You need to log in to the iBMC of each node and perform the following operations.

An OceanStor Pacific 9546 device has one or two nodes. You need to log in to the iBMC of each node and perform the following operations.

An OceanStor Pacific 9346 (One Node per Chassis, Two CPUs per Node) device has one node. You need to log in to the iBMC of the node and perform the following operations.

Step 2 Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 3 Open the virtual KVM interface, and enter user name **root** and its new password to log in to a node.

Step 4 Configure a temporary management IP address for a storage node.

To configure an IPv4 address, run the following commands:

- **ifconfig** *Management plane NIC name Temporary IPv4 address/Number of subnet mask bits* **up**
- **route add default gw** *Default gateway*

```
ifconfig enp125s0f4 192.168.40.15/24 up
route add default gw 192.168.40.1
```

NOTE

Management plane NIC name of OceanStor Pacific 9550/OceanStor Pacific 9350 is **enp125s0f4** or **enp125s0f5**.

Management plane NIC name of OceanStor Pacific 9950 is **enp125s0f2** or **enp125s0f3**.

Management plane NIC name of OceanStor Pacific 9546/OceanStor Pacific 9346 is **enp125s0f4**.

Step 5 Use PuTTY to log in to a storage node as user **fsadmin**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*.

Run the following command to switch to user **root**.

```
su - root
```

NOTE

If you log in as user **fsadmin** for the first time, change the default password.

 Copyright © Huawei Technologies Co., Ltd.

Step 6 Check whether the firmware and driver versions meet the requirements in *OceanStor Pacific Series 8.2.1 Version Mapping* by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*. If no, upgrade the firmware and driver versions to the target versions.

----End

?.5. Checking the Hi1822V120 NIC Mode

Context

This section describes how to check whether the Hi1822V120 NIC mode is Open vSwitch (OVS), and how to switch the NIC mode if it is not OVS.

Prerequisites

This operation applies only to OceanStor Pacific 9546 and OceanStor Pacific 9346.

Procedure

Step 1 Use a remote connection tool to log in to the system and switch to user **root**.

Step 2 Disable the intrusion detection service to prevent a false positive. If the OS does not support this service, skip this step.

```
Euler:~ # systemctl stop secAgent
```

Step 3 Run the following command to check the Hi1822V120 NIC mode.

```
Euler:~ # hinicadm3 info
Card num:2
Device Information:
    Card        PCIe Function
|----hinic0(CAL_4X25G)
        |--------0000:87:00.0(NIC:enp135s0f0)
        |--------0000:87:00.1(NIC:enp135s0f1)
        |--------0000:87:00.2(NIC:enp135s0f2)
        |--------0000:87:00.3(NIC:enp135s0f3)
        |--------0000:87:00.4(NIC:enp135s0f4)
        |--------0000:87:00.5(NIC:enp135s0f5)
|----hinic1(CAL_4X25G)
        |--------0000:01:00.0(NIC:enp1s0f0)
        |--------0000:01:00.1(NIC:enp1s0f1)
        |--------0000:01:00.2(NIC:enp1s0f2)
        |--------0000:01:00.3(NIC:enp1s0f3)
```

If one NIC in the command output contains six NIC records (the NIC information is displayed below **|----hinic*x*(CAL_4X25G)**), the server has NICs in OVS mode. In this case, you do not need to switch the NIC mode. Otherwise, go to **Step 4** to switch the NIC mode.

Step 4 Switch the NIC mode to OVS. For details, see **Installing/Upgrading the Firmware and Drivers (Function Manual)** > **Installing/Upgrading Firmware and Drivers for OceanStor Pacific 9546, 9346, and 9146** > **Installing/Upgrading the Hi1822V120 NIC Firmware and Driver** > **Switching the NIC Mode (Applicable to SFS Scenarios)** in *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*. In NIC mode switching command **./appctl switch_mode -slot** *slotid* **-type** *mode*, the value of *mode* is **ovs**. For details about the value of *slotid*, see **Table 5-9**.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-9 slotid in the device service network

Device Name	slotid in the Service Network
OceanStor Pacific 9546	all
OceanStor Pacific 9346	2

----End

5.4.1.6.2.3 OceanStor Pacific 9540 Kunpeng-based Without a RAID Controller Card, 9520 Kunpeng-based Without a RAID Controller Card, 9920 Kunpeng-based Without a RAID Controller Card, and 9340 Kunpeng-based Without a RAID Controller Card

?.1. OceanStor Pacific 9520 Kunpeng-based 14-Slot Without a RAID Controller Card and 9920 Kunpeng-based (Palm-sized NVMe SSD) Without a RAID Controller Card

?.1. Checking the Node Firmware Version

Procedure

Step 1 Log in to the iBMC system.

Enter the new iBMC IP address in the address box of a browser and enter the user name and password to log in to the iBMC system of a node. The default user name is **Administrator**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

- **https://***iBMC IPv4 address*
- **https://[***iBMC IPv6 address***]**

Step 2 Choose **System** > **System Info** > **Product Info** > **Mainboard Info**.

Step 3 Check whether **iBMC Firmware Version**, **CPLD Version**, and **BIOS Version** meet the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

If the requirements are not met, upgrade the firmware to the target version by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*.

----End

?.2. Checking the OS Version

Procedure

Step 1 Log in to the iBMC system.

Step 2 Go to the **Home** page of iBMC. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Enter user name **root** and its password to log in to the OS of a storage node. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

Step 4 Run the following command to check whether the OS version meets the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

```
cat /proc/version
```

- If the requirements are met, go to **Checking BIOS Settings**.
- If the requirements are not met, perform the following operations in sequence:
  a. Set BIOS parameters by referring to **5.5.5.2.1 Configuring BIOS (Applicable to OceanStor Pacific 9520 Kunpeng-based 14-Slot and 9920 Kunpeng-based (Palm-sized NVMe SSD))**.
  b. Install an OS that meets the requirements by referring to **5.5.6.2.1 Installing an OS (Applicable to OceanStor Pacific 9520 Kunpeng-based 14-Slot Without a RAID Controller Card and 9920 Kunpeng-based (Palm-sized NVMe SSD) Without a RAID Controller Card)**.
  c. Upgrade the NIC and disk firmware and drivers by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*.
  d. Configure networks by referring to **5.4.1.6.3 Configuring the Management Network of a Node**.

----End

?.3. Checking BIOS Settings

Procedure

Step 1 Log in to the iBMC system.

Step 2 Choose **iBMC Settings** > **Configuration Update** > **Export Configuration**.

Step 3 Click **Export**.

Step 4 Check the following information in the exported configuration file:

- Check whether the value of **OneNumaEnable** is **Enabled**.
- For OceanStor Pacific 9520 Kunpeng-based 14-slot, check whether the value of **BbuNvSize** is **16G**.
- For OceanStor Pacific 9920 Kunpeng-based (palm-sized NVMe SSD), check whether the value of **BbuNvSize** is **32G**.
- Check whether the value of **BbuUceEnhance** is **Enable**.
- Check whether the value of **BbuBackForCpuOff** is **Enabled**.

NOTICE

Ensure that the value of **OneNumaEnable** in the configuration file is the same as the preceding value.

If the queried values are different from the preceding values, set the parameters by referring to **5.5.5.2.1 Configuring BIOS (Applicable to OceanStor Pacific**

 Copyright © Huawei Technologies Co., Ltd.

9520 Kunpeng-based 14-Slot and 9920 Kunpeng-based (Palm-sized NVMe SSD)).

----End

?.4. Checking the Device Firmware and Driver Versions

Procedure

Step 1 Log in to the iBMC system.

Step 2 Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 3 Enter user name **root** and its new password to log in to a node.

Step 4 Configure a temporary management IP address for a storage node.

To configure an IPv4 address, run the following commands:

- **ifconfig** *Management plane NIC name Temporary IPv4 address/Number of subnet mask bits* **up**
- **route add default gw** *Default gateway*

```
ifconfig enp125s0f0 192.168.40.15/24 up
route add default gw 192.168.40.1
```

To configure an IPv6 address, run the following commands:

- **ifconfig** *Management plane NIC name* **add** *Temporary IPv6 address/Prefix* **up**
- **route -A inet6 add default gw** *Default gateway*

```
ifconfig enp2s0f0:3 add FC00::102/64 up
route -A inet6 add default gw FC00::101
```

Step 5 Use PuTTY to log in to a storage node as user **fsadmin**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*.

Run the following command to switch to user **root**.

```
su - root
```

NOTE

If you log in as user **fsadmin** for the first time, change the default password.

Step 6 Check whether the firmware and driver versions meet the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping* by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*. If no, upgrade the firmware and driver versions to the target versions.

----End

?.2. Other Kunpeng-based Models Without a RAID Controller Card

 Copyright © Huawei Technologies Co., Ltd.

?.1. Checking the Node Firmware Version

Procedure

Step 1 Log in to the iBMC system.

Enter the new iBMC IP address in the address box of a browser and enter the user name and password to log in to the iBMC system of a node. The default user name is **Administrator**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

- **https://***iBMC IPv4 address*
- **https://[***iBMC IPv6 address***]**

Step 2 Choose **System** > **System Info** > **Product Info** > **Mainboard Info**.

Step 3 Check whether **iBMC Firmware Version**, **CPLD Version**, and **BIOS Version** meet the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

If the requirements are not met, upgrade the firmware to the target version by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*.

----End

?.2. Checking the OS Version

Procedure

Step 1 Go to the **Home** page of iBMC. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 2 Open the virtual KVM interface, and enter user name **root** to log in to the OS of the storage node. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

Step 3 Run the following command to check whether the OS version meets the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

```
cat /proc/version
```

- If the requirements are met, perform the following operations in sequence:
  a. Check the **cloud_vpc.ini** file by referring to **5.5.3 Checking the cloud_vpc.ini File**.
  b. Go to **Checking BIOS Settings**.
- If the requirements are not met, perform the following operations in sequence:
  a. Set BIOS parameters by referring to **5.5.5.2.2 Configuring BIOS (Applicable to Other Kunpeng-based Devices)**.
  b. Install an OS that meets the requirements by referring to **5.5.6.2.2 Installing an OS (Applicable to Other Kunpeng-based Models Without a RAID Controller Card)**.
  c. Upgrade the ES3000 and NIC tools, drivers, and firmware by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*.

 Copyright © Huawei Technologies Co., Ltd.

d. Check the Hi1822V120 NIC mode by referring to **Checking the Hi1822V120 NIC Mode**.

e. Check the compatibility of the disk backplane by referring to **Checking the Compatibility of a Disk Backplane**.

f. Check the **cloud_vpc.ini** file by referring to **5.5.3 Checking the cloud_vpc.ini File**.

g. Configure networks by referring to **5.4.1.6.3 Configuring the Management Network of a Node**.

----End

?.3. Checking BIOS Settings

Procedure

Step 1 Log in to the iBMC system.

Step 2 Choose **iBMC Settings** > **Configuration Update** > **Export Configuration** or **Configuration** > **Import/Export**.

Step 3 Click **Export**.

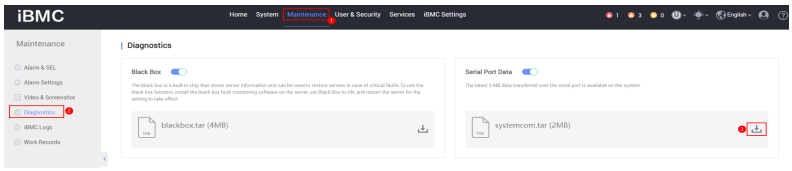
Step 4 Query the following information in the exported configuration file:

- Check whether the value of **EnableSMMU** (corresponding to **Support Smmu** in the BIOS) is **Disabled**.
- Check whether the value of **DieInterleaving** is **Enabled**.
- Check whether the value of **NUMAEn** (corresponding to **NUMA** in the BIOS) is **Enabled**.
- Check whether the value of **OneNumaEnable** (corresponding to **One Numa Per Socket** in the BIOS) is **Enabled**.
- Check whether the value of **ColdBootFastSupport** is **Disabled**.
- Check whether the value of **BbuNvSize** is **16G**.
- Check whether the value of **X8MisCorrEn** (corresponding to **AB Check** in the BIOS) is **Enabled**.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

- Ensure that the values of **NUMAEn** and **OneNumaEnable** in the configuration file are the same as the preceding values.
- If a device uses a 32-core CPU, you do not need to check **OneNumaEnable**. To query the number of CPU cores, log in to the iBMC WebUI and choose **System** > **System Info** > **Processors** > **Cores/Threads**.
- **X8MisCorrEn** (corresponding to **AB Check** in the BIOS) applies to the following BIOS versions of Kunpeng 920-based nodes:
  - BIOS 1.91 or later for the 1620 VD 1.5 mainboard
  - BIOS 5.21 or later for the 1620S VE 2.0/V150 mainboard
- The default value of **SecureBoot** in the BIOS is **Disable**. To avoid installation problems, you are advised to check whether the value is **Disable**. The check methods are as follows:
  - Log in to the iBMC WebUI, choose **Maintenance** > **Diagnostics**, download the **systemcom.tar** file, view the file content, search for **SecureBoot CurrentValue**, and check whether the value of **SecureBoot CurrentValue** is **0**.



  - Check the BIOS. For details, see the step describing how to modify secure boot in **5.5.5.2.2 Configuring BIOS (Applicable to Other Kunpeng-based Devices)**.

If the queried values are different from the preceding values, set the parameters by referring to **5.5.5.2.2 Configuring BIOS (Applicable to Other Kunpeng-based Devices)**.

----End

?.4. Checking the Device Firmware and Driver Versions

Procedure

Step 1 Log in to the iBMC system.

Step 2 Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 3 Enter user name **root** and its new password to log in to a node.

Step 4 Configure a temporary management IP address for a storage node.

To configure an IPv4 address, run the following commands:

- **ifconfig** *Management plane NIC name Temporary IPv4 address/Number of subnet mask bits* **up**
- **route add default gw** *Default gateway*

 Copyright © Huawei Technologies Co., Ltd.

```
ifconfig enp125s0f0 192.168.40.15/24 up
route add default gw 192.168.40.1
```

To configure an IPv6 address, run the following commands:

- **ifconfig** *Management plane NIC name* **add** *Temporary IPv6 address/Prefix* **up**
- **route -A inet6 add default gw** *Default gateway*

```
ifconfig enp2s0f0:3 add FC00::102/64 up
route -A inet6 add default gw FC00::101
```

Step 5 Use PuTTY to log in to a storage node as user **fsadmin**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*.

Run the following command to switch to user **root**.

```
su - root
```

NOTE

If you log in as user **fsadmin** for the first time, change the default password.

Step 6 Check whether the firmware and driver versions meet the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping* by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*. If no, upgrade the firmware and driver versions to the target versions.

----End

?.5. Checking the Hi1822V120 NIC Mode

Context

This section describes how to check whether the Hi1822V120 NIC mode is Open vSwitch (OVS), and how to switch the NIC mode if it is not OVS.

Prerequisites

This operation applies only to OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9920 Kunpeng-based, OceanStor Pacific 9340 Kunpeng-based, and OceanStor Pacific 9520 Kunpeng-based.

Procedure

Step 1 Use a remote connection tool to log in to the system and switch to user **root**.

Step 2 Disable the intrusion detection service to prevent a false positive. If the OS does not support this service, skip this step.

```
Euler:~ # systemctl stop secAgent
```

Step 3 Run the following command to check the Hi1822V120 NIC mode.

```
Euler:~ # hinicadm3 info
Card num:2
Device Information:
    Card        PCIe Function
|----hinic0(CAL_4X25G)
       |--------0000:87:00.0(NIC:enp135s0f0)
       |--------0000:87:00.1(NIC:enp135s0f1)
       |--------0000:87:00.2(NIC:enp135s0f2)
       |--------0000:87:00.3(NIC:enp135s0f3)
```

 Copyright © Huawei Technologies Co., Ltd.

```
        |--------0000:87:00.4(NIC:enp135s0f4)
        |--------0000:87:00.5(NIC:enp135s0f5)
|----hinic1(CAL_4X25G)
        |--------0000:01:00.0(NIC:enp1s0f0)
        |--------0000:01:00.1(NIC:enp1s0f1)
        |--------0000:01:00.2(NIC:enp1s0f2)
        |--------0000:01:00.3(NIC:enp1s0f3)
```

If one NIC in the command output contains six NIC records (the NIC information is displayed below **|----hinic*x*(CAL_4X25G)**), the server has NICs in OVS mode. In this case, you do not need to switch the NIC mode. Otherwise, go to **Step 4** to switch the NIC mode.

Step 4 Switch the NIC mode to OVS. For details, see **Installing/Upgrading the Firmware and Drivers (Function Manual)** > **Installing/Upgrading Firmware and Drivers for OceanStor Pacific 9520, 9540, 9340, and 9920** > **Installing/Upgrading the Hi1822V120 NIC Firmware and Driver** > **Switching the NIC Mode (Applicable to SFS Scenarios)** in *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*. In NIC mode switching command **./appctl switch_mode -slot** *slotid* **-type** *mode*, the value of *mode* is **ovs**. For details about the value of *slotid*, see **Table 5-10**.

Table 5-10 slotid in the device service network

Device Name	slotid in the Service Network
OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9920 Kunpeng-based, or OceanStor Pacific 9340 Kunpeng-based	3
OceanStor Pacific 9520 Kunpeng-based	5

----End

?.6. Checking the Compatibility of a Disk Backplane

Procedure

Step 1 Query the model and version of a disk module.

1. Log in to the target node as user **fsadmin**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. Run the **su - root** command and enter the password of user **root** to switch to user **root**.
2. Run the **lsscsi -g** command to query the model and version of a disk module.

```
                    lsscsi -g
[0:0:42:0]   disk    ATA      WUS721010ALE6L4  W9C0  /dev/sda   /dev/sg0
[0:0:43:0]   disk    ATA      WUS721010ALE6L4  W950  /dev/sdb   /dev/sg1
[0:0:66:0]   enclosu HUAWEI   Expander 12Gx16  131   -          /dev/sg8
[0:2:0:0]    disk    AVAGO    HW-SAS3508       5.14  /dev/sdi   /dev/sg9
```

In the row containing **disk** of the command output, if the model is **HUS726T6TALE600** and the version is **T9***xx* (excluding T9C0) or if the model

 Copyright © Huawei Technologies Co., Ltd.

is **WUS721010ALE6L4** and the version is **W9***xx* (excluding W9C0), go to **Step 2**. Otherwise, there is no compatibility problem.

Step 2 Query the model of the disk backplane.

1. Log in to the iBMC WebUI page of the target node.
2. Choose **System** > **System Info** > **Others** > **Drive Backplanes**, and query **Board ID** of the disk backplane.

   NOTE

   If the iBMC versions are inconsistent, log in to the iBMC WebUI, choose **Information** > **System Info** > **Other Devices** > **Drive Backplanes**, and query **Board ID** of the disk backplane.

   - If the board ID is not **0x0073** or **0x0083**, there is no compatibility problem.
   - If the board ID is **0x0073**, go to **Step 3**.
   - If the board ID is **0x0083**, contact Huawei technical support engineers.

Step 3 Query the firmware version of the spare disk backplane.

Log in to the target node as user **fsadmin**. Run the **su - root** command and enter the password of user **root** to switch to user **root**. Run the **lsscsi -g** command to query the firmware version of the disk backplane.

```
[root@localhost ~]# lsscsi -g
[0:0:5:0]    disk    ATA      HUH721010ALE600  T3X6  /dev/sda   /dev/sg0
[0:0:6:0]    disk    ATA      HUH721010ALE600  T3X6  /dev/sdb   /dev/sg1
[0:0:8:0]    disk    ATA      HUH721010ALE600  T3X6  /dev/sdc   /dev/sg2
[0:0:17:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdd   /dev/sg3
[0:0:18:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sde   /dev/sg4
[0:0:25:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdf   /dev/sg5
[0:0:42:0]   disk    ATA      MG06ACA10TE      0808  /dev/sdg   /dev/sg6
[0:0:44:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdh   /dev/sg7
[0:0:45:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdi   /dev/sg8
[0:0:48:0]   disk    ATA      HUH721010ALN600  T2JC  /dev/sdj   /dev/sg9
[0:0:51:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdk   /dev/sg10
[0:0:55:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdl   /dev/sg11
[0:0:65:0]   enclosu HUAWEI   Expander 12Gx16  331   -          /dev/sg12
[0:2:0:0]    disk    AVAGO    HW-SAS3408       5.03  /dev/sdm   /dev/sg13
```

- If the version in the **enclosu** row in the command output is **331**, there is no compatibility problem.
- If the version in the **enclosu** row in the command output is not **331**, contact Huawei technical support engineers.

----End

5.4.1.6.2.4 OceanStor Pacific 9540 Kunpeng-based with a RAID Controller Card, 9520 Kunpeng-based with a RAID Controller Card, and 9340 Kunpeng-based with a RAID Controller Card

 Copyright © Huawei Technologies Co., Ltd.

?.1. Checking the Node Firmware Version

Procedure

Step 1 Log in to the iBMC system.

Enter the new iBMC IP address in the address box of a browser and enter the user name and password to log in to the iBMC system of a node. The default user name is **Administrator**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

- **https://***iBMC IPv4 address*
- **https://[***iBMC IPv6 address***]**

Step 2 Choose **System** > **System Info** > **Product Info** > **Mainboard Info**.

Step 3 Check whether **iBMC Firmware Version**, **CPLD Version**, and **BIOS Version** meet the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

If the requirements are not met, upgrade the firmware to the target version by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*.

----End

?.2. Checking the OS Version

Procedure

Step 1 Log in to the iBMC system.

Step 2 Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 3 Enter user name **root** and its password to log in to the OS of a storage node. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

Step 4 Run the following command to check whether the OS version meets the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

```
cat /proc/version
```

- If the requirements are met, go to **Checking the Cache Policy of a System Disk**.
- If the requirements are not met, perform the following operations in sequence:
  a. Enable the JBOD function by referring to **5.5.4 Enabling JBOD (Applicable to OceanStor Pacific 9540 Kunpeng-based, 9520 Kunpeng-based, 9920 Kunpeng-based, and 9340 Kunpeng-based)**.
  b. Set BIOS parameters by referring to **5.5.5.2.2 Configuring BIOS (Applicable to Other Kunpeng-based Devices)**.
  c. Install an OS that meets the requirements by referring to **5.5.6.3 Installing an OS (Applicable to OceanStor Pacific 9520 Kunpeng-**

 Copyright © Huawei Technologies Co., Ltd.

based with a RAID Controller Card, 9540 Kunpeng-based with a RAID Controller Card, 9920 Kunpeng-based with a RAID Controller Card, and 9340 Kunpeng-based with a RAID Controller Card)**.

d. Install the ES3000, NIC, and RAID controller card tools, drivers, and firmware by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*.

e. Check the compatibility of the disk backplane by referring to **Checking the Compatibility of a Disk Backplane**.

f. Configure networks by referring to **5.4.1.6.3 Configuring the Management Network of a Node**.

----End

?.3. Checking the Cache Policy of a System Disk

Context

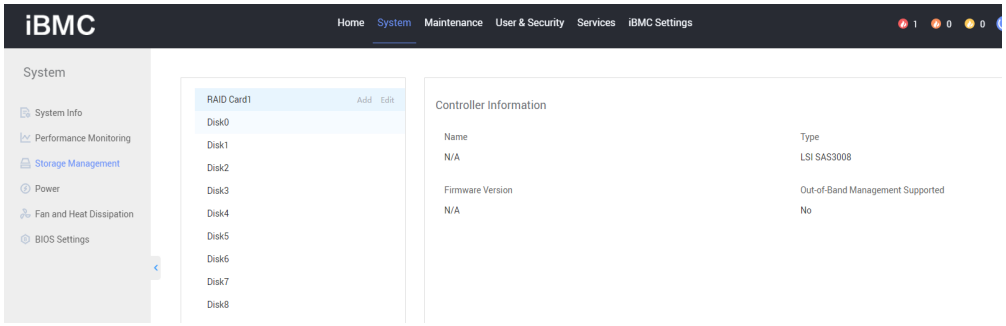
If the RAID controller card configured on the node is not LSI SAS3008IR, you need to manually disable the system disk cache policy to prevent file system damage caused by node restart or unexpected power-off.

Procedure

Step 1 Log in to the iBMC system.

Step 2 Check the model of the RAID controller card which has been installed.

Choose **System** > **Storage Management**, select the desired RAID controller card or PCIe card, and view the **Type** information in the right pane.



- If the type is LSI SAS3008IR, no further action is required.

  NOTE

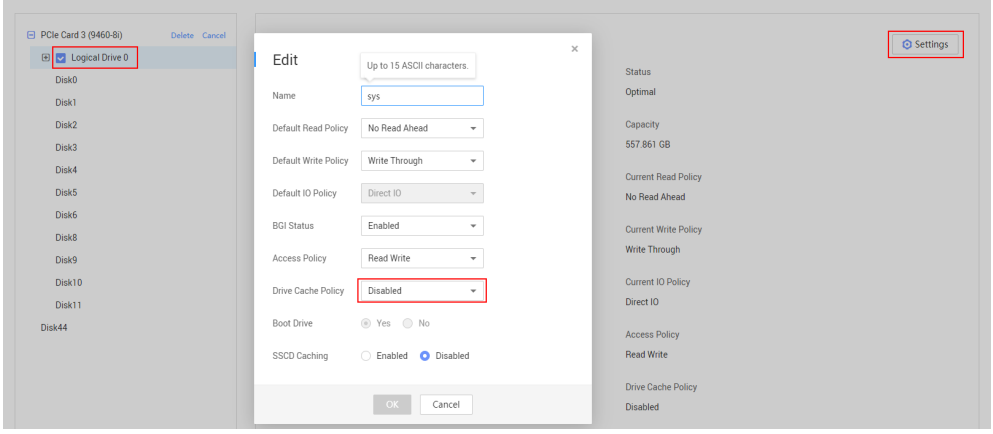
  For the LSI SAS3008IR RAID controller card, the system disk cache policy is disabled by default. Therefore, you do not need to perform the following operations.

- If the type is not LSI SAS3008IR, go to **Step 3**.

Step 3 Disable the cache policy of a system disk.

- When the RAID controller card type is not SP686C-M-16i or SP686C-M-40i, select the system disk to be modified, click **Settings**, and set **Drive Cache Policy** to **Disabled**.

 Copyright © Huawei Technologies Co., Ltd.



- When the RAID controller card type is SP686C-M-16i or SP686C-M-40i:

  a. Log in to the storage node as user **fsadmin**. Run the following command and enter the password of user **root** to switch to user **root**.
  su - root

  b. Run the following command to query *controller_id*.
  /usr/bin/hiraidadm show allctrl

  c. Run the following command to query *enc_id* and *slot_id*.
  /usr/bin/hiraidadm c*controller_id* **show pdlist**

  Check the values of **Enc** and **Slot** whose **Type** is **member**. **Enc** and **Slot** are *enc_id* and *slot_id*, respectively.

```
Index Enc  Slot DID  Intf  Media Type     Status         PreFail LinkSpd Capacity   SecType FUA SED Spin FW       Model
------------------------------------------------------------------------------------------------------------------------------
0     0    1    24   SATA  HDD   rawdrive online         No      6.0G    10.914TB  512E    Sup No  UP   LEBDT3P2 HGST HUH721212ALE600
1     0    2    25   SATA  HDD   rawdrive online         No      6.0G    10.914TB  512E    Sup No  UP   LEBDT3P2 HGST HUH721212ALE600
2     0    3    15   SATA  HDD   rawdrive online         No      6.0G    3.639TB   512N    Sup No  UP   T7R4     HUS726040ALA610
3     0    4    22   SATA  HDD   rawdrive online         No      6.0G    10.914TB  512E    Sup No  UP   LEBDT3P2 HGST HUH721212ALE600
4     0    5    14   SATA  HDD   rawdrive online         No      6.0G    3.639TB   512N    Sup No  UP   T7R4     HUS726040ALA610
5     0    6    1    SATA  HDD   rawdrive online         No      6.0G    3.639TB   512N    Sup No  UP   SN06     ST4000NM0033-9ZM170
6     0    7    2    SATA  HDD   rawdrive online         No      6.0G    3.639TB   512N    Sup No  UP   SN06     ST4000NM0033-9ZM170
7     0    8    3    SAS   SSD   rawdrive online         No      12G     2.911TB   512E    Sup No  UP   3253     HWE52SS33T2M002N
8     0    9    4    SAS   SSD   rawdrive online         No      12G     2.911TB   512E    Sup No  UP   3253     HWE52SS33T2M002N
9     0    10   5    SAS   SSD   rawdrive online         No      12G     2.911TB   512E    Sup No  UP   3253     HWE52SS33T2M002N
10    0    11   6    SAS   SSD   rawdrive online         No      12G     2.911TB   512E    Sup No  UP   3253     HWE52SS33T2M002N
11    0    12   0    SAS   HDD   member   online         No      12G     1.092TB   512N    Sup No  UP   N005     ST1200MM0009
12    0    13   19   SAS   HDD   member   online         No      12G     1.092TB   512N    Sup No  UP   N003     ST1200MM0009
------------------------------------------------------------------------------------------------------------------------------
[root@host184-210 ~]#
```

  d. Disable the pdcache function of the RAID controller card.

    i. Run the following command to query *vd_id*.
    /usr/bin/hiraidadm c*controller_id* **show vdlist**

```
[root@host184-210 network-scripts]# hiraidadm c0 show vdlist
================================== Hiraidadm   Information ==================================
    Name: hiraidadm
    Version :1.2.0.2
    Build Time:Aug 12 2022 05:51:03
==============================================================================================
==============================================================================================
    Status Code = 0
    Status = Success
    Description = None
==============================================================================================
Total vd number is 1
----------------------------------------------------------------------------------------------
VDID RGID Name     Type     Status         Capacity   SUSz   SecSz  RCache    WCache RealWCache
----------------------------------------------------------------------------------------------
0    0    system   normal   normal           1.091TB  256KB    512B No_Ahead WT     WT
----------------------------------------------------------------------------------------------
```

    In the command output, **VDID** is *vd_id*.

    ii. Run the following command to disable the pdcache function of the RAID controller card based on the obtained *vd_id*.
    /usr/bin/hiraidadm c*controller_id***:vd***vd_id* **set pdcache sw=off**

 Copyright © Huawei Technologies Co., Ltd.

```
[root@host184-210 ~]# hiraidadm c0:vd0 set pdcache sw=off
================================== Hiraidadm   Information ==================================
    Name: hiraidadm
    Version :1.2.0.2
    Build Time:Aug 12 2022 05:51:03
=============================================================================================
=============================================================================================
    Status Code = 0
    Status = Success
    Description = None
=============================================================================================
[root@host184-210 ~]#
```

iii. Run the following command to check whether the pdcache function of the RAID controller card is disabled.

/usr/bin/hiraidadm c*controller_id***:e***enc_id***:s***slot_id* **show pdcache**

```
[root@host184-210 ~]# hiraidadm c0:e0:s12 show pdcache
================================== Hiraidadm   Information ==================================
    Name: hiraidadm
    Version :1.2.0.2
    Build Time:Aug 12 2022 05:51:03
=============================================================================================
=============================================================================================
    Status Code = 0
    Status = Success
    Description = None
=============================================================================================
Drive Cache switch = Off
[root@host184-210 ~]#
```

----End

?.4. Checking the JBOD Function

To ensure that the disks on a node can be used properly, you need to configure the RAID controller cards to the RAID mode and enable the JBOD function when the node uses some RAID controller cards. For the RAID controller card models for which JBOD needs to be enabled, see **Huawei Storage Interoperability Navigator**.

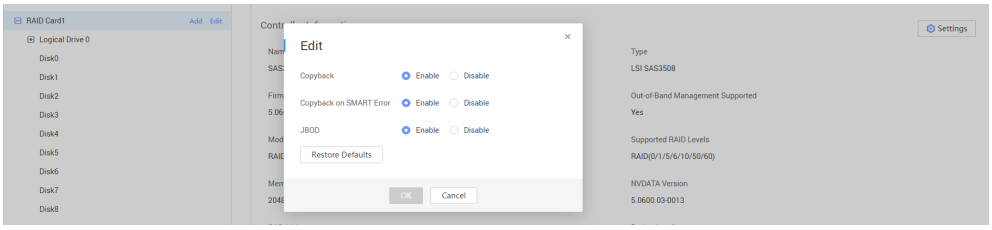
Procedure

Step 1 Log in to the iBMC system.

Step 2 Choose **System** > **Storage Management** and select the desired RAID controller card or PCIe card.

Step 3 Enable JBOD for the RAID controller card.

1. Click **Settings**.
2. Set **JBOD** to **Enable**.



----End

?.5. Checking BIOS Settings

Procedure

Step 1 Log in to the iBMC system.

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Choose **iBMC Settings** > **Configuration Update** > **Export Configuration** or **Configuration** > **Import/Export**.

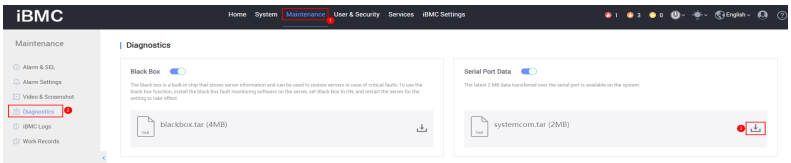
Step 3 Click **Export**.

Step 4 Query the following information in the exported configuration file:

- Check whether the value of **EnableSMMU** (corresponding to **Support Smmu** in the BIOS) is **Disabled**.
- Check whether the value of **DieInterleaving** is **Enabled**.
- Check whether the value of **NUMAEn** (corresponding to **NUMA** in the BIOS) is **Enabled**.
- Check whether the value of **ColdBootFastSupport** is **Disabled**.
- Check whether the value of **ExmbistSupport** (corresponding to **Exmbist Support** in the BIOS) is **Enable**.
- Check whether the value of **BbuNvSize** is **16G**.
- Check whether the value of **X8MisCorrEn** (corresponding to **AB Check** in the BIOS) is **Enabled**.
- Check whether the value of **AdvanceDeviceCorrection** (corresponding to **Advanced Device Correction** in the BIOS) is **SR**.

NOTICE

- Ensure that the value of **NUMAEn** in the configuration file is the same as the preceding value.
- **X8MisCorrEn** (corresponding to **AB Check** in the BIOS) applies to the following BIOS versions of Kunpeng 920-based nodes:
  - BIOS 1.91 or later for the 1620 VD 1.5 mainboard
  - BIOS 5.21 or later for the 1620S VE 2.0/V150 mainboard
- The default value of **SecureBoot** in the BIOS is **Disable**. To avoid installation problems, you are advised to check whether the value is **Disable**. The check methods are as follows:
  - Log in to the iBMC WebUI, choose **Maintenance** > **Diagnostics**, download the **systemcom.tar** file, view the file content, search for **SecureBoot CurrentValue**, and check whether the value of **SecureBoot CurrentValue** is **0**.



  - Check the BIOS. For details, see the step describing how to modify secure boot in **5.5.5.2.2 Configuring BIOS (Applicable to Other Kunpeng-based Devices)**.

If the queried values are different from the preceding values, set the parameters by referring to **5.5.5.2.2 Configuring BIOS (Applicable to Other Kunpeng-based Devices)**.

----End

 Copyright © Huawei Technologies Co., Ltd.

?.6. Checking the Device Firmware and Driver Versions

Procedure

Step 1 Log in to the iBMC system.

Step 2 Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 3 Enter user name **root** and its new password to log in to a node.

Step 4 Configure a temporary management IP address for a storage node.

To configure an IPv4 address, run the following commands:

- **ifconfig** *Management plane NIC name Temporary IPv4 address/Number of subnet mask bits* **up**
- **route add default gw** *Default gateway*

```
ifconfig enp125s0f0 192.168.40.15/24 up
route add default gw 192.168.40.1
```

To configure an IPv6 address, run the following commands:

- **ifconfig** *Management plane NIC name* **add** *Temporary IPv6 address/Prefix* **up**
- **route -A inet6 add default gw** *Default gateway*

```
ifconfig enp2s0f0:3 add FC00::102/64 up
route -A inet6 add default gw FC00::101
```

Step 5 Use PuTTY to log in to a storage node as user **fsadmin**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*.

Run the following command to switch to user **root**.

```
su - root
```

NOTE

If you log in as user **fsadmin** for the first time, change the default password.

Step 6 Check whether the firmware and driver versions meet the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping* by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*. If no, upgrade the firmware and driver versions to the target versions.

----End

?.7. Checking the Hi1822V120 NIC Mode

Context

This section describes how to check whether the Hi1822V120 NIC mode is Open vSwitch (OVS), and how to switch the NIC mode if it is not OVS.

Prerequisites

This operation applies only to OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9920 Kunpeng-based, OceanStor Pacific 9340 Kunpeng-based, and OceanStor Pacific 9520 Kunpeng-based.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Use a remote connection tool to log in to the system and switch to user **root**.

Step 2 Disable the intrusion detection service to prevent a false positive. If the OS does not support this service, skip this step.

```
Euler:~ # systemctl stop secAgent
```

Step 3 Run the following command to check the Hi1822V120 NIC mode.

```
Euler:~ # hinicadm3 info
Card num:2
Device Information:
    Card        PCIe Function
|----hinic0(CAL_4X25G)
        |--------0000:87:00.0(NIC:enp135s0f0)
        |--------0000:87:00.1(NIC:enp135s0f1)
        |--------0000:87:00.2(NIC:enp135s0f2)
        |--------0000:87:00.3(NIC:enp135s0f3)
        |--------0000:87:00.4(NIC:enp135s0f4)
        |--------0000:87:00.5(NIC:enp135s0f5)
|----hinic1(CAL_4X25G)
        |--------0000:01:00.0(NIC:enp1s0f0)
        |--------0000:01:00.1(NIC:enp1s0f1)
        |--------0000:01:00.2(NIC:enp1s0f2)
        |--------0000:01:00.3(NIC:enp1s0f3)
```

If one NIC in the command output contains six NIC records (the NIC information is displayed below **|----hinic*x*(CAL_4X25G)**), the server has NICs in OVS mode. In this case, you do not need to switch the NIC mode. Otherwise, go to **Step 4** to switch the NIC mode.

Step 4 Switch the NIC mode to OVS. For details, see **Installing/Upgrading the Firmware and Drivers (Function Manual)** > **Installing/Upgrading Firmware and Drivers for OceanStor Pacific 9520, 9540, 9340, and 9920** > **Installing/Upgrading the Hi1822V120 NIC Firmware and Driver** > **Switching the NIC Mode (Applicable to SFS Scenarios)** in *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*. In NIC mode switching command **./appctl switch_mode -slot** *slotid* **-type** *mode*, the value of *mode* is **ovs**. For details about the value of *slotid*, see **Table 5-11**.

Table 5-11 slotid in the device service network

Device Name	slotid in the Service Network
OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9920 Kunpeng-based, or OceanStor Pacific 9340 Kunpeng-based	3
OceanStor Pacific 9520 Kunpeng-based	5

----End

 Copyright © Huawei Technologies Co., Ltd.

?.8. Checking the Compatibility of a Disk Backplane

Procedure

Step 1 Query the model and version of a disk module.

1. Log in to the target node as user **fsadmin**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. Run the **su - root** command and enter the password of user **root** to switch to user **root**.
2. Run the **lsscsi -g** command to query the model and version of a disk module.

```
                        lsscsi -g
[0:0:42:0]   disk    ATA      WUS721010ALE6L4  W9C0  /dev/sda   /dev/sg0
[0:0:43:0]   disk    ATA      WUS721010ALE6L4  W950  /dev/sdb   /dev/sg1
[0:0:66:0]   enclosu HUAWEI   Expander 12Gx16  131   -          /dev/sg8
[0:2:0:0]    disk    AVAGO    HW-SAS3508       5.14  /dev/sdi   /dev/sg9
```

In the row containing **disk** of the command output, if the model is **HUS726T6TALE600** and the version is **T9***xx* (excluding T9C0) or if the model is **WUS721010ALE6L4** and the version is **W9***xx* (excluding W9C0), go to **Step 2**. Otherwise, there is no compatibility problem.

Step 2 Query the model of the disk backplane.

1. Log in to the iBMC WebUI page of the target node.
2. Choose **System** > **System Info** > **Others** > **Drive Backplanes**, and query **Board ID** of the disk backplane.

   NOTE

   If the iBMC versions are inconsistent, log in to the iBMC WebUI, choose **Information** > **System Info** > **Other Devices** > **Drive Backplanes**, and query **Board ID** of the disk backplane.

   - If the board ID is not **0x0073** or **0x0083**, there is no compatibility problem.
   - If the board ID is **0x0073**, go to **Step 3**.
   - If the board ID is **0x0083**, contact Huawei technical support engineers.

Step 3 Query the firmware version of the spare disk backplane.

Log in to the target node as user **fsadmin**. Run the **su - root** command and enter the password of user **root** to switch to user **root**. Run the **lsscsi -g** command to query the firmware version of the disk backplane.

```
[root@localhost ~]# lsscsi -g
[0:0:5:0]    disk    ATA      HUH721010ALE600  T3X6  /dev/sda   /dev/sg0
[0:0:6:0]    disk    ATA      HUH721010ALE600  T3X6  /dev/sdb   /dev/sg1
[0:0:8:0]    disk    ATA      HUH721010ALE600  T3X6  /dev/sdc   /dev/sg2
[0:0:17:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdd   /dev/sg3
[0:0:18:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sde   /dev/sg4
[0:0:25:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdf   /dev/sg5
[0:0:42:0]   disk    ATA      MG06ACA10TE      0808  /dev/sdg   /dev/sg6
[0:0:44:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdh   /dev/sg7
[0:0:45:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdi   /dev/sg8
[0:0:48:0]   disk    ATA      HUH721010ALN600  T2JC  /dev/sdj   /dev/sg9
[0:0:51:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdk   /dev/sg10
[0:0:55:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdl   /dev/sg11
[0:0:65:0]   enclosu HUAWEI   Expander 12Gx16  331   -          /dev/sg12
[0:2:0:0]    disk    AVAGO    HW-SAS3408       5.03  /dev/sdm   /dev/sg13
```

 Copyright © Huawei Technologies Co., Ltd.

- If the version in the **enclosu** row in the command output is **331**, there is no compatibility problem.
- If the version in the **enclosu** row in the command output is not **331**, contact Huawei technical support engineers.

----End

5.4.1.6.3 Configuring the Management Network of a Node

5.4.1.6.3.1 Configuration Requirements

- Before installing OceanStor Pacific series software, you need to modify the network port configuration file to configure management IP addresses for all management and storage nodes.
- The management network of the management nodes consists of external and internal management networks. The storage nodes that are deployed separately from the management nodes use only one management network (sharing the internal management network of the management nodes). You can configure external management IP addresses by referring to the steps in this section. Because the internal management network and storage network share network ports and IP addresses, you can configure internal management IP addresses by referring to the storage network configuration procedure.
- This section provides four configuration methods. Select one of the methods based on the actual service scenario.

5.4.1.6.3.2 Configuring a Physical Port IP Address

Context

The description in the following operations is only an example. The actual network port name information prevails.

Procedure

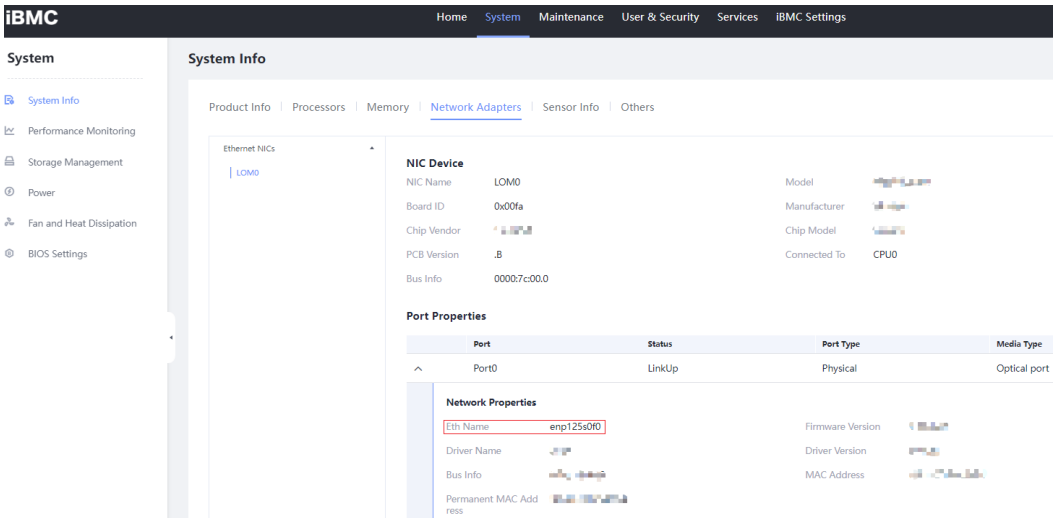
Step 1 Check the name of the network port corresponding to a NIC.

Log in to the iBMC system of a node, choose **System** > **System Info** > **Network Adapters** or **System** > **System Info** > **NICs**, select the corresponding NIC and port, and view the network port name. An example is provided as follows:

NOTE

If **Eth Name** cannot be queried on this page, you need to install the iBMA component. For details, see **5.5.20 Installing the iBMA Component**.

 Copyright © Huawei Technologies Co., Ltd.



Step 2 Use a remote connection tool to log in to the node as user **fsadmin** through the temporary management IP address. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. After the password is changed, log in to the node again.

Step 3 Run the following command to switch to user **root**.

```
su - root
```

Step 4 Go to the path for storing the network port configuration file.

```
cd /etc/sysconfig/network-scripts
```

Step 5 Run the following command to edit the network port configuration file. If the network port configuration file does not exist in the current path, you can run the following command to create and edit the network port configuration file.

```
vi ifcfg-Network port name
```

For details about the configuration file, see **Table 5-12**.

NOTE

In the following example, the management network uses physical network port enp125s0f0. You need to configure the **ifcfg-enp125s0f0** network port configuration file for each node.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-12 Network port configuration file information

Name	Content
ifcfg-*enp125s0f0*	DEVICE=*enp125s0f0* BOOTPROTO=static ONBOOT=yes STARTMODE=onboot IPv4 configuration: IPADDR=*IPv4 address* NETMASK=*subnet mask* DEFROUTE=yes NETWORKING=yes GATEWAY=*Management network gateway* **NOTE** • The external management network cannot use the same subnet as the storage network (the internal management network and storage network share the same IP address), control network, or service network. • A gateway must be configured for the external management network. The gateway must be the same as the default node gateway. IPV6_AUTOCONF=no NM_CONTROLLED=no

Step 6 After editing the configuration file, press **Esc** and enter **:wq** to save the settings and exit.

Step 7 Modify the permission on the network port configuration file.

```
chmod 644 /etc/sysconfig/network-scripts/ifcfg-Network port name
chown -h root:root /etc/sysconfig/network-scripts/ifcfg-Network port name
```

NOTE

All network port configuration files need to be modified.

Step 8 Run the following command to restart the network service:

```
service network restart
```

NOTE

After restarting the network service, you are advised to wait for 2 to 3 minutes to ensure that the network communication is recovered.

Step 9 Repeat **Step 1** to **Step 8** to configure the management IP addresses and gateways for all nodes.

Step 10 After the configuration is complete, ping the management IP addresses of other nodes on one node to check whether the management network communication between nodes is normal.

----End

5.4.1.6.3.3 Configuring a Bond Port IP Address

Context

The description in the following operations is only an example. The actual port information prevails.

 Copyright © Huawei Technologies Co., Ltd.

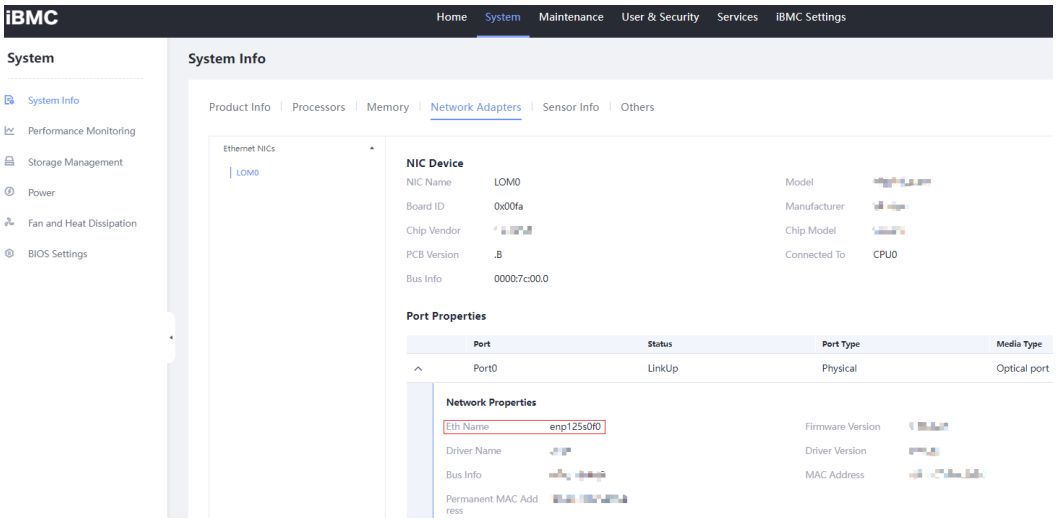
Procedure

Step 1 Check the name of the network port corresponding to a NIC.

Log in to the iBMC system of a node, choose **System** > **System Info** > **Network Adapters** or **System** > **System Info** > **NICs**, select the corresponding NIC and port, and view the network port name. An example is provided as follows:

NOTE

If **Eth Name** cannot be queried on this page, you need to install the iBMA component. For details, see **5.5.20 Installing the iBMA Component**.



Step 2 Use a remote connection tool to log in to the node as user **fsadmin** through the temporary management IP address. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. After the password is changed, log in to the node again.

Step 3 Run the following command to switch to user **root**.

```
su - root
```

Step 4 Go to the path for storing the network port configuration file.

```
cd /etc/sysconfig/network-scripts
```

Step 5 Run the following command to edit the network port configuration file. If the network port configuration file does not exist in the current path, you can run the following command to create and edit the network port configuration file.

```
vi ifcfg-Network port name
```

For details about the configuration file, see **Table 5-13**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

In the following example, the management network uses physical network ports enp125s0f0 and enp125s0f1. You need to configure the following network port configuration files for each node:

- **ifcfg-enp125s0f0**: configuration file of physical network port enp125s0f0
- **ifcfg-enp125s0f1**: configuration file of physical network port enp125s0f1
- **ifcfg-fsb_bond**: configuration file of the bond port corresponding to the two physical network ports

Table 5-13 Network port configuration file information

Name	Content
ifcfg-*enp125s0f0*	DEVICE=*enp125s0f0* BOOTPROTO=none ONBOOT=yes MASTER=*fsb_bond* SLAVE=yes USERCTL=no NM_CONTROLLED=no
ifcfg-*enp125s0f1*	DEVICE=*enp125s0f1* BOOTPROTO=none ONBOOT=yes MASTER=*fsb_bond* SLAVE=yes USERCTL=no NM_CONTROLLED=no

 Copyright © Huawei Technologies Co., Ltd.

Name	Content
ifcfg-*fsb_bond*	DEVICE=*fsb_bond* • IPv4 configuration: IPADDR=*IPv4 address* NETMASK=*subnet mask* DEFROUTE=yes NETWORKING=yes GATEWAY=*Management network gateway* **NOTE** • The external management network cannot use the same subnet as the storage network (the internal management network and storage network share the same IP address), control network, or service network. • A gateway must be configured for the external management network. The gateway must be the same as the default node gateway. IPV6_AUTOCONF=no ONBOOT=yes BOOTPROTO=static USERCTL=no TYPE=Bonding MTU=1500 NM_CONTROLLED=no BONDING_OPTS='mode=1 miimon=100' **NOTE** Configuration description of **BONDING_OPTS**: • The bond1 mode is recommended and the configuration is as follows: BONDING_OPTS='mode=1 miimon=100' • If the bond2 mode is used, the configuration is as follows: BONDING_OPTS='mode=2 miimon=100 xmit_hash_policy=layer3+4' • If the bond4 mode is used, the configuration is as follows: BONDING_OPTS='mode=4 miimon=100 lacp_rate=fast xmit_hash_policy=layer3+4'

Step 6 After editing the configuration file, press **Esc** and enter **:wq** to save the settings and exit.

Step 7 Modify the permission on the network port configuration file.

```
chmod 644 /etc/sysconfig/network-scripts/ifcfg-Network port name
chown -h root:root /etc/sysconfig/network-scripts/ifcfg-Network port name
```

NOTE

All network port configuration files need to be modified.

Step 8 Run the following command to restart the network service:

```
service network restart
```

NOTE

After restarting the network service, you are advised to wait for 2 to 3 minutes to ensure that the network communication is recovered.

Step 9 Repeat **Step 1** to **Step 8** to configure the management IP addresses and gateways for all nodes.

 Copyright © Huawei Technologies Co., Ltd.

Step 10 After the configuration is complete, ping the management IP addresses of other nodes on one node to check whether the management network communication between nodes is normal.

----End

5.4.1.6.3.4 Configuring a Physical Port IP Address and a VLAN

Context

The description in the following operations is only an example. The actual port information prevails.

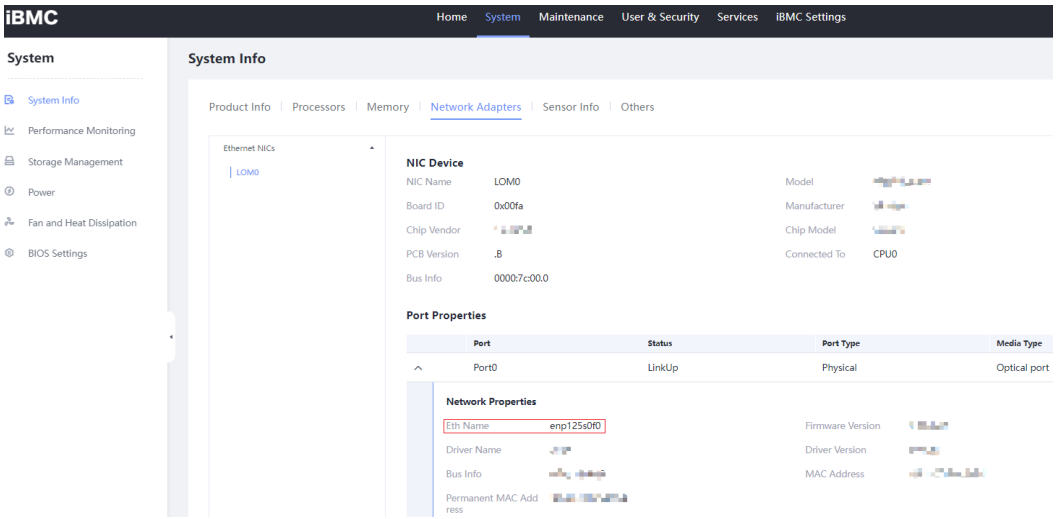
Procedure

Step 1 Check the name of the network port corresponding to a NIC.

Log in to the iBMC system of a node, choose **System** > **System Info** > **Network Adapters** or **System** > **System Info** > **NICs**, select the corresponding NIC and port, and view the network port name. An example is provided as follows:

NOTE

If **Eth Name** cannot be queried on this page, you need to install the iBMA component. For details, see **5.5.20 Installing the iBMA Component**.



Step 2 Use a remote connection tool to log in to the node as user **fsadmin** through the temporary management IP address. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. After the password is changed, log in to the node again.

Step 3 Run the following command to switch to user **root**.

```
su - root
```

Step 4 Go to the path for storing the network port configuration file.

```
cd /etc/sysconfig/network-scripts
```

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Run the following command to edit the network port configuration file. If the network port configuration file does not exist in the current path, you can run the following command to create and edit the network port configuration file.

```
vi ifcfg-Network port name
```

For details about the configuration file, see **Table 5-14**.

NOTE

In the following example, the management network uses physical network port enp125s0f0. You need to configure the following network port configuration files for each node:

- **ifcfg-enp125s0f0**: configuration file of physical network port enp125s0f0
- **ifcfg-v.*XXX***: configuration file of the VLAN port corresponding to the physical network port

Table 5-14 Network port configuration file information

Name	Content
ifcfg-*enp125s0f0*	DEVICE=*enp125s0f0* BOOTPROTO=none ONBOOT=yes STARTMODE=onboot DEFROUTE=yes NM_CONTROLLED=no
ifcfg-*v.XXX*	DEVICE=*v.XXX* **NOTE** • The value of **DEVICE** must contain a period (.) or start with **vlan**. • The value of **DEVICE** cannot contain the at sign (@). • The value of **DEVICE** can contain a maximum of 13 characters. • IPv4 configuration: IPADDR=*IPv4 address* NETMASK=*subnet mask* DEFROUTE=yes NETWORKING=yes GATEWAY=*Management network gateway* **NOTE** • The external management network cannot use the same subnet as the storage network (the internal management network and storage network share the same IP address), control network, or service network. • A gateway must be configured for the external management network. The gateway must be the same as the default node gateway. IPV6_AUTOCONF=no BOOTPROTO=static PHYSDEV=eth0 ONBOOT=yes USERCTL=no VLAN=yes VID=XXX /***VID** is the specified VLAN ID, which must be the same as the VLAN ID configured on the switch.*/ NM_CONTROLLED=no

Step 6 After editing the configuration file, press **Esc** and enter **:wq** to save the settings and exit.

 Copyright © Huawei Technologies Co., Ltd.

Step 7 Modify the permission on the network port configuration file.

```
chmod 644 /etc/sysconfig/network-scripts/ifcfg-Network port name
chown -h root:root /etc/sysconfig/network-scripts/ifcfg-Network port name
```

NOTE

All network port configuration files need to be modified.

Step 8 Run the following command to restart the network service:

```
service network restart
```

NOTE

After restarting the network service, you are advised to wait for 2 to 3 minutes to ensure that the network communication is recovered.

Step 9 Repeat **Step 1** to **Step 8** to configure the management IP addresses and gateways for all nodes.

Step 10 After the configuration is complete, ping the management IP addresses of other nodes on one node to check whether the management network communication between nodes is normal.

----End

5.4.1.6.3.5 Configuring a Bond Port IP Address and a VLAN

Context

The description in the following operations is only an example. The actual port information prevails.

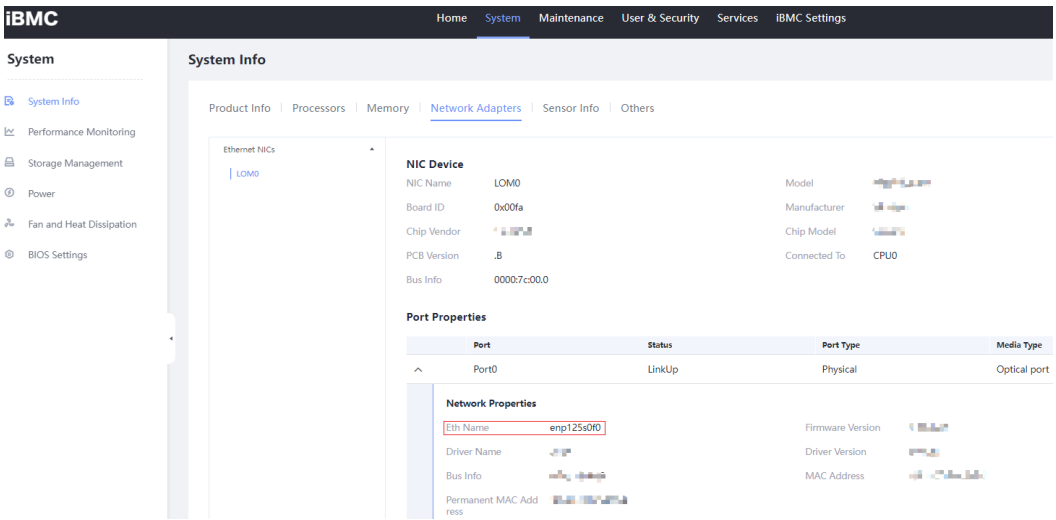
Procedure

Step 1 Check the name of the network port corresponding to a NIC.

Log in to the iBMC system of a node, choose **System** > **System Info** > **Network Adapters** or **System** > **System Info** > **NICs**, select the corresponding NIC and port, and view the network port name. An example is provided as follows:

NOTE

If **Eth Name** cannot be queried on this page, you need to install the iBMA component. For details, see **5.5.20 Installing the iBMA Component**.



 Copyright © Huawei Technologies Co., Ltd.

Step 2 Use a remote connection tool to log in to the node as user **fsadmin** through the temporary management IP address. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. After the password is changed, log in to the node again.

Step 3 Run the following command to switch to user **root**.

```
su - root
```

Step 4 Go to the path for storing the network port configuration file.

```
cd /etc/sysconfig/network-scripts
```

Step 5 Run the following command to edit the network port configuration file. If the network port configuration file does not exist in the current path, you can run the following command to create and edit the network port configuration file.

```
vi ifcfg-Network port name
```

For details about the configuration file, see **Table 5-15**.

NOTE

In the following example, the management network uses physical network ports enp125s0f0 and enp125s0f1. You need to configure the following network port configuration files for each node:

- **ifcfg-enp125s0f0**: configuration file of physical network port enp125s0f0
- **ifcfg-enp125s0f1**: configuration file of physical network port enp125s0f1
- **ifcfg-fsb_bond**: configuration file of the bond port corresponding to the two physical network ports
- **ifcfg-v.*XXX***: configuration file of the VLAN port corresponding to the bond port

Table 5-15 Network port configuration file information

Name	Content
ifcfg-*enp125s0f0*	DEVICE=*enp125s0f0* BOOTPROTO=none ONBOOT=yes MASTER=*fsb_bond* SLAVE=yes USERCTL=no NM_CONTROLLED=no
ifcfg-*enp125s0f1*	DEVICE=*enp125s0f1* BOOTPROTO=none ONBOOT=yes MASTER=*fsb_bond* SLAVE=yes USERCTL=no NM_CONTROLLED=no

 Copyright © Huawei Technologies Co., Ltd.

Name	Content
ifcfg-*fsb_bond*	DEVICE=*fsb_bond* ONBOOT=yes BOOTPROTO=none USERCTL=no TYPE=Bonding MTU=1500 NM_CONTROLLED=no BONDING_OPTS='mode=1 miimon=100' **NOTE** The bond1 mode is recommended for the bond port of the management network and the **BONDING_OPTS** parameter is set as follows: BONDING_OPTS='mode=1 miimon=100' **NOTE** ● If the bond2 mode is configured, the **BONDING_OPTS** parameter is set as follows: BONDING_OPTS='mode=2 miimon=100 xmit_hash_policy=layer3+4' ● If the bond4 mode is configured, the **BONDING_OPTS** parameter is set as follows: BONDING_OPTS='mode=4 miimon=100 lacp_rate=fast xmit_hash_policy=layer3+4'
ifcfg-*v.XXX*	DEVICE=*v.XXX* **NOTE** ● The value of **DEVICE** must contain a period (.) or start with **vlan**. ● The value of **DEVICE** cannot contain the at sign (@). ● The value of **DEVICE** can contain a maximum of 13 characters. IPv4 configuration: IPADDR=*IPv4 address* NETMASK=*subnet mask* DEFROUTE=yes DEFROUTE=yes NETWORKING=yes GATEWAY=*Management network gateway* **NOTE** ● The external management network cannot use the same subnet as the storage network (the internal management network and storage network share the same IP address), control network, or service network. ● A gateway must be configured for the external management network. The gateway must be the same as the default node gateway. IPV6_AUTOCONF=no BOOTPROTO=static PHYSDEV=*fsb_bond* /*The value of *fsb_bond* must be the same as the name of the bond port.*/ ONBOOT=yes USERCTL=no VLAN=yes VID=XXX /***VID** is the VLAN ID specified on the management switch.*/ NM_CONTROLLED=no

Step 6 After editing the configuration file, press **Esc** and enter **:wq** to save the settings and exit.

 Copyright © Huawei Technologies Co., Ltd.

Step 7 Modify the permission on the network port configuration file.

```
chmod 644 /etc/sysconfig/network-scripts/ifcfg-Network port name
chown -h root:root /etc/sysconfig/network-scripts/ifcfg-Network port name
```

NOTE

All network port configuration files need to be modified.

Step 8 Run the following command to restart the network service:

```
service network restart
```

NOTE

After restarting the network service, you are advised to wait for 2 to 3 minutes to ensure that the network communication is recovered.

Step 9 Repeat **Step 1** to **Step 8** to configure the management IP addresses and gateways for all nodes.

Step 10 After the configuration is complete, ping the management IP addresses of other nodes on one node to check whether the management network communication between nodes is normal.

----End

5.4.1.6.4 Installing OceanStor Pacific Series Software

5.4.1.6.4.1 Installing Management Nodes (Applicable to OceanStor Pacific 9550, 9546, 9540, 9520, and 9920)

Prerequisites

- The OS of the installation PC meets the compatibility requirements. For details, see the **DeviceManager-Client** requirements in **Huawei Storage Interoperability Navigator**.
- The network connection between the installation PC and all nodes is normal.
- The command prompt for user **root** is **#**.
- Management networks have been configured on the management nodes. For details, see **5.4.2.7.4 Configuring the Management Network of a Node**. You can run the **ifconfig** command to obtain the information about the ports configured with management networks.
- The communication between the management nodes and storage nodes is normal. You can ping the management IP addresses of other nodes from one node to check whether the communication is normal.

Procedure

Step 1 Decompress **OceanStor-Pacific_8.2.1RC1_DeviceManagerClient.zip** on the installation PC, and double-click **run.bat** in the decompression directory. The browser automatically opens DeviceManager Client.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The OS time of the installation PC must be set to the current time zone and time.
- The OS time of management nodes must be the same. Otherwise, change the time to be the same by referring to **5.5.25.7 Changing the System Time of a Node**.
- During the installation, do not close the **OceanStor-Pacific_devicemanager-client** window.
- The decompression directory of the software package cannot contain spaces or brackets.
- DeviceManager Client cannot be opened using a shared path.
- If the browser does not automatically open, open the browser manually and enter **https://127.0.0.1:***port* in the address box. The value of *port* is the character string in the **OceanStor-Pacific_devicemanager-client** window. For example, in **Starting ProtocolHandler ["https-jsse-nio-127.0.0.1-8088"]**, the port number is **8088**.

Step 2 The browser may display a message indicating that the security certificate of the website is incorrect. You can ignore the security warning message as prompted if the IP address is correct.

Take Google Chrome as an example. On the security prompt page, click **Advanced** and select **Proceed to** *XXX.XXX.XXX.XXX* **(unsafe)**. The OceanStor Pacific series installation page is displayed.

Step 3 Select **Deploy by Wizard**.

Step 4 Add and configure management nodes.

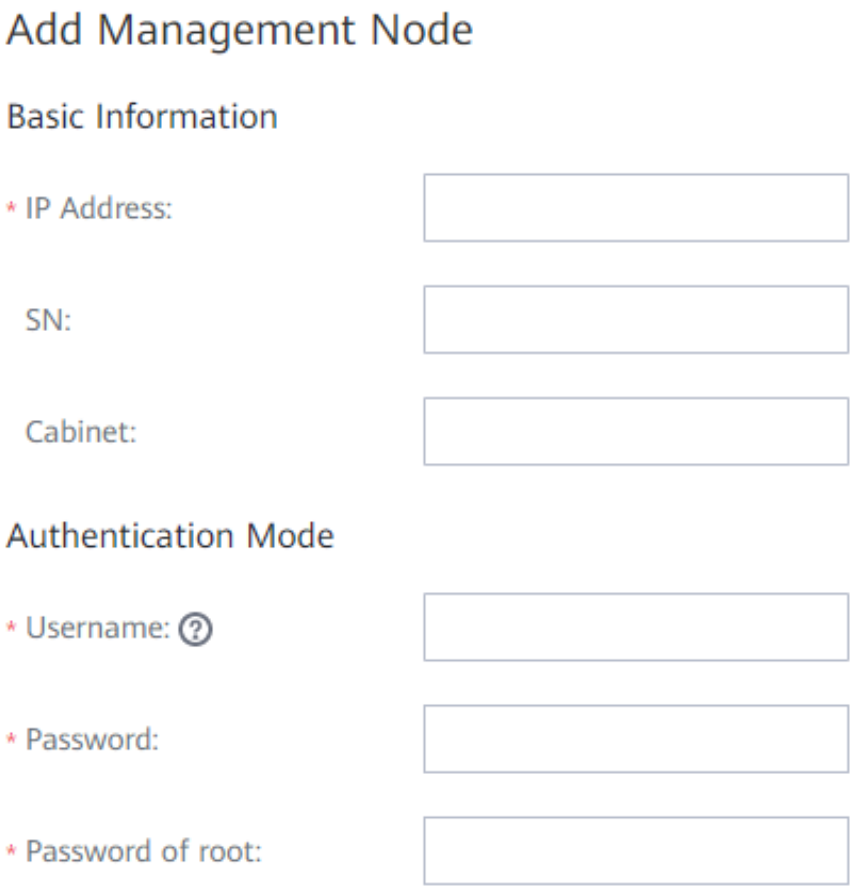
NOTE

If an exception occurs during the installation of the management nodes and the DeviceManager Client tool exits, uninstall the software by referring to **5.5.19 Uninstalling OceanStor Pacific Series Software** and reinstall the software.

1. Click **Add Management Node**. The **Add Management Node** dialog box is displayed, as shown in **Figure 5-6**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-6 Add Management Node



Enter the management node information and click **OK**. **Table 5-16** describes the management node information.

Table 5-16 Management node information

Category	Parameter	Description
Basic Information	IP Address	Indicates the management network IP address of a management node. Set this parameter to the internal management IP address.
	SN	Indicates the SN of a management node.
	Cabinet	Indicates the cabinet where a management node resides. For details, see *OceanStor Pacific Series 8.2.1 LLD Configuration Template*.

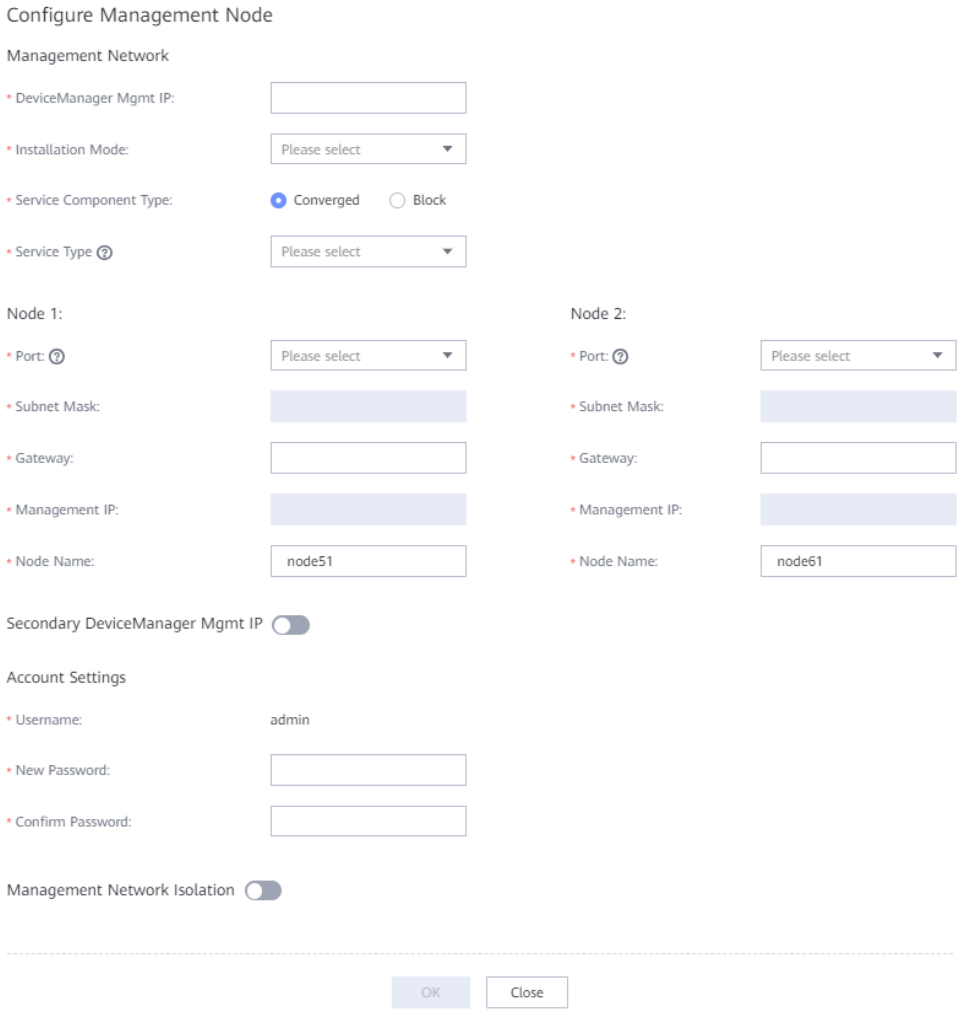
 Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
Authentication Mode	Username	If you use the pre-installed OS, enter **fsadmin** for authentication. **CAUTION** If you use user **fsadmin** for authentication: – If you have changed its default password, use the new password for authentication. – If you have not changed its default password, log in to the node, change the default password, and then use the new password for authentication.
	Password	Indicates the new password of user **fsadmin**.
	Password of root	When the user is a non-root user, enter the password of user **root**. Change the default password upon the first login.

2. Repeat **Step 4.1** to add the other management node.
3. Click **Configure Management Node**. The **Configure Management Node** dialog box is displayed, as shown in **Figure 5-7**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-7 Configure Management Node



Enter the information about the external management network. **Table 5-17** describes information about the external management network.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-17 External management network information

Category	Parameter	Description
Management Network	DeviceManager Mgmt IP	Indicates the floating management IP address of the management nodes. **NOTE** – After logging in to DeviceManager using this IP address, you can access the active and standby FSM nodes at the same time. – The type of the floating management IP address must be the same as that of management IP addresses configured on the nodes.
	Installation Mode	The value can be **Pre-installation** or **Regular installation**. To identify the installation mode, see **5.5.21 Identifying the Installation Mode**. – **Pre-installation**: The basic service package has been pre-installed on management nodes and storage nodes. You are advised to use this mode for configuration. – **Regular installation**: The basic service package is not installed on management nodes and storage nodes. You need to import the basic service package from DeviceManager Client and install it.
	Service Component Type	Select **Converged**.

Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
	Service Type	The value can be **General** or **Media**. Select a service type based on the actual service scenario to achieve optimal system performance. – **General**: provides file, object, and HDFS storage services for upper-layer applications and applies to high-performance computing (HPC) scenarios (such as meteorology, genetics, and oil industries) and big data analysis scenarios (such as 5G log retention and analysis). – **Media**: applies to video editing and media asset archiving in broadcasting, television, and film industries with sequential read and write of large files. **NOTE** In the media scenario, OceanStor Pacific 9950/ OceanStor Pacific 9550/ OceanStor Pacific 9546/ OceanStor Pacific 9540/ OceanStor Pacific 9920 is used.
Management node information	Port	Indicates the network port used by the management network.
	Subnet Mask/Prefix	Indicates the subnet mask of the management network. This parameter cannot be modified. It is automatically generated after a port is selected.
	Gateway	Indicates the gateway of the management network. This parameter cannot be modified. It is automatically generated after a port is selected.

 Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
	Management IP	Indicates the management IP address of a management node. This parameter cannot be modified. It is automatically generated after a port is selected.
	Node Name	Indicates the name of a management node. The value contains 1 to 64 characters, including only letters, digits, hyphens (-), underscores (_), and periods (.), and must start and end with a letter or digit. A period (.) cannot be adjacent to a period (.), hyphen (-), or underscore (_). **NOTE** If the management nodes work in active/standby mode, the value of **Node Name** of the two management nodes must be different.
Secondary DeviceManager Mgmt IP	This parameter cannot be configured. It is disabled (by default).	
DeviceManager login account **NOTE** The login account is used for: – Login to DeviceManager – Login in to the CLI – DSwareTool authentication	Username	The value is fixed to **admin**.

 Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
	New Password	Indicates the new password of the user. **NOTE** – The password contains 8 to 16 characters. – The password contains at least one space or one of the following special characters: `~!@#$%^&*()-_=+|[{}];:'",<.>/? – When the password complexity is **normal**, the password must contain at least two types of the following characters. When the password complexity is **high**, the password must contain the following three types of characters. ■ Lowercase letters: a to z ■ Uppercase letters: A to Z ■ Digits: 0 to 9 – The password can contain a maximum of three consecutive identical characters. – The password cannot be the same as the user name or the user name spelled backwards. – The password cannot be the same as any of the last three passwords. – The password cannot be in the weak password dictionary. For details, see **5.5.8 Weak Password Dictionary**.
	Confirm Password	Enter the new password again.

4. Configure management network isolation.
   Enable **Management Network Isolation**, as shown in **Figure 5-8**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-8 Configuring an internal management network

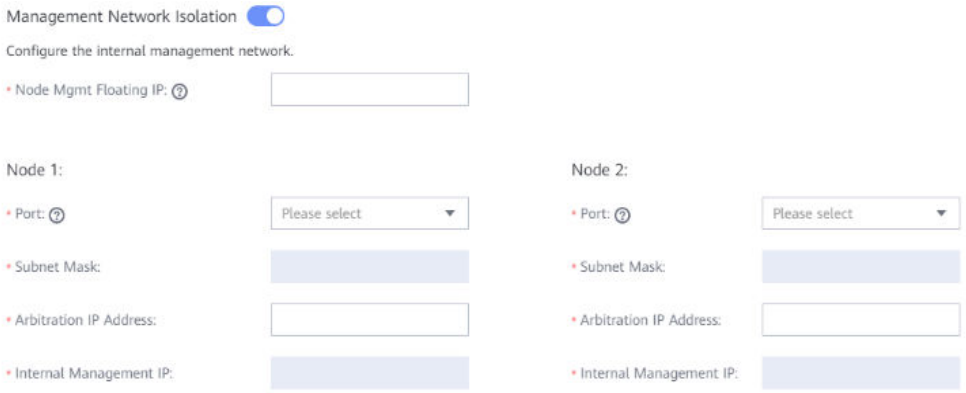


Table 5-18 describes information about the internal management network.

Table 5-18 Internal management network information

Parameter	Description
Node Mgmt Floating IP	Indicates the internal floating management IP address of the management nodes. It is used for the management data communication between management nodes and storage or compute nodes.
Port	Indicates the network port used by the internal management network.
Subnet Mask/Prefix	Indicates the subnet mask or prefix of the internal management network. This parameter cannot be modified. It is automatically generated after a port is selected. **NOTE** When the management IP address is set to an IPv4 address, the corresponding subnet mask is displayed.
Arbitration IP Address	Indicates the HA arbitration IP address. **NOTE** If the internal management network has a gateway, the arbitration IP address is automatically set to the gateway after you select a port. Otherwise, enter the management IP address (internal management IP address) of any storage node that is deployed separately from management nodes in the cluster as the arbitration IP address.
Internal Management IP	Indicates the internal management IP address of a management node. This parameter cannot be modified. It is automatically generated after a port is selected.

5. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Install management nodes.

- If **Installation Mode** is set to **Pre-installation**, the basic service package has been installed on the nodes. Click **Install** to install management nodes.
- If **Installation Mode** is set to **Regular installation** and the basic service package is not installed on the nodes, you need to upload the software package and then install management nodes.
  a. Upload software packages. After the upload is successful, the system displays the software package names.
     i. Click ... next to **Basic Service Package**, select basic service package **OceanStor-Pacific_8.2.1RC1.tar.gz**, and click **Upload**.
     ii. (Optional) If a patch needs to be installed, click ... next to **Patch Package**, select patch package **OceanStor-Pacific_8.2.1RC1.SPH*XXX***, and click **Upload**.
     iii. (Optional) If the data pilot function is required, click ... next to **Data Pilot Service Package**, select data pilot service package **OceanStor-Pacific_8.2.1RC1_Value-addedService.tar.gz**, and click **Upload**.
  b. Click **Install** to start installing the management nodes. After the installation is complete, click **Next** and ignore the security warning information as prompted.

----End

5.4.1.6.4.2 Installing Management Nodes (Applicable to OceanStor Pacific 9350, 9346, and 9340)

Prerequisites

- The OS of the installation PC meets the compatibility requirements. For details, see the **DeviceManager-Client** requirements in **Huawei Storage Interoperability Navigator**.
- The network connection between the installation PC and all nodes is normal.
- The command prompt for user **root** is **#**.
- Management networks have been configured on the management nodes. For details, see **5.4.2.7.4 Configuring the Management Network of a Node**. You can run the **ifconfig** command to obtain the information about the ports configured with management networks.
- The communication between the management nodes and storage nodes is normal. You can ping the management IP addresses of other nodes from one node to check whether the communication is normal.

Procedure

Step 1 Decompress **OceanStor-Pacific_8.2.1RC1_DeviceManagerClient.zip** on the installation PC, and double-click **run.bat** in the decompression directory. The browser automatically opens DeviceManager Client.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The OS time of the installation PC must be set to the current time zone and time.
- The OS time of management nodes must be the same. Otherwise, change the time to be the same by referring to **5.5.25.7 Changing the System Time of a Node**.
- During the installation, do not close the **OceanStor-Pacific_devicemanager-client** window.
- The decompression directory of the software package cannot contain spaces or brackets.
- DeviceManager Client cannot be opened using a shared path.
- If the browser does not automatically open, open the browser manually and enter **https://127.0.0.1:***port* in the address box. The value of *port* is the character string in the **OceanStor-Pacific_devicemanager-client** window. For example, in **Starting ProtocolHandler ["https-jsse-nio-127.0.0.1-8088"]**, the port number is **8088**.

Step 2 The browser may display a message indicating that the security certificate of the website is incorrect. You can ignore the security warning message as prompted if the IP address is correct.

Take Google Chrome as an example. On the security prompt page, click **Advanced** and select **Proceed to** *XXX.XXX.XXX.XXX* **(unsafe)**. The OceanStor Pacific series installation page is displayed.

Step 3 Select **Deploy by Wizard**.

Step 4 Add and configure management nodes.

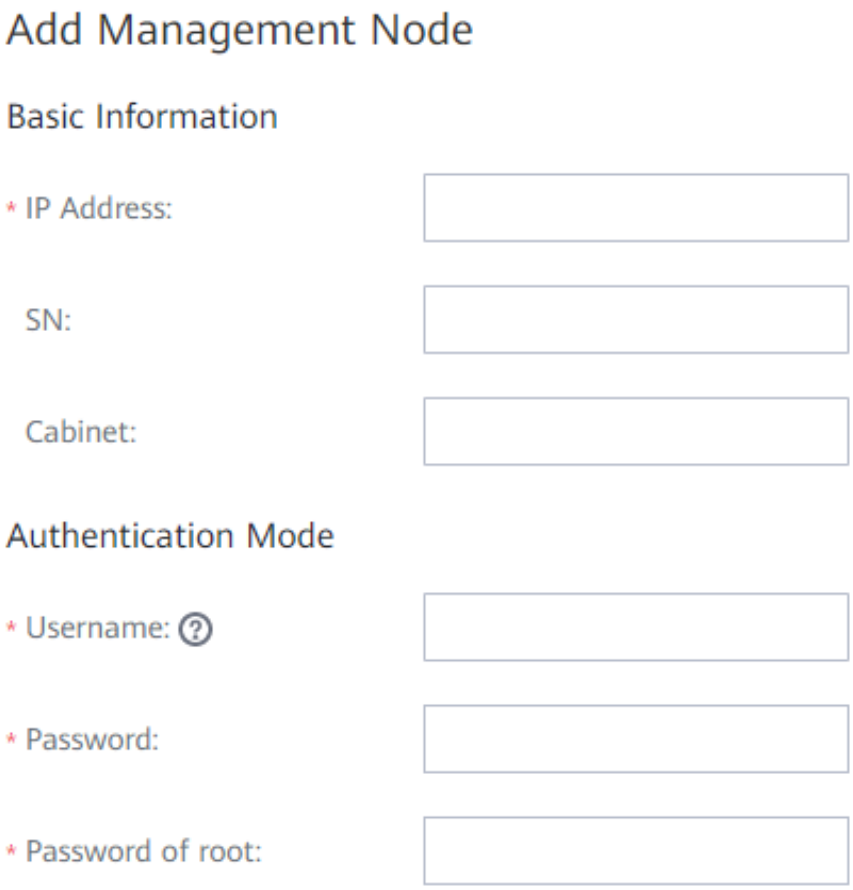
NOTE

If an exception occurs during the installation of the management nodes and the DeviceManager Client tool exits, uninstall the software by referring to **5.5.19 Uninstalling OceanStor Pacific Series Software** and reinstall the software.

1. Click **Add Management Node**. The **Add Management Node** dialog box is displayed, as shown in **Figure 5-9**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-9 Add Management Node



Enter the management node information and click **OK**. **Table 5-19** describes the management node information.

Table 5-19 Management node information

Category	Parameter	Description
Basic Information	IP Address	Indicates the management network IP address of a management node.
	SN	Indicates the SN of a management node.
	Cabinet	Indicates the cabinet where a management node resides. For details, see *OceanStor Pacific Series 8.2.1 LLD Configuration Template*.

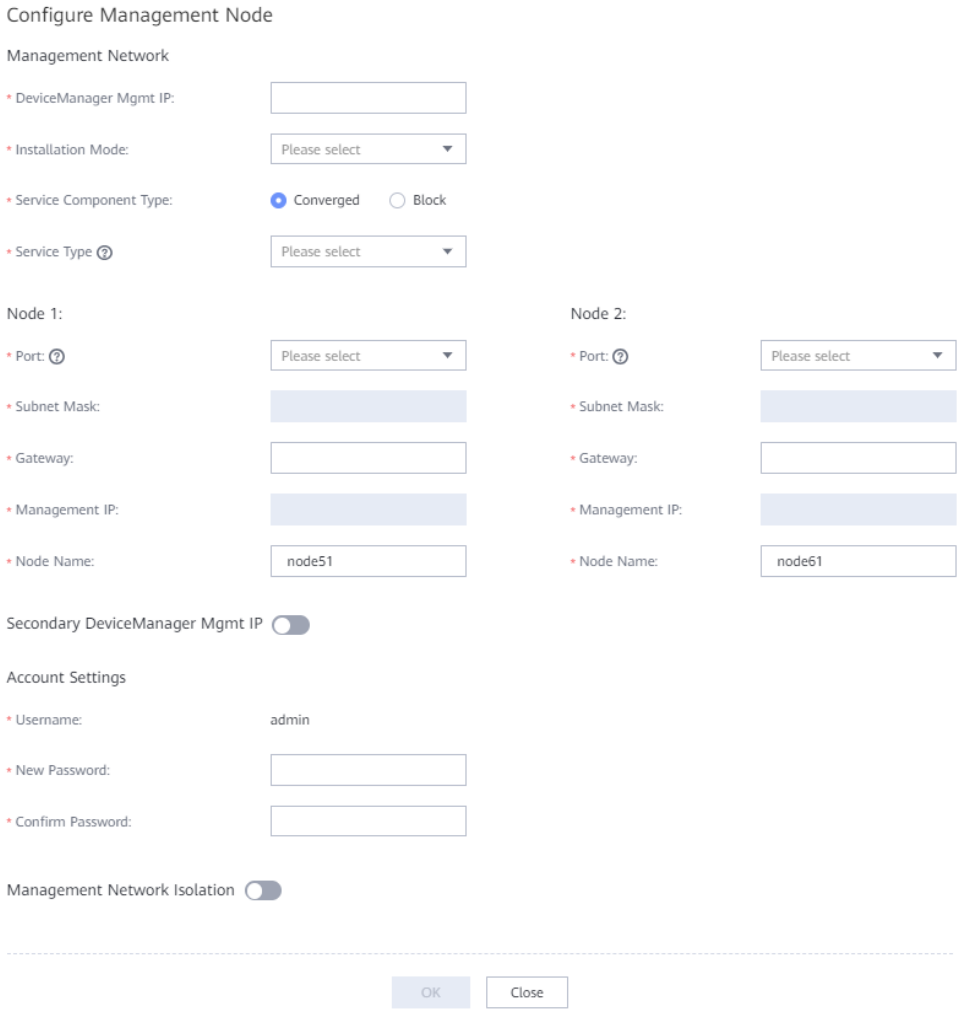
 Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
Authentication Mode	Username	If you use the pre-installed OS, enter **fsadmin** for authentication. **CAUTION** If you use user **fsadmin** for authentication: – If you have changed its default password, use the new password for authentication. – If you have not changed its default password, log in to the node, change the default password, and then use the new password for authentication.
	Password	Indicates the new password of user **fsadmin**.
	Password of root	When the user is a non-root user, enter the password of user **root**. Change the default password upon the first login.

2. Repeat **Step 4.1** to add the other management node.
3. Click **Configure Management Node**. The **Configure Management Node** dialog box is displayed, as shown in **Figure 5-10**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-10 Configure Management Node



Enter the information about the external management network. **Table 5-20** describes information about the external management network.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-20 External management network information

Category	Parameter	Description
Management Network	DeviceManager Mgmt IP	Indicates the floating management IP address of the management nodes. **NOTE** – After logging in to DeviceManager using this IP address, you can access the active and standby FSM nodes at the same time. – The type of the floating management IP address must be the same as that of management IP addresses configured on the nodes.
	Installation Mode	The value can be **Pre-installation** or **Regular installation**. To identify the installation mode, see **5.5.21 Identifying the Installation Mode**. – **Pre-installation**: The basic service package has been pre-installed on management nodes and storage nodes. You are advised to use this mode for configuration. – **Regular installation**: The basic service package is not installed on management nodes and storage nodes. You need to import the basic service package from DeviceManager Client and install it.
	Service Component Type	Select **Converged**.

Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
	Service Type	Select **Intelligent video and image**. **Intelligent video and image**: applies to video and image storage industries, including video stream and checkpoint image storage scenarios. **NOTE** In the intelligent video and image scenario, the HDFS service is not supported.
Management node information	Port	Indicates the network port used by the management network.
	Subnet Mask/ Prefix	Indicates the subnet mask of the management network. This parameter cannot be modified. It is automatically generated after a port is selected.
	Gateway	Indicates the gateway of the management network. This parameter cannot be modified. It is automatically generated after a port is selected.
	Management IP	Indicates the management IP address of a management node. This parameter cannot be modified. It is automatically generated after a port is selected.

 Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
	Node Name	Indicates the name of a management node. The value contains 1 to 64 characters, including only letters, digits, hyphens (-), underscores (_), and periods (.), and must start and end with a letter or digit. A period (.) cannot be adjacent to a period (.), hyphen (-), or underscore (_). **NOTE** If the management nodes work in active/standby mode, the value of **Node Name** of the two management nodes must be different.
Secondary DeviceManager Mgmt IP	This parameter cannot be configured. It is disabled (by default).	
DeviceManager login account **NOTE** The login account is used for: – Login to DeviceManager – Login in to the CLI – DSwareTool authentication	Username	The value is fixed to **admin**.

 Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
	New Password	Indicates the new password of the user. **NOTE** – The password contains 8 to 16 characters. – The password contains at least one space or one of the following special characters: `~!@#$%^&*()-_=+|[{}];:'",<.>/? – When the password complexity is **normal**, the password must contain at least two types of the following characters. When the password complexity is **high**, the password must contain the following three types of characters. ■ Lowercase letters: a to z ■ Uppercase letters: A to Z ■ Digits: 0 to 9 – The password can contain a maximum of three consecutive identical characters. – The password cannot be the same as the user name or the user name spelled backwards. – The password cannot be the same as any of the last three passwords. – The password cannot be in the weak password dictionary. For details, see **5.5.8 Weak Password Dictionary**.
	Confirm Password	Enter the new password again.

4. Configure management network isolation.
   Enable **Management Network Isolation**, as shown in **Figure 5-11**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-11 Configure Management Node

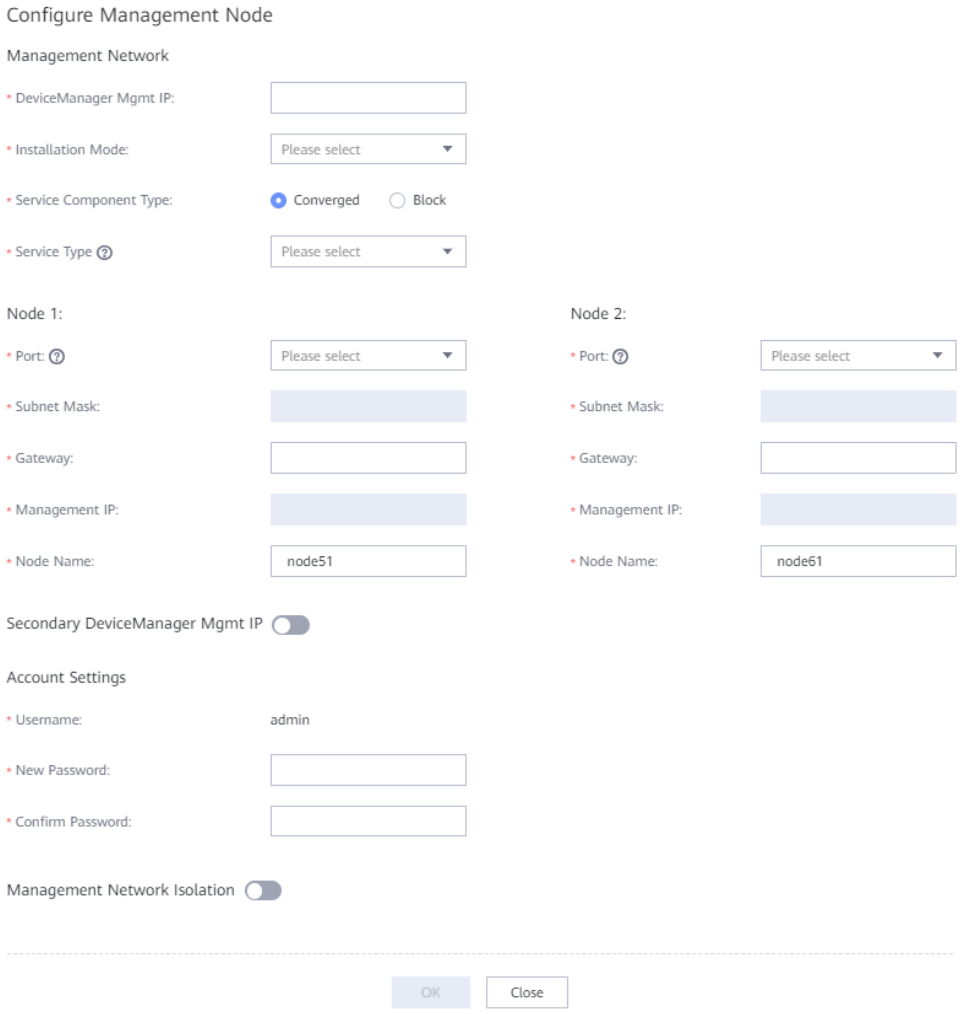


Table 5-21 describes information about the internal management network.

Table 5-21 Internal management network information

Parameter	Description
Node Mgmt Floating IP	Indicates the internal floating management IP address of the management nodes. It is used for the management data communication between management nodes and storage or compute nodes.
Port	Indicates the network port used by the internal management network.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Subnet Mask/Prefix	Indicates the subnet mask or prefix of the internal management network. This parameter cannot be modified. It is automatically generated after a port is selected. **NOTE** When the management IP address is set to an IPv4 address, the corresponding subnet mask is displayed.
Arbitration IP Address	Indicates the HA arbitration IP address. **NOTE** If the internal management network has a gateway, the arbitration IP address is automatically set to the gateway after you select a port. Otherwise, enter the management IP address (internal management IP address) of any storage node that is deployed separately from management nodes in the cluster as the arbitration IP address.
Internal Management IP	Indicates the internal management IP address of a management node. This parameter cannot be modified. It is automatically generated after a port is selected.

5. Click **OK**.

Step 5 Install management nodes.

- If **Installation Mode** is set to **Pre-installation**, the basic service package has been installed on the nodes. Click **Install** to install management nodes.
- If **Installation Mode** is set to **Regular installation** and the basic service package is not installed on the nodes, you need to upload the software package and then install management nodes.
  a. Upload software packages. After the upload is successful, the system displays the software package names.
     i. Click ... next to **Basic Service Package**, select basic service package **OceanStor-Pacific_8.2.1RC1.tar.gz**, and click **Upload**.
     ii. (Optional) If a patch needs to be installed, click ... next to **Patch Package**, select patch package **OceanStor-Pacific_8.2.1RC1.SPH*XXX***, and click **Upload**.
     iii. (Optional) If the data pilot function is required, click ... next to **Data Pilot Service Package**, select data pilot service package **OceanStor-Pacific_8.2.1RC1_Value-addedService.tar.gz**, and click **Upload**.
  b. Click **Install** to start installing the management nodes. After the installation is complete, click **Next** and ignore the security warning information as prompted.

----End

 Copyright © Huawei Technologies Co., Ltd.

5.4.1.6.4.3 Adding Storage Nodes

Prerequisites

- The network connection between the installation PC and all nodes is normal.
- Management network IP addresses have been configured on the storage nodes. For details, see **5.4.1.6.3 Configuring the Management Network of a Node**. You can run the **ifconfig** command to obtain the information about the ports configured with management networks.
- The communication between the management nodes and storage nodes is normal. You can ping the management IP addresses of other nodes from one node to check whether the communication is normal.
- The storage network of the storage nodes is properly connected.

Procedure

You can add storage nodes in a batch or manually.

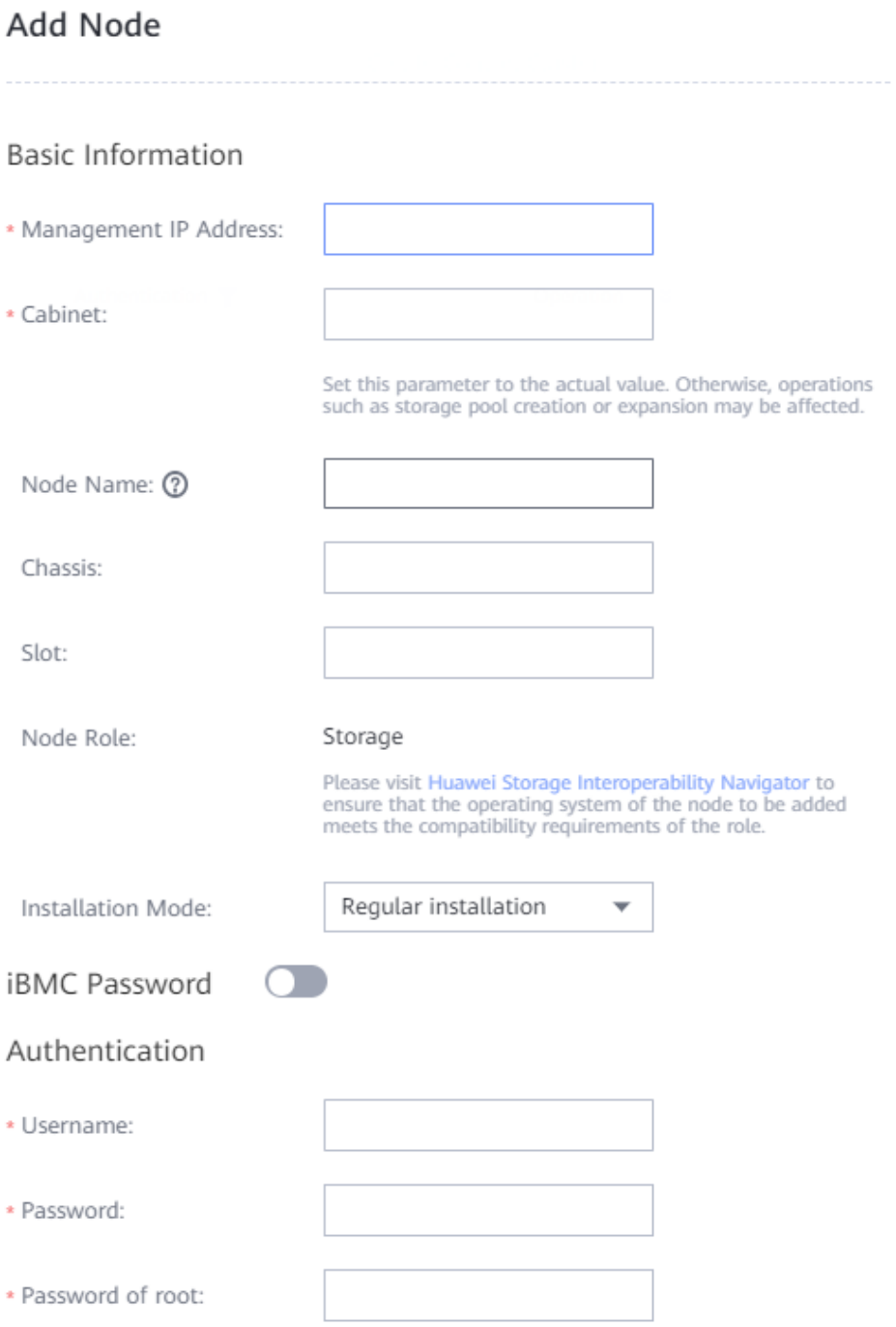
NOTE

Management nodes and storage nodes must be deployed in converged mode. In this case, the management nodes still need to be added again as storage nodes.

- Batch importing nodes
  a. Choose **Add Node > Batch Import Node**.
  b. Click **Download the template** to download the template locally. Fill the information in the template, click ··· and select the template, and then click **Upload**. The nodes are imported to the system in a batch.
  c. Authenticate all nodes. Click **Authenticate**, enter the user name and password, and click **OK**.
  d. After all nodes are authenticated successfully, click **OK**.
  e. Click **Submit**.
  f. After the nodes are successfully configured, click **Next**.
- Manually adding nodes
  a. Choose **Add Node** > **Manually Add Node**. The **Add Node** dialog box is displayed, as shown in **Figure 5-12**.

Copyright © Huawei Technologies Co., Ltd.

Figure 5-12 Add Node



b. Enter the storage node information and click **OK**. **Table 5-22** describes the storage node information.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-22 Storage node information

Category	Parameter	Description
Basic Information	Management IP Address	Indicates the management network IP address of a storage node. Set this parameter to the internal management IP address. IPv4 and IPv6 addresses are supported.
	Cabinet	The value can contain 1 to 256 characters, including only letters, digits, underscores (_), and hyphens (-). Set this parameter based on the site requirements. Otherwise, operations such as creating or expanding a storage pool may be affected.
	Node Name	Indicates the name of a node. The value contains 1 to 64 characters, including only letters, digits, hyphens (-), underscores (_), and periods (.), and must start and end with a letter or digit. A period (.) cannot be adjacent to a period (.), hyphen (-), or underscore (_). **NOTE** If the storage node and a management node are deployed on the same server, this parameter can be left blank.
	Chassis	Indicates the chassis ID.
	Slot	Indicates the slot number.
	Node Role	Indicates the role automatically matched based on the management IP address.

Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
	Installation Mode	The value can be **Pre-installation** or **Regular installation**. • **Pre-installation**: applies to scenarios where pre-installed nodes are added to a cluster. • **Regular installation**: applies to the installation of non-preinstalled nodes.

 Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
		NOTE To check whether a storage node is a pre-installed node, perform the following steps: 1. Use SSH to log in to the storage node to be added as user **fsadmin**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. 2. Run the **su - root** command and enter the password of user **root** as prompted to switch to user **root**. 3. Run the **ls -l** *File name* command to check whether the **/home/.preinstall**, **/opt/fusionstorage/.preinstall**, and **/opt/fusionstorage/.production_preinstall** files exist. If any of the files exists, the node is a pre-installed node. In the following example, the **/home/.preinstall** file exists. [root@FSM1 ~]# **ls -l /opt/fusionstorage/.production_preinstall** ls: cannot access '/opt/fusionstorage/.production_preinstall': No such file or directory [root@FSM1 ~]# **ls -l /opt/fusionstorage/.preinstall** ls: cannot access '/opt/fusionstorage/.preinstall': No such file or directory [root@FSM1 ~]# **ls -l /home/.preinstall** -rw------- 1 root root 0 Feb 21 15:32 /home/.preinstall

 Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
iBMC Password	Username/ Password	If you have changed the default iBMC user name or password, enter the new user name and password so that the system can monitor and manage hardware in a highly reliable manner (for example, high-temperature alarm reporting and power-off due to high temperature). **NOTE** The password must be the same as the node password configured in the iBMC system.
Authentication **NOTE** If the storage node and a management node are deployed on the same server, **Authentication** will not be displayed because the management node has been authenticated when it is added.	Username	If you use the pre-installed OS, enter **fsadmin** for authentication. **CAUTION** If you use user **fsadmin** for authentication: • If you have changed its default password, use the new password for authentication. • If you have not changed its default password, log in to the node, change the default password, and then use the new password for authentication.
	Password	Indicates the new password of user **fsadmin**.
	Password of root	When the user is a non-root user, enter the password of user **root**. Change the default password upon the first login.

c. Add other storage nodes one by one. Click **Submit** to start configuring nodes and installing network management components.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- You can select a newly added node and click **Authenticate** to authenticate the node again.
- You can select a node to be removed and click **Remove Node** to remove the node and uninstall the storage software on the node. You can also click **More** > **Remove Node** to remove the node. After the node is removed, it is no longer managed by the cluster.
  - Nodes that have not been configured and installed can be directly removed. Perform the operations as prompted.
  - Nodes that have been configured and installed can be removed only after being authenticated. Perform the operations as prompted.
- You can click **Set iBMC Password** to configure the user name and password for authenticating the iBMC server.
- You can click **Uninstall Software** to clear the configurations and data related to the storage software on all nodes. Perform the operations as prompted.
- After the operation is successful, you can click **More** on the right of a node and select **Log Details** to view its operation logs.

d. After all storage nodes are added successfully, click **Next**.

NOTE

When the OceanStor Pacific series software is installed for the first time, the security sandbox is automatically enabled on the added storage nodes.

5.4.1.6.4.4 Configuring the Storage Network (When Front- and Back-End Storage Networks Are Shared and Use RoCE and Multiple IP Addresses for Networking)

Configuration Description

Table 5-23 describes the storage network configurations.

Table 5-23 Network configurations

Hardware Type	Storage Network Deployment Mode	Storage Network Protocol	Storage Network Networking Mode	Control Network IP Address
OceanStor Pacific 9550/OceanStor Pacific 9546/ OceanStor Pacific 9920/OceanStor Pacific 9540/ OceanStor Pacific 9520/OceanStor Pacific 9350/ OceanStor Pacific 9346/OceanStor Pacific 9340	Front- and back-end shared network	RoCE	Multiple IP addresses	Required

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- The network connection between the installation PC and all nodes is normal.
- The storage network of the storage nodes is properly connected.
- Management network IP addresses have been configured on the storage nodes. If the IP addresses are not configured, configure them by referring to **5.4.1.6.3 Configuring the Management Network of a Node**. You can run the **ifconfig** command to obtain the information about the ports configured with management networks.
- The communication between the management nodes and storage nodes is normal. You can ping the management IP addresses of other nodes from one node to check whether the communication is normal.

Procedure

Step 1 Configure the storage network and the control network in advance by referring to **5.5.16.2 Configuring the Storage Network (RoCE and Multiple IP Addresses)**. If you have configured them, skip this operation.

Step 2 Select **Front- and Back-End Shared Network**.

Step 3 Select **Yes** in **Use Configured IP Address Only**.

Network IP addresses configured in advance are used. To select this option, all storage nodes must be configured with network IP addresses in advance.

Step 4 Set **Transmission Protocol** to **RoCE**, **Network Flow Classification** to **By using DSCP bits on the IP header**, and **Multiple IP Addresses** to **Yes**.

Step 5 Click **Add Control IP Address Range** to set the IP address segment and subnet mask/prefix of the control network. You can configure multiple control IP address segments. In addition, you can configure the control network across network segments. If the control IP addresses are across network segments, you need to enter the control network gateway.

Step 6 Click **Add Storage IP Address Range** to set the IP address segment and subnet mask/prefix of the storage network. You can configure multiple storage IP address segments. In addition, you can configure the storage network across network segments.

Step 7 Set related parameters. **Table 5-24** describes the parameters.

Table 5-24 Storage network information

Category	Parameter	Description
Transmission protocol	Transmission Protocol	Select **RoCE**.
	Network Flow Classification	Select **By using DSCP bits on the IP header**. **NOTE** **Network Flow Classification** of the front-end storage network on storage nodes must be the same as that on compute nodes. Otherwise, services will be interrupted.

Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
	Congestion Control Algorithm	The DCQCN and LDCP algorithms are supported. ● **DCQCN**: available for all NICs that support the RoCE protocol. This algorithm is recommended. ● **LDCP**: available for only Hi1822V120 NICs. ● All nodes in a cluster support only one algorithm. By default, DCQCN is used. Currently, dynamic switching of congestion control algorithms is not supported.
	Multiple IP Addresses	Select **Yes**.
IP address type: control IP address	IP Address Range	Indicates the IP address segment of the control network. **NOTE** The control network cannot use the same subnet as the external management network or service network. The control network and storage network (the internal management network and storage network share the same IP address) can use the same subnet (recommended) or different subnets. If they use the same subnet, they must use different IP address segments.
	Subnet Mask/ Prefix	Indicates the subnet mask or prefix of the control network. **NOTE** When the IP address of the control network is an IPv4 address, enter the subnet mask.
	Gateway	Gateway of the control network. ● A control network gateway needs to be configured in either of the following scenarios: – The control network crosses subnets. – The control network does not cross subnets currently but needs to cross subnets due to subsequent capacity expansion. In this case, you are advised to configure the gateway first.

 Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
IP address type: storage IP address	IP Address Range	Indicates the IP address segment of the storage network. IPv4 addresses are supported. **NOTE** • The start IP address and end IP address of each IP address segment must be in the same subnet. • The storage network cannot use the same subnet as the external management network or service network. The control network and storage network (the internal management network and storage network share the same IP address) can use the same subnet (recommended) or different subnets. If they use the same subnet, they must use different IP address segments.
	Subnet Mask/ Prefix	Indicates the subnet mask or prefix of the storage network. **NOTE** When the IP address of the storage network is an IPv4 address, enter the subnet mask.

NOTE

You can select the check box next to the storage IP address range ID or control IP address range ID and click **Remove** to remove the corresponding storage IP address range or control IP address range.

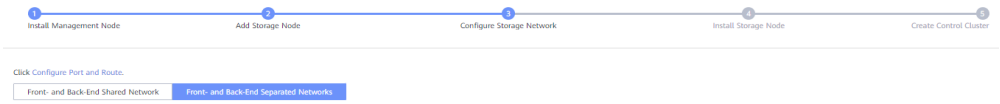
Step 8 On the storage network configuration page, click **Preview**. Because the storage or control IP addresses have been configured, the system displays the storage or control IP address of each node. Check whether the displayed IP addresses are the same as the planned IP addresses.

Step 9 Click **Submit** to start configuring the storage and control networks.

Wait until the storage network is configured successfully.

Step 10 Multiple IP addresses are used for networking. Therefore, you must configure a policy-based route to implement network interworking and data balancing.

1. Click **Configure Port and Route** to go to the route configuration page. Multiple IP addresses are configured on the VLAN port. For details, see **5.5.13.3 Configuring a Policy-based Route for a VLAN Port**.



 Copyright © Huawei Technologies Co., Ltd.

NOTE

To query policy-based route information of a VLAN port, see **5.5.14.1 Querying the Policy-based Routes of a VLAN Port**.

To delete policy-based route information of a VLAN port, see **5.5.15.1 Deleting a Policy-based Route from a VLAN Port**.

2. After the configuration is complete, click **Back** in the upper left corner to return to the **Configure Storage Network** page.

Step 11 After configuring the policy-based route, ping the storage or control IP addresses of other storage nodes from a storage node to ensure that the network communication between storage nodes is normal.

Step 12 Click **Next**.

----End

5.4.1.6.4.5 Configuring the Storage Network (When Front- and Back-End Storage Networks Are Shared and Use TCP for Networking)

Configuration Description

Table 5-25 describes the storage network configurations.

Table 5-25 Network configurations

Hardware Type	Storage Network Deployment Mode	Storage Network Protocol/ Networking Mode	Control Network IP Address
OceanStor Pacific 9550/OceanStor Pacific 9546/ OceanStor Pacific 9920/OceanStor Pacific 9540/ OceanStor Pacific 9520/OceanStor Pacific 9350/ OceanStor Pacific 9346/OceanStor Pacific 9340	Front- and back-end shared network	TCP/bond4	Not required

Prerequisites

- The network connection between the installation PC and all nodes is normal.
- The storage network of the storage nodes is properly connected.
- Management network IP addresses have been configured on the storage nodes. If the IP addresses are not configured, configure them by referring to **5.4.1.6.3 Configuring the Management Network of a Node**. You can run

 Copyright © Huawei Technologies Co., Ltd.

the **ifconfig** command to obtain the information about the ports configured with management networks.

- The communication between the management nodes and storage nodes is normal. You can ping the management IP addresses of other nodes from one node to check whether the communication is normal.

Procedure

Step 1 Select **Front- and Back-End Shared Network**.

Step 2 Select **Yes** or **No** in **Use Configured IP Address Only**, indicating whether only IP addresses configured in advance are used.

- **No**: The system will assign storage IP addresses to the storage nodes that have not been configured with storage IP addresses based on the settings on the GUI.
- **Yes**: Only storage IP addresses configured in advance are used. To select this option, all storage nodes must be configured with storage IP addresses in advance. For details, see **5.5.16.1 Configuring the Storage Network (TCP/IP)**.

  Table 5-26 describes the parameters.

Table 5-26 Storage network information

Parameter	Description
Transmission Protocol	TCP
Bond Mode	**bond4**: dynamic link aggregation mode **NOTE** When the transmission protocol is TCP, the bond4 mode is recommended.
Storage IP Address Range	Indicates the IP address segment of the storage network. IPv4 addresses are supported. **NOTE** – The start IP address and end IP address of each IP address segment must be in the same subnet. – The storage network (the internal management network and storage network share the same IP address) cannot use the same subnet as the external management network or service network. The IP addresses in each IP address segment cannot be in the same subnet as those of other ports on the node.
Mask/Prefix	Indicates the subnet mask or prefix of the storage network. **NOTE** When the IP address of the storage network is an IPv4 address, enter the subnet mask.

 Copyright © Huawei Technologies Co., Ltd.

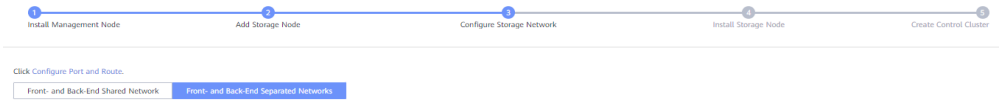
Parameter	Description
Port	Indicates the network port used by the storage network. Check whether the bond port has been configured by modifying the configuration file. – If yes, you do not need to add a port. Enter the configured bond port. – If no, add a port by referring to **5.5.9 Adding a Port** and enter the configured bond port. **NOTE** The bond mode of the added port must be the same as that of the bond port on the storage network.

NOTE

You can select the check box next to the storage IP address range ID and click **Remove** to remove the corresponding storage IP address range.

Step 3 If the storage IP addresses are across network segments, configure a static route.

1. Click **Configure Port and Route** to go to the route configuration page. For details, see **5.5.10 Configuring a Static Route**.



NOTE

– To query static route information, see **5.5.11 Querying a Static Route**.
– To delete static route information, see **5.5.12 Deleting a Static Route**.

2. After the configuration is complete, click **Back** in the upper left corner to return to the **Configure Storage Network** page.

Step 4 On the storage network configuration page, click **Preview**.

- If the storage IP addresses have been configured, the system displays the storage IP address of each node. Check whether the displayed IP addresses are the same as the planned IP addresses.
- If the storage IP addresses are not configured, the system displays the storage IP addresses to be allocated to storage nodes.

NOTE

– If the previewed IP address is not the planned IP address of the storage node, change the IP address of the storage node.
– Select the node whose IP address needs to be changed and click **More** to change the storage IP address of the node.

Step 5 Click **Submit** to start configuring the storage network.

Wait until the storage network is configured successfully.

 Copyright © Huawei Technologies Co., Ltd.

Step 6 After configuring the static route, ping the storage IP addresses of other storage nodes from a storage node to ensure that the network communication between storage nodes is normal.

Step 7 Click **Next**.

----End

5.4.1.6.4.6 Installing Storage Nodes

Procedure

Step 1 Click **Install** to start installing the storage nodes.

NOTE

- During the installation, if **Failure** is displayed in the **Installation Status** column, you can click **Uninstall Software** and reinstall the storage nodes.
- You can click **More** in the row where a storage node resides and select **Details** to view installation log details.

Step 2 After installation is successful, click **Next**.

NOTICE

- If you need to re-configure the storage network after the nodes are installed, remove the storage nodes and go back to the previous step to re-configure the storage network.
- After the storage nodes are installed, the security sandbox is automatically enabled.

----End

5.4.1.6.4.7 Creating a Control Cluster (Applicable to OceanStor Pacific 9550 and 9350)

Procedure

Step 1 Create a control cluster.

Enter the information about the control cluster. **Table 5-27** describes the control cluster information.

Table 5-27 Control cluster information

Parameter	Description
Control Cluster Name	Indicates the name of a control cluster. The value contains 1 to 64 characters, including only letters, digits, underscores (_), and hyphens (-).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Available Nodes	Indicates the nodes that can be used to create a control cluster. The number of nodes in a control cluster must comply with the following rules: Node-level security: • If the cluster contains 3 or 4 nodes, configure 3 nodes. • If the cluster contains 5 or 6 nodes, configure 5 nodes. • If the cluster contains 7 nodes or more, configure 7 nodes. • If the cluster contains 9 nodes or more and the number of EC parity fragments is +4 (not +4:1) in an EC scheme, configure 9 nodes.

Step 2 After entering the control cluster information, click **Create**. After the creation is successful, click **Finish**.

----End

Follow-up Procedure

- On the installation PC, double-click the **shutdown.bat** script in the decompression directory of **OceanStor-Pacific_8.2.1RC1_DeviceManagerClient.zip** to close the DeviceManager Client window. If the window cannot exit normally, click in the upper right corner to close it.
- If the storage network uses the RoCE protocol, you need to configure RoCE flow control on switches. For details, see **5.5.2.2 Configuring Flow Control for a Switch**. If the configuration has been performed, skip this step.
- If the storage network uses the RoCE protocol and the NIC type is Hi1620 or CX series, you need to configure ACL rules for switches. After the configuration, the latency and packet loss rate between storage nodes and access switches can be detected. For details, see **5.5.2.3 Configuring ACL Rules for Switches**. If the configuration has been performed, skip this step.
- If parameter settings are incorrect after the software is installed, uninstall the OceanStor Pacific series software and reinstall it. For details about how to uninstall the OceanStor Pacific series software, see **5.5.19 Uninstalling OceanStor Pacific Series Software**.
- After the installation and deployment are complete, you can use the management IP addresses of DeviceManager and nodes to remotely log in to management and storage nodes.
- Update default accounts in time. For details, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*.
- Update security certificates in time. For details, see section "Security Certificate Management" in *OceanStor Pacific Series 8.2.1 Security Configuration Guide*.

 Copyright © Huawei Technologies Co., Ltd.

5.4.1.6.4.8 Creating a Control Cluster (Applicable to OceanStor Pacific 9540, 9520, 9920, 9340, 9546, and 9346)

Procedure

Step 1 Create a control cluster.

Enter the information about the control cluster. **Table 5-28** describes the control cluster information.

Table 5-28 Control cluster information (custom)

Parameter	Description
Control Cluster Name	Indicates the name of a control cluster.
Metadata Storage Location	The following metadata storage locations are supported: • **Physical disk** • **System disk partition** • **Custom**: **Physical disk** and **System disk partition** can be mixed. This option is used when you need to select different metadata storage locations for different nodes. **NOTE** • For OceanStor Pacific 9520 Kunpeng-based 14-slot, OceanStor Pacific 9920 Kunpeng-based (palm-sized NVMe SSD), OceanStor Pacific 9546 (without an SP186-M-8i RAID controller card), and OceanStor Pacific 9346, you can select only **System disk partition**. • For OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9340 Kunpeng-based, OceanStor Pacific 9520 Kunpeng-based 12-slot, OceanStor Pacific 9920 Kunpeng-based (SAS SSD), and OceanStor Pacific 9546 (with an SP186-M-8i RAID controller card, you can select only **Physical disk**.
Disk Type	This parameter is mandatory when **Metadata Storage Location** is set to **Physical disk**. **NOTE** • For OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9340 Kunpeng-based, OceanStor Pacific 9520 Kunpeng-based 12-slot, OceanStor Pacific 9920 Kunpeng-based (SAS SSD), and OceanStor Pacific 9546 (with an SP186-M-8i RAID controller card, you can select only **M.2 SSD**. • When you need to select different disk types for different nodes, set this parameter to **Custom**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Disk Selection Mode	This parameter is mandatory when **Metadata Storage Location** is set to **Physical disk**. You can select **Specify Slot** or **Manually Select**. • **Specify Slot**: Enter a slot number. A slot number ranges from 0 to 60. • **Manually Select**: Manually select one disk for each node. **NOTE** When **Disk Type** is set to **Custom**, only **Manually Select** is supported.
Available Nodes	Indicates the nodes that can be used to create a control cluster. The number of nodes in a control cluster must comply with the following rules: Node-level security: • If the cluster contains 3 or 4 nodes, configure 3 nodes. • If the cluster contains 5 or 6 nodes, configure 5 nodes. • If the cluster contains 7 nodes or more, configure 7 nodes. • If the cluster contains 9 nodes or more and the number of EC parity fragments is +4 (not +4:1) in an EC scheme, configure 9 nodes. **NOTE** If **Metadata Storage Location** is set to **Custom**, you need to select a metadata storage location (**Physical disk** or **System disk partition**) and metadata disks for each node in the control cluster.

Step 2 After entering the control cluster information, click **Create**. After the creation is successful, click **Finish**.

----End

Follow-up Procedure

- On the installation PC, double-click the **shutdown.bat** script in the decompression directory of **OceanStor-Pacific_8.2.1RC1_DeviceManagerClient.zip** to close the DeviceManager Client window. If the window cannot exit normally, click in the upper right corner to close it.
- If the RoCE network is configured, you need to configure RoCE flow control on switches. For details, see **5.5.2.2 Configuring Flow Control for a Switch**. If you have configured RoCE flow control, skip this operation.
- If the RoCE network is configured, you need to configure ACL rules for switches. For details, see **5.5.2.3 Configuring ACL Rules for Switches**. If you have configured them, skip this operation.

 Copyright © Huawei Technologies Co., Ltd.

- If parameter settings are incorrect after the software is installed, uninstall the OceanStor Pacific series software and reinstall it. For details about how to uninstall the OceanStor Pacific series software, see **5.5.19 Uninstalling OceanStor Pacific Series Software**.
- After the installation and deployment are complete, you can use the management IP addresses of DeviceManager and nodes to remotely log in to management and storage nodes.
- Update default accounts in time. For details, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*.
- Update security certificates in time. For details, see section "Security Certificate Management" in *OceanStor Pacific Series 8.2.1 Security Configuration Guide*.

5.4.1.7 Obtaining and Loading a License

Obtain and load a license by referring to *OceanStor Pacific Series 8.2.1 License Operation Guide* so that the system can obtain a new validity period and service authorization. You need to import a license before using the OceanStor Pacific series storage system.

In wizard-based configuration mode, after the license is loaded, the DeviceManager home page is displayed. In LLD-based configuration mode, after the license is loaded, you can enter the user name and password to go to the DeviceManager home page.

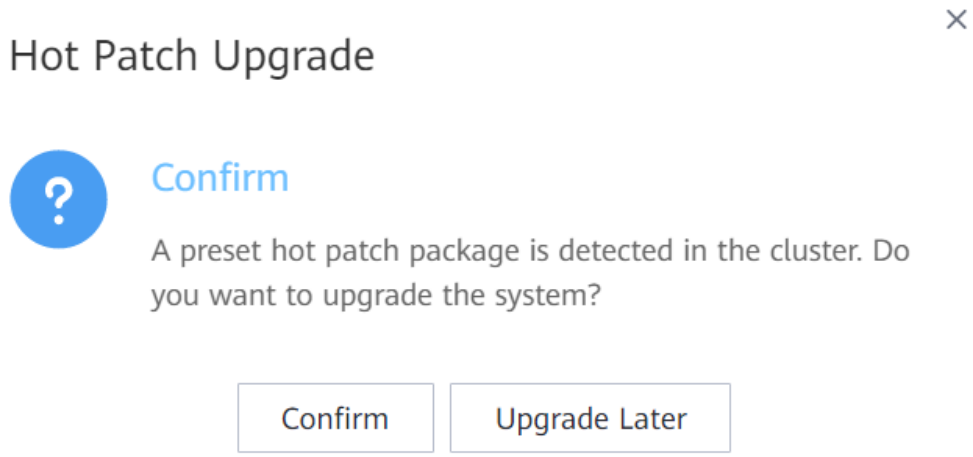
NOTE

After installing the software, create and configure a storage pool so that application servers can access the scale-out storage resources. For details, see **6.4 Configuring Basic Services**.

5.4.1.8 Performing an Upgrade Using a Preset Hot Patch

When the system detects that a preset hot patch exists in the current cluster, the **Hot Patch Upgrade** dialog box is displayed, asking you whether to perform an upgrade, as shown in **Figure 5-13**.

Figure 5-13 Hot patch upgrade prompt



 Copyright © Huawei Technologies Co., Ltd.

Determine whether to perform the upgrade as required. If the upgrade is not required, log in to a management node using the floating IP address, log in to the CLI as user **admin**, and run the **delete cluster patch_pkg** command to delete all patch packages that are not installed in the cluster.

5.4.2 Installing the File Service (DPC Scenario)

5.4.2.1 Node Requirements

Requirements on Node OS Time

The OS time of all nodes must be the same as the local time.

Management Node Deployment Requirements

Management nodes can be deployed only in active/standby mode, and the active and standby management nodes must use the same platform architecture (Kunpeng or x86).

Requirements for Compute and Storage Nodes

In RoCE networking scenarios, the lldpad service must be disabled. Otherwise, nodes will be isolated and services will be interrupted.

Log in to a node as user **fsadmin**, run the **su - root** command to switch to user **root**, and run the following command to disable the lldpad service:

```
systemctl stop lldpad.service
```

Memory Requirements for a DPC Node

The memory required for running DPC software on the compute node is greater than or equal to 16 GB, and the memory reserved for the OS is greater than or equal to 8 GB.

5.4.2.2 DPC Node Configuration Description

- Created directories and files

  When the DPC software is installed, the following directories and files are created. Do not delete or modify them.

  Table 5-29 Directories and files to be created and their functions

Directory or File Name	Function
/opt/fusionstorage /opt/dsware /opt/dpc_usr /opt/dfv /opt/network /OSM	Directories for storing storage software.

Copyright © Huawei Technologies Co., Ltd.

Directory or File Name	Function
/home/fdadmin /home/oam /home/omm /home/persistence /home/dpc_usr /home/storage	Directories generated by the system for storing user information after a system user is created.
/opt/storage_home	Directory generated by the system for storing user information after a system user is created when **/home** is unwritable.
/var/log/oam /var/log/deploy /var/log/infrastructure /var/log/dsware /var/log/dpc_script /var/log/dpc_public /var/log/dfv	Directories for storing storage software logs.
/sys/fs/cgroup/memory/cg_root/fusionstorage_dpc /cgroup/memory/cg_root/fusionstorage_dpc	Directories generated after cgroup named **fusionstorage_dpc** is added, used for managing the memory occupied by the DPC process.
/sys/kernel/slab/odc_cache_1024 /sys/kernel/slab/odc_cache_1536	Directories generated after the slab used by DPC is registered, used for managing memory allocation.
/var/crash/coredump	Directory for storing files that record process exit information.
/sys/module/odc_core /sys/module/odc_base /sys/module/odc_intf	Directories for storing .ko files on which the DPC process depends.
/etc/dfv	Directory for storing files that record the storage software version and chassis information of the current node.
/etc/node_manager_ip	File for recording the management IP address of the current node.
/etc/policy_route.cfg	File for recording the policy-based route information of the current node configured using dswareTool.sh.

 Copyright © Huawei Technologies Co., Ltd.

Directory or File Name	Function
/etc/sudoers.d/dsware_agent_sudoers /etc/sudoers.d/deploymanager_sudoers /etc/sudoers.d/nma_sudoers /etc/sudoers.d/snm_sudoers	**sudoers** configuration files of the storage software, used for controlling related permissions of the storage software.
/dev/odc_chrdev /sys/devices/virtual/misc/odc_chrdev	Character device file used by the DPC process to communicate with the kernel.
/etc/systemd/system/dpc_scheduled_task.service /etc/systemd/system/dpc_scheduled_task.timer /etc/systemd/system/timers.target.wants	Scheduled tasks for checking and dumping DPC kernel logs.
/run/lock/snm	Directory for storing the identification files and communication socket files of the snm process.
/run/lock/snm_*xxx*	File for recording the initialization, communication, or installation status of the snm process.
/dev/shm/diag_server_usr_lock	File lock of the Diagnose tool, used for determining whether the Diagnose process exists.
/dev/shm/snm_*xxx* /dev/shm/SNM_*xxx*	Files for recording the version and status of the snm process.
/etc/cron.d/snm_cron	File for recording information about scheduled tasks of the snm process.

- Created system users and user groups

  During DPC installation, the following system users and user groups are created. Do not delete them.

  - Users: **fdadmin**, **oam**, **omm**, **persistence**, and **dpc_usr**
  - User groups: **storage**, **omm**, **oam**, **dpc_usr**, **dfvgroup**, and **ops**
- System services on which DPC depends

  The running of the DPC software depends on some system services, as listed in **Table 5-30**.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-30 System services on which DPC depends and their functions

System Service Name	Function
SSH service	Remotely logs in to a server. **NOTE** When installing DPC on a compute node, you need to use the SSH service to access the compute node through port 22. If the firewall of the compute node blocks port 22, DPC will fail to be installed.
SFTP service	Transfers software packages.
cgroup service	Manages process memory.
crontab service	Manages scheduled tasks.
systemd service	Starts and stops services.
iptables service	Configures iptables rules.
firewall service	Configures firewall rules.
rsyslog service	Records and dumps logs.
secAgent service	Monitors system security.

- Table 5-31 lists the system configuration files on which DPC depends.

Table 5-31 System configuration files on which DPC depends and their functions

System Configuration File Name	Function
/etc/os-release or **/etc/system-release** **NOTE** The configuration file varies according to the OS.	Contains the release version of the OS.

- Table 5-32 lists the system configuration files that can be modified.

Table 5-32 System configuration files that can be modified, their functions, and modification methods

System Configuration File Name	Function	How to Modify
/proc/sys/vm/max_map_count	Sets the number of virtual memory areas (VMAs) that a process can have.	Set value **1000000** in the file.

 Copyright © Huawei Technologies Co., Ltd.

System Configuration File Name	Function	How to Modify
/etc/passwd	When a user is created, the system automatically adds a piece of user information to the file.	Create a system user.
/etc/group	When a system user group is created, the system automatically adds a piece of user group information to the file.	Create a system user group.
/etc/ssh/ ssh_host_*.pub	Key file for SSH login.	Modify the permission on the file.
/etc/security/ limits.conf	Configures resource limits on the OS.	Add the following configuration items to the file to change the hard limit and soft limit of the maximum locked-in-memory address space of user **omm** to unlimited: **omm hard memlock unlimited** **omm soft memlock unlimited** **NOTE** • Hard limit: When the hard limit threshold is reached, processes of user **omm** cannot apply for memory anymore. • Soft limit: When the soft limit threshold is reached, an alarm is generated but processes of user **omm** can still apply for memory.
/etc/sysconfig/ iptables /etc/sysconfig/ ip6tables	Saves iptables firewall rules.	Set value **iptables-save** in **/etc/sysconfig/iptables** and value **ip6tables-save** in **/etc/sysconfig/ ip6tables**.

 Copyright © Huawei Technologies Co., Ltd.

System Configuration File Name	Function	How to Modify
/etc/iptables/rule.v4 /etc/iptables/rule.v6	When iptables firewall rules are configured, the system automatically adds the firewall rule information to the file.	Run the **iptables** or **ip6tables** command to configure firewall rules related to the storage software.
/etc/sysctl.conf	If the storage network uses multiple IP addresses for networking, the system automatically adds the configuration information about disabling the storage network port proxy ARP function to the file.	Add **net.ipv4.conf.***Storage network port name***.arp_ignore=1** to the file.

5.4.2.3 Installation Process

Software installation in the DPC scenario includes software installation and deployment on management nodes and storage nodes. A management node and a storage node are deployed on the same server. The software installation also includes pre-installation of the DPC software on compute nodes.

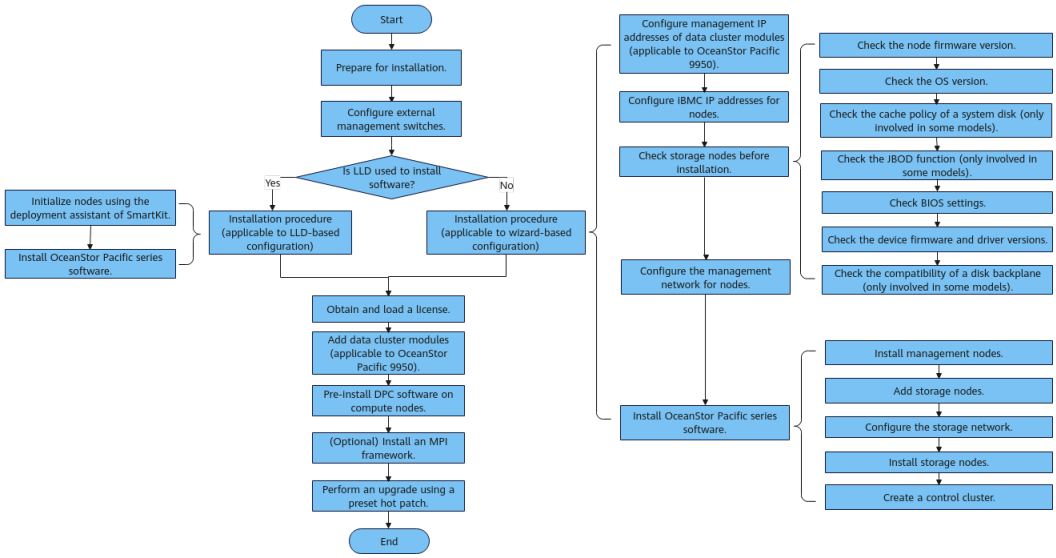
The software can be installed in LLD configuration mode or wizard configuration mode. **Figure 5-14** shows the installation process.

NOTE

- In LLD-based configuration mode, use the LLDesigner tool to plan nodes, networks, and clusters, export the deployment configuration file, and use the deployment assistant of SmartKit to initialize the nodes based on the deployment configuration file. Node initialization includes: configuring iBMC IP addresses of nodes, checking storage nodes before installation, and configuring management and storage networks for nodes. Then use DeviceManager Client to install the OceanStor Pacific series software in LLD-based configuration mode.
- In wizard-based configuration mode, manually add nodes, configure networks, and create a control cluster on DeviceManager for OceanStor Pacific series software installation.

Copyright © Huawei Technologies Co., Ltd.

Figure 5-14 File service installation process (DPC scenario)



During the OceanStor Pacific series installation process, you need to configure IP addresses and related components for nodes of each role. **Table 5-33** describes the network configuration of each hardware type.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-33 Network configurations

Hardware Type	Network to Be Configured	Deployment Requirements on Nodes
OceanStor Pacific 9550/OceanStor Pacific 9950/ OceanStor Pacific 9546/OceanStor Pacific 9540/ OceanStor Pacific 9920	• External management network **NOTE** • Network protocol: TCP • Networking mode: 1. OceanStor Pacific 9550: When the 25GE network is used, the number of network ports can be one or two. Two management network ports can be bonded only in bond4 mode. When the GE network is used, the number of network ports can be only one and bond is not supported. 2. OceanStor Pacific 9950: When the 100GE network is used, the number of network ports can be one or two. Two management network ports can be bonded only in bond4 mode. When the GE network is used, the number of network ports can be one or two. Two management network ports can be bonded only in bond1 mode. 3. OceanStor Pacific 9546: The number of network ports can be one or two. Two management network ports can be bonded only in bond1 mode. 4. OceanStor Pacific 9540/ OceanStor Pacific 9920: The number of network ports can be one or two. You are advised to bond two network ports in bond1 mode. • Storage network (front- and back-end shared) **NOTE** The network protocol and networking mode are RoCE and multiple IP addresses respectively.	• OceanStor Pacific 9540/OceanStor Pacific 9920/ OceanStor Pacific 9546 (One Node per Chassis, Two CPUs per Node): ≥ 3 • OceanStor Pacific 9950/OceanStor Pacific 9550/ OceanStor Pacific 9546 (Two Nodes per Chassis): ≥ 4

 Copyright © Huawei Technologies Co., Ltd.

Hardware Type	Network to Be Configured	Deployment Requirements on Nodes
	• Shared internal management network and storage network	

5.4.2.4 Preparing for Installation

5.4.2.4.1 Preparing Documents and Tools

Documents

Table 5-34 describes how to obtain documents.

Table 5-34 Obtaining documents

Name	How to Obtain
OceanStor Pacific Series 8.2.1RC1 Version Mapping (SFS)	This document defines the version numbers of the storage software, node firmware, NIC driver and firmware, RAID controller card driver and firmware used with OceanStor Pacific series, and the addresses for obtaining them. For enterprise users, log in to **https://support.huawei.com/enterprise**. For carrier users, log in to **https://support.huawei.com**. Enter **OceanStor Pacific** in the search box and click the suggested path to enter the product page. Search for and download the document of the desired version.
OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)	For enterprise users, log in to **https://support.huawei.com/enterprise**. For carrier users, log in to **https://support.huawei.com**. Enter the document name in the search box and click the search button. Search for and download the document of the desired version.
OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide	
CE6800 series switch documents	For enterprise users, log in to **https://support.huawei.com/enterprise**. For carrier users, log in to **https://support.huawei.com**. Enter **CloudEngine 58&68&78&88&98** in the search box and click the suggested path to enter the product page. Search for and download the document of the desired version.
CE8800 series switch documents	
CE9800 series switch documents	

Copyright © Huawei Technologies Co., Ltd.

Name	How to Obtain
ES3000 V5 NVMe PCIe SSD User Guide	For enterprise users, log in to **https://support.huawei.com/enterprise**. For carrier users, log in to **https://support.huawei.com**. Enter **ES3000 V5** in the search box and click the suggested path to enter the product page. Search for and download the document of the desired version.

Tools

Table 5-35 lists the required tools.

Table 5-35 Tools

Item	Description
One network cable	Connects an installation PC to a storage node or switch.
One console cable	Connects switches. One end of the console cable is an RJ-45 port, and the other end is a DB-9 port (connecting to an installation PC). If the installation PC has no serial port, prepare a USB-to-serial cable.

5.4.2.4.2 Obtaining Software Packages

Table 5-36 and **Table 5-37** describe how to obtain the OceanStor Pacific series software package, device firmware, and drivers.

NOTE

The version of the obtained software package is subject to *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

Copyright © Huawei Technologies Co., Ltd.

Table 5-36 Obtaining the OceanStor Pacific series software package

Type	Name	Description	How to Obtain
Software package	**OceanStor-Pacific_8.2.1RC1.tar.gz**	OceanStor Pacific series software package, including all components of OceanStor Pacific series	• You can obtain the OceanStor Pacific series software package, deployment tool, tool set, and file service OS software package, and data pilot service package from Huawei official website. For enterprise users, log in to **https://support.huawei.com/enterprise**. For carrier users, log in to **https://support.huawei.com**. In the search box, enter **OceanStor Pacific** and click the suggested path to enter the corresponding product page. For enterprise users, click **Software Download**. For carrier users, click **Software**. Then, search for and download the software package of the desired version and its ***.asc** digital certificate file. • For details about other compatible OSs, visit **Huawei Storage Interoperability Navigator**. You need to prepare the OS installation
	OceanStor-Pacific_8.2.1RC1_DPC.tar.gz	DPC client installation package of OceanStor Pacific series. For details about supported OS versions, visit **Huawei Storage Interoperability Navigator**.	
	OceanStor-Pacific_8.2.1RC1_DeviceManagerClient.zip	OceanStor Pacific series deployment tool, used for installing the OceanStor Pacific series software For details about supported OS and browser versions, visit **Huawei Storage Interoperability Navigator**.	
	• File service OS software package: **OceanStor-Pacific**_8.2.1RC1_**OS***xxx*.**SP***xx*_**aarch64.tgz** • For the names of third-party OS software, see the official website.	Storage node OS software package. For details about the package name, see *OceanStor Pacific Series 8.2.1RC1 Version Mapping*. If the version of the storage node file service OS software package does not meet the requirements in the version	

 Copyright © Huawei Technologies Co., Ltd.

Type	Name	Description	How to Obtain
		mapping, you need to reinstall the OS software package.	package by yourself.
	OceanStor-Pacific_8.2.1RC1_Tools.tar.gz	OceanStor Pacific series tool set, used to install the dependency packages of third-party OSs	
	OceanStor-Pacific_8.2.1RC1_Value-addedService.tar.gz	Data pilot service package, used to configure the SmartIndexing function	

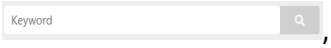
 Copyright © Huawei Technologies Co., Ltd.

Type	Name	Description	How to Obtain
Software digital signature validation tool	PGP Verify	To prevent a software package from being maliciously tampered with during transmission or storage, download the corresponding digital signature file for integrity verification when downloading the software package. After the software package is downloaded, verify its PGP digital signature according to *OpenPGP Signature Verification Guide*. If the software package fails the verification, do not use the software package, and contact Huawei technical support engineers. Before a software package is used in installation or upgrade, its digital signature also needs to be verified according to *OpenPGP Signature Verification Guide* to ensure that the software	For carrier users: **https://support.huawei.com/carrier/digitalSignatureAction** For enterprise users: **https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054**

 Copyright © Huawei Technologies Co., Ltd.

Type	Name	Description	How to Obtain
		package is not tampered with.	

Table 5-37 Device drivers and firmware

Type	Description	How to Obtain
Half-palm NVMe SSD, NVMe SSD card, NVMe SSD, and HDD drivers, firmware, and tools	For details about the firmware, driver, and tool versions used with the hardware, see *OceanStor Pacific Series 8.2.1RC1 Version Mapping*. If the device driver, firmware, and tool versions are earlier than those required in the version mapping, you need to upgrade them. If the device driver, firmware, and tool versions are later than those required in the version mapping, you need to reinstall them.	For details about the firmware, driver, and tool package names used with the hardware and how to obtain the packages, see *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.
IB and RoCE NIC drivers and firmware		
RAID controller card firmware and driver		
CLI tools of some RAID controller cards	For some RAID controller cards, a CLI tool needs to be installed for disk configuration and management. Query the models of the RAID controller cards where a CLI tool needs to be installed, as well as the name and version of the CLI tool from **Huawei Storage Interoperability Navigator**.	Obtain the CLI tool from the official website of the RAID controller card manufacturer. You can obtain the CLI tool as follows: 1. Log in to the official website of the RAID controller card manufacturer. 2. Enter the tool name in search box  , click the search icon, click **Management Software and Tools**, and then click the name of the tool to be downloaded in the **Title** column.

 Copyright © Huawei Technologies Co., Ltd.

Type	Description	How to Obtain
Node firmware	For details about the firmware version used with the node, see *OceanStor Pacific Series 8.2.1RC1 Version Mapping*. If the node firmware version does not meet the requirements in the version mapping, you need to upgrade the firmware.	For details about the firmware package name used with the node and how to obtain the package, see *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

5.4.2.5 Configuring Switches

5.4.2.5.1 Switch Configuration Requirements and Installation Data

Table 5-38 lists the switch configuration requirements.

Table 5-38 Switch configuration requirements

Type	Configuration Requirements
External management switch	Use the non-stacking mode. A VLAN needs to be configured for TCP/IP.

Table 5-39 describes the parameters used in the subsequent configuration. Replace the parameters according to the actual situation.

Table 5-39 Installation data

Type	Sub-type	Parameter	Remarks
External management switch	External management plane VLAN	manage-vlan	In the port parameters, a letter indicates only a digit. The actual port prevails.
	External management plane gateway	manage-ip	
	Subnet mask	Subnet mask or prefix	
	External management ports	*1/0/e* to *1/0/n*	

Copyright © Huawei Technologies Co., Ltd.

Type	Sub-type	Parameter	Remarks
	ETH-Trunk	manage-eth1 to manage-eth*n*	
	Uplink Eth-Trunk	up-eth	
	Uplink ports	1/0/*c* to 1/0/*d*	

5.4.2.5.2 Configuring GE External Management Switches

Context

Replace the italic parameters in the commands based on the site requirements. For details about the parameters, see **5.4.2.5.1 Switch Configuration Requirements and Installation Data**.

Procedure

Step 1 Log in to a switch. For details, see **5.5.2.1 Logging In to a Switch**.

Step 2 Configure a management network VLAN.

```
<HUAWEI> system-view
[~HUAWEI] vlan manage-vlan
[*HUAWEI-Vlanmanage-vlan] description management
[*HUAWEI-Vlanmanage-vlan] commit
[*HUAWEI-Vlanmanage-vlan] quit
```

Step 3 Configure a management network gateway.

NOTE

If the gateway has been configured, skip this step.

```
[*HUAWEI] interface vlanif manage-vlan
[*HUAWEI-Vlanmanage-vlan] ip address manage-ip Subnet mask
[*HUAWEI-Vlanmanage-vlan] commit
[*HUAWEI-Vlanmanage-vlan] quit
```

Step 4 Add the management ports on the switch to the port group.

```
[~HUAWEI] port-group 1
[~HUAWEI-port-group1] group-member ge 1/0/e to ge 1/0/n
[*HUAWEI-port-group1] port link-type trunk
[*HUAWEI-port-group1] port trunk pvid vlan manage-vlan  #Run this command only when no VLAN is configured for the management network ports of nodes.
[*HUAWEI-port-group1] undo port trunk allow-pass vlan 1
[*HUAWEI-port-group1] port trunk allow-pass vlan manage-vlan
[*HUAWEI-port-group1] commit
[~HUAWEI-port-group1] quit
[~HUAWEI]quit
<HUAWEI> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: Y
```

Step 5 (Optional) Configure uplink ports. Uplink ports must be configured only when the switch is connected to an upper-level switch.

```
[~HUAWEI] interface eth-trunk up-eth     # Configure the ports to work in trunk mode.
[*HUAWEI-Eth-Trunkup-eth] port link-type trunk
[*HUAWEI-Eth-Trunkup-eth] undo port trunk allow-pass vlan 1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-Eth-Trunkup-eth] port trunk allow-pass vlan manage-vlan
[*HUAWEI-Eth-Trunkup-eth] trunkport interface-type 1/0/c to 1/0/d
[*HUAWEI-Eth-Trunkup-eth] commit
[~HUAWEI-Eth-Trunkup-eth] quit
[~HUAWEI]quit
<HUAWEI> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: Y
```

Step 6 Run the **display current-configuration** command to check the related configuration in sequence.

----End

5.4.2.5.3 Configuring 25GE External Management Switches (Applicable to CE6865)

Context

Replace the italic parameters in the commands based on the site requirements. For details about the parameters, see **5.4.2.5.1 Switch Configuration Requirements and Installation Data**.

Procedure

NOTE

- This section uses V200R021C00 as an example. If you encounter compatibility issues when running commands for other versions, see the product documentation of the desired switch version. For enterprise users, **click here**. For carrier users, **click here**.
- Replace the contents in italic based on site requirements.

Step 1 Log in to a switch. For details, see **5.5.2.1 Logging In to a Switch**.

Step 2 Configure the IP address of the management network port on a switch.

To configure an IPv4 address, run the following commands:

```
<HUAWEI> system-view
[~HUAWEI] interface meth 0/0/0
[~HUAWEI-MEth0/0/0] ip address Management IP address of the switch Subnet mask
[*HUAWEI-MEth0/0/0] commit
[~HUAWEI-MEth0/0/0] quit
Warning: The current configuration will be written to the device. Continue? [Y/N]: Y
```

Step 3 Configure a VLAN for the external management network.

```
[~HUAWEI] vlan manage-vlan
[*HUAWEI-Vlanmanage-vlan] description SFS_OM_SFS_TOR
[*HUAWEI-Vlanmanage-vlan] commit
[~HUAWEI-Vlanmanage-vlan] quit
```

Step 4 Configure a gateway of the external management network.

```
[~HUAWEI] interface vlanif manage-vlan
[*HUAWEI-Vlanmanage-vlan] ip address manage-ip Subnet mask
[*HUAWEI-Vlanmanage-vlan] arp timeout 60
[*HUAWEI-Vlanmanage-vlan] arp proxy anyway enable
[*HUAWEI-Vlanmanage-vlan] mac-address 0000-5e00-0101 #The virtual MAC address range is
0000-5e00-0101 to 0000-5e00-01fe. 0000-5e00-0101 is recommended.
[*HUAWEI-Vlanmanage-vlan] arp delete trigger link-down enable
[*HUAWEI-Vlanmanage-vlan] arp direct-route enable
[*HUAWEI-Vlanmanage-vlan] arp direct-route preference 1
[*HUAWEI-Vlanmanage-vlan] commit
[~HUAWEI-Vlanmanage-vlan] quit
```

Step 5 Configure Ethernet link aggregation on the external management network and add member interfaces to the Eth-Trunk.

 Copyright © Huawei Technologies Co., Ltd.

```
[~HUAWEI] interface eth-trunk manage-eth1
[*HUAWEI-Eth-Trunkmanage-eth1] mode lacp-dynamic
[*HUAWEI-Eth-Trunkmanage-eth1] lacp timeout fast
[*HUAWEI-Eth-Trunkmanage-eth1] lacp port-id-extension enable
[*HUAWEI-Eth-Trunkmanage-eth1] trunkport 25ge 1/0/e    #Determine the port based on the NIC type and the number of bonded network ports.
[*HUAWEI-Eth-Trunkmanage-eth1] commit
[~HUAWEI-Eth-Trunkmanage-eth1] quit
...#Repeat the preceding operations to add other Eth-Trunk interfaces.
[~HUAWEI] interface eth-trunk manage-ethn
[*HUAWEI-Eth-Trunkmanage-ethn] mode lacp-dynamic
[*HUAWEI-Eth-Trunkmanage-ethn] lacp timeout fast
[*HUAWEI-Eth-Trunkmanage-ethn] lacp port-id-extension enable
[*HUAWEI-Eth-Trunkmanage-ethn] trunkport 25ge 1/0/n    #Determine the port based on the NIC type and the number of bonded network ports.
[*HUAWEI-Eth-Trunkmanage-ethn] commit
[~HUAWEI-Eth-Trunkmanage-ethn] quit
```

Step 6 Add the VLANs planned for the external management network to each group of ports.

```
[~HUAWEI] interface eth-trunk manage-eth1    /*manage-eth1 is an Ethernet link aggregation port.*/
[*HUAWEI-Eth-Trunkmanage-eth1] port link-type trunk
[*HUAWEI-Eth-Trunkmanage-eth1] undo port trunk allow-pass vlan 1
[*HUAWEI-Eth-Trunkmanage-eth1] port trunk allow-pass vlan manage-vlan  /*manage-vlan is the VLAN ID.*/
[*HUAWEI-Eth-Trunkmanage-eth1] commit
[~HUAWEI-Eth-Trunkmanage-eth1] quit
...#Repeat the preceding operations to add a VLAN to each group of interfaces.
[~HUAWEI] interface eth-trunk manage-ethn   /*manage-eth is an Ethernet link aggregation port.*/
[*HUAWEI-Eth-Trunkmanage-ethn] port link-type trunk
[*HUAWEI-Eth-Trunkmanage-ethn] undo port trunk allow-pass vlan 1
[*HUAWEI-Eth-Trunkmanage-ethn] port trunk allow-pass vlan manage-vlan /*manage-vlan is the VLAN ID.*/
[*HUAWEI-Eth-Trunkmanage-ethn] commit
[~HUAWEI-Eth-Trunkmanage-ethn] quit
```

Step 7 (Optional) Configure uplink ports. Uplink ports must be configured only when the switch is connected to an upper-level switch.

```
[~HUAWEI] interface eth-trunk up-eth
[*HUAWEI-Eth-Trunkup-eth] undo portswitch
[*HUAWEI-Eth-Trunkup-eth] mode lacp-static
[*HUAWEI-Eth-Trunkup-eth] ip address Management IP address of the uplink switch Subnet mask
[*HUAWEI-Eth-Trunkup-eth] trunkport 100ge 1/0/c to 1/0/d
[*HUAWEI-Eth-Trunkup-eth] commit
[~HUAWEI-Eth-Trunkup-eth] quit
[~HUAWEI] quit
<HUAWEI> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: Y
```

Step 8 Run the **display current-configuration** command to check the related configuration in sequence.

----End

5.4.2.5.4 Configuring 100GE External Management Switches (Applicable to CE8850)

Context

Replace the italic parameters in the commands based on the site requirements. For details about the parameters, see **5.4.2.5.1 Switch Configuration Requirements and Installation Data**.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

NOTE

- This section uses V200R021C00 as an example. If you encounter compatibility issues when running commands for other versions, see the product documentation of the desired switch version. For enterprise users, **click here**. For carrier users, **click here**.
- Replace the contents in italic based on site requirements.

Step 1 Log in to a switch. For details, see **5.5.2.1 Logging In to a Switch**.

Step 2 Configure the IP address of the management network port on a switch.

To configure an IPv4 address, run the following commands:

```
<HUAWEI> system-view
[~HUAWEI] interface meth 0/0/0
[~HUAWEI-MEth0/0/0] ip address Management IP address of the switch Subnet mask
[*HUAWEI-MEth0/0/0] commit
[~HUAWEI-MEth0/0/0] quit
Warning: The current configuration will be written to the device. Continue? [Y/N]: Y
```

Step 3 Configure a VLAN for the external management network.

```
[~HUAWEI] vlan manage-vlan
[*HUAWEI-Vlanmanage-vlan] description SFS_OM_SFS_TOR
[*HUAWEI-Vlanmanage-vlan] commit
[~HUAWEI-Vlanmanage-vlan] quit
```

Step 4 Configure a gateway of the external management network.

```
[~HUAWEI] interface vlanif manage-vlan
[*HUAWEI-Vlanmanage-vlan] ip address manage-ip Subnet mask
[*HUAWEI-Vlanmanage-vlan] arp timeout 60
[*HUAWEI-Vlanmanage-vlan] arp proxy anyway enable
[*HUAWEI-Vlanmanage-vlan] mac-address 0000-5e00-0101 #The virtual MAC address range is
0000-5e00-0101 to 0000-5e00-01fe. 0000-5e00-0101 is recommended.
[*HUAWEI-Vlanmanage-vlan] arp delete trigger link-down enable
[*HUAWEI-Vlanmanage-vlan] arp direct-route enable
[*HUAWEI-Vlanmanage-vlan] arp direct-route preference 1
[*HUAWEI-Vlanmanage-vlan] commit
[~HUAWEI-Vlanmanage-vlan] quit
```

Step 5 Configure Ethernet link aggregation on the external management network and add member interfaces to the Eth-Trunk.

```
[~HUAWEI] interface eth-trunk manage-eth1
[*HUAWEI-Eth-Trunkmanage-eth1] mode lacp-dynamic
[*HUAWEI-Eth-Trunkmanage-eth1] lacp timeout fast
[*HUAWEI-Eth-Trunkmanage-eth1] lacp port-id-extension enable
[*HUAWEI-Eth-Trunkmanage-eth1] trunkport 100ge 1/0/e    #Determine the port based on the NIC type
and the number of bonded network ports.
[*HUAWEI-Eth-Trunkmanage-eth1] commit
[~HUAWEI-Eth-Trunkmanage-eth1] quit
...#Repeat the preceding operations to add other Eth-Trunk interfaces.
[~HUAWEI] interface eth-trunk manage-ethn
[*HUAWEI-Eth-Trunkmanage-ethn] mode lacp-dynamic
[*HUAWEI-Eth-Trunkmanage-ethn] lacp timeout fast
[*HUAWEI-Eth-Trunkmanage-ethn] lacp port-id-extension enable
[*HUAWEI-Eth-Trunkmanage-ethn] trunkport 100ge 1/0/n    #Determine the port based on the NIC type
and the number of bonded network ports.
[*HUAWEI-Eth-Trunkmanage-ethn] commit
[~HUAWEI-Eth-Trunkmanage-ethn] quit
```

Step 6 Add the VLANs planned for the external management network to each group of ports.

```
[~HUAWEI] interface eth-trunk manage-eth1    /*manage-eth1 is an Ethernet link aggregation port.*/
[*HUAWEI-Eth-Trunkmanage-eth1] port link-type trunk
[*HUAWEI-Eth-Trunkmanage-eth1] undo port trunk allow-pass vlan 1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-Eth-Trunkmanage-eth1] port trunk allow-pass vlan manage-vlan  /*manage-vlan is the VLAN ID.*/
[*HUAWEI-Eth-Trunkmanage-eth1] commit
[~HUAWEI-Eth-Trunkmanage-eth1] quit
...#Repeat the preceding operations to add a VLAN to each group of interfaces.
[~HUAWEI] interface eth-trunk manage-ethn   /*manage-eth is an Ethernet link aggregation port.*/
[*HUAWEI-Eth-Trunkmanage-ethn] port link-type trunk
[*HUAWEI-Eth-Trunkmanage-ethn] undo port trunk allow-pass vlan 1
[*HUAWEI-Eth-Trunkmanage-ethn] port trunk allow-pass vlan manage-vlan /*manage-vlan is the VLAN ID.*/
[*HUAWEI-Eth-Trunkmanage-ethn] commit
[~HUAWEI-Eth-Trunkmanage-ethn] quit
```

Step 7 (Optional) Configure uplink ports. Uplink ports must be configured only when the switch is connected to an upper-level switch.

```
[~HUAWEI] interface eth-trunk up-eth
[*HUAWEI-Eth-Trunkup-eth] undo portswitch
[*HUAWEI-Eth-Trunkup-eth] mode lacp-static
[*HUAWEI-Eth-Trunkup-eth] ip address Management IP address of the uplink switch Subnet mask
[*HUAWEI-Eth-Trunkup-eth] trunkport 100ge 1/0/c to 1/0/d
[*HUAWEI-Eth-Trunkup-eth] commit
[~HUAWEI-Eth-Trunkup-eth] quit
[~HUAWEI] quit
<HUAWEI> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: Y
```

Step 8 Run the **display current-configuration** command to check the related configuration in sequence.

----End

5.4.2.6 Installation Procedure (Applicable to LLD-based Configuration)

5.4.2.6.1 Initializing Nodes Using SmartKit

5.4.2.6.1.1 Preparing the Deployment File Template and SmartKit

Context

This section describes how to prepare the LLD configuration file, download and install the SmartKit tool, and go to the main page of the tool for initializing nodes.

Procedure

Step 1 Obtain the deployment file template. If you have obtained it, skip this step.

Use LLDesigner to prepare the deployment file template. For details, see section "LLD Planning and Implementation" in *OceanStor Pacific Series 8.2.1 Network Planning Guide (SFS)*.

Step 2 Download and install SmartKit.

- For enterprise users: Log in to **https://support.huawei.com/enterprise**, enter **SmartKit** in the search box, and select **Distributed Storage > Tools and Platform > SmartKit** from the suggested paths. The SmartKit page is displayed.
  a. On the SmartKit page, click **Software Download**, and select and download SmartKit of the latest version according to the publication date.

 Copyright © Huawei Technologies Co., Ltd.

b. On the SmartKit page, click **Documentation**, find *SmartKit User Guide* of the desired version, and install and run SmartKit respectively by following the instructions provided in sections "Installing SmartKit" and "Running SmartKit".

- For carrier users: Log in to **https://support.huawei.com**, enter **SmartKit** in the search box, and select **Carrier IT > Data Storage > Storage Common > SmartKit** from the suggested paths. The SmartKit page is displayed.

  a. On the SmartKit page, click **Software**, and select and download SmartKit of the latest version according to the release date.

  b. On the SmartKit page, click **Product Documentation**, find *SmartKit User Guide* of the desired version, and install and run SmartKit respectively by following the instructions provided in sections "Installing SmartKit" and "Running SmartKit".

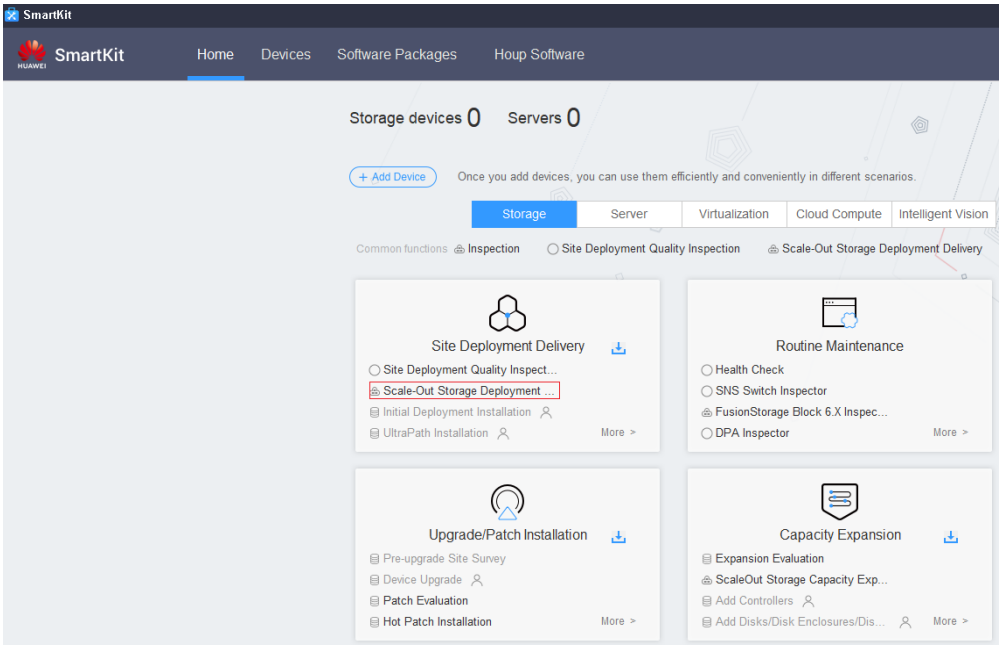
Step 3 Install the Scale-Out Storage Deployment Delivery tool by referring to section "Installing Functions" in *SmartKit User Guide*.

Step 4 Go to the **Site Deployment Delivery** page.

NOTE

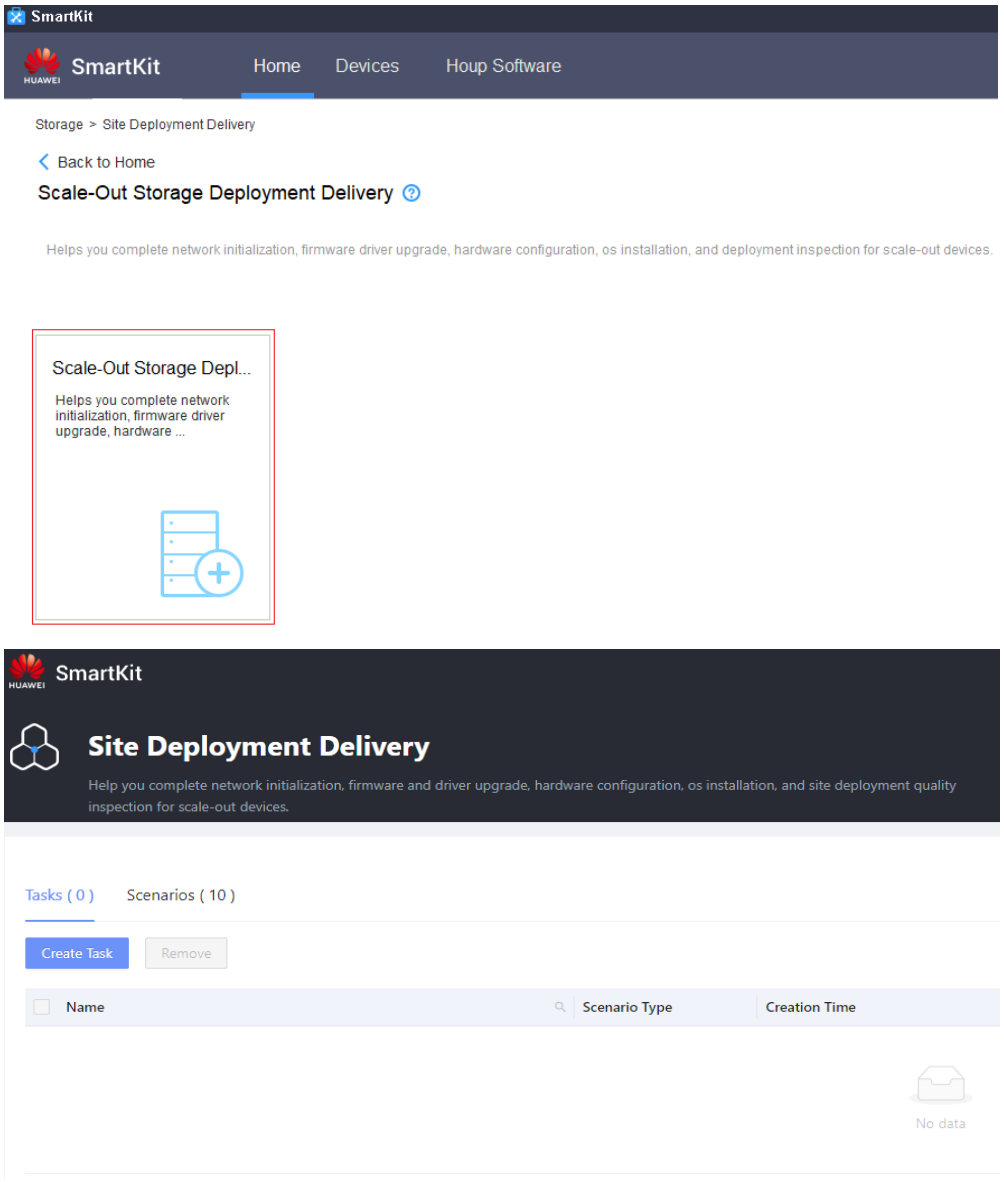
The GUI of SmartKit may vary with the version.

1. On the home page of SmartKit, choose **Site Deployment Delivery** > **Scale-Out Storage Deployment Delivery**. The **Scale-Out Storage Deployment Delivery** page is displayed.



2. On the **Scale-Out Storage Deployment Delivery** page, click **Scale-Out Storage Deployment Delivery**. The **Site Deployment Delivery** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



----End

5.4.2.6.1.2 Configuring iBMC IP Addresses for Nodes

?.1. Configuring iBMC IP Addresses for Nodes in Batches

Context

This section describes how to use SmartKit to batch configure iBMC IP addresses for nodes by node SN or chassis SN.

If the node name is specified when the LLD configuration file is prepared, the node name will be automatically configured when an iBMC IP address is configured. If an OceanStor Pacific 9950 device exists, you also need to configure the management IP addresses of its data cluster modules and the system will automatically change the passwords of the data cluster modules.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The GUI of SmartKit may vary with the version.

Prerequisites

- If the storage software has been installed on the nodes to be deployed, uninstall the storage software by referring to **5.5.19 Uninstalling OceanStor Pacific Series Software**, clear the network and route information configured on the nodes, and then initialize the nodes using SmartKit.
- When using LLDesigner to prepare an LLD configuration file, you need to enter the node SN or enclosure SN.

Procedure

- If no OceanStor Pacific 9950 device exists in the cluster, configure iBMC IP addresses by referring to **Scenario 1**.
- If an OceanStor Pacific 9950 device exists in the cluster:

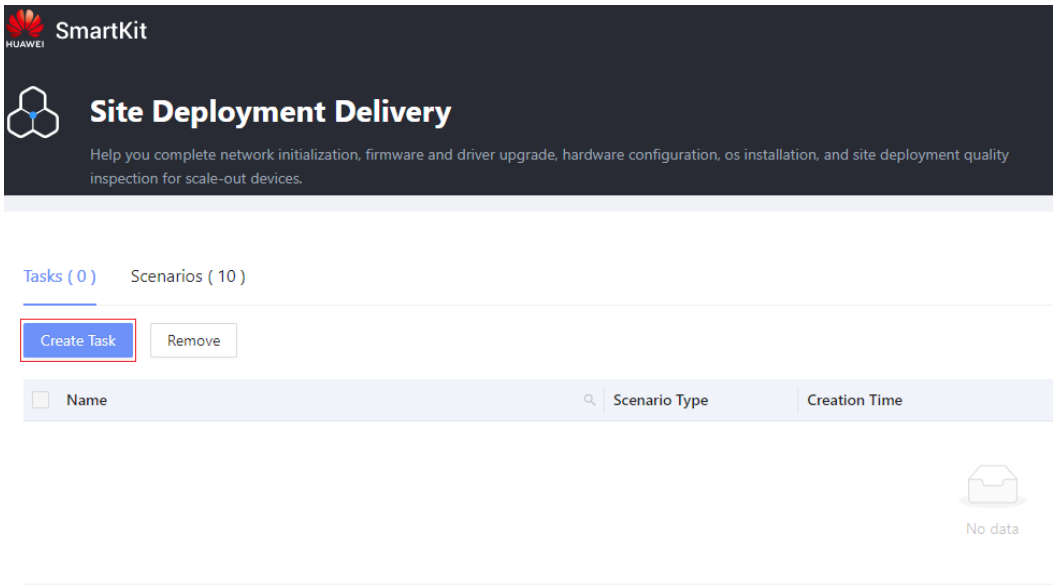
  Data cluster modules provide the back-end network switching function for OceanStor Pacific 9950 scale-out storage clusters. A data cluster module connects to a storage device and detects the hardware of the storage device. When it detects a risk, it reports an alarm. You can view alarms reported by the data cluster module on DeviceManager. Management IP addresses must be configured for the data cluster modules on the OceanStor Pacific 9950 device, and the management IP addresses of the data cluster modules must be able to communicate with the management network.

  - If the management network can communicate with the iBMC network, you only need to connect the installation PC to the iBMC switch, and configure the management IP addresses and iBMC IP addresses of the data cluster modules at the same time. For details, see **Scenario 1**.
  - If the management network cannot communicate with the iBMC network, you need to connect the installation PC to the management switch and iBMC switch, and configure the management IP addresses and iBMC IP addresses of the data cluster modules separately. For details, see **Scenario 2**.

Scenario 1

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

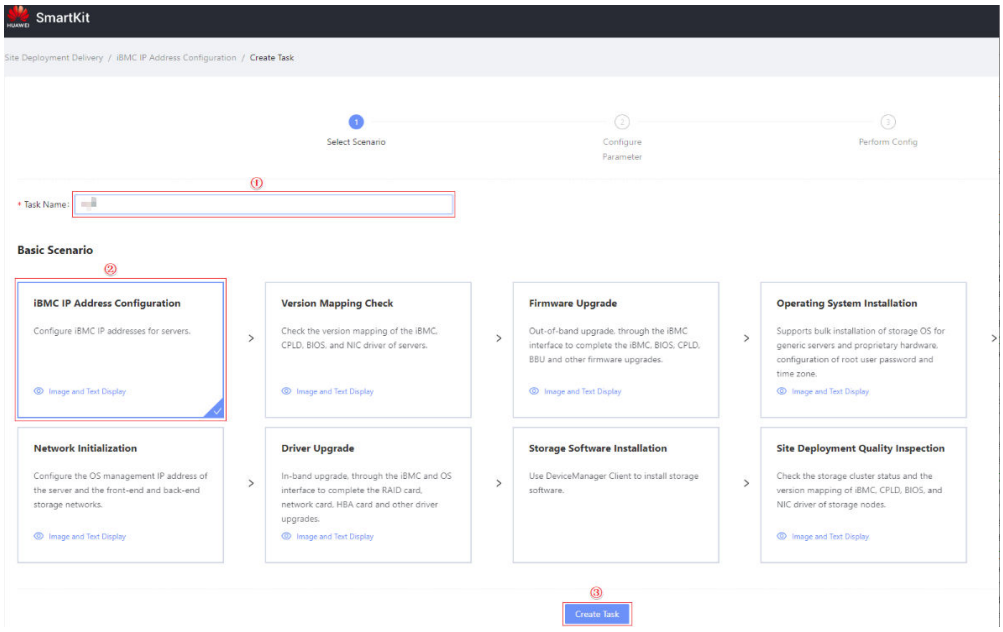


Step 2 Select an iBMC IP address configuration scenario.

1. Set **Task Name**, select **iBMC IP Address Configuration**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).



2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

   NOTE

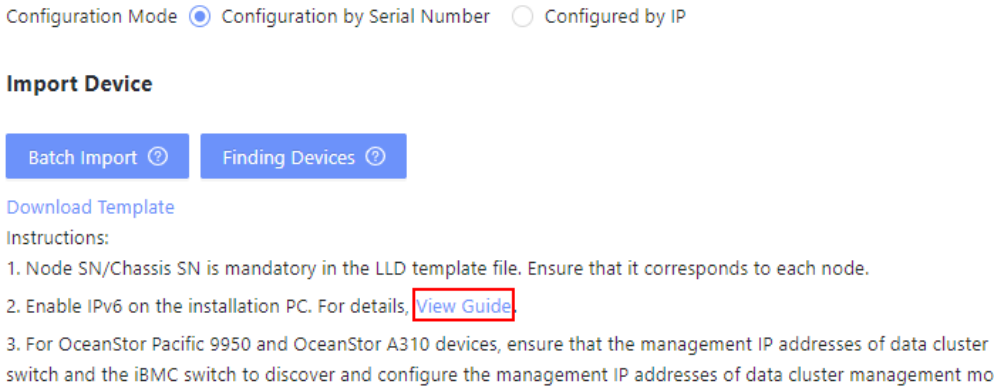
   If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

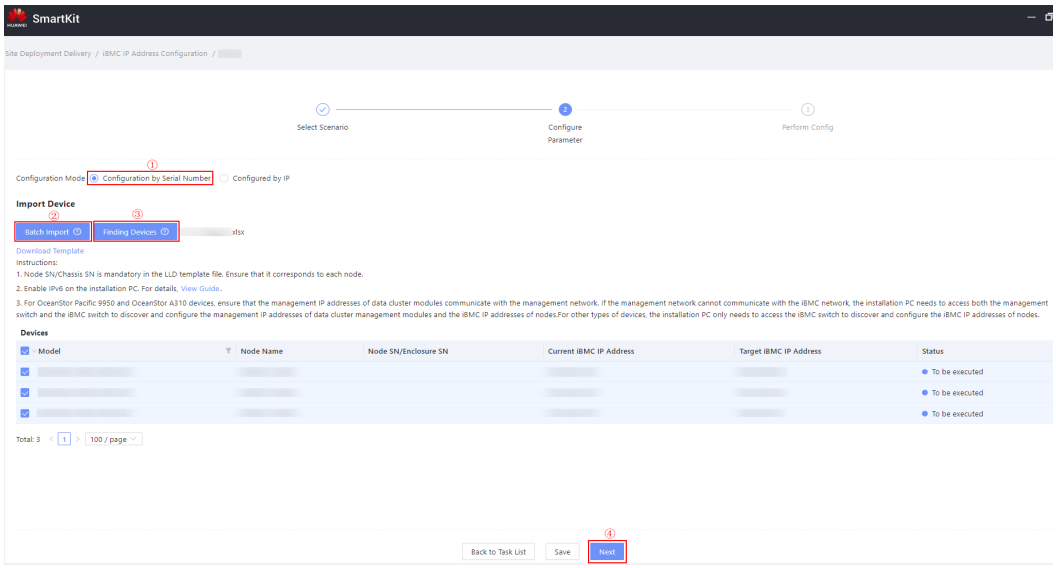
 Copyright © Huawei Technologies Co., Ltd.

Step 3 Configure parameters.

NOTE

- The installation PC must be connected to an iBMC switch.
- The IPv6 function must be enabled on the installation PC. For details, click **View Guide** under **Usage Notes** in the following figure.





1. Set **Configuration Mode** to **Configuration by Serial Number**.
2. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.
3. Click **Finding Devices**. The system will discover the current iBMC IP addresses of the nodes by SN. After the discovery is complete, view the discovery result in the **Status** column.

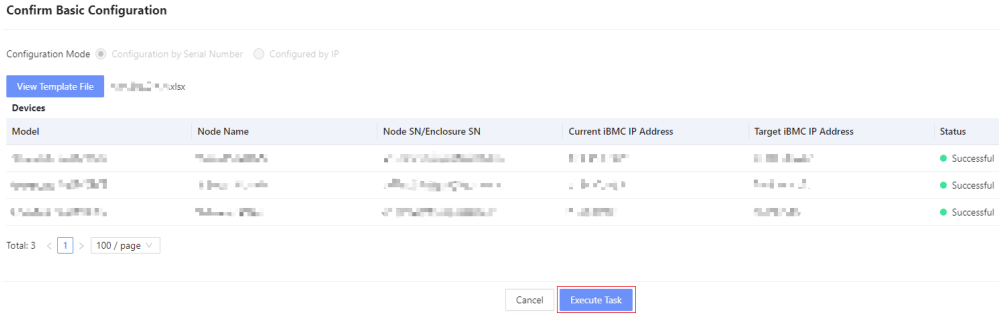
   NOTE

   - If the discovery is successful, the system will update the current iBMC IP addresses of the discovered nodes to the **Current iBMC IP Address** column.
   - If the discovery fails, click **View Guide** under **Usage Notes**, rectify the fault according to the guide, and click **Finding Devices** again.
4. Click **Next**.

Step 4 Perform the configuration.

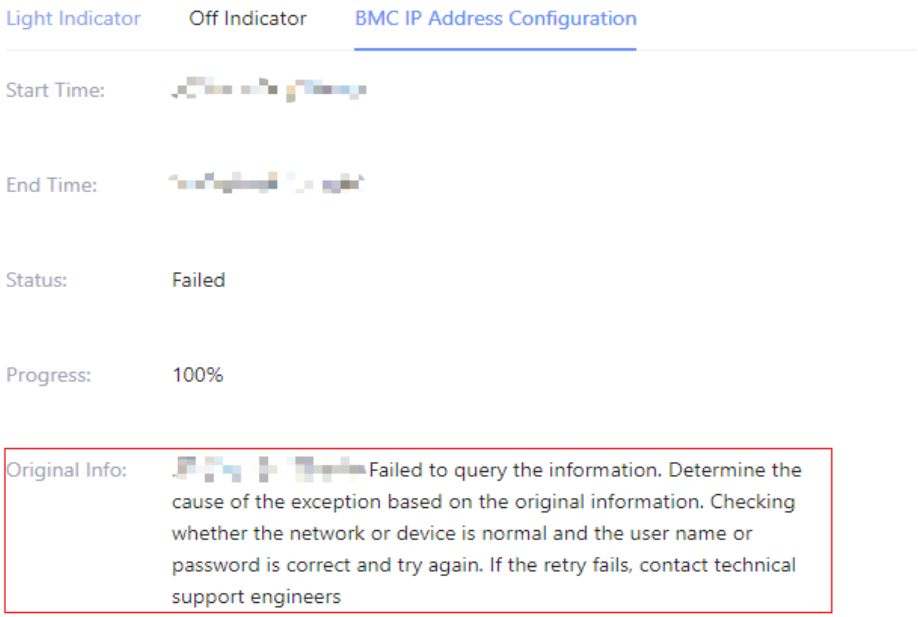
 Copyright © Huawei Technologies Co., Ltd.

1. Click **View Template File**. The imported LLD configuration file will be automatically opened. Confirm the information to be configured. After confirming that the information is correct, click **Execute Task**.



2. After the configuration is complete, view the configuration results of all nodes in the **Configuration Status** column.

   If **Config failed** is displayed in the **Configuration Status** column, click **Details** in the **Operation** column. Click the **BMC IP Address Configuration** tab, and rectify the fault based on the information in **Original Info**. The following is an example:



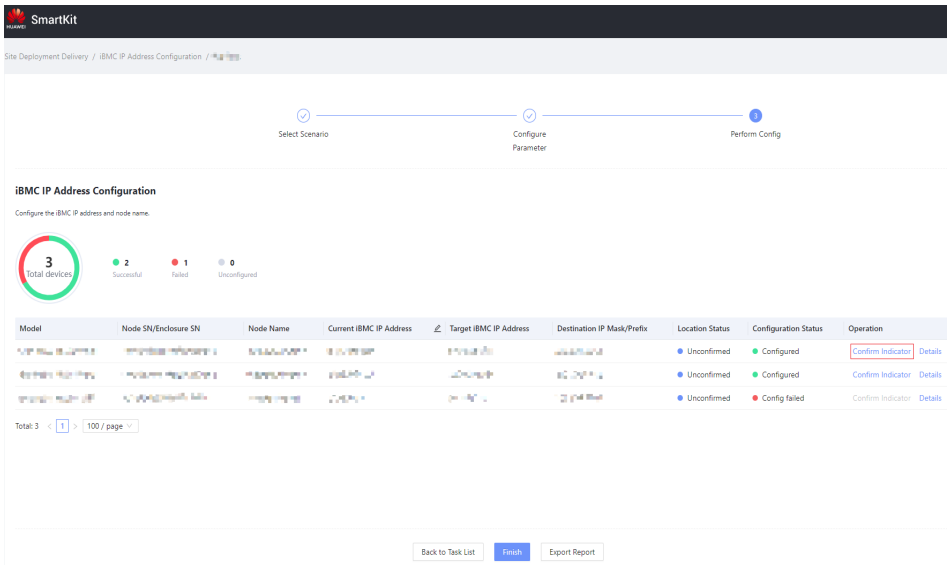
   NOTE

   You can also click **Export Report** in the lower part to collect and view the configuration results of all nodes.

3. Confirm indicators.

   Click **Confirm Indicator** in the **Operation** column corresponding to each IP address.

 Copyright © Huawei Technologies Co., Ltd.



NOTE

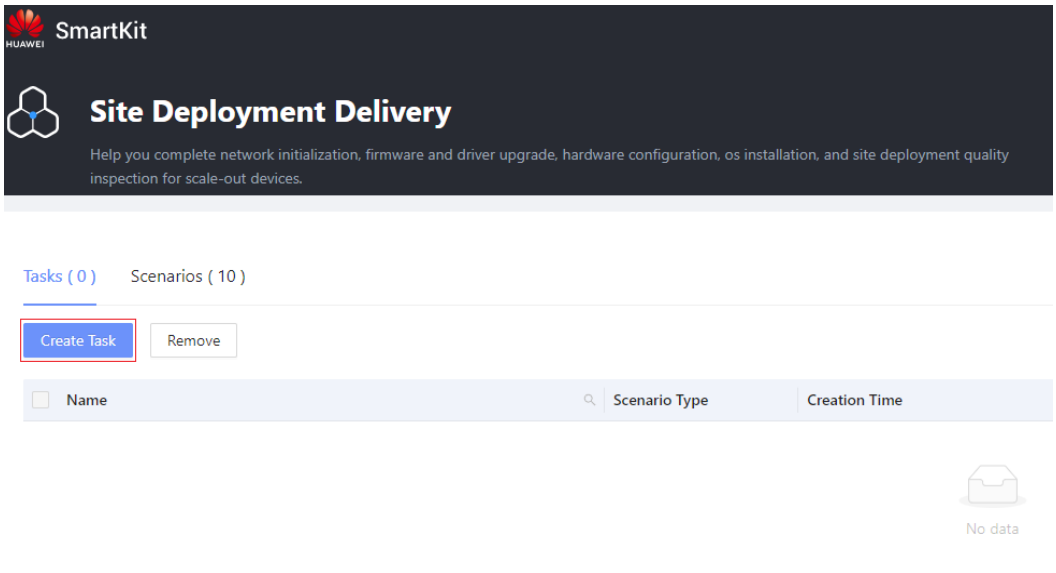
- For details about the positions of device location indicators, see **Appendix** > **Indicators and Buttons** in *OceanStor Pacific Series 8.2.1 Hardware Installation Guide*.
- If the location indicator of the corresponding device is on, the configuration is successful. In the **Confirm Indicator** dialog box that is displayed, click **Correct**. The location indicator will be automatically turned off.
- If the location indicator status is not as expected, re-plan the iBMC IP addresses and configure them from the beginning. If the fault persists, contact Huawei technical support engineers.

4. Click **Finish**.

----End

Scenario 2

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.



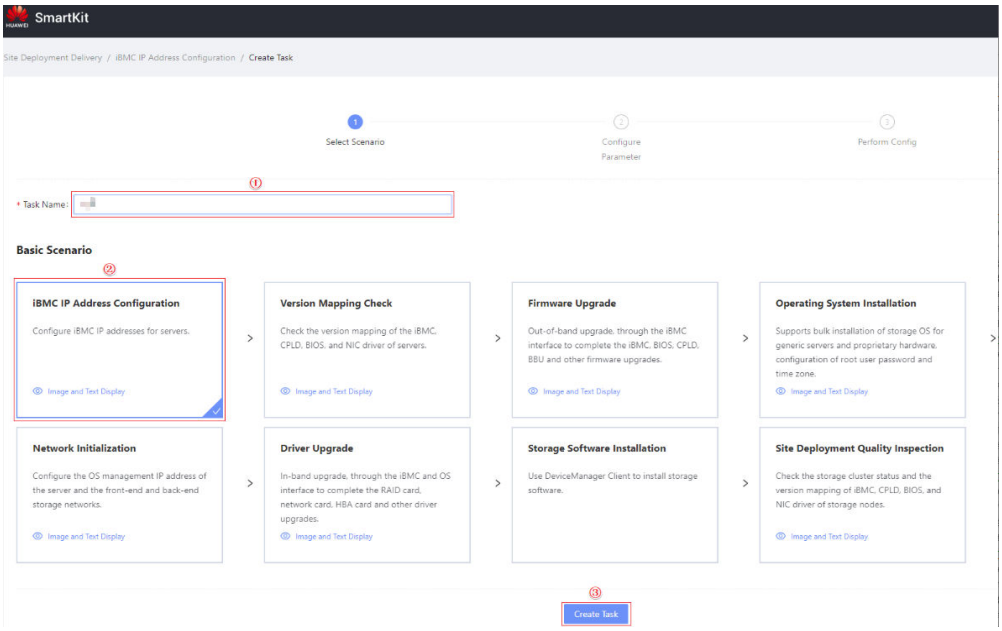
 Copyright © Huawei Technologies Co., Ltd.

Step 2 Select an iBMC IP address configuration scenario.

1. Set **Task Name**, select **iBMC IP Address Configuration**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).



2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

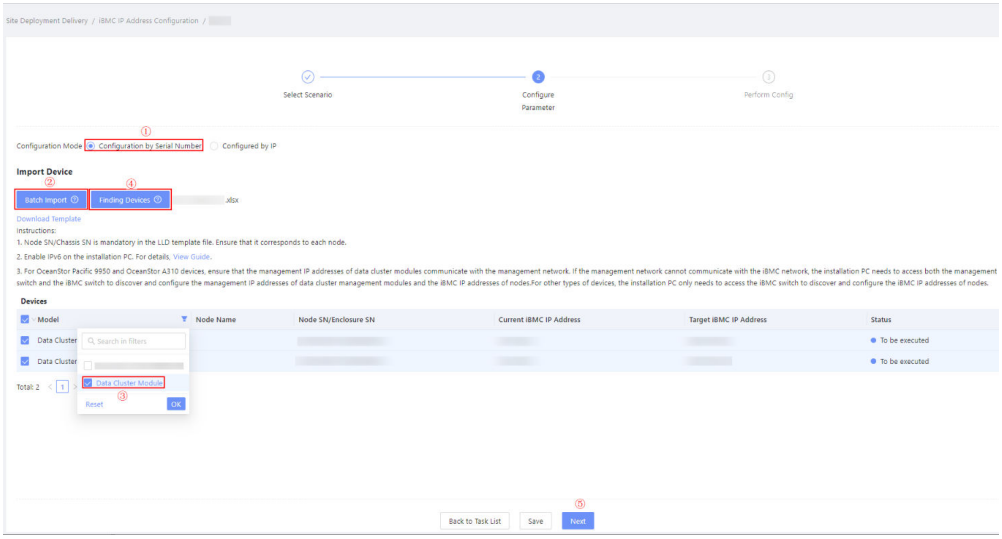
   NOTE

   If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

Step 3 Configure management IP addresses for data cluster modules.

1. Connect the installation PC to the management switch.
2. Configure parameters.

 Copyright © Huawei Technologies Co., Ltd.



a. Set **Configuration Mode** to **Configuration by Serial Number**.

b. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.

c. In the **Model** drop-down list, select **Data Cluster Module** (that is, select all data cluster modules).

d. Click **Finding Devices**. The system will discover the current management IP addresses of the data cluster modules by SN. After the discovery is complete, view the discovery result in the **Status** column.

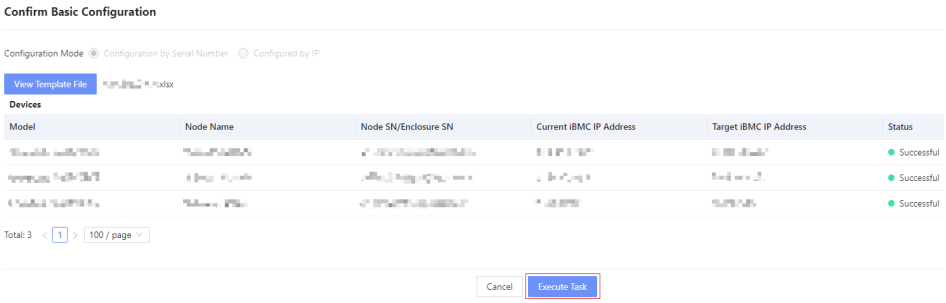
NOTE

- If the discovery is successful, the system will update the current management IP addresses of the discovered data cluster modules to the **Current iBMC IP Address** column.
- If the discovery fails, click **View Guide** under **Usage Notes**, rectify the fault according to the guide, and click **Finding Devices** again.

e. Click **Next**.

3. Execute the task.

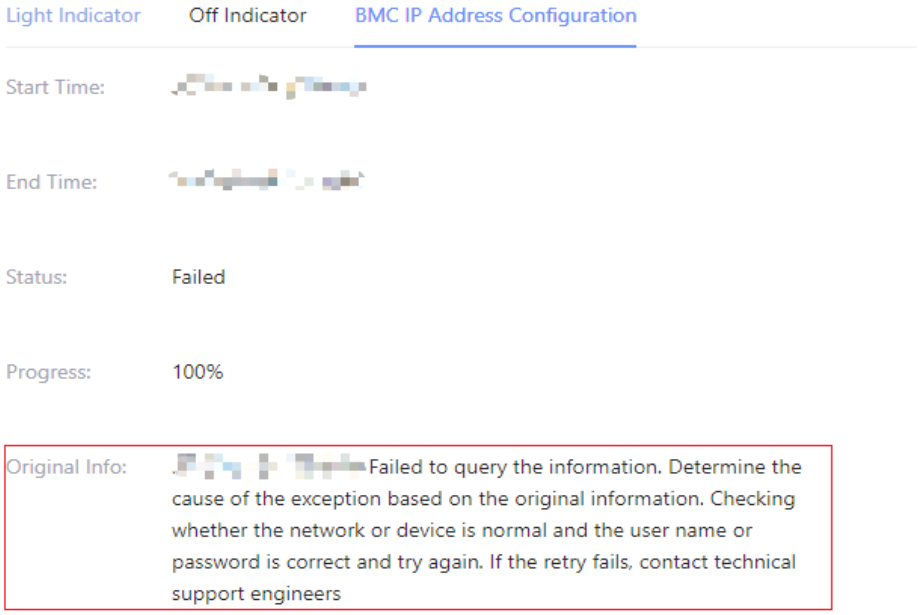
a. Click **View Template File**. The imported LLD configuration file will be automatically opened. Confirm the information to be configured. After confirming that the information is correct, click **Execute Task**.



b. After the configuration is complete, view the configuration results of all nodes in the **Configuration Status** column.

 Copyright © Huawei Technologies Co., Ltd.

If **Config failed** is displayed in the **Configuration Status** column, click **Details** in the **Operation** column. Click the **BMC IP Address Configuration** tab, and rectify the fault based on the information in **Original Info**. The following is an example:

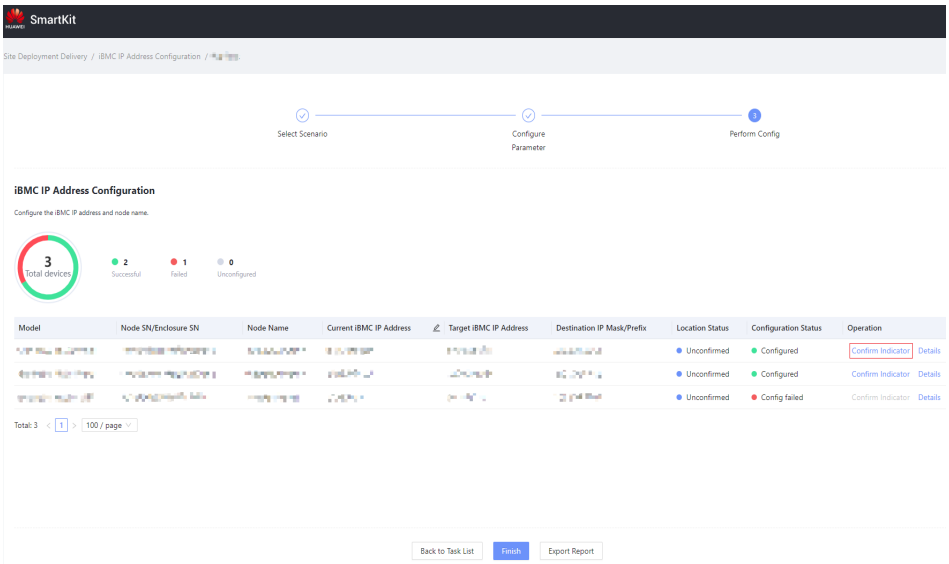


NOTE

You can also click **Export Report** in the lower part to collect and view the configuration results of all nodes.

4. Confirm indicators.

   Click **Confirm Indicator** in the **Operation** column corresponding to each IP address.



 Copyright © Huawei Technologies Co., Ltd.

NOTE

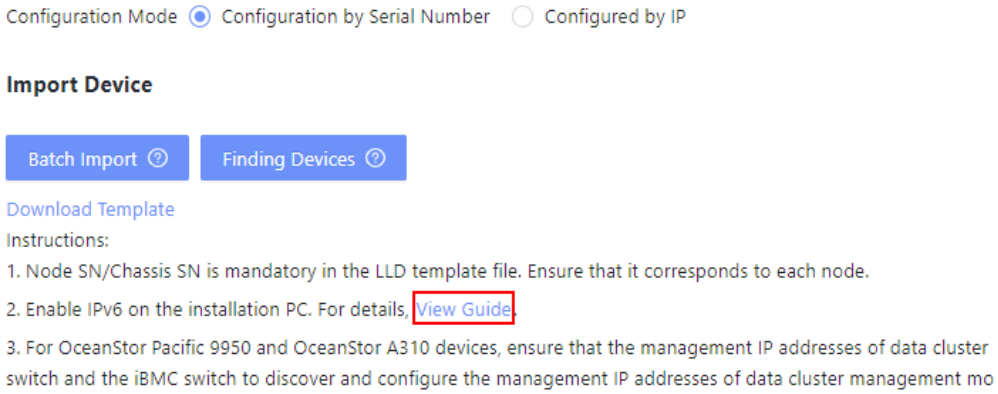
- For details about the positions of device location indicators, see **Appendix** > **Indicators and Buttons** in *OceanStor Pacific Series 8.2.1 Hardware Installation Guide*.
- If the location indicator of the corresponding device is on, the configuration is successful. In the **Confirm Indicator** dialog box that is displayed, click **Correct**. The location indicator will be automatically turned off.
- If the location indicator status is not as expected, re-plan the iBMC IP addresses and configure them from the beginning. If the fault persists, contact Huawei technical support engineers.

Step 4 Configure iBMC IP addresses for nodes.

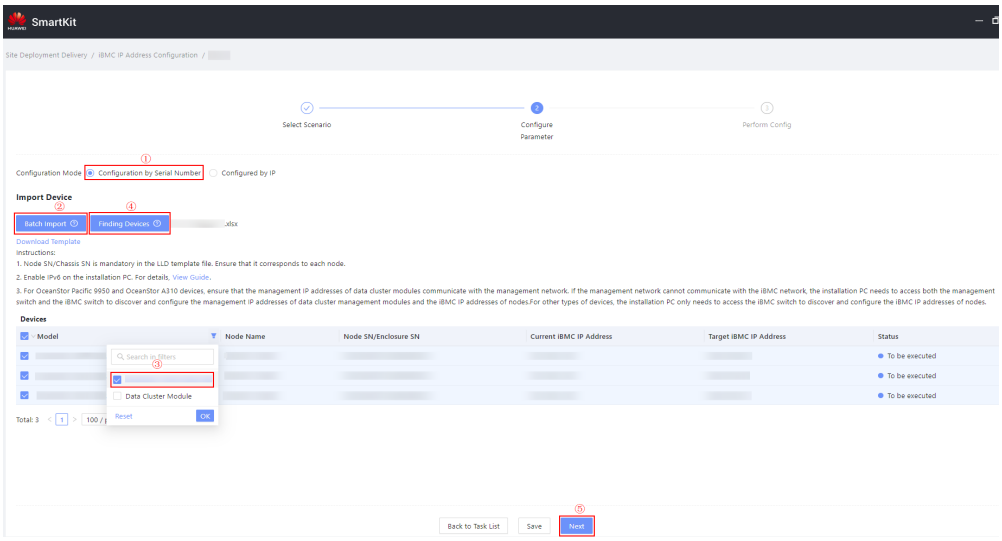
1. Connect the installation PC to the iBMC switch.

   NOTE

   The IPv6 function must be enabled on the installation PC. For details, click **View Guide** under **Usage Notes** in the following figure.

2. Configure parameters.

   a. Set **Configuration Mode** to **Configuration by Serial Number**.

   b. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.

 Copyright © Huawei Technologies Co., Ltd.

c. In the **Model** drop-down list, select the device models of all nodes for which iBMC IP addresses are to be configured.

d. Click **Finding Devices**. The system will discover the current iBMC IP addresses of the nodes by SN. After the discovery is complete, view the discovery result in the **Status** column.

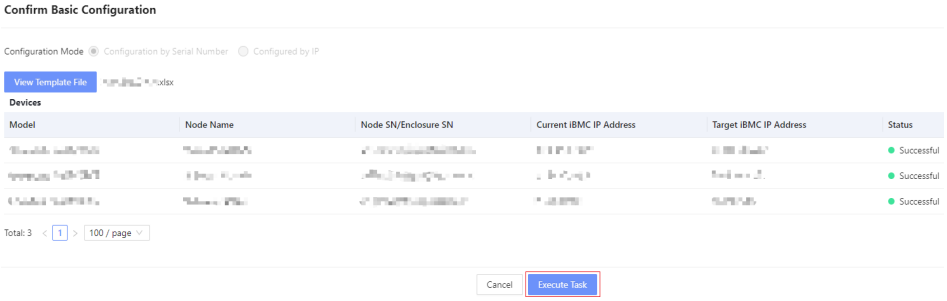
NOTE

- If the discovery is successful, the system will update the current iBMC IP addresses of the discovered nodes to the **Current iBMC IP Address** column.
- If the discovery fails, click **View Guide** under **Usage Notes**, rectify the fault according to the guide, and click **Finding Devices** again.

e. Click **Next**.

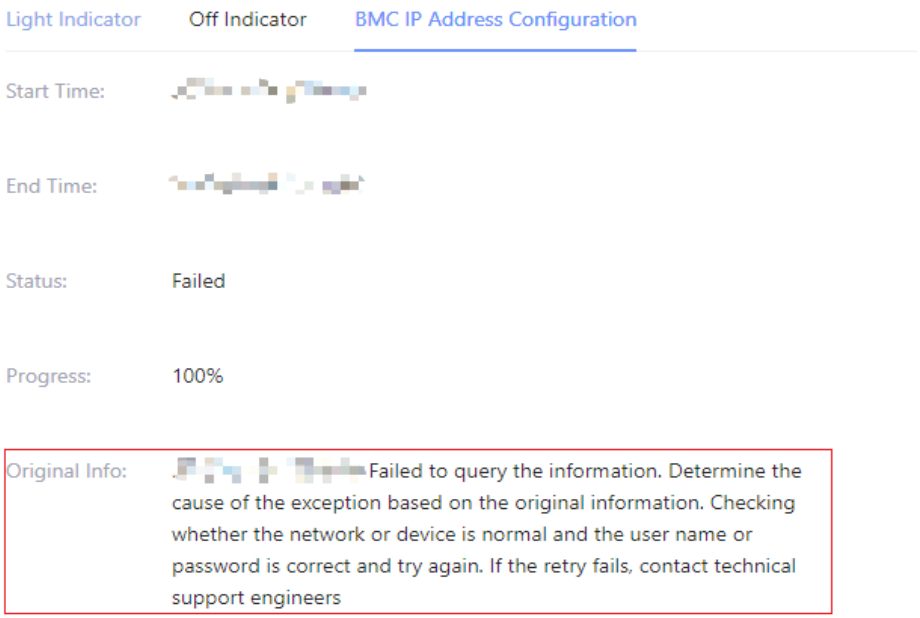
3. Execute the task.

a. Click **View Template File**. The imported LLD configuration file will be automatically opened. Confirm the information to be configured. After confirming that the information is correct, click **Execute Task**.



b. After the configuration is complete, view the configuration results of all nodes in the **Configuration Status** column.

If **Config failed** is displayed in the **Configuration Status** column, click **Details** in the **Operation** column. Click the **BMC IP Address Configuration** tab, and rectify the fault based on the information in **Original Info**. The following is an example:



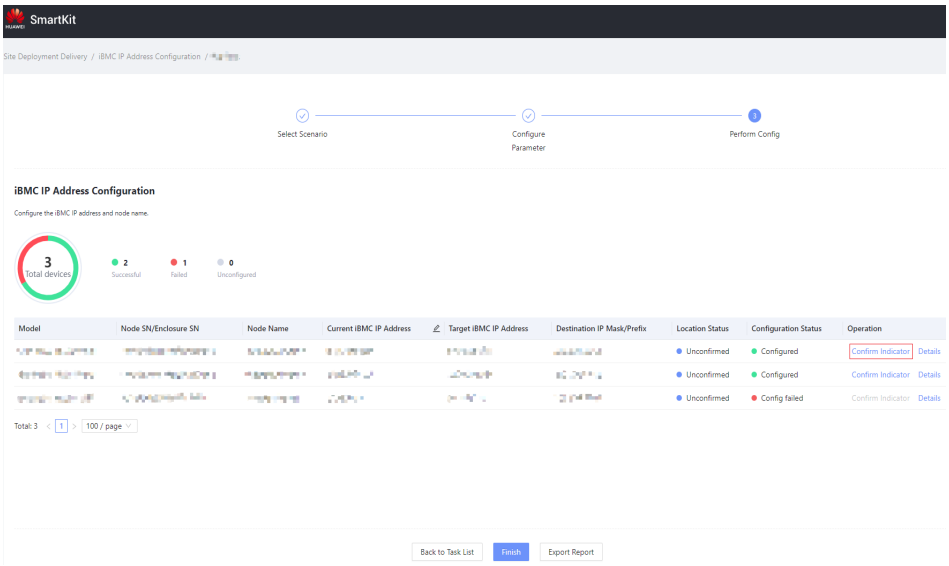
 Copyright © Huawei Technologies Co., Ltd.

NOTE

You can also click **Export Report** in the lower part to collect and view the configuration results of all nodes.

4. Confirm indicators.

   Click **Confirm Indicator** in the **Operation** column corresponding to each IP address.



NOTE

- For details about the positions of device location indicators, see **Appendix** > **Indicators and Buttons** in *OceanStor Pacific Series 8.2.1 Hardware Installation Guide*.
- If the location indicator of the corresponding device is on, the configuration is successful. In the **Confirm Indicator** dialog box that is displayed, click **Correct**. The location indicator will be automatically turned off.
- If the location indicator status is not as expected, re-plan the iBMC IP addresses and configure them from the beginning. If the fault persists, contact Huawei technical support engineers.

----End

?.2. Configuring an iBMC IP Address for a Single Node

Context

This section describes how to use SmartKit to configure the target iBMC IP address using the default iBMC IP address of a node. This method can configure an iBMC IP address for only one node at a time.

If the node name is specified when the LLD configuration file is prepared, the node name will be automatically configured when an iBMC IP address is configured. If an OceanStor Pacific 9950 device exists, you also need to configure the management IP addresses of its data cluster modules and the system will automatically change the passwords of the data cluster modules.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

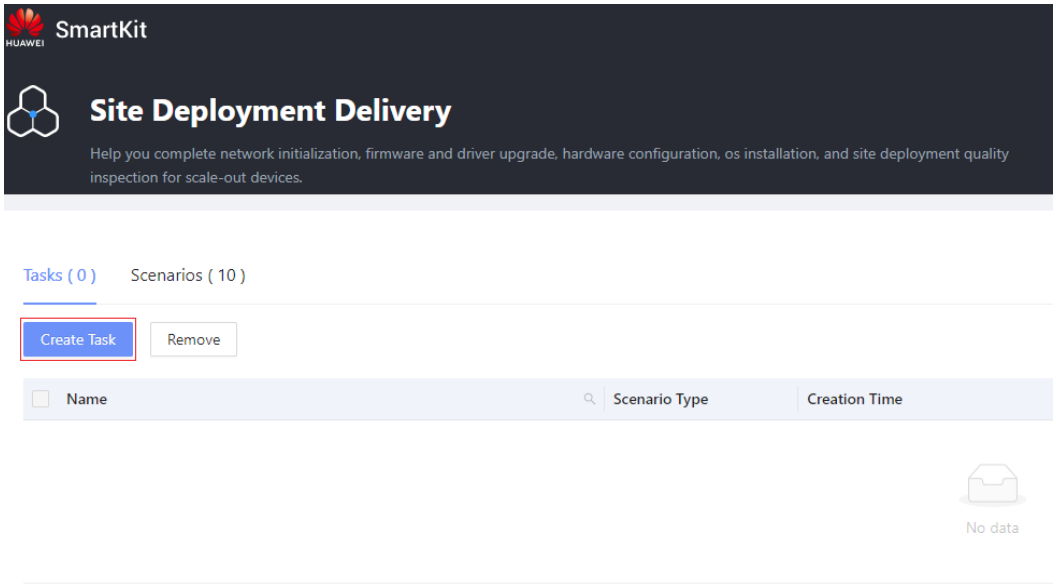
The GUI of SmartKit may vary with the version.

Prerequisites

If the storage software has been installed on the nodes to be deployed, uninstall the storage software by referring to **5.5.19 Uninstalling OceanStor Pacific Series Software**, clear the network and route information configured on the nodes, and then initialize the nodes using SmartKit.

Procedure

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.



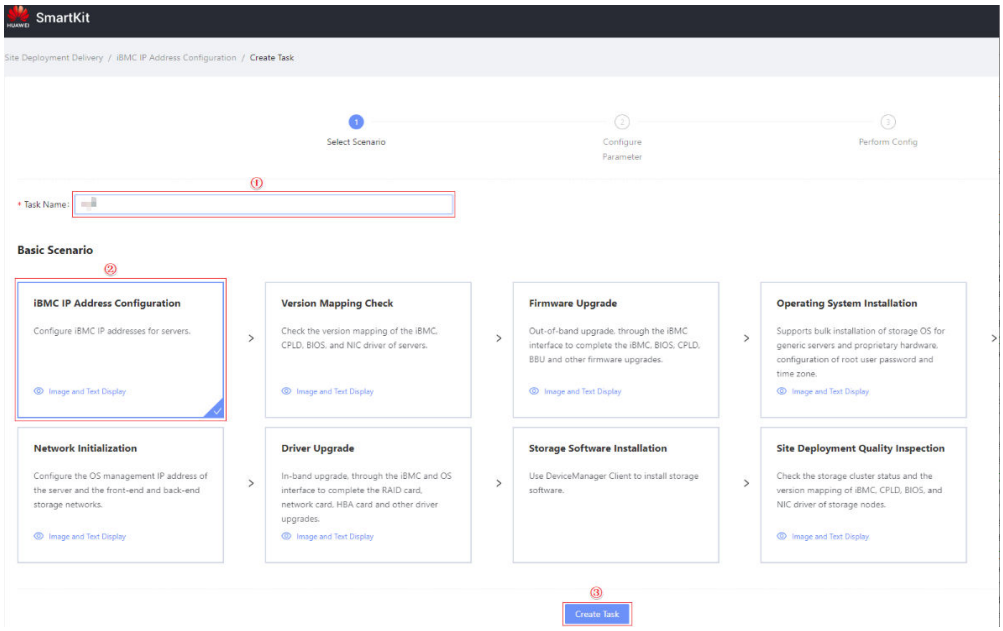
Step 2 Select an iBMC IP address configuration scenario.

1. Set **Task Name**, select **iBMC IP Address Configuration**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).

 Copyright © Huawei Technologies Co., Ltd.

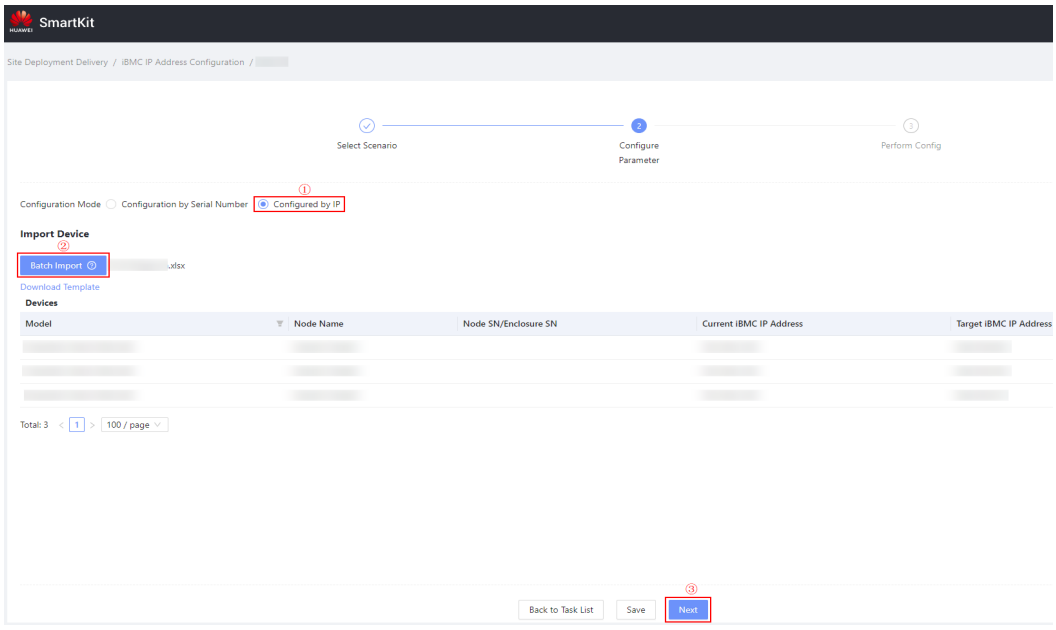


2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

   NOTE

   If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

Step 3 Configure parameters.

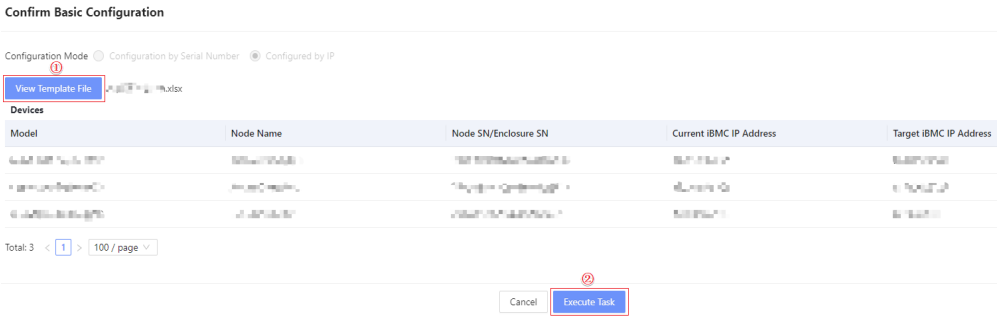


1. Set **Configuration Mode** to **Configured by IP**.
2. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.
3. Click **Next**.

Step 4 Perform the configuration.

 Copyright © Huawei Technologies Co., Ltd.

1. Click **View Template File**. The imported LLD configuration file will be automatically opened. Confirm the information to be configured. After confirming that the information is correct, click **Execute Task**.

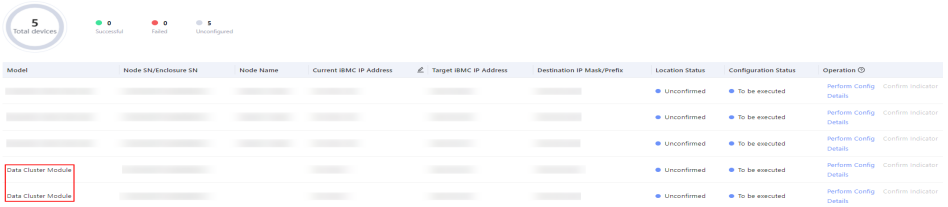


2. Configure iBMC IP addresses.

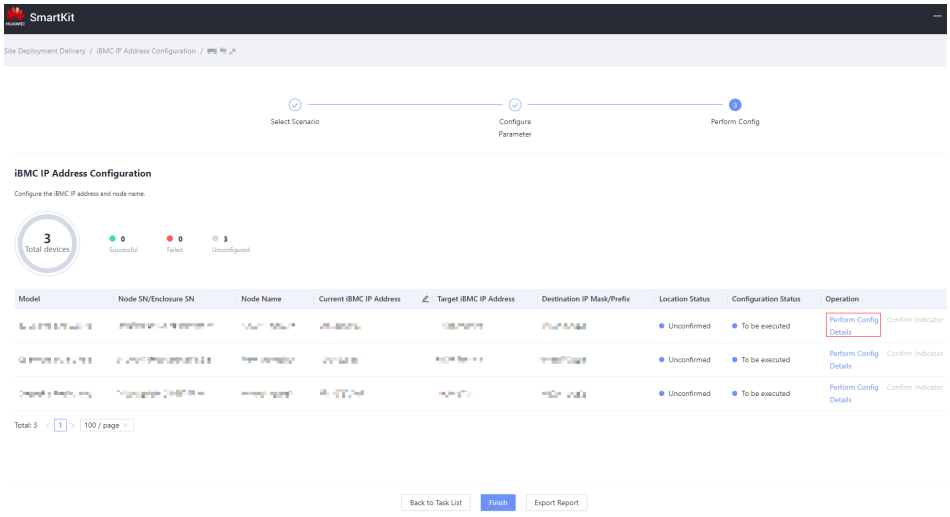
   Only one IP address can be configured at a time. To configure a single IP address, perform the following steps:

   NOTE

   If an OceanStor Pacific 9950 device exists, management IP addresses must be configured for its data cluster modules. The configuration information about the data cluster modules (whose **Model** is **Data Cluster Module**) is displayed.



   a. Click **Perform Config** in the **Operation** column of the node to be configured.

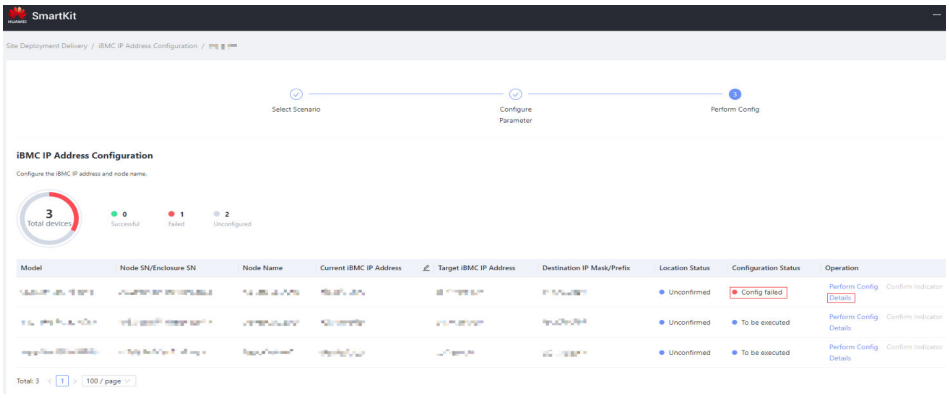


   NOTE

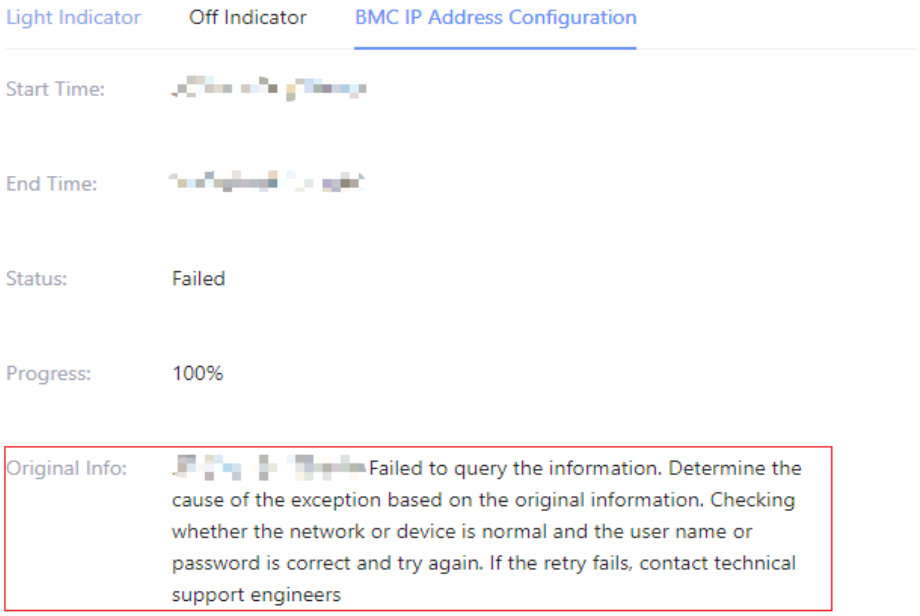
   Before the configuration, the IP address of the installation PC must be in the same subnet as the default IP address. You can view the default IP address in the **Current iBMC IP Address** column. The default mask is 255.255.255.0.

 Copyright © Huawei Technologies Co., Ltd.

b. After the configuration is complete, view the configuration result of the node in the **Configuration Status** column.



If **Config failed** is displayed in the **Configuration Status** column, click **Details** in the **Operation** column. Click the **BMC IP Address Configuration** tab, and rectify the fault based on the information in **Original Info**. The following is an example:



NOTE

You can also click **Export Report** in the lower part to collect and view the configuration results of all IP addresses.

3. Confirm indicators.

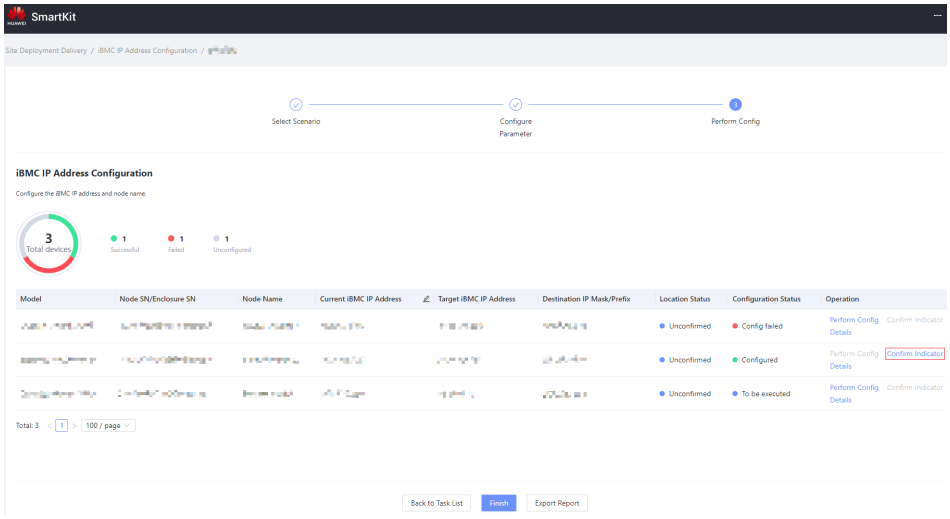
NOTE

If an OceanStor Pacific 9950 device exists, the management IP addresses of the data cluster modules must be able to communicate with the management network. If the management network cannot communicate with the iBMC network, you need to connect the installation PC to the management switch and iBMC switch, and check the configuration results for the management IP addresses and iBMC IP addresses of the data cluster modules separately.

a. Connect the installation PC to the corresponding switch and configure the installation PC to be in the same subnet as **Target iBMC IP Address**.

 Copyright © Huawei Technologies Co., Ltd.

b. Click **Confirm Indicator** in the **Operation** column corresponding to each IP address.



NOTE

- For details about the positions of device location indicators, see **Appendix** > **Indicators and Buttons** in *OceanStor Pacific Series 8.2.1 Hardware Installation Guide*.
- If the location indicator of the corresponding device is on, the configuration is successful. In the **Confirm Indicator** dialog box that is displayed, click **Correct**. The location indicator will be automatically turned off.
- If the location indicator status is not as expected, re-plan the iBMC IP addresses and configure them from the beginning. If the fault persists, contact Huawei technical support engineers.

4. After confirming that the information is correct, click **Finish**.

----End

5.4.2.6.1.3 Checking Version Mappings

Context

This section describes how to use SmartKit to check the version mapping of a node, such as the OS, firmware, and driver.

NOTE

The GUI of SmartKit may vary with the version.

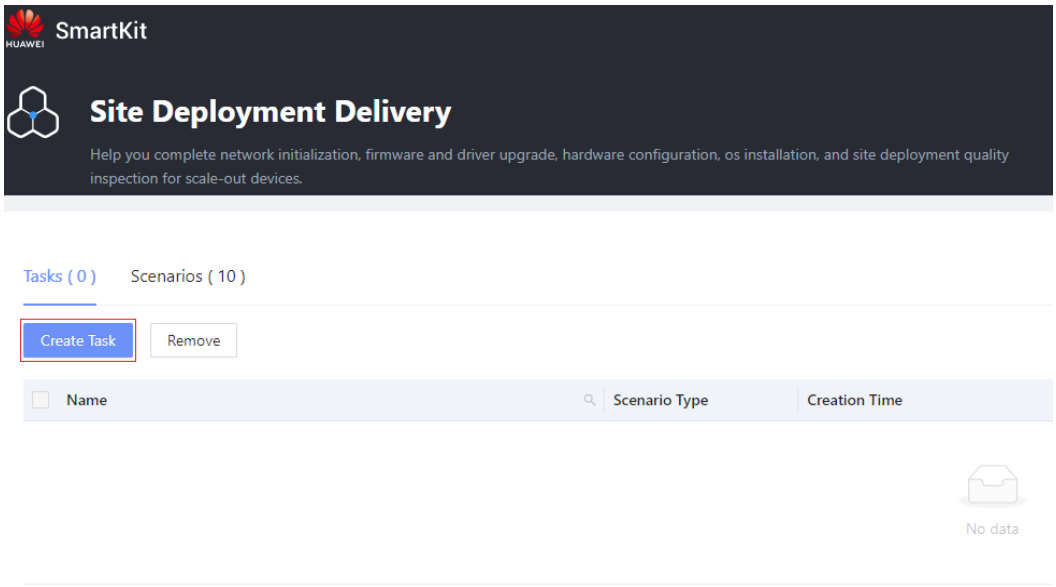
Prerequisites

The installation PC communicates properly with the newly configured iBMC network of a node.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.

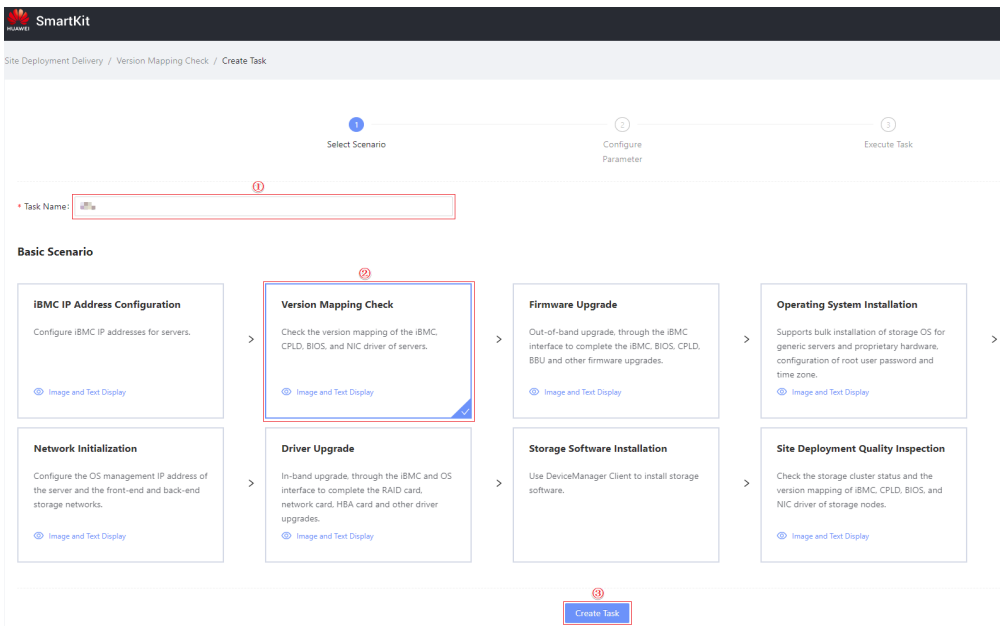


Step 2 Select a scenario.

1. Set **Task Name**, select **Version Mapping Check**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).

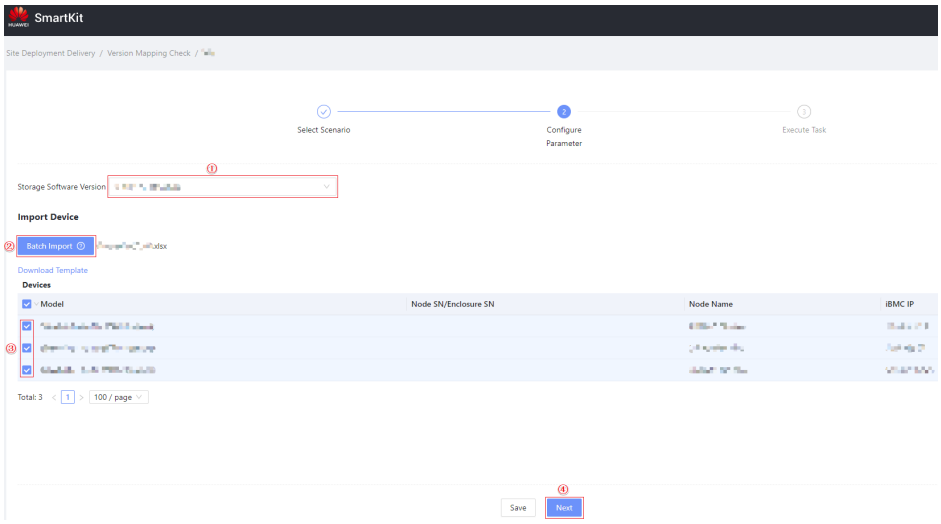


2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

 Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

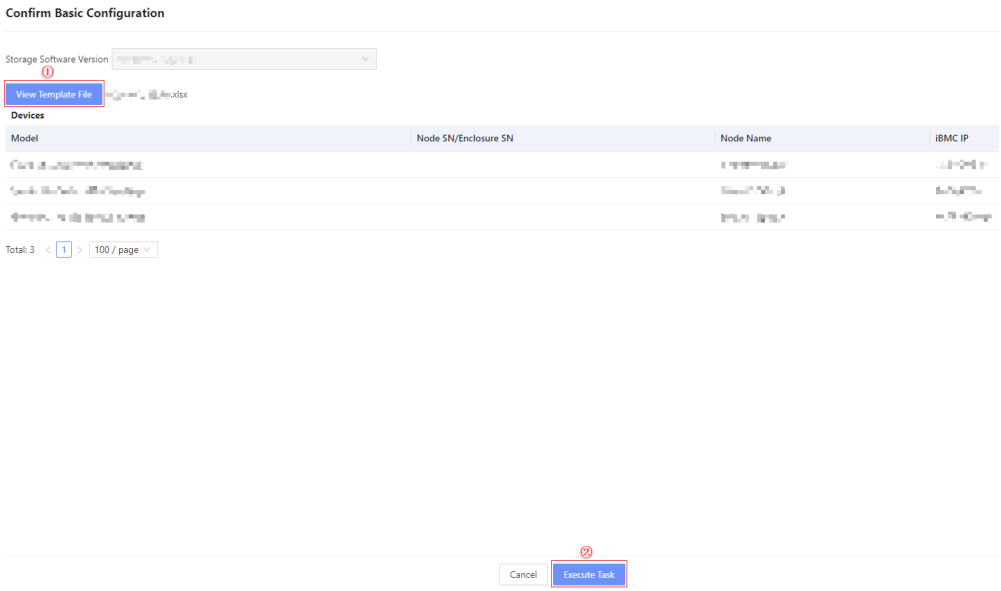
Step 3 Configure parameters.



1. Set **Storage Software Version**.
2. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.
3. In **Devices**, select the nodes for which you want to check version mapping.
4. Click **Next**.

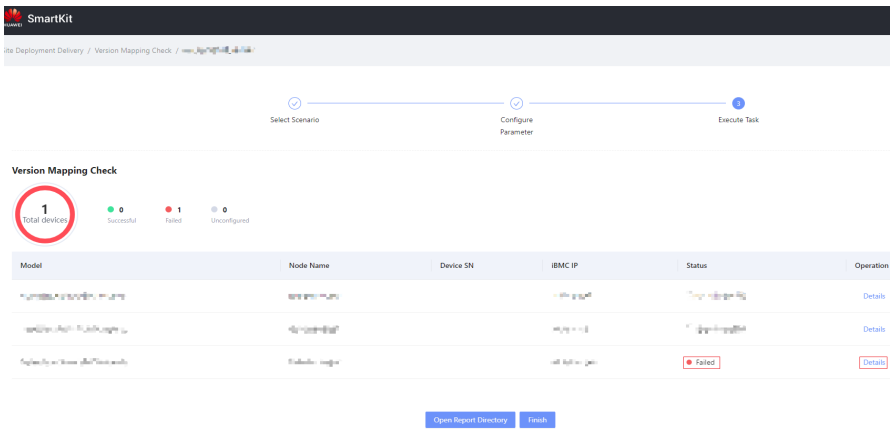
Step 4 Execute the task.

1. Click **View Template File**. The imported LLD configuration file will be automatically opened. Confirm the information to be configured. After confirming that the information is correct, click **Execute Task**.



 Copyright © Huawei Technologies Co., Ltd.

2. After the task is complete, check whether **Successfully** is displayed in the **Status** column of each node.
   - If yes, click **Finish**.
   - If no, perform the following steps for each failed node (after the troubleshooting is complete, click **Finish**):
     i. Click **Details** in the **Operation** column of the node.



NOTE

You can also click **Open Report Directory** in the lower part to collect and view the check results of all nodes.

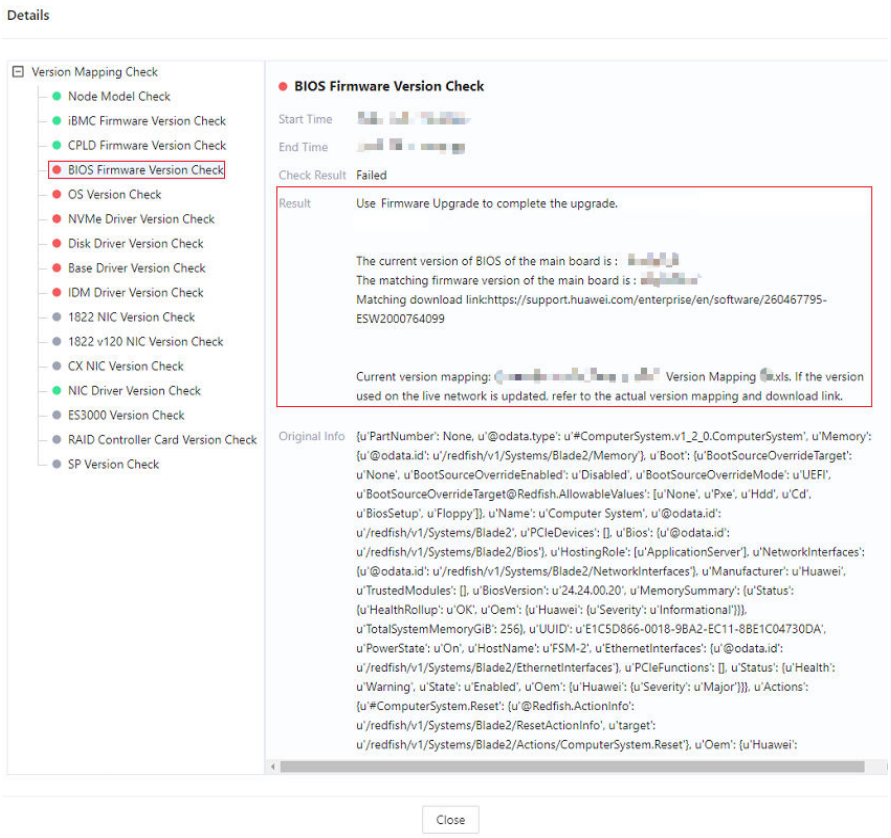
     ii. On the **Details** page, click each failed check item (marked in red) on the left and perform troubleshooting according to the description in **Result**. The following are examples:

NOTE

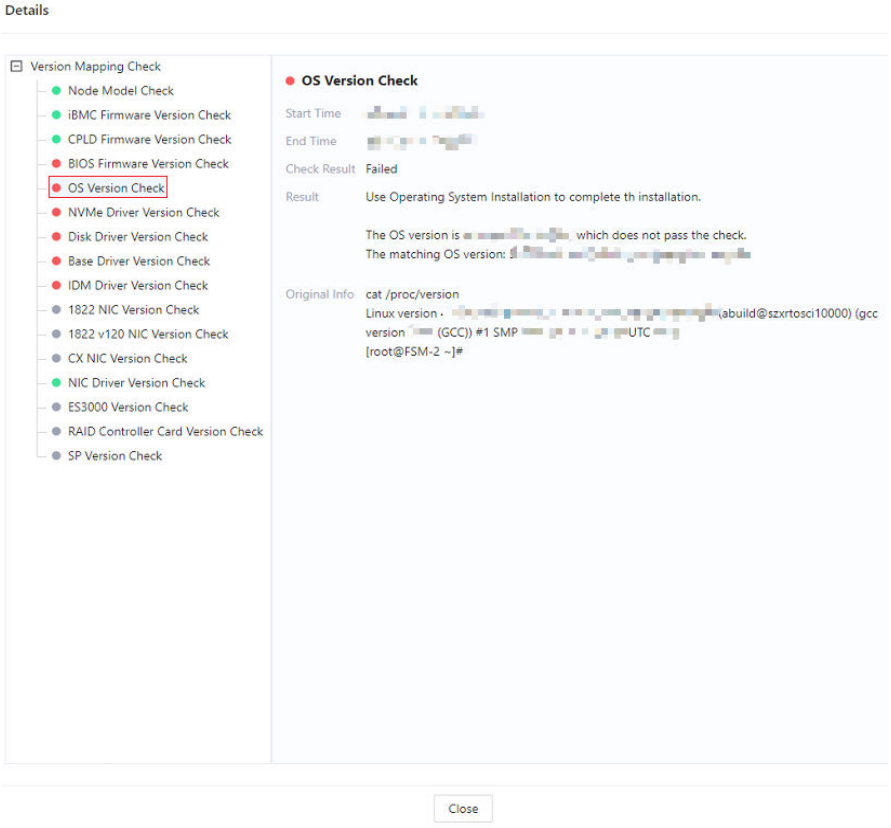
- The check items on the left of the **Details** page are displayed in the operation sequence. Handle the failed check items from top to bottom.
- For a check item that fails, the link for downloading the related software package is displayed in **Result**. You can click the link to download the software package. If the download link is not provided, obtain the related software package by referring to **5.4.2.4.2 Obtaining Software Packages**.

Firmware:

 Copyright © Huawei Technologies Co., Ltd.

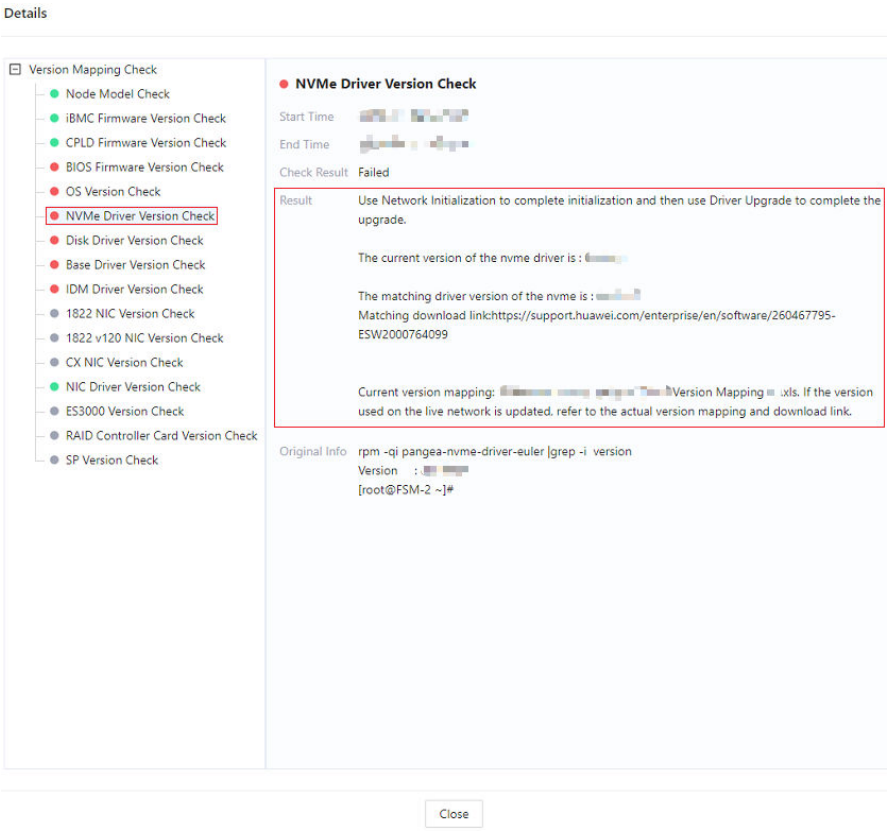


OS:



Driver:

 Copyright © Huawei Technologies Co., Ltd.



----End

5.4.2.6.1.4 (Optional) Upgrading Firmware

Context

This section describes how to upgrade firmware on SmartKit.

NOTE

The GUI of SmartKit may vary with the version.

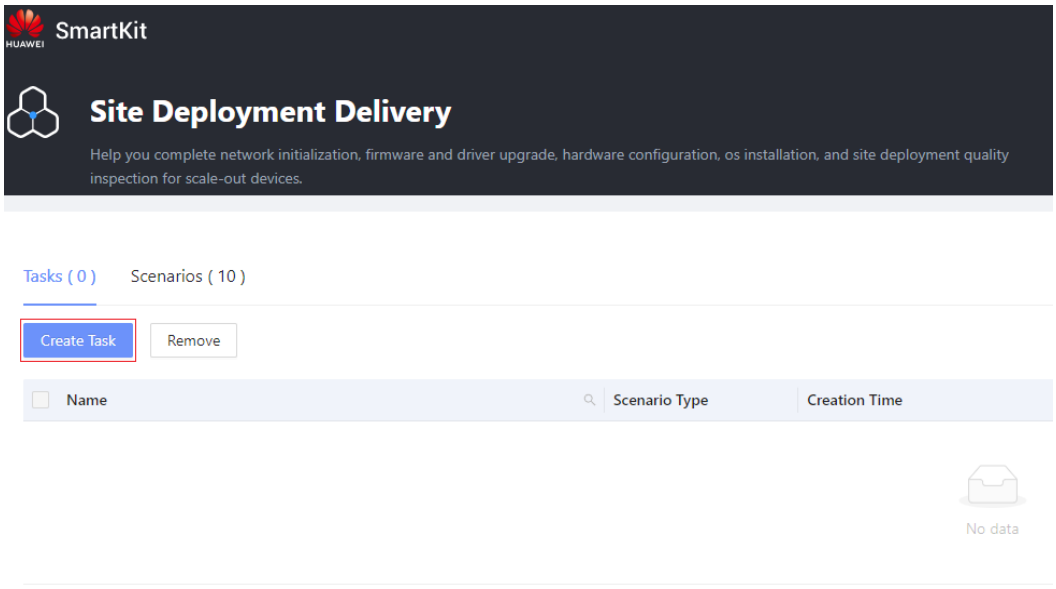
Prerequisites

- You have determined that firmware needs to be upgraded according to the check results in **Checking Version Mappings** and downloaded the corresponding firmware package.
- The installation PC communicates properly with the newly configured iBMC network of a node.

Procedure

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

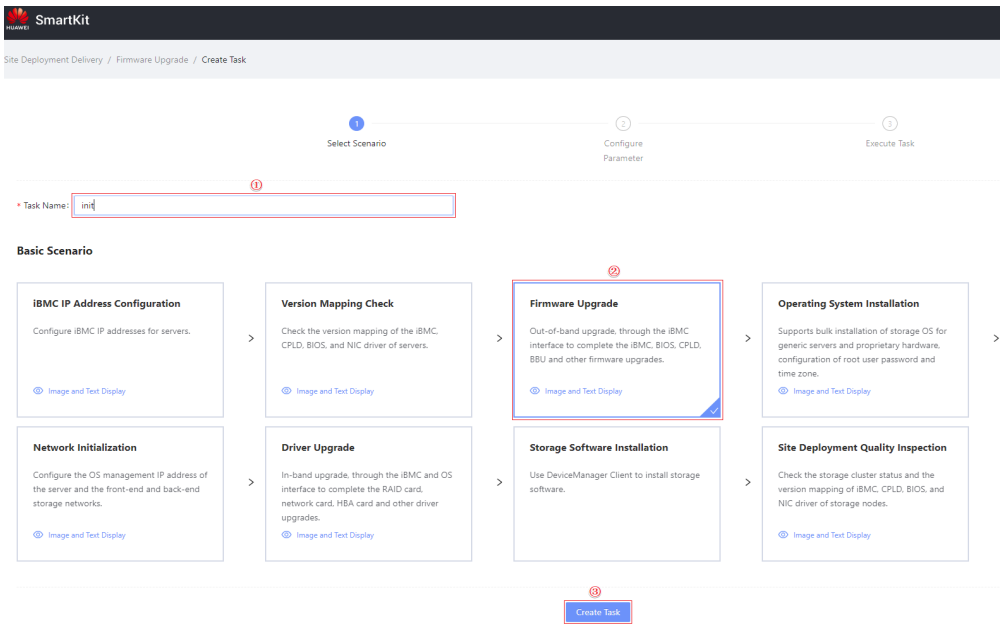


Step 2 Select a scenario.

1. Set **Task Name**, select **Firmware Upgrade**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).



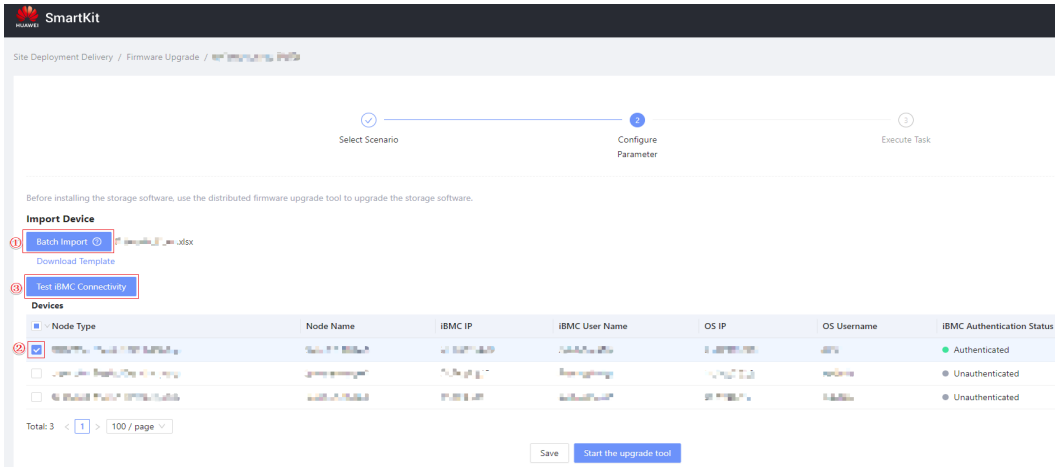
2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

   NOTE

   If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Configure parameters.



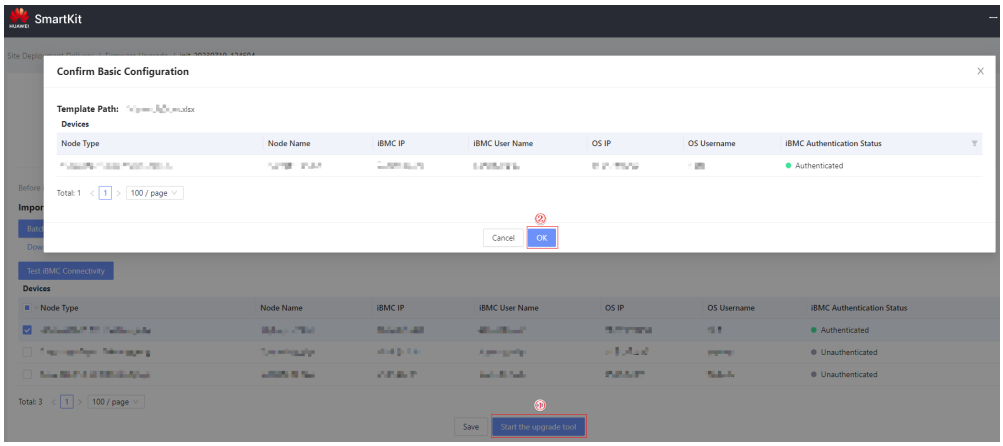
1. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.
2. In **Devices**, select a node whose firmware needs to be upgraded.
3. Click **Test iBMC Connectivity** for authentication.

   NOTE

   If authentication failure is displayed in the **iBMC Authentication Status** column of a node, rectify the fault according to the description in .

Step 4 Execute the task.

1. Click **Start the upgrade tool**. A dialog box is displayed for you to confirm the configuration information. After confirming that the information is correct, click **OK**. The firmware upgrade page is displayed.



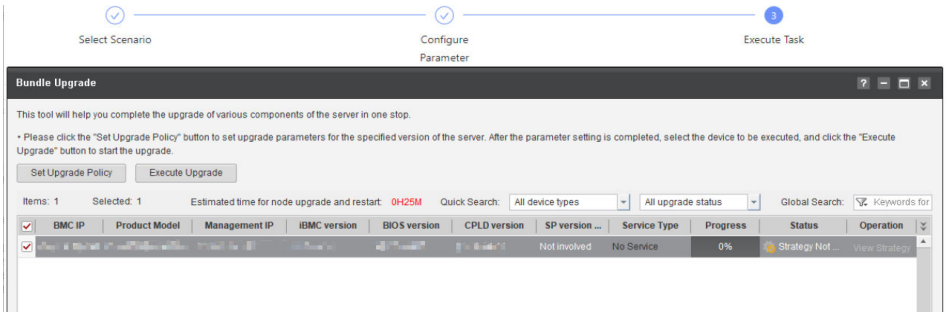
2. Set the upgrade policy.

   a. Select the devices to be upgraded.

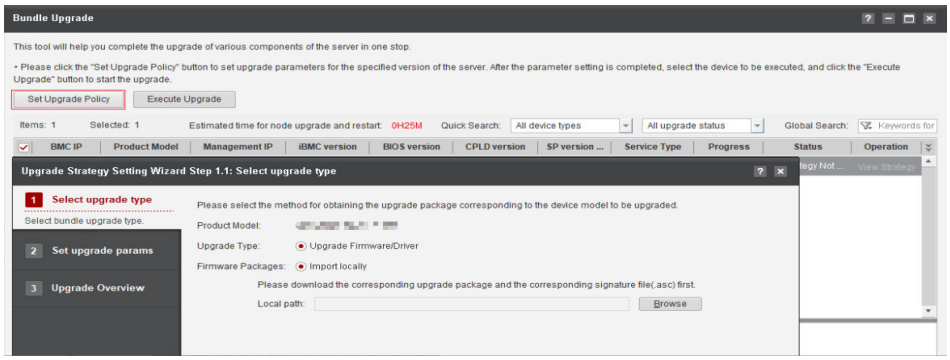
      NOTE

      Devices of different models need to be upgraded in different batches. Select devices of the same model to set the upgrade policy.

 Copyright © Huawei Technologies Co., Ltd.

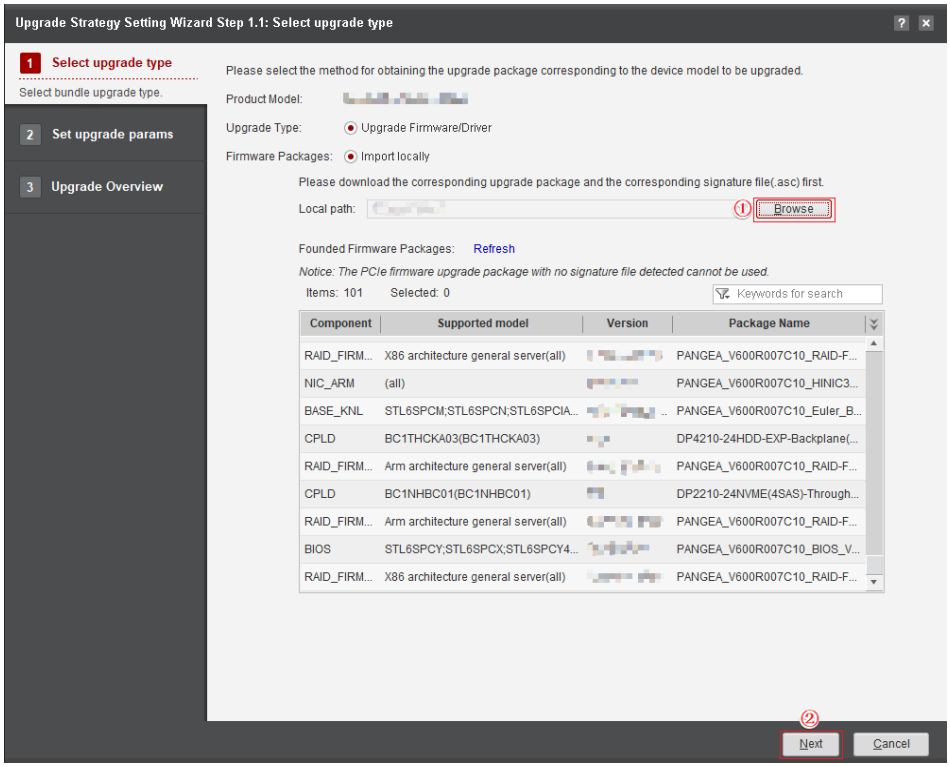


b. Click **Set Upgrade Policy**. The **Upgrade Strategy Setting Wizard** dialog box is displayed.



c. Import the firmware upgrade package.

Click **Browse**, select the path for storing the firmware upgrade package, and click **Next**.

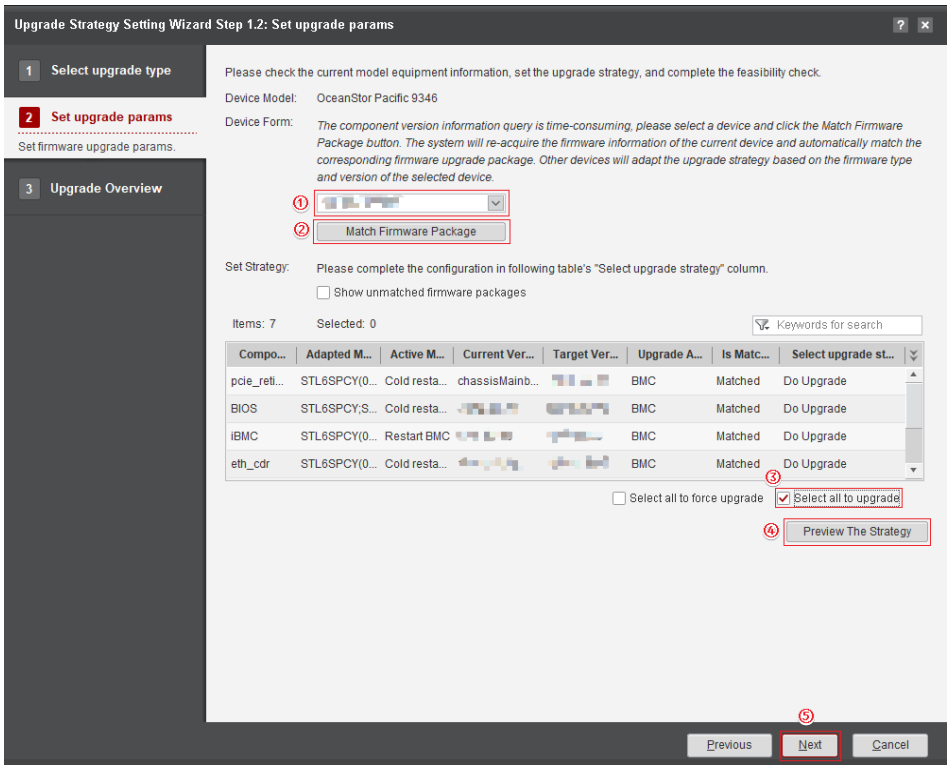


 Copyright © Huawei Technologies Co., Ltd.

NOTE

You are advised not to store other files in the path for storing the firmware upgrade package. Otherwise, the parsing efficiency of the tool will be affected.

d. Set parameters.



i. Select any node as the device form.

ii. Click **Match Firmware Package**. The matched firmware information will be displayed.

iii. Select the firmware to be upgraded. Based on the check result in **Checking Version Mappings**, select **Do Upgrade** in the **Select upgrade strategy** column for the firmware whose current version is earlier than the target version.

NOTE

Select all to force upgrade: In special scenarios, if the current firmware version is later than the target version, select this option. This option forcibly upgrades all firmware to the target version.

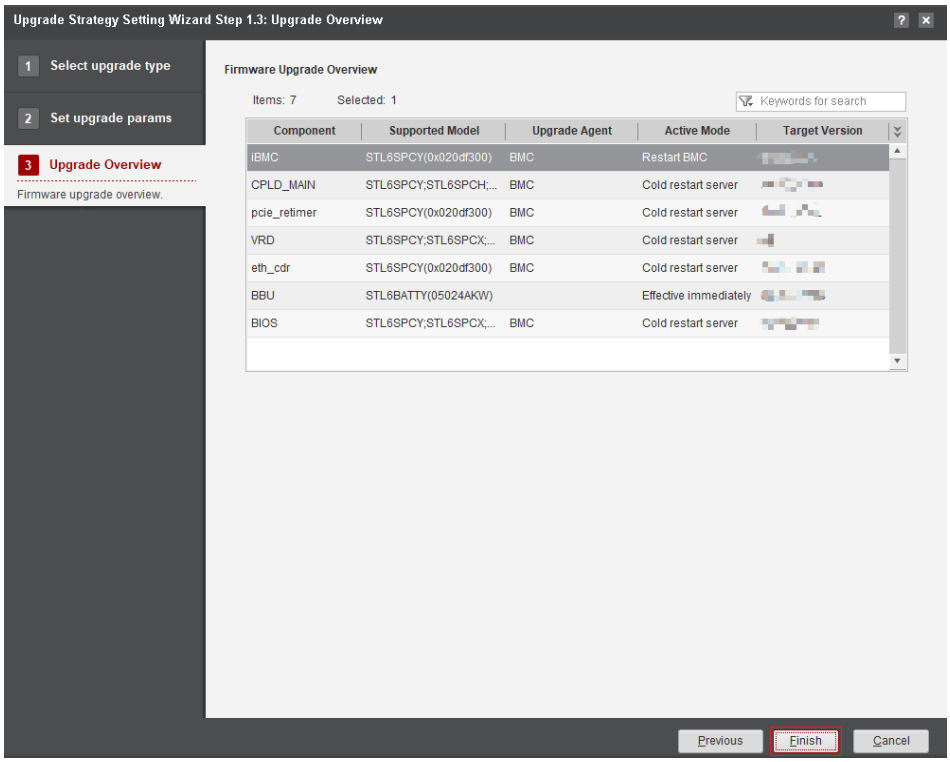
iv. (Optional) Click **Preview The Strategy**. The **Upgrade Strategy Preview** dialog box is displayed.

In the **Upgrade strategy** area, check that the upgrade policy to be executed in the **Expected Result** column is correct and click **OK**.

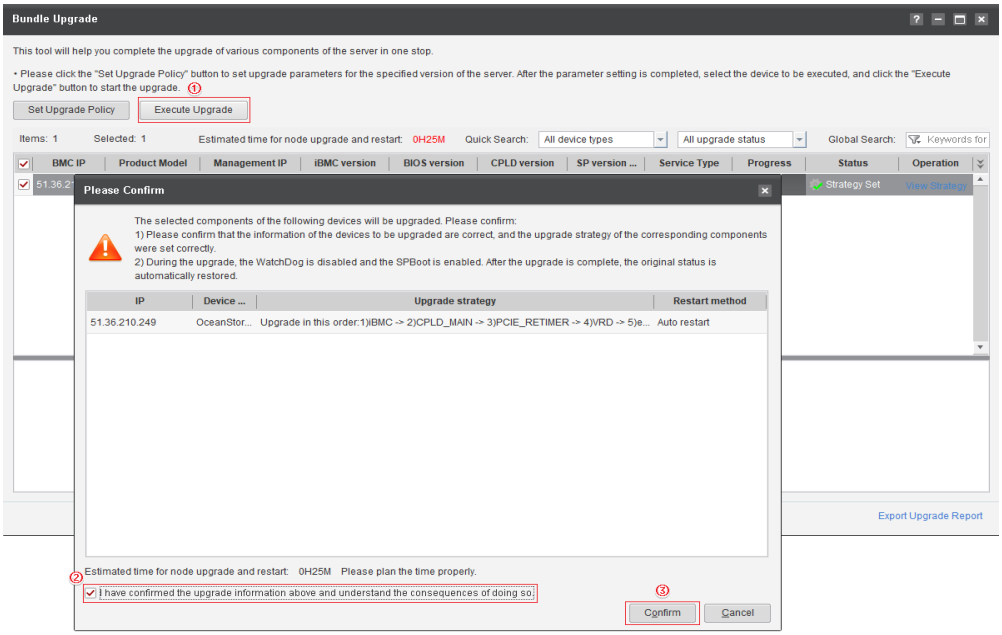
v. Click **Next**.

e. View the basic information about the firmware upgrade and click **Finish**.

 Copyright © Huawei Technologies Co., Ltd.

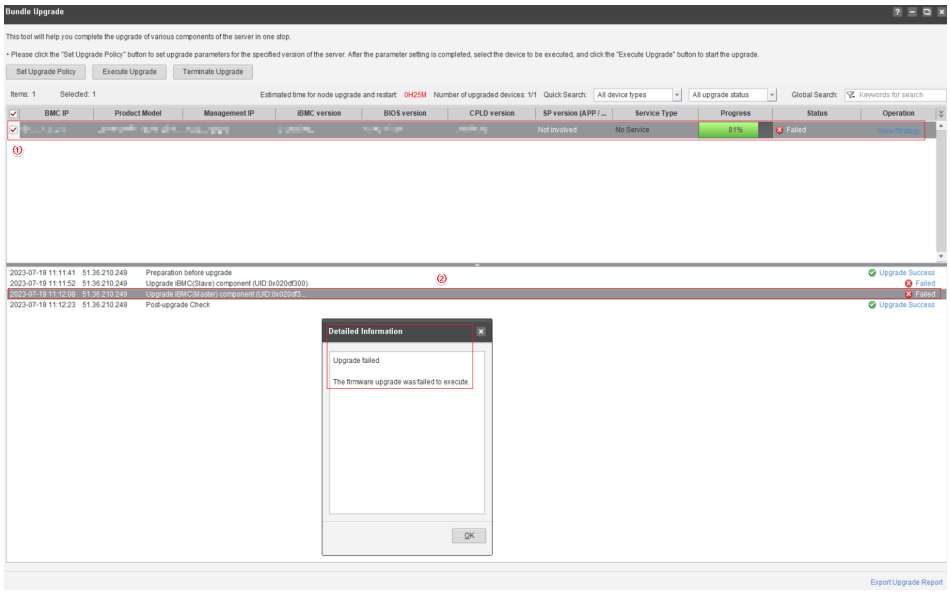


3. Click **Execute Upgrade**. A confirmation dialog box is displayed. After confirming the information, select **I have confirmed...** and click **Confirm**.



4. After the upgrade is complete, check whether **Upgrade Success** is displayed in the **Status** column of all nodes.
   - If yes, click ✕ in the upper right corner of the dialog box to end the upgrade process.
   - If no, perform the following steps for each failed node (after the troubleshooting is complete, click ✕ in the upper right corner of the dialog box):

 Copyright © Huawei Technologies Co., Ltd.



i. Select the failed node. The upgrade details are displayed in the lower part.

ii. In the details area, locate the failed steps and click them one by one. Then perform troubleshooting according to the description in the displayed **Detailed Information** dialog box.

NOTE

You can also click **Export Upgrade Report** in the lower right corner to collect and view the upgrade results of all nodes.

----End

5.4.2.6.1.5 (Optional) Installing the OS

Context

This section describes how to install the OS on SmartKit.

NOTE

The GUI of SmartKit may vary with the version.

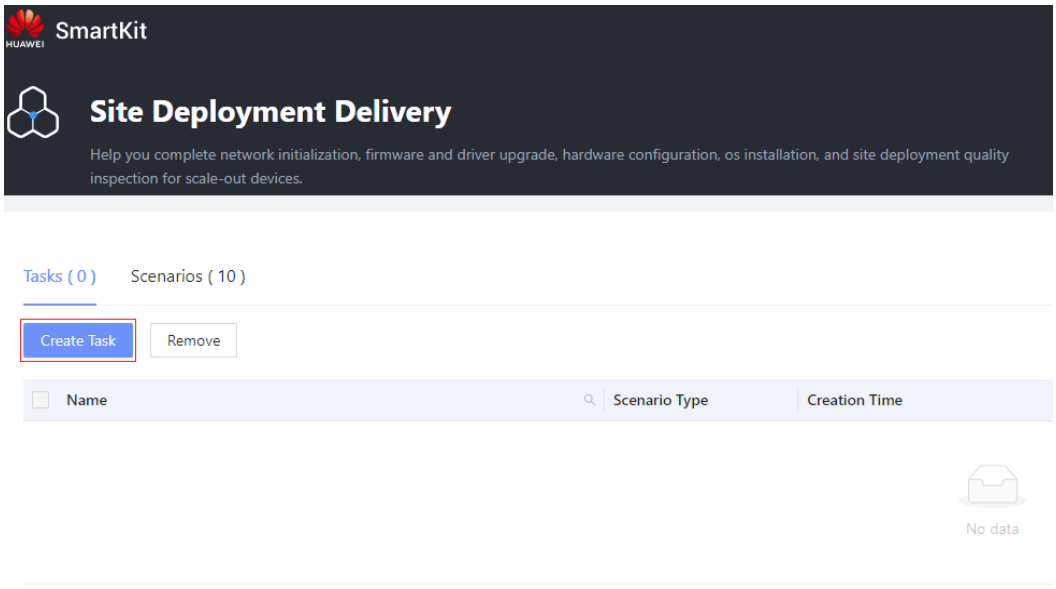
Prerequisites

- You have determined that the OS needs to be installed according to the check results in **Checking Version Mappings** and downloaded the OS image file.
- The installation PC communicates properly with the newly configured iBMC network of a node.

Procedure

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

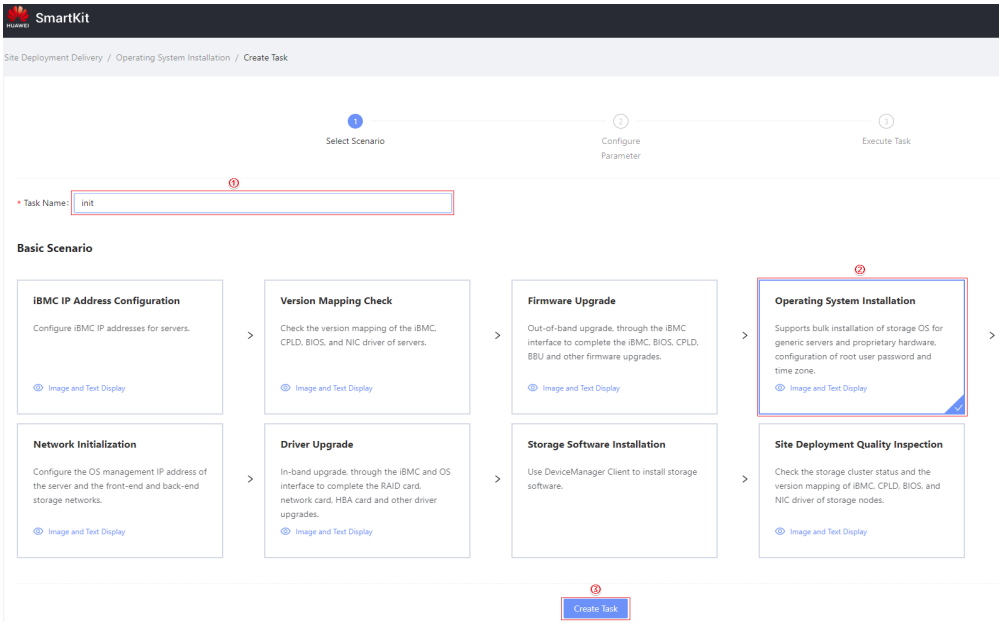


Step 2 Select a scenario.

1. Set **Task Name**, select **Operating System Installation**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).



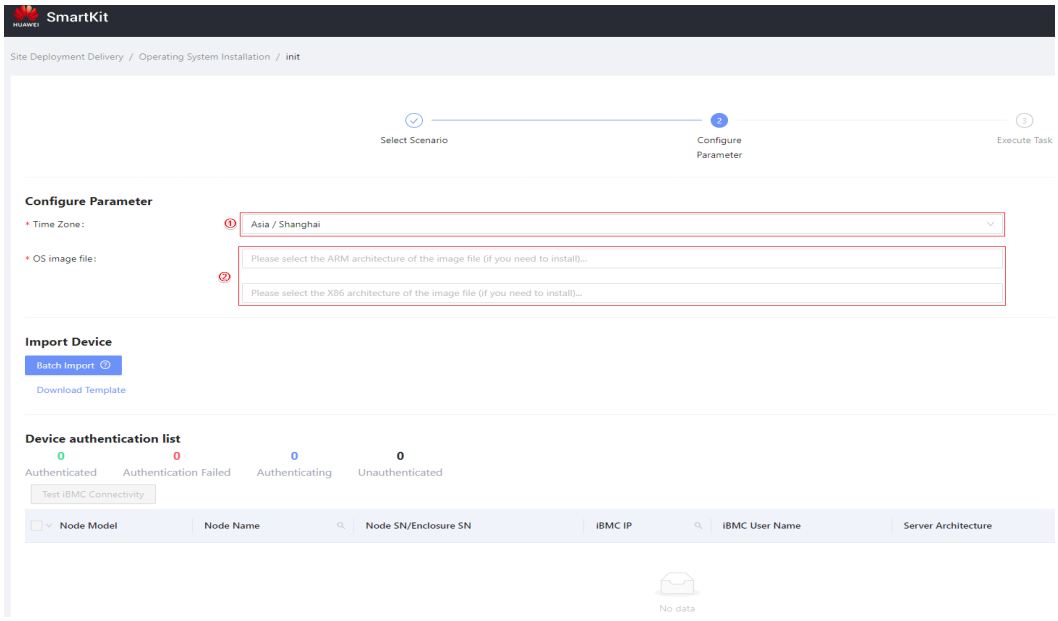
2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

   NOTE

   If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Configure parameters.

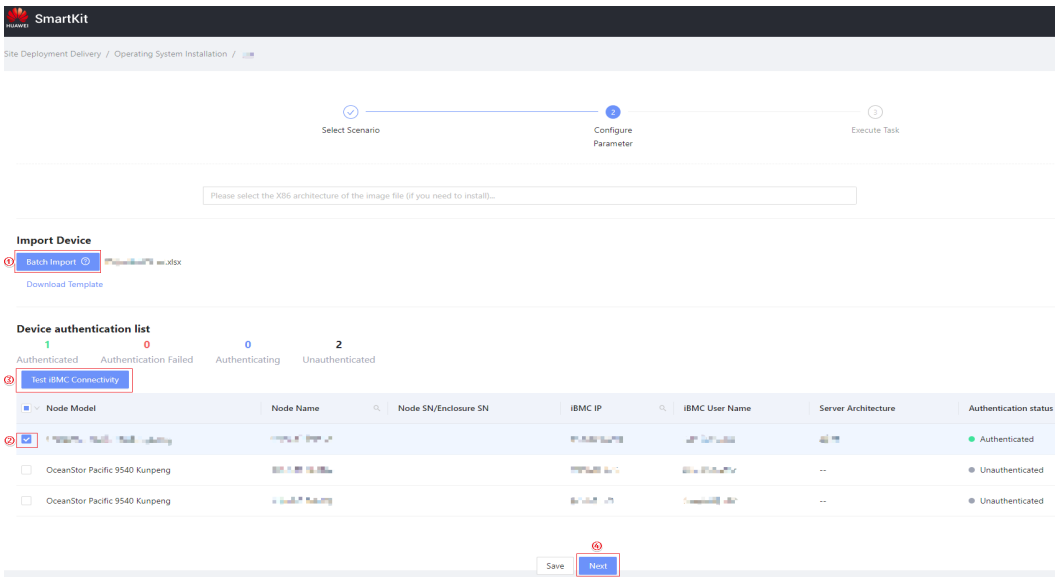


1. In the **Time Zone** drop-down list, select a time zone as required.
2. In the **OS image file** text box, select the path for storing the image file according to the architecture of the nodes where the OS is to be installed.

   NOTE

   - Image files of the Arm and x86 architectures can be uploaded. If only one node architecture is involved, upload only the OS image file of the architecture. If two node architectures are involved, upload the OS image files of the two architectures.
   - If you are uncertain about the node architecture, see the **Server Architecture** column after the iBMC authentication is complete in **Step 4.2**.

Step 4 Import and authenticate devices.



1. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.

 Copyright © Huawei Technologies Co., Ltd.

2. In **Device authentication list**, select a node where the OS is to be installed and click **Test iBMC Connectivity** for authentication.

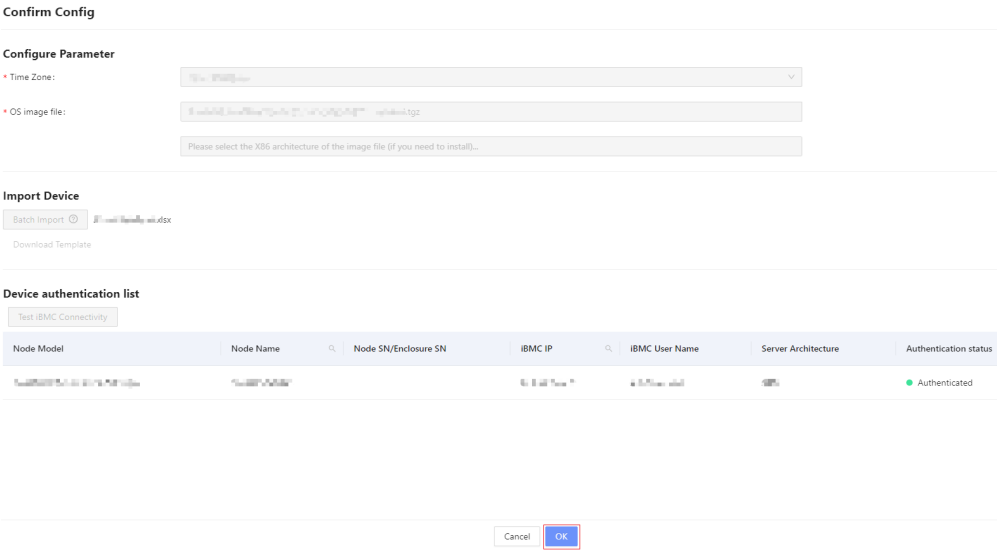
   NOTE

   If authentication failure is displayed in the **Authentication status** column of a node, rectify the fault according to the description in .

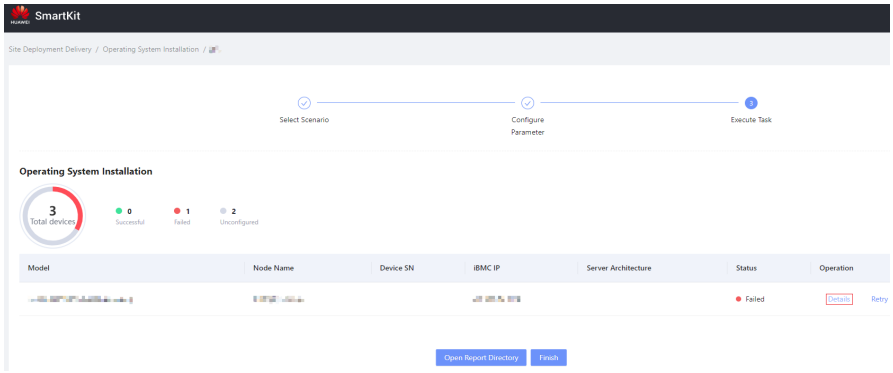
3. After the authentication is complete, click **Next**.

Step 5 Execute the task.

1. After confirming that the basic configuration information is correct, click **OK**.



2. After the task is complete, check whether **Successfully** is displayed in the **Status** column of each node.
   - If yes, click **Finish**.
   - If no, perform the following steps for each failed node (after the troubleshooting is complete, click **Finish**):
     i. Click **Details** in the **Operation** column of the node.

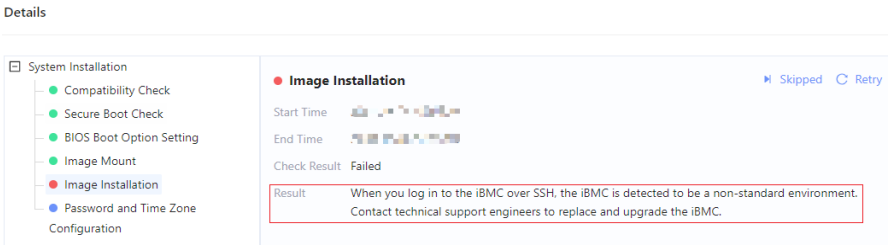


     NOTE

     You can also click **Open Report Directory** in the lower part to collect and view the installation results of all nodes.

     ii. On the **Details** page, click each failed item (marked in red) on the left and perform troubleshooting according to the description in **Result**. The following is an example:

 Copyright © Huawei Technologies Co., Ltd.



----End

5.4.2.6.1.6 Initializing Networks

Context

This section describes how to initialize networks on SmartKit, including configuring the management IP addresses of all nodes and front-end and back-end storage IP addresses of storage nodes.

NOTE

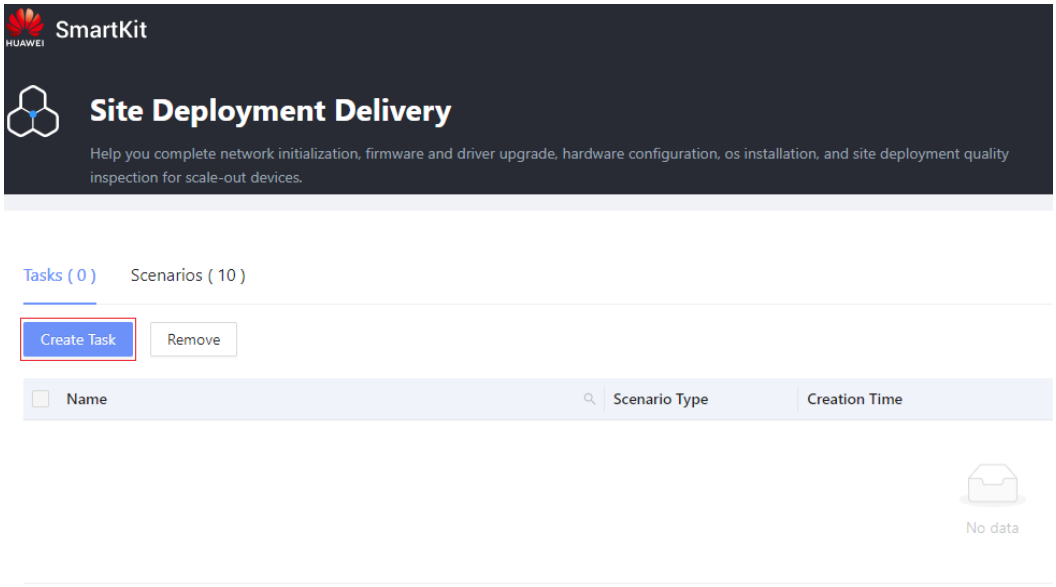
The GUI of SmartKit may vary with the version.

Prerequisites

- The installation PC communicates properly with the newly configured iBMC network of a node.

Procedure

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.



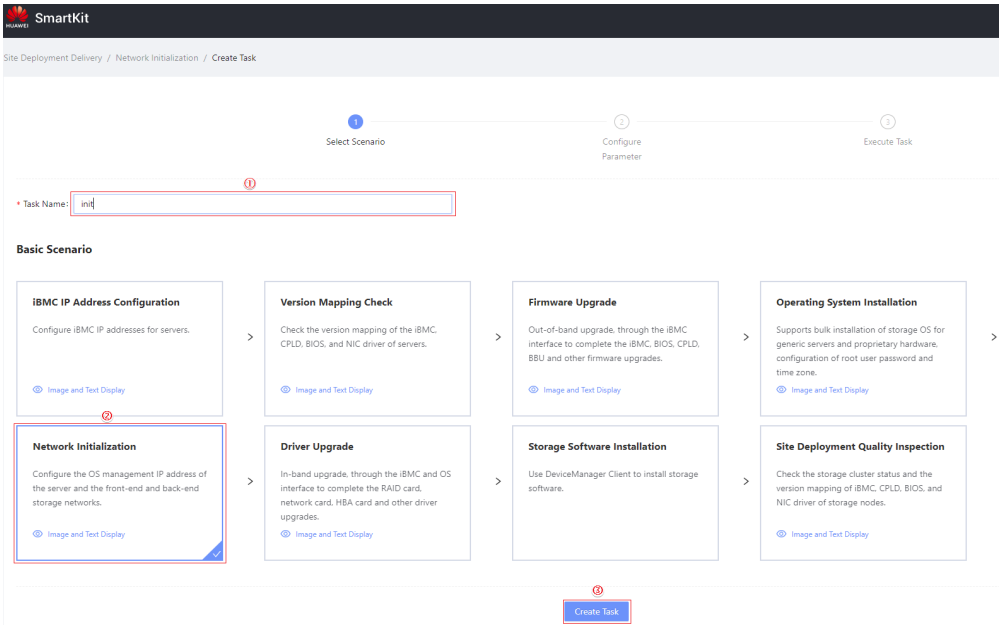
Step 2 Select a scenario.

1. Set **Task Name**, select **Network Initialization**, and click **Create Task**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).

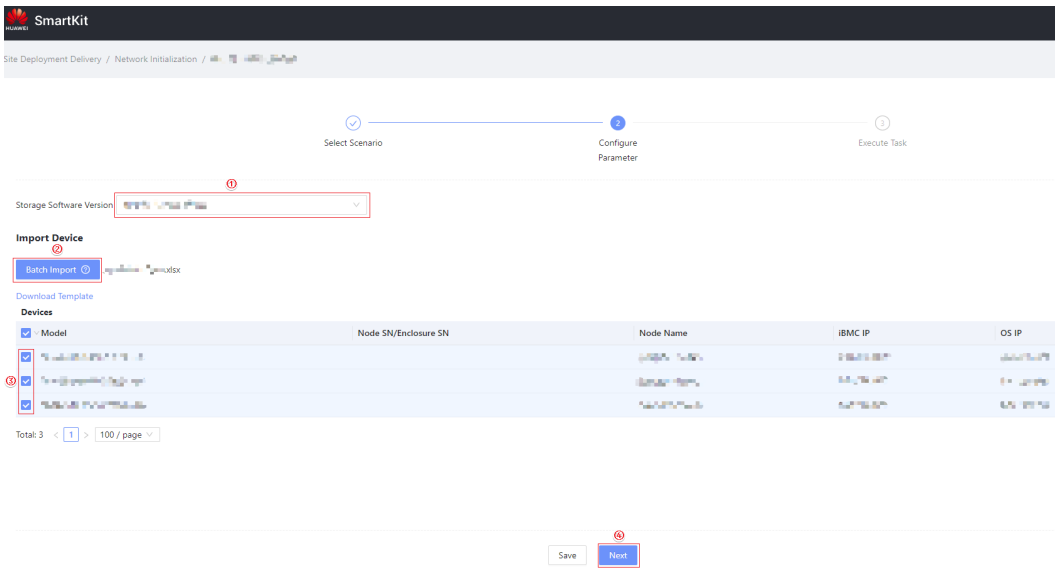


2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

NOTE

If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

Step 3 Configure parameters.



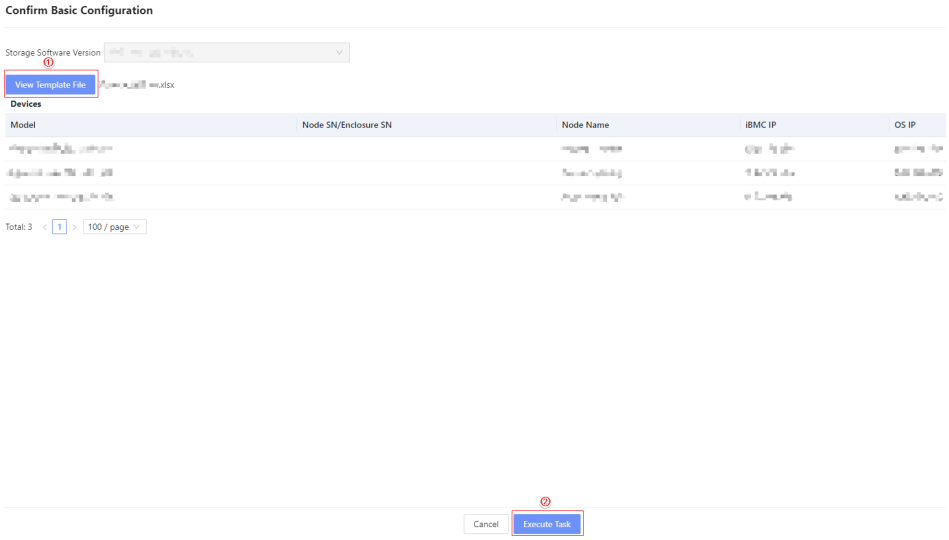
1. Set **Storage Software Version**.
2. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.

 Copyright © Huawei Technologies Co., Ltd.

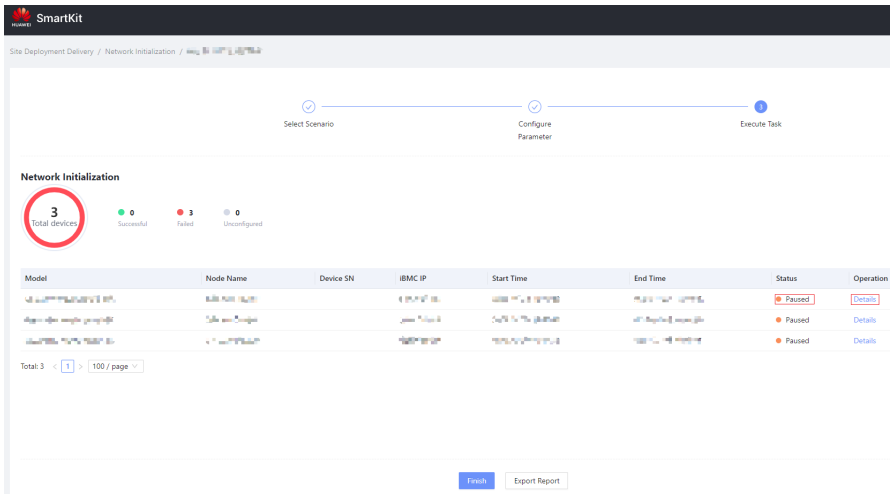
3. In **Devices**, select the nodes for which you want to initialize networks.
4. Click **Next**.

Step 4 Execute the task.

1. Click **View Template File**. The imported LLD configuration file will be automatically opened. Confirm the information to be configured. After confirming that the information is correct, click **Execute Task**.

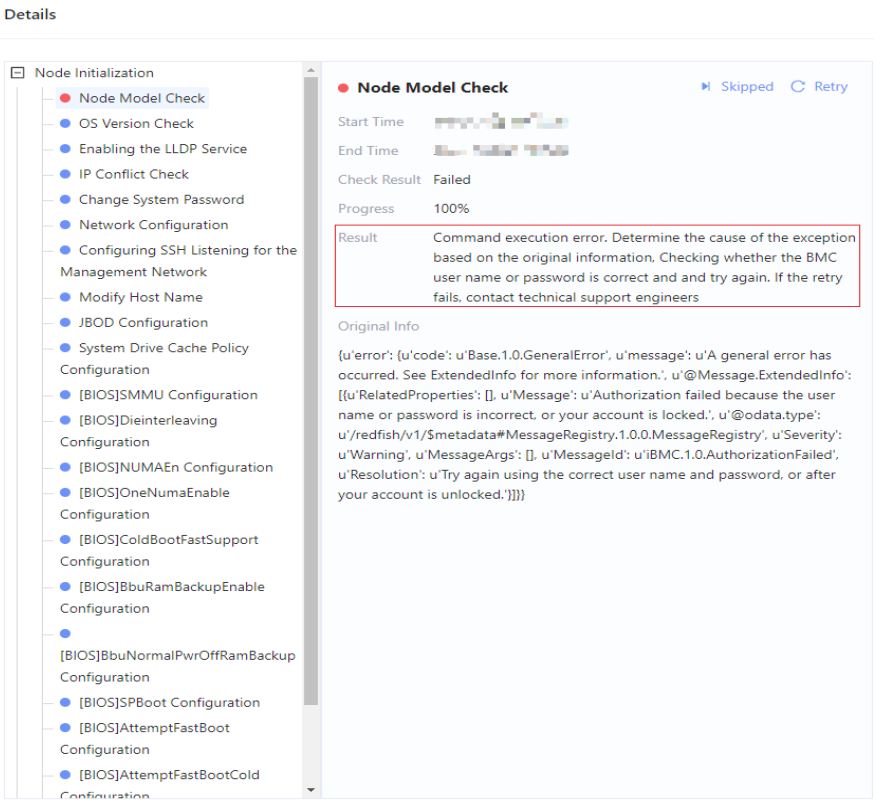


2. After the task is complete, check whether **Successfully** is displayed in the **Status** column of each node.
   - If yes, click **Finish**.
   - If no, perform the following steps for each failed node (after the troubleshooting is complete, click **Finish**):
     i. Click **Details** in the **Operation** column of the node.



     ii. On the **Details** page, click each failed item (marked in red) on the left and perform troubleshooting according to the description in **Result**. The following is an example:

 Copyright © Huawei Technologies Co., Ltd.



NOTE

You can also click **Export Report** in the lower part to collect and view the configuration results of all nodes.

----End

5.4.2.6.1.7 (Optional) Upgrading Drivers

Context

This section describes how to upgrade drivers on SmartKit.

NOTE

The GUI of SmartKit may vary with the version.

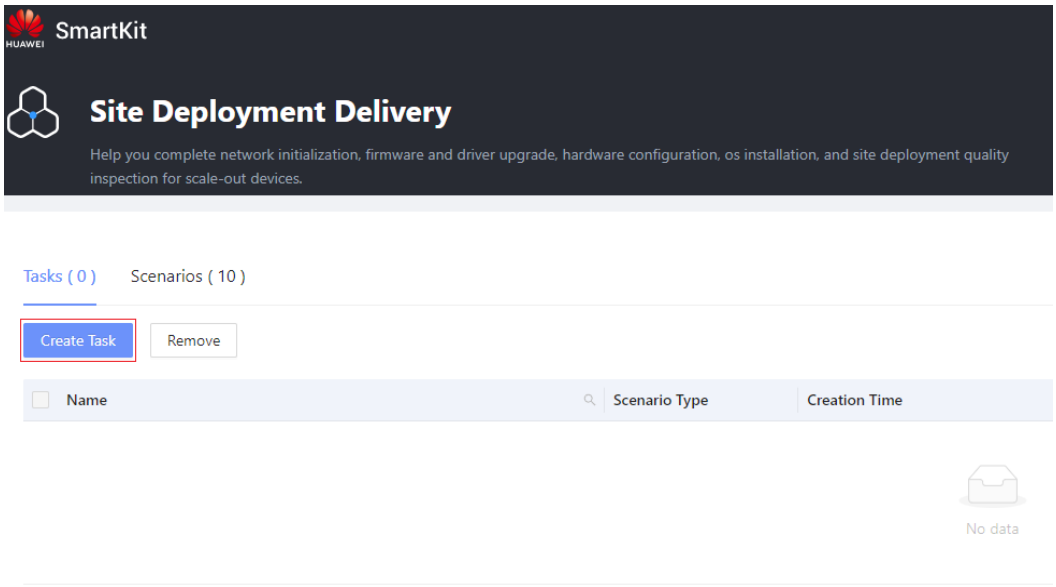
Prerequisites

- You have determined that a driver needs to be upgraded according to the check results in **Checking Version Mappings** and downloaded the corresponding driver package.
- The installation PC communicates properly with the management network of a node.
- The installation PC communicates properly with the newly configured iBMC network of a node.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 On the **Site Deployment Delivery** page, click the **Tasks** tab and click **Create Task**. The **Select Scenario** page is displayed.

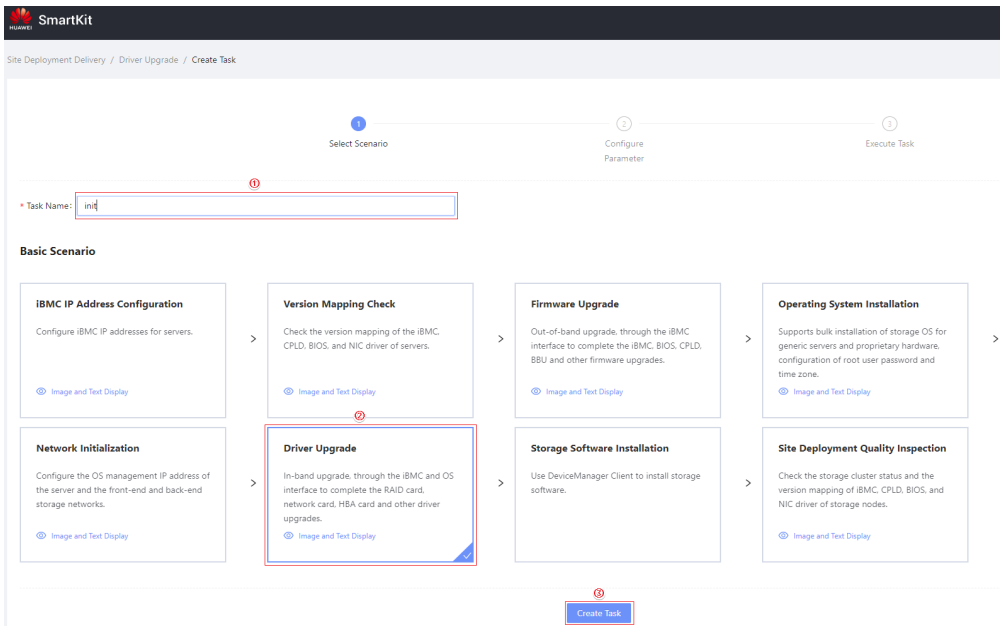


Step 2 Select a scenario.

1. Set **Task Name**, select **Driver Upgrade**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).



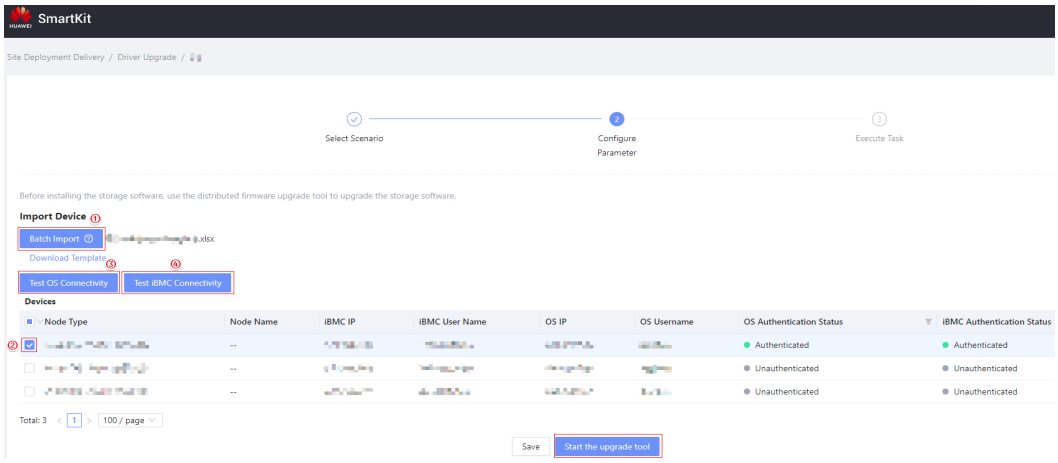
2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

Step 3 Configure parameters.



1. Click **Batch Import** to import the LLD configuration file. After the import is complete, you can view information about the imported devices in **Devices**.
2. In **Devices**, select a node whose driver needs to be upgraded.
3. Click **Test OS Connectivity** to perform OS authentication.

   NOTE

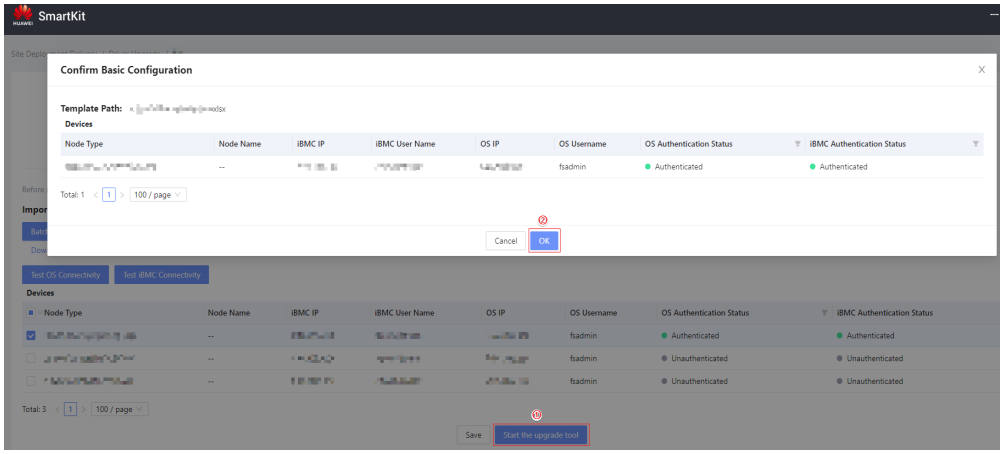
   If authentication failure is displayed in the **OS Authentication Status** column, rectify the fault according to the description in .
4. Click **Test iBMC Connectivity** to perform iBMC authentication.

   NOTE

   If authentication failure is displayed in the **iBMC Authentication Status** column, rectify the fault according to the description in .

Step 4 Execute the task.

1. Click **Start the upgrade tool**. A dialog box is displayed for you to confirm the configuration information. After confirming that the information is correct, click **OK**. The driver upgrade page is displayed.

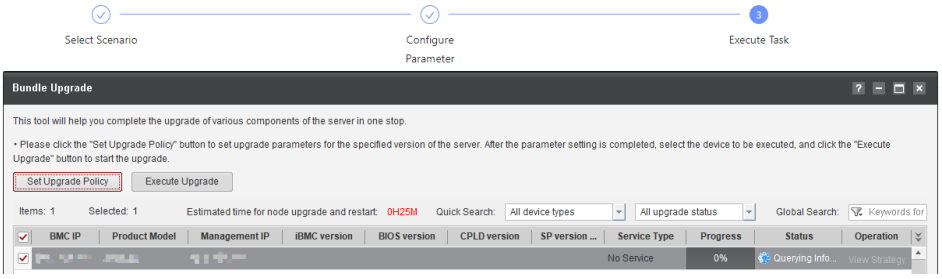


 Copyright © Huawei Technologies Co., Ltd.

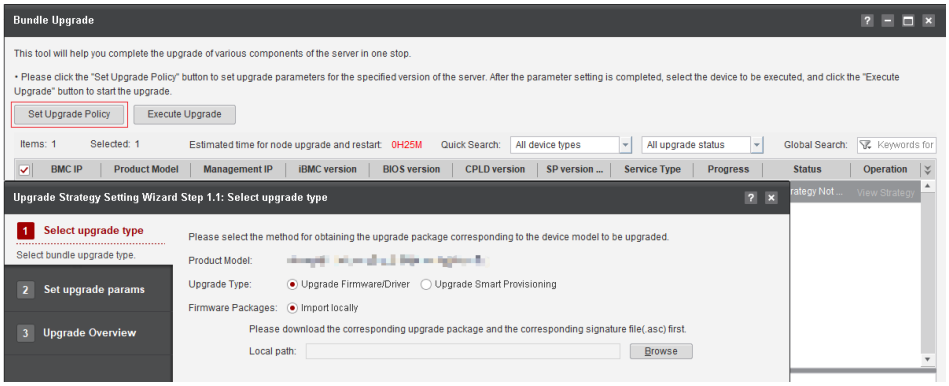
2. Set the upgrade policy.
   a. Select the devices to be upgraded.

      NOTE

      Devices of different models need to be upgraded in different batches. Select devices of the same model to set the upgrade policy.

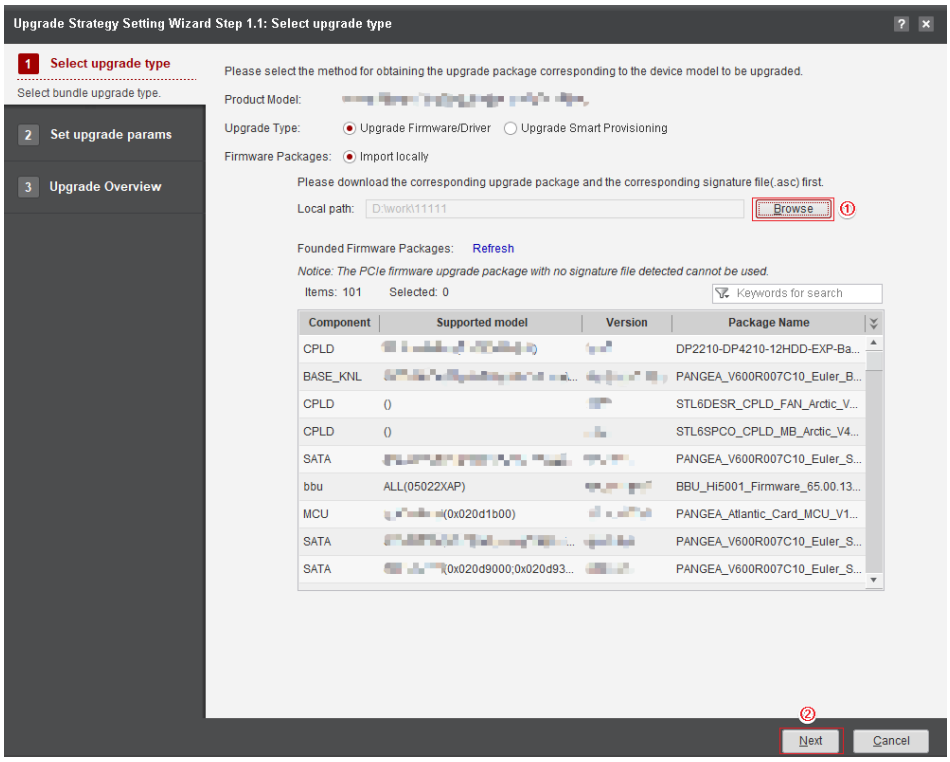
   b. Click **Set Upgrade Policy**. The **Upgrade Strategy Setting Wizard** dialog box is displayed.

   c. Import the driver upgrade package.

      Click **Browse**, select the path for storing the driver upgrade package, and click **Next**.

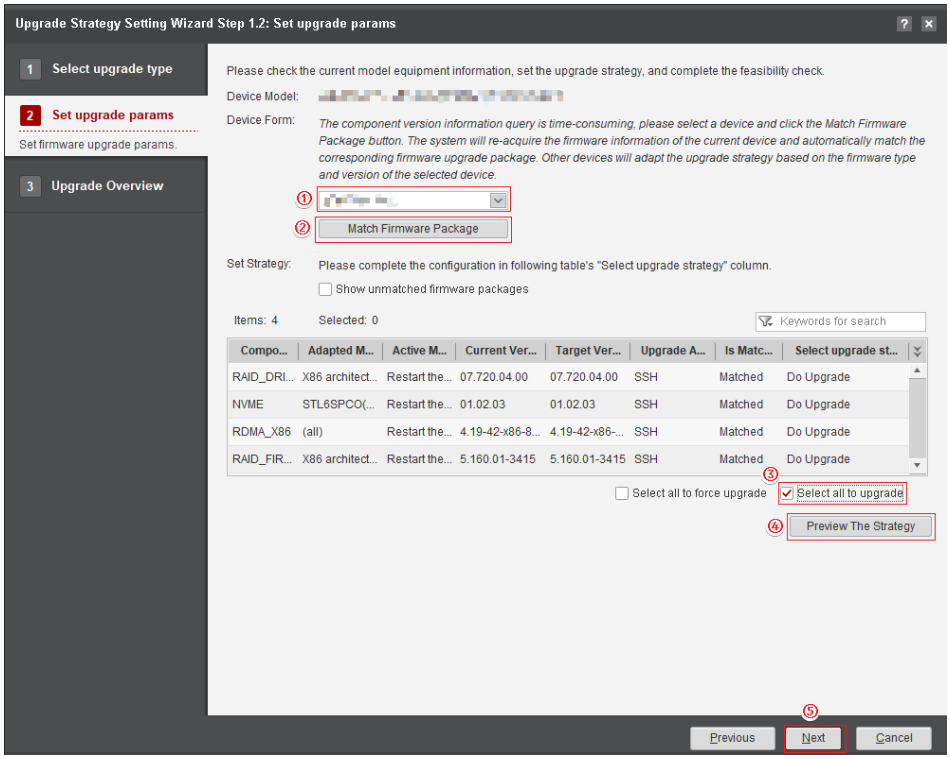
 Copyright © Huawei Technologies Co., Ltd.



NOTE

You are not advised to store other files in the path for storing the driver upgrade package. Otherwise, the parsing efficiency of the tool will be affected.

d. Set parameters.



i. Select any node as the device form.

ii. Click **Match Firmware Package**. The matched driver information will be displayed.

iii. Select the drivers to be upgraded. Based on the check result in **Checking Version Mappings**, select **Do Upgrade** in the **Select upgrade strategy** column for the drivers whose current version is earlier than the target version.

NOTE

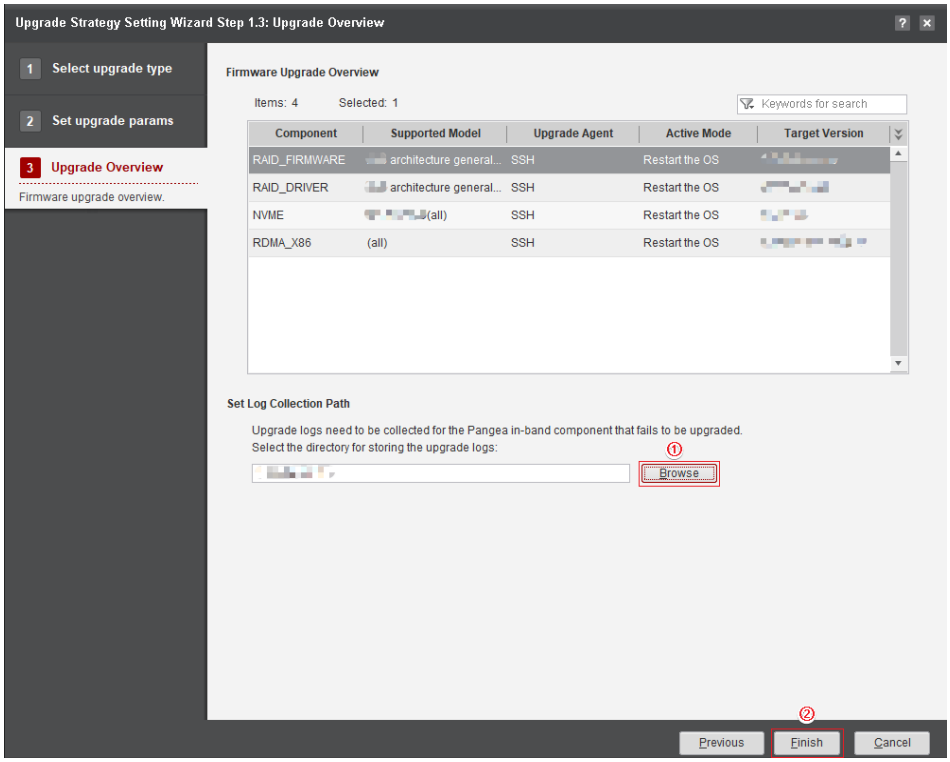
Select all to force upgrade: In special scenarios, if the current driver version is later than the target version, select this option. This option forcibly upgrades all drivers to the target version.

iv. (Optional) Click **Preview The Strategy**. The **Upgrade Strategy Preview** dialog box is displayed.

In the **Upgrade strategy** area, check that the upgrade policy to be executed in the **Expected Result** column is correct and click **OK**.

v. Click **Next**.

e. View the basic information about the driver upgrade.

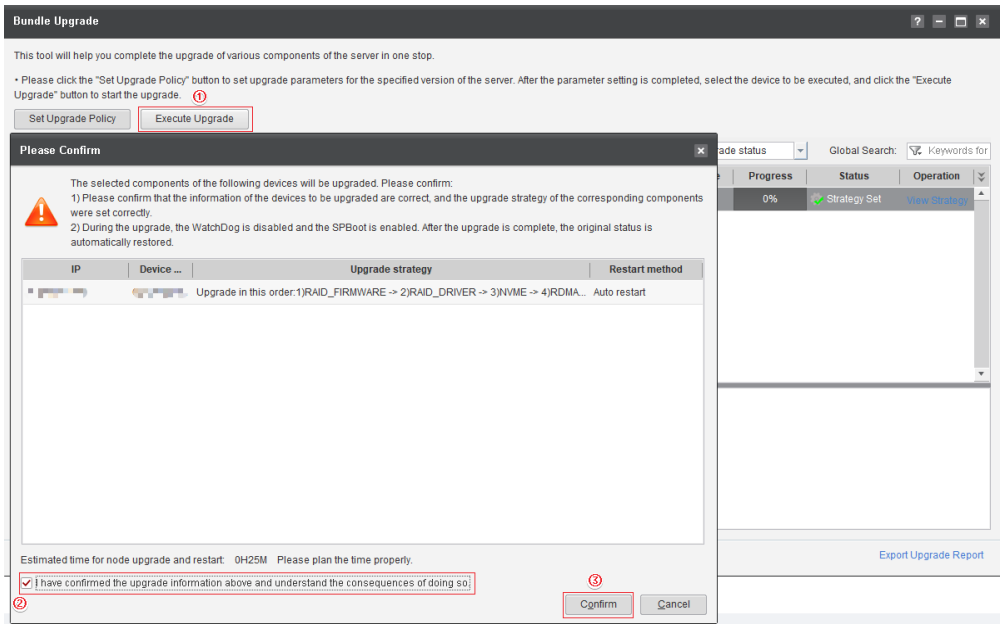


i. (Optional) Click **Browse** to set the log collection path.

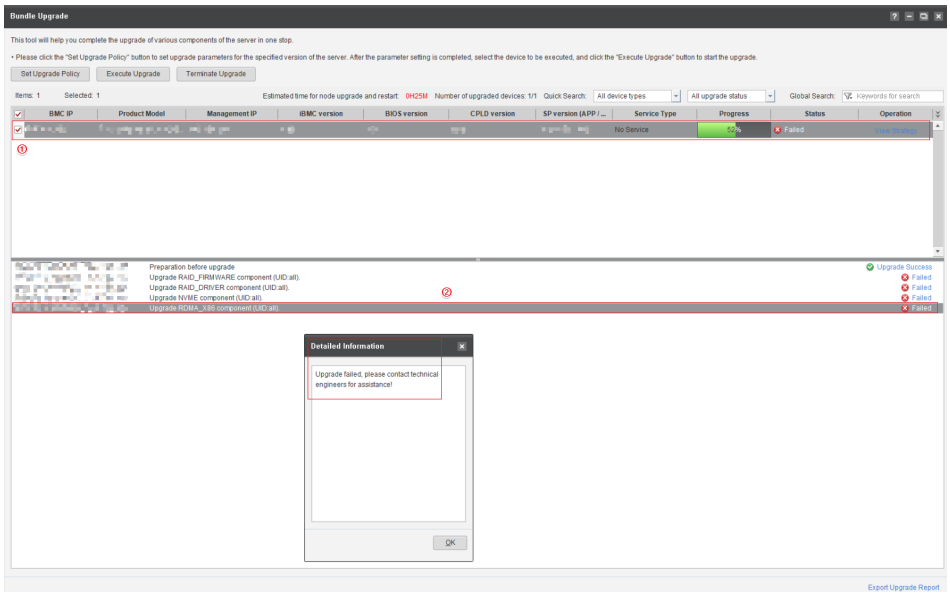
ii. Click **Finish**.

3. Click **Execute Upgrade**. A confirmation dialog box is displayed. After confirming the information, select **I have confirmed...** and click **Confirm**.

 Copyright © Huawei Technologies Co., Ltd.



4. After the upgrade is complete, check whether **Upgrade Success** is displayed in the **Status** column of all nodes.
   - If yes, click in the upper right corner of the dialog box to end the upgrade process.
   - If no, perform the following steps for each failed node (after the troubleshooting is complete, click in the upper right corner of the dialog box):



   i. Select the failed node. The upgrade details are displayed in the lower part.
   ii. In the details area, locate the failed steps and click them one by one. Then perform troubleshooting according to the description in the displayed **Detailed Information** dialog box.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

You can also click **Export Upgrade Report** in the lower right corner to collect and view the upgrade results of all nodes.

----End

5.4.2.6.2 Installing OceanStor Pacific Series Software

Scenarios

Use DeviceManager to install the OceanStor Pacific series software in LLD-based configuration mode.

Prerequisites

- The OS of the installation PC meets the compatibility requirements. For details, see the **DeviceManager-Client** requirements in **Huawei Storage Interoperability Navigator**.
- The network connection between the installation PC and all nodes is normal.
- The command prompt for user **root** is **#**.
- For OceanStor Pacific 9550/OceanStor Pacific 9350 devices, you must select all disks to create a storage pool.

Procedure

Step 1 Check the **cloud_vpc.ini** file. Perform the following operations on each storage node:

1. Use SSH to log in to a storage node as user **fsadmin**. To obtain the default user password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. After the password is changed, log in to the node again.
2. Run the **su - root** command to switch to user **root**.
3. Check the **cloud_vpc.ini** file by referring to **5.5.3 Checking the cloud_vpc.ini File**.

Step 2 Decompress **OceanStor-Pacific_8.2.1RC1_DeviceManagerClient.zip** on the installation PC, and double-click **run.bat** in the decompression directory. The browser automatically opens DeviceManager Client.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

The OS time of management nodes must be the same. Otherwise, change the time to be the same by referring to **5.5.25.7 Changing the System Time of a Node**.

During the installation, do not close the **OceanStor-Pacific_devicemanager-client** window.

The decompression directory of the software package cannot contain spaces or brackets.

DeviceManager Client cannot be opened using a shared path.

If the browser does not automatically open, open the browser manually and enter **https://127.0.0.1:***port* in the address box. The value of *port* is the character string in the **OceanStor-Pacific_devicemanager-client** window. For example, in **Starting ProtocolHandler ["https-jsse-nio-127.0.0.1-8088"]**, the port number is **8088**.

If multiple clusters need to be installed, close the **OceanStor-Pacific_devicemanager-client** window after one cluster is installed, and then open the **OceanStor-Pacific_devicemanager-client** window again to install the next cluster.

Step 3 The browser may display a message indicating that the security certificate of the website is incorrect. You can ignore the security warning message as prompted if the IP address is correct.

Take Google Chrome as an example. On the security prompt page, click **Advanced** and select **Proceed to** *XXX.XXX.XXX.XXX* **(unsafe)**. The OceanStor Pacific series installation page is displayed.

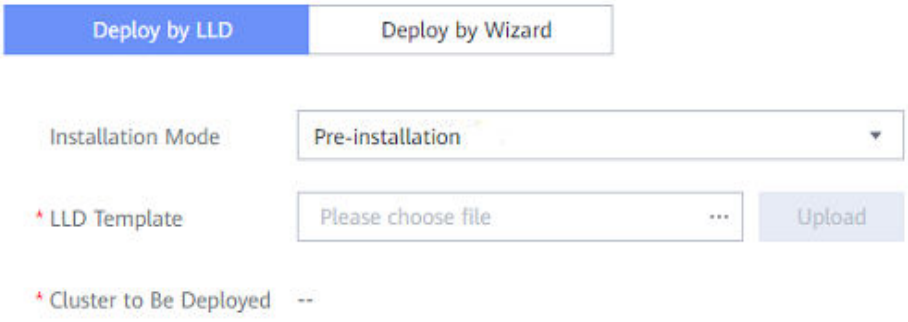
Step 4 Select **Deploy by LLD**.

Step 5 Use the LLD template to install and deploy the OceanStor Pacific series software. Two installation modes are supported: **Pre-installation** and **Regular installation**.

NOTE

- **Pre-installation**: The basic service package has been installed on the nodes and you do not need to upload the software package.
- **Regular installation**: The basic service package is not installed on the nodes and you need to upload the software package.

1. Identify the installation mode. For details, see **5.5.21 Identifying the Installation Mode**.
2. Perform the following operations depending on the installation mode.
   - Pre-installation:



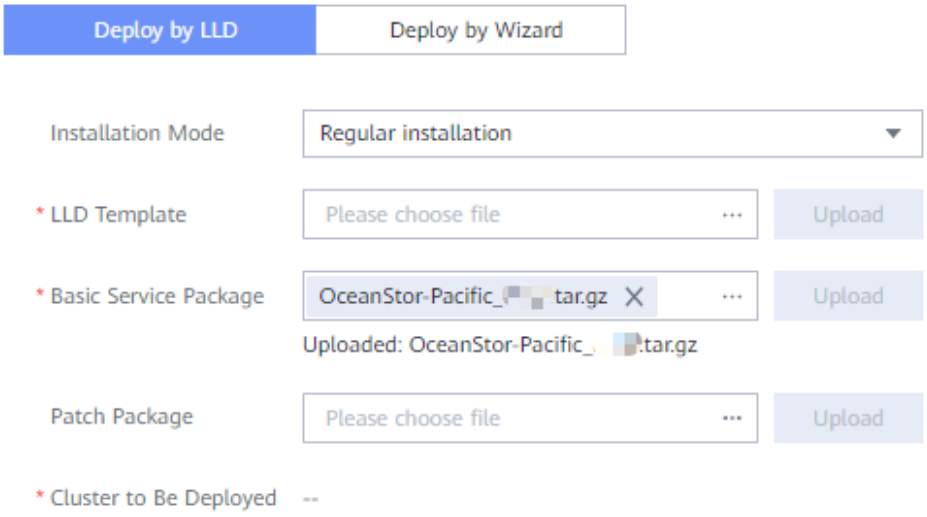
 Copyright © Huawei Technologies Co., Ltd.

i. Click ... next to **LLD Template**, select the configured LLD configuration file, and click **Upload**.

ii. **Cluster to Be Deployed** indicates the cluster name set in the LLD configuration file.

iii. Click **Deploy** to start installation and deployment of the OceanStor Pacific series software.

– Regular installation:



i. Click ... next to **LLD Template**, select the configured LLD configuration file, and click **Upload**.

ii. Upload software packages. After the upload is successful, the system displays the software package names.

1) Click ... next to **Basic Service Package**, select basic service package **OceanStor-Pacific_8.2.1RC1.tar.gz**, and click **Upload**. After the package is uploaded successfully, the system displays the package name.

2) (Optional) If a patch needs to be installed, click ... next to **Patch Package**, select patch package **OceanStor-Pacific_8.2.1RC1.SPH*XXX***, and click **Upload**.

iii. **Cluster to Be Deployed** indicates the cluster name set in the LLD configuration file.

iv. Click **Deploy** to start installation and deployment of the OceanStor Pacific series software.

Step 6 The system automatically starts to deploy the cluster.

Step 7 After the deployment is complete, ping the management, storage, or control IP addresses of other nodes from a node to ensure that the network communication between nodes is normal.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

To run the **ping** command, you need to enter the minisystem view first as follows:

1. Use an SSH tool to log in to a node as user **fsadmin** and enter the cliportal view. To obtain the default user password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. After the password is changed, log in to the node again. If the default password has been changed, use the new password to log in.
2. Run the **minisystem** command and enter the password of user **root** as prompted to go to the minisystem view.

Step 8 Load a license by referring to **5.4.2.8 Obtaining and Loading a License** so that the system can obtain a new validity period and service authorization.

----End

Follow-up Procedure

- On the installation PC, double-click the **shutdown.bat** script in the decompression directory of **OceanStor-Pacific_8.2.1RC1_DeviceManagerClient.zip** to close the DeviceManager Client window. If the window cannot exit normally, click in the upper right corner to close it.
- If the RoCE network is configured, you need to configure RoCE flow control on switches. For details, see **5.5.2.2 Configuring Flow Control for a Switch**. If you have configured RoCE flow control, skip this operation.
- If the RoCE network is configured, you need to configure ACL rules for switches. For details, see **5.5.2.3 Configuring ACL Rules for Switches**. If you have configured them, skip this operation.
- If parameter settings are incorrect after the software is installed, uninstall the OceanStor Pacific series software and reinstall it. For details about how to uninstall the OceanStor Pacific series software, see **5.5.19 Uninstalling OceanStor Pacific Series Software**.
- After the installation and deployment are complete, you can use the management IP addresses of DeviceManager and nodes to remotely log in to management and storage nodes.
- Update default accounts in time. For details, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*.
- Update security certificates in time. For details, see section "Security Certificate Management" in *OceanStor Pacific Series 8.2.1 Security Configuration Guide*.

5.4.2.7 Installation Procedure (Applicable to Wizard-based Configuration)

5.4.2.7.1 Configuring the Management IP Address of a Data Cluster Module (Applicable to OceanStor Pacific 9950)

Scenarios

Data cluster modules provide the back-end network switching function for OceanStor Pacific 9950 scale-out storage clusters. A data cluster module connects to a storage device and detects the hardware of the storage device. When it

 Copyright © Huawei Technologies Co., Ltd.

detects a risk, it reports an alarm. You can view alarms reported by the data cluster module on DeviceManager.

This section describes how to configure the management IP address of a data cluster module for subsequent management and connection of the data cluster module.

Procedure

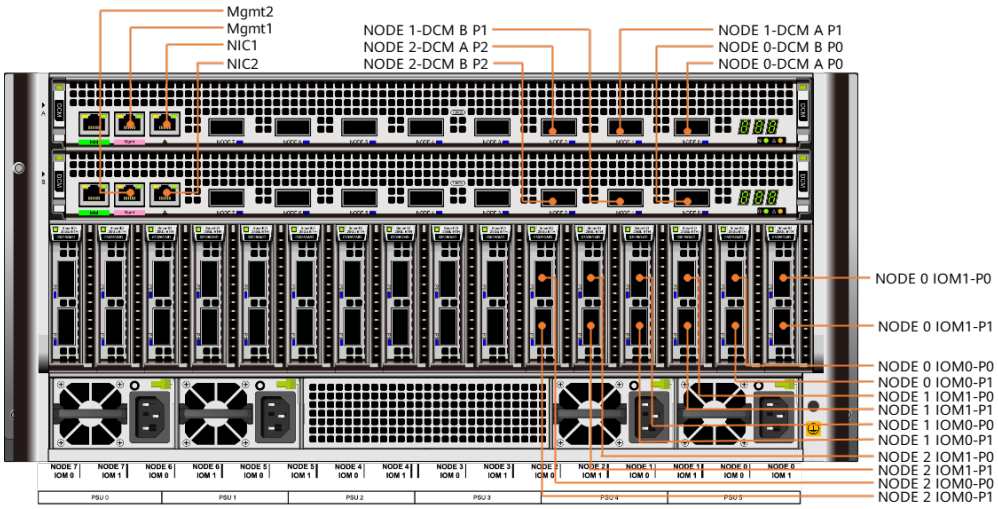
Step 1 Connect the installation PC to NIC network ports using network cables.

NOTE

The IP address of the installation PC must be in the same network segment as the default IP addresses of the NIC network ports.

Connect NIC1 and NIC2 for OceanStor Pacific 9950, as shown in **Figure 5-15**.

Figure 5-15 Example of planning ports for a storage node (using 2-port NICs)



Step 2 Configure management IP addresses. The management IP addresses of the two NIC network ports must be configured.

1. Log in to the management system.

   In the address box of a browser, enter **https://***Default IP address of a NIC network port* and enter the user name and password to log in to the management system. The default user name is **Administrator**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

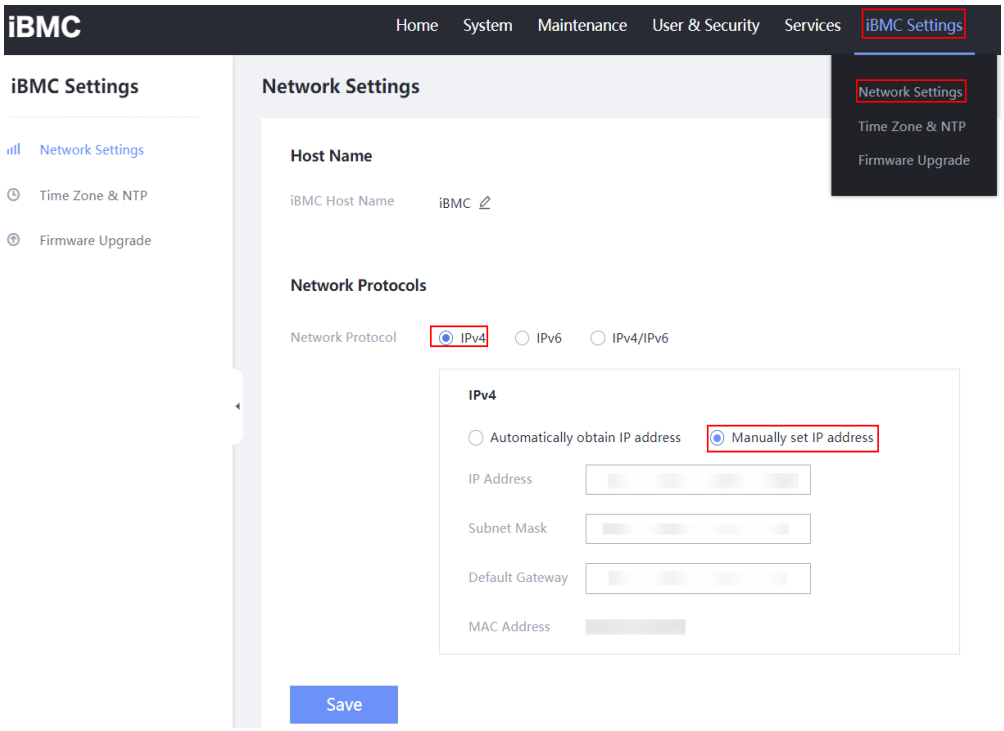
   NOTE

   The default IP address of NIC1 is 192.168.2.1, and the default IP address of NIC2 is 192.168.2.2.

2. Choose **iBMC Settings** > **Network Settings**.

   Select **IPv4** and **Manually set IP address**, and set **IP Address**, **Subnet Mask**, and **Default Gateway** in sequence.

 Copyright © Huawei Technologies Co., Ltd.



3. Click **Save**. After the modification is successful, the system displays a success message.

----End

5.4.2.7.2 Configuring iBMC IP Addresses for Nodes

Scenarios

iBMC is a remote management system. It monitors and manages hardware in a highly reliable manner.

Procedure

Step 1 Obtain the default IP addresses of iBMC management network ports.

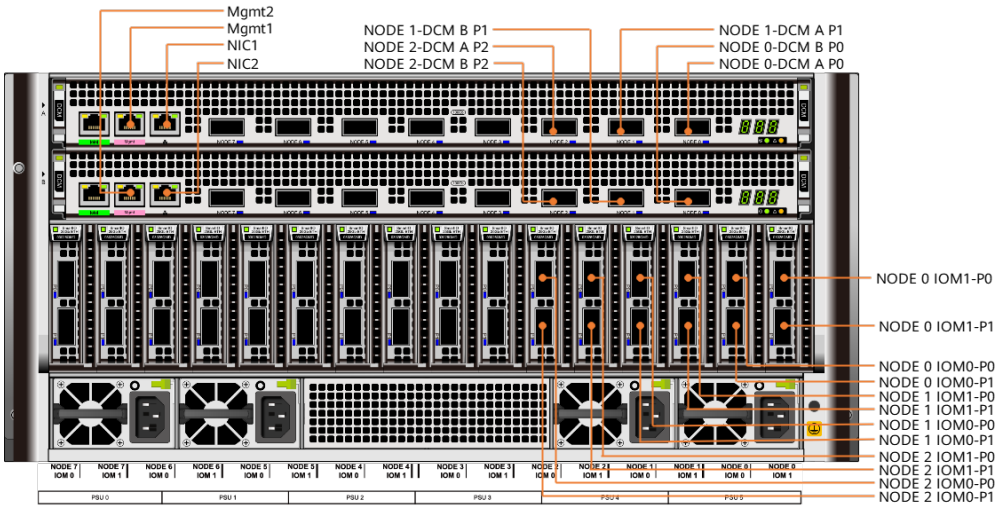
NOTE

The IP address of the installation PC must be in the same network segment as the default iBMC IP address. The default iBMC masks of all devices are 255.255.255.0.

- OceanStor Pacific 9520/OceanStor Pacific 9920:
  - For OceanStor Pacific 9520 Kunpeng-based 14-slot and OceanStor Pacific 9920 Kunpeng-based (palm-sized NVMe SSD), the default IP address is 192.168.2.101.
  - For other models of OceanStor Pacific 9520/OceanStor Pacific 9920, the default IP address is 192.168.2.100.
- For OceanStor Pacific 9540, the default iBMC IP address is 192.168.2.100.
- An OceanStor Pacific 9950 device has eight nodes whose default iBMC IP addresses are 192.168.2.101 to 192.168.2.108. The iBMC network ports of OceanStor Pacific 9950 are Mgmt1 and Mgmt2, as shown in **Figure 5-16**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-16 Example of planning ports for a storage node

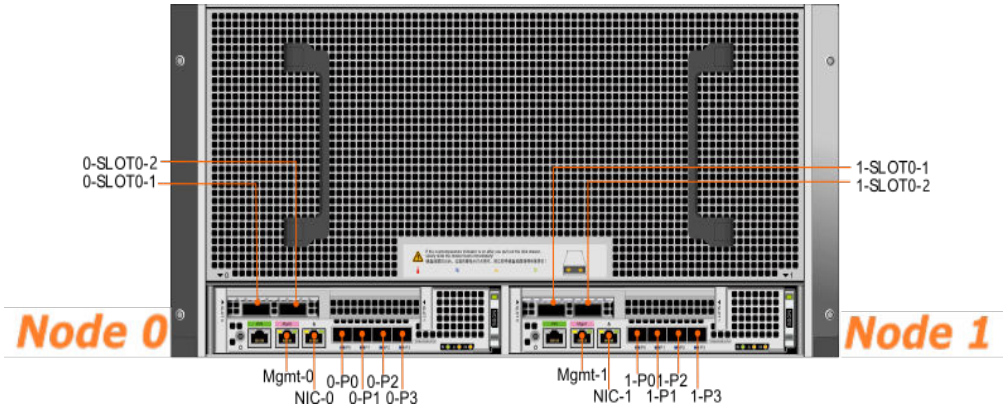


NOTE

When configuring iBMC IP addresses, connect the installation PC to either the Mgmt1 or Mgmt2 port, and do not connect the other Mgmt port to other devices. Otherwise, the installation PC cannot communicate with the default iBMC IP address.

- An OceanStor Pacific 9550 device has two nodes, whose iBMC network ports are Mgmt-0 and Mgmt-1 respectively. The default iBMC IP address corresponding to the Mgmt-0 port is 192.168.2.101, and the default iBMC IP address corresponding to the Mgmt-1 port is 192.168.2.102. **Figure 5-17** shows the iBMC network ports of OceanStor Pacific 9550.

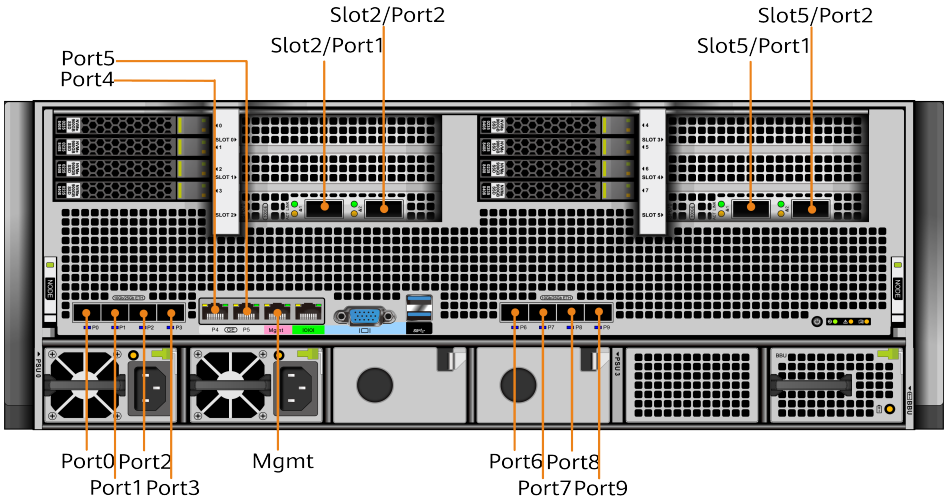
Figure 5-17 Example of planning ports for a storage node (using 2-port NICs)



- OceanStor Pacific 9546
  - The iBMC network port of OceanStor Pacific 9546 (One Node per Chassis) is the Mgmt port, and its default IP address is 192.168.2.102, as shown in **Figure 5-18**.

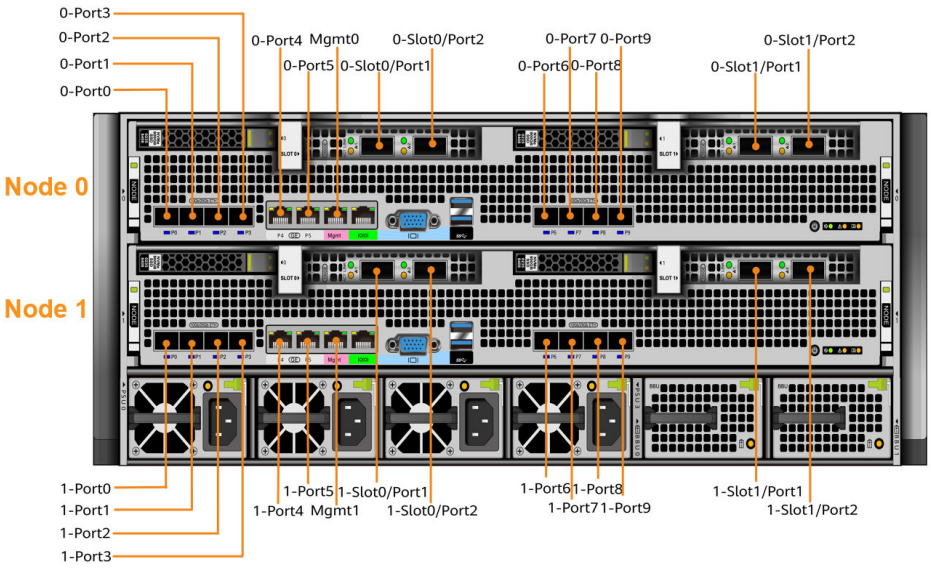
 Copyright © Huawei Technologies Co., Ltd.

Figure 5-18 Example of planning ports for a storage node



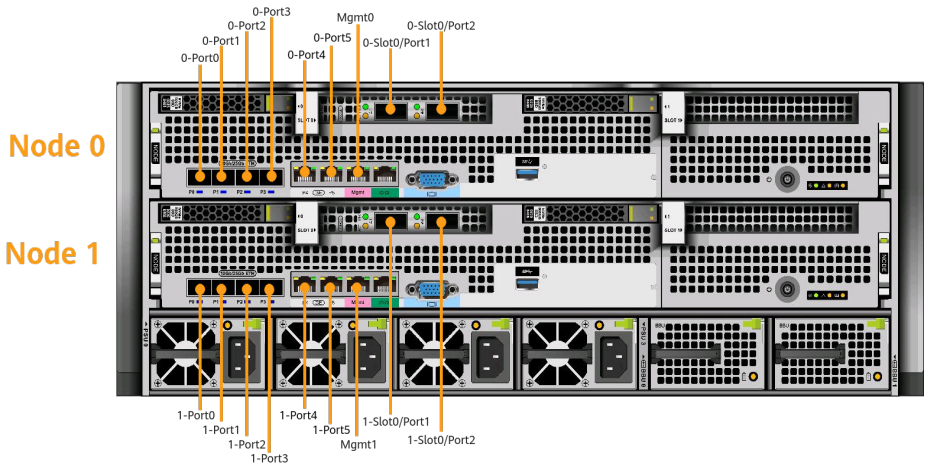
– An OceanStor Pacific 9546 (Two Nodes per Chassis) device has two nodes, whose iBMC network ports are Mgmt0 and Mgmt1 respectively. The default iBMC IP address corresponding to the Mgmt0 port is 192.168.2.101, and the default iBMC IP address corresponding to the Mgmt1 port is 192.168.2.102. **Figure 5-19** shows the iBMC network ports of OceanStor Pacific 9546 (Two Nodes per Chassis), and **Figure 5-20** shows the iBMC network ports of OceanStor Pacific 9546 (Two Nodes per Chassis, One CPU per Node).

Figure 5-19 Example of planning ports for a node with two CPUs



 Copyright © Huawei Technologies Co., Ltd.

Figure 5-20 Example of planning ports for a node with one CPU



Step 2 In the address box of a browser, enter **https://***Default IP address of the iBMC management network port* and enter the user name and password to log in to the iBMC system of a node. The default user name is **Administrator**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

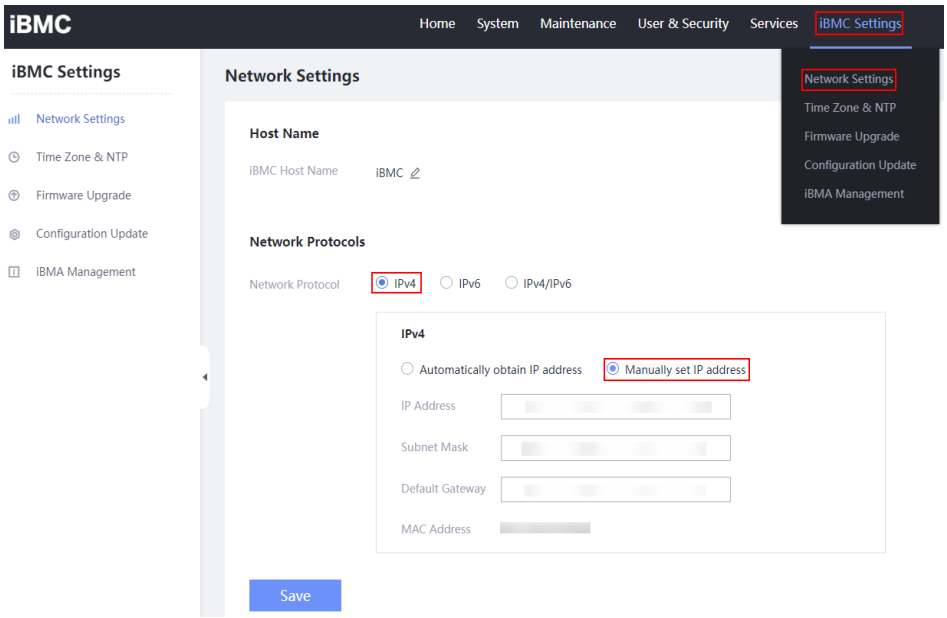
Step 3 Configure iBMC IP addresses.

1. Choose **iBMC Settings** > **Network Settings**.

   NOTE

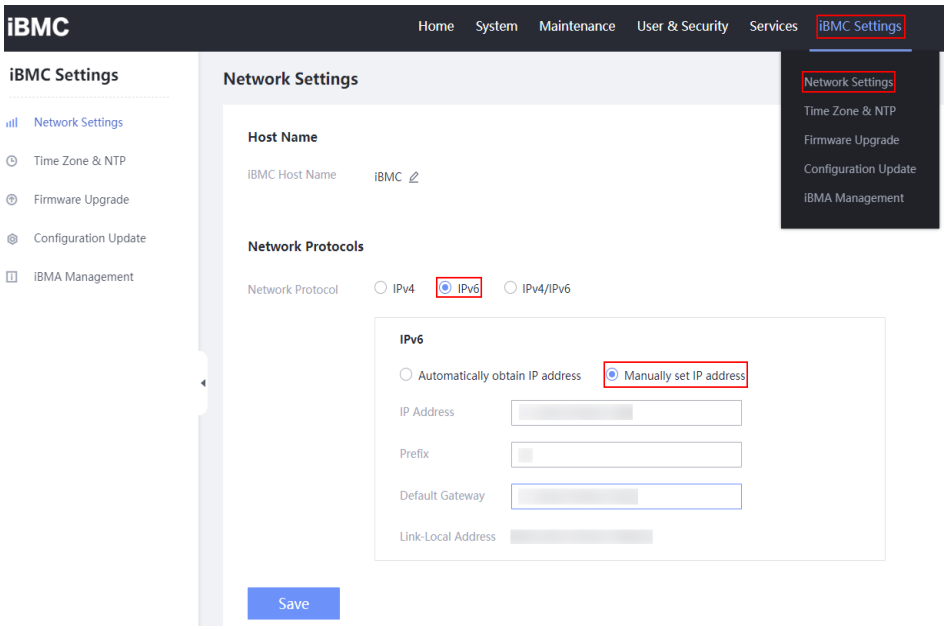
   For details about the support for IPv4 and IPv6, see section "Network Requirements" of the desired scenario in *OceanStor Pacific Series 8.2.1 Network Planning Guide (SFS)*.

   - When configuring IPv4 addresses, select **IPv4** and **Manually set IP address**, and set **IP Address**, **Subnet Mask**, and **Default Gateway** in sequence.



   - When configuring IPv6 addresses, select **IPv6** and **Manually set IP address**, and set **IP Address**, **Prefix**, and **Default Gateway** in sequence.

 Copyright © Huawei Technologies Co., Ltd.



2. Click **Save**. After the modification is successful, the system displays a success message.

----End

5.4.2.7.3 Checking Storage Nodes Before Installation

5.4.2.7.3.1 Checking Whether a RAID Controller Card Is Used (Applicable to Kunpeng-based Devices)

Procedure

Step 1 Log in to the iBMC system.

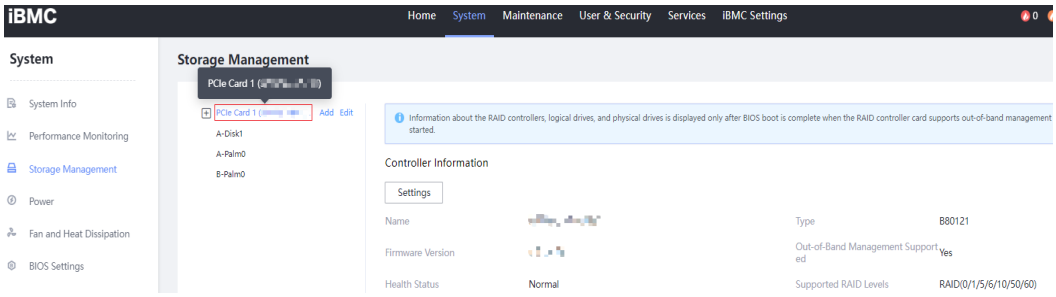
Enter the new iBMC IP address in the address box of a browser and enter the user name and password to log in to the iBMC system of a node. The default user name is **Administrator**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

- **https://***iBMC IPv4 address*
- **https://[***iBMC IPv6 address***]**

Step 2 Choose **System** > **Storage Management**. If **PCIe Card** *Slot number* **(***RAID controller card model***)** or **RAID Card***Slot number* is displayed, a RAID controller card is used.

An example is provided as follows:

 Copyright © Huawei Technologies Co., Ltd.



----End

5.4.2.7.3.2 OceanStor Pacific 9950, 9550, and 9546

?.1. Checking the Node Firmware Version

Procedure

Step 1 Log in to the iBMC system.

Enter the new iBMC IP address in the address box of a browser and enter the user name and password to log in to the iBMC system of a node. The default user name is **Administrator**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

https://*iBMC IPv4 address*

Step 2 Go to the **Home** page. Check whether **iBMC Firmware Version** and **BIOS Firmware Version** of the node meet the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

Step 3 Choose **iBMC Settings** > **Firmware Upgrade** > **Version Info**. Check whether **CPLD Version** meets the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

Step 4 If the requirements are not met, upgrade the firmware to the target version by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*.

----End

?.2. Checking the OS Version

Procedure

Step 1 Go to the **Home** page of iBMC. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 2 Open the virtual KVM interface, and enter user name **root** to log in to the OS of the storage node. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

Step 3 Run the following command to check whether the OS version meets the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

 Copyright © Huawei Technologies Co., Ltd.

```
cat /proc/version
```

- If the requirements are met, perform the following operations in sequence:
  a. Check the **cloud_vpc.ini** file by referring to **5.5.3 Checking the cloud_vpc.ini File**.
  b. Go to **Checking BIOS Settings**.
- If the requirements are not met, perform the following operations in sequence:
  a. Set BIOS parameters by referring to **5.5.5.1 Configuring BIOS (Applicable to OceanStor Pacific 9950, 9550, 9546, 9350, and 9346)**.
  b. Install an OS that meets the requirements by referring to **5.5.6.1 Installing an OS (Applicable to OceanStor Pacific 9950, 9550, 9546, 9350, and 9346)**.
  c. Upgrade the NIC and disk firmware and drivers by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*.
  d. Check the Hi1822V120 NIC mode by referring to **Checking the Hi1822V120 NIC Mode**.
  e. Check the **cloud_vpc.ini** file by referring to **5.5.3 Checking the cloud_vpc.ini File**.
  f. Configure networks by referring to **5.4.2.7.4 Configuring the Management Network of a Node**.

----End

?.3. Checking BIOS Settings

Procedure

Step 1 Log in to the iBMC system.

Step 2 Choose **iBMC Settings** > **Configuration Update** > **Export Configuration**.

Step 3 Click **Export**.

Step 4 Query the following information in the exported configuration file:

- Check whether the value of **BbuBackForCpuOff** is **Enabled**.
- Check whether the value of **OneNumaEnable** is **Enabled**.
- For OceanStor Pacific 9950, check whether the value of **BbuNvSize** is **32G**.
- For OceanStor Pacific 9550, check whether the value of **BbuNvSize** is **16G**.
- For OceanStor Pacific 9546, check whether the value of **BbuNvSize** is **16G**.
- Check whether the value of **BbuUceEnhance** is **Enable**.

NOTICE

Ensure that the value of **OneNumaEnable** in the configuration file is the same as the preceding value.

Copyright © Huawei Technologies Co., Ltd.

If the queried values are different from the preceding values, set the parameters by referring to **5.5.5.1 Configuring BIOS (Applicable to OceanStor Pacific 9950, 9550, 9546, 9350, and 9346)**.

----End

?.4. Checking the Device Firmware and Driver Versions

Procedure

Step 1 Log in to the iBMC system.

NOTE

An OceanStor Pacific 9950 device has eight nodes. You need to log in to the iBMC of each node and perform the following operations.

An OceanStor Pacific 9550 device has two nodes. You need to log in to the iBMC of each node and perform the following operations.

An OceanStor Pacific 9546 device has one or two nodes. You need to log in to the iBMC of each node and perform the following operations.

Step 2 Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 3 Enter user name **root** and its new password to log in to a node.

Step 4 Configure a temporary management IP address for a storage node.

- **ifconfig** *Management plane NIC name Temporary IPv4 address/Number of subnet mask bits* **up**
- **route add default gw** *Default gateway*

```
ifconfig enp125s0f4 192.168.40.15/24 up
route add default gw 192.168.40.1
```

NOTE

Management plane NIC name of OceanStor Pacific 9550 is **enp125s0f4** or **enp125s0f5**.

Management plane NIC name of OceanStor Pacific 9950 is **enp125s0f2** or **enp125s0f3**.

Management plane NIC name of OceanStor Pacific 9546 is **enp125s0f4**.

Step 5 Use PuTTY to log in to a storage node as user **fsadmin**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*.

Run the following command to switch to user **root**.

```
su - root
```

NOTE

If you log in as user **fsadmin** for the first time, change the default password.

Step 6 Check whether the firmware and driver versions meet the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping* by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*. If no, upgrade the firmware and driver versions to the target versions.

----End

 Copyright © Huawei Technologies Co., Ltd.

?.5. Checking the Hi1822V120 NIC Mode

Context

This section describes how to check whether the Hi1822V120 NIC mode is Open vSwitch (OVS), and how to switch the NIC mode if it is not OVS.

Prerequisites

This operation applies only to OceanStor Pacific 9546 and OceanStor Pacific 9346.

Procedure

Step 1 Use a remote connection tool to log in to the system and switch to user **root**.

Step 2 Disable the intrusion detection service to prevent a false positive. If the OS does not support this service, skip this step.

```
Euler:~ # systemctl stop secAgent
```

Step 3 Run the following command to check the Hi1822V120 NIC mode.

```
Euler:~ # hinicadm3 info
Card num:2
Device Information:
    Card        PCIe Function
|----hinic0(CAL_4X25G)
        |--------0000:87:00.0(NIC:enp135s0f0)
        |--------0000:87:00.1(NIC:enp135s0f1)
        |--------0000:87:00.2(NIC:enp135s0f2)
        |--------0000:87:00.3(NIC:enp135s0f3)
        |--------0000:87:00.4(NIC:enp135s0f4)
        |--------0000:87:00.5(NIC:enp135s0f5)
|----hinic1(CAL_4X25G)
        |--------0000:01:00.0(NIC:enp1s0f0)
        |--------0000:01:00.1(NIC:enp1s0f1)
        |--------0000:01:00.2(NIC:enp1s0f2)
        |--------0000:01:00.3(NIC:enp1s0f3)
```

If one NIC in the command output contains six NIC records (the NIC information is displayed below **|----hinic*x*(CAL_4X25G)**), the server has NICs in OVS mode. In this case, you do not need to switch the NIC mode. Otherwise, go to **Step 4** to switch the NIC mode.

Step 4 Switch the NIC mode to OVS. For details, see **Installing/Upgrading the Firmware and Drivers (Function Manual)** > **Installing/Upgrading Firmware and Drivers for OceanStor Pacific 9546, 9346, and 9146** > **Installing/Upgrading the Hi1822V120 NIC Firmware and Driver** > **Switching the NIC Mode (Applicable to SFS Scenarios)** in *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*. In NIC mode switching command **./appctl switch_mode -slot** *slotid* **-type** *mode*, the value of *mode* is **ovs**. For details about the value of *slotid*, see **Table 5-40**.

Table 5-40 slotid in the device service network

Device Name	slotid in the Service Network
OceanStor Pacific 9546	all
OceanStor Pacific 9346	2

Copyright © Huawei Technologies Co., Ltd.

----End

5.4.2.7.3.3 OceanStor Pacific 9540 Kunpeng-based Without a RAID Controller Card and 9920 Kunpeng-based Without a RAID Controller Card

?.1. OceanStor Pacific 9920 Kunpeng-based (Palm-sized NVMe SSD) Without a RAID Controller Card

?.1. Checking the Node Firmware Version

Procedure

Step 1 Log in to the iBMC system.

Enter the new iBMC IP address in the address box of a browser and enter the user name and password to log in to the iBMC system of a node. The default user name is **Administrator**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

- **https://***iBMC IPv4 address*
- **https://[***iBMC IPv6 address***]**

Step 2 Choose **System** > **System Info** > **Product Info** > **Mainboard Info**.

Step 3 Check whether **iBMC Firmware Version**, **CPLD Version**, and **BIOS Version** meet the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

If the requirements are not met, upgrade the firmware to the target version by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*.

----End

?.2. Checking the OS Version

Procedure

Step 1 Log in to the iBMC system.

Step 2 Go to the **Home** page of iBMC. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 3 Enter user name **root** and its password to log in to the OS of a storage node. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

Step 4 Run the following command to check whether the OS version meets the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

```
cat /proc/version
```

- If the requirements are met, go to **Checking BIOS Settings**.

 Copyright © Huawei Technologies Co., Ltd.

- If the requirements are not met, perform the following operations in sequence:
  a. Set BIOS parameters by referring to **5.5.5.2.1 Configuring BIOS (Applicable to OceanStor Pacific 9520 Kunpeng-based 14-Slot and 9920 Kunpeng-based (Palm-sized NVMe SSD))**.
  b. Install an OS that meets the requirements by referring to **5.5.6.2.1 Installing an OS (Applicable to OceanStor Pacific 9520 Kunpeng-based 14-Slot Without a RAID Controller Card and 9920 Kunpeng-based (Palm-sized NVMe SSD) Without a RAID Controller Card)**.
  c. Upgrade the NIC and disk firmware and drivers by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*.
  d. Configure networks by referring to **5.4.2.7.4 Configuring the Management Network of a Node**.

----End

?.3. Checking BIOS Settings

Procedure

Step 1 Log in to the iBMC system.

Step 2 Choose **iBMC Settings** > **Configuration Update** > **Export Configuration**.

Step 3 Click **Export**.

Step 4 Check the following information in the exported configuration file:

- Check whether the value of **OneNumaEnable** is **Enabled**.
- For OceanStor Pacific 9520 Kunpeng-based 14-slot, check whether the value of **BbuNvSize** is **16G**.
- For OceanStor Pacific 9920 Kunpeng-based (palm-sized NVMe SSD), check whether the value of **BbuNvSize** is **32G**.
- Check whether the value of **BbuUceEnhance** is **Enable**.
- Check whether the value of **BbuBackForCpuOff** is **Enabled**.

NOTICE

Ensure that the value of **OneNumaEnable** in the configuration file is the same as the preceding value.

If the queried values are different from the preceding values, set the parameters by referring to **5.5.5.2.1 Configuring BIOS (Applicable to OceanStor Pacific 9520 Kunpeng-based 14-Slot and 9920 Kunpeng-based (Palm-sized NVMe SSD))**.

----End

 Copyright © Huawei Technologies Co., Ltd.

?.4. Checking the Device Firmware and Driver Versions

Procedure

Step 1 Log in to the iBMC system.

Step 2 Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 3 Enter user name **root** and its new password to log in to a node.

Step 4 Configure a temporary management IP address for a storage node.

To configure an IPv4 address, run the following commands:

- **ifconfig** *Management plane NIC name Temporary IPv4 address/Number of subnet mask bits* **up**
- **route add default gw** *Default gateway*

```
ifconfig enp125s0f0 192.168.40.15/24 up
route add default gw 192.168.40.1
```

To configure an IPv6 address, run the following commands:

- **ifconfig** *Management plane NIC name* **add** *Temporary IPv6 address/Prefix* **up**
- **route -A inet6 add default gw** *Default gateway*

```
ifconfig enp2s0f0:3 add FC00::102/64 up
route -A inet6 add default gw FC00::101
```

Step 5 Use PuTTY to log in to a storage node as user **fsadmin**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*.

Run the following command to switch to user **root**.

```
su - root
```

NOTE

If you log in as user **fsadmin** for the first time, change the default password.

Step 6 Check whether the firmware and driver versions meet the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping* by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*. If no, upgrade the firmware and driver versions to the target versions.

----End

?.2. Other Kunpeng-based Models Without a RAID Controller Card

?.1. Checking the Node Firmware Version

Procedure

Step 1 Log in to the iBMC system.

Enter the new iBMC IP address in the address box of a browser and enter the user name and password to log in to the iBMC system of a node. The default user name is **Administrator**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

 Copyright © Huawei Technologies Co., Ltd.

- **https://***iBMC IPv4 address*
- **https://[***iBMC IPv6 address***]**

Step 2 Choose **System** > **System Info** > **Product Info** > **Mainboard Info**.

Step 3 Check whether **iBMC Firmware Version**, **CPLD Version**, and **BIOS Version** meet the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

If the requirements are not met, upgrade the firmware to the target version by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*.

----End

?.2. Checking the OS Version

Procedure

Step 1 Go to the **Home** page of iBMC. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 2 Open the virtual KVM interface, and enter user name **root** to log in to the OS of the storage node. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

Step 3 Run the following command to check whether the OS version meets the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

```
cat /proc/version
```

- If the requirements are met, perform the following operations in sequence:
  a. Check the **cloud_vpc.ini** file by referring to **5.5.3 Checking the cloud_vpc.ini File**.
  b. Go to **Checking BIOS Settings**.
- If the requirements are not met, perform the following operations in sequence:
  a. Set BIOS parameters by referring to **5.5.5.2.2 Configuring BIOS (Applicable to Other Kunpeng-based Devices)**.
  b. Install an OS that meets the requirements by referring to **5.5.6.2.2 Installing an OS (Applicable to Other Kunpeng-based Models Without a RAID Controller Card)**.
  c. Upgrade the ES3000 and NIC tools, drivers, and firmware by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*.
  d. Check the Hi1822V120 NIC mode by referring to **Checking the Hi1822V120 NIC Mode**.
  e. Check the compatibility of the disk backplane by referring to **Checking the Compatibility of a Disk Backplane**.
  f. Check the **cloud_vpc.ini** file by referring to **5.5.3 Checking the cloud_vpc.ini File**.
  g. Configure networks by referring to **5.4.2.7.4 Configuring the Management Network of a Node**.

----End

 Copyright © Huawei Technologies Co., Ltd.

?.3. Checking BIOS Settings

Procedure

Step 1 Log in to the iBMC system.

Step 2 Choose **iBMC Settings** > **Configuration Update** > **Export Configuration** or **Configuration** > **Import/Export**.

Step 3 Click **Export**.

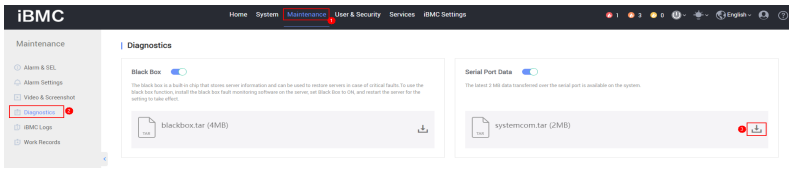
Step 4 Query the following information in the exported configuration file:

- Check whether the value of **EnableSMMU** (corresponding to **Support Smmu** in the BIOS) is **Disabled**.
- Check whether the value of **DieInterleaving** is **Enabled**.
- Check whether the value of **NUMAEn** (corresponding to **NUMA** in the BIOS) is **Enabled**.
- Check whether the value of **OneNumaEnable** (corresponding to **One Numa Per Socket** in the BIOS) is **Enabled**.
- Check whether the value of **ColdBootFastSupport** is **Disabled**.
- Check whether the value of **BbuNvSize** is **16G**.
- Check whether the value of **X8MisCorrEn** (corresponding to **AB Check** in the BIOS) is **Enabled**.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

- Ensure that the values of **NUMAEn** and **OneNumaEnable** in the configuration file are the same as the preceding values.
- If a device uses a 32-core CPU, you do not need to check **OneNumaEnable**. To query the number of CPU cores, log in to the iBMC WebUI and choose **System** > **System Info** > **Processors** > **Cores/Threads**.
- **X8MisCorrEn** (corresponding to **AB Check** in the BIOS) applies to the following BIOS versions of Kunpeng 920-based nodes:
  - BIOS 1.91 or later for the 1620 VD 1.5 mainboard
  - BIOS 5.21 or later for the 1620S VE 2.0/V150 mainboard
- The default value of **SecureBoot** in the BIOS is **Disable**. To avoid installation problems, you are advised to check whether the value is **Disable**. The check methods are as follows:
  - Log in to the iBMC WebUI, choose **Maintenance** > **Diagnostics**, download the **systemcom.tar** file, view the file content, search for **SecureBoot CurrentValue**, and check whether the value of **SecureBoot CurrentValue** is **0**.



  - Check the BIOS. For details, see the step describing how to modify secure boot in **5.5.5.2.2 Configuring BIOS (Applicable to Other Kunpeng-based Devices)**.

If the queried values are different from the preceding values, set the parameters by referring to **5.5.5.2.2 Configuring BIOS (Applicable to Other Kunpeng-based Devices)**.

----End

?.4. Checking the Device Firmware and Driver Versions

Procedure

Step 1 Log in to the iBMC system.

Step 2 Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 3 Enter user name **root** and its new password to log in to a node.

Step 4 Configure a temporary management IP address for a storage node.

To configure an IPv4 address, run the following commands:

- **ifconfig** *Management plane NIC name Temporary IPv4 address/Number of subnet mask bits* **up**
- **route add default gw** *Default gateway*

 Copyright © Huawei Technologies Co., Ltd.

```
ifconfig enp125s0f0 192.168.40.15/24 up
route add default gw 192.168.40.1
```

To configure an IPv6 address, run the following commands:

- **ifconfig** *Management plane NIC name* **add** *Temporary IPv6 address/Prefix* **up**
- **route -A inet6 add default gw** *Default gateway*

```
ifconfig enp2s0f0:3 add FC00::102/64 up
route -A inet6 add default gw FC00::101
```

Step 5 Use PuTTY to log in to a storage node as user **fsadmin**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*.

Run the following command to switch to user **root**.

```
su - root
```

NOTE

If you log in as user **fsadmin** for the first time, change the default password.

Step 6 Check whether the firmware and driver versions meet the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping* by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*. If no, upgrade the firmware and driver versions to the target versions.

----End

?.5. Checking the Hi1822V120 NIC Mode

Context

This section describes how to check whether the Hi1822V120 NIC mode is Open vSwitch (OVS), and how to switch the NIC mode if it is not OVS.

Prerequisites

This operation applies only to OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9920 Kunpeng-based, OceanStor Pacific 9340 Kunpeng-based, and OceanStor Pacific 9520 Kunpeng-based.

Procedure

Step 1 Use a remote connection tool to log in to the system and switch to user **root**.

Step 2 Disable the intrusion detection service to prevent a false positive. If the OS does not support this service, skip this step.

```
Euler:~ # systemctl stop secAgent
```

Step 3 Run the following command to check the Hi1822V120 NIC mode.

```
Euler:~ # hinicadm3 info
Card num:2
Device Information:
    Card        PCIe Function
|----hinic0(CAL_4X25G)
       |--------0000:87:00.0(NIC:enp135s0f0)
       |--------0000:87:00.1(NIC:enp135s0f1)
       |--------0000:87:00.2(NIC:enp135s0f2)
       |--------0000:87:00.3(NIC:enp135s0f3)
```

 Copyright © Huawei Technologies Co., Ltd.

```
        |--------0000:87:00.4(NIC:enp135s0f4)
        |--------0000:87:00.5(NIC:enp135s0f5)
|----hinic1(CAL_4X25G)
        |--------0000:01:00.0(NIC:enp1s0f0)
        |--------0000:01:00.1(NIC:enp1s0f1)
        |--------0000:01:00.2(NIC:enp1s0f2)
        |--------0000:01:00.3(NIC:enp1s0f3)
```

If one NIC in the command output contains six NIC records (the NIC information is displayed below **|----hinic*x*(CAL_4X25G)**), the server has NICs in OVS mode. In this case, you do not need to switch the NIC mode. Otherwise, go to **Step 4** to switch the NIC mode.

Step 4 Switch the NIC mode to OVS. For details, see **Installing/Upgrading the Firmware and Drivers (Function Manual)** > **Installing/Upgrading Firmware and Drivers for OceanStor Pacific 9520, 9540, 9340, and 9920** > **Installing/Upgrading the Hi1822V120 NIC Firmware and Driver** > **Switching the NIC Mode (Applicable to SFS Scenarios)** in *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*. In NIC mode switching command **./appctl switch_mode -slot** *slotid* **-type** *mode*, the value of *mode* is **ovs**. For details about the value of *slotid*, see **Table 5-41**.

Table 5-41 slotid in the device service network

Device Name	slotid in the Service Network
OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9920 Kunpeng-based, or OceanStor Pacific 9340 Kunpeng-based	3
OceanStor Pacific 9520 Kunpeng-based	5

----End

?.6. Checking the Compatibility of a Disk Backplane

Procedure

Step 1 Query the model and version of a disk module.

1. Log in to the target node as user **fsadmin**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. Run the **su - root** command and enter the password of user **root** to switch to user **root**.
2. Run the **lsscsi -g** command to query the model and version of a disk module.

```
                    lsscsi -g
[0:0:42:0]   disk    ATA      WUS721010ALE6L4  W9C0  /dev/sda   /dev/sg0
[0:0:43:0]   disk    ATA      WUS721010ALE6L4  W950  /dev/sdb   /dev/sg1
[0:0:66:0]   enclosu HUAWEI   Expander 12Gx16  131   -          /dev/sg8
[0:2:0:0]    disk    AVAGO    HW-SAS3508       5.14  /dev/sdi   /dev/sg9
```

In the row containing **disk** of the command output, if the model is **HUS726T6TALE600** and the version is **T9***xx* (excluding T9C0) or if the model

 Copyright © Huawei Technologies Co., Ltd.

is **WUS721010ALE6L4** and the version is **W9***xx* (excluding W9C0), go to **Step 2**. Otherwise, there is no compatibility problem.

Step 2 Query the model of the disk backplane.

1. Log in to the iBMC WebUI page of the target node.
2. Choose **System** > **System Info** > **Others** > **Drive Backplanes**, and query **Board ID** of the disk backplane.

   NOTE

   If the iBMC versions are inconsistent, log in to the iBMC WebUI, choose **Information** > **System Info** > **Other Devices** > **Drive Backplanes**, and query **Board ID** of the disk backplane.

   - If the board ID is not **0x0073** or **0x0083**, there is no compatibility problem.
   - If the board ID is **0x0073**, go to **Step 3**.
   - If the board ID is **0x0083**, contact Huawei technical support engineers.

Step 3 Query the firmware version of the spare disk backplane.

Log in to the target node as user **fsadmin**. Run the **su - root** command and enter the password of user **root** to switch to user **root**. Run the **lsscsi -g** command to query the firmware version of the disk backplane.

```
[root@localhost ~]# lsscsi -g
[0:0:5:0]    disk    ATA      HUH721010ALE600  T3X6  /dev/sda   /dev/sg0
[0:0:6:0]    disk    ATA      HUH721010ALE600  T3X6  /dev/sdb   /dev/sg1
[0:0:8:0]    disk    ATA      HUH721010ALE600  T3X6  /dev/sdc   /dev/sg2
[0:0:17:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdd   /dev/sg3
[0:0:18:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sde   /dev/sg4
[0:0:25:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdf   /dev/sg5
[0:0:42:0]   disk    ATA      MG06ACA10TE      0808  /dev/sdg   /dev/sg6
[0:0:44:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdh   /dev/sg7
[0:0:45:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdi   /dev/sg8
[0:0:48:0]   disk    ATA      HUH721010ALN600  T2JC  /dev/sdj   /dev/sg9
[0:0:51:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdk   /dev/sg10
[0:0:55:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdl   /dev/sg11
[0:0:65:0]   enclosu HUAWEI   Expander 12Gx16  331   -          /dev/sg12
[0:2:0:0]    disk    AVAGO    HW-SAS3408       5.03  /dev/sdm   /dev/sg13
```

- If the version in the **enclosu** row in the command output is **331**, there is no compatibility problem.
- If the version in the **enclosu** row in the command output is not **331**, contact Huawei technical support engineers.

----End

5.4.2.7.3.4 OceanStor Pacific 9540 Kunpeng-based with a RAID Controller Card

?.1. Checking the Node Firmware Version

Procedure

Step 1 Log in to the iBMC system.

Enter the new iBMC IP address in the address box of a browser and enter the user name and password to log in to the iBMC system of a node. The default user

 Copyright © Huawei Technologies Co., Ltd.

name is **Administrator**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

- **https://***iBMC IPv4 address*
- **https://[***iBMC IPv6 address***]**

Step 2 Choose **System** > **System Info** > **Product Info** > **Mainboard Info**.

Step 3 Check whether **iBMC Firmware Version**, **CPLD Version**, and **BIOS Version** meet the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

If the requirements are not met, upgrade the firmware to the target version by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*.

----End

?.2. Checking the OS Version

Procedure

Step 1 Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 2 Open the virtual KVM interface, and enter user name **root** to log in to the OS of the storage node. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

Step 3 Run the following command to check whether the OS version meets the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.

```
cat /proc/version
```

- If the requirements are met, perform the following operations in sequence:
  a. Check the **cloud_vpc.ini** file by referring to **5.5.3 Checking the cloud_vpc.ini File**.
  b. Go to **Checking the Cache Policy of a System Disk**.
- If the requirements are not met, perform the following operations in sequence:
  a. Enable the JBOD function by referring to **5.5.4 Enabling JBOD (Applicable to OceanStor Pacific 9540 Kunpeng-based, 9520 Kunpeng-based, 9920 Kunpeng-based, and 9340 Kunpeng-based)**.
  b. Set BIOS parameters by referring to **5.5.5.2.2 Configuring BIOS (Applicable to Other Kunpeng-based Devices)**.
  c. Install an OS that meets the requirements by referring to **5.5.6.3 Installing an OS (Applicable to OceanStor Pacific 9520 Kunpeng-based with a RAID Controller Card, 9540 Kunpeng-based with a RAID Controller Card, 9920 Kunpeng-based with a RAID Controller Card, and 9340 Kunpeng-based with a RAID Controller Card)**.
  d. Install the ES3000, NIC, and RAID controller card tools, drivers, and firmware by referring to *OceanStor Pacific Series Firmware Installation and Upgrade Guide*.

 Copyright © Huawei Technologies Co., Ltd.

e. Check the Hi1822V120 NIC mode by referring to **Checking the Hi1822V120 NIC Mode**.

f. Check the compatibility of the disk backplane by referring to **Checking the Compatibility of a Disk Backplane**.

g. Check the **cloud_vpc.ini** file by referring to **5.5.3 Checking the cloud_vpc.ini File**.

h. Configure networks by referring to **5.4.2.7.4 Configuring the Management Network of a Node**.

----End

?.3. Checking the Cache Policy of a System Disk

Context

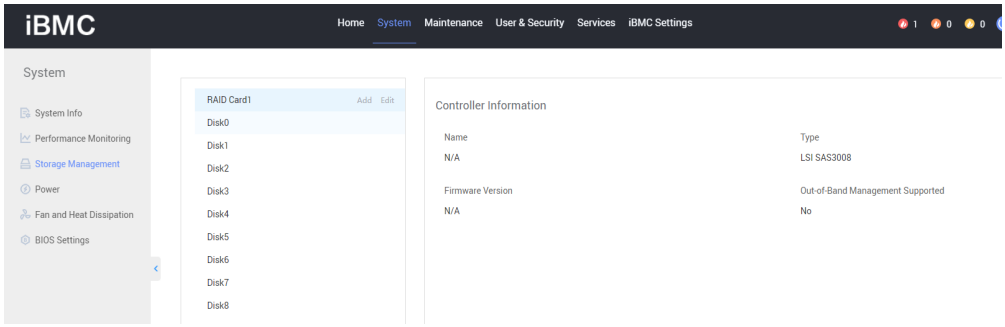
If the RAID controller card configured on the node is not LSI SAS3008IR, you need to manually disable the system disk cache policy to prevent file system damage caused by node restart or unexpected power-off.

Procedure

Step 1 Log in to the iBMC system.

Step 2 Check the model of the RAID controller card which has been installed.

Choose **System** > **Storage Management**, select the desired RAID controller card or PCIe card, and view the **Type** information in the right pane.



- If the type is LSI SAS3008IR, no further action is required.

  NOTE

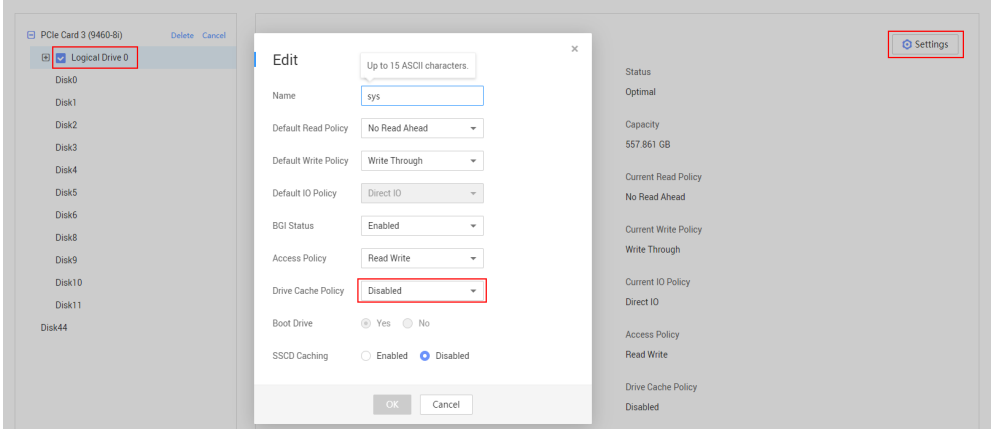
  For the LSI SAS3008IR RAID controller card, the system disk cache policy is disabled by default. Therefore, you do not need to perform the following operations.

- If the type is not LSI SAS3008IR, go to **Step 3**.

Step 3 Disable the cache policy of a system disk.

- When the RAID controller card type is not SP686C-M-16i or SP686C-M-40i, select the system disk to be modified, click **Settings**, and set **Drive Cache Policy** to **Disabled**.

 Copyright © Huawei Technologies Co., Ltd.



- When the RAID controller card type is SP686C-M-16i or SP686C-M-40i:

  a. Log in to the storage node as user **fsadmin**. Run the following command and enter the password of user **root** to switch to user **root**.
  su - root

  b. Run the following command to query *controller_id*.
  /usr/bin/hiraidadm show allctrl

  c. Run the following command to query *enc_id* and *slot_id*.
  /usr/bin/hiraidadm c*controller_id* **show pdlist**

  Check the values of **Enc** and **Slot** whose **Type** is **member**. **Enc** and **Slot** are *enc_id* and *slot_id*, respectively.

```
Index Enc  Slot DID  Intf  Media Type     Status        PreFail LinkSpd Capacity   SecType FUA SED Spin FW       Model
------------------------------------------------------------------------------------------------------------------------------
0     0    1    24   SATA  HDD   rawdrive online        No      6.0G    10.914TB  512E    Sup No  UP   LEBDT3P2 HGST HUH721212ALE600
1     0    2    25   SATA  HDD   rawdrive online        No      6.0G    10.914TB  512E    Sup No  UP   LEBDT3P2 HGST HUH721212ALE600
2     0    3    15   SATA  HDD   rawdrive online        No      6.0G    3.639TB   512N    Sup No  UP   T7R4     HUS726040ALA610
3     0    4    22   SATA  HDD   rawdrive online        No      6.0G    10.914TB  512E    Sup No  UP   LEBDT3P2 HGST HUH721212ALE600
4     0    5    14   SATA  HDD   rawdrive online        No      6.0G    3.639TB   512N    Sup No  UP   T7R4     HUS726040ALA610
5     0    6    1    SATA  HDD   rawdrive online        No      6.0G    3.639TB   512N    Sup No  UP   SN06     ST4000NM0033-9ZM170
6     0    7    2    SATA  HDD   rawdrive online        No      6.0G    3.639TB   512N    Sup No  UP   SN06     ST4000NM0033-9ZM170
7     0    8    3    SAS   SSD   rawdrive online        No      12G     2.911TB   512E    Sup No  UP   3253     HWE52SS33T2M002N
8     0    9    4    SAS   SSD   rawdrive online        No      12G     2.911TB   512E    Sup No  UP   3253     HWE52SS33T2M002N
9     0    10   5    SAS   SSD   rawdrive online        No      12G     2.911TB   512E    Sup No  UP   3253     HWE52SS33T2M002N
10    0    11   6    SAS   SSD   rawdrive online        No      12G     2.911TB   512E    Sup No  UP   3253     HWE52SS33T2M002N
11    0    12   0    SAS   HDD   member    online       No      12G     1.092TB   512N    Sup No  UP   N005     ST1200MM0009
12    0    13   19   SAS   HDD   member    online       No      12G     1.092TB   512N    Sup No  UP   N003     ST1200MM0009
------------------------------------------------------------------------------------------------------------------------------
[root@host184-210 ~]#
```

  d. Disable the pdcache function of the RAID controller card.

    i. Run the following command to query *vd_id*.
    /usr/bin/hiraidadm c*controller_id* **show vdlist**

```
[root@host184-210 network-scripts]# hiraidadm c0 show vdlist
================================== Hiraidadm   Information ==================================
    Name: hiraidadm
    Version :1.2.0.2
    Build Time:Aug 12 2022 05:51:03
==============================================================================================
==============================================================================================
    Status Code = 0
    Status = Success
    Description = None
==============================================================================================
Total vd number is 1
----------------------------------------------------------------------------------------------
VDID RGID Name     Type     Status         Capacity   SUSz   SecSz  RCache    WCache RealWCache
----------------------------------------------------------------------------------------------
0    0    system   normal   normal           1.091TB  256KB    512B No_Ahead WT     WT
----------------------------------------------------------------------------------------------
```

    In the command output, **VDID** is *vd_id*.

    ii. Run the following command to disable the pdcache function of the RAID controller card based on the obtained *vd_id*.
    /usr/bin/hiraidadm c*controller_id***:vd***vd_id* **set pdcache sw=off**

 Copyright © Huawei Technologies Co., Ltd.

```
[root@host184-210 ~]# hiraidadm c0:vd0 set pdcache sw=off
================================== Hiraidadm   Information ==================================
    Name: hiraidadm
    Version :1.2.0.2
    Build Time:Aug 12 2022 05:51:03
=============================================================================================
=============================================================================================
    Status Code = 0
    Status = Success
    Description = None
=============================================================================================
[root@host184-210 ~]#
```

iii. Run the following command to check whether the pdcache function of the RAID controller card is disabled.

/usr/bin/hiraidadm c*controller_id***:e***enc_id***:s***slot_id* **show pdcache**

```
[root@host184-210 ~]# hiraidadm c0:e0:s12 show pdcache
================================== Hiraidadm   Information ==================================
    Name: hiraidadm
    Version :1.2.0.2
    Build Time:Aug 12 2022 05:51:03
=============================================================================================
=============================================================================================
    Status Code = 0
    Status = Success
    Description = None
=============================================================================================
Drive Cache switch = Off
[root@host184-210 ~]#
```

----End

?.4. Checking the JBOD Function

To ensure that the disks on a node can be used properly, you need to configure the RAID controller cards to the RAID mode and enable the JBOD function when the node uses some RAID controller cards. For the RAID controller card models for which JBOD needs to be enabled, see **Huawei Storage Interoperability Navigator**.

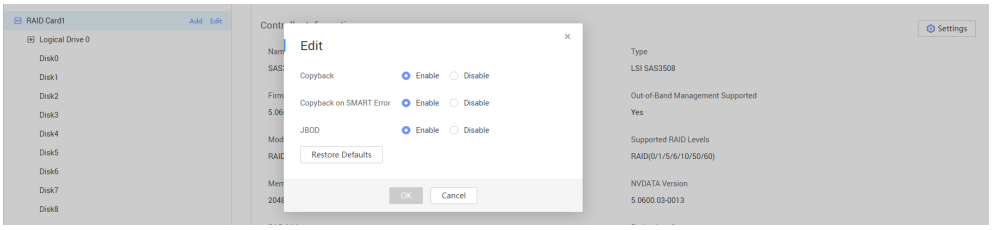
Procedure

Step 1 Log in to the iBMC system.

Step 2 Choose **System** > **Storage Management** and select the desired RAID controller card or PCIe card.

Step 3 Enable JBOD for the RAID controller card.

1. Click **Settings**.
2. Set **JBOD** to **Enable**.



----End

?.5. Checking BIOS Settings

Procedure

Step 1 Log in to the iBMC system.

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Choose **iBMC Settings** > **Configuration Update** > **Export Configuration** or **Configuration** > **Import/Export**.

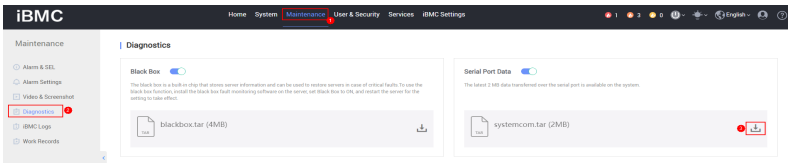
Step 3 Click **Export**.

Step 4 Query the following information in the exported configuration file:

- Check whether the value of **EnableSMMU** (corresponding to **Support Smmu** in the BIOS) is **Disabled**.
- Check whether the value of **DieInterleaving** is **Enabled**.
- Check whether the value of **NUMAEn** (corresponding to **NUMA** in the BIOS) is **Enabled**.
- Check whether the value of **ColdBootFastSupport** is **Disabled**.
- Check whether the value of **ExmbistSupport** (corresponding to **Exmbist Support** in the BIOS) is **Enable**.
- Check whether the value of **BbuNvSize** is **16G**.
- Check whether the value of **X8MisCorrEn** (corresponding to **AB Check** in the BIOS) is **Enabled**.
- Check whether the value of **AdvanceDeviceCorrection** (corresponding to **Advanced Device Correction** in the BIOS) is **SR**.

NOTICE

- Ensure that the value of **NUMAEn** in the configuration file is the same as the preceding value.
- **X8MisCorrEn** (corresponding to **AB Check** in the BIOS) applies to the following BIOS versions of Kunpeng 920-based nodes:
  - BIOS 1.91 or later for the 1620 VD 1.5 mainboard
  - BIOS 5.21 or later for the 1620S VE 2.0/V150 mainboard
- The default value of **SecureBoot** in the BIOS is **Disable**. To avoid installation problems, you are advised to check whether the value is **Disable**. The check methods are as follows:
  - Log in to the iBMC WebUI, choose **Maintenance** > **Diagnostics**, download the **systemcom.tar** file, view the file content, search for **SecureBoot CurrentValue**, and check whether the value of **SecureBoot CurrentValue** is **0**.



  - Check the BIOS. For details, see the step describing how to modify secure boot in **5.5.5.2.2 Configuring BIOS (Applicable to Other Kunpeng-based Devices)**.

If the queried values are different from the preceding values, set the parameters by referring to **5.5.5.2.2 Configuring BIOS (Applicable to Other Kunpeng-based Devices)**.

----End

 Copyright © Huawei Technologies Co., Ltd.

?.6. Checking the Device Firmware and Driver Versions

Procedure

Step 1 Log in to the iBMC system.

Step 2 Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 3 Enter user name **root** and its new password to log in to a node.

Step 4 Configure a temporary management IP address for a storage node.

To configure an IPv4 address, run the following commands:

- **ifconfig** *Management plane NIC name Temporary IPv4 address/Number of subnet mask bits* **up**
- **route add default gw** *Default gateway*

```
ifconfig enp125s0f0 192.168.40.15/24 up
route add default gw 192.168.40.1
```

To configure an IPv6 address, run the following commands:

- **ifconfig** *Management plane NIC name* **add** *Temporary IPv6 address/Prefix* **up**
- **route -A inet6 add default gw** *Default gateway*

```
ifconfig enp2s0f0:3 add FC00::102/64 up
route -A inet6 add default gw FC00::101
```

Step 5 Use PuTTY to log in to a storage node as user **fsadmin**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*.

Run the following command to switch to user **root**.

```
su - root
```

NOTE

If you log in as user **fsadmin** for the first time, change the default password.

Step 6 Check whether the firmware and driver versions meet the requirements in *OceanStor Pacific Series 8.2.1RC1 Version Mapping* by referring to *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*. If no, upgrade the firmware and driver versions to the target versions.

----End

?.7. Checking the Hi1822V120 NIC Mode

Context

This section describes how to check whether the Hi1822V120 NIC mode is Open vSwitch (OVS), and how to switch the NIC mode if it is not OVS.

Prerequisites

This operation applies only to OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9920 Kunpeng-based, OceanStor Pacific 9340 Kunpeng-based, and OceanStor Pacific 9520 Kunpeng-based.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Use a remote connection tool to log in to the system and switch to user **root**.

Step 2 Disable the intrusion detection service to prevent a false positive. If the OS does not support this service, skip this step.

```
Euler:~ # systemctl stop secAgent
```

Step 3 Run the following command to check the Hi1822V120 NIC mode.

```
Euler:~ # hinicadm3 info
Card num:2
Device Information:
    Card        PCIe Function
|----hinic0(CAL_4X25G)
        |--------0000:87:00.0(NIC:enp135s0f0)
        |--------0000:87:00.1(NIC:enp135s0f1)
        |--------0000:87:00.2(NIC:enp135s0f2)
        |--------0000:87:00.3(NIC:enp135s0f3)
        |--------0000:87:00.4(NIC:enp135s0f4)
        |--------0000:87:00.5(NIC:enp135s0f5)
|----hinic1(CAL_4X25G)
        |--------0000:01:00.0(NIC:enp1s0f0)
        |--------0000:01:00.1(NIC:enp1s0f1)
        |--------0000:01:00.2(NIC:enp1s0f2)
        |--------0000:01:00.3(NIC:enp1s0f3)
```

If one NIC in the command output contains six NIC records (the NIC information is displayed below **|----hinic*x*(CAL_4X25G)**), the server has NICs in OVS mode. In this case, you do not need to switch the NIC mode. Otherwise, go to **Step 4** to switch the NIC mode.

Step 4 Switch the NIC mode to OVS. For details, see **Installing/Upgrading the Firmware and Drivers (Function Manual)** > **Installing/Upgrading Firmware and Drivers for OceanStor Pacific 9520, 9540, 9340, and 9920** > **Installing/Upgrading the Hi1822V120 NIC Firmware and Driver** > **Switching the NIC Mode (Applicable to SFS Scenarios)** in *OceanStor Pacific Series 8.2.1 Firmware Installation and Upgrade Guide*. In NIC mode switching command **./appctl switch_mode -slot** *slotid* **-type** *mode*, the value of *mode* is **ovs**. For details about the value of *slotid*, see **Table 5-42**.

Table 5-42 slotid in the device service network

Device Name	slotid in the Service Network
OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9920 Kunpeng-based, or OceanStor Pacific 9340 Kunpeng-based	3
OceanStor Pacific 9520 Kunpeng-based	5

----End

 Copyright © Huawei Technologies Co., Ltd.

?.8. Checking the Compatibility of a Disk Backplane

Procedure

Step 1 Query the model and version of a disk module.

1. Log in to the target node as user **fsadmin**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. Run the **su - root** command and enter the password of user **root** to switch to user **root**.
2. Run the **lsscsi -g** command to query the model and version of a disk module.

```
                        lsscsi -g
[0:0:42:0]   disk    ATA      WUS721010ALE6L4  W9C0  /dev/sda   /dev/sg0
[0:0:43:0]   disk    ATA      WUS721010ALE6L4  W950  /dev/sdb   /dev/sg1
[0:0:66:0]   enclosu HUAWEI   Expander 12Gx16  131   -          /dev/sg8
[0:2:0:0]    disk    AVAGO    HW-SAS3508       5.14  /dev/sdi   /dev/sg9
```

In the row containing **disk** of the command output, if the model is **HUS726T6TALE600** and the version is **T9***xx* (excluding T9C0) or if the model is **WUS721010ALE6L4** and the version is **W9***xx* (excluding W9C0), go to **Step 2**. Otherwise, there is no compatibility problem.

Step 2 Query the model of the disk backplane.

1. Log in to the iBMC WebUI page of the target node.
2. Choose **System** > **System Info** > **Others** > **Drive Backplanes**, and query **Board ID** of the disk backplane.

   NOTE

   If the iBMC versions are inconsistent, log in to the iBMC WebUI, choose **Information** > **System Info** > **Other Devices** > **Drive Backplanes**, and query **Board ID** of the disk backplane.

   - If the board ID is not **0x0073** or **0x0083**, there is no compatibility problem.
   - If the board ID is **0x0073**, go to **Step 3**.
   - If the board ID is **0x0083**, contact Huawei technical support engineers.

Step 3 Query the firmware version of the spare disk backplane.

Log in to the target node as user **fsadmin**. Run the **su - root** command and enter the password of user **root** to switch to user **root**. Run the **lsscsi -g** command to query the firmware version of the disk backplane.

```
[root@localhost ~]# lsscsi -g
[0:0:5:0]    disk    ATA      HUH721010ALE600  T3X6  /dev/sda   /dev/sg0
[0:0:6:0]    disk    ATA      HUH721010ALE600  T3X6  /dev/sdb   /dev/sg1
[0:0:8:0]    disk    ATA      HUH721010ALE600  T3X6  /dev/sdc   /dev/sg2
[0:0:17:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdd   /dev/sg3
[0:0:18:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sde   /dev/sg4
[0:0:25:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdf   /dev/sg5
[0:0:42:0]   disk    ATA      MG06ACA10TE      0808  /dev/sdg   /dev/sg6
[0:0:44:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdh   /dev/sg7
[0:0:45:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdi   /dev/sg8
[0:0:48:0]   disk    ATA      HUH721010ALN600  T2JC  /dev/sdj   /dev/sg9
[0:0:51:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdk   /dev/sg10
[0:0:55:0]   disk    ATA      HUH721010ALE600  T3X6  /dev/sdl   /dev/sg11
[0:0:65:0]   enclosu HUAWEI   Expander 12Gx16  331   -          /dev/sg12
[0:2:0:0]    disk    AVAGO    HW-SAS3408       5.03  /dev/sdm   /dev/sg13
```

 Copyright © Huawei Technologies Co., Ltd.

- If the version in the **enclosu** row in the command output is **331**, there is no compatibility problem.
- If the version in the **enclosu** row in the command output is not **331**, contact Huawei technical support engineers.

----End

5.4.2.7.4 Configuring the Management Network of a Node

5.4.2.7.4.1 Configuration Requirements

- Before installing OceanStor Pacific series software, you need to modify the network port configuration file to configure management IP addresses for all management and storage nodes.
- The management network of the management nodes consists of external and internal management networks. The storage nodes that are deployed separately from the management nodes use only one management network (sharing the internal management network of the management nodes). You can configure external management IP addresses by referring to the steps in this section. Because the internal management network and storage network share network ports and IP addresses, you can configure internal management IP addresses by referring to the storage network configuration procedure.
- This section provides four configuration methods. Select one of the methods based on the actual service scenario.

5.4.2.7.4.2 Configuring a Physical Port IP Address

Context

The description in the following operations is only an example. The actual network port name information prevails.

Procedure

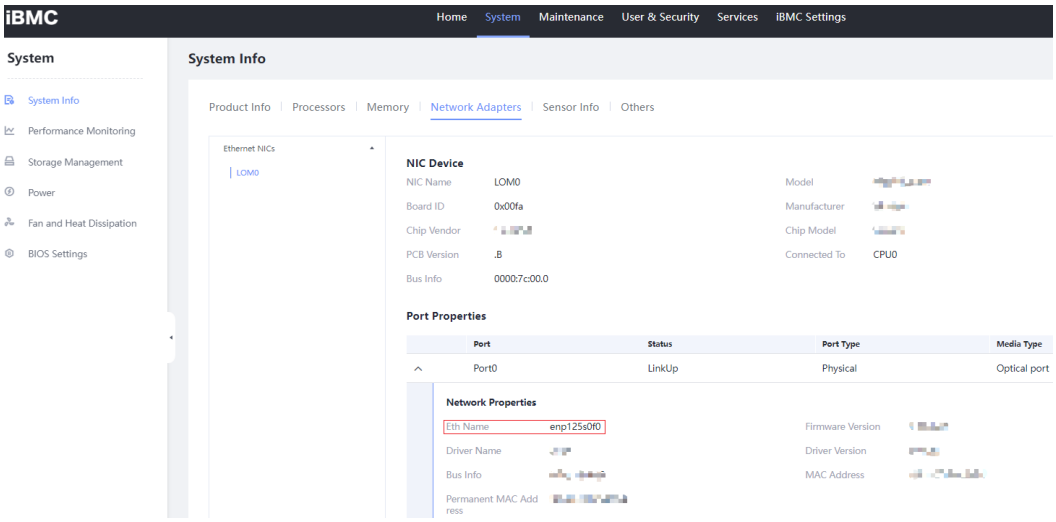
Step 1 Check the name of the network port corresponding to a NIC.

Log in to the iBMC system of a node, choose **System** > **System Info** > **Network Adapters** or **System** > **System Info** > **NICs**, select the corresponding NIC and port, and view the network port name. An example is provided as follows:

NOTE

If **Eth Name** cannot be queried on this page, you need to install the iBMA component. For details, see **5.5.20 Installing the iBMA Component**.

 Copyright © Huawei Technologies Co., Ltd.



Step 2 Use a remote connection tool to log in to the node as user **fsadmin** through the temporary management IP address. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. After the password is changed, log in to the node again.

Step 3 Run the following command to switch to user **root**.

```
su - root
```

Step 4 Go to the path for storing the network port configuration file.

```
cd /etc/sysconfig/network-scripts
```

Step 5 Run the following command to edit the network port configuration file. If the network port configuration file does not exist in the current path, you can run the following command to create and edit the network port configuration file.

```
vi ifcfg-Network port name
```

For details about the configuration file, see **Table 5-43**.

NOTE

In the following example, the management network uses physical network port enp125s0f0. You need to configure the **ifcfg-enp125s0f0** network port configuration file for each node.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-43 Network port configuration file information

Name	Content
ifcfg-*enp125s0f0*	DEVICE=*enp125s0f0* BOOTPROTO=static ONBOOT=yes STARTMODE=onboot IPv4 configuration: IPADDR=*IPv4 address* NETMASK=*subnet mask* DEFROUTE=yes NETWORKING=yes GATEWAY=*Management network gateway* **NOTE** • The external management network cannot use the same subnet as the storage network (the internal management network and storage network share the same IP address) or control network. • A gateway must be configured for the external management network. The gateway must be the same as the default node gateway. IPV6_AUTOCONF=no NM_CONTROLLED=no

Step 6 After editing the configuration file, press **Esc** and enter **:wq** to save the settings and exit.

Step 7 Modify the permission on the network port configuration file.

```
chmod 644 /etc/sysconfig/network-scripts/ifcfg-Network port name
chown -h root:root /etc/sysconfig/network-scripts/ifcfg-Network port name
```

NOTE

All network port configuration files need to be modified.

Step 8 Run the following command to restart the network service:

```
service network restart
```

NOTE

After restarting the network service, you are advised to wait for 2 to 3 minutes to ensure that the network communication is recovered.

Step 9 Repeat **Step 1** to **Step 8** to configure the management IP addresses and gateways for all nodes.

Step 10 After the configuration is complete, ping the management IP addresses of other nodes on one node to check whether the management network communication between nodes is normal.

----End

5.4.2.7.4.3 Configuring a Bond Port IP Address

Context

The description in the following operations is only an example. The actual port information prevails.

 Copyright © Huawei Technologies Co., Ltd.

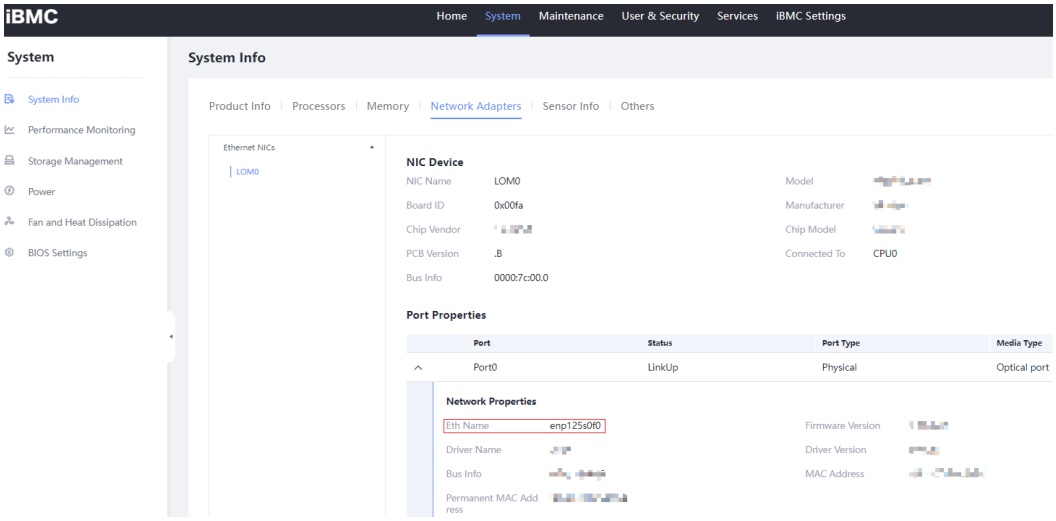
Procedure

Step 1 Check the name of the network port corresponding to a NIC.

Log in to the iBMC system of a node, choose **System** > **System Info** > **Network Adapters** or **System** > **System Info** > **NICs**, select the corresponding NIC and port, and view the network port name. An example is provided as follows:

NOTE

If **Eth Name** cannot be queried on this page, you need to install the iBMA component. For details, see **5.5.20 Installing the iBMA Component**.



Step 2 Use a remote connection tool to log in to the node as user **fsadmin** through the temporary management IP address. You need to change the default password upon the first login. After the password is changed, log in to the node again.

Step 3 Run the following command to switch to user **root**.

```
su - root
```

Step 4 Go to the path for storing the network port configuration file.

```
cd /etc/sysconfig/network-scripts
```

Step 5 Run the following command to edit the network port configuration file. If the network port configuration file does not exist in the current path, you can run the following command to create and edit the network port configuration file.

```
vi ifcfg-Network port name
```

For details about the configuration file, see **Table 5-44**.

NOTE

In the following example, the management network uses physical network ports enp125s0f0 and enp125s0f1. You need to configure the following network port configuration files for each node:

- **ifcfg-enp125s0f0**: configuration file of physical network port enp125s0f0
- **ifcfg-enp125s0f1**: configuration file of physical network port enp125s0f1
- **ifcfg-fsb_bond**: configuration file of the bond port corresponding to the two physical network ports

 Copyright © Huawei Technologies Co., Ltd.

Table 5-44 Network port configuration file information

Name	Content
ifcfg-*enp125s0f0*	DEVICE=*enp125s0f0* BOOTPROTO=none ONBOOT=yes MASTER=*fsb_bond* SLAVE=yes USERCTL=no NM_CONTROLLED=no
ifcfg-*enp125s0f1*	DEVICE=*enp125s0f1* BOOTPROTO=none ONBOOT=yes MASTER=*fsb_bond* SLAVE=yes USERCTL=no NM_CONTROLLED=no
ifcfg-*fsb_bond*	DEVICE=*fsb_bond* IPv4 configuration: IPADDR=*IPv4 address* NETMASK=*subnet mask* DEFROUTE=yes NETWORKING=yes GATEWAY=*Management network gateway* **NOTE** • The external management network cannot use the same subnet as the storage network (the internal management network and storage network share the same IP address) or control network. • A gateway must be configured for the external management network. The gateway must be the same as the default node gateway. IPV6_AUTOCONF=no ONBOOT=yes BOOTPROTO=static USERCTL=no TYPE=Bonding MTU=1500 NM_CONTROLLED=no BONDING_OPTS='mode=1 miimon=100' **NOTE** Configuration description of **BONDING_OPTS**: • The bond1 mode is recommended and the configuration is as follows: BONDING_OPTS='mode=1 miimon=100' • If the bond2 mode is used, the configuration is as follows: BONDING_OPTS='mode=2 miimon=100 xmit_hash_policy=layer3+4' • If the bond4 mode is used, the configuration is as follows: BONDING_OPTS='mode=4 miimon=100 lacp_rate=fast xmit_hash_policy=layer3+4'

Step 6 After editing the configuration file, press **Esc** and enter **:wq** to save the settings and exit.

Step 7 Modify the permission on the network port configuration file.

```
chmod 644 /etc/sysconfig/network-scripts/ifcfg-Network port name
chown -h root:root /etc/sysconfig/network-scripts/ifcfg-Network port name
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

All network port configuration files need to be modified.

Step 8 Run the following command to restart the network service:

```
service network restart
```

Step 9 Repeat **Step 1** to **Step 8** to configure the management IP addresses and gateways for all nodes.

Step 10 After the configuration is complete, ping the management IP addresses of other nodes on one node to check whether the management network communication between nodes is normal.

----End

5.4.2.7.4.4 Configuring a Physical Port IP Address and a VLAN

Context

The description in the following operations is only an example. The actual port information prevails.

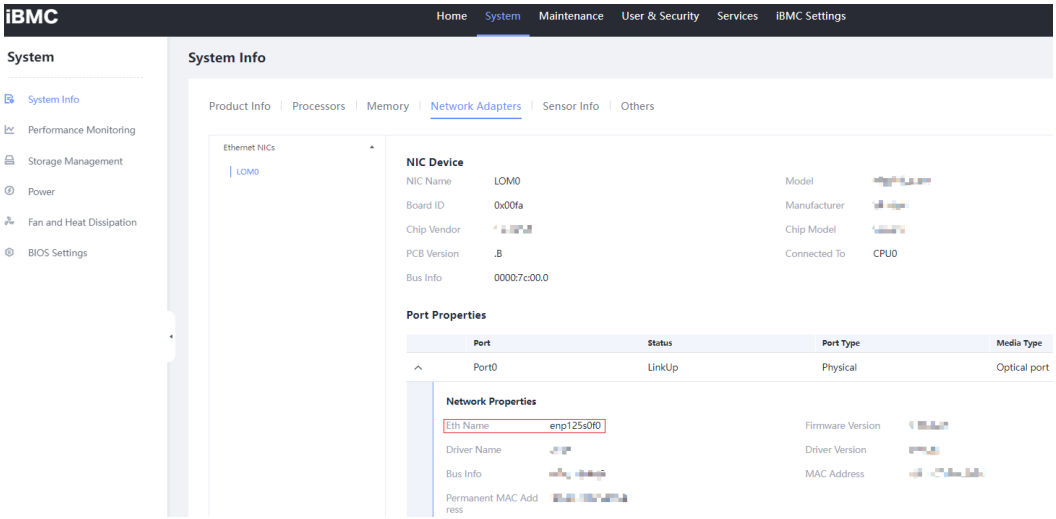
Procedure

Step 1 Check the name of the network port corresponding to a NIC.

Log in to the iBMC system of a node, choose **System** > **System Info** > **Network Adapters** or **System** > **System Info** > **NICs**, select the corresponding NIC and port, and view the network port name. An example is provided as follows:

NOTE

If **Eth Name** cannot be queried on this page, you need to install the iBMA component. For details, see **5.5.20 Installing the iBMA Component**.



Step 2 Use a remote connection tool to log in to the node as user **fsadmin** through the temporary management IP address. You need to change the default password upon the first login. After the password is changed, log in to the node again.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Run the following command to switch to user **root**.

```
su - root
```

Step 4 Go to the path for storing the network port configuration file.

```
cd /etc/sysconfig/network-scripts
```

Step 5 Run the following command to edit the network port configuration file. If the network port configuration file does not exist in the current path, you can run the following command to create and edit the network port configuration file.

```
vi ifcfg-Network port name
```

For details about the configuration file, see **Table 5-45**.

NOTE

In the following example, the management network uses physical network port enp125s0f0. You need to configure the following network port configuration files for each node:

- **ifcfg-enp125s0f0**: configuration file of physical network port enp125s0f0
- **ifcfg-v.*XXX***: configuration file of the VLAN port corresponding to the physical network port

Table 5-45 Network port configuration file information

Name	Content
ifcfg-*enp125s0f0*	DEVICE=*enp125s0f0* BOOTPROTO=none ONBOOT=yes STARTMODE=onboot DEFROUTE=yes NM_CONTROLLED=no

 Copyright © Huawei Technologies Co., Ltd.

Name	Content
ifcfg-*v.XXX*	DEVICE=*v.XXX* **NOTE** • The value of **DEVICE** must contain a period (.) or start with **vlan**. • The value of **DEVICE** cannot contain the at sign (@). • The value of **DEVICE** can contain a maximum of 13 characters. IPv4 configuration: IPADDR=*IPv4 address* NETMASK=*subnet mask* DEFROUTE=yes NETWORKING=yes GATEWAY=*Management network gateway* **NOTE** • The external management network cannot use the same subnet as the storage network (the internal management network and storage network share the same IP address) or control network. • A gateway must be configured for the external management network. The gateway must be the same as the default node gateway. IPV6_AUTOCONF=no BOOTPROTO=static PHYSDEV=eth0 ONBOOT=yes USERCTL=no VLAN=yes VID=XXX /***VID** is the specified VLAN ID, which must be the same as the VLAN ID configured on the switch.*/ NM_CONTROLLED=no

Step 6 After editing the configuration file, press **Esc** and enter **:wq** to save the settings and exit.

Step 7 Modify the permission on the network port configuration file.

```
chmod 644 /etc/sysconfig/network-scripts/ifcfg-Network port name
chown -h root:root /etc/sysconfig/network-scripts/ifcfg-Network port name
```

NOTE

All network port configuration files need to be modified.

Step 8 Run the following command to restart the network service:

```
service network restart
```

Step 9 Repeat **Step 1** to **Step 8** to configure the management IP addresses and gateways for all nodes.

Step 10 After the configuration is complete, ping the management IP addresses of other nodes on one node to check whether the management network communication between nodes is normal.

----End

 Copyright © Huawei Technologies Co., Ltd.

5.4.2.7.4.5 Configuring a Bond Port IP Address and a VLAN

Context

The description in the following operations is only an example. The actual port information prevails.

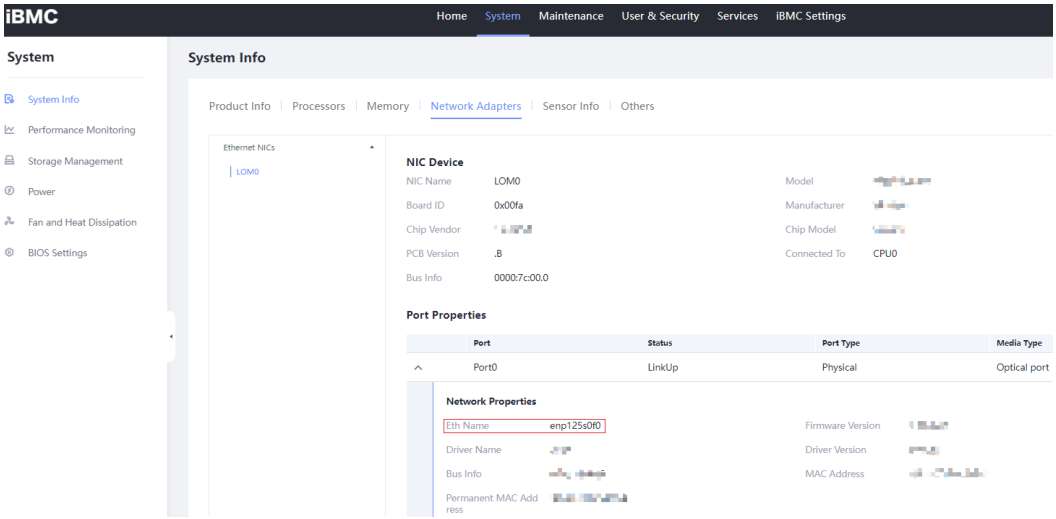
Procedure

Step 1 Check the name of the network port corresponding to a NIC.

Log in to the iBMC system of a node, choose **System** > **System Info** > **Network Adapters** or **System** > **System Info** > **NICs**, select the corresponding NIC and port, and view the network port name. An example is provided as follows:

NOTE

If **Eth Name** cannot be queried on this page, you need to install the iBMA component. For details, see **5.5.20 Installing the iBMA Component**.



Step 2 Use a remote connection tool to log in to the node as user **fsadmin** through the temporary management IP address. You need to change the default password upon the first login. After the password is changed, log in to the node again.

Step 3 Run the following command to switch to user **root**.

```
su - root
```

Step 4 Go to the path for storing the network port configuration file.

```
cd /etc/sysconfig/network-scripts
```

Step 5 Run the following command to edit the network port configuration file. If the network port configuration file does not exist in the current path, you can run the following command to create and edit the network port configuration file.

```
vi ifcfg-Network port name
```

For details about the configuration file, see **Table 5-46**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

In the following example, the management network uses physical network ports enp125s0f0 and enp125s0f1. You need to configure the following network port configuration files for each node:

- **ifcfg-enp125s0f0**: configuration file of physical network port enp125s0f0
- **ifcfg-enp125s0f1**: configuration file of physical network port enp125s0f1
- **ifcfg-fsb_bond**: configuration file of the bond port corresponding to the two physical network ports
- **ifcfg-v.*XXX***: configuration file of the VLAN port corresponding to the bond port

Table 5-46 Network port configuration file information

Name	Content
ifcfg-*enp125s0f0*	DEVICE=*enp125s0f0* BOOTPROTO=none ONBOOT=yes MASTER=*fsb_bond* SLAVE=yes USERCTL=no NM_CONTROLLED=no
ifcfg-*enp125s0f1*	DEVICE=*enp125s0f1* BOOTPROTO=none ONBOOT=yes MASTER=*fsb_bond* SLAVE=yes USERCTL=no NM_CONTROLLED=no
ifcfg-*fsb_bond*	DEVICE=*fsb_bond* ONBOOT=yes BOOTPROTO=none USERCTL=no TYPE=Bonding MTU=1500 NM_CONTROLLED=no BONDING_OPTS='mode=1 miimon=100' **NOTE** The bond1 mode is recommended for the bond port of the management network and the **BONDING_OPTS** parameter is set as follows: BONDING_OPTS='mode=1 miimon=100' **NOTE** • If the bond2 mode is configured, the **BONDING_OPTS** parameter is set as follows: BONDING_OPTS='mode=2 miimon=100 xmit_hash_policy=layer3+4' • If the bond4 mode is configured, the **BONDING_OPTS** parameter is set as follows: BONDING_OPTS='mode=4 miimon=100 lacp_rate=fast xmit_hash_policy=layer3+4'

 Copyright © Huawei Technologies Co., Ltd.

Name	Content
ifcfg-*v.XXX*	DEVICE=*v.XXX* **NOTE** • The value of **DEVICE** must contain a period (.) or start with **vlan**. • The value of **DEVICE** cannot contain the at sign (@). • The value of **DEVICE** can contain a maximum of 13 characters. IPv4 configuration: IPADDR=*IPv4 address* NETMASK=*subnet mask* DEFROUTE=yes DEFROUTE=yes NETWORKING=yes GATEWAY=*Management network gateway* **NOTE** • The external management network cannot use the same subnet as the storage network (the internal management network and storage network share the same IP address) or control network. • A gateway must be configured for the external management network. The gateway must be the same as the default node gateway. IPV6_AUTOCONF=no BOOTPROTO=static PHYSDEV=*fsb_bond* /*The value of *fsb_bond* must be the same as the name of the bond port.*/ ONBOOT=yes USERCTL=no VLAN=yes VID=XXX /***VID** is the VLAN ID specified on the management switch.*/ NM_CONTROLLED=no

Step 6 After editing the configuration file, press **Esc** and enter **:wq** to save the settings and exit.

Step 7 Modify the permission on the network port configuration file.

```
chmod 644 /etc/sysconfig/network-scripts/ifcfg-Network port name
chown -h root:root /etc/sysconfig/network-scripts/ifcfg-Network port name
```

NOTE

All network port configuration files need to be modified.

Step 8 Run the following command to restart the network service:

```
service network restart
```

Step 9 Repeat **Step 1** to **Step 8** to configure the management IP addresses and gateways for all nodes.

Step 10 After the configuration is complete, ping the management IP addresses of other nodes on one node to check whether the management network communication between nodes is normal.

----End

5.4.2.7.5 Installing OceanStor Pacific Series Software

 Copyright © Huawei Technologies Co., Ltd.

5.4.2.7.5.1 Installing Management Nodes (Applicable to OceanStor Pacific 9950, 9550, 9546, 9540, and 9920)

Prerequisites

- The OS of the installation PC meets the compatibility requirements. For details, see the **DeviceManager-Client** requirements in **Huawei Storage Interoperability Navigator**.
- The network connection between the installation PC and all nodes is normal.
- The command prompt for user **root** is **#**.
- Management networks have been configured on the management nodes. For details, see **5.4.2.7.4 Configuring the Management Network of a Node**. You can run the **ifconfig** command to obtain the information about the ports configured with management networks.
- The communication between the management nodes and storage nodes is normal. You can ping the management IP addresses of other nodes from one node to check whether the communication is normal.

Procedure

Step 1 Decompress **OceanStor-Pacific_8.2.1RC1_DeviceManagerClient.zip** on the installation PC, and double-click **run.bat** in the decompression directory. The browser automatically opens DeviceManager Client.

NOTE

- The OS time of the installation PC must be set to the current time zone and time.
- The OS time of management nodes must be the same. Otherwise, change the time to be the same by referring to **5.5.25.7 Changing the System Time of a Node**.
- During the installation, do not close the **OceanStor-Pacific_devicemanager-client** window.
- The decompression directory of the software package cannot contain spaces or brackets.
- DeviceManager Client cannot be opened using a shared path.
- If the browser does not automatically open, open the browser manually and enter **https://127.0.0.1:***port* in the address box. The value of *port* is the character string in the **OceanStor-Pacific_devicemanager-client** window. For example, in **Starting ProtocolHandler ["https-jsse-nio-127.0.0.1-8088"]**, the port number is **8088**.

Step 2 The browser may display a message indicating that the security certificate of the website is incorrect. You can ignore the security warning message as prompted if the IP address is correct.

Take Google Chrome as an example. On the security prompt page, click **Advanced** and select **Proceed to** *XXX.XXX.XXX.XXX* **(unsafe)**. The OceanStor Pacific series installation page is displayed.

Step 3 Select **Deploy by Wizard**.

Step 4 Add and configure management nodes.

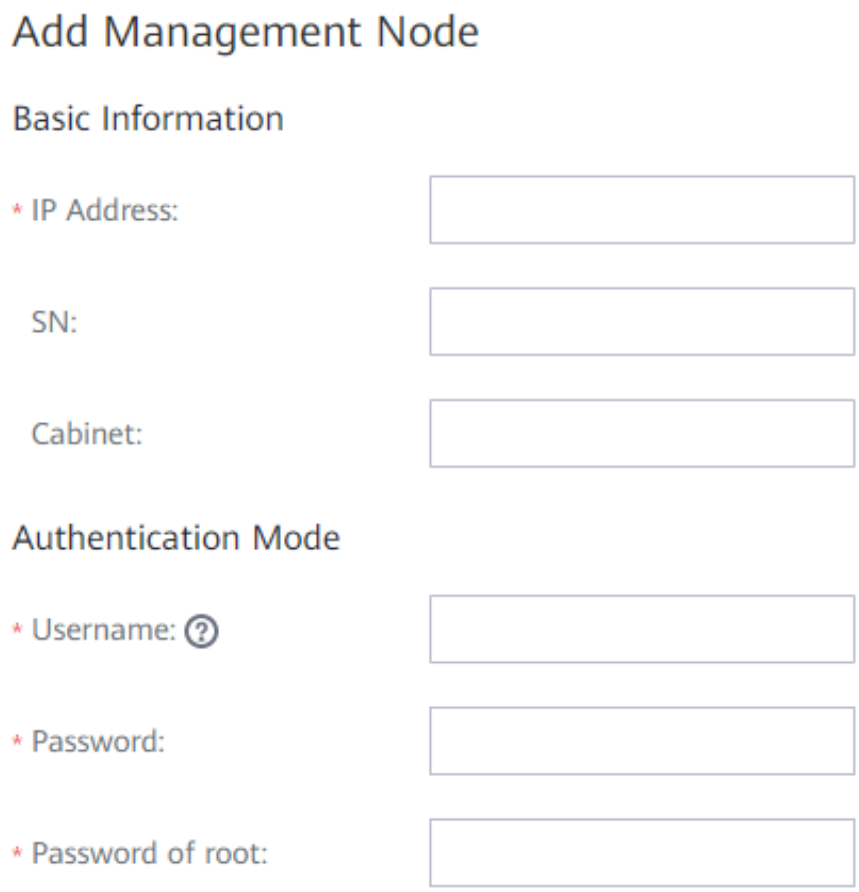
NOTE

If an exception occurs during the installation of the management nodes and the DeviceManager Client tool exits, uninstall the software by referring to **5.5.19 Uninstalling OceanStor Pacific Series Software** and reinstall the software.

Copyright © Huawei Technologies Co., Ltd.

1. Click **Add Management Node**. The **Add Management Node** dialog box is displayed, as shown in **Figure 5-21**.

Figure 5-21 Add Management Node



Enter the management node information and click **OK**. **Table 5-47** describes the management node information.

Table 5-47 Management node information

Category	Parameter	Description
Basic Information	IP Address	Indicates the management network IP address of a management node. Set this parameter to the internal management IP address.
	SN	Indicates the SN of a management node.
	Cabinet	Indicates the cabinet where a management node resides. For details, see *OceanStor Pacific Series 8.2.1 LLD Configuration Template*.

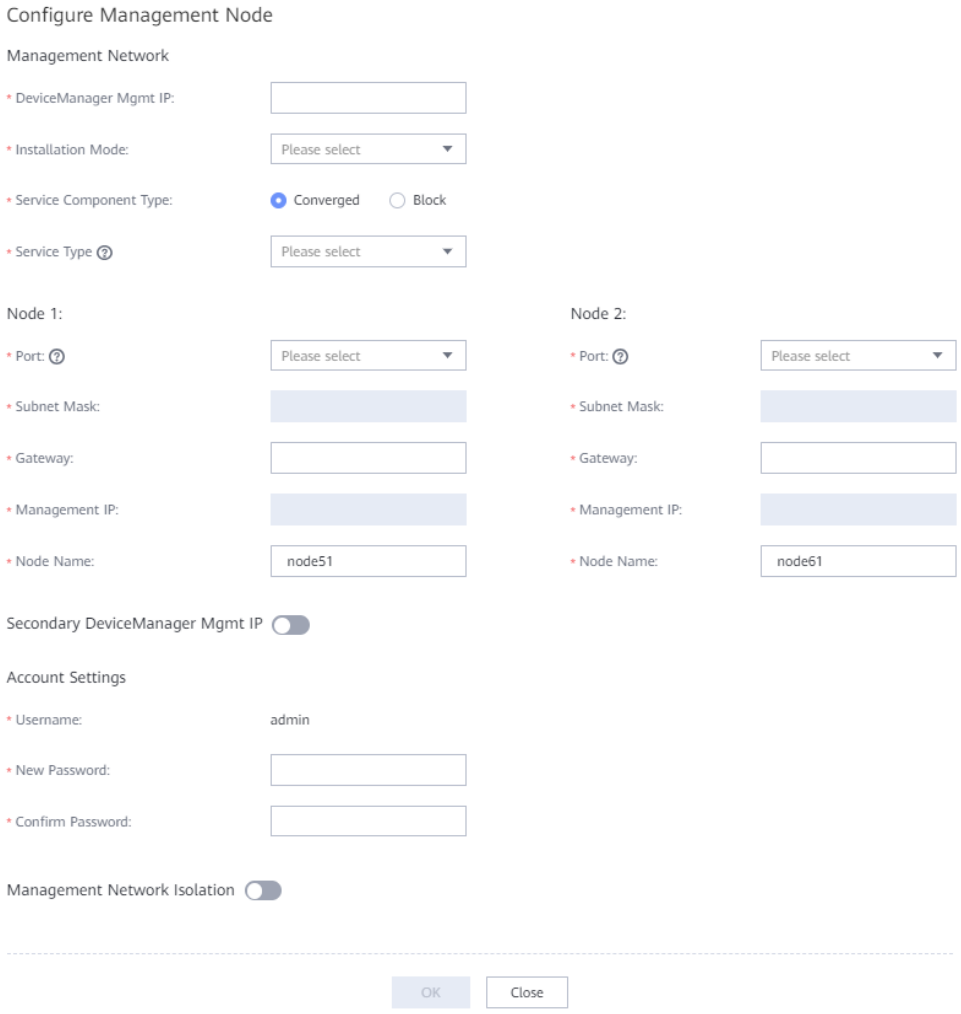
 Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
Authentication Mode	Username	If you use the pre-installed OS, enter **fsadmin** for authentication. **CAUTION** If you use user **fsadmin** for authentication: – If you have changed its default password, use the new password for authentication. – If you have not changed its default password, log in to the node, change the default password, and then use the new password for authentication.
	Password	Indicates the new password of user **fsadmin**.
	Password of root	When the user is a non-root user, enter the password of user **root**. Change the default password upon the first login.

2. Repeat **Step 4.1** to add the other management node.
3. Click **Configure Management Node**. The **Configure Management Node** dialog box is displayed, as shown in **Figure 5-22**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-22 Configure Management Node



Enter the information about the external management network. **Table 5-48** describes information about the external management network.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-48 External management network information

Category	Parameter	Description
Management Network	DeviceManager Mgmt IP	Indicates the floating management IP address of the management nodes. IPv4 and IPv6 addresses are supported. **NOTE** – After logging in to DeviceManager using this IP address, you can access the active and standby FSM nodes at the same time. – The type of the floating management IP address must be the same as that of management IP addresses configured on the nodes.
	Installation Mode	The value can be **Pre-installation** or **Regular installation**. To identify the installation mode, see **5.5.21 Identifying the Installation Mode**. – **Pre-installation**: The basic service package has been pre-installed on management nodes and storage nodes. You are advised to use this mode for configuration. – **Regular installation**: The basic service package is not installed on management nodes and storage nodes. You need to import the basic service package from DeviceManager Client and install it.
	Service Component Type	Select **Converged**.

Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
	Service Type	Select **General**. **General**: provides file, object, and HDFS storage services for upper-layer applications and applies to high-performance computing (HPC) scenarios (such as meteorology, genetics, and oil industries) and big data analysis scenarios (such as 5G log retention and analysis).
Management node information	Port	Indicates the network port used by the management network.
	Subnet Mask/Prefix	Indicates the subnet mask of the management network. This parameter cannot be modified. It is automatically generated after a port is selected.
	Gateway	Indicates the gateway of the management network. This parameter cannot be modified. It is automatically generated after a port is selected.
	Management IP	Indicates the management IP address of a management node. This parameter cannot be modified. It is automatically generated after a port is selected.

 Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
	Node Name	Indicates the name of a management node. The value contains 1 to 64 characters, including only letters, digits, hyphens (-), underscores (_), and periods (.), and must start and end with a letter or digit. A period (.) cannot be adjacent to a period (.), hyphen (-), or underscore (_). **NOTE** If the management nodes work in active/standby mode, the value of **Node Name** of the two management nodes must be different.
Secondary DeviceManager Mgmt IP	This parameter cannot be configured. It is disabled (by default).	
DeviceManager login account **NOTE** The login account is used for: – Login to DeviceManager – Login in to the CLI – DSwareTool authentication	Username	The value is fixed to **admin**.

 Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
	New Password	Indicates the new password of the user. **NOTE** – The password contains 8 to 16 characters. – The password contains at least one space or one of the following special characters: `~!@#$%^&*()-_=+|[{}];:'",<.>/? – When the password complexity is **normal**, the password must contain at least two types of the following characters. When the password complexity is **high**, the password must contain the following three types of characters. ■ Lowercase letters: a to z ■ Uppercase letters: A to Z ■ Digits: 0 to 9 – The password can contain a maximum of three consecutive identical characters. – The password cannot be the same as the user name or the user name spelled backwards. – The password cannot be the same as any of the last three passwords. – The password cannot be in the weak password dictionary. For details, see **5.5.8 Weak Password Dictionary**.
	Confirm Password	Enter the new password again.

4. Configure management network isolation.
   Enable **Management Network Isolation**, as shown in **Figure 5-23**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-23 Configuring an internal management network

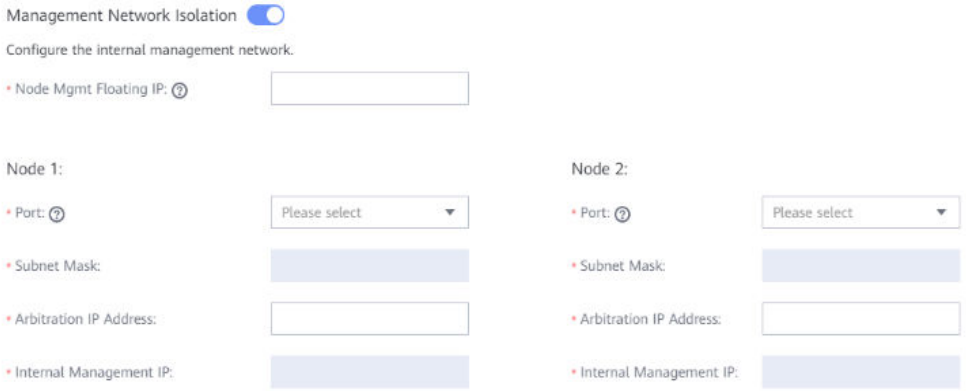


Table 5-49 describes information about the internal management network.

Table 5-49 Internal management network information

Parameter	Description
Node Mgmt Floating IP	Indicates the internal floating management IP address of the management nodes. It is used for the management data communication between management nodes and storage or compute nodes.
Port	Indicates the network port used by the internal management network.
Subnet Mask/Prefix	Indicates the subnet mask or prefix of the internal management network. This parameter cannot be modified. It is automatically generated after a port is selected. **NOTE** When the management IP address is set to an IPv4 address, the corresponding subnet mask is displayed.
Arbitration IP Address	Indicates the HA arbitration IP address. **NOTE** If the internal management network has a gateway, the arbitration IP address is automatically set to the gateway after you select a port. Otherwise, enter the management IP address (internal management IP address) of any storage node that is deployed separately from management nodes in the cluster as the arbitration IP address.
Internal Management IP	Indicates the internal management IP address of a management node. This parameter cannot be modified. It is automatically generated after a port is selected.

5. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Install management nodes.

- If **Installation Mode** is set to **Pre-installation**, the basic service package has been installed on the nodes. Click **Install** to install management nodes.
- If **Installation Mode** is set to **Regular installation** and the basic service package is not installed on the nodes, you need to upload the software package and then install management nodes.
  a. Upload software packages. After the upload is successful, the system displays the software package names.
     i. Click ... next to **Basic Service Package**, select basic service package **OceanStor-Pacific_8.2.1RC1.tar.gz**, and click **Upload**.
     ii. (Optional) If a patch needs to be installed, click ... next to **Patch Package**, select patch package **OceanStor-Pacific_8.2.1RC1.SPH*XXX***, and click **Upload**.
     iii. (Optional) If the data pilot function is required, click ... next to **Data Pilot Service Package**, select data pilot service package **OceanStor-Pacific_8.2.1RC1_Value-addedService.tar.gz**, and click **Upload**.
  b. Click **Install** to start installing the management nodes. After the installation is complete, click **Next** and ignore the security warning information as prompted.

----End

5.4.2.7.5.2 Adding Storage Nodes

Prerequisites

- The network connection between the installation PC and all nodes is normal.
- Management network IP addresses have been configured on the storage nodes. For details, see **5.4.1.6.3 Configuring the Management Network of a Node**. You can run the **ifconfig** command to obtain the information about the ports configured with management networks.
- The communication between the management nodes and storage nodes is normal. You can ping the management IP addresses of other nodes from one node to check whether the communication is normal.
- The storage network of the storage nodes is properly connected.

Procedure

You can add storage nodes in a batch or manually.

NOTE

Management nodes and storage nodes must be deployed in converged mode. In this case, the management nodes still need to be added again as storage nodes.

- Batch importing nodes
  a. Choose **Add Node > Batch Import Node**.

 Copyright © Huawei Technologies Co., Ltd.

b. Click **Download the template** to download the template locally. Fill the information in the template, click ··· and select the template, and then click **Upload**. The nodes are imported to the system in a batch.

c. Authenticate all nodes. Click **Authenticate**, enter the user name and password, and click **OK**.

d. After all nodes are authenticated successfully, click **OK**.

e. Click **Submit**.

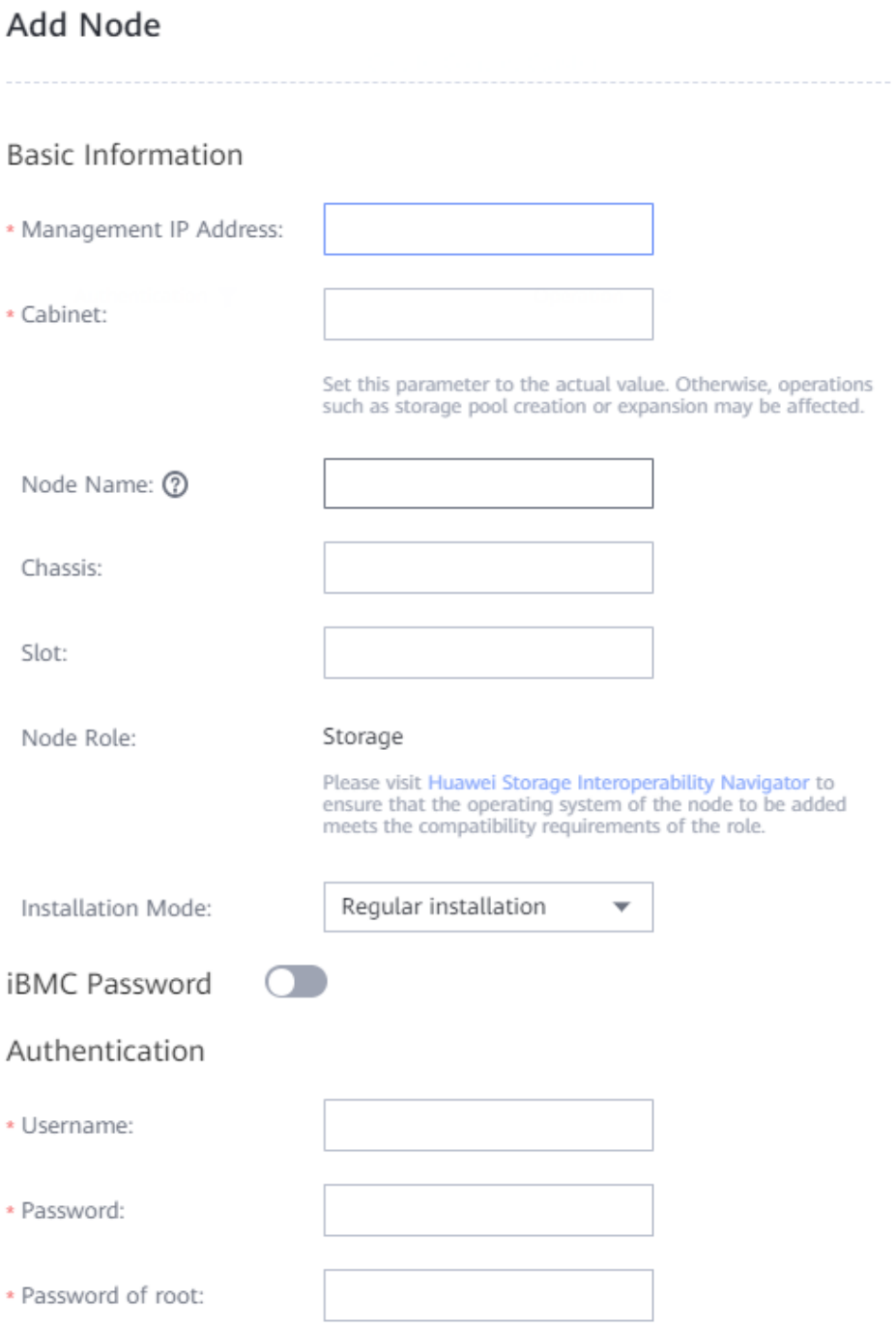
f. After the nodes are successfully configured, click **Next**.

- Manually adding nodes

  a. Choose **Add Node** > **Manually Add Node**. The **Add Node** dialog box is displayed, as shown in **Figure 5-24**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-24 Add Node



b. Enter the storage node information and click **OK**. **Table 5-50** describes the storage node information.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-50 Storage node information

Category	Parameter	Description
Basic Information	Management IP Address	Indicates the management network IP address of a storage node. Set this parameter to the internal management IP address. IPv4 and IPv6 addresses are supported.
	Cabinet	The value can contain 1 to 256 characters, including only letters, digits, underscores (_), and hyphens (-). Set this parameter based on the site requirements. Otherwise, operations such as creating or expanding a storage pool may be affected.
	Node Name	Indicates the name of a node. The value contains 1 to 64 characters, including only letters, digits, hyphens (-), underscores (_), and periods (.), and must start and end with a letter or digit. A period (.) cannot be adjacent to a period (.), hyphen (-), or underscore (_). **NOTE** If the storage node and a management node are deployed on the same server, this parameter can be left blank.
	Chassis	Indicates the chassis ID.
	Slot	Indicates the slot number.
	Node Role	Indicates the role automatically matched based on the management IP address.

Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
	Installation Mode	The value can be **Pre-installation** or **Regular installation**. • **Pre-installation**: applies to scenarios where pre-installed nodes are added to a cluster. • **Regular installation**: applies to the installation of non-preinstalled nodes.

 Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
		NOTE To check whether a storage node is a pre-installed node, perform the following steps: 1. Use SSH to log in to the storage node to be added as user **fsadmin**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. 2. Run the **su - root** command and enter the password of user **root** as prompted to switch to user **root**. 3. Run the **ls -l** *File name* command to check whether the **/home/.preinstall**, **/opt/fusionstorage/.preinstall**, and **/opt/fusionstorage/.production_preinstall** files exist. If any of the files exists, the node is a pre-installed node. In the following example, the **/home/.preinstall** file exists. [root@FSM1 ~]# **ls -l /opt/fusionstorage/.production_preinstall** ls: cannot access '/opt/fusionstorage/.production_preinstall': No such file or directory [root@FSM1 ~]# **ls -l /opt/fusionstorage/.preinstall** ls: cannot access '/opt/fusionstorage/.preinstall': No such file or directory [root@FSM1 ~]# **ls -l /home/.preinstall** -rw------- 1 root root 0 Feb 21 15:32 /home/.preinstall

 Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
iBMC Password	Username/ Password	If you have changed the default iBMC user name or password, enter the new user name and password so that the system can monitor and manage hardware in a highly reliable manner (for example, high-temperature alarm reporting and power-off due to high temperature). **NOTE** The password must be the same as the node password configured in the iBMC system.
Authentication **NOTE** If the storage node and a management node are deployed on the same server, **Authentication** will not be displayed because the management node has been authenticated when it is added.	Username	If you use the pre-installed OS, enter **fsadmin** for authentication. **CAUTION** If you use user **fsadmin** for authentication: • If you have changed its default password, use the new password for authentication. • If you have not changed its default password, log in to the node, change the default password, and then use the new password for authentication.
	Password	Indicates the new password of user **fsadmin**.
	Password of root	When the user is a non-root user, enter the password of user **root**. Change the default password upon the first login.

c. Add other storage nodes one by one. Click **Submit** to start configuring nodes and installing network management components.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- You can select a newly added node and click **Authenticate** to authenticate the node again.
- You can select a node to be removed and click **Remove Node** to remove the node and uninstall the storage software on the node. You can also click **More** > **Remove Node** to remove the node. After the node is removed, it is no longer managed by the cluster.
  - Nodes that have not been configured and installed can be directly removed. Perform the operations as prompted.
  - Nodes that have been configured and installed can be removed only after being authenticated. Perform the operations as prompted.
- You can click **Set iBMC Password** to configure the user name and password for authenticating the iBMC server.
- You can click **Uninstall Software** to clear the configurations and data related to the storage software on all nodes. Perform the operations as prompted.
- After the operation is successful, you can click **More** on the right of a node and select **Log Details** to view its operation logs.

d. After all storage nodes are added successfully, click **Next**.

NOTE

When the OceanStor Pacific series software is installed for the first time, the security sandbox is automatically enabled on the added storage nodes.

5.4.2.7.5.3 Configuring the Storage Network (When Front- and Back-End Storage Networks Are Shared and Use RoCE and Multiple IP Addresses for Networking)

Configuration Description

Table 5-51 describes the storage network configurations.

Table 5-51 Network configurations

Hardware Type	Storage Network Deployment Mode	Storage Network Protocol	Storage Network Networking Mode	Control Network IP Address
OceanStor Pacific 9950/OceanStor Pacific 9550/ OceanStor Pacific 9546/OceanStor Pacific 9920/ OceanStor Pacific 9540/	Front- and back-end shared network	RoCE	Multiple IP addresses	Required

Prerequisites

- The network connection between the installation PC and all nodes is normal.
- The storage network of the storage nodes is properly connected.

Copyright © Huawei Technologies Co., Ltd.

- Management network IP addresses have been configured on the storage nodes. If the IP addresses are not configured, configure them by referring to **5.4.2.7.4 Configuring the Management Network of a Node**. You can run the **ifconfig** command to obtain the information about the ports configured with management networks.
- The communication between the management nodes and storage nodes is normal. You can ping the management IP addresses of other nodes from one node to check whether the communication is normal.

Procedure

Step 1 Configure the storage network and the control network in advance by referring to **5.5.16.2 Configuring the Storage Network (RoCE and Multiple IP Addresses)**. If you have configured them, skip this operation.

Step 2 Select **Front- and Back-End Shared Network**.

Step 3 Select **Yes** in **Use Configured IP Address Only**.

Network IP addresses configured in advance are used. To select this option, all storage nodes must be configured with network IP addresses in advance.

Step 4 Set **Transmission Protocol** to **RoCE**, **Network Flow Classification** to **By using DSCP bits on the IP header**, and **Multiple IP Addresses** to **Yes**.

Step 5 Click **Add Control IP Address Range** to set the IP address segment and subnet mask/prefix of the control network. You can configure multiple control IP address segments. In addition, you can configure the control network across network segments. If the control IP addresses are across network segments, you need to enter the control network gateway.

Step 6 Click **Add Storage IP Address Range** to set the IP address segment and subnet mask/prefix of the storage network. You can configure multiple storage IP address segments. In addition, you can configure the storage network across network segments.

Step 7 Set related parameters. **Table 5-52** describes the parameters.

Table 5-52 Storage network information

Category	Parameter	Description
Transmission protocol	Transmission Protocol	Select **RoCE**.
	Network Flow Classification	Select **By using DSCP bits on the IP header**. **NOTE** **Network Flow Classification** of the front-end storage network on storage nodes must be the same as that on compute nodes. Otherwise, services will be interrupted.

Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
	Congestion Control Algorithm	The DCQCN and LDCP algorithms are supported. ● **DCQCN**: available for all NICs that support the RoCE protocol. This algorithm is recommended. ● **LDCP**: available for only Hi1822V120 NICs. ● All nodes in a cluster support only one algorithm. By default, DCQCN is used. Currently, dynamic switching of congestion control algorithms is not supported.
	Multiple IP Addresses	Select **Yes**.
IP address type: control IP address	IP Address Range	Indicates the IP address segment of the control network. **NOTE** The control network and external management network cannot use the same subnet. The control network and storage network (the internal management network and storage network share the same IP address) can use the same subnet (recommended) or different subnets. If they use the same subnet, they must use different IP address segments.
	Subnet Mask/ Prefix	Indicates the subnet mask or prefix of the control network. **NOTE** When the IP address of the control network is an IPv4 address, enter the subnet mask.
	Gateway	Gateway of the control network. ● A control network gateway needs to be configured in either of the following scenarios: – The control network crosses subnets. – The control network does not cross subnets currently but needs to cross subnets due to subsequent capacity expansion. In this case, you are advised to configure the gateway first.

 Copyright © Huawei Technologies Co., Ltd.

Category	Parameter	Description
IP address type: storage IP address	IP Address Range	Indicates the IP address segment of the storage network. IPv4 addresses are supported. **NOTE** The storage network and external management network cannot use the same subnet. The control network and storage network (the internal management network and storage network share the same IP address) can use the same subnet (recommended) or different subnets. If they use the same subnet, they must use different IP address segments.
	Subnet Mask/ Prefix	Indicates the subnet mask or prefix of the storage network. **NOTE** When the IP address of the storage network is an IPv4 address, enter the subnet mask.

NOTE

You can select the check box next to the storage IP address range ID or control IP address range ID and click **Remove** to remove the corresponding storage IP address range or control IP address range.

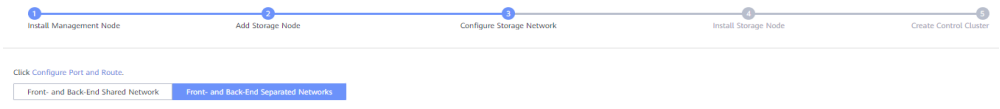
Step 8 On the storage network configuration page, click **Preview**. Because the storage or control IP addresses have been configured, the system displays the storage or control IP address of each node. Check whether the displayed IP addresses are the same as the planned IP addresses.

Step 9 Click **Submit** to start configuring the storage and control networks.

Wait until the storage network is configured successfully.

Step 10 Multiple IP addresses are used for networking. Therefore, you must configure a policy-based route to implement network interworking and data balancing.

1. Click **Configure Port and Route** to go to the route configuration page. Multiple IP addresses are configured on the VLAN port. For details, see **5.5.13.3 Configuring a Policy-based Route for a VLAN Port**.



NOTE

To query policy-based route information of a VLAN port, see **5.5.14.1 Querying the Policy-based Routes of a VLAN Port**.

To delete policy-based route information of a VLAN port, see **5.5.15.1 Deleting a Policy-based Route from a VLAN Port**.

2. After the configuration is complete, click **Back** in the upper left corner to return to the **Configure Storage Network** page.

 Copyright © Huawei Technologies Co., Ltd.

Step 11 After configuring the policy-based route, ping the storage or control IP addresses of other storage nodes from a storage node to ensure that the network communication between storage nodes is normal.

Step 12 Click **Next**.

----End

5.4.2.7.5.4 Installing Storage Nodes

Procedure

Step 1 Click **Install** to start installing the storage nodes.

NOTE

- During the installation, if **Failure** is displayed in the **Installation Status** column, you can click **Uninstall Software** and reinstall the storage nodes.
- You can click **More** in the row where a storage node resides and select **Details** to view installation log details.

Step 2 After installation is successful, click **Next**.

NOTICE

- If you need to re-configure the storage network after the nodes are installed, remove the storage nodes and go back to the previous step to re-configure the storage network.
- After the storage nodes are installed, the security sandbox is automatically enabled.

----End

5.4.2.7.5.5 Creating a Control Cluster (Applicable to OceanStor Pacific 9950 and 9550)

Procedure

Step 1 Create a control cluster.

Enter the information about the control cluster. **Table 5-53** describes the control cluster information.

Table 5-53 Control cluster information

Parameter	Description
Control Cluster Name	Indicates the name of a control cluster. The value contains 1 to 64 characters, including only letters, digits, underscores (_), and hyphens (-).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Available Nodes	Indicates the nodes that can be used to create a control cluster. The number of nodes in a control cluster must comply with the following rules: Node-level security: • If the cluster contains 3 or 4 nodes, configure 3 nodes. • If the cluster contains 5 or 6 nodes, configure 5 nodes. • If the cluster contains 7 nodes or more, configure 7 nodes. • If the cluster contains 9 nodes or more and the number of EC parity fragments is +4 (not +4:1) in an EC scheme, configure 9 nodes.

Step 2 After entering the control cluster information, click **Create**. After the creation is successful, click **Finish**.

----End

Follow-up Procedure

- On the installation PC, double-click the **shutdown.bat** script in the decompression directory of **OceanStor-Pacific_8.2.1RC1_DeviceManagerClient.zip** to close the DeviceManager Client window. If the window cannot exit normally, click in the upper right corner to close it.
- If the storage network uses the RoCE protocol, you need to configure RoCE flow control on switches. For details, see **5.5.2.2 Configuring Flow Control for a Switch**. If the configuration has been performed, skip this step.
- If the storage network uses the RoCE protocol and the NIC type is Hi1620 or CX series, you need to configure ACL rules for switches. After the configuration, the latency and packet loss rate between storage nodes and access switches can be detected. For details, see **5.5.2.3 Configuring ACL Rules for Switches**. If the configuration has been performed, skip this step.
- If parameter settings are incorrect after the software is installed, uninstall the OceanStor Pacific series software and reinstall it. For details about how to uninstall the OceanStor Pacific series software, see **5.5.19 Uninstalling OceanStor Pacific Series Software**.
- After the installation and deployment are complete, you can use the management IP addresses of DeviceManager and nodes to remotely log in to management and storage nodes.
- Update default accounts in time. For details, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*.
- Update security certificates in time. For details, see section "Security Certificate Management" in *OceanStor Pacific Series 8.2.1 Security Configuration Guide*.

Copyright © Huawei Technologies Co., Ltd.

5.4.2.7.5.6 Creating a Control Cluster (Applicable to OceanStor Pacific 9540, 9520, 9920, and 9546)

Procedure

Step 1 Create a control cluster.

Enter the information about the control cluster. **Table 5-54** describes the control cluster information.

Table 5-54 Control cluster information

Parameter	Description
Control Cluster Name	Indicates the name of a control cluster. The value contains 1 to 64 characters, including only letters, digits, underscores (_), and hyphens (-).
Metadata Storage Location	The following metadata storage locations are supported: • **Physical disk** • **System disk partition** • **Custom**: **Physical disk** and **System disk partition** can be mixed. This option is used when you need to select different metadata storage locations for different nodes. **NOTE** • For OceanStor Pacific 9520 Kunpeng-based 14-slot, OceanStor Pacific 9920 Kunpeng-based (palm-sized NVMe SSD), and OceanStor Pacific 9546 (without an SP186-M-8i RAID controller card), you can select only **System disk partition**. • For OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9520 Kunpeng-based 12-slot, OceanStor Pacific 9920 Kunpeng-based (SAS SSD) 12-slot, and OceanStor Pacific 9546 (with an SP186-M-8i RAID controller card), you can select only **Physical disk**.
Disk Type	This parameter is mandatory when **Metadata Storage Location** is set to **Physical disk**. **NOTE** • For OceanStor Pacific 9540 Kunpeng-based, OceanStor Pacific 9520 Kunpeng-based 12-slot, OceanStor Pacific 9920 Kunpeng-based (SAS SSD) 12-slot, and OceanStor Pacific 9546 (with an SP186-M-8i RAID controller card), you can select only **M.2 SSD**. • When you need to select different disk types for different nodes, set this parameter to **Custom**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Disk Selection Mode	This parameter is mandatory when **Metadata Storage Location** is set to **Physical disk**. You can select **Specify Slot** or **Manually Select**. • **Specify Slot**: Enter a slot number. A slot number ranges from 0 to 60. • **Manually Select**: Manually select one disk for each node. **NOTE** When **Disk Type** is set to **Custom**, only **Manually Select** is supported.
Available Nodes	Indicates the nodes that can be used to create a control cluster. The number of nodes in a control cluster must comply with the following rules: Node-level security: • If the cluster contains 3 or 4 nodes, configure 3 nodes. • If the cluster contains 5 or 6 nodes, configure 5 nodes. • If the cluster contains 7 nodes or more, configure 7 nodes. • If the cluster contains 9 nodes or more and the number of EC parity fragments is +4 (not +4:1) in an EC scheme, configure 9 nodes. **NOTE** If **Metadata Storage Location** is set to **Custom**, you need to select a metadata storage location (**Physical disk** or **System disk partition**) and metadata disks for each node in the control cluster.

Step 2 After entering the control cluster information, click **Create**. After the creation is successful, click **Finish**.

----End

Follow-up Procedure

- On the installation PC, double-click the **shutdown.bat** script in the decompression directory of **OceanStor-Pacific_8.2.1RC1_DeviceManagerClient.zip** to close the DeviceManager Client window. If the window cannot exit normally, click in the upper right corner to close it.
- If the storage network uses the RoCE protocol, you need to configure RoCE flow control on switches. For details, see **5.5.2.2 Configuring Flow Control for a Switch**. If the configuration has been performed, skip this step.
- If the storage network uses the RoCE protocol and the NIC type is Hi1620 or CX series, you need to configure ACL rules for switches. After the configuration, the latency and packet loss rate between storage nodes and

 Copyright © Huawei Technologies Co., Ltd.

access switches can be detected. For details, see **5.5.2.3 Configuring ACL Rules for Switches**. If the configuration has been performed, skip this step.

- If parameter settings are incorrect after the software is installed, uninstall the OceanStor Pacific series software and reinstall it. For details about how to uninstall the OceanStor Pacific series software, see **5.5.19 Uninstalling OceanStor Pacific Series Software**.
- After the installation and deployment are complete, you can use the management IP addresses of DeviceManager and nodes to remotely log in to management and storage nodes.
- Update default accounts in time. For details, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*.
- Update security certificates in time. For details, see section "Security Certificate Management" in *OceanStor Pacific Series 8.2.1 Security Configuration Guide*.

5.4.2.8 Obtaining and Loading a License

Obtain and load a license by referring to *OceanStor Pacific Series 8.2.1 License Operation Guide* so that the system can obtain a new validity period and service authorization. You need to import a license before using the OceanStor Pacific series storage system.

In wizard-based configuration mode, after the license is loaded, the DeviceManager home page is displayed. In LLD-based configuration mode, after the license is loaded, you can enter the user name and password to go to the DeviceManager home page.

NOTE

After installing the software, create and configure a storage pool so that application servers can access the scale-out storage resources. For details, see **6.4 Configuring Basic Services**.

5.4.2.9 Configuring the System Time (Applicable to the Huawei Cloud Stack Online Scenario)

In the Huawei Cloud Stack Online scenario, upper-layer services have time requirements on compute nodes and storage nodes. Therefore, you need to configure automatic NTP synchronization for the storage system. Automatic NTP synchronization uses an NTP server as an external time source to automatically and periodically synchronize the time to storage nodes.

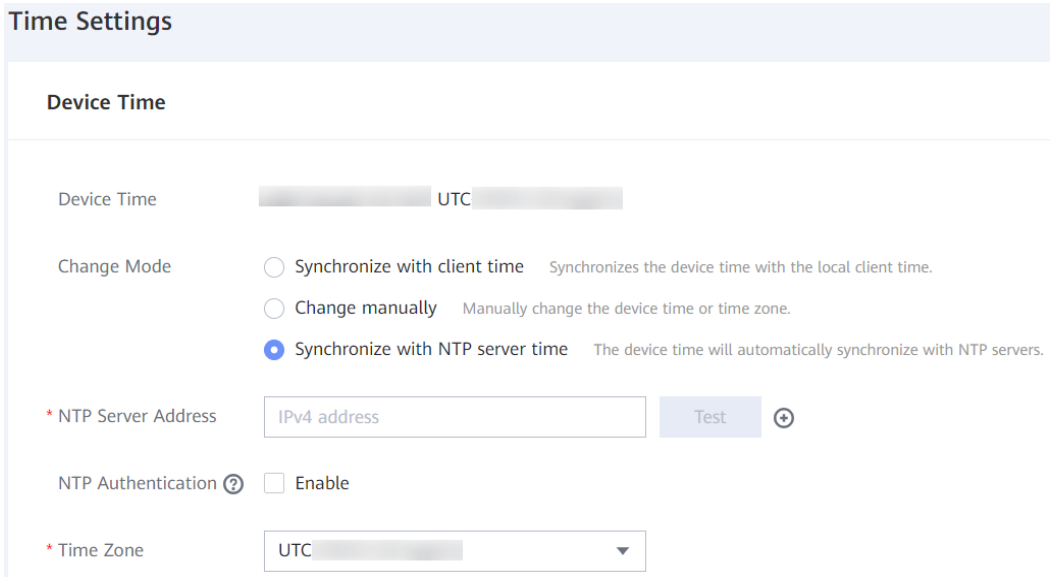
Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Time Settings**.

Step 3 Click **Modify**. The time setting page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



1. Select **Synchronize with NTP server time**.
2. In **NTP Server Address**, enter the IPv4 or IPv6 address of the NTP server.

   NOTE

   - You are advised to use an independent NTP server other than the storage system. Otherwise, time synchronization may be abnormal.
   - A maximum of three NTP servers can be added. If the time of one NTP server cannot be automatically synchronized to the device, the system attempts to synchronize the time of another NTP server to the device. If all NTP servers added on the page are faulty, the system time will be synchronized to the device.
   - When adding an NTP server, if the system has been configured with other NTP servers and times on such NTP servers are different, the time synchronization function will be in disorder. Ensure that times on all NTP servers are the same.
   - Ensure that the IP address type of an NTP server is the same as that of a management node.
3. (Optional) Click **Test**.
4. (Optional) Select **Enable** next to **NTP Authentication**.

   NOTE

   Only when NTPv4 or later is used, NTP authentication can be enabled to authenticate the NTP server and automatically synchronize the time to the storage device.
5. Select the time zone where the device is located from the **Time Zone** drop-down list box.

Step 4 Click **Save** and confirm your operation as prompted.

----End

5.4.2.10 Adding Data Cluster Modules (Applicable to OceanStor Pacific 9950)

After a data cluster module is added, it is connected to the storage system and detects hardware of the storage system. When it detects a risk, it reports an alarm. You can view alarms reported by the data cluster module on DeviceManager.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- Only OceanStor Pacific 9950 has data cluster modules.
- You have obtained the management IP address of the data cluster modules as well as the user name and password for logging in to a data cluster module.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Cluster** > **Cluster** > **Hardware**.

Step 3 In the lower part of the function pane, click the **Data Cluster Modules** tab.

Step 4 Add a data cluster module.

1. Click **Add**.

   The **Add Data Cluster Module** page is displayed.

2. Enter information about the data cluster module. **Table 5-55** describes related parameters.

   Table 5-55 Data cluster module parameters

Parameter	Description
Management IP Address	Management IP address of the data cluster module. You can log in to the data cluster module management system through this IP address.
Username	User name for logging in to the data cluster module.
Password	Password for logging in to the data cluster module.

3. Click **OK**.

   NOTE

   If the fan or power supply of the data cluster module is faulty, a corresponding alarm will be reported on the **Data Cluster Module Alarms** page. To view the alarm, choose **Monitor** > **Alarms and Events** > **Alarms** or **Monitor** > **Alarms and Events** > **Data Cluster Module Alarms**.

Step 5 Modify login information about the data cluster module. If the user name or password of the data cluster module changes, synchronize the change on DeviceManager.

1. Select the desired data cluster module and click **Modify**.

   The **Modify Data Cluster Module** page is displayed.

   NOTE

   You can also click **More** on the right of a desired data cluster module and select **Modify**.

 Copyright © Huawei Technologies Co., Ltd.

2. Change the user name, password, or chassis of the data cluster module.

   NOTE

   When changing the chassis of a data cluster module, you also need to change the chassis of the other data cluster module in the same chassis.

3. Click **OK**.

Step 6 If a data cluster module is no longer needed, select it and click **Delete** to delete it.

NOTE

You can also click **More** on the right of a desired data cluster module and select **Delete**.

----End

Follow-up Procedure

After the data cluster module is successfully connected to the storage system, you can choose **Monitor** > **Alarms and Events** > **Data Cluster Module Alarms** to view the reported alarms.

5.4.2.11 (Optional) Installing an MPI Framework

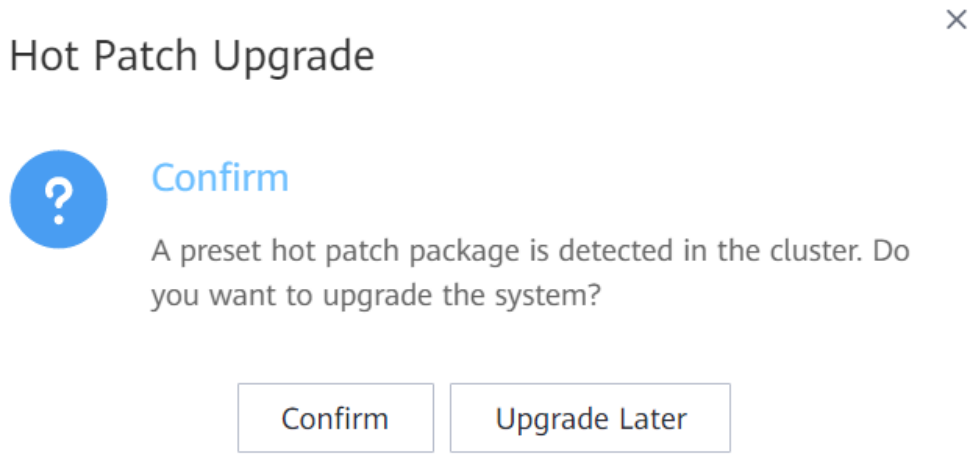
DPC is mainly used in HPC scenarios, such as meteorology, life science, gene sequencing, and scientific research. An MPI framework needs to be installed for a large amount of application software to execute parallel computing.

For details about how to install an MPI framework, see *OceanStor Pacific Series 8.2.1 DPC Usage Guide for File* and choose **Software Installation** > **(Optional) Installing an MPI Framework**.

5.4.2.12 Performing an Upgrade Using a Preset Hot Patch

When the system detects that a preset hot patch exists in the current cluster, the **Hot Patch Upgrade** dialog box is displayed, asking you whether to perform an upgrade, as shown in **Figure 5-25**.

Figure 5-25 Hot patch upgrade prompt



 Copyright © Huawei Technologies Co., Ltd.

Determine whether to perform the upgrade as required. If the upgrade is not required, log in to a management node using the floating IP address, log in to the CLI as user **admin**, and run the **delete cluster patch_pkg** command to delete all patch packages that are not installed in the cluster.

5.4.3 Installing the File/Object Service (DPC and Standard Protocol Hybrid Scenario)

The installation and deployment methods for the DPC and standard protocol hybrid scenario are basically the same as those for installing the file service in the DPC scenario. For details about the process, see **5.4.2 Installing the File Service (DPC Scenario)**.

- For details about how to configure service switches, see **5.4.1.4.3 Configuring 10GE/25GE Service Switches (Applicable to CE6865)**. For details about how to configure the storage network, see **Table 5-56**.

Table 5-56 Network configurations

Hardware Type	Storage Network Deployment Mode	Storage Network Protocol/ Networking Mode	Control Network IP Address	How to Configure the Storage Network	Service Network Protocol/ Networking Mode
OceanStor Pacific 9950/ OceanStor Pacific 9550/ OceanStor Pacific 9546/ OceanStor Pacific 9540/ OceanStor Pacific 9920	Front- and back-end shared network	RoCE/ Multiple IP addresses	Required	For details, see **Configuring the Storage Network (When Front- and Back-End Storage Networks Are Shared and Use RoCE and Multiple IP Addresses for Networking)**.	TCP/bond4 (recommended) **NOTE**

- If the service network uses the Hi1822V120 NIC, you need to check the Hi1822V120 NIC mode after the following operation: **Checking Storage Nodes Before Installation** > **Checking the Device Firmware and Driver Versions**. The procedure is as follows:

Copyright © Huawei Technologies Co., Ltd.

a. For OceanStor Pacific 9546, see **Checking the Hi1822V120 NIC Mode**.
b. For OceanStor Pacific 9540, see **Checking the Hi1822V120 NIC Mode**.

5.5 Appendix

5.5.1 Logging In to a Node

This section describes how to log in to a node.

5.5.1.1 Logging In to a Node Using PuTTY (Network Port Mode)

Prerequisites

- A management terminal properly communicates with the management network port of a storage node.
- PuTTY has been installed on the management terminal.

  NOTE

  - PuTTY is a piece of Windows-based client software used for remote configuration and management. You can visit the chiark website and download the PuTTY software from the home page.
  - You are advised to use PuTTY of the latest version to ensure successful login to the storage system.
  - This document uses PuTTY 0.70 as an example.

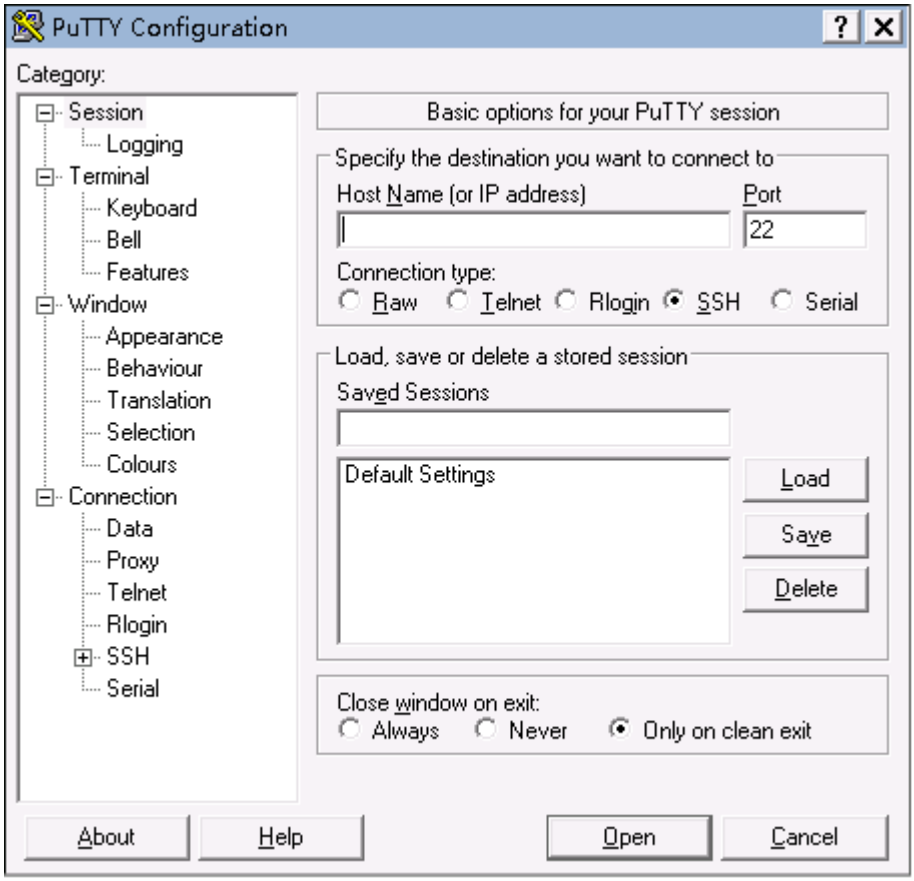
Procedure

Step 1 Run PuTTY on the management terminal.

The **PuTTY Configuration** dialog box is displayed, as shown in **Figure 5-26**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-26 PuTTY Configuration



Step 2 Enter the node management IP address in **Host Name (or IP address)**. Use the default values for other parameters.

Step 3 Click **Open**.

The PuTTY window is displayed. Then **login as:** is displayed, prompting you to enter a user name.

Step 4 Enter the user name, press **Enter**, enter the password, and press **Enter** again.

Step 5 (Optional) Run the **su - root** command to switch to user **root**.

NOTICE

To ensure account security, you are advised to change the initial password upon the first login after the software installation and periodically update the password.

----End

5.5.1.2 Using PuTTY to Log In to a Node in Key Pair Authentication Mode

Scenarios

After security hardening is performed on the SSH login mode for nodes in the system, SSH-based password authentication is disabled for login. This section

 Copyright © Huawei Technologies Co., Ltd.

describes how to use PuTTY and the required private key for authentication to log in to a target node.

Prerequisites

- Security hardening has been performed on the SSH login mode for the target node by:
  - Enabling the SSH key pair authentication mode and configuring the public key certificate on the node.
  - Disabling the SSH-based password authentication.
- You have obtained the private key certificate matching the public key certificate.

  If the private key certificate is encrypted, you also need to obtain its password.

Procedure

Step 1 Check whether PuTTY on the local PC has been used to log in to a node in key pair authentication mode.

- If yes, go to **7**.
- If no, or you are uncertain about it, go to **2**.

Step 2 Run PuTTY and enter the IP address of the target node and the SSH port (default value: **22**).

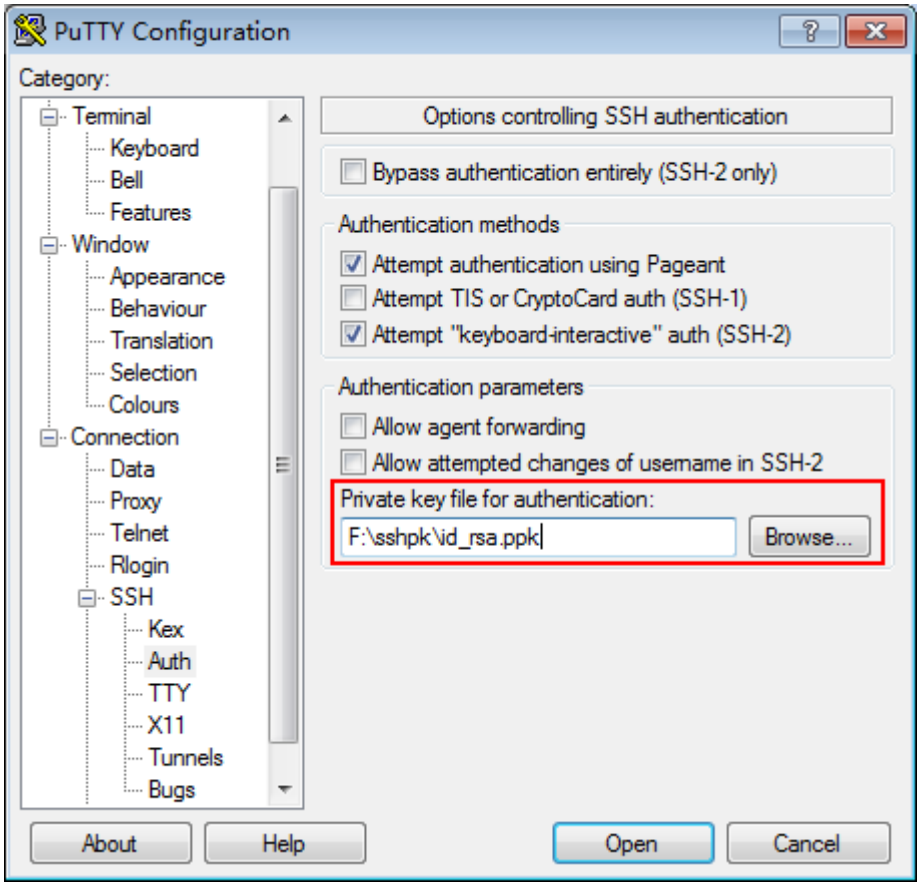
Step 3 In the **Category** area in the left pane, choose **Connection** > **SSH** > **Auth**.

The SSH authentication configuration page is displayed.

Step 4 Click **Browse**. In the dialog box that is displayed, select the obtained private key certificate and click **Open**. The private key certificate file name is ***.ppk**, as shown in **Figure 5-27**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-27 Configuring the private key certificate



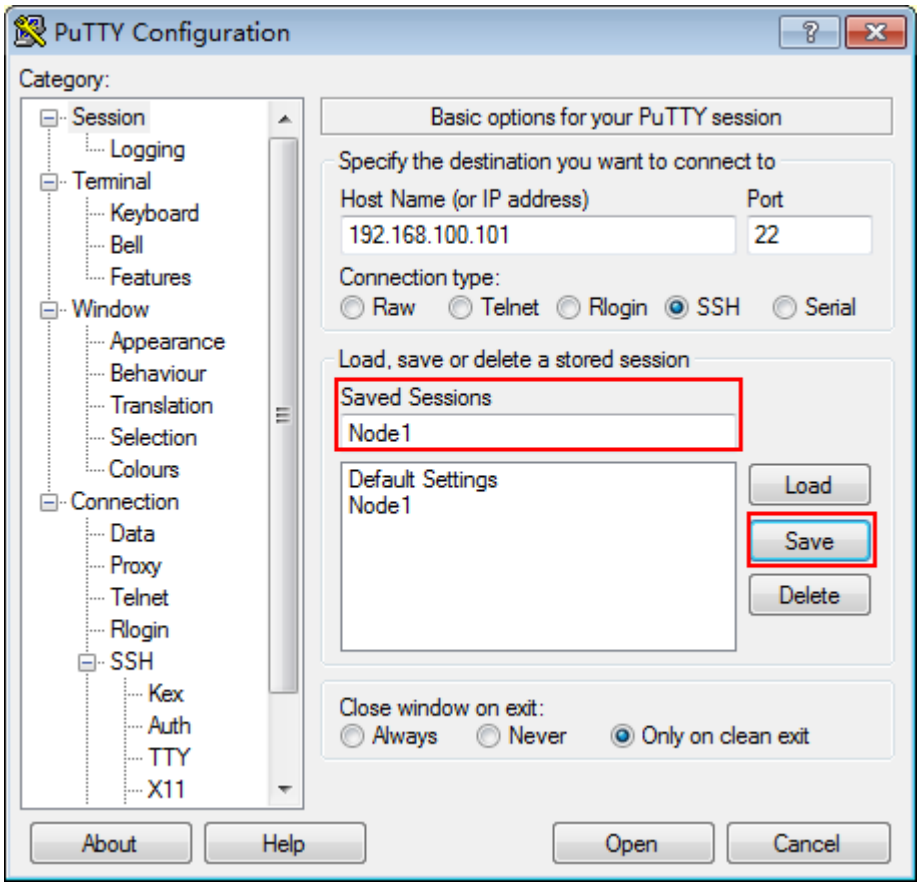
Step 5 In the **Category** area in the left pane, select **Session**.

Step 6 To facilitate subsequent access, create a customized session in **Saved Sessions** and click **Save**, as shown in **Figure 5-28**.

After this step is performed, go to **8**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-28 Saving a session



Step 7 Select a saved session and click **Load** to load the session.

Step 8 Click **Open** to open the session.

Step 9 Enter the user name for logging in to the target node as prompted.

If the private key certificate is encrypted, enter its password as prompted.

----End

5.5.1.3 Logging In to a Node Using a KVM

Context

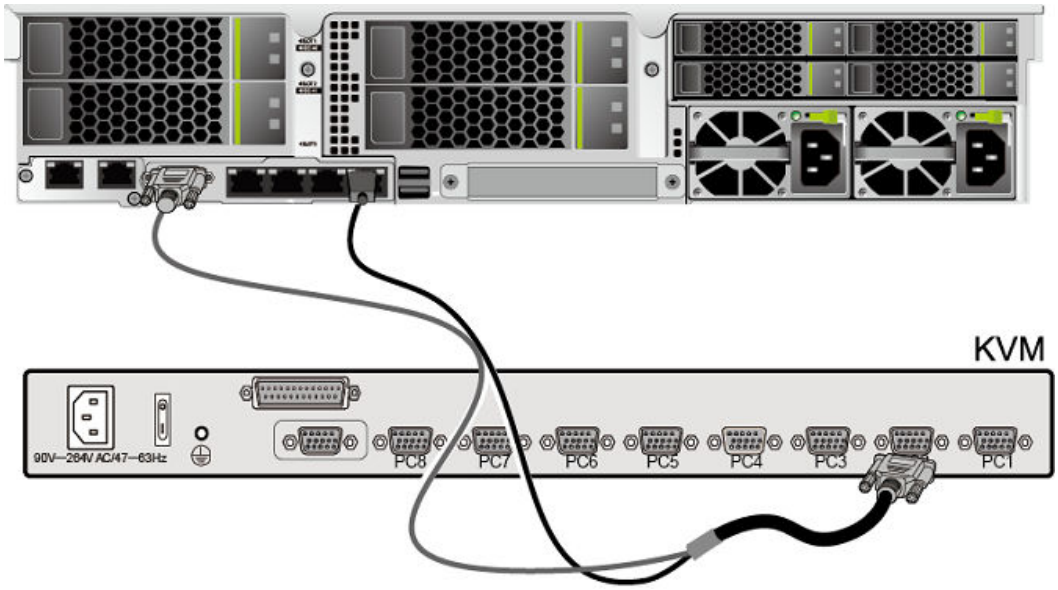
A video graphic array (VGA) cable, display, mouse, and keyboard can work together to serve as a KVM. You can connect a display to a node using a VGA cable and VGA port and then connect a mouse and keyboard to the node through USB ports. After the display is connected, the OS login page of the node will appear. If the login page is not displayed, press **Enter**.

Procedure

Step 1 Connect the node to any port from PC1 to PC8 on the KVM, as shown in **Figure 5-29**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-29 Connecting a node to a KVM



Step 2 Press a number key on the KVM.

For example, to connect the node to port PC2 on the KVM, press **2**.

Step 3 Enter the user name **root** and its password for logging in to the Linux OS. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)* or *OceanStor Pacific Series 8.2.1 Account List (Block Service)*. You need to change the default password upon the first login.

NOTE

If the KVM connected to the node is not delivered with the node, logging to the node may fail. In this case, disconnect the KVM and connect a display and a keyboard to the node.

----End

5.5.2 Switch-Related Operations

This section describes how to log in to a switch and configure the switch.

5.5.2.1 Logging In to a Switch

Prerequisites

- A console cable is available.
- HyperTerminal software, such as PuTTY, has been installed on the PC.

  You can use the built-in HyperTerminal software (such as the HyperTerminal of Windows 2000) on the PC. If no built-in HyperTerminal software is available, use the third-party HyperTerminal software. For details, see the software user guide or online help.

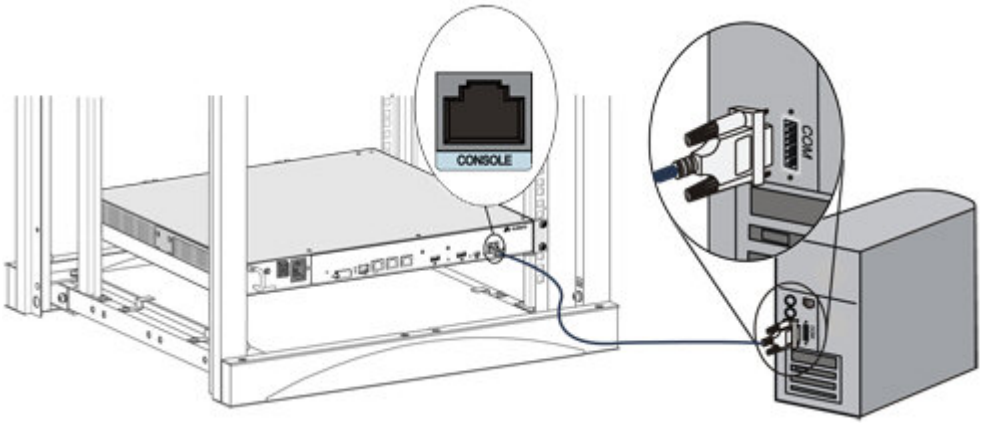
Procedure

Step 1 Insert the DB-9 connector of the console cable to the 9-pin serial port on the PC, and insert the RJ-45 connector to the CONSOLE port of the switch.

 Copyright © Huawei Technologies Co., Ltd.

The location of the CONSOLE port varies depending on the specific switch model, as shown in **Figure 5-30**.

Figure 5-30 Connecting to the switch through the CONSOLE port



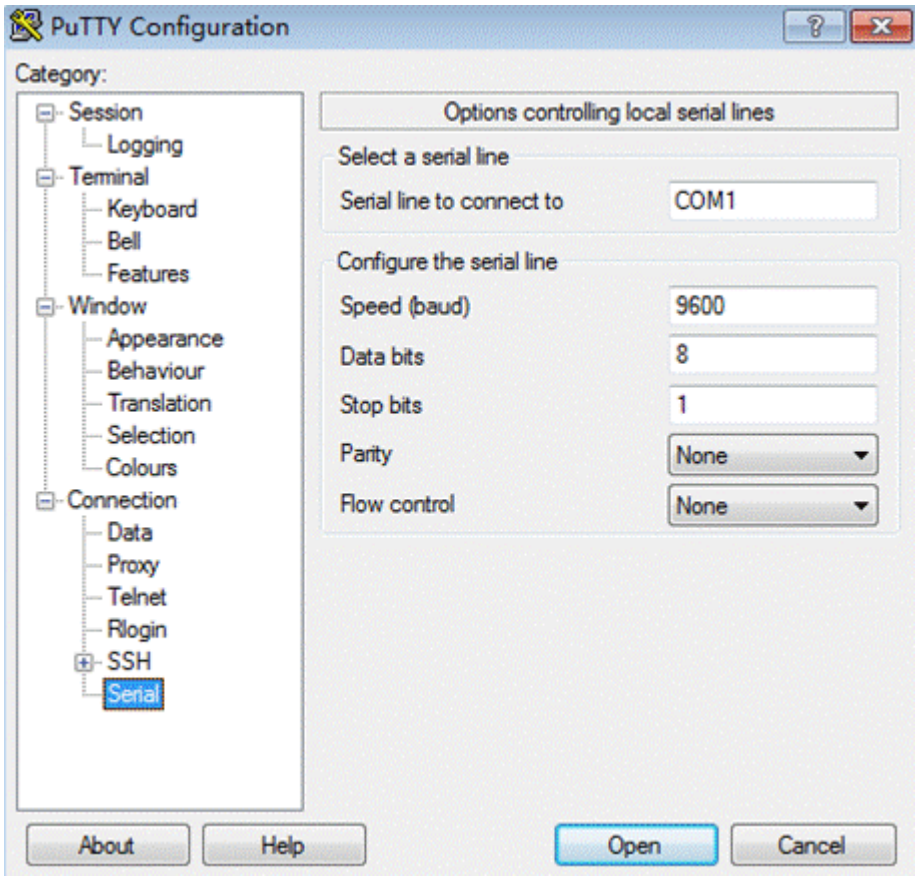
Step 2 Open the HyperTerminal on the PC, establish a connection, and set the connected port and communication parameters. The following uses PuTTY as an example, as shown in **Figure 5-31**.

Because multiple ports may exist on the PC, select the one that connects to the console cable.

Set **Speed (baud)** to **9600**, **Data bits** to **8**, **Stop bits** to **1**, **Parity** to **None**, and **Flow control** to **None**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-31 Login page of the HyperTerminal



Step 3 If the following information is displayed, press **Ctrl+C**.

```
USB discovery phase started...
Press CTRL+C to abort Zero Touch Provisioning in 10 seconds...
```

Step 4 When the following information is displayed, set the login password as prompted (the information displayed in the following figure is for reference only):

```
An initial password is required for the first login via the console.
Continue to set it? [Y/N]: y
Set a password and keep it safe! Otherwise you will not be able to login via the
console.
Please configure the login password (8-16)
Enter Password:
Confirm Password:
```

----End

5.5.2.2 Configuring Flow Control for a Switch

In a new cluster, if the transmission protocol is RoCE, set **Network Flow Classification** to **By using DSCP bits on the IP header** during storage deployment and use the DSCP flow control algorithm for the flow control of the corresponding switch.

5.5.2.2.1 DSCP Flow Control Algorithm

 Copyright © Huawei Technologies Co., Ltd.

5.5.2.2.1.1 Configuring Flow Control for a Switch (Recommended Configuration of AI Fabric)

Scenarios

If a storage node or DPC compute node uses RoCE NICs, you need to configure the layer 2 Priority-based Flow Control (PFC) protocol and layer 3 Explicit Congestion Notification (ECN) protocol for the ports on the access and aggregation switches.

In this section, the AI Fabric function is enabled for the flow control configuration of the switches. This function aims to provide a network environment with zero packet loss, low latency, and high throughput for RoCE to meet high performance requirements.

This section covers the following switches (applicable to both front- and back-end storage switches):

- **CE6857/CE6857E/CE6857F Switch**
- **CE6865/CE6865E Switch**
- **CE6866 Switch**
- **CE8850 Switch**
- **CE8851 Switch**
- **CE16804/CE16808 Switch**

NOTE

The CE16804 and CE16808 switches support only the AI Fabric function.

This section uses different versions as examples to describe the commands for different switches. The mappings are as follows. If you encounter compatibility issues when running commands for other versions, see the product documentation of the desired switch version. CE series switches: For enterprise users, **click here**. For carrier users, **click here**.

- V200R021C00 is used as an example to describe the commands for the CE6865, CE6865E, CE8850, CE6857, CE6857E, and CE6857F switches.
- V300R021C00 is used as an example to describe the commands for the CE6866 and CE8851 switches.
- V300R021C10 is used as an example to describe the commands for the CE16804 and CE16808 switches.

Prerequisites

- You have obtained the login information about the switch to be configured.
- The AI Fabric function has been enabled. The required switch versions are as follows:
  - The software version of the CE6857, CE6857E, or CE6857F switch cannot be earlier than V200R021C00. If the version is earlier than V200R021C00, upgrade the switch software by referring to *CloudEngine 8800, 7800, 6800, and 5800 Upgrade Guide* of the desired version.
  - The software version of the CE6865, CE6865E, or CE8850 switch cannot be earlier than V200R019C10. If the version is earlier than V200R019C10, upgrade the switch software by referring to *CloudEngine 8800, 7800, 6800, and 5800 Upgrade Guide* of the desired version.
  - The software version of the CE6866 or CE8851 switch cannot be earlier than V300R021C00. If the version is earlier than V300R021C00, upgrade

 Copyright © Huawei Technologies Co., Ltd.

the switch software by referring to *CloudEngine 8800 and 6800 Upgrade Guide* of the desired version.

- The software version of the CE16804 or CE16808 switch cannot be earlier than V300R021C10. If the version is earlier than V300R021C10, upgrade the switch software by referring to *CloudEngine 16800 Upgrade Guide* of the desired version.

- The AI Fabric function is controlled by a license, which needs to be loaded on the switch. The following describes how to check whether a license takes effect on a switch:
  - CE6865, CE6865E, CE8850, CE6857, CE6857E, or CE6857F: Check whether the command output contains **CE-LIC-LLETH**:
    - If yes, the license of the switch contains the AI Fabric function. Configure flow control by referring to this section.
    - If no, the license of the switch does not contain the AI Fabric function. Configure flow control by referring to **Configuring Flow Control for a Switch**.
  - CE6866, CE8851, CE16804, or CE16808: Check whether the command output contains **CE-LIC-AFRD**:
    - If yes, the license of the switch contains the AI Fabric function. Configure flow control by referring to this section.
    - If no, the license of the switch does not contain the AI Fabric function. Configure flow control by referring to **Configuring Flow Control for a Switch**. The CE16804 and CE16808 switches support only the AI Fabric function.

```
<CE8850-Leaf1>display license
MainBoard:
 Active License    :
 License state     : Trial
 Revoke ticket     : No ticket
 RD of Huawei Technologies Co., Ltd.
 Product name      : CloudEngine 8800
 Product version   : V200R020
 License Serial No : LIC202106294QOG50
 Creator           : Huawei Technologies Co., Ltd.
 Created Time      : 2021-06-29 20:07:35
 SnS End Date      : --
 ----------------------------------------------------------------
 Item name          Item type      Value      Description
 ----------------------------------------------------------------
 CE-LIC-VXLAN       Function       YES        CE-LIC-VXLAN
 CE-LIC-FCF-PORT    Resource       512        CE-LIC-FCF-PORT
 CE-LIC-FCF-ALL     Function       YES        CE-LIC-FCF-ALL
 CE-LIC-NPV         Function       YES        CE-LIC-NPV
 CE-LIC-TLM         Function       YES        CE-LIC-TLM
 CE-LIC-LLETH       Function       YES        CE-LIC-LLETH
 CE-LIC-PTP         Function       YES        CE-LIC-PTP
 CE-LIC-FINHA       Function       YES        CE-LIC-FINHA
 CE-LIC-25G01       Resource       1          CE-LIC-25G01
 CE-LIC-40G01       Resource       1          CE-LIC-40G01
 CE-LIC-100G01      Resource       1          CE-LIC-100G01
 License state: Trial. The trial days remains 57 day(s).
 Apply for authentic license before the current license expires.
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Obtain the validity period of the license according to **License state: Trial. The trial days remains 57 day(s)** in the command output.

CE6857/CE6857E/CE6857F Switch

Step 1 Configure the PFC priority and PFC deadlock detection.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

If the following error information is displayed when you run the **priority 2 4** command, rectify the fault by referring to **5.5.24.2 How Do I Solve the Problem That the Number of PFC-enabled Queues Exceeds the Upper Limit?**.

```
Error:The number of PFC-enabled queues exceeds the upper limit (2).
```

```
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 2 4
[*HUAWEI-dcb-pfc-default]priority 4 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 4 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 4 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
Info: The deadlock recovery time is rounded up to an integer multiple of 100 as the actually configured value.[*HUAWEI]dcb pfc deadlock recovery-behavior forwarding slot 1
[*HUAWEI]commit
[~HUAWEI]quit
```

Step 2 Enable AI Fabric.

NOTE

When AI Fabric is enabled, the VIQ function is enabled by default. You need to restart the switch.

```
<HUAWEI> system-view
[*HUAWEI] low-latency fabric
[*HUAWEI-low-latency-fabric] commit
[~HUAWEI-low-latency-fabric] quit
[~HUAWEI] ai-service
[*HUAWEI-ai-service] ai-ecn
[*HUAWEI-ai-service-ai-ecn] ai-ecn enable
[*HUAWEI-ai-service-ai-ecn] commit
[~HUAWEI-ai-service-ai-ecn] quit
[~HUAWEI-ai-service] quit
[~HUAWEI] quit
```

Step 3 Save the configuration and restart the switch.

```
<HUAWEI> save
Warning: The current configuration will be written to the device. Continue? [Y/N]:y
Info: Save the configuration successfully.
<HUAWEI> reboot
Warning: The system will reboot. Continue? [Y/N]:y
```

Step 4 Configure the buffer alarm function for ports.

```
[~HUAWEI]qos buffer overrun alarm enable
[*HUAWEI]qos buffer overrun threshold 80
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI]commit
[~HUAWEI]quit
```

Step 5 Configure flow control for uplink ports.

NOTE

- The uplink ports refer to the ports on access switches for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other uplink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI]interface 100GE1/0/1 #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]qos drr 0 4
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 4 drr weight 90
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]dcb pfc buffer 0 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]dcb pfc buffer 4 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]storm suppression broadcast packets 1000
[*HUAWEI-100GE1/0/1]storm suppression multicast packets 200
[*HUAWEI-100GE1/0/1]storm suppression unknown-unicast 1
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23-27-CE]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells   B:bytes   K:kilobytes   M:megabytes   D:dynamic alpha
------------------------------------------------------------------------------
Interface      Queue    Guaranteed        Xon Xon-Offset       Xoff        Hdrm
------------------------------------------------------------------------------
100GE1/0/1         4         8(C)       50(C)      20(C)       4(D)      330(C)
                   5         8(C)       50(C)      20(C)     200(C)      180(C)
------------------------------------------------------------------------------
```

Step 6 Configure flow control for downlink ports.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The downlink ports refer to the ports on access switches for connecting to storage devices.
- Repeat the following operations to configure flow control for other downlink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- If switch ports are connected to LOM NICs, the DSCP flow control information of the LOM NICs is recorded in VLAN packets. In this case, do not run the **trust dscp** command. Otherwise, the obtained flow control information is incorrect. If switch ports are connected to non-LOM NICs, the DSCP flow control information of the NICs is recorded in IP packets. In this case, you must run the **trust dscp** command to obtain the DSCP queue information.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI]interface 10GE1/0/1  #This port is only an example. The actual port prevails.
[~HUAWEI-10GE1/0/1]trust dscp
[*HUAWEI-10GE1/0/1]qos drr 0 4
[*HUAWEI-10GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-10GE1/0/1]qos queue 4 drr weight 90
[*HUAWEI-10GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-10GE1/0/1]dcb pfc buffer 0 xoff dynamic 4 hdrm 250
[*HUAWEI-10GE1/0/1]dcb pfc buffer 4 xoff dynamic 4 hdrm 250
[*HUAWEI-10GE1/0/1]storm suppression broadcast packets 1000
[*HUAWEI-10GE1/0/1]storm suppression multicast packets 200
[*HUAWEI-10GE1/0/1]storm suppression unknown-unicast 1
[*HUAWEI-10GE1/0/1]commit
[~HUAWEI-10GE1/0/1]quit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23-27-CE-10GE1/0/1]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells    B:bytes    K:kilobytes    M:megabytes    D:dynamic alpha
-------------------------------------------------------------------------------
Interface      Queue    Guaranteed         Xon Xon-Offset       Xoff        Hdrm
-------------------------------------------------------------------------------
100GE1/0/1         4          8(C)       50(C)      20(C)       4(D)      330(C)
                   5          8(C)       50(C)      20(C)     200(C)      180(C)

10GE1/0/1          4          8(C)       50(C)      20(C)       4(D)      250(C)
                   5          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
[~A23-27-CE-10GE1/0/1]
```

Steps **Step 7** to **Step 10** are performed on a Layer 2 network with an aggregation switch.

Step 7 Enable PFC to implement backpressure based on the priority after DSCP mapping (configured when CE6857/CE6857E/CE6857F switches function as access switches).

```
[~HUAWEI] dcb pfc dscp-mapping enable slot 1
[*HUAWEI] commit
```

Step 8 Enable the DSCP mapping function only on uplink ports of access switches.

 Copyright © Huawei Technologies Co., Ltd.

```
[~HUAWEI] interface 100GE1/0/1
[~HUAWEI-100GE1/0/1] qos phb marking dscp enable
[*HUAWEI-100GE1/0/1] commit
[~HUAWEI] quit
```

NOTE

The uplink ports refer to the ports on access switches for connecting to aggregation switches.

Step 9 Configure static ECN on the peer-link interface (configured on the peer-link interface when CE6857/CE6857E/CE6857F switches function as access switches and form M-LAG).

```
[~HUAWEI]drop-profile ecn_100G
[*HUAWEI-drop-ecn_100G]ecn buffer-size low-limit 425000 high-limit 750000 discard-percentage 10
[*HUAWEI-drop-ecn_100G]commit
[~HUAWEI-drop-drop100G]interface 100GE1/0/1
[~HUAWEI-100GE1/0/1]qos queue 4 wred ecn_100G
[*HUAWEI-100GE1/0/1]qos queue 4 ecn
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

Step 10 Configure PFC deadlock prevention only on uplink ports of access switches. (Configure this function only when there are at least six switches, including four access switches and two aggregation switches.)

```
[~HUAWEI]dcb pfc uplink group mygroup
[*HUAWEI-dcb-pfc-uplink-group-mygroup]group-member interface 100GE 1/0/1 to 100GE 1/0/6
[*HUAWEI-dcb-pfc-uplink-group-mygroup]adjust priority 5 dscp 40
Warning: This command will change the priority of the queues that match hook flows. Continue? [Y/N]:y
[*HUAWEI-dcb-pfc-uplink-group-mygroup]commit
[~HUAWEI-dcb-pfc-uplink-group-mygroup]quit
```

----End

CE6865/CE6865E Switch

Step 1 Configure the PFC priority and PFC deadlock detection.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

You are advised to configure **priority 4 turn-off threshold 10** on an access switch.

If the following error information is displayed when you run the **priority 4 5** command, rectify the fault by referring to **5.5.24.2 How Do I Solve the Problem That the Number of PFC-enabled Queues Exceeds the Upper Limit?**.

```
Error:The number of PFC-enabled queues exceeds the upper limit (2).
```

```
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 4 5
[*HUAWEI-dcb-pfc-default]priority 4 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 4 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
[~HUAWEI]commit
[~HUAWEI]quit
```

Step 2 Enable AI Fabric.

 Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> When AI Fabric is enabled, the VIQ function is enabled by default. You need to restart the switch.

```
<HUAWEI> system-view
[*HUAWEI] low-latency fabric
[*HUAWEI-low-latency-fabric] undo qos dynamic-ecn-threshold enable
[*HUAWEI-low-latency-fabric] commit
[~HUAWEI-low-latency-fabric] quit
[~HUAWEI] ai-service
[*HUAWEI-ai-service] ai-ecn
[*HUAWEI-ai-service-ai-ecn] ai-ecn enable
[*HUAWEI-ai-service-ai-ecn] commit
[~HUAWEI-ai-service-ai-ecn] quit
[~HUAWEI-ai-service] quit
[~HUAWEI] quit
```

Step 3 Save the configuration and restart the switch.

```
<HUAWEI> save
Warning: The current configuration will be written to the device. Continue? [Y/N]:y
Info: Save the configuration successfully.
<HUAWEI> reboot
Warning: The system will reboot. Continue? [Y/N]:y
```

Step 4 Enable PFC to implement backpressure based on the priority after DSCP mapping.

```
[~HUAWEI]dcb pfc dscp-mapping enable slot 1
[*HUAWEI]diffserv domain default
[*HUAWEI-dsdomain-default]commit
[~HUAWEI-dsdomain-default]quit
```

Step 5 Configure the buffer alarm function for ports.

```
[~HUAWEI]qos buffer overrun alarm enable
[*HUAWEI]qos buffer overrun threshold 80
[*HUAWEI]commit
[~HUAWEI]quit
```

Step 6 Configure flow control for uplink ports.

> **NOTE**
>
- The uplink ports refer to the ports on access switches for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other uplink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI]interface 100GE1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]qos drr 0 4
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 4 drr weight 90
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23_25G_02-dcb-pfc-default]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells   B:bytes   K:kilobytes   M:megabytes   D:dynamic alpha
-------------------------------------------------------------------------------
Interface      Queue    Guaranteed        Xon Xon-Offset       Xoff        Hdrm
-------------------------------------------------------------------------------
100GE1/0/1         4          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/2         4          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/3         4          8(C)       50(C)      20(C)       4(D)      330(C)
-------------------------------------------------------------------------------
25GE1/0/11         4          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
25GE1/0/12         4          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
25GE1/0/13         4          8(C)       50(C)      20(C)     200(C)      180(C)
```

Step 7 Configure flow control for downlink ports.

NOTE

- The downlink ports refer to the ports on access switches for connecting to storage devices.
- Repeat the following operations to configure flow control for other downlink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- If switch ports are connected to LOM NICs, the DSCP flow control information of the LOM NICs is recorded in VLAN packets. In this case, do not run the **trust dscp** command. Otherwise, the obtained flow control information is incorrect. If switch ports are connected to non-LOM NICs, the DSCP flow control information of the NICs is recorded in IP packets. In this case, you must run the **trust dscp** command to obtain the DSCP queue information.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI]interface 25GE1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-25GE1/0/1]trust dscp
[*HUAWEI-25GE1/0/1]qos drr 0 4
[*HUAWEI-25GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-25GE1/0/1]qos queue 4 drr weight 90
[*HUAWEI-25GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A26-27-Y2-dcb-pfc-default]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the larger value between the value
of xon and the value of xoff minus the value of xon-offset.
C:cells    B:bytes    K:kilobytes    M:megabytes D:dynamic alpha
--------------------------------------------------------------------------------
Interface      Queue    Guaranteed         Xon Xon-Offset       Xoff        Hdrm
--------------------------------------------------------------------------------
25GE1/0/5          4          8(C)       50(C)      20(C)       4(D)      250(C)
                   5          8(C)       50(C)      20(C)     200(C)      180(C)

[~A26-27-Y2-dcb-pfc-default]
```

Step 8 Configure PFC deadlock prevention only on uplink ports of access switches. (Configure this function only when there are at least six switches, including four access switches and two aggregation switches.)

```
[*HUAWEI]dcb pfc uplink group mygroup
[*HUAWEI-dcb-pfc-uplink-group-mygroup]group-member interface 100GE 1/0/1 to 100GE 1/0/6
[*HUAWEI-dcb-pfc-uplink-group-mygroup]adjust priority 5 dscp 40
Warning: This command will change the priority of the queues that match hook flows. Continue? [Y/N]:y
[*HUAWEI-dcb-pfc-uplink-group-mygroup]commit
[~HUAWEI-dcb-pfc-uplink-group-mygroup]quit
```

----End

CE6866 Switch

Step 1 Enable AI ECN.

```
[~HUAWEI]ai-service
[~HUAWEI-ai-service]ai-ecn
[*HUAWEI-ai-service-ai-ecn]ai-ecn enable
[*HUAWEI-ai-service-ai-ecn]assign queue 4
[*HUAWEI-ai-service-ai-ecn]quit
[*HUAWEI-ai-service]quit
[*HUAWEI]commit
```

Step 2 Configure the PFC priority and PFC deadlock detection.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

You are advised to configure **priority 4 turn-off threshold 10** on an access switch.

If the following error information is displayed when you run the **priority 4 5** command, rectify the fault by referring to **5.5.24.2 How Do I Solve the Problem That the Number of PFC-enabled Queues Exceeds the Upper Limit?**.

```
Error:The number of PFC-enabled queues exceeds the upper limit (2).
```

```
[~HUAWEI]dcb pfc
[*HUAWEI-dcb-pfc-default]priority 4 5
[*HUAWEI-dcb-pfc-default]priority 4 turn-off threshold 10
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]dcb pfc deadlock-detect timer 100
[~HUAWEI]dcb pfc deadlock-recovery timer 100
[~HUAWEI]commit
```

Step 3 Configure the buffer alarm function for ports.

```
[~HUAWEI]qos buffer overrun alarm enable
[*HUAWEI]qos buffer overrun threshold 80
[*HUAWEI]commit
```

Step 4 Configure flow control for uplink ports.

NOTE

- The uplink ports refer to the ports on access switches for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other uplink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI-100GE1/0/1]interface 100GE1/0/1 #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]trust dscp
[*HUAWEI-100GE1/0/1]qos drr 0 4
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 4 drr weight 90
[*HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-100GE1/0/1]qos buffer queue 4 shared-threshold dynamic 10
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]dcb pfc buffer 4 xon static 550 KB xoff static 600 KB
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the values in the **Xon** and **Xoff** columns do not exist for the configured network ports in the table in the command output, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

If the command is successfully executed, an example of the command output is as follows:

```
[~A31-23]display dcb pfc buffer
Xon:       PFC backpressure stop threshold
Xoff:      PFC backpressure threshold
K:kilobytes
-------------------------------------------------
Interface      Queue          Xon          Xoff
-------------------------------------------------
100GE1/0/1         4        550(K)        600(K)
-------------------------------------------------
100GE1/0/2         4        550(K)        600(K)
-------------------------------------------------
100GE1/0/3         4        550(K)        600(K)
-------------------------------------------------
100GE1/0/4         4        550(K)        600(K)
-------------------------------------------------
```

Step 5 Configure flow control for downlink ports.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The downlink ports refer to the ports on access switches for connecting to storage devices.
- Repeat the following operations to configure flow control for other downlink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- If switch ports are connected to LOM NICs, the DSCP flow control information of the LOM NICs is recorded in VLAN packets. In this case, do not run the **trust dscp** command. Otherwise, the obtained flow control information is incorrect. If switch ports are connected to non-LOM NICs, the DSCP flow control information of the NICs is recorded in IP packets. In this case, you must run the **trust dscp** command to obtain the DSCP queue information.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI-25GE1/0/1]interface 25GE1/0/1  #This port is only an example. The actual port prevails.
[~HUAWEI-25GE1/0/1]trust dscp
[*HUAWEI-25GE1/0/1]qos drr 0 4
[*HUAWEI-25GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-25GE1/0/1]qos queue 4 drr weight 90
[*HUAWEI-25GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-25GE1/0/1]qos buffer queue 4 shared-threshold dynamic 10
[*HUAWEI-25GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-25GE1/0/1]dcb pfc buffer 4 xon static 550 KB xoff static 600 KB
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the values in the **Xon** and **Xoff** columns do not exist for the configured network ports in the table in the command output, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

If the command is successfully executed, an example of the command output is as follows:

```
[~A31-23]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
K:kilobytes
-------------------------------------------------
Interface     Queue          Xon          Xoff
-------------------------------------------------
25GE1/0/1         4        550(K)        600(K)
-------------------------------------------------
25GE1/0/2         4        550(K)        600(K)
-------------------------------------------------
25GE1/0/3         4        550(K)        600(K)
-------------------------------------------------
```

Step 6 Configure PFC deadlock prevention only on uplink ports of access switches. (Configure this function only when there are at least six switches, including four access switches and two aggregation switches.)

```
[~HUAWEI]dcb pfc uplink group mygroup
[*HUAWEI-dcb-pfc-uplink-group-mygroup]group-member interface 100GE 1/0/1 to 100GE 1/0/6
Info: The current interface has been added to an Eth-Trunk interface, and PFC deadlock prevention takes effect based on the Eth-Trunk interface.
[*HUAWEI-dcb-pfc-uplink-group-mygroup]adjust original-dscp 32 to priority 5 dscp 40
[*HUAWEI-dcb-pfc-uplink-group-mygroup]commit
[~HUAWEI-dcb-pfc-uplink-group-mygroup]quit
```

----End

 Copyright © Huawei Technologies Co., Ltd.

CE8850 Switch

Step 1 Configure the PFC priority and PFC deadlock detection.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

You are advised to configure **priority 4 turn-off threshold 10** on an access switch.

If the following error information is displayed when you run the **priority 4 5** command, rectify the fault by referring to **5.5.24.2 How Do I Solve the Problem That the Number of PFC-enabled Queues Exceeds the Upper Limit?**.

```
Error:The number of PFC-enabled queues exceeds the upper limit (2).
```

```
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 4 5
[*HUAWEI-dcb-pfc-default]priority 4 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 4 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
[~HUAWEI]commit
[~HUAWEI]quit
```

Step 2 Enable AI Fabric.

NOTE

When AI Fabric is enabled, the VIQ function is enabled by default. You need to restart the switch.

```
<HUAWEI> system-view
[*HUAWEI] low-latency fabric
[*HUAWEI-low-latency-fabric] undo qos dynamic-ecn-threshold enable
[*HUAWEI-low-latency-fabric] commit
[~HUAWEI-low-latency-fabric] quit
[~HUAWEI] ai-service
[*HUAWEI-ai-service] ai-ecn
[*HUAWEI-ai-service-ai-ecn] ai-ecn enable
[*HUAWEI-ai-service-ai-ecn] commit
[~HUAWEI-ai-service-ai-ecn] quit
[~HUAWEI-ai-service] quit
[~HUAWEI] quit
```

Step 3 Save the configuration and restart the switch.

```
<HUAWEI> save
Warning: The current configuration will be written to the device. Continue? [Y/N]:y
Info: Save the configuration successfully.
<HUAWEI> reboot
Warning: The system will reboot. Continue? [Y/N]:y
```

Step 4 Enable PFC to implement backpressure based on the priority after DSCP mapping.

```
[~HUAWEI]dcb pfc dscp-mapping enable slot 1
[*HUAWEI]diffserv domain default
[*HUAWEI-dsdomain-default]commit
[~HUAWEI-dsdomain-default]quit
```

Step 5 Configure the buffer alarm function for ports.

```
[~HUAWEI]qos buffer overrun alarm enable
[*HUAWEI]qos buffer overrun threshold 80
[*HUAWEI]commit
[~HUAWEI]quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 6 Configure flow control for ports.

NOTE

- For aggregation switches, the ports refer to the ports on the aggregation switches for connecting to access switches. For access switches, the ports refer to the ports on the access switches for connecting to storage devices and those for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- If switch ports are connected to LOM NICs, the DSCP flow control information of the LOM NICs is recorded in VLAN packets. In this case, do not run the **trust dscp** command. Otherwise, the obtained flow control information is incorrect. If switch ports are connected to non-LOM NICs, the DSCP flow control information of the NICs is recorded in IP packets. In this case, you must run the **trust dscp** command to obtain the DSCP queue information.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI]interface 100GE1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]trust dscp
[~HUAWEI-100GE1/0/1]qos drr 0 4
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 4 drr weight 90
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23_25G_02-dcb-pfc-default]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells   B:bytes   K:kilobytes   M:megabytes   D:dynamic alpha
--------------------------------------------------------------------------------
Interface      Queue    Guaranteed        Xon Xon-Offset       Xoff        Hdrm
--------------------------------------------------------------------------------
100GE1/0/1         4         8(C)       50(C)      20(C)     200(C)      180(C)
--------------------------------------------------------------------------------
100GE1/0/2         4         8(C)       50(C)      20(C)     200(C)      180(C)
--------------------------------------------------------------------------------
100GE1/0/3         4         8(C)       50(C)      20(C)       4(D)      330(C)
--------------------------------------------------------------------------------
25GE1/0/11         4         8(C)       50(C)      20(C)     200(C)      180(C)
--------------------------------------------------------------------------------
25GE1/0/12         4         8(C)       50(C)      20(C)     200(C)      180(C)
--------------------------------------------------------------------------------
25GE1/0/13         4         8(C)       50(C)      20(C)     200(C)      180(C)
```

Step 7 (Optional) Configure PFC deadlock prevention only on uplink ports of access switches. (Configure this function only when there are at least six switches, including four access switches and two aggregation switches.)

NOTE

CE8850 switches support this operation, but FM8850 switches do not.

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI]dcb pfc uplink group mygroup
[*HUAWEI-dcb-pfc-uplink-group-mygroup]group-member interface 100GE 1/0/1 to 100GE 1/0/6
[*HUAWEI-dcb-pfc-uplink-group-mygroup]adjust priority 5 dscp 40
Warning: This command will change the priority of the queues that match hook flows. Continue? [Y/N]:y
[*HUAWEI-dcb-pfc-uplink-group-mygroup]commit
[~HUAWEI-dcb-pfc-uplink-group-mygroup]quit
```

----End

CE8851 Switch

Step 1 Enable AI ECN.

```
[~HUAWEI]ai-service
[~HUAWEI-ai-service]ai-ecn
[*HUAWEI-ai-service-ai-ecn]ai-ecn enable
[*HUAWEI-ai-service-ai-ecn]assign queue 4
[*HUAWEI-ai-service-ai-ecn]quit
[*HUAWEI-ai-service]quit
[*HUAWEI]commit
```

Step 2 Configure the PFC priority and PFC deadlock detection.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

You are advised to configure **priority 4 turn-off threshold 10** on an access switch.

If the following error information is displayed when you run the **priority 4 5** command, rectify the fault by referring to **5.5.24.2 How Do I Solve the Problem That the Number of PFC-enabled Queues Exceeds the Upper Limit?**.

```
Error:The number of PFC-enabled queues exceeds the upper limit (2).
```

```
[~HUAWEI]dcb pfc
[*HUAWEI-dcb-pfc-default]priority 4 5
[*HUAWEI-dcb-pfc-default]priority 4 turn-off threshold 10
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]dcb pfc deadlock-detect timer 100
[~HUAWEI]dcb pfc deadlock-recovery timer 100
[~HUAWEI]commit
```

Step 3 Configure the buffer alarm function for ports.

```
[~HUAWEI]qos buffer overrun alarm enable
[*HUAWEI]qos buffer overrun threshold 80
[*HUAWEI]commit
```

Step 4 Configure flow control for ports.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- For aggregation switches, the ports refer to the ports on the aggregation switches for connecting to access switches. For access switches, the ports refer to the ports on the access switches for connecting to storage devices and those for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- If switch ports are connected to LOM NICs, the DSCP flow control information of the LOM NICs is recorded in VLAN packets. In this case, do not run the **trust dscp** command. Otherwise, the obtained flow control information is incorrect. If switch ports are connected to non-LOM NICs, the DSCP flow control information of the NICs is recorded in IP packets. In this case, you must run the **trust dscp** command to obtain the DSCP queue information.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI-100GE1/0/1]interface 100GE1/0/1  #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]trust dscp
[*HUAWEI-100GE1/0/1]qos drr 0 4
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 4 drr weight 90
[*HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-100GE1/0/1]qos buffer queue 4 shared-threshold dynamic 10
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]dcb pfc buffer 4 xon static 550 KB xoff static 600 KB
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the values in the **Xon** and **Xoff** columns do not exist for the configured network ports in the table in the command output, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

If the command is successfully executed, an example of the command output is as follows:

```
[~A31-23]display dcb pfc buffer
Xon:       PFC backpressure stop threshold
Xoff:      PFC backpressure threshold
K:kilobytes
-------------------------------------------------
Interface     Queue          Xon          Xoff
-------------------------------------------------
100GE1/0/1        4       550(K)        600(K)
-------------------------------------------------
100GE1/0/2        4       550(K)        600(K)
-------------------------------------------------
100GE1/0/3        4       550(K)        600(K)
-------------------------------------------------
100GE1/0/4        4       550(K)        600(K)
-------------------------------------------------
```

Step 5 Configure PFC deadlock prevention only on uplink ports of access switches. (Configure this function only when there are at least six switches, including four access switches and two aggregation switches.)

```
[~HUAWEI]dcb pfc uplink group mygroup
[*HUAWEI-dcb-pfc-uplink-group-mygroup]group-member interface 100GE 1/0/1 to 100GE 1/0/6
Info: The current interface has been added to an Eth-Trunk interface, and PFC deadlock prevention takes effect based on the Eth-Trunk interface.
[*HUAWEI-dcb-pfc-uplink-group-mygroup]adjust original-dscp 32 to priority 5 dscp 40
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-dcb-pfc-uplink-group-mygroup]commit
[~HUAWEI-dcb-pfc-uplink-group-mygroup]quit
```

----End

CE16804/CE16808 Switch

Step 1 Enable AI ECN.

```
[~HUAWEI]ai-service
[~HUAWEI-ai-service]ai-ecn
[*HUAWEI-ai-service-ai-ecn]ai-ecn enable
[*HUAWEI-ai-service-ai-ecn]assign queue 4
[*HUAWEI-ai-service-ai-ecn]quit
[*HUAWEI-ai-service]quit
[*HUAWEI]commit
```

Step 2 Enable PFC to implement backpressure based on the priority after DSCP mapping. (This command applies only to aggregation switches.)

```
dcb pfc dscp-mapping enable slot slot-id
```

NOTE

Description of the *slot-id* parameter:

slot-id indicates the slot ID of the specified switch. The value is an integer and can be determined according to the port name. For example, *slot-id* of port 100GE4/0/1 is **4**, and *slot-id* of port 100GE8/0/1 is **8**. If multiple slots are used, for example, slots 4 and 8 are used at the same time, run the following commands for reference:

```
dcb pfc dscp-mapping enable slot 4
dcb pfc dscp-mapping enable slot 8
```

Step 3 Configure DCB PFC.

NOTE

- If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.
- After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.
- You are advised to configure **priority 4 turn-off threshold 10** on an access switch.

```
[~HUAWEI]dcb pfc
[*HUAWEI-dcb-pfc-default]priority 0 4
[*HUAWEI-dcb-pfc-default]priority 0 turn-off threshold 10
[*HUAWEI-dcb-pfc-default]priority 4 turn-off threshold 10
[*HUAWEI-dcb-pfc-default]commit
```

Step 4 Enable PFC deadlock monitoring.

```
[~HUAWEI]dcb pfc deadlock-detect timer 100
[~HUAWEI]dcb pfc deadlock-recovery timer 100
[~HUAWEI]dcb pfc deadlock recovery-behavior discard slot slot-id
[~HUAWEI]commit
```

NOTE

Description of the *slot-id* parameter:

slot-id indicates the slot ID of the specified switch. The value is an integer and can be determined according to the port name. For example, *slot-id* of port 100GE4/0/1 is **4**, and *slot-id* of port 100GE8/0/1 is **8**. If multiple slots are used, for example, slots 4 and 8 are used at the same time, run the following commands for reference:

```
dcb pfc deadlock recovery-behavior discard slot 4
dcb pfc deadlock recovery-behavior discard slot 8
```

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure the switch to generate an alarm when the queue buffer exceeds the threshold.

```
[~HUAWEI]qos buffer overrun alarm enable
[*HUAWEI]qos buffer overrun threshold 80
[*HUAWEI]commit
```

Step 6 Configure flow control for ports.

NOTE

- For aggregation switches, the ports refer to the ports on the aggregation switches for connecting to access switches. For access switches, the ports refer to the ports on the access switches for connecting to storage devices and those for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- If switch ports are connected to LOM NICs, the DSCP flow control information of the LOM NICs is recorded in VLAN packets. In this case, do not run the **trust dscp** command. Otherwise, the obtained flow control information is incorrect. If switch ports are connected to non-LOM NICs, the DSCP flow control information of the NICs is recorded in IP packets. In this case, you must run the **trust dscp** command to obtain the DSCP queue information.
- The **trust dscp** command is configured only on the access switch port connected to a storage device.
- The **qos phb marking dscp enable** command is configured only on the access switch port connected to an aggregation switch.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
# The following uses a 25GE port as an example. The configuration also applies to 100GE ports.
[~HUAWEI-25GE1/0/1]interface 25GE1/0/1  #This port is only an example. The actual port prevails.
[~HUAWEI-25GE1/0/1]qos phb marking dscp enable
[~HUAWEI-25GE1/0/1]trust dscp
[*HUAWEI-25GE1/0/1]qos drr 0 4
[*HUAWEI-25GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-25GE1/0/1]qos queue 4 drr weight 90
[*HUAWEI-25GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-25GE1/0/1]qos buffer queue 4 shared-threshold dynamic 10
[*HUAWEI-25GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-25GE1/0/1]dcb pfc buffer 0 xon static 100 kbytes xoff static 125 kbyte
[*HUAWEI-25GE1/0/1]dcb pfc buffer 4 xon static 100 kbytes xoff static 125 kbytes
[*HUAWEI-25GE1/0/1]storm suppression broadcast packets 1000
[*HUAWEI-25GE1/0/1]storm suppression multicast packets 200
[*HUAWEI-25GE1/0/1]storm suppression unknown-unicast packets 200
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the values in the **Xon** and **Xoff** columns do not exist for the configured network ports in the table in the command output, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

If the command is successfully executed, an example of the command output is as follows:

```
[~A31-23]display dcb pfc buffer
Xon:       PFC backpressure stop threshold
Xoff:      PFC backpressure threshold
K:kilobytes
-------------------------------------------------
Interface     Queue          Xon          Xoff
-------------------------------------------------
25GE1/0/0         0        100(K)        125(K)
                  4        100(K)        125(K)
-------------------------------------------------
25GE1/0/1         0        100(K)        125(K)
                  4        100(K)        125(K)
-------------------------------------------------
25GE1/0/2         0        100(K)        125(K)
                  4        100(K)        125(K)
-------------------------------------------------
```

----End

5.5.2.2.1.2 Configuring Flow Control for a Switch

Scenarios

If a storage node or DPC compute node uses RoCE NICs, you need to configure the layer 2 Priority-based Flow Control (PFC) protocol and layer 3 Explicit Congestion Notification (ECN) protocol for the ports on the access and aggregation switches.

This section covers the following switches (applicable to both front- and back-end storage switches):

- **CE6857/CE6857E/CE6857F Switch**
- **CE6865/CE6865E Switch**
- **CE6866 Switch**
- **CE8850 Switch**
- **CE8851 Switch**

NOTE

This section uses different versions as examples to describe the commands for different switches. The mappings are as follows. If you encounter compatibility issues when running commands for other versions, see the product documentation of the desired switch version. CE series switches: For enterprise users, **click here**. For carrier users, **click here**.

- V200R021C00 is used as an example to describe the commands for the CE6865, CE6865E, CE8850, CE6857, CE6857E, and CE6857F switches.
- V300R021C00 is used as an example to describe the commands for the CE6866 and CE8851 switches.

Prerequisites

You have obtained the login information about the switch to be configured.

 Copyright © Huawei Technologies Co., Ltd.

CE6857/CE6857E/CE6857F Switch

Step 1 Configure the PFC priority and PFC deadlock detection.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

If the following error information is displayed when you run the **priority 4 5** command, rectify the fault by referring to **5.5.24.2 How Do I Solve the Problem That the Number of PFC-enabled Queues Exceeds the Upper Limit?**.

```
Error:The number of PFC-enabled queues exceeds the upper limit (2).
```

```
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 4 5
[*HUAWEI-dcb-pfc-default]priority 4 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 4 deadlock-recovery time 10
[~HUAWEI-dcb-pfc-default]priority 4 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
[~HUAWEI]commit
[~HUAWEI]quit
```

Step 2 Configure ECN.

```
[~HUAWEI]drop-profile ecn_10G
[*HUAWEI-drop-ecn_10G]ecn buffer-size low-limit 250000 high-limit 700000 discard-percentage 10
[*HUAWEI-drop-ecn_10G]commit
[~HUAWEI-drop-ecn_10G]quit
[~HUAWEI]drop-profile ecn_100G
[*HUAWEI-drop-ecn_100G]ecn buffer-size low-limit 425000 high-limit 750000 discard-percentage 10
[*HUAWEI-drop-ecn_100G]commit
[~HUAWEI-drop-ecn_100G]quit
```

Step 3 Configure the buffer alarm function for ports.

```
[~HUAWEI]qos buffer overrun alarm enable
[~HUAWEI]qos buffer overrun threshold 80
[~HUAWEI]commit
[~HUAWEI]quit
```

Step 4 Configure flow control for uplink ports.

NOTE

- The uplink ports refer to the ports on access switches for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other uplink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI]interface 100GE1/0/1  #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]qos drr 0 4
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 4 drr weight 90
[*HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-100GE1/0/1]qos buffer queue 4 shared-threshold dynamic 10
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]qos queue 4 wred ecn_100G
[*HUAWEI-100GE1/0/1]qos queue 4 ecn
[*HUAWEI-100GE1/0/1]dcb pfc buffer 0 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]dcb pfc buffer 4 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]storm suppression broadcast packets 1000
[*HUAWEI-100GE1/0/1]storm suppression multicast packets 200
[*HUAWEI-100GE1/0/1]storm suppression unknown-unicast 1
[~HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23-27-CE]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells   B:bytes   K:kilobytes   M:megabytes   D:dynamic alpha
-------------------------------------------------------------------------------
Interface      Queue    Guaranteed         Xon Xon-Offset       Xoff        Hdrm
-------------------------------------------------------------------------------
100GE1/0/1         4          8(C)       50(C)      20(C)       4(D)      330(C)
                   5          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
```

Step 5 Configure flow control for downlink ports.

NOTE

- The downlink ports refer to the ports on access switches for connecting to storage devices.
- Repeat the following operations to configure flow control for other downlink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- If switch ports are connected to LOM NICs, the DSCP flow control information of the LOM NICs is recorded in VLAN packets. In this case, do not run the **trust dscp** command. Otherwise, the obtained flow control information is incorrect. If switch ports are connected to non-LOM NICs, the DSCP flow control information of the NICs is recorded in IP packets. In this case, you must run the **trust dscp** command to obtain the DSCP queue information.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI]interface  10GE1/0/1  #This port is only an example. The actual port prevails.
[~HUAWEI-10GE1/0/1]trust dscp
[*HUAWEI-10GE1/0/1]qos drr 0 4
[*HUAWEI-10GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-10GE1/0/1]qos queue 4 drr weight 90
[*HUAWEI-10GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-10GE1/0/1]qos buffer queue 4 shared-threshold dynamic 10
[*HUAWEI-10GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-10GE1/0/1]qos queue 4 wred ecn_10G
[*HUAWEI-10GE1/0/1]qos queue 4 ecn
[*HUAWEI-10GE1/0/1]dcb pfc buffer 0 xoff dynamic 4 hdrm 250
[*HUAWEI-10GE1/0/1]dcb pfc buffer 4 xoff dynamic 4 hdrm 250
[*HUAWEI-10GE1/0/1]storm suppression broadcast packets 1000
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-10GE1/0/1]storm suppression multicast packets 200
[*HUAWEI-10GE1/0/1]storm suppression unknown-unicast 1
[*HUAWEI-10GE1/0/1]commit
[~HUAWEI-10GE1/0/1]quit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23-27-CE-10GE1/0/1]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells    B:bytes    K:kilobytes    M:megabytes    D:dynamic alpha
--------------------------------------------------------------------------------
Interface      Queue    Guaranteed         Xon Xon-Offset       Xoff        Hdrm
--------------------------------------------------------------------------------
100GE1/0/1         4          8(C)       50(C)      20(C)       4(D)      330(C)
                   5          8(C)       50(C)      20(C)     200(C)      180(C)

10GE1/0/1          4          8(C)       50(C)      20(C)       4(D)      250(C)
                   5          8(C)       50(C)      20(C)     200(C)      180(C)
--------------------------------------------------------------------------------
[~A23-27-CE-10GE1/0/1]
```

Steps **Step 6** to **Step 9** are performed on a Layer 2 network with an aggregation switch.

Step 6 Enable PFC to implement backpressure based on the priority after DSCP mapping (configured when CE6857/CE6857E/CE6857F switches function as access switches).

```
[~HUAWEI] dcb pfc dscp-mapping enable slot 1
[~HUAWEI] commit
```

Step 7 Enable the DSCP mapping function for ports (configured on ports connecting access switches to aggregation switches).

```
[~HUAWEI] interface 100GE1/0/1
[~HUAWEI-100GE1/0/1] qos phb marking dscp enable
[~HUAWEI-100GE1/0/1] commit
[~HUAWEI] quit
```

Step 8 Configure static ECN on the peer-link interface (configured on the peer-link interface when CE6857/CE6857E/CE6857F switches function as access switches and form M-LAG).

```
[~HUAWEI-drop-drop100G] interface 100GE1/0/1
[~HUAWEI-100GE1/0/1]qos queue 4 wred ecn_100G
[*HUAWEI-100GE1/0/1] qos queue 4 ecn
[*HUAWEI-100GE1/0/1] commit
[~HUAWEI-100GE1/0/1] quit
```

Step 9 Configure PFC deadlock prevention only on uplink ports of access switches. (Configure this function only when there are at least six switches, including four access switches and two aggregation switches.)

```
[*HUAWEI]dcb pfc uplink group mygroup
[*HUAWEI-dcb-pfc-uplink-group-mygroup]group-member interface 100GE 1/0/1 to 100GE 1/0/6
[*HUAWEI-dcb-pfc-uplink-group-mygroup]adjust priority 5 dscp 40
Warning: This command will change the priority of the queues that match hook flows. Continue? [Y/N]:y
[*HUAWEI-dcb-pfc-uplink-group-mygroup]commit
[~HUAWEI-dcb-pfc-uplink-group-mygroup]quit
```

----End

 Copyright © Huawei Technologies Co., Ltd.

CE6865/CE6865E Switch

Step 1 Configure the PFC priority and PFC deadlock detection.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

You are advised to configure **priority 4 turn-off threshold 10** on an access switch.

If the following error information is displayed when you run the **priority 4 5** command, rectify the fault by referring to **5.5.24.2 How Do I Solve the Problem That the Number of PFC-enabled Queues Exceeds the Upper Limit?**.

```
Error:The number of PFC-enabled queues exceeds the upper limit (2).
```

```
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 4 5
[*HUAWEI-dcb-pfc-default]priority 4 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 4 deadlock-recovery time 10
[~HUAWEI-dcb-pfc-default]priority 4 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
[~HUAWEI]commit
[~HUAWEI]quit
```

Step 2 Configure ECN.

```
[~HUAWEI]drop-profile ecn_25G
[*HUAWEI-drop-ecn_25G]ecn buffer-size low-limit 250000 high-limit 700000 discard-percentage 10
[*HUAWEI-drop-ecn_25G]commit
[~HUAWEI-drop-ecn_25G]quit
[~HUAWEI]drop-profile ecn_100G
[*HUAWEI-drop-ecn_100G]ecn buffer-size low-limit 425000 high-limit 750000 discard-percentage 10
[*HUAWEI-drop-ecn_100G]commit
[~HUAWEI-drop-ecn_100G]quit
```

Step 3 Enable PFC to implement backpressure based on the priority after DSCP mapping.

```
[~HUAWEI]dcb pfc dscp-mapping enable slot 1
[~HUAWEI]diffserv domain default
[~HUAWEI-dsdomain-default]commit
[~HUAWEI-dsdomain-default]quit
```

Step 4 Configure the buffer alarm function for ports.

```
[~HUAWEI]qos buffer overrun alarm enable
[~HUAWEI]qos buffer overrun threshold 80
[~HUAWEI]commit
[~HUAWEI]quit
```

Step 5 Configure flow control for uplink ports.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The uplink ports refer to the ports on access switches for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other uplink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI]interface 100GE1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]trust dscp
[~HUAWEI-100GE1/0/1]qos drr 0 4
[~HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[~HUAWEI-100GE1/0/1]qos queue 4 drr weight 90
[~HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[~HUAWEI-100GE1/0/1]qos buffer queue 4 shared-threshold dynamic 10
[~HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[~HUAWEI-100GE1/0/1]qos queue 4 wred ecn_100G
[~HUAWEI-100GE1/0/1]qos queue 4 ecn
[~HUAWEI-100GE1/0/1]dcb pfc buffer 4 xoff dynamic 4 hdrm 330
[~HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23_25G_02-dcb-pfc-default]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells   B:bytes   K:kilobytes   M:megabytes   D:dynamic alpha
-------------------------------------------------------------------------------
Interface      Queue    Guaranteed        Xon Xon-Offset       Xoff        Hdrm
-------------------------------------------------------------------------------
100GE1/0/1         4          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/2         4          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/3         4          8(C)       50(C)      20(C)       4(D)      330(C)
-------------------------------------------------------------------------------
25GE1/0/11         4          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
25GE1/0/12         4          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
25GE1/0/13         4          8(C)       50(C)      20(C)     200(C)      180(C)
```

Step 6 Configure flow control for downlink ports.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The downlink ports refer to the ports on access switches for connecting to storage devices.
- Repeat the following operations to configure flow control for other downlink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- If switch ports are connected to LOM NICs, the DSCP flow control information of the LOM NICs is recorded in VLAN packets. In this case, do not run the **trust dscp** command. Otherwise, the obtained flow control information is incorrect. If switch ports are connected to non-LOM NICs, the DSCP flow control information of the NICs is recorded in IP packets. In this case, you must run the **trust dscp** command to obtain the DSCP queue information.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI]interface 25GE1/0/1  #This port is only an example. The actual port prevails.
[~HUAWEI-25GE1/0/1]trust dscp
[*HUAWEI-25GE1/0/1]qos drr 0 4
[*HUAWEI-25GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-25GE1/0/1]qos queue 4 drr weight 90
[*HUAWEI-25GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-25GE1/0/1]qos buffer queue 4 shared-threshold dynamic 10
[*HUAWEI-25GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-25GE1/0/1]qos queue 4 wred ecn_25G
[*HUAWEI-25GE1/0/1]qos queue 4 ecn
[*HUAWEI-25GE1/0/1]dcb pfc buffer 4 xoff dynamic 4 hdrm 250
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A26-27-Y2-dcb-pfc-default]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the larger value between the value
of xon and the value of xoff minus the value of xon-offset.
C:cells   B:bytes    K:kilobytes   M:megabytes D:dynamic alpha
------------------------------------------------------------------------------
Interface      Queue    Guaranteed         Xon Xon-Offset       Xoff        Hdrm
------------------------------------------------------------------------------
25GE1/0/5          4          8(C)       50(C)      20(C)       4(D)      250(C)
                   5          8(C)       50(C)      20(C)     200(C)      180(C)

[~A26-27-Y2-dcb-pfc-default]
```

----End

CE6866 Switch

Step 1 Configure the PFC priority and PFC deadlock detection.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

You are advised to configure **priority 4 turn-off threshold 10** on an access switch.

If the following error information is displayed when you run the **priority 4 5** command, rectify the fault by referring to **5.5.24.2 How Do I Solve the Problem That the Number of PFC-enabled Queues Exceeds the Upper Limit?**.

```
Error:The number of PFC-enabled queues exceeds the upper limit (2).
```

```
[~HUAWEI]dcb pfc
[*HUAWEI-dcb-pfc-default]priority 4 5
[*HUAWEI-dcb-pfc-default]priority 4 turn-off threshold 10
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]dcb pfc deadlock-detect timer 100
[~HUAWEI]dcb pfc deadlock-recovery timer 100
[~HUAWEI]commit
```

Step 2 Configure the buffer alarm function for ports.

```
[~HUAWEI]qos buffer overrun alarm enable
[*HUAWEI]qos buffer overrun threshold 80
[*HUAWEI]commit
```

Step 3 Configure ECN.

```
[~HUAWEI]drop-profile ecn_25G
[*HUAWEI-drop-ecn_25G]ecn buffer-size low-limit 250000 high-limit 700000 discard-percentage 10
[~HUAWEI-drop-ecn_25G]commit
[~HUAWEI-drop-ecn_25G]quit
[~HUAWEI]drop-profile ecn_100G
[*HUAWEI-drop-ecn_100G]ecn buffer-size low-limit 425000 high-limit 750000 discard-percentage 10
[*HUAWEI-drop-ecn_100G]commit
[~HUAWEI-drop-ecn_100G]quit
```

Step 4 Configure flow control for uplink ports.

NOTE

- The uplink ports refer to the ports on access switches for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other uplink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI-100GE1/0/1]interface 100GE1/0/1  #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]trust dscp
[*HUAWEI-100GE1/0/1]qos drr 0 4
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 4 drr weight 90
[*HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-100GE1/0/1]qos buffer queue 4 shared-threshold dynamic 10
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[~HUAWEI-100GE1/0/1]qos queue 4 wred ecn_100G
[*HUAWEI-100GE1/0/1]qos queue 4 ecn
[*HUAWEI-100GE1/0/1]dcb pfc buffer 4 xon static 550 KB xoff static 600 KB
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the values in the **Xon** and **Xoff** columns do not exist for the configured network ports in the table in the command output, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

If the command is successfully executed, an example of the command output is as follows:

```
[~A31-23]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
K:kilobytes
-------------------------------------------------
Interface      Queue          Xon          Xoff
-------------------------------------------------
100GE1/0/1         4        550(K)        600(K)
-------------------------------------------------
100GE1/0/2         4        550(K)        600(K)
-------------------------------------------------
100GE1/0/3         4        550(K)        600(K)
-------------------------------------------------
100GE1/0/4         4        550(K)        600(K)
-------------------------------------------------
```

Step 5 Configure flow control for downlink ports.

NOTE

- The downlink ports refer to the ports on access switches for connecting to storage devices.
- Repeat the following operations to configure flow control for other downlink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- If switch ports are connected to LOM NICs, the DSCP flow control information of the LOM NICs is recorded in VLAN packets. In this case, do not run the **trust dscp** command. Otherwise, the obtained flow control information is incorrect. If switch ports are connected to non-LOM NICs, the DSCP flow control information of the NICs is recorded in IP packets. In this case, you must run the **trust dscp** command to obtain the DSCP queue information.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI-100GE1/0/1]interface 25GE1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-25GE1/0/1]trust dscp
[~HUAWEI-25GE1/0/1]qos drr 0 4
[~HUAWEI-25GE1/0/1]qos queue 0 drr weight 10
[~HUAWEI-25GE1/0/1]qos queue 4 drr weight 90
[~HUAWEI-25GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[~HUAWEI-25GE1/0/1]qos buffer queue 4 shared-threshold dynamic 10
[~HUAWEI-25GE1/0/1]dcb pfc enable mode manual
[~HUAWEI-25GE1/0/1]qos queue 4 wred ecn_25G
[*HUAWEI-25GE1/0/1]qos queue 4 ecn
[*HUAWEI-25GE1/0/1]dcb pfc buffer 4 xon static 550 KB xoff static 600 KB
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the values in the **Xon** and **Xoff** columns do not exist for the configured network ports in the table in the command output, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

If the command is successfully executed, an example of the command output is as follows:

```
[~A31-23]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
K:kilobytes
-------------------------------------------------
Interface      Queue          Xon          Xoff
-------------------------------------------------
25GE1/0/1        4        550(K)        600(K)
-------------------------------------------------
25GE1/0/2        4        550(K)        600(K)
-------------------------------------------------
25GE1/0/3        4        550(K)        600(K)
-------------------------------------------------
```

----End

CE8850 Switch

Step 1 Configure the PFC priority and PFC deadlock detection.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

You are advised to configure **priority 4 turn-off threshold 10** on an access switch.

If the following error information is displayed when you run the **priority 4 5** command, rectify the fault by referring to **5.5.24.2 How Do I Solve the Problem That the Number of PFC-enabled Queues Exceeds the Upper Limit?**.

```
Error:The number of PFC-enabled queues exceeds the upper limit (2).
```

```
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 4 5
[*HUAWEI-dcb-pfc-default]priority 4 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 4 deadlock-recovery time 10
[~HUAWEI-dcb-pfc-default]priority 4 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
[~HUAWEI]commit
[~HUAWEI]quit
```

Step 2 Configure ECN.

```
drop-profile ecn
ecn buffer-size low-limit 425000 high-limit 750000 discard-percentage 10
commit
quit
```

Step 3 Enable PFC to implement backpressure based on the priority after DSCP mapping.

```
[~HUAWEI]dcb pfc dscp-mapping enable slot 1
[~HUAWEI]diffserv domain default
```

 Copyright © Huawei Technologies Co., Ltd.

```
[~HUAWEI-dsdomain-default]commit
[~HUAWEI-dsdomain-default]quit
```

Step 4 Configure the buffer alarm function for ports.

```
[~HUAWEI]qos buffer overrun alarm enable
[~HUAWEI]qos buffer overrun threshold 80
[~HUAWEI]commit
[~HUAWEI]quit
```

Step 5 Configure flow control for ports.

NOTE

- For aggregation switches, the ports refer to the ports on the aggregation switches for connecting to access switches. For access switches, the ports refer to the ports on the access switches for connecting to storage devices and those for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- If switch ports are connected to LOM NICs, the DSCP flow control information of the LOM NICs is recorded in VLAN packets. In this case, do not run the **trust dscp** command. Otherwise, the obtained flow control information is incorrect. If switch ports are connected to non-LOM NICs, the DSCP flow control information of the NICs is recorded in IP packets. In this case, you must run the **trust dscp** command to obtain the DSCP queue information.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI]interface 100GE1/0/1
[~HUAWEI-100GE1/0/1]trust dscp
[~HUAWEI-100GE1/0/1]qos drr 0 4
[~HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[~HUAWEI-100GE1/0/1]qos queue 4 drr weight 90
[~HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[~HUAWEI-100GE1/0/1]qos buffer queue 4 shared-threshold dynamic 10
[~HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[~HUAWEI-100GE1/0/1]qos queue 4 wred ecn
[~HUAWEI-100GE1/0/1]qos queue 4 ecn
[~HUAWEI-100GE1/0/1]dcb pfc buffer 4 xoff dynamic 4 hdrm 330
[~HUAWEI-100GE1/0/1]qos buffer overrun alarm enable
[~HUAWEI-100GE1/0/1]qos buffer overrun threshold 80
[~HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23_25G_02-dcb-pfc-default]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells   B:bytes   K:kilobytes   M:megabytes   D:dynamic alpha
-------------------------------------------------------------------------------
Interface      Queue    Guaranteed        Xon Xon-Offset       Xoff        Hdrm
-------------------------------------------------------------------------------
100GE1/0/1         4          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/2         4          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/3         4          8(C)       50(C)      20(C)       4(D)      330(C)
-------------------------------------------------------------------------------
25GE1/0/11         4          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
25GE1/0/12         4          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
25GE1/0/13         4          8(C)       50(C)      20(C)     200(C)      180(C)
```

----End

CE8851 Switch

Step 1 Configure the PFC priority and PFC deadlock detection.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

You are advised to configure **priority 4 turn-off threshold 10** on an access switch.

If the following error information is displayed when you run the **priority 4 5** command, rectify the fault by referring to **5.5.24.2 How Do I Solve the Problem That the Number of PFC-enabled Queues Exceeds the Upper Limit?**.

```
Error:The number of PFC-enabled queues exceeds the upper limit (2).
```

```
[~HUAWEI]dcb pfc
[*HUAWEI-dcb-pfc-default]priority 4 5
[*HUAWEI-dcb-pfc-default]priority 4 turn-off threshold 10
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]dcb pfc deadlock-detect timer 100
[~HUAWEI]dcb pfc deadlock-recovery timer 100
[~HUAWEI]commit
```

Step 2 Configure ECN.

```
drop-profile ecn
ecn buffer-size low-limit 425000 high-limit 750000 discard-percentage 10
commit
quit
```

Step 3 Configure the buffer alarm function for ports.

 Copyright © Huawei Technologies Co., Ltd.

```
[~HUAWEI]qos buffer overrun alarm enable
[*HUAWEI]qos buffer overrun threshold 80
[*HUAWEI]commit
```

Step 4 Configure flow control for ports.

NOTE

- For aggregation switches, the ports refer to the ports on the aggregation switches for connecting to access switches. For access switches, the ports refer to the ports on the access switches for connecting to storage devices and those for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- If switch ports are connected to LOM NICs, the DSCP flow control information of the LOM NICs is recorded in VLAN packets. In this case, do not run the **trust dscp** command. Otherwise, the obtained flow control information is incorrect. If switch ports are connected to non-LOM NICs, the DSCP flow control information of the NICs is recorded in IP packets. In this case, you must run the **trust dscp** command to obtain the DSCP queue information.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI-100GE1/0/1]interface 100GE1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]trust dscp
[*HUAWEI-100GE1/0/1]qos drr 0 4
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 4 drr weight 90
[*HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-100GE1/0/1]qos buffer queue 4 shared-threshold dynamic 10
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[~HUAWEI-100GE1/0/1]qos queue 4 wred ecn
[*HUAWEI-100GE1/0/1]qos queue 4 ecn
[*HUAWEI-100GE1/0/1]dcb pfc buffer 4 xon static 550 KB xoff static 600 KB
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the values in the **Xon** and **Xoff** columns do not exist for the configured network ports in the table in the command output, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

If the command is successfully executed, an example of the command output is as follows:

```
[~A31-23]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
K:kilobytes
-------------------------------------------------
Interface      Queue          Xon          Xoff
-------------------------------------------------
100GE1/0/1         4        550(K)        600(K)
-------------------------------------------------
100GE1/0/2         4        550(K)        600(K)
-------------------------------------------------
100GE1/0/3         4        550(K)        600(K)
-------------------------------------------------
100GE1/0/4         4        550(K)        600(K)
-------------------------------------------------
```

----End

 Copyright © Huawei Technologies Co., Ltd.

5.5.2.2.2 PCP Flow Control Algorithm

Select the configuration section based on your scenario:

- If the service network uses the NFS over RDMA service, shares network ports with the front-end storage network, and uses CE8850/FM8850/CE8851 switches, complete the configuration by referring to **Configuring Flow Control for a Switch (CE6857E/CE6857F/FM6857E/CE6865/CE6865E/CE8850)** or **Configuring Flow Control for a Switch (CE6866/CE8851)** according to the switch model.
- In other scenarios, complete the configuration by referring to the corresponding section according to the site requirements.

5.5.2.2.2.1 Configuring Flow Control for a Switch (Recommended Configuration of AI Fabric)

Scenarios

If a storage node or DPC compute node uses RoCE NICs, you need to configure the layer 2 Priority-based Flow Control (PFC) protocol and layer 3 Explicit Congestion Notification (ECN) protocol for the ports on the access and aggregation switches.

In this section, the AI Fabric function is enabled for the flow control configuration of the switches. This function aims to provide a network environment with zero packet loss, low latency, and high throughput for RoCE to meet high performance requirements.

This section covers the following switches (applicable to both front- and back-end storage switches):

- **CE6857/CE6857E/CE6857F Switch**
- **CE6865/CE6865E Switch**
- **CE8850 Switch**
- **CE6866 Switch**
- **CE8851 Switch**
- **CE16804/CE16808 Switch**
- **CE6885**
- **CE6855-48XS8CQ**
- **CE8855**

Copyright © Huawei Technologies Co., Ltd.

NOTE

The CE16804 and CE16808 switches support only the AI Fabric function.

This section uses different versions as examples to describe the commands for different switches. The mappings are as follows. If you encounter compatibility issues when running commands for other versions, see the product documentation of the desired switch version. CE series switches: For enterprise users, **click here**. For carrier users, **click here**.

- V200R021C00 is used as an example to describe the commands for the CE6865, CE6865E, CE8850, CE6857, CE6857E, and CE6857F switches.
- V300R021C00 is used as an example to describe the commands for the CE6866 and CE8851 switches.
- V300R021C10 is used as an example to describe the commands for the CE16804 and CE16808 switches.
- V300R023C00 is used as an example to describe the commands for the CE6885, CE6855-48XS8CQ, and CE8855 switches.

Prerequisites

- You have obtained the login information about the switch to be configured.
- The AI Fabric function has been enabled. The required switch versions are as follows:
  - The software version of the CE6857, CE6857E, or CE6857F switch cannot be earlier than V200R021C00. If the version is earlier than V200R021C00, upgrade the switch software by referring to *CloudEngine 8800, 7800, 6800, and 5800 Upgrade Guide* of the desired version.
  - The software version of the CE6865, CE6865E, or CE8850 switch cannot be earlier than V200R019C10. If the version is earlier than V200R019C10, upgrade the switch software by referring to *CloudEngine 8800, 7800, 6800, and 5800 Upgrade Guide* of the desired version.
  - The software version of the CE6866 or CE8851 switch cannot be earlier than V300R021C00. If the version is earlier than V300R021C00, upgrade the switch software by referring to *CloudEngine 8800 and 6800 Upgrade Guide* of the desired version.
  - The software version of the CE16804 or CE16808 switch cannot be earlier than V300R021C10. If the version is earlier than V300R021C10, upgrade the switch software by referring to *CloudEngine 16800 Upgrade Guide* of the desired version.
  - The software version of the CE6885, CE6855-48XS8CQ, or CE8855 switch cannot be earlier than V300R023C00. If the version is earlier than V300R023C00, upgrade the switch software by referring to *CloudEngine 8800 and 6800 Upgrade Guide* of the desired version.
- The AI Fabric function is controlled by a license, which needs to be loaded on the switch. The following describes how to check whether a license takes effect on a switch:
  - CE6865, CE6865E, CE8850, CE6857, CE6857E, or CE6857F: Check whether the command output contains **CE-LIC-LLETH**:
    - If yes, the license of the switch contains the AI Fabric function. Configure flow control by referring to this section.
    - If no, the license of the switch does not contain the AI Fabric function. Configure flow control by referring to **Configuring Flow**

 Copyright © Huawei Technologies Co., Ltd.

Control for a Switch (CE6857E/CE6857F/FM6857E/CE6865/CE6865E/CE8850).

- CE6866, CE8851, CE16804, or CE16808: Check whether the command output contains **CE-LIC-AFRD**:
  - If yes, the license of the switch contains the AI Fabric function. Configure flow control by referring to this section.
  - If no, the license of the switch does not contain the AI Fabric function. Configure flow control by referring to **Configuring Flow Control for a Switch (CE6866/CE8851)**. The CE16804 and CE16808 switches support only the AI Fabric function.
- CE6885, CE6855-48XS8CQ, or CE8855: Check whether the command output contains **CE-LIC-AFRD**:
  - If yes, the license of the switch contains the AI Fabric function. Configure flow control by referring to this section.
  - If no, the license of the switch does not contain the AI Fabric function. Configure flow control by referring to **Configuring Flow Control for a Switch (CE6866/CE8851)**.

```
<CE8850-Leaf1>display license
MainBoard:
 Active License    :
 License state     : Trial
 Revoke ticket     : No ticket
 RD of Huawei Technologies Co., Ltd.
 Product name      : CloudEngine 8800
 Product version   : V200R020
 License Serial No : LIC202106294QOG50
 Creator           : Huawei Technologies Co., Ltd.
 Created Time      : 2021-06-29 20:07:35
 SnS End Date      : --
 ------------------------------------------------------------
 Item name         Item type     Value      Description
 ------------------------------------------------------------
 CE-LIC-VXLAN      Function      YES        CE-LIC-VXLAN
 CE-LIC-FCF-PORT   Resource      512        CE-LIC-FCF-PORT
 CE-LIC-FCF-ALL    Function      YES        CE-LIC-FCF-ALL
 CE-LIC-NPV        Function      YES        CE-LIC-NPV
 CE-LIC-TLM        Function      YES        CE-LIC-TLM
 CE-LIC-LLETH      Function      YES        CE-LIC-LLETH
 CE-LIC-PTP        Function      YES        CE-LIC-PTP
 CE-LIC-FINHA      Function      YES        CE-LIC-FINHA
 CE-LIC-25G01      Resource      1          CE-LIC-25G01
 CE-LIC-40G01      Resource      1          CE-LIC-40G01
 CE-LIC-100G01     Resource      1          CE-LIC-100G01
 License state: Trial. The trial days remains 57 day(s).
 Apply for authentic license before the current license expires.
```

NOTE

Obtain the validity period of the license according to **License state: Trial. The trial days remains 57 day(s)** in the command output.

CE6857/CE6857E/CE6857F Switch

Step 1 Log in to a switch.

Step 2 Enable AI Fabric.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

When AI Fabric is enabled, the VIQ function is enabled by default. You need to restart the switch.

```
<HUAWEI> system-view
[*HUAWEI] low-latency fabric
[*HUAWEI-low-latency-fabric] commit
[~HUAWEI-low-latency-fabric] quit
[~HUAWEI] ai-service
[*HUAWEI-ai-service] ai-ecn
[*HUAWEI-ai-service-ai-ecn] ai-ecn enable
[*HUAWEI-ai-service-ai-ecn] commit
[~HUAWEI-ai-service-ai-ecn] quit
[~HUAWEI-ai-service] quit
[~HUAWEI] quit
```

Step 3 Save the configuration and restart the switch.

```
<HUAWEI> save
Warning: The current configuration will be written to the device. Continue? [Y/N]:y
Info: Save the configuration successfully.
<HUAWEI> reboot
Warning: The system will reboot. Continue? [Y/N]:y
```

Step 4 Configure the PFC priority and PFC deadlock detection.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
<HUAWEI> system-view
# Repeat the following operations to disable other interfaces.
[~HUAWEI] interface 10GE 1/0/1
[~HUAWEI-10GE1/0/1] shutdown
[*HUAWEI-10GE1/0/1] commit
[~HUAWEI-10GE1/0/1] quit
# The following is the global configuration. You do not need to perform the configuration again.
[~HUAWEI] dcb pfc deadlock-detect interval 10
[*HUAWEI] dcb pfc
[*HUAWEI-dcb-pfc-default] priority 0 3
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] priority 3 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default] priority 0 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 0 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] priority 0 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default] commit
[~HUAWEI-dcb-pfc-default] quit
# Repeat the following operations to enable other interfaces.
[~HUAWEI] interface 10GE 1/0/1
[~HUAWEI-10GE1/0/1] undo shutdown
[*HUAWEI-10GE1/0/1] commit
[~HUAWEI-10GE1/0/1] quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used for RoCE (priorities 0, 1, and 3 are used as examples), configure the following information:

 Copyright © Huawei Technologies Co., Ltd.

```
<HUAWEI> system-view
# Repeat the following operations to disable other interfaces.
[~HUAWEI] interface 10GE 1/0/1
[~HUAWEI-10GE1/0/1] shutdown
[*HUAWEI-10GE1/0/1] commit
[~HUAWEI-10GE1/0/1] quit
# The following is the global configuration. You do not need to perform the configuration again.
[~HUAWEI] dcb pfc deadlock-detect interval 10
[*HUAWEI] dcb pfc
[*HUAWEI-dcb-pfc-default] priority 0 1 3
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] priority 3 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is exceeded. If you
need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default] priority 1 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 1 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] priority 1 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is exceeded. If you
need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default] priority 0 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 0 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] priority 0 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is exceeded. If you
need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default] commit
[~HUAWEI-dcb-pfc-default] quit
# Repeat the following operations to enable other interfaces.
[~HUAWEI] interface 10GE 1/0/1
[~HUAWEI-10GE1/0/1] undo shutdown
[*HUAWEI-10GE1/0/1] commit
[~HUAWEI-10GE1/0/1] quit
```

Step 5 Configure flow control for downlink ports.

NOTE

- The downlink ports refer to the ports on access switches for connecting to storage devices.
- Repeat the following operations to configure flow control for other downlink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
[~HUAWEI] interface 10GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-10GE1/0/1]qos drr 0 3
[*HUAWEI-10GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-10GE1/0/1]qos queue 3 drr weight 90
[*HUAWEI-10GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-10GE1/0/1]dcb pfc buffer 0 xoff dynamic 4 hdrm 250
[*HUAWEI-10GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 250
[*HUAWEI-10GE1/0/1]storm suppression broadcast packets 1000
[*HUAWEI-10GE1/0/1]storm suppression multicast packets 200
[*HUAWEI-10GE1/0/1]storm suppression unknown-unicast 1
[*HUAWEI-25GE1/0/1] commit
[~HUAWEI-25GE1/0/1] quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (Priorities 0, 1, and 3 are used as examples and their traffic ratios are 10%, 10%, and 80% respectively. Adjust the ratios according to actual situations), configure the following information:

 Copyright © Huawei Technologies Co., Ltd.

```
[~HUAWEI] interface 10GE 1/0/1
[~HUAWEI-10GE1/0/1]qos drr 0 1 3
[*HUAWEI-10GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-10GE1/0/1]qos queue 1 drr weight 10
[*HUAWEI-10GE1/0/1]qos queue 3 drr weight 80
[*HUAWEI-10GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-10GE1/0/1]dcb pfc buffer 0 xoff dynamic 4 hdrm 250
[*HUAWEI-10GE1/0/1]dcb pfc buffer 1 xoff dynamic 4 hdrm 250
[*HUAWEI-10GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 250
[*HUAWEI-10GE1/0/1]storm suppression broadcast packets 1000
[*HUAWEI-10GE1/0/1]storm suppression multicast packets 200
[*HUAWEI-10GE1/0/1]storm suppression unknown-unicast 1
[*HUAWEI-10GE1/0/1] commit
[~HUAWEI-10GE1/0/1] quit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23-27-CE-100GE1/0/1]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells    B:bytes    K:kilobytes    M:megabytes    D:dynamic alpha
--------------------------------------------------------------------------------
Interface      Queue    Guaranteed         Xon Xon-Offset       Xoff        Hdrm
--------------------------------------------------------------------------------
100GE1/0/1         0          8(C)       50(C)      20(C)       4(D)      330(C)
                   3          8(C)       50(C)      20(C)       4(D)      330(C)
--------------------------------------------------------------------------------
10GE1/0/1          0          8(C)       50(C)      20(C)       4(D)      250(C)
                   3          8(C)       50(C)      20(C)       4(D)      250(C)
--------------------------------------------------------------------------------
[~A23-27-CE-100GE1/0/1]
```

Step 6 Configure flow control for uplink ports.

NOTE

- The uplink ports refer to the ports on access switches for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other uplink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
[~HUAWEI-100GE1/0/1]interface 100GE1/0/1  #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]qos drr 0 3
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 3 drr weight 90
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]dcb pfc buffer 0 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]storm suppression broadcast packets 1000
[*HUAWEI-100GE1/0/1]storm suppression multicast packets 200
[*HUAWEI-100GE1/0/1]storm suppression unknown-unicast 1
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

 Copyright © Huawei Technologies Co., Ltd.

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (Priorities 0, 1, and 3 are used as examples and their traffic ratios are 10%, 10%, and 80% respectively. Adjust the ratios according to actual situations), configure the following information:

```
[~HUAWEI-100GE1/0/1]interface 100GE1/0/1  #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]qos drr 0 1 3
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 1 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 3 drr weight 80
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]dcb pfc buffer 0 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]dcb pfc buffer 1 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]storm suppression broadcast packets 1000
[*HUAWEI-100GE1/0/1]storm suppression multicast packets 200
[*HUAWEI-100GE1/0/1]storm suppression unknown-unicast 1
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23-27-CE-100GE1/0/1]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells   B:bytes   K:kilobytes   M:megabytes   D:dynamic alpha
--------------------------------------------------------------------------------
Interface      Queue    Guaranteed         Xon Xon-Offset       Xoff        Hdrm
--------------------------------------------------------------------------------
100GE1/0/1         0          8(C)       50(C)      20(C)       4(D)      330(C)
                   3          8(C)       50(C)      20(C)       4(D)      330(C)
--------------------------------------------------------------------------------
10GE1/0/1          0          8(C)       50(C)      20(C)       4(D)      250(C)
                   3          8(C)       50(C)      20(C)       4(D)      250(C)
--------------------------------------------------------------------------------
[~A23-27-CE-100GE1/0/1]
```

The following step is performed on a Layer 2 network with an aggregation switch.

Step 7 Configure static ECN on the peer-link interface (configured on the peer-link interface when CE6857/CE6857E/CE6857F switches function as access switches and form M-LAG).

```
[~HUAWEI]drop-profile ecn_100G
[*HUAWEI-drop-ecn_100G]ecn buffer-size low-limit 425000 high-limit 750000 discard-percentage 10
[*HUAWEI-drop-ecn_100G]commit
[~HUAWEI-drop-drop100G] interface 100GE1/0/1
[~HUAWEI-100GE1/0/1]qos queue 4 wred ecn_100G
[*HUAWEI-100GE1/0/1] qos queue 4 ecn
[*HUAWEI-100GE1/0/1] commit
[~HUAWEI-100GE1/0/1] quit
```

----End

CE6865/CE6865E Switch

Step 1 Log in to a switch.

Step 2 Enable AI Fabric.

NOTE

When AI Fabric is enabled, the VIQ function is enabled by default. You need to restart the switch.

```
<HUAWEI> system-view
[*HUAWEI] low-latency fabric
[*HUAWEI-low-latency-fabric] undo qos dynamic-ecn-threshold enable
[*HUAWEI-low-latency-fabric] commit
[~HUAWEI-low-latency-fabric] quit
[~HUAWEI] ai-service
[*HUAWEI-ai-service] ai-ecn
[*HUAWEI-ai-service-ai-ecn] ai-ecn enable
[*HUAWEI-ai-service-ai-ecn] commit
[~HUAWEI-ai-service-ai-ecn] quit
[~HUAWEI-ai-service] quit
[~HUAWEI] quit
```

Step 3 Save the configuration and restart the switch.

```
<HUAWEI> save
Warning: The current configuration will be written to the device. Continue? [Y/N]:y
Info: Save the configuration successfully.
<HUAWEI> reboot
Warning: The system will reboot. Continue? [Y/N]:y
```

Step 4 Configure the PFC priority and PFC deadlock detection.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
<HUAWEI> system-view
[~HUAWEI] interface 25GE 1/0/1
[~HUAWEI-25GE1/0/1] shutdown
[*HUAWEI-25GE1/0/1] commit
[~HUAWEI-25GE1/0/1] quit
[~HUAWEI] dcb pfc deadlock-detect interval 10
[*HUAWEI] dcb pfc
[*HUAWEI-dcb-pfc-default] priority 0 3
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] priority 0 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 0 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] commit
[~HUAWEI-dcb-pfc-default] quit
[~HUAWEI] interface 25ge 1/0/1
[~HUAWEI-25GE1/0/1] undo shutdown
[*HUAWEI-25GE1/0/1] commit
[~HUAWEI-25GE1/0/1] quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used for RoCE (priorities 0, 1, and 3 are used as examples), configure the following information:

```
<HUAWEI> system-view
[~HUAWEI] interface 25GE 1/0/1
[~HUAWEI-25GE1/0/1] shutdown
[*HUAWEI-25GE1/0/1] commit
[~HUAWEI-25GE1/0/1] quit
[~HUAWEI] dcb pfc deadlock-detect interval 10
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI] dcb pfc
[*HUAWEI-dcb-pfc-default] priority 0 1 3
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] priority 1 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 1 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] priority 0 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 0 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] commit
[~HUAWEI-dcb-pfc-default] quit
[~HUAWEI] interface 25ge 1/0/1
[~HUAWEI-25GE1/0/1] undo shutdown
[*HUAWEI-25GE1/0/1] commit
[~HUAWEI-25GE1/0/1] quit
```

Step 5 Configure flow control for downlink ports.

NOTE

- The downlink ports refer to the ports on access switches for connecting to storage devices.
- Repeat the following operations to configure flow control for other downlink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
[~HUAWEI]
[~HUAWEI] interface 25GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-25GE1/0/1] dcb pfc enable mode manual
[*HUAWEI-25GE1/0/1] qos drr 0 3
[*HUAWEI-25GE1/0/1] qos queue 0 drr weight 10
[*HUAWEI-25GE1/0/1] qos queue 3 drr weight 90
[*HUAWEI-25GE1/0/1] commit
[~HUAWEI-25GE1/0/1] quit
[~HUAWEI]
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (Priorities 0, 1, and 3 are used as examples and their traffic ratios are 10%, 10%, and 80% respectively. Adjust the ratios according to actual situations), configure the following information:

```
[~HUAWEI]
[~HUAWEI] interface 25GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-25GE1/0/1] dcb pfc enable mode manual
[*HUAWEI-25GE1/0/1] qos drr 0 1 3
[*HUAWEI-25GE1/0/1] qos queue 0 drr weight 10
[*HUAWEI-25GE1/0/1] qos queue 1 drr weight 10
[*HUAWEI-25GE1/0/1] qos queue 3 drr weight 80
[*HUAWEI-25GE1/0/1] commit
[~HUAWEI-25GE1/0/1] quit
[~HUAWEI]
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A26-27-Y2]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the larger value between the value
of xon and the value of xoff minus the value of xon-offset.
C:cells    B:bytes    K:kilobytes    M:megabytes D:dynamic alpha
-------------------------------------------------------------------------------
Interface      Queue    Guaranteed         Xon Xon-Offset       Xoff        Hdrm
-------------------------------------------------------------------------------
25GE1/0/5          3          8(C)       50(C)      20(C)       4(D)      250(C)
-------------------------------------------------------------------------------
[~A26-27-Y2]
[~A26-27-Y2]
[~A26-27-Y2]
```

Step 6 Configure flow control for uplink ports.

NOTE

- The uplink ports refer to the ports on access switches for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other uplink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
[~HUAWEI]
[~HUAWEI] interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1] dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1] qos drr 0 3
[*HUAWEI-100GE1/0/1] qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1] qos queue 3 drr weight 90
[*HUAWEI-100GE1/0/1] commit
[~HUAWEI-100GE1/0/1] quit
[~HUAWEI]
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (Priorities 0, 1, and 3 are used as examples and their traffic ratios are 10%, 10%, and 80% respectively. Adjust the ratios according to actual situations), configure the following information:

```
[~HUAWEI]
[~HUAWEI] interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1] dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1] qos drr 0 1 3
[*HUAWEI-100GE1/0/1] qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1] qos queue 1 drr weight 10
[*HUAWEI-100GE1/0/1] qos queue 3 drr weight 80
[*HUAWEI-100GE1/0/1] commit
[~HUAWEI-100GE1/0/1] quit
[~HUAWEI]
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23_25G_02-100GE1/0/3]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells    B:bytes    K:kilobytes    M:megabytes    D:dynamic alpha
-------------------------------------------------------------------------------
Interface      Queue    Guaranteed        Xon Xon-Offset       Xoff        Hdrm
-------------------------------------------------------------------------------
100GE1/0/1         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/2         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/3         3         8(C)       50(C)      20(C)       4(D)      330(C)
-------------------------------------------------------------------------------
25GE1/0/11         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
25GE1/0/12         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
```

----End

CE8850 Switch

Step 1 Log in to a switch.

Step 2 Enable AI Fabric.

NOTE

When AI Fabric is enabled, the VIQ function is enabled by default. You need to restart the switch.

```
<HUAWEI> system-view
[*HUAWEI] low-latency fabric
[*HUAWEI-low-latency-fabric] undo qos dynamic-ecn-threshold enable
[*HUAWEI-low-latency-fabric] commit
[~HUAWEI-low-latency-fabric] quit
[~HUAWEI] ai-service
[*HUAWEI-ai-service] ai-ecn
[*HUAWEI-ai-service-ai-ecn] ai-ecn enable
[*HUAWEI-ai-service-ai-ecn] commit
[~HUAWEI-ai-service-ai-ecn] quit
[~HUAWEI-ai-service] quit
[~HUAWEI] quit
```

Step 3 Save the configuration and restart the switch.

```
<HUAWEI> save
Warning: The current configuration will be written to the device. Continue? [Y/N]:y
Info: Save the configuration successfully.
<HUAWEI> reboot
Warning: The system will reboot. Continue? [Y/N]:y
```

Step 4 Configure the PFC priority and PFC deadlock detection.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
<HUAWEI> system-view
[~HUAWEI] interface 100ge 1/0/1
[~HUAWEI-100GE1/0/1] shutdown
[*HUAWEI-100GE1/0/1] commit
[~HUAWEI-100GE1/0/1] quit
[~HUAWEI] dcb pfc deadlock-detect interval 10
[*HUAWEI] dcb pfc
[*HUAWEI-dcb-pfc-default] priority 0 3
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] priority 0 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 0 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] commit
[~HUAWEI-dcb-pfc-default] quit
[~HUAWEI] interface 100ge 1/0/1
[~HUAWEI-100GE1/0/1] undo shutdown
[*HUAWEI-100GE1/0/1] commit
[~HUAWEI-100GE1/0/1] quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used for RoCE (priorities 0, 1, and 3 are used as examples), configure the following information:

```
<HUAWEI> system-view
[~HUAWEI] interface 100ge 1/0/1
[~HUAWEI-100GE1/0/1] shutdown
[*HUAWEI-100GE1/0/1] commit
[~HUAWEI-100GE1/0/1] quit
[~HUAWEI] dcb pfc deadlock-detect interval 10
[*HUAWEI] dcb pfc
[*HUAWEI-dcb-pfc-default] priority 0 1 3
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] priority 1 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 1 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] priority 0 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 0 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] commit
[~HUAWEI-dcb-pfc-default] quit
[~HUAWEI] interface 100ge 1/0/1
[~HUAWEI-100GE1/0/1] undo shutdown
[*HUAWEI-100GE1/0/1] commit
[~HUAWEI-100GE1/0/1] quit
```

Step 5 Configure flow control for ports.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- For aggregation switches, the ports refer to the ports on the aggregation switches for connecting to access switches. For access switches, the ports refer to the ports on the access switches for connecting to storage devices and those for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
[~HUAWEI]
[~HUAWEI] interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1] dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1] qos drr 0 3
[*HUAWEI-100GE1/0/1] qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1] qos queue 3 drr weight 90
[*HUAWEI-100GE1/0/1] commit
[~HUAWEI-100GE1/0/1] quit
[~HUAWEI]
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (Priorities 0, 1, and 3 are used as examples and their traffic ratios are 10%, 10%, and 80% respectively. Adjust the ratios according to actual situations), configure the following information:

```
[~HUAWEI]
[~HUAWEI] interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1] dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1] qos drr 0 1 3
[*HUAWEI-100GE1/0/1] qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1] qos queue 1 drr weight 10
[*HUAWEI-100GE1/0/1] qos queue 3 drr weight 80
[*HUAWEI-100GE1/0/1] commit
[~HUAWEI-100GE1/0/1] quit
[~HUAWEI]
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23_25G_02-100GE1/0/3]
[~A23_25G_02-100GE1/0/3]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells   B:bytes   K:kilobytes   M:megabytes   D:dynamic alpha
-------------------------------------------------------------------------------
Interface      Queue    Guaranteed        Xon Xon-Offset       Xoff        Hdrm
-------------------------------------------------------------------------------
100GE1/0/1         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/2         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/3         3         8(C)       50(C)      20(C)       4(D)      330(C)
-------------------------------------------------------------------------------
25GE1/0/11         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
25GE1/0/12         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
```

----End

CE6866 Switch

Step 1 Log in to a switch.

Step 2 Configure AI ECN.

```
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]ai-service
[~HUAWEI-ai-service]ai-ecn
[~HUAWEI-ai-service-ai-ecn]assign queue 3
[*HUAWEI-ai-service-ai-ecn]ai-ecn enable
[*HUAWEI-ai-service-ai-ecn]quit
[*HUAWEI-ai-service]quit
[*HUAWEI]commit
```

Step 3 Configure the PFC priority and PFC deadlock detection.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

You are advised to configure **priority 3 turn-off threshold 10** on an access switch.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]dcb pfc deadlock-detect timer 100
[~HUAWEI]dcb pfc deadlock-recovery timer 100
[~HUAWEI]dcb pfc deadlock recovery-behavior discard slot 1
[~HUAWEI]dcb pfc
[*HUAWEI-dcb-pfc-default]priority 3
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 3 is used for RoCE (priorities 1 and 3 are used as examples), configure the following information:

```
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]dcb pfc deadlock-detect timer 100
[~HUAWEI]dcb pfc deadlock-recovery timer 100
[~HUAWEI]dcb pfc deadlock recovery-behavior discard slot 1
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 1 3
[*HUAWEI-dcb-pfc-default]priority 1 turn-off threshold 10
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
```

Step 4 Configure flow control for ports.

NOTE

- For aggregation switches, the ports refer to the ports on the aggregation switches for connecting to access switches. For access switches, the ports refer to the ports on the access switches for connecting to storage devices and those for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
[~HUAWEI]interface 25GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-25GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[~HUAWEI-25GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[~HUAWEI-25GE1/0/1]qos drr 0 3
[~HUAWEI-25GE1/0/1]qos queue 0 drr weight 10
[~HUAWEI-25GE1/0/1]qos queue 3 drr weight 90
[~HUAWEI-25GE1/0/1]dcb pfc buffer 3 xon static 550 KB xoff static 600 KB
[~HUAWEI-25GE1/0/1]dcb pfc enable mode manual
[~HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (Priorities 0, 1, and 3 are used as examples and their traffic ratios are 10%, 10%, and 80% respectively. Adjust the ratios according to actual situations), configure the following information:

```
[~HUAWEI]interface 25GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-25GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[~HUAWEI-25GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[~HUAWEI-25GE1/0/1]qos drr 0 1 3
[*HUAWEI-25GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-25GE1/0/1]qos queue 1 drr weight 10
[*HUAWEI-25GE1/0/1]qos queue 3 drr weight 80
[*HUAWEI-25GE1/0/1]dcb pfc buffer 3 xon static 550 KB xoff static 600 KB
[*HUAWEI-25GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the values in the **Xon** and **Xoff** columns do not exist for the configured network ports in the table in the command output, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

If the command is successfully executed, an example of the command output is as follows:

```
[~A31-23]display dcb pfc buffer
Xon:       PFC backpressure stop threshold
Xoff:      PFC backpressure threshold
K:kilobytes
-------------------------------------------------------
Interface     Queue          Xon          Xoff
-------------------------------------------------------
25GE1/0/1         3       550(K)        600(K)
-------------------------------------------------------
25GE1/0/2         3       550(K)        600(K)
-------------------------------------------------------
25GE1/0/3         3       550(K)        600(K)
-------------------------------------------------------
```

----End

CE8851 Switch

NOTE

The configuration of the CE8851 switch functioning as an aggregation switch is the same as that of an access switch.

Step 1 Log in to a switch.

Step 2 Configure AI ECN.

```
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]ai-service
[~HUAWEI-ai-service]ai-ecn
[~HUAWEI-ai-service-ai-ecn]assign queue 3
[*HUAWEI-ai-service-ai-ecn]ai-ecn enable
[*HUAWEI-ai-service-ai-ecn]quit
[*HUAWEI-ai-service]quit
[*HUAWEI]commit
```

Step 3 Configure the PFC priority and PFC deadlock detection.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

You are advised to configure **priority 3 turn-off threshold 10** on an access switch.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]dcb pfc deadlock-detect timer 100
[~HUAWEI]dcb pfc deadlock-recovery timer 100
[~HUAWEI]dcb pfc deadlock recovery-behavior discard slot 1
[~HUAWEI]dcb pfc
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-dcb-pfc-default]priority 3
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 3 is used for RoCE (priorities 1 and 3 are used as examples), configure the following information:

```
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]dcb pfc deadlock-detect timer 100
[~HUAWEI]dcb pfc deadlock-recovery timer 100
[~HUAWEI]dcb pfc deadlock recovery-behavior discard slot 1
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 1 3
[*HUAWEI-dcb-pfc-default]priority 1 turn-off threshold 10
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
```

Step 4 Configure flow control for ports.

NOTE

- For aggregation switches, the ports refer to the ports on the aggregation switches for connecting to access switches. For access switches, the ports refer to the ports on the access switches for connecting to storage devices and those for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
[~HUAWEI]interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[~HUAWEI-100GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[~HUAWEI-100GE1/0/1]qos drr 0 3
[~HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[~HUAWEI-100GE1/0/1]qos queue 3 drr weight 90
[~HUAWEI-100GE1/0/1]dcb pfc buffer 3 xon static 550 KB xoff static 600 KB
[~HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[~HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (Priorities 0, 1, and 3 are used as examples and their traffic ratios are 10%, 10%, and 80% respectively. Adjust the ratios according to actual situations), configure the following information:

```
[~HUAWEI]interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[~HUAWEI-100GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[~HUAWEI-100GE1/0/1]qos drr 0 1 3
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 1 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 3 drr weight 80
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xon static 550 KB xoff static 600 KB
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the values in the **Xon** and **Xoff** columns do not exist for the configured network ports in the table in the command output, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

If the command is successfully executed, an example of the command output is as follows:

```
[~A31-23]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
K:kilobytes
-----------------------------------------------------
Interface      Queue          Xon          Xoff
-----------------------------------------------------
100GE1/0/1         3        550(K)        600(K)
-----------------------------------------------------
100GE1/0/2         3        550(K)        600(K)
-----------------------------------------------------
100GE1/0/3         3        550(K)        600(K)
-----------------------------------------------------
100GE1/0/4         3        550(K)        600(K)
-----------------------------------------------------
```

----End

CE16804/CE16808 Switch

NOTE

The configuration of the CE16804/CE16808 switch functioning as an aggregation switch is the same as that of an access switch.

Step 1 Log in to a switch.

Step 2 Configure AI ECN.

```
[~HUAWEI]ai-service
[~HUAWEI-ai-service]ai-ecn
[*HUAWEI-ai-service-ai-ecn]ai-ecn enable
[*HUAWEI-ai-service-ai-ecn]assign queue 3
[*HUAWEI-ai-service-ai-ecn]quit
[*HUAWEI-ai-service]quit
[*HUAWEI]commit
```

Step 3 Configure DCB PFC.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

You are advised to configure **priority 3 turn-off threshold 10** on an access switch.

```
<HUAWEI>system-view
[~HUAWEI]dcb pfc
[*HUAWEI-dcb-pfc-default]priority 0 3
[*HUAWEI-dcb-pfc-default]priority 0 turn-off threshold 10
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
[*HUAWEI-dcb-pfc-default]commit
[*HUAWEI-dcb-pfc-default]quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 4 Enable PFC deadlock monitoring.

```
<HUAWEI>system-view
[~HUAWEI]dcb pfc deadlock-detect timer 100
[~HUAWEI]dcb pfc deadlock-recovery timer 100
[~HUAWEI]dcb pfc deadlock recovery-behavior discard slot slot-id
[~HUAWEI]commit
```

NOTE

Description of the *slot-id* parameter:

slot-id indicates the slot ID of the specified switch. The value is an integer and can be determined according to the port name. For example, *slot-id* of port 100GE4/0/1 is **4**, and *slot-id* of port 100GE8/0/1 is **8**. If multiple slots are used, for example, slots 4 and 8 are used at the same time, run the following commands for reference:

```
dcb pfc deadlock recovery-behavior discard slot 4
dcb pfc deadlock recovery-behavior discard slot 8
```

Step 5 Configure the switch to generate an alarm when the queue buffer exceeds the threshold.

```
[~HUAWEI]qos buffer overrun alarm enable
[*HUAWEI]qos buffer overrun threshold 80
[*HUAWEI]commit
[~HUAWEI]quit
```

Step 6 Configure flow control for ports.

NOTE

- For aggregation switches, the ports refer to the ports on the aggregation switches for connecting to access switches. For access switches, the ports refer to the ports on the access switches for connecting to storage devices and those for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
# The following uses a 25GE port as an example. The configuration also applies to 100GE ports.
[~HUAWEI-25GE1/0/1]interface 25GE1/0/1   #This port is only an example. The actual port prevails.
[*HUAWEI-25GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-25GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[*HUAWEI-25GE1/0/1]qos drr 0 3
[*HUAWEI-25GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-25GE1/0/1]qos queue 3 drr weight 90
[*HUAWEI-25GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-25GE1/0/1]dcb pfc buffer 0 xon static 100 kbytes xoff static 125 kbyte
[*HUAWEI-25GE1/0/1]dcb pfc buffer 3 xon static 100 kbytes xoff static 125 kbytes
[*HUAWEI-25GE1/0/1]storm suppression broadcast packets 1000
[*HUAWEI-25GE1/0/1]storm suppression multicast packets 200
[*HUAWEI-25GE1/0/1]storm suppression unknown-unicast packets 200
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the values in the **Xon** and **Xoff** columns do not exist for the configured network ports in the table in the command output, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

If the command is successfully executed, an example of the command output is as follows:

```
[~A31-23]display dcb pfc buffer
Xon:       PFC backpressure stop threshold
Xoff:      PFC backpressure threshold
K:kilobytes
-----------------------------------------------------
Interface     Queue          Xon          Xoff
-----------------------------------------------------
25GE1/0/0         0       100(K)       125(K)
                  3       100(K)       125(K)
-----------------------------------------------------
25GE1/0/1         0       100(K)       125(K)
                  3       100(K)       125(K)
-----------------------------------------------------
25GE1/0/2         0       100(K)       125(K)
                  3       100(K)       125(K)
-----------------------------------------------------
```

----End

CE6885

Step 1 Configure the PFC priority and PFC deadlock detection.

```
[~HUAWEI] qos buffer headroom-pool size 6 mbytes slot 1
[*HUAWEI] commit
[~HUAWEI] dcb pfc
[~HUAWEI-dcb-pfc-default] priority 2 3
[*HUAWEI-dcb-pfc-default] priority 3 turn-off threshold 10
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] commit
[~HUAWEI-dcb-pfc-default] quit
[~HUAWEI] dcb pfc deadlock-detect interval 10
[*HUAWEI] dcb pfc deadlock recovery-behavior forwarding slot 1
[*HUAWEI] commit
[~HUAWEI] quit
```

Step 2 Enable AI Fabric.

```
[~HUAWEI] ai-service
[*HUAWEI-ai-service] ai-ecn
[*HUAWEI-ai-service-ai-ecn] ai-ecn enable
[*HUAWEI-ai-service-ai-ecn] assign queue 3 model ai_ecn_distributedfilestorage
[*HUAWEI-ai-service-ai-ecn] commit
[~HUAWEI-ai-service-ai-ecn] quit
[~HUAWEI-ai-service] quit
```

Step 3 Enable PFC to implement backpressure based on the priority after DSCP mapping.

```
[~HUAWEI] dcb pfc dscp-mapping enable slot 1
[*HUAWEI] diffserv domain default
[*HUAWEI-dsdomain-default] commit
[~HUAWEI-dsdomain-default] quit
```

Step 4 Configure the buffer alarm function for ports.

```
[~HUAWEI] qos buffer overrun alarm enable
[*HUAWEI] qos buffer overrun threshold 80
[*HUAWEI] commit
[~HUAWEI] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure flow control for downlink ports.

NOTE

- For aggregation switches, the ports refer to the ports on the aggregation switches for connecting to access switches. For access switches, the ports refer to the ports on the access switches for connecting to storage devices and those for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- If switch ports are connected to LOM NICs, the DSCP flow control information of the LOM NICs is recorded in VLAN packets. In this case, do not run the **trust dscp** command. Otherwise, the obtained flow control information is incorrect. If switch ports are connected to non-LOM NICs, the DSCP flow control information of the NICs is recorded in IP packets. In this case, you must run the **trust dscp** command to obtain the DSCP queue information.
- The **trust dscp** command is configured only on the access switch port connected to a storage device.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI] interface 25GE 1/0/1
[~HUAWEI-25GE1/0/1] dcb pfc buffer 3 guaranteed 5 kbytes
[*HUAWEI-25GE1/0/1] dcb pfc buffer 3 hdrm 512 kbytes
[*HUAWEI-25GE1/0/1] dcb pfc buffer 3 xoff dynamic 4 xon offset 6 kbytes
[*HUAWEI-25GE1/0/1] qos buffer queue 3 shared-threshold static 33280 kbytes
[*HUAWEI-25GE1/0/1] qos drr 0 3
[*HUAWEI-25GE1/0/1] qos queue 0 drr weight 8
[*HUAWEI-25GE1/0/1] qos queue 3 drr weight 90
[*HUAWEI-25GE1/0/1] qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-25GE1/0/1] dcb pfc enable mode manual
[*HUAWEI-25GE1/0/1] storm suppression broadcast packets 1000
[*HUAWEI-25GE1/0/1] storm suppression multicast packets 1000
[*HUAWEI-25GE1/0/1] storm suppression unknown-unicast packets 200
[*HUAWEI-25GE1/0/1] qos queue 0 shaping cir 64 kbps pir 25 gbps
[*HUAWEI-25GE1/0/1] qos queue 3 shaping cir 64 kbps pir 25 gbps
[*HUAWEI-25GE1/0/1] commit
[~HUAWEI-25GE1/0/1] quit
```

Step 6 Repeat **Step 5** to configure flow control for each group of ports (including 25GE1/0/2, 25GE1/0/3, and 25GE1/0/4).

Step 7 Configure flow control for peer-link ports.

```
[~HUAWEI]interface 100GE1/0/1
[~HUAWEI-100GE1/0/1]qos buffer queue 3 shared-threshold static 33280 kbytes
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 guaranteed 5 kbytes
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 xon offset 6 kbytes
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 hdrm 512 kbytes
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
...#Repeat the preceding operations to configure flow control for each peer-link port (including 100GE1/0/2).
[*HUAWEI-100GE1/0/2]commit
[~HUAWEI-100GE1/0/2]quit
```

----End

CE6855-48XS8CQ

Step 1 Configure the PFC priority and PFC deadlock detection.

```
[~HUAWEI] qos buffer headroom-pool size 6 mbytes slot 1
[*HUAWEI] commit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[~HUAWEI] dcb pfc
[~HUAWEI-dcb-pfc-default] priority 2 3
[*HUAWEI-dcb-pfc-default] priority 3 turn-off threshold 10
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default] priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default] commit
[~HUAWEI-dcb-pfc-default] quit
[~HUAWEI] dcb pfc deadlock-detect interval 10
[*HUAWEI] dcb pfc deadlock recovery-behavior forwarding slot 1
[*HUAWEI] commit
```

Step 2 Enable AI Fabric.

```
[~HUAWEI] ai-service
[*HUAWEI-ai-service] ai-ecn
[*HUAWEI-ai-service-ai-ecn] ai-ecn enable
[*HUAWEI-ai-service-ai-ecn] assign queue 3 model ai_ecn_distributedfilestorage
[*HUAWEI-ai-service-ai-ecn] commit
[~HUAWEI-ai-service-ai-ecn] quit
[~HUAWEI-ai-service] quit
```

Step 3 Enable PFC to implement backpressure based on the priority after DSCP mapping.

```
[~HUAWEI] dcb pfc dscp-mapping enable slot 1
[*HUAWEI] diffserv domain default
[*HUAWEI-dsdomain-default] commit
[~HUAWEI-dsdomain-default] quit
```

Step 4 Configure the buffer alarm function for ports.

```
[~HUAWEI] qos buffer overrun alarm enable
[*HUAWEI] qos buffer overrun threshold 80
[*HUAWEI] commit
```

Step 5 Configure flow control for downlink ports.

NOTE

- For aggregation switches, the ports refer to the ports on the aggregation switches for connecting to access switches. For access switches, the ports refer to the ports on the access switches for connecting to storage devices and those for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- If switch ports are connected to LOM NICs, the DSCP flow control information of the LOM NICs is recorded in VLAN packets. In this case, do not run the **trust dscp** command. Otherwise, the obtained flow control information is incorrect. If switch ports are connected to non-LOM NICs, the DSCP flow control information of the NICs is recorded in IP packets. In this case, you must run the **trust dscp** command to obtain the DSCP queue information.
- The **trust dscp** command is configured only on the access switch port connected to a storage device.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI] interface 10GE 1/0/1
[~HUAWEI-10GE1/0/1] dcb pfc buffer 3 guaranteed 5 kbytes
[*HUAWEI-10GE1/0/1] dcb pfc buffer 3 hdrm 512 kbytes
[*HUAWEI-10GE1/0/1] dcb pfc buffer 3 xoff dynamic 4 xon offset 6 kbytes
[*HUAWEI-10GE1/0/1] qos buffer queue 3 shared-threshold static 33280 kbytes
[*HUAWEI-10GE1/0/1] qos drr 0 3
[*HUAWEI-10GE1/0/1] qos queue 0 drr weight 8
[*HUAWEI-10GE1/0/1] qos queue 3 drr weight 90
[*HUAWEI-10GE1/0/1] qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-10GE1/0/1] dcb pfc enable mode manual
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-10GE1/0/1] storm suppression broadcast packets 1000
[*HUAWEI-10GE1/0/1] storm suppression multicast packets 1000
[*HUAWEI-10GE1/0/1] storm suppression unknown-unicast packets 200
[*HUAWEI-10GE1/0/1] qos queue 0 shaping cir 64 kbps pir 10 gbps
[*HUAWEI-10GE1/0/1] qos queue 3 shaping cir 64 kbps pir 10 gbps
[*HUAWEI-10GE1/0/1] commit
[~HUAWEI-10GE1/0/1] quit
```

Step 6 Repeat **Step 5** to configure flow control for each group of ports (including 10GE1/0/2, 10GE1/0/3, and 10GE1/0/4).

Step 7 Configure flow control for peer-link ports.

```
[~HUAWEI]interface 100GE1/0/1
[~HUAWEI-100GE1/0/1]qos buffer queue 3 shared-threshold static 33280 kbytes
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 guaranteed 5 kbytes
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 xon offset 6 kbytes
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 hdrm 512 kbytes
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
...#Repeat the preceding operations to configure flow control for each peer-link port (including 100GE1/0/2).
[*HUAWEI-100GE1/0/2]commit
[~HUAWEI-100GE1/0/2]quit
```

----End

CE8855

Step 1 Configure the PFC priority and PFC deadlock detection.

```
[~HUAWEI]qos buffer headroom-pool size 6 mbytes slot 1
[*HUAWEI]commit
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 2 3
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
[*HUAWEI]dcb pfc deadlock recovery-behavior forwarding slot 1
[*HUAWEI]commit
[~HUAWEI]quit
```

Step 2 Enable AI Fabric.

```
[~HUAWEI]ai-service
[*HUAWEI-ai-service]ai-ecn
[*HUAWEI-ai-service-ai-ecn]ai-ecn enable
[*HUAWEI-ai-service-ai-ecn]assign queue 3 model ai_ecn_distributedfilestorage
[*HUAWEI-ai-service-ai-ecn]commit
[~HUAWEI-ai-service-ai-ecn]quit
[~HUAWEI-ai-service]quit
```

Step 3 Enable PFC to implement backpressure based on the priority after DSCP mapping.

```
[~HUAWEI]dcb pfc dscp-mapping enable slot 1
[*HUAWEI]diffserv domain default
[*HUAWEI-dsdomain-default]commit
[~HUAWEI-dsdomain-default]quit
```

Step 4 Configure the buffer alarm function for ports.

```
[~HUAWEI]qos buffer overrun alarm enable
[*HUAWEI]qos buffer overrun threshold 80
[*HUAWEI]commit
[~HUAWEI]quit
```

Step 5 Configure flow control for downlink ports.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- For aggregation switches, the ports refer to the ports on the aggregation switches for connecting to access switches. For access switches, the ports refer to the ports on the access switches for connecting to storage devices and those for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- If switch ports are connected to LOM NICs, the DSCP flow control information of the LOM NICs is recorded in VLAN packets. In this case, do not run the **trust dscp** command. Otherwise, the obtained flow control information is incorrect. If switch ports are connected to non-LOM NICs, the DSCP flow control information of the NICs is recorded in IP packets. In this case, you must run the **trust dscp** command to obtain the DSCP queue information.
- The **trust dscp** command is configured only on the access switch port connected to a storage device.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI]interface 100GE1/0/1
[~HUAWEI-100GE1/0/1]dcb pfc buffer 3 guaranteed 5 kbytes
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 hdrm 512 kbytes
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 xon offset 6 kbytes
[*HUAWEI-100GE1/0/1]qos buffer queue 3 shared-threshold static 33280 kbytes
```

```
[*HUAWEI-100GE1/0/1]qos drr 0 3
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 8
[*HUAWEI-100GE1/0/1]qos queue 3 drr weight 90
[*HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]storm suppression broadcast packets 1000
[*HUAWEI-100GE1/0/1]storm suppression multicast packets 1000
[*HUAWEI-100GE1/0/1]storm suppression unknown-unicast packets 200
[*HUAWEI-100GE1/0/1]qos queue 0 shaping cir 64 kbps pir 100 gbps
[*HUAWEI-100GE1/0/1]qos queue 3 shaping cir 64 kbps pir 100 gbps
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

Step 6 Repeat **Step 5** to configure flow control for each group of ports (including 100GE1/0/2, 100GE1/0/3, and 100GE1/0/4).

Step 7 Configure flow control for peer-link ports.

```
[~HUAWEI]interface 100GE1/0/35
[~HUAWEI-100GE1/0/35]qos buffer queue 3 shared-threshold static 33280 kbytes
[*HUAWEI-100GE1/0/35]dcb pfc buffer 3 guaranteed 5 kbytes
[*HUAWEI-100GE1/0/35]dcb pfc buffer 3 xoff dynamic 4 xon offset 6 kbytes
[*HUAWEI-100GE1/0/35]dcb pfc buffer 3 hdrm 512 kbytes
[*HUAWEI-100GE1/0/35]dcb pfc enable mode manual
...#Repeat the preceding operations to configure flow control for each peer-link port (including 100GE1/0/36).
[*HUAWEI-100GE1/0/36]commit
[~HUAWEI-100GE1/0/36]quit
```

----End

 Copyright © Huawei Technologies Co., Ltd.

5.5.2.2.2.2 Configuring Flow Control for a Switch (CE6857E/CE6857F/FM6857E/CE6865/CE6865E/CE8850)

Scenarios

If a storage node or DPC compute node uses RoCE NICs, you need to configure the layer 2 Priority-based Flow Control (PFC) protocol and layer 3 Explicit Congestion Notification (ECN) protocol for the ports on the access and aggregation switches.

For details about how to configure front-end and back-end switches, see this section.

NOTE

This section uses different versions as examples to describe the commands for different switches. The mappings are as follows. If you encounter compatibility issues when running commands for other versions, see the product documentation of the desired switch version. CE series switches: For enterprise users, **click here**. For carrier users, **click here**.

- V200R021C00 is used as an example to describe the commands for the CE6865, CE6865E, CE8850, CE6857, CE6857E, and CE6857F switches.

Prerequisites

You have obtained the login information about the switch to be configured.

Procedure

Step 1 Determine the combination mode of access and aggregation switches by referring to **Table 5-57**.

- Mode 2: For details about the configuration method, see **Step 2**.
- Mode 3: For details about the configuration method, see **Step 3**.
- Mode 4: For details about the configuration method, see **Step 4**.
- Mode 5: For details about the configuration method, see **Step 5**.

Table 5-57 Combination modes of access and aggregation switches

Mode	Access Switch Type	Access Switch Example	Aggregation Switch Type	Aggregation Switch Example
2	25GE	CE6865/CE6865E	100GE (fixed switch)	CE8850
3	10GE	CE6865/CE6865E	100GE (fixed switch)	CE8850
4	100GE	CE8850	100GE (fixed switch)	CE8850
5	10GE	CE6857/ CE6857E/ CE6857F	100GE (fixed switch)	CE8850

Copyright © Huawei Technologies Co., Ltd.

NOTE

If storage nodes and DPC compute nodes are connected to different types of switches, configure flow control separately as required.

Step 2 Configure RoCE flow control as follows if mode 2 in **Table 5-57** is used.

- To configure an access switch:
  a. Log in to the access switch.
  b. Configure the PFC priority and PFC deadlock detection.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

You are advised to configure **priority 3 turn-off threshold 10** on an access switch.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]interface 25ge 1/0/1
[~HUAWEI-25GE1/0/1]shutdown
Info: Operating, please wait for a moment.....done.
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 3
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]interface 25ge 1/0/1
[~HUAWEI-25GE1/0/1]undo shutdown
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used for RoCE (priorities 0, 1, and 3 are used as examples), configure the following information:

```
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]interface 25ge 1/0/1
[~HUAWEI-25GE1/0/1]shutdown
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 0 1 3
[*HUAWEI-dcb-pfc-default]priority 0 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 0 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 0 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]priority 1 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 1 deadlock-recovery time 10
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-dcb-pfc-default]priority 1 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]interface 25ge 1/0/1
[~HUAWEI-25GE1/0/1]undo shutdown
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
```

c. Configure ECN.

```
[~HUAWEI]drop-profile ecn_25G
[~HUAWEI-drop-ecn_25G]ecn buffer-size low-limit 250000 high-limit 700000 discard-percentage 10
[~HUAWEI-drop-ecn_25G]commit
[~HUAWEI-drop-ecn_25G]quit
[~HUAWEI]drop-profile ecn_100G
[~HUAWEI-drop-ecn_100G]ecn buffer-size low-limit 425000 high-limit 750000 discard-percentage 10
[~HUAWEI-drop-ecn_100G]commit
[~HUAWEI-drop-ecn_100G]quit
```

d. Configure flow control for downlink ports.

NOTE

- The downlink ports refer to the ports on access switches for connecting to storage devices.
- Repeat the following operations to configure flow control for other downlink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
[~HUAWEI]interface 25GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-25GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-25GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[*HUAWEI-25GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-25GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 250
[*HUAWEI-25GE1/0/1]qos drr 0 3
[*HUAWEI-25GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-25GE1/0/1]qos queue 3 drr weight 90
[*HUAWEI-25GE1/0/1]qos queue 3 wred ecn_25G
[*HUAWEI-25GE1/0/1]qos queue 3 ecn
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (Priorities 0, 1, and 3 are used as examples and their traffic ratios are 10%, 10%, and 80% respectively. Adjust the ratios according to actual situations), configure the following information:

```
[~HUAWEI]interface 25GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-25GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-25GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[*HUAWEI-25GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-25GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 250
[*HUAWEI-25GE1/0/1]dcb pfc buffer 1 xoff dynamic 4 hdrm 250
[*HUAWEI-25GE1/0/1]qos drr 0 1 3
[*HUAWEI-25GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-25GE1/0/1]qos queue 1 drr weight 10
[*HUAWEI-25GE1/0/1]qos queue 3 drr weight 80
[*HUAWEI-25GE1/0/1]qos queue 3 wred ecn_25G
[*HUAWEI-25GE1/0/1]qos queue 3 ecn
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A26-27-Y2]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the larger value between the value
of xon and the value of xoff minus the value of xon-offset.
C:cells    B:bytes    K:kilobytes    M:megabytes D:dynamic alpha
-------------------------------------------------------------------------------
Interface      Queue    Guaranteed         Xon Xon-Offset       Xoff        Hdrm
-------------------------------------------------------------------------------
25GE1/0/5          3          8(C)       50(C)      20(C)       4(D)      250(C)
-------------------------------------------------------------------------------
[~A26-27-Y2]
[~A26-27-Y2]
[~A26-27-Y2]
```

e. Configure flow control for uplink ports.

NOTE

- The uplink ports refer to the ports on access switches for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other uplink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
[~HUAWEI]interface 100GE 1/0/1  #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-100GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]qos drr 0 3
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 3 drr weight 90
[*HUAWEI-100GE1/0/1]qos queue 3 wred ecn_100G
[*HUAWEI-100GE1/0/1]qos queue 3 ecn
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

 Copyright © Huawei Technologies Co., Ltd.

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (Priorities 0, 1, and 3 are used as examples and their traffic ratios are 10%, 10%, and 80% respectively. Adjust the ratios according to actual situations), configure the following information:

```
[~HUAWEI]interface 100GE 1/0/1  #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[~HUAWEI-100GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[~HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[~HUAWEI-100GE1/0/1]dcb pfc buffer 1 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]qos drr 0 1 3
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 1 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 3 drr weight 80
[*HUAWEI-100GE1/0/1]qos queue 3 wred ecn_100G
[*HUAWEI-100GE1/0/1]qos queue 3 ecn
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

  NOTE

  Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23_25G_02-100GE1/0/3]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells   B:bytes   K:kilobytes   M:megabytes   D:dynamic alpha
-------------------------------------------------------------------------------
Interface      Queue    Guaranteed         Xon Xon-Offset       Xoff        Hdrm
-------------------------------------------------------------------------------
100GE1/0/1         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/2         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/3         3         8(C)       50(C)      20(C)       4(D)      330(C)
-------------------------------------------------------------------------------
25GE1/0/11         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
25GE1/0/12         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
```

- To configure an aggregation switch:
  a. Log in to the aggregation switch.
  b. Configure the PFC priority and PFC deadlock detection.

  NOTE

  You are advised to configure **priority 3 turn-off threshold 10** on an access switch.

  - When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]interface 100ge 1/0/1
[~HUAWEI-100GE1/0/1]shutdown
Info: Operating, please wait for a moment.....done.
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
```

 Copyright © Huawei Technologies Co., Ltd.

```
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 3
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]interface 100ge 1/0/1
[~HUAWEI-100GE1/0/1]undo shutdown
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used for RoCE (priorities 0, 1, and 3 are used as examples), configure the following information:

```
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]interface 100ge 1/0/1
[~HUAWEI-100GE1/0/1]shutdown
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 0 1 3
[*HUAWEI-dcb-pfc-default]priority 0 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 0 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 0 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]priority 1 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 1 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 1 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]interface 100ge 1/0/1
[~HUAWEI-100GE1/0/1]undo shutdown
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

c. Configure ECN.

```
[~HUAWEI]drop-profile ecn_100G
[~HUAWEI-drop-ecn_100G]ecn buffer-size low-limit 425000 high-limit 750000 discard-
percentage 10
[~HUAWEI-drop-ecn_100G]commit
[~HUAWEI-drop-ecn_100G]quit
```

d. Configure flow control for ports.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The ports refer to the ports on aggregation switches for connecting to access switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
[~HUAWEI]interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-100GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]qos drr 0 3
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 3 drr weight 90
[*HUAWEI-100GE1/0/1]qos queue 3 wred ecn_100G
[*HUAWEI-100GE1/0/1]qos queue 3 ecn
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (Priorities 0, 1, and 3 are used as examples and their traffic ratios are 10%, 10%, and 80% respectively. Adjust the ratios according to actual situations), configure the following information:

```
[~HUAWEI]interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-100GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]qos drr 0 1 3
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 1 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 3 drr weight 80
[*HUAWEI-100GE1/0/1]qos queue 3 wred ecn_100G
[*HUAWEI-100GE1/0/1]qos queue 3 ecn
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23_25G_02-100GE1/0/3]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells   B:bytes   K:kilobytes   M:megabytes   D:dynamic alpha
-------------------------------------------------------------------------------
Interface      Queue    Guaranteed        Xon Xon-Offset       Xoff        Hdrm
-------------------------------------------------------------------------------
100GE1/0/1         3         8(C)      50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/2         3         8(C)      50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/3         3         8(C)      50(C)      20(C)      4(D)       330(C)
-------------------------------------------------------------------------------
25GE1/0/11         3         8(C)      50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
25GE1/0/12         3         8(C)      50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
```

Step 3 Configure RoCE flow control as follows if mode 3 in **Table 5-57** is used.

- To configure an access switch:
  a. Log in to the access switch.
  b. Configure the PFC priority and PFC deadlock detection.

NOTE

If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

You are advised to configure **priority 3 turn-off threshold 10** on an access switch.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]interface 25ge 1/0/1
[~HUAWEI-25GE1/0/1]shutdown
Info: Operating, please wait for a moment.....done.
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 3
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
[~HUAWEI]commit
[~HUAWEI]interface 25ge 1/0/1
[~HUAWEI-25GE1/0/1]undo shutdown
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (priorities 0, 1, and 3 are used as examples), configure the following information:

```
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]interface 25ge 1/0/1
[~HUAWEI-25GE1/0/1]shutdown
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 0 1 3
[*HUAWEI-dcb-pfc-default]priority 0 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 0 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 0 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]priority 1 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 1 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 1 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
[~HUAWEI]commit
[~HUAWEI]interface 25ge 1/0/1
[~HUAWEI-25GE1/0/1]undo shutdown
[*HUAWEI-25GE1/0/1]commit
[~HUAWEI-25GE1/0/1]quit
```

c. Query the priority queues used by PFC.

```
dcb pfc
display this
commit
```

NOTE

The priority queue ranges from 0 to 7. 0 is dedicated for TCP.

As shown in the following figure, priority queue 3 has been used, and priority queues 1, 2, 4, 5, 6, and 7 are available.

```
[~leaf2-dcb-pfc-default]display this
#
dcb pfc
 priority 3
#
return
[~leaf2-dcb-pfc-default]
```

d. Configure ECN.

```
[~HUAWEI]drop-profile ecn_25G
[~HUAWEI-drop-ecn_25G]ecn buffer-size low-limit 250000 high-limit 700000 discard-
percentage 10
[~HUAWEI-drop-ecn_25G]commit
[~HUAWEI-drop-ecn_25G]quit
[~HUAWEI]drop-profile ecn_100G
[~HUAWEI-drop-ecn_100G]ecn buffer-size low-limit 425000 high-limit 750000 discard-
```

 Copyright © Huawei Technologies Co., Ltd.

```
percentage 10
[~HUAWEI-drop-ecn_100G]commit
[~HUAWEI-drop-ecn_100G]quit
```

e. Configure flow control for downlink ports.

NOTE

- The downlink ports refer to the ports on access switches for connecting to storage devices.
- Repeat the following operations to configure flow control for other downlink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
interface 25GE 1/0/1
dcb pfc enable mode manual
dcb pfc buffer 3 xoff dynamic 4 hdrm 250
qos buffer queue 0 shared-threshold dynamic 1
qos buffer queue 3 shared-threshold dynamic 10
qos queue 3 wred ecn_25G
qos queue 3 ecn
commit
quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (priorities 0, 1, and 3 are used as examples), configure the following information:

```
interface 25GE 1/0/1
dcb pfc enable mode manual
dcb pfc buffer 1 xoff dynamic 4 hdrm 250
dcb pfc buffer 3 xoff dynamic 4 hdrm 250
qos buffer queue 0 shared-threshold dynamic 1
qos buffer queue 3 shared-threshold dynamic 10
qos queue 3 wred ecn_25G
qos queue 3 ecn
commit
quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A26-27-Y2]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the larger value between the value
of xon and the value of xoff minus the value of xon-offset.
C:cells   B:bytes    K:kilobytes   M:megabytes D:dynamic alpha
--------------------------------------------------------------------------------
Interface      Queue    Guaranteed         Xon Xon-Offset       Xoff        Hdrm
--------------------------------------------------------------------------------
25GE1/0/5          3          8(C)       50(C)      20(C)       4(D)      250(C)
--------------------------------------------------------------------------------
[~A26-27-Y2]
[~A26-27-Y2]
[~A26-27-Y2]
```

f. Configure flow control for uplink ports.

NOTE

- The uplink ports refer to the ports on access switches for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other uplink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
[~HUAWEI]interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-100GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[*HUAWEI-100GE1/0/1]qos queue 3 wred ecn_100G
[*HUAWEI-100GE1/0/1]qos queue 3 ecn
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (priorities 0, 1, and 3 are used as examples), configure the following information:

```
[~HUAWEI]interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]dcb pfc buffer 0 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]dcb pfc buffer 1 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-100GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[*HUAWEI-100GE1/0/1]qos queue 3 wred ecn_100G
[*HUAWEI-100GE1/0/1]qos queue 3 ecn
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23_25G_02-100GE1/0/3]
[~A23_25G_02-100GE1/0/3]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells    B:bytes    K:kilobytes    M:megabytes    D:dynamic alpha
-------------------------------------------------------------------------------
Interface      Queue    Guaranteed        Xon Xon-Offset       Xoff        Hdrm
-------------------------------------------------------------------------------
100GE1/0/1         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/2         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/3         3         8(C)       50(C)      20(C)       4(D)      330(C)
-------------------------------------------------------------------------------
25GE1/0/11         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
25GE1/0/12         3         8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
```

- To configure an aggregation switch:
  a. Log in to the aggregation switch.
  b. Configure load balancing.

```
system-view
load-balance profile default
eth-trunk universal-id 3
commit
quit
```

  c. Configure the PFC priority.

```
[~HUAWEI]dcb pfc
[*HUAWEI-dcb-pfc-default]priority 3
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
```

  d. Configure ECN.

```
[~HUAWEI]drop-profile ecn_100G
[~HUAWEI-drop-ecn_100G]ecn buffer-size low-limit 425000 high-limit 750000 discard-percentage 10
[~HUAWEI-drop-ecn_100G]commit
[~HUAWEI-drop-ecn_100G]quit
```

  e. Configure flow control for ports.

NOTE

- The ports refer to the ports on aggregation switches for connecting to access switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces).
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
dcb pfc enable mode manual
dcb pfc buffer 3 xoff dynamic 4 hdrm 330
```

 Copyright © Huawei Technologies Co., Ltd.

```
qos buffer queue 0 shared-threshold dynamic 1
qos buffer queue 3 shared-threshold dynamic 10
qos queue 3 wred ecn_100G
qos queue 3 ecn
commit
quit
quit
save
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23_25G_02-100GE1/0/3]display dcb pfc buffer
Xon:         PFC backpressure stop threshold
Xoff:        PFC backpressure threshold
Hdrm:        Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells    B:bytes    K:kilobytes    M:megabytes    D:dynamic alpha
-------------------------------------------------------------------------------
Interface      Queue    Guaranteed         Xon Xon-Offset       Xoff        Hdrm
-------------------------------------------------------------------------------
100GE1/0/1         3          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/2         3          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/3         3          8(C)       50(C)      20(C)       4(D)      330(C)
-------------------------------------------------------------------------------
25GE1/0/11         3          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
25GE1/0/12         3          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
```

Step 4 Configure RoCE flow control as follows if mode 4 in **Table 5-57** is used.

- To configure an access switch:
  a. Log in to the access switch.
  b. Configure the PFC priority and PFC deadlock detection.

  NOTE

  You are advised to configure **priority 3 turn-off threshold 10** on an access switch.

  - When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]interface 100ge 1/0/1
[~HUAWEI-100GE1/0/1]shutdown
Info: Operating, please wait for a moment.....done.
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 3
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]interface 100ge 1/0/1
[~HUAWEI-100GE1/0/1]undo shutdown
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used for RoCE (priorities 0, 1, and 3 are used as examples), configure the following information:

```
<HUAWEI>system-view
Enter system view, return user view with return command.
[~HUAWEI]interface 100ge 1/0/1
[~HUAWEI-100GE1/0/1]shutdown
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 0 1 3
[*HUAWEI-dcb-pfc-default]priority 0 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 0 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 0 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]priority 1 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 1 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 1 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]interface 100ge 1/0/1
[~HUAWEI-100GE1/0/1]undo shutdown
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

c. Configure ECN.

```
[~HUAWEI]drop-profile ecn
```

- If the service network uses the NFS over RDMA service and shares network ports with the front-end storage network, run the following command:

```
[*HUAWEI-drop-ecn]ecn buffer-size low-limit 2125000 high-limit 6000000 discard-
percentage 1
```

- In other scenarios, run the following command:

```
[*HUAWEI-drop-ecn]ecn buffer-size low-limit 425000 high-limit 750000 discard-
percentage 10
```

```
[*HUAWEI-drop-ecn]commit
[~HUAWEI-drop-ecn]quit
```

d. Configure flow control for downlink ports.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The downlink ports refer to the ports on access switches for connecting to storage devices.
- Repeat the following operations to configure flow control for other downlink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
qos buffer queue 0 shared-threshold dynamic 1
qos buffer queue 3 shared-threshold dynamic 10
dcb pfc enable mode manual
dcb pfc buffer 3 xoff dynamic 4 hdrm 330
qos drr 0 3
qos queue 0 drr weight 10
qos queue 3 drr weight 90
qos queue 3 wred ecn
qos queue 3 ecn
commit
quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (Priorities 0, 1, and 3 are used as examples and their traffic ratios are 10%, 10%, and 80% respectively. Adjust the ratios according to actual situations), configure the following information:

```
interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
qos buffer queue 0 shared-threshold dynamic 1
qos buffer queue 3 shared-threshold dynamic 10
dcb pfc enable mode manual
dcb pfc buffer 3 xoff dynamic 4 hdrm 330
qos drr 0 1 3
qos queue 0 drr weight 10
qos queue 1 drr weight 10
qos queue 3 drr weight 80
qos queue 3 wred ecn
qos queue 3 ecn
commit
quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23_25G_02-100GE1/0/3]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells   B:bytes   K:kilobytes   M:megabytes   D:dynamic alpha
------------------------------------------------------------------------------
Interface      Queue    Guaranteed        Xon Xon-Offset       Xoff        Hdrm
------------------------------------------------------------------------------
100GE1/0/1         3         8(C)       50(C)      20(C)     200(C)      180(C)
------------------------------------------------------------------------------
100GE1/0/2         3         8(C)       50(C)      20(C)     200(C)      180(C)
------------------------------------------------------------------------------
100GE1/0/3         3         8(C)       50(C)      20(C)       4(D)      330(C)
------------------------------------------------------------------------------
25GE1/0/11         3         8(C)       50(C)      20(C)     200(C)      180(C)
------------------------------------------------------------------------------
25GE1/0/12         3         8(C)       50(C)      20(C)     200(C)      180(C)
------------------------------------------------------------------------------
```

e. Configure flow control for uplink ports.

NOTE

- The uplink ports refer to the ports on access switches for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other uplink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
qos buffer queue 0 shared-threshold dynamic 1
qos buffer queue 3 shared-threshold dynamic 10
dcb pfc enable mode manual
dcb pfc buffer 3 xoff dynamic 4 hdrm 330
qos drr 0 3
qos queue 0 drr weight 10
qos queue 3 drr weight 90
qos queue 3 wred ecn
qos queue 3 ecn
commit
quit
quit
save
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (Priorities 0, 1, and 3 are used as examples and their traffic ratios are 10%, 10%, and 80% respectively. Adjust the ratios according to actual situations), configure the following information:

 Copyright © Huawei Technologies Co., Ltd.

```
interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
qos buffer queue 0 shared-threshold dynamic 1
qos buffer queue 3 shared-threshold dynamic 10
dcb pfc enable mode manual
dcb pfc buffer 3 xoff dynamic 4 hdrm 330
qos drr 0 1 3
qos queue 0 drr weight 10
qos queue 1 drr weight 10
qos queue 3 drr weight 80
qos queue 3 wred ecn
qos queue 3 ecn
commit
quit
quit
save
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23_25G_02-100GE1/0/3]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells   B:bytes   K:kilobytes   M:megabytes   D:dynamic alpha
-------------------------------------------------------------------------------
Interface      Queue    Guaranteed        Xon Xon-Offset       Xoff        Hdrm
-------------------------------------------------------------------------------
100GE1/0/1         3          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/2         3          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
100GE1/0/3         3          8(C)       50(C)      20(C)      4(D)       330(C)
-------------------------------------------------------------------------------
25GE1/0/11         3          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
25GE1/0/12         3          8(C)       50(C)      20(C)     200(C)      180(C)
-------------------------------------------------------------------------------
```

Step 5 Configure RoCE flow control as follows if mode 5 in **Table 5-57** is used.

- To configure an access switch:
  a. Log in to the access switch.
  b. Configure the PFC priority and PFC deadlock detection.

  NOTE

  If you need to modify the PFC deadlock detection configuration, run the **shutdown** command before the configuration modification to disable all the interfaces where the PFC profile is applied to prevent configuration modification failures caused by deadlock recovery on the switch.

  After configuring the PFC priority and PFC deadlock detection, you need to enable the interfaces.

  - When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
<HUAWEI>system-view
Enter system view, return user view with return command.
# Repeat the following operations to disable other interfaces.
[~HUAWEI]interface 10GE 1/0/1
[~HUAWEI-10GE1/0/1]shutdown
Info: Operating, please wait for a moment.....done.
[*HUAWEI-10GE1/0/1]commit
[~HUAWEI-10GE1/0/1]quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
# The following is the global configuration. You do not need to perform the configuration
again.
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 3
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
[~HUAWEI]commit
# Repeat the following operations to enable other interfaces.
[~HUAWEI]interface 10GE 1/0/1
[~HUAWEI-10GE1/0/1]undo shutdown
[*HUAWEI-10GE1/0/1]commit
[~HUAWEI-10GE1/0/1]quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (priorities 0, 1, and 3 are used as examples), configure the following information:

```
<HUAWEI>system-view
Enter system view, return user view with return command.
# Repeat the following operations to disable other interfaces.
[~HUAWEI]interface 10GE 1/0/1
[~HUAWEI-10GE1/0/1]shutdown
Info: Operating, please wait for a moment.....done.
[*HUAWEI-10GE1/0/1]commit
[~HUAWEI-10GE1/0/1]quit
# The following is the global configuration. You do not need to perform the configuration
again.
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 0 1 3
[*HUAWEI-dcb-pfc-default]priority 0 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 0 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 0 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]priority 1 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 1 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 1 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-detect time 10
[*HUAWEI-dcb-pfc-default]priority 3 deadlock-recovery time 10
[*HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
Info: PFC will be disabled if the threshold for the number of detected deadlocks is
exceeded. If you need to use PFC again, reconfigure PFC on an interface.
[*HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
[~HUAWEI]dcb pfc deadlock-detect interval 10
[~HUAWEI]commit
# Repeat the following operations to enable other interfaces.
[~HUAWEI]interface 10GE 1/0/1
[~HUAWEI-10GE1/0/1]undo shutdown
[*HUAWEI-10GE1/0/1]commit
[~HUAWEI-10GE1/0/1]quit
```

c. Configure ECN.

```
[~HUAWEI]drop-profile ecn_10G
[~HUAWEI-drop-ecn_10G]ecn buffer-size low-limit 250000 high-limit 700000 discard-
percentage 10
[~HUAWEI-drop-ecn_10G]commit
[~HUAWEI-drop-ecn_10G]quit
[~HUAWEI]drop-profile ecn_100G
[~HUAWEI-drop-ecn_100G]ecn buffer-size low-limit 425000 high-limit 750000 discard-
percentage 10
```

 Copyright © Huawei Technologies Co., Ltd.

```
[~HUAWEI-drop-ecn_100G]commit
[~HUAWEI-drop-ecn_100G]quit
```

d. Configure flow control for downlink ports.

NOTE

- The downlink ports refer to the ports on access switches for connecting to storage devices.
- Repeat the following operations to configure flow control for other downlink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
[~HUAWEI]interface 10GE1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-10GE1/0/1]qos drr 0 3
[*HUAWEI-10GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-10GE1/0/1]qos queue 3 drr weight 90
[*HUAWEI-10GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-10GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[*HUAWEI-10GE1/0/1]qos queue 3 wred ecn_10G
[*HUAWEI-10GE1/0/1]qos queue 3 ecn
[*HUAWEI-10GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-10GE1/0/1]dcb pfc buffer 0 xoff dynamic 4 hdrm 250
[*HUAWEI-10GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 250
[*HUAWEI-10GE1/0/1]storm suppression broadcast packets 1000
[*HUAWEI-10GE1/0/1]storm suppression multicast packets 200
[*HUAWEI-10GE1/0/1]storm suppression unknown-unicast 1
[~HUAWEI-10GE1/0/1]commit
[~HUAWEI-10GE1/0/1]quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (priorities 0, 1, and 3 are used as examples), configure the following information:

```
[~HUAWEI/0/1]interface 10GE1/0/1   #This port is only an example. The actual port
prevails.
[~HUAWEI-10GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[~HUAWEI-10GE1/0/1]qos buffer queue 1 shared-threshold dynamic 3
[*HUAWEI-10GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[*HUAWEI-10GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-10GE1/0/1]dcb pfc buffer 1 xoff dynamic 4 hdrm 250
[*HUAWEI-10GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 250
[*HUAWEI-10GE1/0/1]qos drr 0 1 3
[*HUAWEI-10GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-10GE1/0/1]qos queue 1 drr weight 10
[*HUAWEI-10GE1/0/1]qos queue 3 drr weight 80
[*HUAWEI-10GE1/0/1]qos queue 1 wred ecn_10G
[*HUAWEI-10GE1/0/1]qos queue 1 ecn
[*HUAWEI-10GE1/0/1]qos queue 3 wred ecn_10G
[*HUAWEI-10GE1/0/1]qos queue 3 ecn
[*HUAWEI-10GE1/0/1]commit
[~HUAWEI-10GE1/0/1]quit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23-27-CE-10GE1/0/1]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells    B:bytes    K:kilobytes    M:megabytes    D:dynamic alpha
--------------------------------------------------------------------------------
Interface      Queue    Guaranteed         Xon Xon-Offset       Xoff        Hdrm
--------------------------------------------------------------------------------
100GE1/0/1         0          8(C)       50(C)      20(C)       4(D)      330(C)
                   3          8(C)       50(C)      20(C)       4(D)      250(C)
--------------------------------------------------------------------------------
10GE1/0/1          0          8(C)       50(C)      20(C)       4(D)      250(C)
                   3          8(C)       50(C)      20(C)       4(D)      250(C)
--------------------------------------------------------------------------------
[~A23-27-CE-10GE1/0/1]
```

e. Configure flow control for uplink ports.

NOTE

- The uplink ports refer to the ports on access switches for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other uplink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

- When the compute service and storage service of a DPC node use independent NICs, configure the following information:

```
[~HUAWEI]interface 100GE1/0/1  #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-100GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 250
[*HUAWEI-100GE1/0/1]qos drr 0 3
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 3 drr weight 90
[*HUAWEI-100GE1/0/1]qos queue 3 wred ecn_100G
[*HUAWEI-100GE1/0/1]qos queue 3 ecn
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

- When the compute service and DPC of a compute node share NICs and a priority other than 0 and 3 is used (priorities 0, 1, and 3 are used as examples), configure the following information:

```
[~HUAWEI]interface 100GE 1/0/1  #This port is only an example. The actual port prevails.
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]dcb pfc buffer 1 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xoff dynamic 4 hdrm 330
[*HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-100GE1/0/1]qos buffer queue 1 shared-threshold dynamic 3
[*HUAWEI-100GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-100GE1/0/1]qos drr 0 1 3
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 1 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 3 drr weight 80
[*HUAWEI-100GE1/0/1]qos queue 1 wred ecn_100G
[*HUAWEI-100GE1/0/1]qos queue 1 ecn
[*HUAWEI-100GE1/0/1]qos queue 3 wred ecn_100G
[*HUAWEI-100GE1/0/1]qos queue 3 ecn
[*HUAWEI-100GE1/0/1]commit
[~HUAWEI-100GE1/0/1]quit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23-27-CE-10GE1/0/1]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells   B:bytes   K:kilobytes   M:megabytes   D:dynamic alpha
--------------------------------------------------------------------------------
Interface      Queue    Guaranteed         Xon Xon-Offset       Xoff        Hdrm
--------------------------------------------------------------------------------
100GE1/0/1         0          8(C)       50(C)      20(C)       4(D)      330(C)
                   3          8(C)       50(C)      20(C)       4(D)      250(C)
--------------------------------------------------------------------------------
10GE1/0/1          0          8(C)       50(C)      20(C)       4(D)      250(C)
                   3          8(C)       50(C)      20(C)       4(D)      250(C)
--------------------------------------------------------------------------------
[~A23-27-CE-10GE1/0/1]
```

- To configure an aggregation switch:
  a. Log in to the aggregation switch.
  b. Configure load balancing.

     ```
     system-view
     load-balance profile default
     eth-trunk universal-id 3
     commit
     quit
     ```

  c. Configure the PFC priority.

     ```
     [~HUAWEI]dcb pfc
     [*HUAWEI-dcb-pfc-default]priority 3
     [*HUAWEI-dcb-pfc-default]commit
     [~HUAWEI-dcb-pfc-default]quit
     ```

  d. Configure ECN.

     ```
     [~HUAWEI]drop-profile ecn_100G
     [~HUAWEI-drop-ecn_100G]ecn buffer-size low-limit 425000 high-limit 750000 discard-percentage 10
     [~HUAWEI-drop-ecn_100G]commit
     [~HUAWEI-drop-ecn_100G]quit
     ```

  e. Configure flow control for ports.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The ports refer to the ports on aggregation switches for connecting to access switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces).
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
dcb pfc enable mode manual
dcb pfc buffer 3 xoff dynamic 4 hdrm 330
qos buffer queue 0 shared-threshold dynamic 1
qos buffer queue 3 shared-threshold dynamic 10
qos queue 3 wred ecn_100G
qos queue 3 ecn
commit
quit
quit
save
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the value in the **Hdrm** column or another column is empty, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

```
[~A23_25G_02-100GE1/0/3]
[~A23_25G_02-100GE1/0/3]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
Hdrm:       Headroom buffer threshold
Guaranteed: PFC guaranteed buffer threshold
The actual PFC backpressure stop threshold is the higher value between the value
of xon and the difference between the value of xoff and the value of xon-offset.
C:cells   B:bytes   K:kilobytes   M:megabytes   D:dynamic alpha
------------------------------------------------------------------------------
Interface      Queue    Guaranteed        Xon Xon-Offset       Xoff        Hdrm
------------------------------------------------------------------------------
100GE1/0/1         3         8(C)       50(C)      20(C)     200(C)      180(C)
------------------------------------------------------------------------------
100GE1/0/2         3         8(C)       50(C)      20(C)     200(C)      180(C)
------------------------------------------------------------------------------
100GE1/0/3         3         8(C)       50(C)      20(C)       4(D)      330(C)
------------------------------------------------------------------------------
25GE1/0/11         3         8(C)       50(C)      20(C)     200(C)      180(C)
------------------------------------------------------------------------------
25GE1/0/12         3         8(C)       50(C)      20(C)     200(C)      180(C)
------------------------------------------------------------------------------
```

----End

5.5.2.2.2.3 Configuring Flow Control for a Switch (CE6866/CE8851)

Scenarios

If a storage node or DPC compute node uses RoCE NICs, you need to configure the layer 2 Priority-based Flow Control (PFC) protocol and layer 3 Explicit Congestion Notification (ECN) protocol for the ports on the access and aggregation switches. This section uses CE6866 and CE8851 switches as examples.

This section covers the following switches (applicable to both front- and back-end storage switches):

 Copyright © Huawei Technologies Co., Ltd.

- **CE6866 Switch**
- **CE8851 Switch**

NOTE

This section uses V300R021C00 as an example to describe the commands for the CE6866 and CE8851 switches.

Prerequisites

You have obtained the login information about the switch to be configured.

CE6866 Switch

Step 1 Log in to a switch.

Step 2 Configure the PFC priority and PFC deadlock detection.

NOTE

You are advised to configure **priority 3 turn-off threshold 10** on an access switch.

```
[~HUAWEI]dcb pfc deadlock-detect timer 100
[~HUAWEI]dcb pfc deadlock-recovery timer 100
[~HUAWEI]dcb pfc deadlock recovery-behavior discard slot 1
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 3
[~HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
[~HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
```

Step 3 Configure ECN.

```
[~HUAWEI]drop-profile ecn_25G
[*HUAWEI-drop-ecn_25G]ecn buffer-size low-limit 250000 high-limit 700000 discard-percentage 10
[~HUAWEI-drop-ecn_25G]commit
[~HUAWEI-drop-ecn_25G]quit
[~HUAWEI]drop-profile ecn_100G
[*HUAWEI-drop-ecn_100G]ecn buffer-size low-limit 425000 high-limit 750000 discard-percentage 10
[*HUAWEI-drop-ecn_100G]commit
[~HUAWEI-drop-ecn_100G]quit
```

Step 4 Configure flow control for downlink ports.

NOTE

- The downlink ports refer to the ports on access switches for connecting to storage devices.
- Repeat the following operations to configure flow control for other downlink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI]interface 25GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-25GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[~HUAWEI-25GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[~HUAWEI-25GE1/0/1]dcb pfc enable mode manual
[~HUAWEI-25GE1/0/1]qos queue 3 wred ecn_25G
[*HUAWEI-25GE1/0/1]qos drr 0 3
[*HUAWEI-25GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-25GE1/0/1]qos queue 3 drr weight 90
[*HUAWEI-25GE1/0/1]qos queue 3 ecn
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-25GE1/0/1]dcb pfc buffer 3 xon static 550 KB xoff static 600 KB
[*HUAWEI-25GE1/0/1]commit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the values in the **Xon** and **Xoff** columns do not exist for the configured network ports in the table in the command output, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

If the command is successfully executed, an example of the command output is as follows:

```
[~A31-23]display dcb pfc buffer
Xon:       PFC backpressure stop threshold
Xoff:      PFC backpressure threshold
K:kilobytes
-------------------------------------------------
Interface      Queue          Xon          Xoff
-------------------------------------------------
25GE1/0/1        3        550(K)        600(K)
-------------------------------------------------
25GE1/0/2        3        550(K)        600(K)
-------------------------------------------------
25GE1/0/3        3        550(K)        600(K)
-------------------------------------------------
```

Step 5 Configure flow control for uplink ports.

NOTE

- The uplink ports refer to the ports on access switches for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other uplink ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI]interface 100GE 1/0/1   #This port is only an example. The actual port prevails.
[~HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[~HUAWEI-100GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[~HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[~HUAWEI-100GE1/0/1]qos queue 3 wred ecn_100G
[*HUAWEI-100GE1/0/1]qos drr 0 3
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 3 drr weight 90
[*HUAWEI-100GE1/0/1]qos queue 3 ecn
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xon static 550 KB xoff static 600 KB
[*HUAWEI-100GE1/0/1]commit
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the values in the **Xon** and **Xoff** columns do not exist for the configured network ports in the table in the command output, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

If the command is successfully executed, an example of the command output is as follows:

```
[~A31-23]display dcb pfc buffer
Xon:        PFC backpressure stop threshold
Xoff:       PFC backpressure threshold
K:kilobytes
-------------------------------------------------
Interface      Queue          Xon          Xoff
-------------------------------------------------
100GE1/0/1         3        550(K)        600(K)
-------------------------------------------------
100GE1/0/2         3        550(K)        600(K)
-------------------------------------------------
100GE1/0/3         3        550(K)        600(K)
-------------------------------------------------
100GE1/0/4         3        550(K)        600(K)
-------------------------------------------------
```

----End

CE8851 Switch

Step 1 Log in to a switch.

Step 2 Configure the PFC priority and PFC deadlock detection.

NOTE

You are advised to configure **priority 3 turn-off threshold 10** on an access switch.

```
[~HUAWEI]dcb pfc deadlock-detect timer 100
[~HUAWEI]dcb pfc deadlock-recovery timer 100
[~HUAWEI]dcb pfc deadlock recovery-behavior discard slot 1
[~HUAWEI]dcb pfc
[~HUAWEI-dcb-pfc-default]priority 3
[~HUAWEI-dcb-pfc-default]priority 3 turn-off threshold 10
[~HUAWEI-dcb-pfc-default]commit
[~HUAWEI-dcb-pfc-default]quit
```

Step 3 Configure ECN.

```
[~HUAWEI]drop-profile ecn
```

- If the service network uses the NFS over RDMA service and shares network ports with the front-end storage network, run the following command:
  ```
  [*HUAWEI-drop-ecn]ecn buffer-size low-limit 2125000 high-limit 6000000 discard-percentage 1
  ```
- In other scenarios, run the following command:
  ```
  [*HUAWEI-drop-ecn]ecn buffer-size low-limit 425000 high-limit 750000 discard-percentage 10
  ```

Step 4 Configure flow control for ports.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- For aggregation switches, the ports refer to the ports on the aggregation switches for connecting to access switches. For access switches, the ports refer to the ports on the access switches for connecting to storage devices and those for connecting to aggregation switches.
- Repeat the following operations to configure flow control for other ports (not configured for peer-link interfaces). You can use the port group function to perform batch configuration. For details, see **5.5.25.6 Configuring Switch Ports in a Batch**.
- To prevent flow control from failing to be configured due to heavy service volume, you are advised to run the **shutdown** command to disable all ports with flow control to be configured. After the configuration is complete, run the **undo shutdown** command to enable the ports.

```
[~HUAWEI]interface 100GE 1/0/1
[~HUAWEI-100GE1/0/1]qos buffer queue 0 shared-threshold dynamic 1
[*HUAWEI-100GE1/0/1]qos buffer queue 3 shared-threshold dynamic 10
[*HUAWEI-100GE1/0/1]dcb pfc enable mode manual
[*HUAWEI-100GE1/0/1]qos drr 0 3
[*HUAWEI-100GE1/0/1]qos queue 0 drr weight 10
[*HUAWEI-100GE1/0/1]qos queue 3 drr weight 90
[*HUAWEI-100GE1/0/1]qos queue 3 wred ecn
[*HUAWEI-100GE1/0/1]qos queue 3 ecn
[*HUAWEI-100GE1/0/1]dcb pfc buffer 3 xon static 550 KB xoff static 600 KB
[*HUAWEI-100GE1/0/1]commit
```

NOTE

Run the following command to check whether the PFC configuration of the switch takes effect. If the values in the **Xon** and **Xoff** columns do not exist for the configured network ports in the table in the command output, the PFC configuration does not take effect.

```
display dcb pfc buffer
```

If the command is successfully executed, an example of the command output is as follows:

```
[~A31-23]display dcb pfc buffer
Xon:       PFC backpressure stop threshold
Xoff:      PFC backpressure threshold
K:kilobytes
-------------------------------------------------
Interface     Queue          Xon          Xoff
-------------------------------------------------
100GE1/0/1        3       550(K)        600(K)
-------------------------------------------------
100GE1/0/2        3       550(K)        600(K)
-------------------------------------------------
100GE1/0/3        3       550(K)        600(K)
-------------------------------------------------
100GE1/0/4        3       550(K)        600(K)
-------------------------------------------------
```

----End

5.5.2.3 Configuring ACL Rules for Switches

If the transmission protocol used by the storage network is RoCE, you need to configure ACL rules for access switches. After the configuration, the latency and packet loss rate between storage nodes and the access switches can be detected. To view the first-hop latency and first-hop packet loss rate, choose **Cluster** > **Network** > **Diagnosis** > **Subhealthy Links** on DeviceManager after creating a control cluster.

This section describes two configuration methods: using a script and using switch commands.

 Copyright © Huawei Technologies Co., Ltd.

- To configure ACL rules for a switch using a script, log in to a storage node, import the switch login information and all downlink ports to be configured to the script, and execute the script.
- To configure ACL rules for a switch using switch commands, log in to an access switch and run several switch configuration commands for each downlink port of the switch.

5.5.2.3.1 Using a Script

Scenarios

This section describes how to configure ACL rules for a switch using a script.

- To configure ACL rules for a switch using a script, log in to a storage node, import the switch login information and all downlink ports to be configured to the script, and execute the script.
- The script supports the following switches (applicable to both front- and back-end storage switches):
  - CE6857/CE6857E/CE6857F/CE6865/CE6865E switch
  - CE8850 switch
  - CE6866/CE8851/CE16804/CE16808 switch

Prerequisites

- You have obtained the login information about the access switch to be configured.
- You have created a control cluster.

  NOTE

  The script supports the following switch versions. For details about how to configure this function for switches of other versions, see **5.5.2.3.2 Using Switch Commands**.

  - The version of the CE6857/CE6857E/CE6857F/CE6865/CE6865E/CE8850 switch must be V200R021C00SPC200 or later.
  - The version of the CE6866/CE8851/CE16804/CE16808 switch must be V300R021C00SPC200 or later.

Procedure

Step 1 To use the script on nodes, you need to configure the Telnet function on access switches. If the function is not configured, configure it by referring to the product documentation of the switch of the desired version. CE series switches: For enterprise users, **click here**. For carrier users, **click here**.

Step 2 Log in to a storage node in the cluster.

1. Use an SSH tool to log in to a node as user **fsadmin** and enter the cliportal view.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

To obtain the default user password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)* or *OceanStor Pacific Series 8.2.1 Account List (Block Service)*. You need to change the default password upon the first login. After the password is changed, log in to the node again. If the default password has been changed, use the new password to log in.

2. Run the **minisystem** command and enter the password of user **root** as prompted to go to the minisystem view.
3. Run the **ping** command to ping the IP address of an access switch. Ensure that the network communication between the node and the access switch is normal. If the communication between the node and the access switch is abnormal, you cannot use the script on the node.

Step 3 Run script configuration command **pingmesh_switch_acl.py -i** *Switch IP address* **-t 0 -p** *Switch ports* **-u** *Switch user name* and enter the user password as prompted to configure ACL rules for the switch ports. For details about the command parameters, see **Table 5-58**.

Table 5-58 Command parameter description

Parameter	Description
Switch IP address	IP address of the access switch to be configured.
Switch ports	All downlink ports on the access switch. Use commas (,) to separate multiple ports, for example, **100GE1/0/1,100GE1/0/2**. **NOTE** The downlink ports refer to the ports on access switches for connecting to storage devices.
Switch user name	Telnet user name of the access switch, which is the Telnet user configured in **Step 1**. This parameter is optional. If it is not specified, the system prompts you to enter the switch user name after the script command is executed. The following is an example: minisystem> **pingmesh_switch_acl.py -i** *192.168.0.1* **-t 0 -p** *100GE1/0/1,100GE1/0/2* Switch username:

The following are examples of the script configuration command and configuration result. In the command output, the information under **Checking configuration...** is the configuration result of the switch ports.

- If **Check configuration of** *Switch port* **success.** is displayed for all switch ports in the command output, the configuration is successful. The following is an example.

```
minisystem> pingmesh_switch_acl.py -i 192.168.0.1 -t 0 -p 100GE1/0/1,100GE1/0/2 -u test
Switch password:
Log in to switch 192.168.0.1 success.
Switch info: board type=FM6865-48S8CQ-EI, version=V200R021C00SPC200, ACL_MODEL=2.
Configure interface 100GE1/0/1 complete.
Configure interface 100GE1/0/2 complete.
Checking configuration...
```

 Copyright © Huawei Technologies Co., Ltd.

```
Check configuration of 100GE1/0/1 success.
Check configuration of 100GE1/0/2 success.
```

- If other information is displayed, rectify the fault as prompted or contact technical support.

Step 4 Repeat **Step 3** to configure ACL rules for other access switch ports.

----End

5.5.2.3.2 Using Switch Commands

Scenarios

This section describes how to configure ACL rules for a switch using switch commands.

- To configure ACL rules for a switch using switch commands, log in to an access switch and run several switch configuration commands for each downlink port of the switch.
- This section covers the following switches (applicable to both front- and back-end storage switches):
  - **CE6857/CE6857E/CE6857F/CE6865/CE6865E Switch**
  - **CE8850 Switch**
  - **CE6866/CE8851/CE16804/CE16808 Switch**

  NOTE

  This section uses different versions as examples to describe the commands for different switches. The mappings are as follows. If you encounter compatibility issues when running commands for other versions, see the product documentation of the desired switch version. CE series switches: For enterprise users, **click here**. For carrier users, **click here**.

  - V200R021C00SPC200 is used as an example to describe the commands for the CE6857/CE6857E/CE6857F/CE6865/CE6865E/CE8850 switch.
  - V300R021C00SPC200 is used as an example to describe the commands for the CE6866/CE8851/CE16804/CE16808 switch.

Prerequisites

You have obtained the login information about the access switch to be configured.

CE6857/CE6857E/CE6857F/CE6865/CE6865E Switch

Step 1 Log in to an access switch.

Step 2 Create a template.

```
<HUAWEI>system-view
[~HUAWEI]system tcam acl
Warning: Enabling the TCAM ACL will cause ACL resources to be replanned. Incorrectly using these commands will cause some services to be unavailable. Therefore, use these commands with the guidance of Huawei engineers. Continue? [Y/N]:Y
[*HUAWEI]commit
[~HUAWEI]system tcam acl template c1
[*HUAWEI-tcam-acl-c1]group g1
[*HUAWEI-tcam-acl-c1-group-g1]match forwarding source-interface
[*HUAWEI-tcam-acl-c1-group-g1]match udf l4-head 0 4 udf l4-head 8 4 udf l4-head 20 4 udf l4-head 28 4
```

 Copyright © Huawei Technologies Co., Ltd.

```
[*HUAWEI-tcam-acl-c1-group-g1]service trafficpolicy-l3global group g1
[*HUAWEI-tcam-acl-c1]commit
[~HUAWEI-tcam-acl-c1]sys tcam acl template c1 all
[*HUAWEI]commit
```

Step 3 Create an ACL rule.

```
[~HUAWEI]acl number 5501
[*HUAWEI-acl-user-5501]rule 15 permit l4-head 0x000012b7 0x0000ffff 0 0x64000000 0xff000000 8 0x22222222 0xffffffff 20 0xd19e6b08 0xffffffff 28
[*HUAWEI-acl-user-5501]commit
[~HUAWEI-acl-user-5501]quit
```

Step 4 Create a traffic classifier.

```
[~HUAWEI]traffic classifier acl_classifier type and
[*HUAWEI-classifier-acl_classifier]if-match acl 5501
[*HUAWEI-classifier-acl_classifier]commit
[~HUAWEI-classifier-acl_classifier]quit
```

Step 5 Apply the ACL rule to a downlink port.

NOTE

The downlink port refers to a port on an access switch for connecting to a storage device.

1. Create a traffic behavior.

   ```
   [~HUAWEI]traffic behavior acl_behavior_1 # Create a traffic behavior. The traffic behavior name corresponding to each port must be unique.
   [*HUAWEI-behavior-acl_behavior_1]remark dscp 63
   [*HUAWEI-behavior-acl_behavior_1]redirect interface 100GE1/0/1  # The 100GE1/0/1 port is only an example.
   [*HUAWEI-behavior-acl_behavior_1]commit
   [~HUAWEI-behavior-acl_behavior_1]quit
   ```

2. Create a traffic policy.

   ```
   [~HUAWEI]traffic policy acl_policy_1  # Create a traffic policy. The traffic policy name corresponding to each port must be unique.
   [*HUAWEI-trafficpolicy-acl_policy_1]classifier acl_classifier behavior acl_behavior_1
   [*HUAWEI-trafficpolicy-acl_policy_1]commit
   [~HUAWEI-trafficpolicy-acl_policy_1]quit
   ```

   NOTE

   acl_behavior_1 is the name of the traffic behavior created in **Step 5.1**.

3. Apply the traffic policy to the port.

   ```
   [~HUAWEI]int 100GE1/0/1
   [~HUAWEI-100GE1/0/1]traffic-policy acl_policy_1 inbound
   [*HUAWEI-100GE1/0/1]commit
   [~HUAWEI-100GE1/0/1]quit
   ```

   NOTE

   - *100GE1/0/1* is the port name in **Step 5.1**.
   - *acl_policy_1* is the name of the traffic policy created in **Step 5.2**.

4. Check whether the traffic policy is successfully configured. If the value in the **State** column of the traffic policy is **success**, the configuration is successful.

   ```
   [~HUAWEI]dis traffic-policy applied-record
   Total records : 1
   ---------------------------------------------------------------------------
   Policy Type/Name                Apply Parameter              Slot  State
   ---------------------------------------------------------------------------
   acl_policy_1                    100GE1/0/1(IN)               1     success
   ```

Step 6 Repeat **Step 5** to apply the ACL rule to other downlink ports.

Step 7 Save the configurations.

 Copyright © Huawei Technologies Co., Ltd.

```
<~HUAWEI>quit
<HUAWEI>save
```

----End

CE8850 Switch

Step 1 Log in to an access switch.

Step 2 Create an ACL rule.

```
<HUAWEI>system-view
[~HUAWEI]acl number 5501
[*HUAWEI-acl-user-5501]rule 15 permit l4-head 0x000012b7 0x0000ffff 0 0x64000000 0xff000000 8 0x22222222 0xffffffff 20 0xd19e6b08 0xffffffff 28
[*HUAWEI-acl-user-5501]commit
[~HUAWEI-acl-user-5501]quit
```

Step 3 Create a traffic classifier.

```
[~HUAWEI]traffic classifier acl_classifier type and
[*HUAWEI-classifier-acl_classifier]if-match acl 5501
[*HUAWEI-classifier-acl_classifier]commit
[~HUAWEI-classifier-acl_classifier]quit
```

Step 4 Apply the ACL rule to a downlink port.

NOTE

The downlink port refers to a port on an access switch for connecting to a storage device.

1. Create a traffic behavior.

   ```
   [~HUAWEI]traffic behavior acl_behavior_1 # Create a traffic behavior. The traffic behavior name corresponding to each port must be unique.
   [*HUAWEI-behavior-acl_behavior_1]remark dscp 63
   [*HUAWEI-behavior-acl_behavior_1]redirect interface 100GE1/0/1  # The 100GE1/0/1 port is only an example.
   [*HUAWEI-behavior-acl_behavior_1]commit
   [~HUAWEI-behavior-acl_behavior_1]quit
   ```

2. Create a traffic policy.

   ```
   [~HUAWEI]traffic policy acl_policy_1  # Create a traffic policy. The traffic policy name corresponding to each port must be unique.
   [*HUAWEI-trafficpolicy-acl_policy_1]classifier acl_classifier behavior acl_behavior_1
   [*HUAWEI-trafficpolicy-acl_policy_1]commit
   [~HUAWEI-trafficpolicy-acl_policy_1]quit
   ```

   NOTE

   acl_behavior_1 is the name of the traffic behavior created in **Step 4.1**.

3. Apply the traffic policy to the port.

   ```
   [~HUAWEI]int 100GE1/0/1
   [~HUAWEI-100GE1/0/1]traffic-policy acl_policy_1 inbound
   [*HUAWEI-100GE1/0/1]commit
   [~HUAWEI-100GE1/0/1]quit
   ```

   NOTE

   - *100GE1/0/1* is the port name in **Step 4.1**.
   - *acl_policy_1* is the name of the traffic policy created in **Step 4.2**.

4. Check whether the traffic policy is successfully configured. If the value in the **State** column of the traffic policy is **success**, the configuration is successful.

   ```
   [~HUAWEI]dis traffic-policy applied-record
   Total records : 1
   --------------------------------------------------------------------------------
   Policy Type/Name                Apply Parameter          Slot  State
   ```

 Copyright © Huawei Technologies Co., Ltd.

```
--------------------------------------------------------------------------------
acl_policy_1                    100GE1/0/10(IN)          1     success
```

Step 5 Repeat **Step 4** to apply the ACL rule to other downlink ports.

Step 6 Save the configurations.

```
<~HUAWEI>quit
<HUAWEI>save
```

----End

CE6866/CE8851/CE16804/CE16808 Switch

Step 1 Log in to an access switch.

Step 2 Create an ACL rule.

```
<HUAWEI>system-view
[~HUAWEI]acl number 5501
[~HUAWEI-acl-user-5501]rule 15 permit l4-head 0x000012b7 0x0000ffff 0 0x64000000 0xff000000 8 0x22222222 0xffffffff 20 0xd19e6b08 0xffffffff 28
[*HUAWEI-acl-user-5501]commit
[~HUAWEI-acl-user-5501]quit
```

Step 3 Configure a traffic classifier and a traffic behavior for a downlink port and add them to a global traffic policy.

NOTE

The downlink port refers to a port on an access switch for connecting to a storage device.

1. Create a traffic classifier.

   ```
   [~HUAWEI]traffic classifier acl_classifier_1 type and  # Create a traffic classifier. The traffic classifier name corresponding to each port must be unique.
   [*HUAWEI-classifier-acl_classifier_1]if-match acl 5501
   [*HUAWEI-classifier-acl_classifier_1]if-match inbound-interface 100GE1/0/1  # The 100GE1/0/1 port is only an example.
   [*HUAWEI-classifier-acl_classifier_1]commit
   [~HUAWEI-classifier-acl_classifier_1]quit
   ```

2. Create a traffic behavior.

   ```
   [~HUAWEI]traffic behavior acl_behavior_1 # Create a traffic behavior. The traffic behavior name corresponding to each port must be unique.
   [*HUAWEI-behavior-acl_behavior_1]remark dscp 63
   [*HUAWEI-behavior-acl_behavior_1]redirect interface 100GE1/0/1
   [*HUAWEI-behavior-acl_behavior_1]commit
   [~HUAWEI-behavior-acl_behavior_1]quit
   ```

   NOTE

   100GE1/0/1 is the port name in **Step 3.1**.

3. Add the traffic classifier and the traffic behavior to a global traffic policy.

   ```
   [~HUAWEI]traffic policy acl_policy  # acl_policy indicates the global traffic policy name. If you run this command for the first time, a global traffic policy is created. If you run this command subsequently, the global traffic policy is accessed.
   [*HUAWEI-trafficpolicy-acl_policy]classifier acl_classifier_1 behavior acl_behavior_1
   [*HUAWEI-trafficpolicy-acl_policy]commit
   [~HUAWEI-trafficpolicy-acl_policy]quit
   ```

   NOTE

   - *acl_classifier_1* is the name of the traffic classifier created in **Step 3.1**.
   - *acl_behavior_1* is the name of the traffic behavior created in **Step 3.2**.

Step 4 Repeat **Step 3** to configure a traffic classifier and a traffic behavior for other downlink ports and add them to the global traffic policy.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Make the global traffic policy take effect.

```
[~HUAWEI]traffic-policy acl_policy global inbound
[*HUAWEI]commit
[~HUAWEI]quit
```

Step 6 Check whether the configuration is successful.

1. Check whether the traffic policy is successfully configured. If the value in the **State** column of the traffic policy is **success**, the configuration is successful.

```
<HUAWEI>dis traffic-policy applied-record
Total records : 1
-------------------------------------------------------------------------------
Policy Type/Name                Apply Parameter          Slot  State
-------------------------------------------------------------------------------
acl_policy                      Global(IN)               1     success
-------------------------------------------------------------------------------
```

2. Check whether the ACL rules of all downlink ports are successfully configured.

```
<HUAWEI>system-view
[~HUAWEI]traffic policy acl_policy
[*HUAWEI-trafficpolicy-acl_policy]dis this
#
traffic policy acl_policy
 classifier acl_classifier_1 behavior acl_behavior_1 precedence 5
 classifier acl_classifier_2 behavior acl_behavior_2 precedence 10
 ......
#
return
[*HUAWEI-trafficpolicy-acl_policy]quit
<~HUAWEI>quit
```

NOTE

In the output of the **dis this** command, **classifier** *acl_classifier_xxx* **behavior** *acl_behavior_xxx* **precedence** *xxx* under **traffic policy acl_policy** indicates the traffic classifier and traffic behavior of a downlink port. If the information is configured for each downlink port, the ACL rules of all downlink ports are successfully configured.

acl_classifier_xxx is the name of the traffic classifier configured for the downlink port in **Step 3.1**, and *acl_behavior_xxx* is the name of the traffic behavior configured for the downlink port in **Step 3.2**.

Step 7 Save the configurations.

```
<HUAWEI>save
```

----End

5.5.2.4 Querying the ACL Rule Configuration of a Switch

Scenarios

This section describes how to use a script to query the configuration result of ACL rules on a switch.

Prerequisites

- You have obtained the login information about the switch to be queried.
- You have created a control cluster.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The script supports the following switch versions. Switches of other versions cannot be queried using the script.

- The version of the CE6857/CE6857E/CE6857F/CE6865/CE6865E/CE8850 switch must be V200R021C00SPC200 or later.
- The version of the CE6866/CE8851/CE16804/CE16808 switch must be V300R021C00SPC200 or later.

Procedure

Step 1 To use the script to query the switch ACL rule configuration on a node, you need to configure the Telnet function on access switches. If the function is not configured, configure it by referring to the product documentation of the switch of the desired version. CE series switches: For enterprise users, **click here**. For carrier users, **click here**.

Step 2 Log in to a storage node in the cluster.

1. Use an SSH tool to log in to a node as user **fsadmin** and enter the cliportal view.

   NOTE

   To obtain the default user password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)* or *OceanStor Pacific Series 8.2.1 Account List (Block Service)*. You need to change the default password upon the first login. After the password is changed, log in to the node again. If the default password has been changed, use the new password to log in.

2. Run the **minisystem** command and enter the password of user **root** as prompted to go to the minisystem view.
3. Run the **ping** command to ping the IP address of an access switch. Ensure that the network communication between the node and the access switch is normal. If the communication between the node and the access switch is abnormal, you cannot use the script on the node.

Step 3 Run script query command **pingmesh_switch_acl.py -i** *Switch IP address* **-t 2 -u** *Switch user name* and enter the user password as prompted to query the ACL rule configuration of the specified switch. For details about the command parameters, see **Table 5-59**.

Table 5-59 Command parameter description

Parameter	Description
Switch IP address	IP address of the access switch to be queried.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Switch user name	Telnet user name of the access switch, which is the Telnet user configured in **Step 1**. This parameter is optional. If it is not specified, the system prompts you to enter the switch user name after the script command is executed. The following is an example: minisystem> **pingmesh_switch_acl.py -i** *182.168.0.1* **-t 2** Switch username:

The following are examples of the script query command and query result. In the command output, the information under **Total records :** is the query result of the switch port configuration.

- In the command output, if the value in the **State** column is **success**, the corresponding port is configured successfully. The following is an example.

```
minisystem> pingmesh_switch_acl.py -i 192.168.0.1 -t 2 -u test
Switch password:
Log in to switch 192.168.0.1 success.
Switch info: board type=CE8850-64CQ-EI, version=V200R021C00SPC200, ACL_MODEL=0.
acl number 5501
 rule 15 permit l4-head 0x000012b7 0x0000ffff 0 0x64000000 0xff000000 8 0x22222222 0xffffffff 20
0xd19e6b08 0xffffffff 28
traffic classifier c_pingmesh type and
 if-match acl 5501
traffic behavior b100GE1/0/1_pingmesh
 remark dscp 63
 redirect interface 100GE1/0/1
traffic behavior b100GE1/0/2_pingmesh
 remark dscp 63
 redirect interface 100GE1/0/2
traffic policy p100GE1/0/1_pingmesh
 classifier c_pingmesh behavior b100GE1/0/1_pingmesh precedence 5
traffic policy p100GE1/0/2_pingmesh
 classifier c_pingmesh behavior b100GE1/0/2_pingmesh precedence 10
interface 100GE1/0/1
 traffic-policy p100GE1/0/1_pingmesh inbound
interface 100GE1/0/2
 traffic-policy p100GE1/0/2_pingmesh inbound
Total records : 2
--------------------------------------------------------------------------------
Policy Type/Name                Apply Parameter          Slot  State
--------------------------------------------------------------------------------
p100GE1/0/1_pingmesh              100GE1/0/1(IN)           1     success
p100GE1/0/2_pingmesh              100GE1/0/2(IN)           1     success
--------------------------------------------------------------------------------
```

- In the command output, if the value in the **State** column is **fail(***xxx***)** or another value other than **success**, the corresponding port fails to be configured. The following is an example. If the configuration fails, rectify the fault as prompted or contact technical support.

```
minisystem> pingmesh_switch_acl.py -i 192.168.0.1 -t 2 -u test
Switch password:
Log in to switch 51.36.141.248 success.
Switch info: board type=CE8850-64CQ-EI, version=V200R021C00SPC200, ACL_MODEL=0.
acl number 5501
 rule 15 permit l4-head 0x000012b7 0x0000ffff 0 0x64000000 0xff000000 8 0x22222222 0xffffffff 20
0xd19e6b08 0xffffffff 28
traffic classifier c_pingmesh type and
```

 Copyright © Huawei Technologies Co., Ltd.

```
 if-match acl 5501
traffic behavior b100GE1/0/1_pingmesh
 remark dscp 63
 redirect interface 100GE1/0/1
traffic behavior b100GE1/0/2_pingmesh
 remark dscp 63
 redirect interface 100GE1/0/2
traffic policy p100GE1/0/1_pingmesh
 classifier c_pingmesh behavior b100GE1/0/1_pingmesh precedence 5
traffic policy p100GE1/0/2_pingmesh
 classifier c_pingmesh behavior b100GE1/0/2_pingmesh precedence 10
interface 100GE1/0/1
 traffic-policy p100GE1/0/1_pingmesh inbound
interface 100GE1/0/2
 traffic-policy p100GE1/0/2_pingmesh inbound
Total records : 2
-------------------------------------------------------------------------------
Policy Type/Name                Apply Parameter          Slot  State
-------------------------------------------------------------------------------
p100GE1/0/1_pingmesh              100GE1/0/1(IN)           1     fail(3)
p100GE1/0/2_pingmesh              100GE1/0/2(IN)           1     fail(3)
-------------------------------------------------------------------------------
Fail reason:
  3 -- The numbers of matched conditions and actions in the traffic policy exceed the limit.
```

----End

5.5.3 Checking the cloud_vpc.ini File

Context

This section describes how to check the **cloud_vpc.ini** file, and how to create the file when it does not exist.

Procedure

Step 1 Run the following commands to check whether the **cloud_vpc.ini** file exists.

```
cd /opt/forApplication/system/
ls -l|grep cloud_vpc.ini
```

Step 2 If the **cloud_vpc.ini** file does not exist, run the following commands to create it for installing the EVS component.

```
mkdir -p /opt/forApplication/system
chmod 755 /opt/forApplication
chmod 755 /opt/forApplication/system
touch /opt/forApplication/system/cloud_vpc.ini
chmod 644 /opt/forApplication/system/cloud_vpc.ini
```

NOTE

The **cloud_vpc.ini** file must be created on each node.

----End

5.5.4 Enabling JBOD (Applicable to OceanStor Pacific 9540 Kunpeng-based, 9520 Kunpeng-based, 9920 Kunpeng-based, and 9340 Kunpeng-based)

To ensure that the disks on a node can be used properly, you need to configure the RAID controller cards to the RAID mode and enable the JBOD function when

 Copyright © Huawei Technologies Co., Ltd.

the node uses some RAID controller cards. For the RAID controller card models for which JBOD needs to be enabled, see **Huawei Storage Interoperability Navigator**.

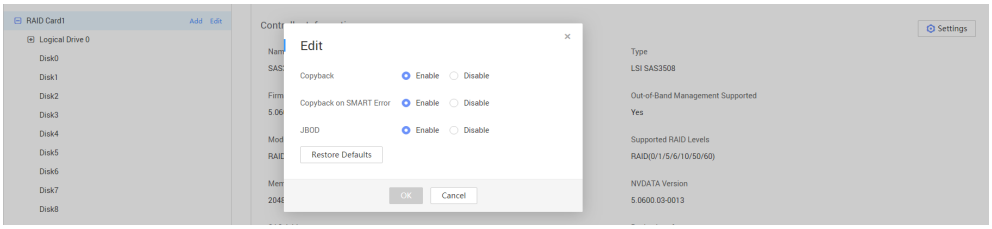
Procedure

Step 1 Log in to the iBMC system.

Step 2 Choose **System** > **Storage Management** and select the desired RAID controller card or PCIe card.

Step 3 Enable JBOD for the RAID controller card.

1. Click **Settings**.
2. Set **JBOD** to **Enable**.



----End

5.5.5 Configuring BIOS

5.5.5.1 Configuring BIOS (Applicable to OceanStor Pacific 9950, 9550, 9546, 9350, and 9346)

Procedure

Step 1 Enter the iBMC IP address in the address box of a browser to log in to the iBMC system of a node.

Step 2 Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

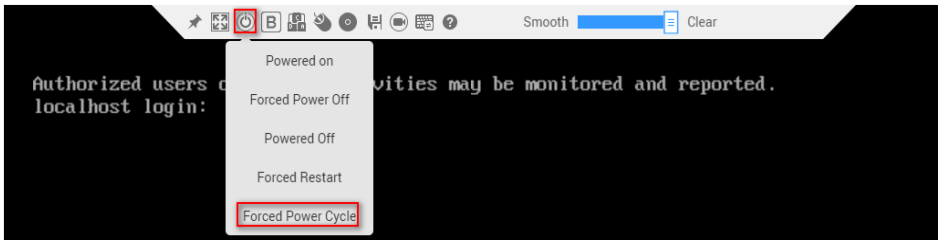
The **Confirm** dialog box is displayed. Read the information in the dialog box carefully, and then click **Yes**.

Step 3 Go to the BIOS configuration page.

1. Choose **Power Control** > **Forced Power Cycle** to forcibly start the node.

   NOTE

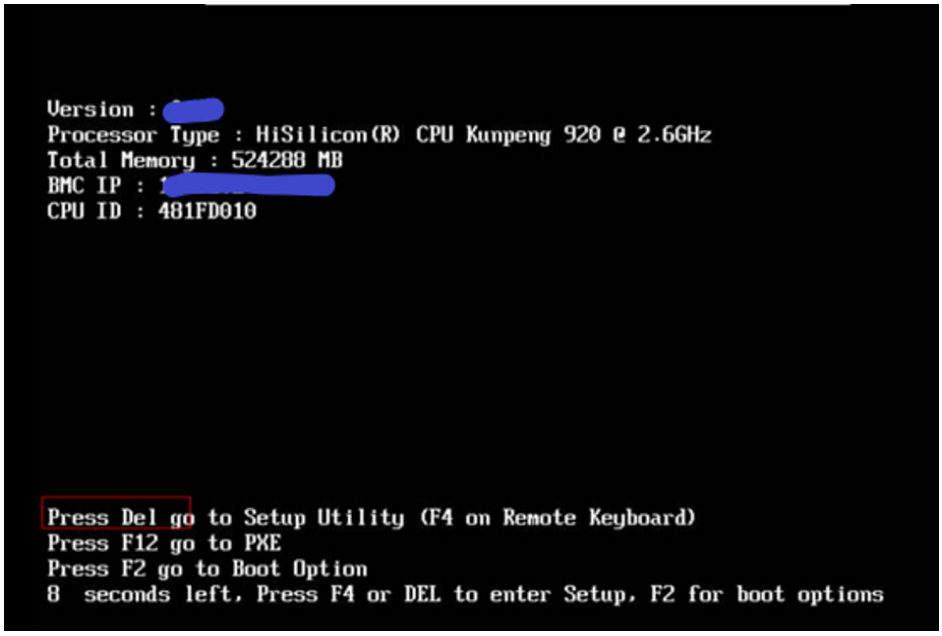
   The power-off process takes 1 to 2 minutes.



Copyright © Huawei Technologies Co., Ltd.

The **Confirm** dialog box is displayed. Read the information in the dialog box carefully, and then click **Yes**.

2. Press **Del** to enter the BIOS mode.



3. Set the BIOS password as prompted and enter the new password. If the password has been set, skip this step.

Step 4 Set **One Numa Per Socket** to **Enabled**.

CAUTION

After services are connected to the system, do not change the parameter values on the **Memory Config** page in the BIOS of a storage node. Otherwise, data in the battery-protected memory may be lost.

1. On the BIOS page, choose **Advanced** > **Memory Config**.
2. Set **NUMA** to **Enable**.
3. Set **One Numa Per Socket** to **Enabled**.

Step 5 Set BBU parameters.

CAUTION

After services are connected to the system, do not change the value of **NV Size** under **BBU Configuration** in the BIOS of a storage node. Otherwise, data in the battery-protected memory may be lost.

1. On the **Advanced** tab page, select **BBU Configuration**. The **BBU Configuration** window is displayed.
2. Set **NV Size**.
   - For OceanStor Pacific 9950, set the parameter to **32G**.

 Copyright © Huawei Technologies Co., Ltd.

- For other devices, set the parameter to **16G**.

3. Set **Back Up For Cpu Off** to **Enable**.
4. Set **Bbu Uce Enhance** to **Enable**.

Step 6 Press **F10** to save the settings and restart the system.

----End

5.5.5.2 Configuring BIOS (Applicable to OceanStor Pacific 9540 Kunpeng-based, 9520 Kunpeng-based, 9920 Kunpeng-based, and 9340 Kunpeng-based)

5.5.5.2.1 Configuring BIOS (Applicable to OceanStor Pacific 9520 Kunpeng-based 14-Slot and 9920 Kunpeng-based (Palm-sized NVMe SSD))

Procedure

Step 1 Enter the iBMC IP address in the address box of a browser to log in to the iBMC system of a node.

Step 2 Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

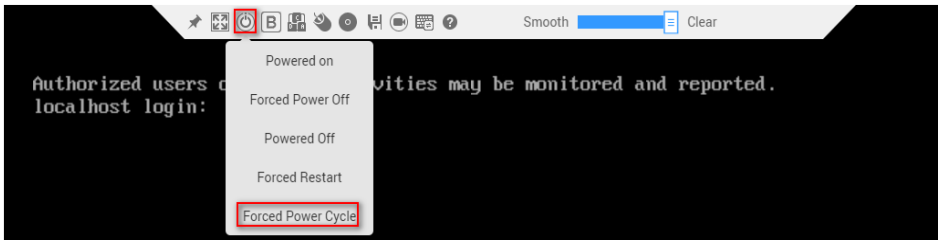
The **Confirm** dialog box is displayed. Read the information in the dialog box carefully, and then click **Yes**.

Step 3 Go to the BIOS configuration page.

1. Choose **Power Control** > **Forced Power Cycle** to forcibly start the node.

   NOTE

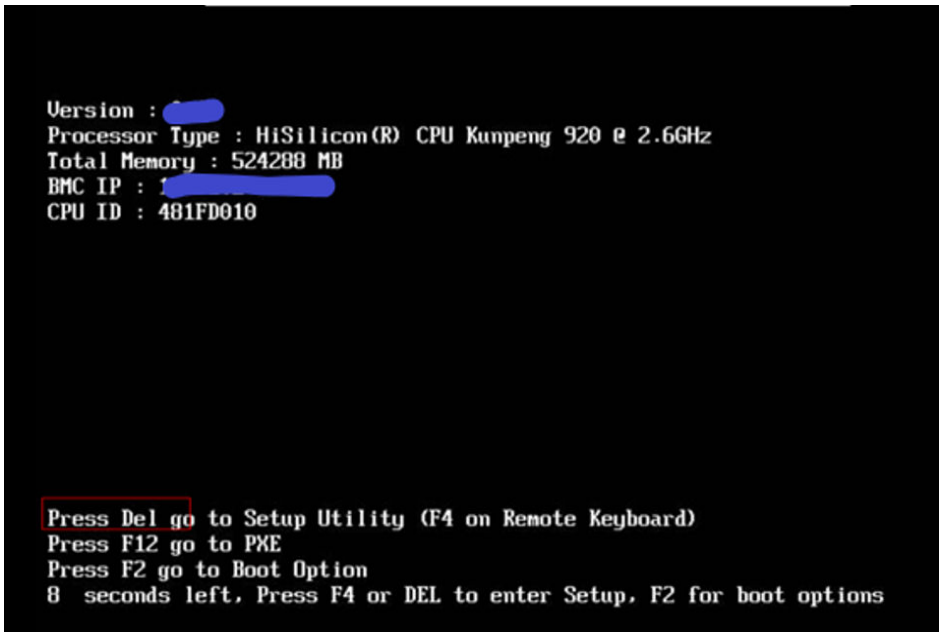
   The power-off process takes 1 to 2 minutes.

   The **Confirm** dialog box is displayed. Read the information in the dialog box carefully, and then click **Yes**.

2. Press **Del** to enter the BIOS mode.

Copyright © Huawei Technologies Co., Ltd.



3. Set the BIOS password as prompted and enter the new password. If the password has been set, skip this step.

Step 4 Set **One Numa Per Socket** to **Enabled**.

CAUTION

After services are connected to the system, do not change the parameter values on the **Memory Config** page in the BIOS of a storage node. Otherwise, data in the battery-protected memory may be lost.

1. On the BIOS page, choose **Advanced** > **Memory Config**.
2. Set **NUMA** to **Enable**.
3. Set **One Numa Per Socket** to **Enabled**.

Step 5 Set BBU parameters.

1. On the **Advanced** tab page, select **BBU Configuration**. The **BBU Configuration** window is displayed.
2. Set BBU parameters.

CAUTION

After services are connected to the system, do not change the value of **NV Size** under **BBU Configuration** in the BIOS of a storage node. Otherwise, data in the battery-protected memory may be lost.

a. Set **NV Size**.

- For OceanStor Pacific 9520 Kunpeng-based 14-slot, set the parameter to **16G**.

 Copyright © Huawei Technologies Co., Ltd.

- For OceanStor Pacific 9920 Kunpeng-based (palm-sized NVMe SSD), set the parameter to **32G**.

b. Set **Back Up For Cpu Off** to **Enable**.

c. Set **Back Up For Cpu Off** to **Disable**.

Step 6 Press **F10** to save the settings and restart the system.

----End

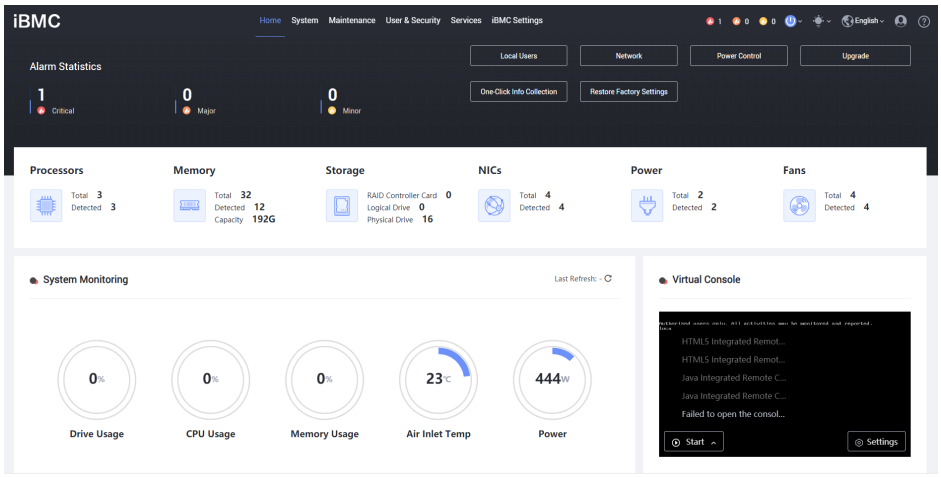
5.5.5.2.2 Configuring BIOS (Applicable to Other Kunpeng-based Devices)

Procedure

Step 1 Enter the iBMC IP address in the address box of a browser to log in to the iBMC system of a node.

Step 2 Go to the KVM page.

Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.



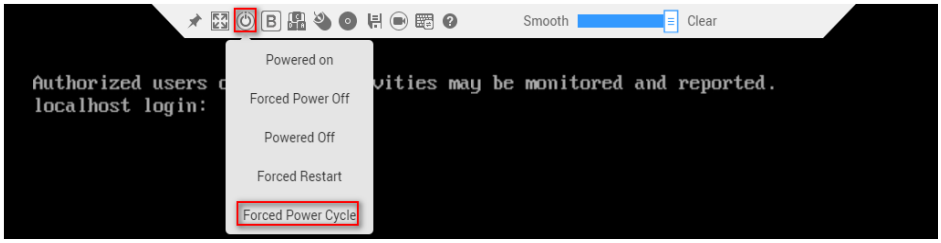
The **Confirm** dialog box is displayed. Read the information in the dialog box carefully, and then click **Yes**.

Step 3 Go to the BIOS configuration page.

1. Choose **Power Control** > **Forced Power Cycle** to forcibly start the node.

   NOTE

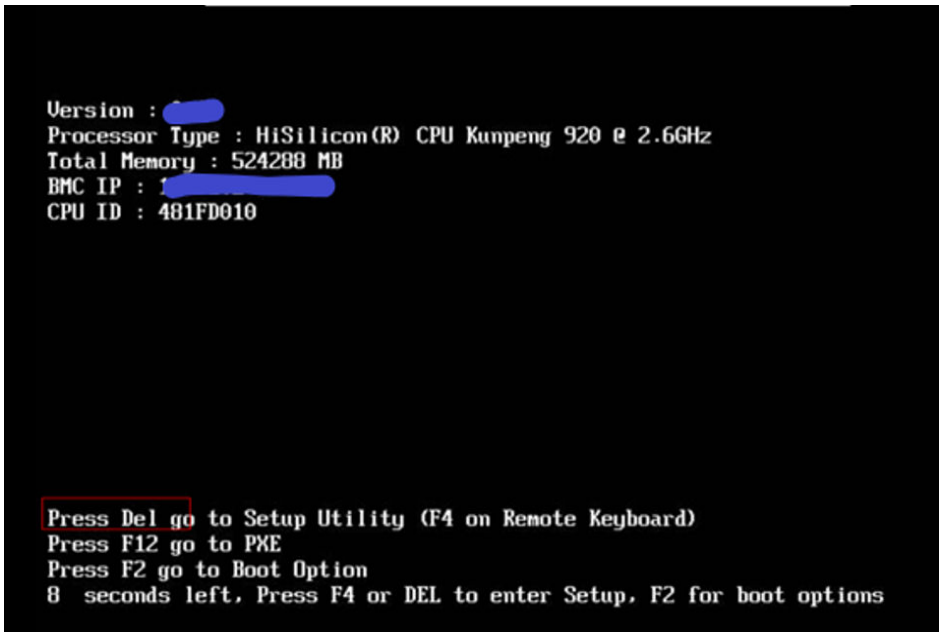
   The power-off process takes 1 to 2 minutes.



The **Confirm** dialog box is displayed. Read the information in the dialog box carefully, and then click **Yes**.

 Copyright © Huawei Technologies Co., Ltd.

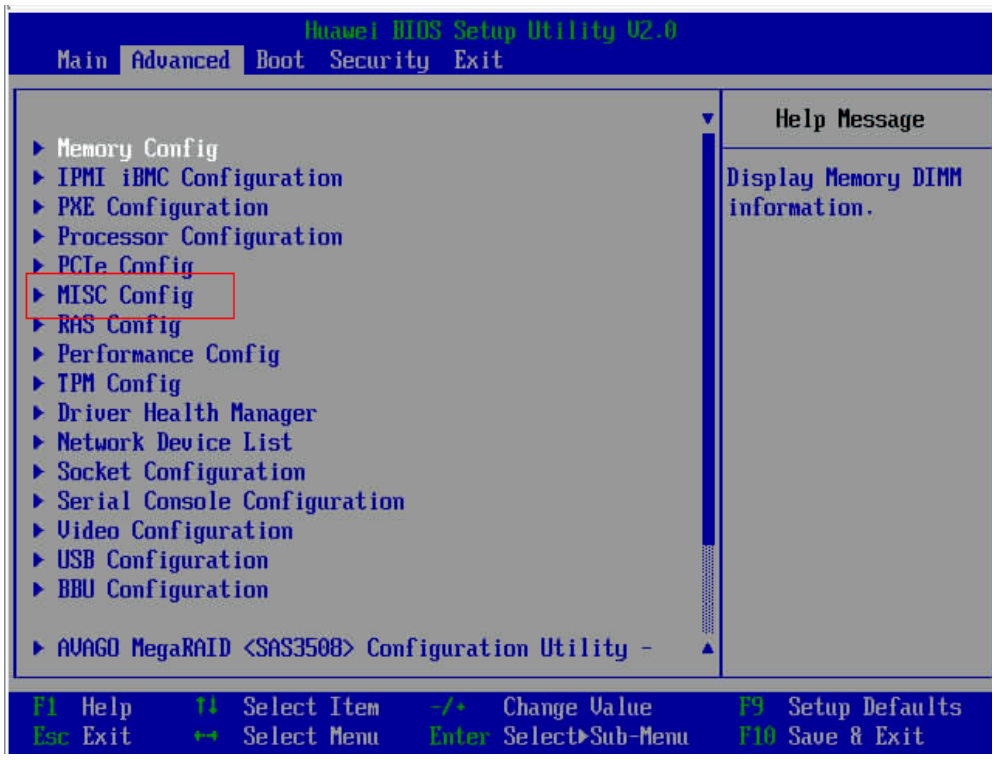
2. Press **Del** to enter the BIOS mode.



3. Set the BIOS password as prompted and enter the new password. If the password has been set, skip this step.

Step 4 Set parameters under **MISC Config**.

1. Click the **Advanced** tab and select **MISC Config**. The **MISC Config** page is displayed.



2. Set **Support Smmu** to **Disabled**.
3. Set **Kaslr Support** to **Disabled**.

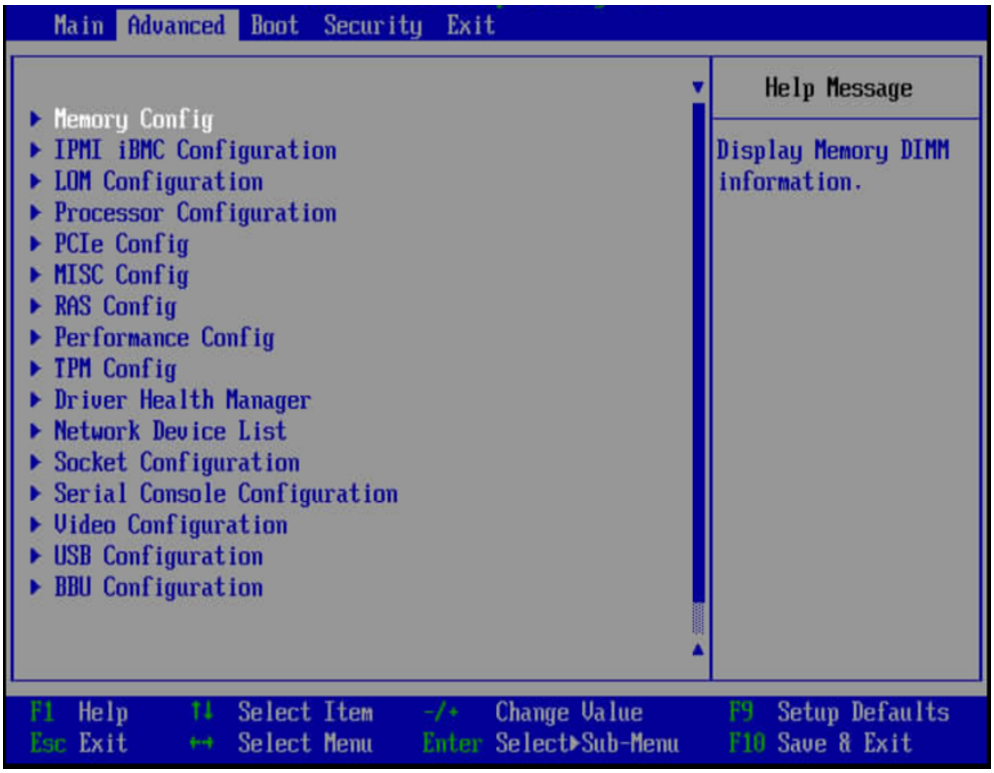
 Copyright © Huawei Technologies Co., Ltd.

Step 5 Set parameters under **Memory Config**.

1. Click the **Advanced** tab and select **Memory Config**. The **Memory Config** page is displayed.

CAUTION

After services are connected to the system, do not change the parameter values on the **Memory Config** page in the BIOS of a storage node. Otherwise, data in the battery-protected memory may be lost.



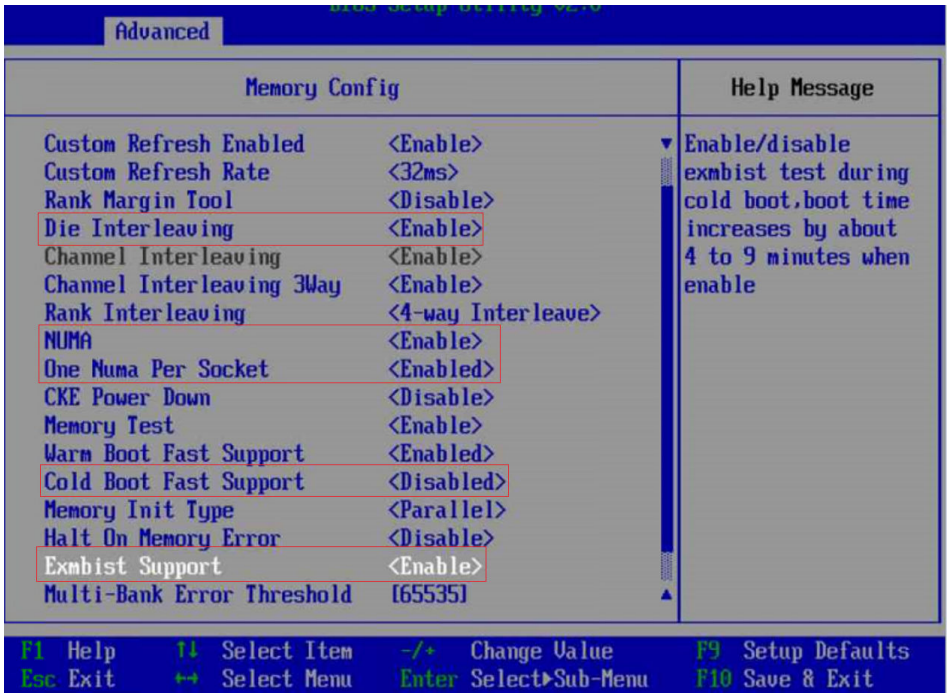
2. Set parameters under **Memory Config**.
   a. Set **Die Interleaving** to **Enable**.
   b. Set **NUMA** to **Enable**.
   c. Set **One Numa Per Socket** to **Enabled**.

      NOTE

      If a device uses a 32-core CPU, you do not need to set the **One Numa Per Socket** parameter. To query the number of CPU cores, log in to the iBMC WebUI and choose **System** > **System Info** > **Processors** > **Cores/Threads**.

   d. Set **Cold Boot Fast Support** to **Disabled**.
   e. Set **Exmbist Support** to **Enable**.

 Copyright © Huawei Technologies Co., Ltd.



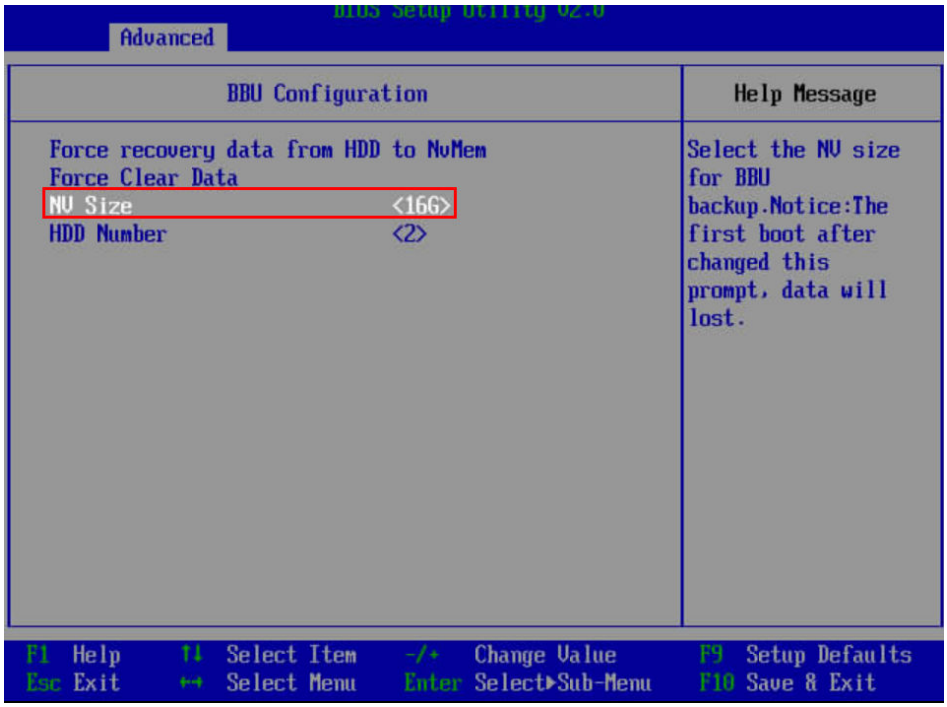
Step 6 Set **NV Size**.

CAUTION

After services are connected to the system, do not change the value of **NV Size** under **BBU Configuration** in the BIOS of a storage node. Otherwise, data in the battery-protected memory may be lost.

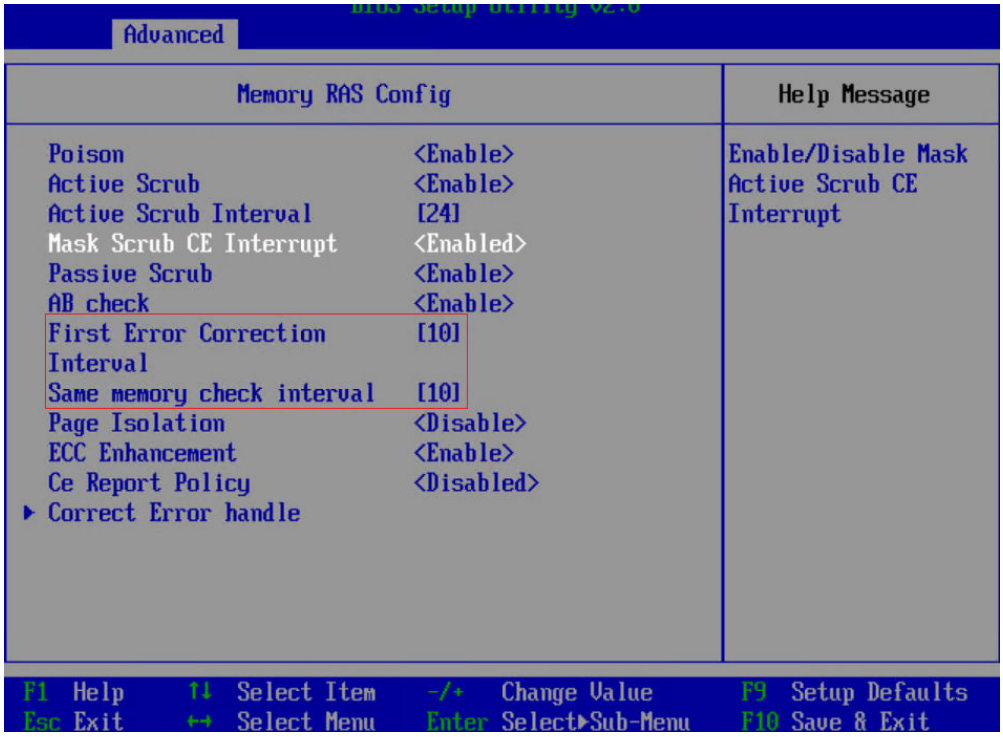
1. On the BIOS page, choose **Advanced** > **BBU Configuration**.
2. Set **NV Size** to **16G**.

 Copyright © Huawei Technologies Co., Ltd.



Step 7 Set parameters under **Memory RAS Config**.

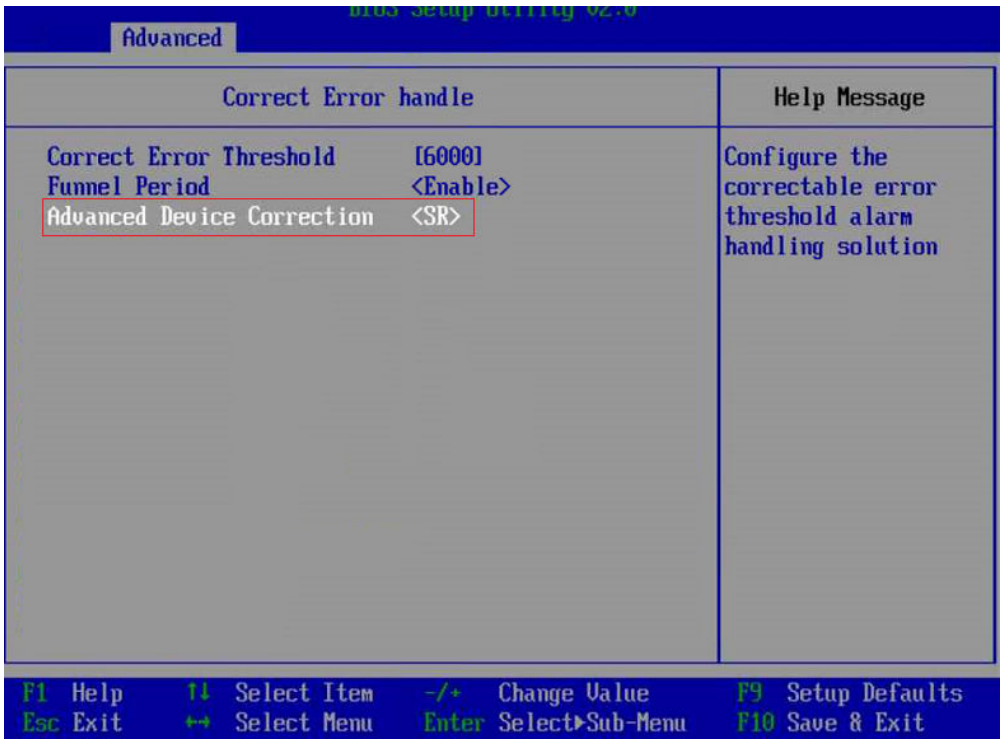
1. On the **Advanced** tab page, choose **RAS Config** > **Memory RAS Config**.
2. Set **AB check** to **Enable**.
3. Set **Mask Scrub CE Interrupt** to **Enabled**.
4. If the following options are displayed, retain the default values.



Step 8 Set **Advanced Device Correction**.

 Copyright © Huawei Technologies Co., Ltd.

1. On the **Advanced** tab page, choose **RAS Config** > **Memory RAS Config** > **Correct Error handle**.
2. Set **Advanced Device Correction** to **SR**.



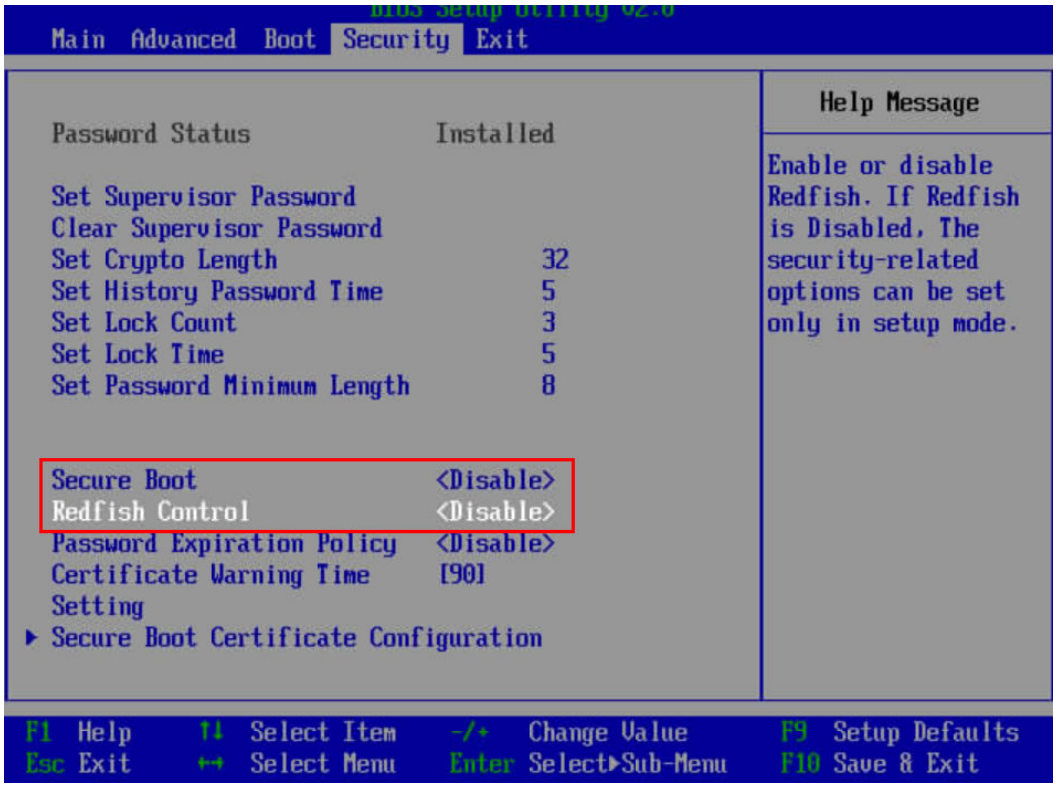
Step 9 Modify secure boot and Redfish Control.

1. Click the **Security** tab.
2. Set **Secure Boot** to **Disable**.

   NOTE

   If an SP686C-M-16i or SP686C-M-40i RAID controller card is configured for a device, set **Secure Boot** to **Enable**.
3. Set **Redfish Control** to **Disable**.

 Copyright © Huawei Technologies Co., Ltd.



Step 10 Press **F10** to save the settings and restart the system.

----End

5.5.6 Installing OSs for Storage Nodes

5.5.6.1 Installing an OS (Applicable to OceanStor Pacific 9950, 9550, 9546, 9350, and 9346)

Prerequisites

- You have obtained the OS image installation package by referring to *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.
- You have disabled the firewall of the installation PC.
- You have obtained the user name and password of a node, such as the iBMC user.
- You have obtained the iBMC IP addresses of the node.

Precautions

- The language of the OS must be English.
- During the installation, do not disconnect the remote connection between the mounted image and the KVM. Otherwise, the OS cannot be installed. If the connection is disconnected, you need to reinstall the OS.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the iBMC system of a node.

Step 2 Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

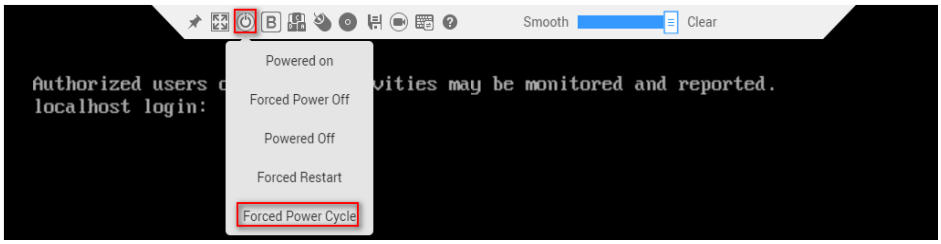
The **Confirm** dialog box is displayed. Read the information in the dialog box carefully, and then click **Yes**.

Step 3 Go to the BIOS configuration page.

1. Choose **Power Control** > **Forced Power Cycle** to forcibly start the node.

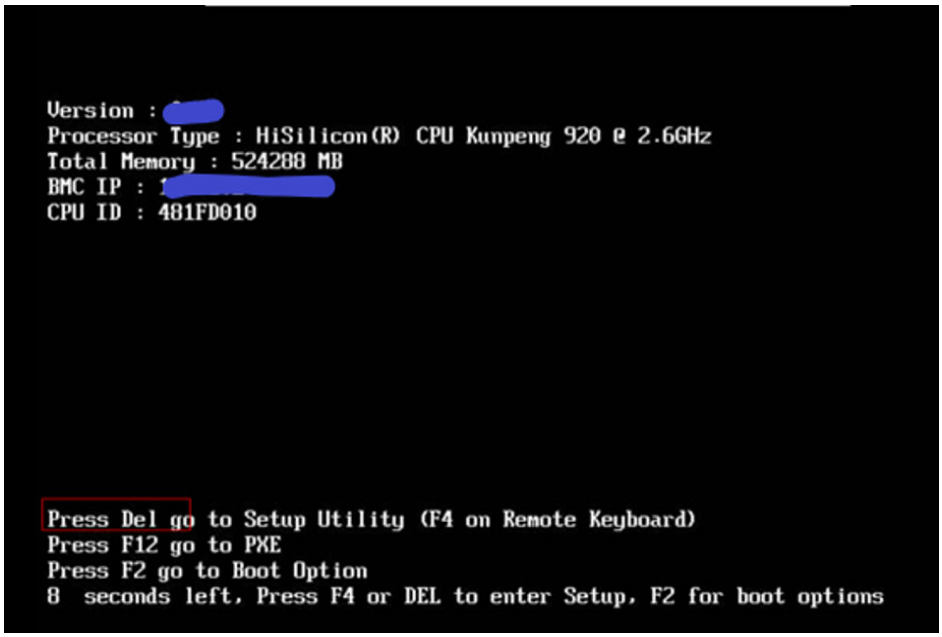
   NOTE

   The power-off process takes 1 to 2 minutes.

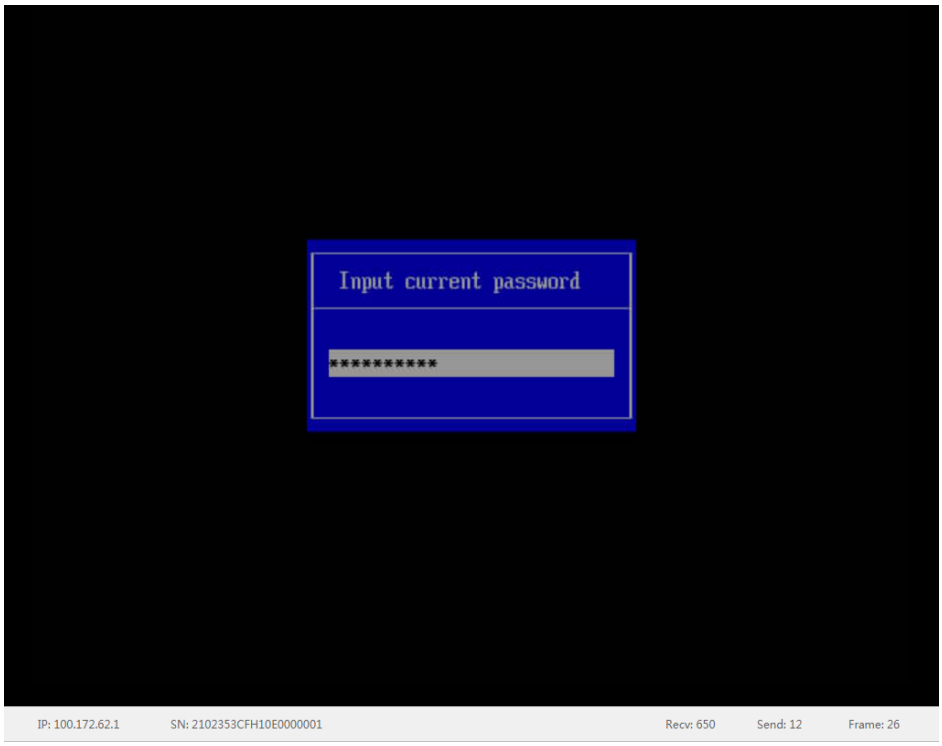
   The **Confirm** dialog box is displayed. Read the information in the dialog box carefully, and then click **Yes**.

2. Press **Del** to enter the BIOS mode.

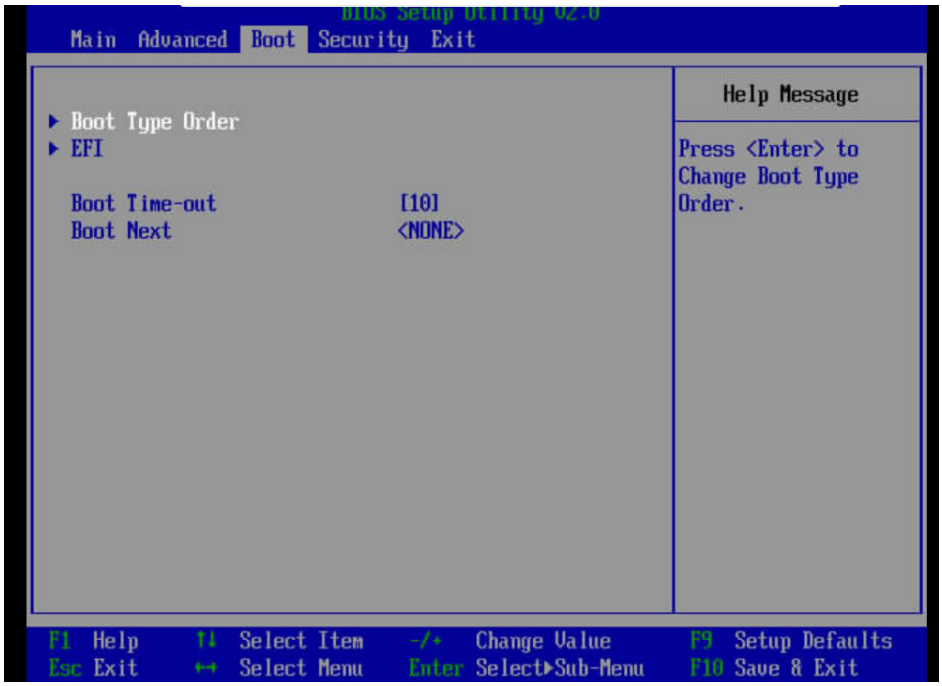
   

3. Enter the set BIOS password and press **Enter**.

 Copyright © Huawei Technologies Co., Ltd.



4. Set the preferred boot mode.
   a. On the **Boot** tab, select **Boot Type Order** and press **Enter**.

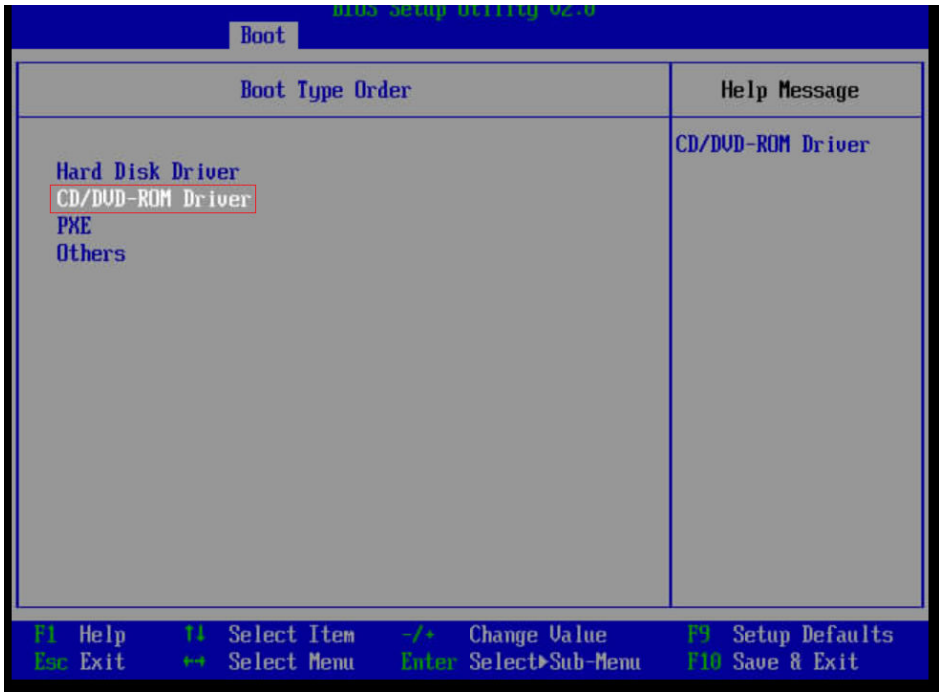


   b. Set **CD/DVD-ROM Driver** as the preferred boot mode.

      NOTE

      Change the boot order with **-** (down) or **Shift+** (up).

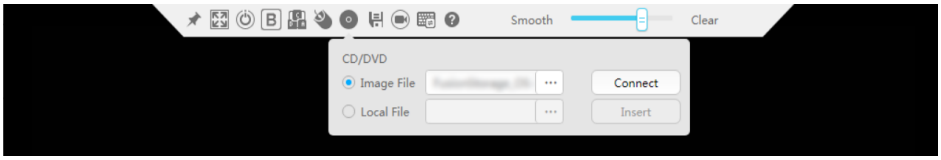
 Copyright © Huawei Technologies Co., Ltd.



5. Press **F10** to save the settings and restart the system.

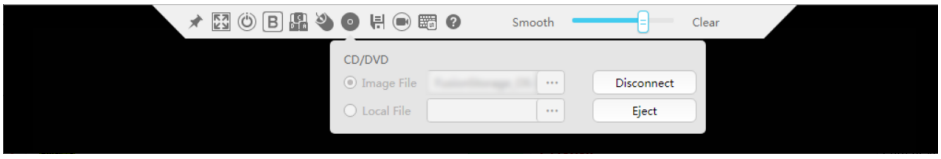
Step 4 Mount an image.

1. Select **Image File**, click ***, and select an ISO image file.

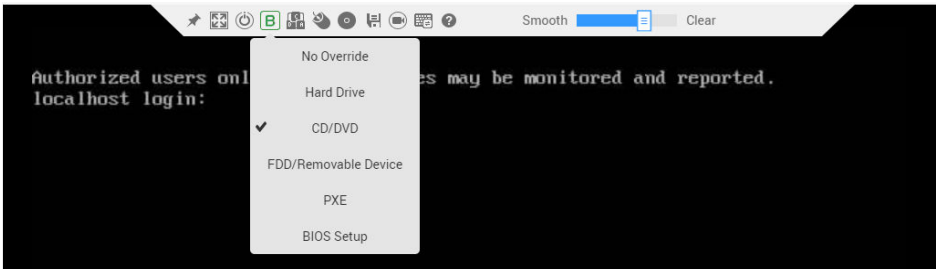


2. Click **Connect**.

   If **Disconnect** is displayed, the connection is successful.



Step 5 Set the system boot options. Select **CD/DVD**.



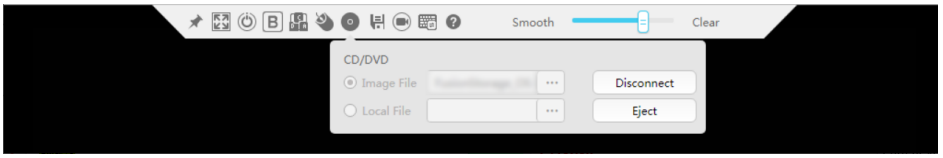
Step 6 On the KVM page, click and select **Forced Power Cycle**. Wait for the system to automatically install the OS.

 Copyright © Huawei Technologies Co., Ltd.

The **Confirm** dialog box is displayed. Read the information in the dialog box carefully, and then click **Yes**.

During the startup, Select **Install EulerOS** *XXX* **with text mode** to install the OS.

1. The system automatically installs the OS. After the installation is complete, the system automatically restarts.
2. After the system restarts, click **Disconnect** to disconnect the image.



3. After the system automatically restarts, log in to the system as user **root**. After the login, change the default password. Then run the **reboot** command. All system configurations take effect after the system is restarted.

   NOTE

   To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)* or *OceanStor Pacific Series 8.2.1 Account List (Block Service)*.

Step 7 (Optional) Configure the time zone.

NOTE

- For Chinese mainland, the default time zone is Shanghai. You do not need to manually configure the time zone.
- For regions outside Chinese mainland, you need to manually set the time zone to the local time.

1. Run the following command and select the time zone to be set, as shown in **Figure 5-32**.

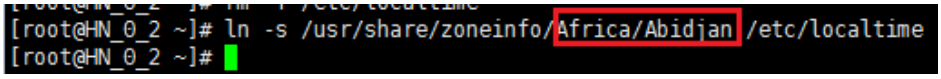
```
tzselect
```

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-32 Selecting a time zone

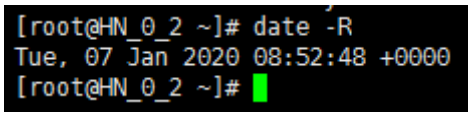
2. Run the following command to delete the default time zone.
   ```
   rm -f /etc/localtime
   ```
3. Run the following command to set the time zone to the target time zone, as shown in **Figure 5-33**.
   ```
   ln -s /usr/share/zoneinfo/Target time zone /etc/localtime
   ```

Figure 5-33 Setting the time zone



4. Run the following command to check whether the time zone is set correctly, as shown in **Figure 5-34**.
   ```
   date -R
   ```

Figure 5-34 Checking the time zone



----End

5.5.6.2 Installing an OS (Applicable to OceanStor Pacific 9520 Kunpeng-based Without a RAID Controller Card, 9540 Kunpeng-based Without a RAID Controller Card, 9920 Kunpeng-based Without a RAID Controller Card, and 9340 Kunpeng-based Without a RAID Controller Card)

5.5.6.2.1 Installing an OS (Applicable to OceanStor Pacific 9520 Kunpeng-based 14-Slot Without a RAID Controller Card and 9920 Kunpeng-based (Palm-sized NVMe SSD) Without a RAID Controller Card)

Prerequisites

- You have obtained the OS image installation package by referring to *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.
- You have disabled the firewall of the installation PC.
- You have obtained the user name and password of a node, such as the iBMC user.
- You have obtained the iBMC IP addresses of the node.

Precautions

- The language of the OS must be English.
- During the installation, do not disconnect the remote connection between the mounted image and the KVM. Otherwise, the OS cannot be installed. If the connection is disconnected, you need to reinstall the OS.

Procedure

Step 1 Log in to the iBMC system of a node.

Step 2 Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

The **Confirm** dialog box is displayed. Read the information in the dialog box carefully, and then click **Yes**.

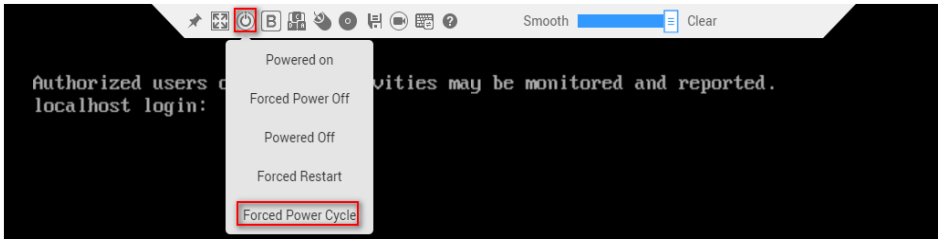
Step 3 Go to the BIOS configuration page.

1. Choose **Power Control** > **Forced Power Cycle** to forcibly start the node.

   NOTE

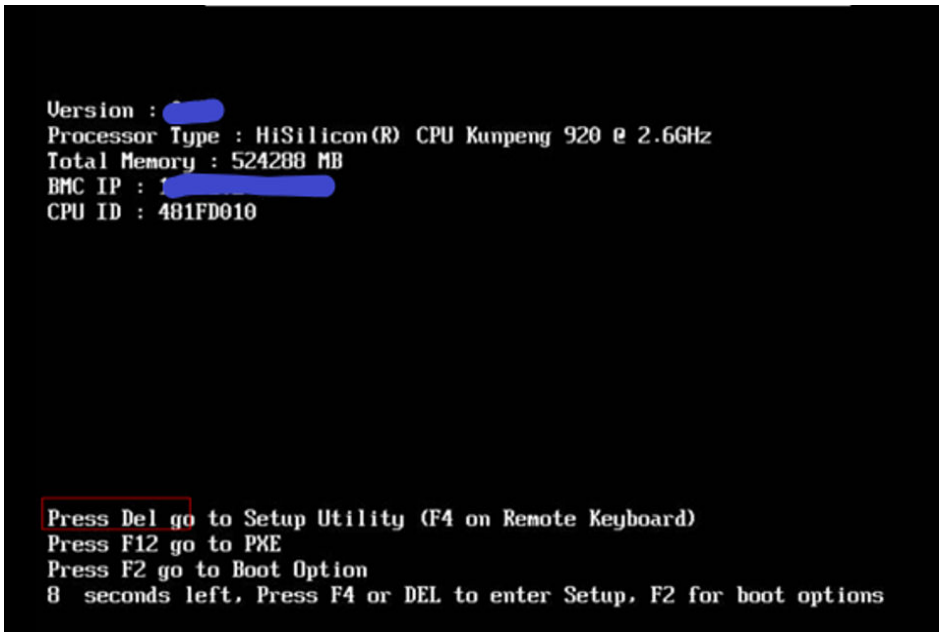
   The power-off process takes 1 to 2 minutes.

 Copyright © Huawei Technologies Co., Ltd.



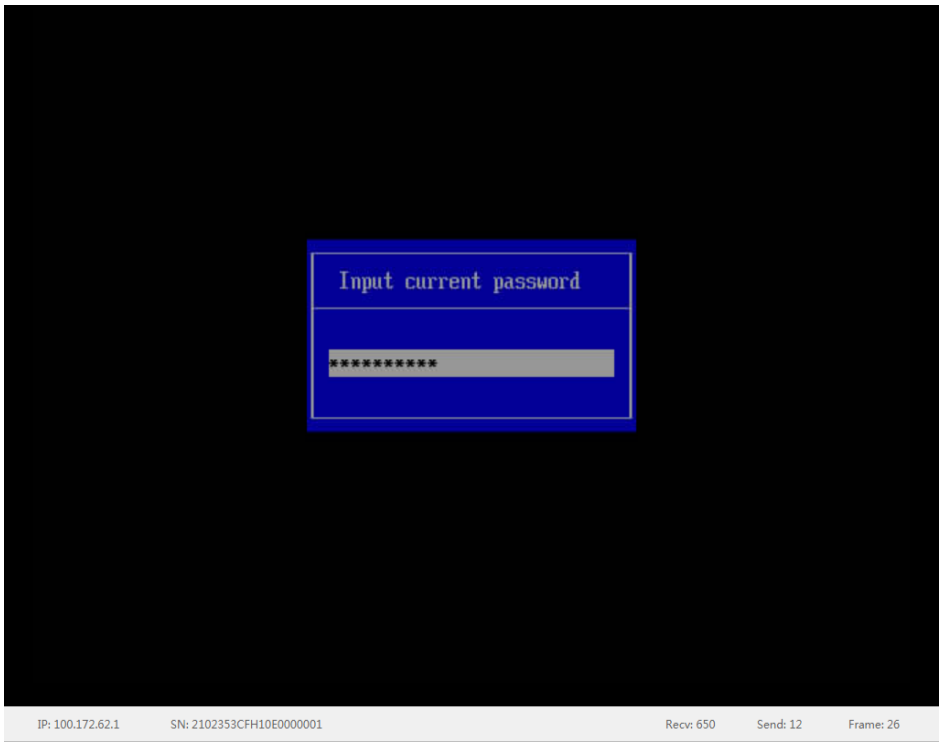
The **Confirm** dialog box is displayed. Read the information in the dialog box carefully, and then click **Yes**.

2. Press **Del** to enter the BIOS mode.

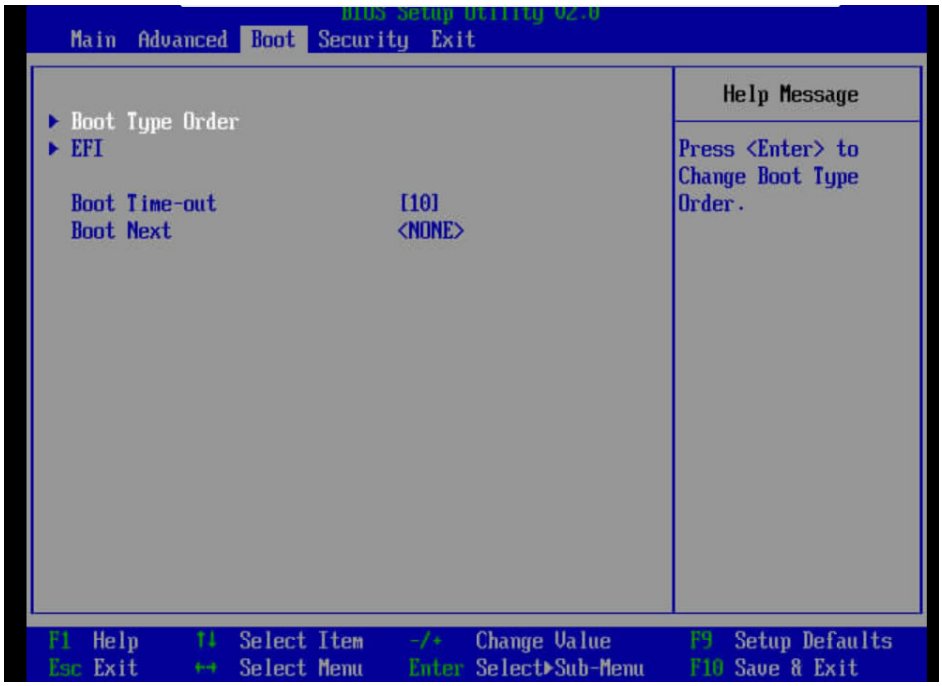


3. Enter the set BIOS password and press **Enter**.

 Copyright © Huawei Technologies Co., Ltd.



4. Set the preferred boot mode.
   a. On the **Boot** tab, select **Boot Type Order** and press **Enter**.

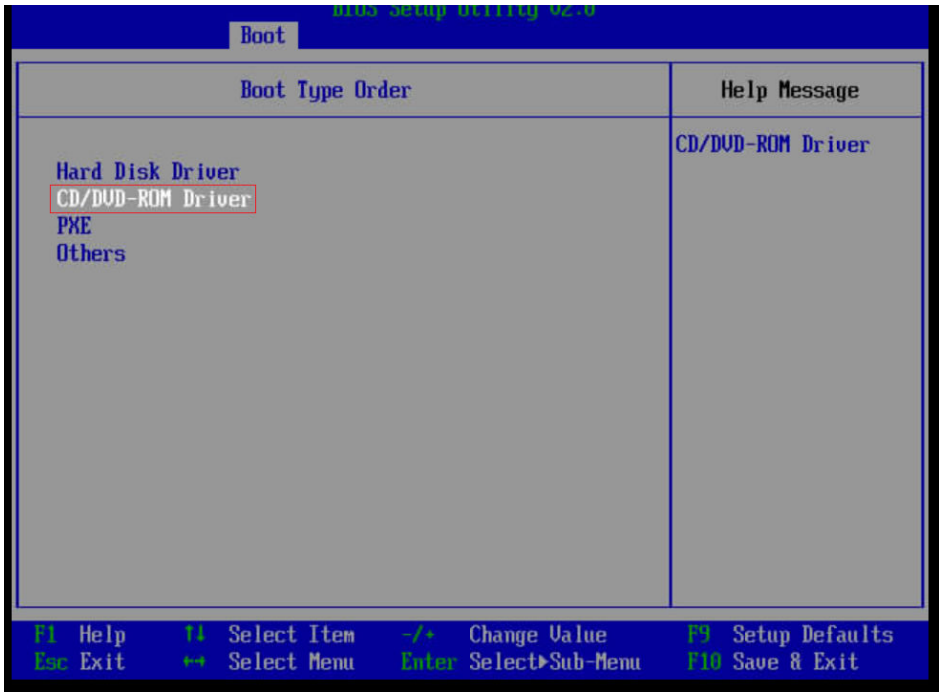


   b. Set **CD/DVD-ROM Driver** as the preferred boot mode.

      NOTE

      Change the boot order with **-** (down) or **Shift+** (up).

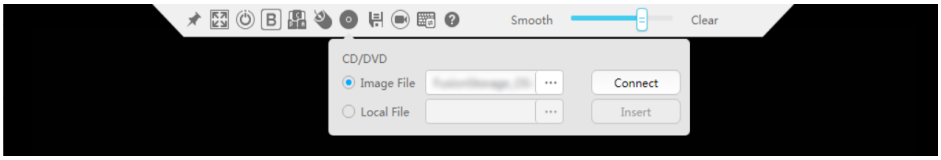
 Copyright © Huawei Technologies Co., Ltd.



5. Press **F10** to save the settings and restart the system.

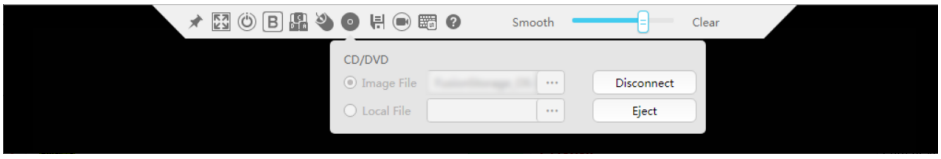
Step 4 Mount an image.

1. Select **Image File**, click ***, and select an ISO image file.

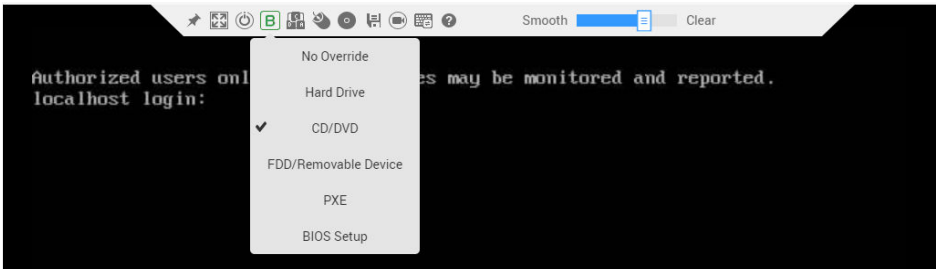


2. Click **Connect**.

   If **Disconnect** is displayed, the connection is successful.



Step 5 Set the system boot options. Select **CD/DVD**.



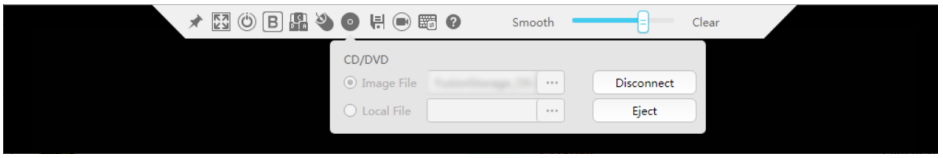
Step 6 On the KVM page, click and select **Forced Power Cycle**. Wait for the system to automatically install the OS.

 Copyright © Huawei Technologies Co., Ltd.

The **Confirm** dialog box is displayed. Read the information in the dialog box carefully, and then click **Yes**.

During the startup, Select **Install EulerOS** *XXX* **with text mode** to install the OS.

1. The system automatically installs the OS. After the installation is complete, the system automatically restarts.
2. After the system restarts, click **Disconnect** to disconnect the image.



3. After the system automatically restarts, log in to the system as user **root**. After the login, change the default password. Then run the **reboot** command. All system configurations take effect after the system is restarted.

   NOTE

   To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)* or *OceanStor Pacific Series 8.2.1 Account List (Block Service)*.

Step 7 (Optional) Configure the time zone.

NOTE

- For Chinese mainland, the default time zone is Shanghai. You do not need to manually configure the time zone.
- For regions outside Chinese mainland, you need to manually set the time zone to the local time.

1. Run the following command and select the time zone to be set, as shown in **Figure 5-35**.

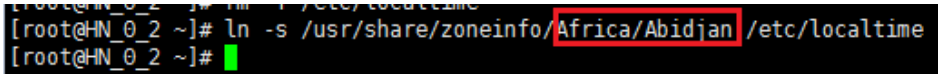
```
tzselect
```

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-35 Selecting a time zone

2. Run the following command to delete the default time zone.
   ```
   rm -f /etc/localtime
   ```
3. Run the following command to set the time zone to the target time zone, as shown in **Figure 5-36**.
   ```
   ln -s /usr/share/zoneinfo/Target time zone /etc/localtime
   ```

Figure 5-36 Setting the time zone



4. Run the following command to check whether the time zone is set correctly, as shown in **Figure 5-37**.
   ```
   date -R
   ```

Figure 5-37 Checking the time zone

```
[root@HN_0_2 ~]# date -R
Tue, 07 Jan 2020 08:52:48 +0000
[root@HN_0_2 ~]#
```

----End

5.5.6.2.2 Installing an OS (Applicable to Other Kunpeng-based Models Without a RAID Controller Card)

Prerequisites

- You have obtained the OS image installation package by referring to *OceanStor Pacific Series 8.2.1RC1 Version Mapping*.
- You have disabled the firewall of the installation PC.
- You have obtained the user name and password of a node, such as the iBMC user.
- You have obtained the iBMC IP addresses of the node.

Precautions

During the installation, do not disconnect the remote connection between the mounted image and the KVM. Otherwise, the OS cannot be installed. If the connection is disconnected, you need to reinstall the OS.

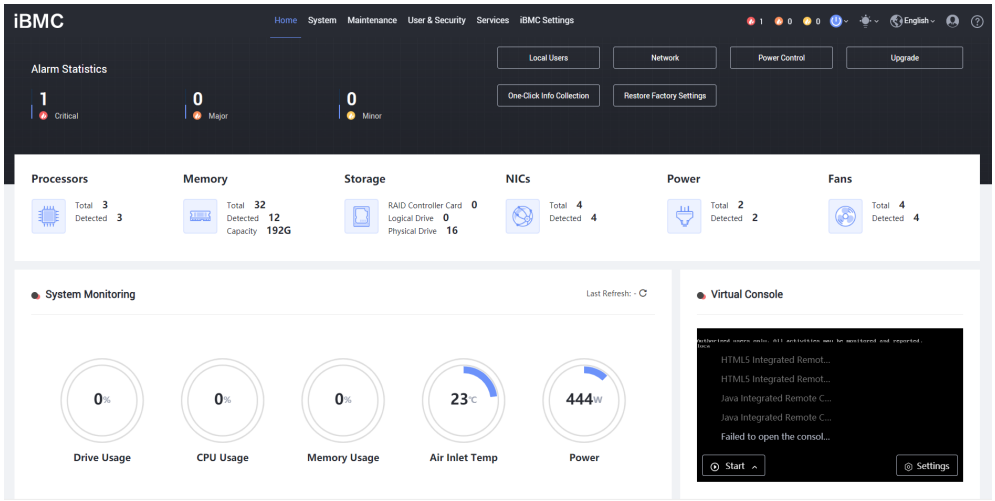
NOTICE

The language of the OS must be English.

Procedure

Step 1 Log in to the iBMC system of a node.

Step 2 Go to the **Home** page. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.



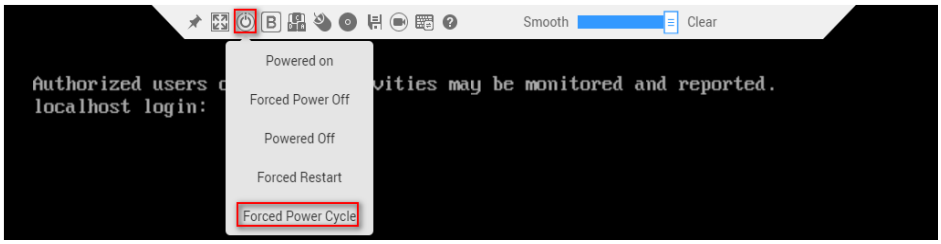
The **Confirm** dialog box is displayed. Read the information in the dialog box carefully, and then click **Yes**.

Step 3 Go to the BIOS configuration page.

1. Choose **Power Control** > **Forced Power Cycle** to forcibly start the node.

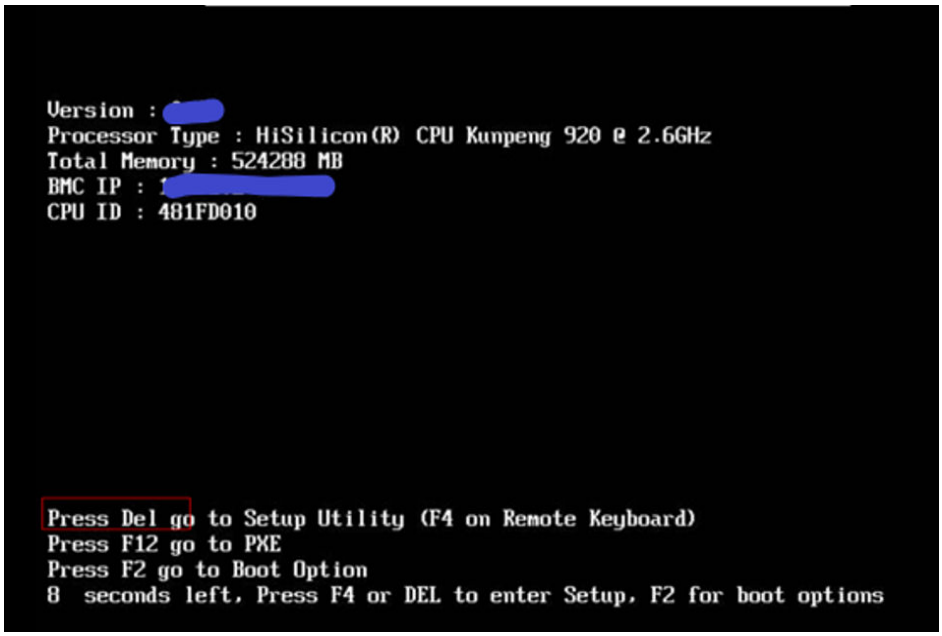
   NOTE

   The power-off process takes 1 to 2 minutes.

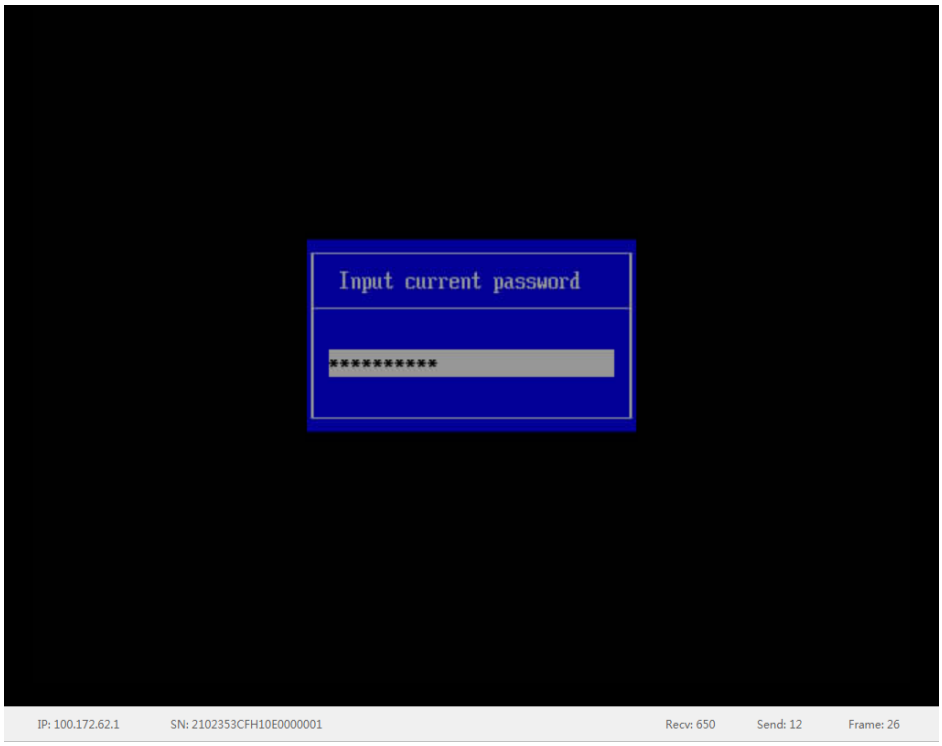
   The **Confirm** dialog box is displayed. Read the information in the dialog box carefully, and then click **Yes**.

2. Press **Del** to enter the BIOS mode.

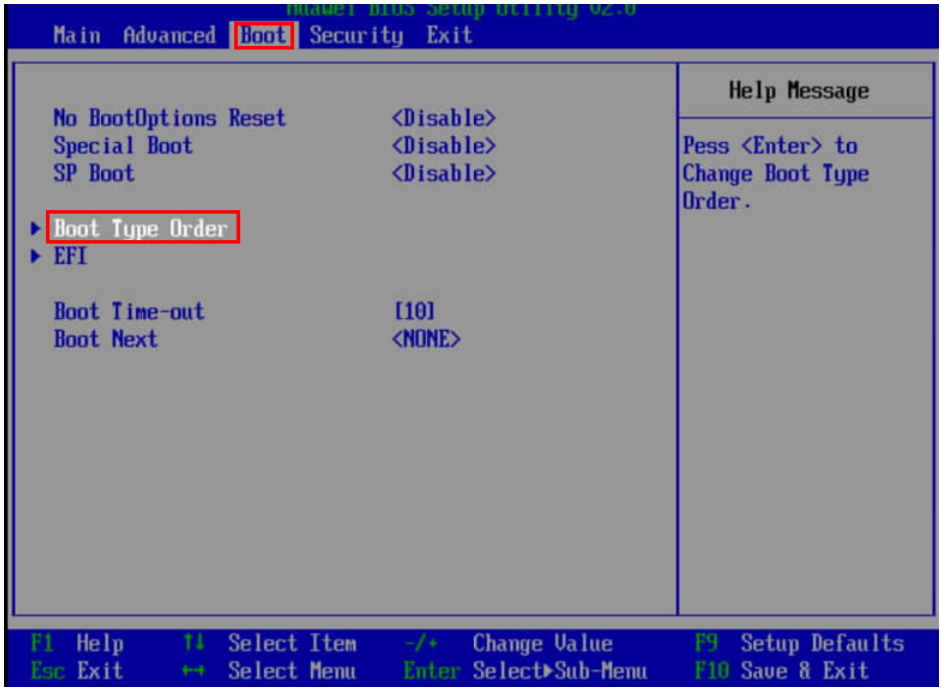
   

3. Enter the set BIOS password and press **Enter**.

 Copyright © Huawei Technologies Co., Ltd.



4. On the **Boot** tab, select **Boot Type Order** and press **Enter**.

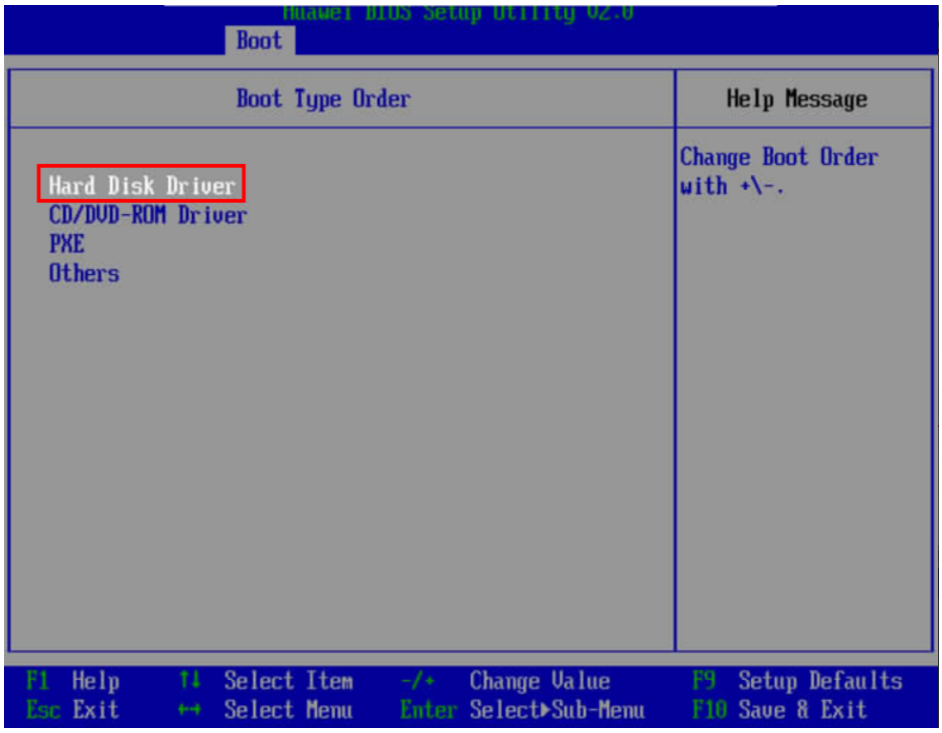


5. Set **Hard Disk Driver** as the preferred boot mode.

NOTE

Change the boot order with **-** (down) or **Shift+** (up).

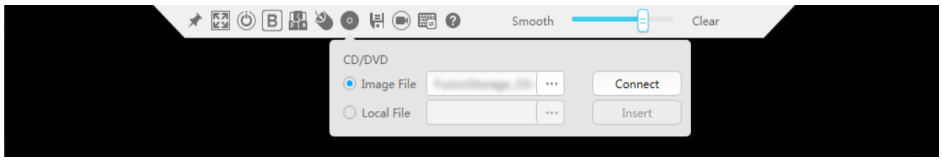
 Copyright © Huawei Technologies Co., Ltd.



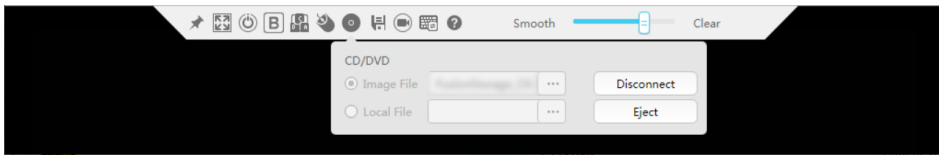
6. Select the **Security** tab and set **SecureBoot** to **Disabled**.
7. Press **F10** to save the settings and restart the system.

Step 4 Mount an image.

1. Select **Image File**, click ***, and select an ISO image file.

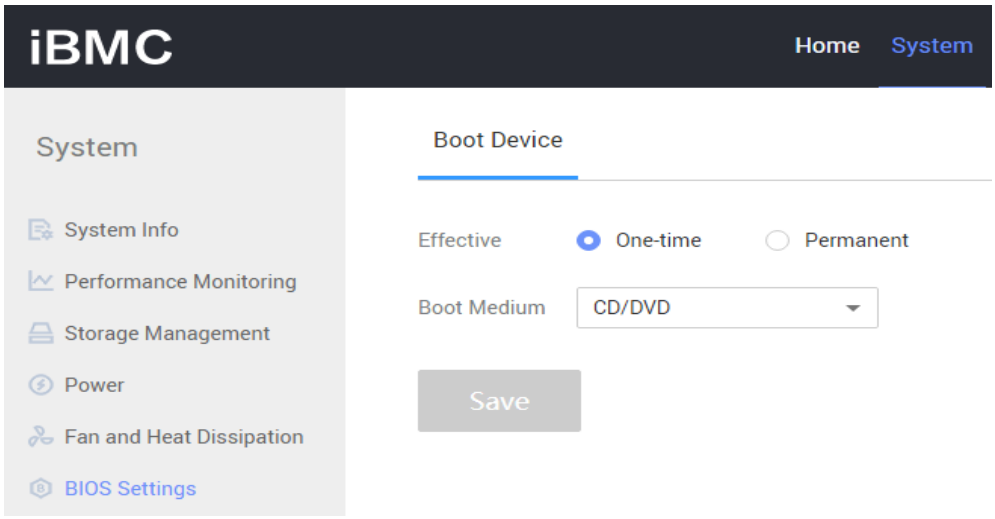


2. Click **Connect**.
   If **Disconnect** is displayed, the connection is successful.



Step 5 Set the system boot options.

 Copyright © Huawei Technologies Co., Ltd.



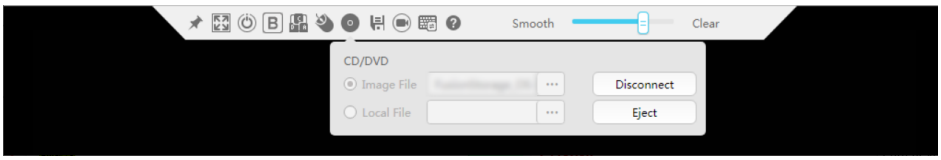
1. On the iBMC WebUI, choose **System** > **BIOS Settings**.
2. Set **Effective** to **One-time** and **Boot Medium** to **CD/DVD**, and then click **Save**.

Step 6 On the KVM page, click and select **Forced Power Cycle**. Wait for the system to automatically install the OS.

The **Confirm** dialog box is displayed. Read the information in the dialog box carefully, and then click **Yes**.

During the startup, Select **Install EulerOS** *XXX* **with text mode** to install the OS.

1. The system automatically installs the OS. After the installation is complete, the system automatically restarts.
2. After the system restarts, click **Disconnect** to disconnect the image.



3. After the system automatically restarts, log in to the system as user **root**. After the login, change the default password. Then run the **reboot** command. All system configurations take effect after the system is restarted.

   NOTE

   To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)* or *OceanStor Pacific Series 8.2.1 Account List (Block Service)*.

Step 7 (Optional) Configure the time zone.

NOTE

- For Chinese mainland, the default time zone is Shanghai. You do not need to manually configure the time zone.
- For regions outside Chinese mainland, you need to manually set the time zone to the local time.

 Copyright © Huawei Technologies Co., Ltd.

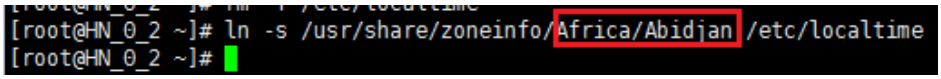
1. Run the following command and select the time zone to be set, as shown in **Figure 5-38**.
```
tzselect
```

Figure 5-38 Selecting a time zone

2. Run the following command to delete the default time zone.
```
rm -f /etc/localtime
```
3. Run the following command to set the time zone to the target time zone, as shown in **Figure 5-39**.
```
ln -s /usr/share/zoneinfo/Target time zone /etc/localtime
```

 Copyright © Huawei Technologies Co., Ltd.

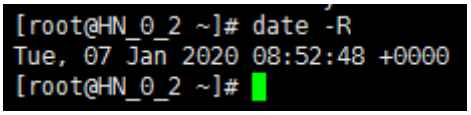
Figure 5-39 Setting the time zone



4. Run the following command to check whether the time zone is set correctly, as shown in **Figure 5-40**.

```
date -R
```

Figure 5-40 Checking the time zone



----End

5.5.6.3 Installing an OS (Applicable to OceanStor Pacific 9520 Kunpeng-based with a RAID Controller Card, 9540 Kunpeng-based with a RAID Controller Card, 9920 Kunpeng-based with a RAID Controller Card, and 9340 Kunpeng-based with a RAID Controller Card)

5.5.6.4 Installing a Third-Party OS

This section describes how to install a third-party OS on a node.

NOTICE

The language of the OS must be English.

Prerequisites

The OS type and version must meet the compatibility requirements. For details, see **Huawei Storage Interoperability Navigator**.

Installing the OS

For details about how to install a third-party OS, see its official website.

OS Partition Requirements

The following describes the OS partition requirements. For management nodes, create OS partitions by referring to **Table 5-60**. For storage nodes, create OS partitions by referring to **Table 5-61**.

NOTE

If the management node and storage node are deployed on the same node, create OS partitions on the node based on **Table 5-61**.

Copyright © Huawei Technologies Co., Ltd.

Table 5-60 Management node partition requirements

Mount Point	Recommended Partition Size (GB)	Description
/	10	Indicates the system root directory.
/boot	0.4	Indicates the file used by the kernel of the OS in the boot process.
/boot/efi	0.3	This partition is required for the node that uses EFI BIOS.
/usr	5	Indicates the directory used to store system programs.
/opt	• 3 to 128 storage nodes: 60 • 129 to 256 storage nodes: 120 • 257 to 4096 storage nodes: 260	Indicates the directory used to store third-party software.
/tmp	2	Indicates the directory used to store temporary files generated by users or running programs.
/var	5	Indicates the directory used to store changed data during system running.
/var/log	10	Indicates the log partition.
NOTE You must use independent partitions for **/boot** and **/boot/efi**, and you are advised to use LVM logical partitions for other partitions.		

Table 5-61 Storage node partition requirements

Mount Point	Recommended Partition Size (GB)	Description
/	20	Indicates the system root directory.
/home	10	Indicates the default **home** directory of a user. When a user is added, the **home** directory of the user is stored in this directory.
/boot	0.4	Indicates the file used by the kernel of the OS in the boot process.
/boot/efi	0.3	This partition is required for the node that uses EFI BIOS.

 Copyright © Huawei Technologies Co., Ltd.

Mount Point	Recommended Partition Size (GB)	Description
/usr	20	Indicates the directory used to store system programs.
/opt	100	Indicates the directory used to store third-party software.
/tmp	40	Indicates the directory used to store temporary files generated by users or running programs.
/var	5	Indicates the directory used to store changed data during system running.
/var/log	80	Indicates the log partition.
/var/log/audit	1	Indicates the audit log partition.
/var/crash	30	Indicates the crash log partition.
/opt/zk_disk	65	Indicates the directory used to store the data of ZooKeeper.
/opt/ccdb_disk	15	Indicates a directory used to store global distributed configuration data.
/opt/ccdb_disk2	10	Indicates a directory used to store global distributed configuration data.
NOTE **/boot** and **/boot/efi** must use independent partitions, and other partitions must use LVM logical partitions.		

5.5.7 Installing the OS Dependency Package

If a third-party OS is installed on a compute node, the OS dependency package must be installed.

Prerequisites

- You have obtained software package **OceanStor-Pacific_8.2.1RC1_Tools.tar.gz** for installing DPC on a compute node.
- You have configured a management IP address for the compute node.

Procedure

Step 1 Log in to a target compute node through the management IP address as user **root**. If you have logged in as another user, run the **su - root** command to switch to user **root**.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Upload the **OceanStor-Pacific_8.2.1RC1_Tools.tar.gz** software package to the compute node and run the following command to decompress the software package.

```
tar -xzf OceanStor-Pacific_8.2.1RC1_Tools.tar.gz
```

NOTE

If error message "-bash: tar: command not found" is displayed, the .tar software package is not installed on the OS. In this case, you need to manually install the .tar software package.

Step 3 Install the OS dependency package.

1. Obtain the script for installing the OS dependency package in the **install_lib** directory.

   For the OS dependency package script, see **Table 5-62**. To query the supported OSs, see **Huawei Storage Interoperability Navigator** and set **Compatible With** to **DPC Basic Connectivity**, as shown in **Figure 5-41**.

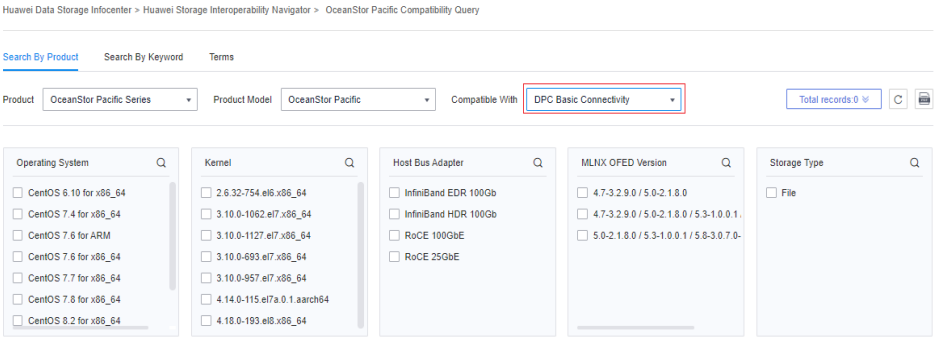
Table 5-62 OS dependency package scripts of a DPC node

OS	Node Role	OS Dependency Package Script Name
Red Hat Enterprise Linux	compute	install_lib_for_rhel.sh
CentOS	compute	install_lib_for_centos.sh
SUSE Linux Enterprise Server	compute	install_lib_for_suse.sh
Ubuntu	compute	install_lib_for_ubuntu.sh
Kylin Linux Advanced Server	compute	install_lib_for_kylin.sh
KylinSecOS	compute	install_lib_for_kylinsec.sh
AlmaLinux	compute	install_lib_for_alma.sh
Rocky Linux	compute	install_lib_for_rocky.sh
openEuler	compute	install_lib_for_openeuler.sh
EulerOS	compute	install_lib_for_euler.sh
BigCloud Enterprise Linux	compute	install_lib_for_bclinux.sh

 Copyright © Huawei Technologies Co., Ltd.

OS	Node Role	OS Dependency Package Script Name
Debian GNU/Linux	compute	install_lib_for_debian.sh
CTyunOS	compute	install_lib_for_ctyun.sh
Huawei Cloud EulerOS	compute	install_lib_for_hce.sh
UnionTech OS Server	compute	install_lib_for_uos.sh
CULinux	compute	install_lib_for_culinux.sh

Figure 5-41 Path for querying the OSs supported by DPC nodes



2. Use the script to install the OS dependency package.

   Check whether a software repository is configured onsite.

   – If yes, perform the following operations:

      i. Edit **install_lib_for_*xxx*.sh** and change the value of **YUM_REPO_IS_EXIST** to **1**.

      NOTE

      - Skip this operation if Ubuntu is used.
      - For the SUSE OS, change the value of **ZYPPER_REPO_IS_EXIST** to **1**.
      - For detailed OS dependency package script names of a DPC node, see **Table 5-62**.

      ii. Copy the OS dependency package script upon modification to the **/tmp** directory on the compute node.

      ```
      cp install_lib_for_xxx.sh /tmp
      ```

      iii. Run the following command to go to the directory where the script for installing the dependency package is stored.

      ```
      cd /tmp
      ```

 Copyright © Huawei Technologies Co., Ltd.

iv. Run the following command to install the OS dependency package.
```
bash install_lib_for_xxx.sh node_type
```

– If no, perform the following operations:

i. Upload the OS dependency package script to the **/tmp** directory on the compute node.

ii. Run the following command to go to the directory where the script for installing the dependency package is stored.
```
cd /tmp
```

iii. Obtain the OS image file. Upload the local OS ISO image file to the compute node.

iv. Run the following command to install the OS dependency package.
```
bash install_lib_for_xxx.sh node_type /Directory for storing the OS ISO image file/OS ISO image file name
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- When installing the dependency package of the Ubuntu OS, configure the software repository to configure the software installation source and run the following commands.
  ```
  apt-get update
  bash install_lib_for_ubuntu.sh node_type
  ```
- In the commands, *node_type* indicates the role of a node, such as **compute**, **storage**, and **manager**. For details about the node roles supported by the OS, see **Table 5-62**. If a node has multiple roles, use a hyphen (-) to connect the roles, for example:
  - compute-manager
  - compute-storage
  - manager-storage
  - compute-manager-storage
- The installation takes about 10 minutes. The required time depends on the hardware configuration and whether a software repository is used.
- If **Other yum repo configurations exist in /etc/yum.repos.d/. Please delete them.** is displayed after the script is executed, manually move the **.repo** file from the **/etc/yum.repos.d/** directory to another temporary directory and run the script again to install the OS dependency package. After the installation is complete, move the file back to the original directory.
- The automatic update of the Ubuntu OS must be disabled. You can run the following commands on a supported OS to change all configuration items in the **10periodic** and **20auto-upgrades** files (only one of the two files may exist) from **1** to **0**. For details about the supported OSs, see **Huawei Storage Interoperability Navigator**.
  - **vi /etc/apt/apt.conf.d/10periodic**

    Change all configuration items from **1** to **0**.
  - **vi /etc/apt/apt.conf.d/20auto-upgrades**

    Change all configuration items from **1** to **0**.

  ```
  root@ubuntu:/home/testTools/vdbench# cat /etc/apt/apt.conf.d/10periodic
  APT::Periodic::Update-Package-Lists "0";
  APT::Periodic::Download-Upgradeable-Packages "0";
  APT::Periodic::AutocleanInterval "0";
  root@ubuntu:/home/testTools/vdbench# cat /etc/apt/apt.conf.d/20auto-upgrades
  APT::Periodic::Update-Package-Lists "0";
  APT::Periodic::Unattended-Upgrade "0";
  root@ubuntu:/home/testTools/vdbench#
  ```
- Hardware Enablement (HWE) cannot be installed on Ubuntu Server.

Step 4 Repeat **Step 1** to **Step 3** to install the OS dependency package on other compute nodes.

----End

 Copyright © Huawei Technologies Co., Ltd.

5.5.8 Weak Password Dictionary

NOTICE

The password of the operating system account in the OceanStor Pacific series storage system is restricted by the password complexity of the operating system. Ensure that the password meets the password complexity requirements of both the OceanStor Pacific series storage system and operating system.

The complexity requirements for the operating system password are as follows:

1. The password contains at least eight characters.
2. Contains at least three types of the following characters:
   - Lowercase letters: a to z
   - Uppercase letters: A to Z
   - Digits: 0 to 9
   - Special characters: `~!@#$%^&*()-_=+\|[{}];:'",<.>/? and space
3. The password cannot be the same as the user name or the user name spelled backwards.
4. The password cannot be the same as any of the last five passwords.
5. Differs from any word in dictionaries.

   Query the dictionary:

   1. Use SSH to log in to a management node as user **fsadmin**.
   2. Run the **minisystem** command and enter the password of user **root** as prompted to log in to minisystem.
   3. Run the following command to query the exported dictionary library file **dictionary.txt**.
      ```
      weak_password export dictionary.txt
      ```
6. Use an algorithm to verify passwords. When setting or changing a user password, use the following method to check whether the password meets the requirements:
   1. Use SSH to log in to a management node as user **fsadmin**.
   2. Run the **minisystem** command and enter the password of user **root** as prompted to log in to minisystem.
   3. Run the following command to check whether the password meets the requirements.
      ```
      weak_password check xxx
      ```

For details about how to obtain the weak password dictionary, see **Table 5-63**.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-63 Obtaining the weak password dictionary

Type	Obtaining Method

Storage system	1. Use the SSH tool to log in to any management node as user **fsadmin**. After the login is successful, the cliportal mode is displayed.
	2. In cliportal mode, run the following command and enter the password of user **root** as prompted to go to the minisystem view.
	`minisystem`
	3. Run the following command to query the weak password dictionary.
	`weak_password query`

OS	For details, see **Query the dictionary** in 5.
iBMC	1. Use SSH to log in to a node as user **Administrator**. 2. Run the following command to query the weak password dictionary. `ipmcset -t user -d weakpwddic -v export` The following weak passwords can be queried: Admin123@, admin123@, Root123@, root123@, Admin123#, admin123#, Root123#, root123#, Admin123!, admin123!, Root123!, root123!, Admin@123, admin@123, Root@123, root@123, Admin123, admin123, Admin_123, admin_123, Root_123, root_123, Administrator, Password, Password123, Password@123, Password_123, Password123!, and Admin@9000

5.5.9 Adding a Port

This section describes how to configure bond ports based on service requirements.

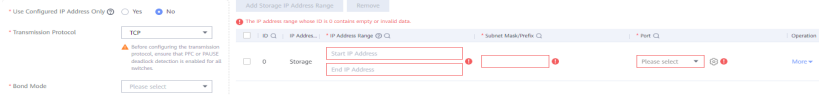
This operation takes effect for all storage nodes.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Click on the right of the **Port** parameter, as shown in **Figure 5-42**.

Figure 5-42 Managing bond ports



The **Manage Bond Ports** page is displayed.

NOTE

You can also click **Preview**, click **More** on the right of a node in the table displayed on the page, and select **Manage Bond Ports**.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Click **Add**.

Step 4 Configure the port information. **Table 5-64** describes related parameters.

Table 5-64 Port parameters

Parameter	Description
Bond Port Name	Indicates the name of the bond port.
Transmission Protocol	Indicates the transmission protocol used by the bond port. Possible options are **TCP**, **IB**, and **RoCE**.
Physical Port	Indicates the physical port to be bonded. **NOTE** The physical ports to be bonded must be the same for all storage nodes.
Bond Mode	Indicates the bond mode of the port. • **bond1**: active/standby mode • **bond4**: dynamic link aggregation mode
MTU (Bytes)	Indicates the maximum transmission unit of the bond port. **NOTE** **IB protocol scenario:** • During RDMA communication, OpenSM is used to allocate the MTU and transmission rate to each port. The MTU value is configured on OpenSM. The value can be **2048** or **4096**, and the default value is **2048**. You are advised not to change the configured value. • The MTU of the CX5/CX6 NIC is set to **2044** in the network port configuration file and cannot be changed. **Ethernet scenario:** • The default MTU of the Hi1620/Hi1822/Hi1822V120/CX4/CX5/CX6 NIC is **1500** and cannot be changed. • If the RoCE protocol is running on a port, the MTU cannot be changed. • If only the TCP protocol runs on a port and the MTU is changed, its value must be the same on all network elements (switches, routers, and ports on compute nodes).

Step 5 Click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

5.5.10 Configuring a Static Route

5.5.10.1 Configuring a Static Route for a Physical Port

This section describes how to configure static route information for a physical port.

Procedure

Step 1 Select one or more desired ports and click **Configure Static Route**.

The **Configure Static Route** page is displayed.

NOTE

You can also click **More** on the right of a desired port and select **Manage Static Route**. On the **Manage Static Route** page that is displayed, click **Add** to configure a static route.

Step 2 Configure static route information for the physical port.

- Selecting **New** in **Configuration Mode**
  a. Set the parameters listed in **Table 5-65**.

  Table 5-65 Route parameters

Parameter	Description
Destination IP Address	IP address or network segment of the target node network port connected to the physical port.
Subnet Mask/ Prefix	Subnet mask or prefix of the network segment where the target node network port connected to the physical port resides.
Gateway	Gateway where the local physical port's IP address resides.

  b. (Optional) Click **Add** to add another static route.
- Selecting **Copy from** in **Configuration Mode**
  a. In **Node**, click **Choose** to select a node.
  b. In **Port**, click **Choose** to select a port.
  c. In the **Available Static Routes** list, select one or more required static routes.
  d. (Optional) Click **More** on the right of a desired route and select **Modify** to modify it.

  NOTE

  This operation does not change the route information of the source node.

Step 3 Click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

5.5.10.2 Configuring a Static Route for a Bond Port

This section describes how to configure static route information for a bond port.

Procedure

Step 1 Select one or more desired ports and click **Configure Static Route**.

The **Configure Static Route** page is displayed.

NOTE

You can also click **More** on the right of a desired port and select **Manage Static Route**. On the **Manage Static Route** page that is displayed, click **Add** to configure a static route.

Step 2 Configure the static route information for a bond port.

- Selecting **New** in **Configuration Mode**
  a. Set the parameters listed in **Table 5-66**.

  Table 5-66 Route parameters

Parameter	Description
Destination IP Address	IP address or network segment of the target node network port connected to the bond port.
Subnet Mask/ Prefix	Subnet mask or prefix of the network segment where the target node network port connected to the bond port resides.
Gateway	Gateway where the local bond port's IP address resides.

  b. (Optional) Click **Add** to add another static route.
- Selecting **Copy from** in **Configuration Mode**
  a. In **Node**, click **Choose** to select a node.
  b. In **Port**, click **Choose** to select a port.
  c. In the **Available Static Routes** list, select one or more required static routes.
  d. (Optional) Click **More** on the right of a desired route and select **Modify** to modify it.

  NOTE

  This operation does not change the route information of the source node.

Step 3 Click **OK**.

----End

5.5.10.3 Configuring a Static Route for a VLAN Port

This section describes how to configure a static route for a VLAN port.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Select one or more desired VLAN ports and click **Configure Static Route**.

The **Configure Static Route** page is displayed.

NOTE

You can also click **More** on the right of a desired VLAN port and select **Manage Static Route**. On the **Manage Static Route** page that is displayed, click **Add** to configure a static route.

Step 2 Configure the static route information for a VLAN port.

- Selecting **New** in **Configuration Mode**
  a. Set the parameters listed in **Table 5-67**.

  Table 5-67 Route parameters

Parameter	Description
Destination IP Address	IP address or network segment of the target node network port connected to the VLAN port.
Subnet Mask/ Prefix	Subnet mask or prefix of the target network segment where the node network port connected to the VLAN port resides.
Gateway	Gateway where the local VLAN port's IP address resides.

  b. (Optional) Click **Add** to add another static route.
- Selecting **Copy from** in **Configuration Mode**
  a. In **Node**, click **Choose** to select a node.
  b. In **Port**, click **Choose** to select a port.
  c. In the **Available Static Routes** list, select one or more required static routes.
  d. (Optional) Click **More** on the right of a desired route and select **Modify** to modify it.

  NOTE

  This operation does not change the route information of the source node.

Step 3 Click **OK**.

----End

5.5.11 Querying a Static Route

5.5.11.1 Querying the Static Routes of a Physical Port

This section describes how to query the static routes of a physical port.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Click **More** on the right of a desired physical port and select **Manage Static Route**.

The **Manage Static Route** dialog box is displayed, showing the static route information of the physical port. For details about related parameters, see **Table 5-68**.

Table 5-68 Route parameters

Parameter	Description
Destination IP Address	IP address or network segment of the target node network port connected to the physical port.
Subnet Mask/ Prefix	Subnet mask or prefix of the network segment where the target node network port connected to the physical port resides.
Gateway	Gateway where the local physical port's IP address resides.

NOTE

You can also click the name of a physical port to go to the details page, and click the **Static Route** tab to view the static route information of the physical port.

5.5.11.2 Querying the Static Routes of a Bond Port

This section describes how to query the static routes of a bond port.

Procedure

Click **More** on the right of a desired bond port and select **Manage Static Route**.

The **Manage Static Route** dialog box is displayed, showing the static route information of the bond port. For details about related parameters, see **Table 5-69**.

Table 5-69 Route parameters

Parameter	Description
Destination IP Address	IP address or network segment of the target node network port connected to the bond port.
Subnet Mask/ Prefix	Subnet mask or prefix of the network segment where the target node network port connected to the bond port resides.
Gateway	Gateway where the local bond port's IP address resides.

Copyright © Huawei Technologies Co., Ltd.

NOTE

You can also click the name of a bond port to go to the details page, and click the **Static Route** tab to view the static route information of the bond port.

5.5.11.3 Querying the Static Routes of a VLAN Port

This section describes how to query the static routes of a VLAN port.

Procedure

Click **More** on the right of a desired VLAN port and select **Manage Static Route**.

The **Manage Static Route** dialog box is displayed, showing the static route information of the VLAN port. For details about related parameters, see **Table 5-70**.

Table 5-70 Route parameters

Parameter	Description
Destination IP Address	IP address or network segment of the target node network port connected to the VLAN port.
Subnet Mask/ Prefix	Subnet mask or prefix of the target network segment where the node network port connected to the VLAN port resides.
Gateway	Gateway where the local VLAN port's IP address resides.

NOTE

You can also click the name of a VLAN port to go to the details page, and click the **Static Route** tab to view the static route information of the VLAN port.

5.5.12 Deleting a Static Route

5.5.12.1 Deleting a Static Route from a Physical Port

This section describes how to delete a static route from a physical port.

Procedure

Step 1 Click **More** on the right of a desired port and select **Manage Static Route**.

The **Manage Static Route** dialog box is displayed.

Step 2 Select one or more desired routes and click **Delete**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

You can also click **More** on the right of a desired route and select **Delete**.

----End

5.5.12.2 Deleting a Static Route from a Bond Port

This section describes how to delete a static route from a bond port.

Procedure

Step 1 Click **More** on the right of a desired port and select **Manage Static Route**.

The **Manage Static Route** dialog box is displayed.

Step 2 Select one or more desired routes and click **Delete**.

NOTE

You can also click **More** on the right of a desired route and select **Delete**.

----End

5.5.12.3 Deleting a Static Route from a VLAN Port

This section describes how to delete a static route from a VLAN port.

Procedure

Step 1 Click **More** on the right of a desired port and select **Manage Static Route**.

The **Manage Static Route** dialog box is displayed.

Step 2 Select one or more desired routes and click **Delete**.

NOTE

You can also click **More** on the right of a desired route and select **Delete**.

----End

5.5.13 Configuring a Policy-Based Route

5.5.13.1 Configuring a Policy-based Route for a Physical Port

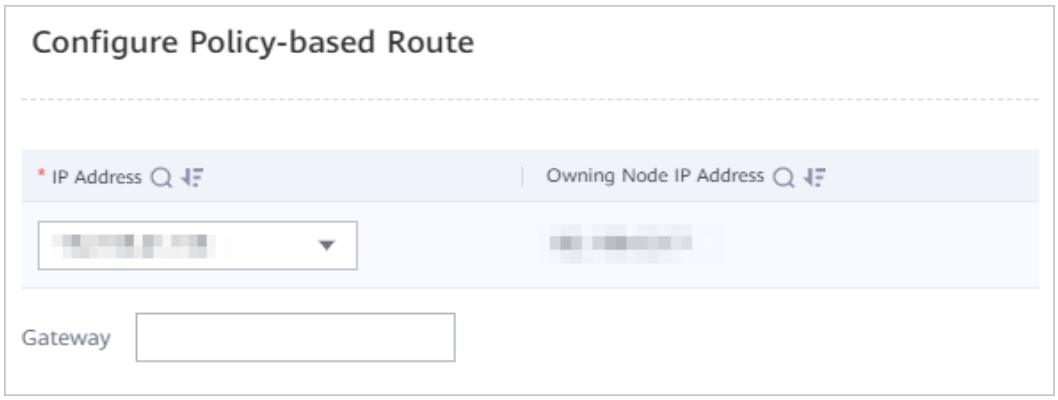
This section describes how to configure policy-based route information for a physical port.

Procedure

Step 1 Select one or more desired physical ports and click **Configure Policy-based Route**.

The **Configure Policy-based Route** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



NOTE

You can also click **More** on the right of a desired port and select **Manage Policy-based Route**. On the **Manage Policy-based Route** page that is displayed, click **Add** to configure a policy-based route.

Step 2 If a physical port is configured with multiple IP addresses, you need to select an IP address to configure the route.

NOTE

If the storage network has multiple IP addresses, select an IP address in the storage network segment.

Step 3 (Optional) Configure a gateway.

NOTE

A gateway needs to be configured for communication across network segments. If IP addresses are in the same network segment, the configuration of the gateway is not required. If capacity expansion is performed across network segments, it is recommended that the gateway be configured first.

Step 4 Click **OK**.

----End

5.5.13.2 Configuring a Policy-based Route for a Bond Port

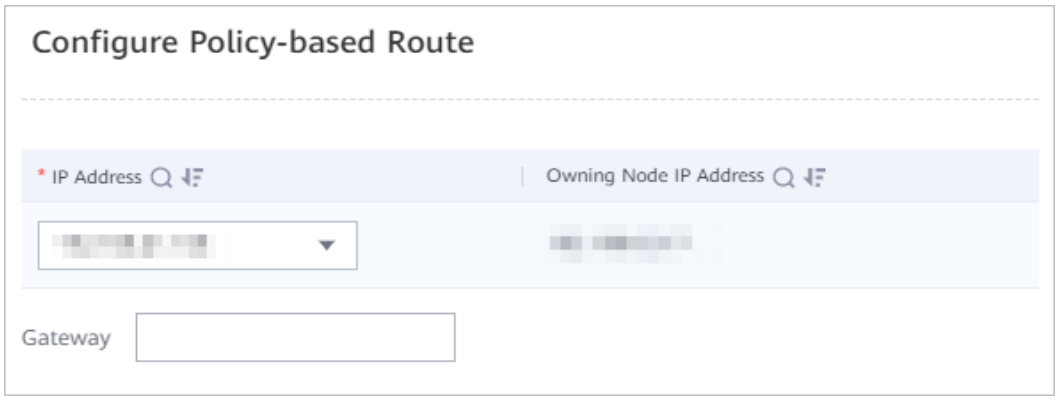
This section describes how to configure policy-based route information for a bond port.

Procedure

Step 1 Select one or more desired bond ports and click **Configure Policy-based Route**.

The **Configure Policy-based Route** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



NOTE

You can also click **More** on the right of a desired port and select **Manage Policy-based Route**. On the **Manage Policy-based Route** page that is displayed, click **Add** to configure a policy-based route.

Step 2 If a bond port is configured with multiple IP addresses, you need to select an IP address to configure the route.

Step 3 (Optional) Configure a gateway.

NOTE

A gateway needs to be configured for communication across network segments. If IP addresses are in the same network segment, the configuration of the gateway is not required. If capacity expansion is performed across network segments, it is recommended that the gateway be configured first.

Step 4 Click **OK**.

----End

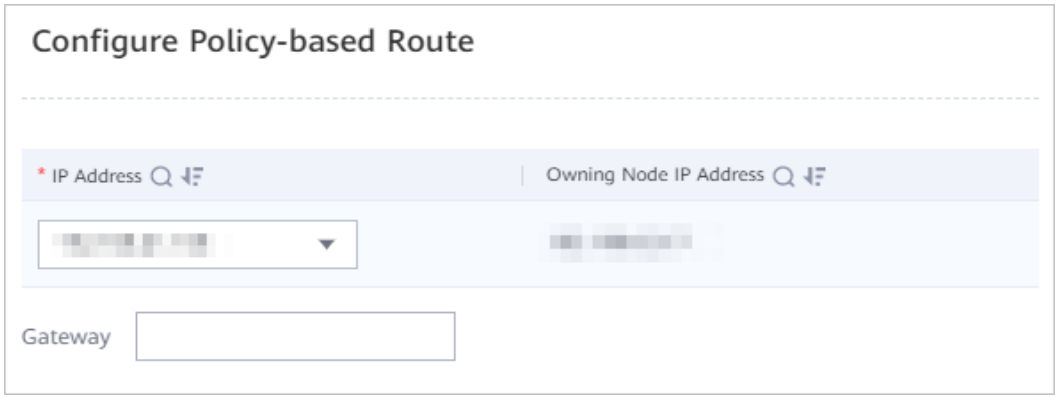
5.5.13.3 Configuring a Policy-based Route for a VLAN Port

This operation enables you to configure a policy-based route for a VLAN. If the storage network has multiple IP addresses, you need to configure a policy-based route for each VLAN port on each storage node.

Procedure

Step 1 Select a desired VLAN port and click **Configure Policy-based Route**.

The **Configure Policy-based Route** page is displayed.



 Copyright © Huawei Technologies Co., Ltd.

NOTE

You can also click **More** on the right of a desired VLAN port and select **Manage Policy-based Route**. On the **Manage Policy-based Route** page that is displayed, click **Add** to configure a policy-based route.

Step 2 If a VLAN port is configured with multiple IP addresses, you need to select an IP address to configure the route.

NOTE

If the storage network has multiple IP addresses, select an IP address in the storage network segment. After the storage network is configured, the system automatically configures the policy-based route for the control network. Do not manually configure the policy-based route.

Step 3 (Optional) Configure a gateway.

NOTE

A gateway needs to be configured for communication across network segments. If IP addresses are in the same network segment, the configuration of the gateway is not required. If capacity expansion is performed across network segments, it is recommended that the gateway be configured first.

Step 4 Click **OK**.

----End

5.5.14 Querying a Policy-Based Route

5.5.14.1 Querying the Policy-based Routes of a VLAN Port

This section describes how to query the policy-based routes of a VLAN port.

Procedure

Click **More** on the right of a desired VLAN port and select **Manage Policy-based Route**.

The **Manage Policy-based Route** dialog box is displayed, showing the policy-based route information of the VLAN port. For details about related parameters, see **Table 5-71**.

Table 5-71 Policy-based route parameters

Parameter	Description
IP Address	IP address of a VLAN port.
Subnet Mask/ Prefix	Subnet mask or prefix of a VLAN port.
Gateway	Gateway of the storage IP address of a VLAN port.

Copyright © Huawei Technologies Co., Ltd.

NOTE

You can also click the name of a VLAN port to go to the details page, and click the **Policy-based Route** tab to view the policy-based route information of the VLAN port.

5.5.15 Deleting a Policy-based Route

5.5.15.1 Deleting a Policy-based Route from a VLAN Port

This section describes how to delete a policy-based route from a VLAN port.

Procedure

Step 1 Click **More** on the right of a desired port and select **Manage Policy-based Route**.

The **Manage Policy-based Route** page is displayed.

Step 2 Select one or more desired routes and click **Delete**.

NOTE

You can also click **More** on the right of a desired route and select **Delete**.

----End

5.5.16 Configuring the Storage Network IP Address by Modifying the Configuration File

Context

This section describes how to configure the storage network IP address by modifying the configuration file. Select the corresponding section based on the actual networking scenario.

5.5.16.1 Configuring the Storage Network (TCP/IP)

Context

The description in the following operations is only an example. The actual port information prevails.

After installing a storage node, you are not allowed to modify any configuration information of the storage network ports on the node.

Prerequisites

The management network IP address has been configured for a storage node.

Procedure

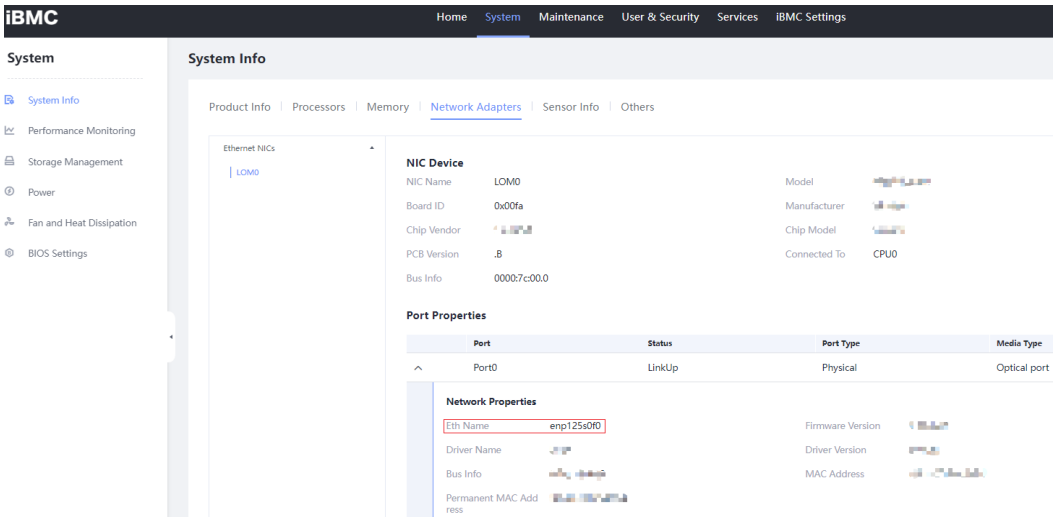
Step 1 Check the name of the network port corresponding to a NIC.

 Copyright © Huawei Technologies Co., Ltd.

Log in to the iBMC system of a node, choose **System** > **System Info** > **Network Adapters** or **System** > **System Info** > **NICs**, select the corresponding NIC and port, and view the network port name. An example is provided as follows:

NOTE

If **Eth Name** cannot be queried on this page, you need to install the iBMA component. For details, see **5.5.20 Installing the iBMA Component**.



Step 2 Use a remote connection tool to log in to the node as user **fsadmin** through the temporary management IP address. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. After the password is changed, log in to the node again.

Step 3 Run the following command to switch to user **root**.

```
su - root
```

Step 4 Go to the path for storing the network port configuration file.

```
cd /etc/sysconfig/network-scripts
```

Step 5 Run the following command to edit the network port configuration file. If the network port configuration file does not exist in the current path, you can run the following command to create and edit the network port configuration file.

```
vi ifcfg-Network port name
```

For details about the configuration file, see **Table 5-72** or **Table 5-73**.

NOTE

In the following example, the storage network uses physical network ports enp125s0f0 and enp125s0f1. You need to configure the following network port configuration files for each storage node:

- **ifcfg-enp125s0f0**: configuration file of physical network port enp125s0f0
- **ifcfg-enp125s0f1**: configuration file of physical network port enp125s0f1
- **ifcfg-fsb_bond**: configuration file of the bond port corresponding to the two physical network ports
- **ifcfg-v.*XXX***: configuration file of the VLAN port corresponding to the bond port. This configuration file is required if you configure VLANs.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-72 Network port configuration file information (using bond ports, without VLANs)

Name	Content
ifcfg-*enp125s0f0*	DEVICE=*enp125s0f0* BOOTPROTO=none ONBOOT=yes MASTER=*fsb_bond* SLAVE=yes USERCTL=no NM_CONTROLLED=no
ifcfg-*enp125s0f1*	DEVICE=*enp125s0f1* BOOTPROTO=none ONBOOT=yes MASTER=*fsb_bond* SLAVE=yes USERCTL=no NM_CONTROLLED=no
ifcfg-*fsb_bond*	DEVICE=*fsb_bond* IPv4 configuration: IPADDR=*IPv4 address* NETMASK=*subnet mask* DEFROUTE=no **NOTE** The storage network (the internal management network and storage network share the same IP address) cannot use the same subnet as the external management network or service network. The IP addresses in each IP address segment cannot be in the same subnet as those of other ports on the node. IPV6_AUTOCONF=no ONBOOT=yes BOOTPROTO=static USERCTL=no TYPE=Bonding MTU=1500 **NOTE** ● The default MTU of the Hi1620/Hi1822/ Hi1822V120/CX4/CX5/CX6 NIC is **1500** and cannot be changed. ● If only the TCP protocol runs on a port and the MTU is changed, its value must be the same on all network elements (switches, routers, and ports on compute nodes). NM_CONTROLLED=no BONDING_OPTS='mode=4 miimon=100 lacp_rate=fast xmit_hash_policy=layer3+4' **NOTE** In the example, the bond4 mode is used. If the bond1 mode is configured, the **BONDING_OPTS** parameter is as follows: BONDING_OPTS='mode=1 miimon=100' BONDING_SLAVE0=*eth0* BONDING_SLAVE1=*eth1*

 Copyright © Huawei Technologies Co., Ltd.

Table 5-73 Network port configuration file information (using bond ports, with VLANs)

Name	Content
ifcfg-*enp125s0f0*	DEVICE=*enp125s0f0* BOOTPROTO=none ONBOOT=yes MASTER=*fsb_bond* SLAVE=yes USERCTL=no NM_CONTROLLED=no DEVICE=eth0 BOOTPROTO=static STARTMODE=onboot USERCONTROL=no NM_CONTROLLED=no
ifcfg-*enp125s0f1*	DEVICE=*enp125s0f1* BOOTPROTO=none ONBOOT=yes MASTER=*fsb_bond* SLAVE=yes USERCTL=no NM_CONTROLLED=no DEVICE=eth1 BOOTPROTO=static STARTMODE=onboot USERCONTROL=no NM_CONTROLLED=no

 Copyright © Huawei Technologies Co., Ltd.

Name	Content
ifcfg-*fsb_bond*	DEVICE=*fsb_bond* ONBOOT=yes BOOTPROTO=none USERCTL=no TYPE=Bonding MTU=1500 **NOTE** • The default MTU of the Hi1620/Hi1822/Hi1822V120/CX4/CX5/CX6 NIC is **1500** and cannot be changed. • If only the TCP protocol runs on a port and the MTU is changed, its value must be the same on all network elements (switches, routers, and ports on compute nodes). NM_CONTROLLED=no BONDING_OPTS='mode=4 miimon=100 lacp_rate=fast xmit_hash_policy=layer3+4' **NOTE** In the example, the bond4 mode is used. If the bond1 mode is configured, the **BONDING_OPTS** parameter is as follows: BONDING_OPTS='mode=1 miimon=100' BONDING_SLAVE0=*eth0* BONDING_SLAVE1=*eth1* DEVICE=fsb_bond BOOTPROTO=none STARTMODE=onboot IPV6_DAD_WAIT=0 BONDING_MASTER=yes BONDING_MODULE_OPTS='mode=4 miimon=100 lacp_rate=fast xmit_hash_policy=layer3+4' BONDING_SLAVE0=eth0 BONDING_SLAVE1=eth1 **NOTE** In the example, the bond4 mode is used. If the bond1 mode is configured, the **BONDING_MODULE_OPTS** parameter is as follows: BONDING_MODULE_OPTS='mode=1 miimon=100'

 Copyright © Huawei Technologies Co., Ltd.

Name	Content
ifcfg-v.*XXX*	DEVICE=*v.XXX* /*The value of *v.XXX* must be the same as the name of the configuration file.*/ **NOTE** • The value of **DEVICE** must contain a period (.) or start with **vlan**. • The value of **DEVICE** cannot contain the at sign (@). • The value of **DEVICE** can contain a maximum of 13 characters. IPv4 configuration: IPADDR=*IPv4 address* NETMASK=*subnet mask* DEFROUTE=no • IPv6 configuration: IPV6INIT=yes IPV6ADDR=*IPv6 address/prefix* IPV6_DEFROUTE=no **NOTE** The storage network (the internal management network and storage network share the same IP address) cannot use the same subnet as the external management network or service network. The IP addresses in each IP address segment cannot be in the same subnet as those of other ports on the node. IPV6_AUTOCONF=no BOOTPROTO=static PHYSDEV=*fsb_bond*/*The value of *fsb_bond* must be the same as the name of the bond port.*/ ONBOOT=yes USERCTL=no VLAN=yes • VID=XXX /*For the pre-installed OS, specify *VLAN ID* by entering *VID* in the configuration file. */ • VLAN_ID=XXX /*For Red Hat, Oracle, or CentOS, specify *VLAN ID* by entering *VLAN_ID* in the configuration file. */ NM_CONTROLLED=no DEVICE=vlanXXX /*The value of *vlanXXX* must be the same as the name of the configuration file. */ • IPv4 configuration: – IPADDR=*IPv4 address* – NETMASK=*subnet mask* • IPv6 configuration: – IPADDR_0=*IPv6 address* – PREFIXLEN_0=*prefix* – IPV6_AUTOCONF=no BOOTPROTO=static ETHERDEVICE=fsb_bond/*The value of *fsb_bond* must be the same as the name of the bond port. */ STARTMODE=onboot IPV6_DAD_WAIT=0

 Copyright © Huawei Technologies Co., Ltd.

Name	Content
	USERCONTROL=no VLAN=yes VLAN_ID=*ID* /*Specify the VLAN ID. */

Step 6 After editing the configuration file, press **Esc** and enter **:wq** to save the settings and exit.

Step 7 Modify the permission on the network port configuration file.

```
chmod 644 /etc/sysconfig/network-scripts/ifcfg-Network port name
chown -h root:root /etc/sysconfig/network-scripts/ifcfg-Network port name
```

NOTE

All network port configuration files need to be modified.

Step 8 Run the following command to restart the network service:

```
service network restart
```

NOTE

After restarting the network service, you are advised to wait for 2 to 3 minutes to ensure that the network communication is recovered.

Step 9 Configure storage IP addresses for all storage nodes by following the instructions provided in **Step 1** to **Step 8**.

Step 10 After the configuration is complete, ping the storage IP addresses of other storage nodes from a storage node to ensure that the storage network communication between storage nodes is normal.

----End

5.5.16.2 Configuring the Storage Network (RoCE and Multiple IP Addresses)

Context

- The description in the following operations is only an example. The actual port information prevails.
- If the storage network is a RoCE network, the storage network port must be configured with a VLAN.
- Control network IP addresses must be configured for storage nodes. You can select any storage port to configure control network IP addresses.
- The storage network must be configured for each node.
- After installing a storage node, you are not allowed to modify any configuration information of the storage network ports on the node.

Prerequisites

The management network IP address has been configured for a storage node.

 Copyright © Huawei Technologies Co., Ltd.

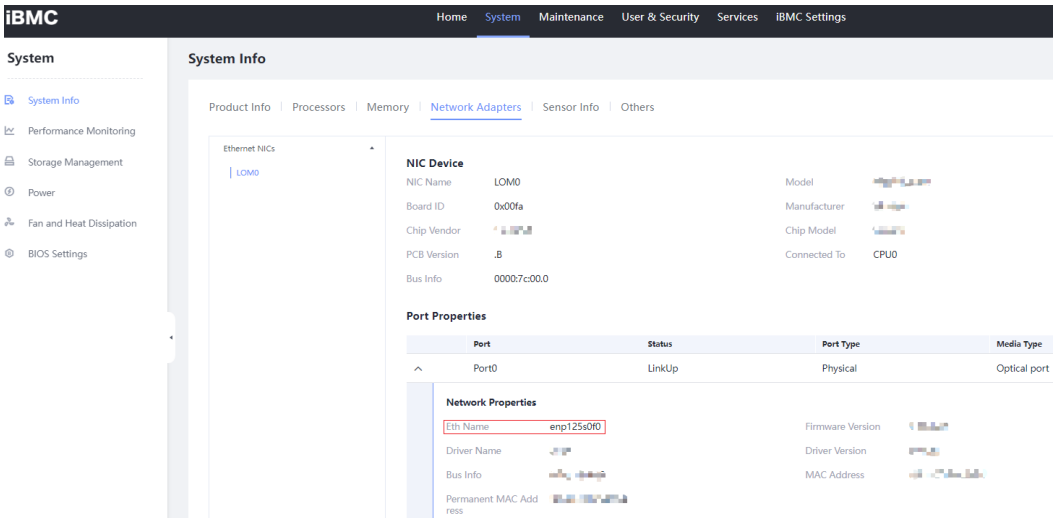
Procedure

Step 1 Check the name of the network port corresponding to a NIC.

Log in to the iBMC system of a node, choose **System** > **System Info** > **Network Adapters** or **System** > **System Info** > **NICs**, select the corresponding NIC and port, and view the network port name. An example is provided as follows:

NOTE

If **Eth Name** cannot be queried on this page, you need to install the iBMA component. For details, see **5.5.20 Installing the iBMA Component**.



Step 2 Use a remote connection tool to log in to the node as user **fsadmin** through the temporary management IP address. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login. After the password is changed, log in to the node again.

Step 3 Run the following command to switch to user **root**.

```
su - root
```

Step 4 Go to the path for storing the network port configuration file.

```
cd /etc/sysconfig/network-scripts
```

Step 5 Run the following command to edit the network port configuration file. If the network port configuration file does not exist in the current path, you can run the following command to create and edit the network port configuration file.

```
vi ifcfg-Network port name
```

Configure the front-end storage network and control network by referring to **Table 5-74**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Example: The storage network uses RoCE and multiple IP addresses for networking. The number of IP addresses is 2. The storage IP addresses are configured on physical network ports enp125s0f0 and enp125s0f1, and the control IP address is configured on network port enp125s0f0. The network port configuration files to be configured for each storage node are as follows:

- **ifcfg-enp125s0f0**: configuration file of physical network port 0
- **ifcfg-vlan0.12**: VLAN port configuration file corresponding to physical network port 0. VLANs need to be configured for RoCE networking.
- **ifcfg-vlan0.12:0**: control network configuration file. Only one control IP address needs to be configured for each storage node.
- **ifcfg-enp125s0f1**: configuration file of physical network port 1
- **ifcfg-vlan1.12**: VLAN port configuration file corresponding to physical network port 1. VLANs need to be configured for RoCE networking.

Table 5-74 Network port configuration file information (multiple IP addresses are used for the storage network)

Name	Content
ifcfg-*enp125s0f0* **NOTE** Physical network port configuration file.	DEVICE=*enp125s0f0* BOOTPROTO=none ONBOOT=yes STARTMODE=onboot DEFROUTE=no NM_CONTROLLED=no

 Copyright © Huawei Technologies Co., Ltd.

Name	Content
ifcfg-*vlan.12* **NOTE** VLAN port configuration file.	DEVICE=*vlan.12* **NOTE** • The value of **DEVICE** consists of a user-defined prefix, a period (.), and VLAN ID. • The value of **DEVICE** can contain a maximum of 13 characters. • The value of **DEVICE** must be unique in the OS. • The user-defined prefix can contain only letters and digits and must start with a letter. IPv4 configuration: NETMASK=*subnet mask* DEFROUTE=no IPADDR=*IPv4 address* **NOTICE** When multiple IP addresses are used for networking, they must be assigned to the **IPADDR** value of each node based on the same rule. The IP addresses are assigned in ascending or descending order of the network port names. For example: IP addresses are assigned in ascending order of the network port names (all nodes must comply with this rule): enp13s0f0: *192.168.100.12* enp13s0f1: *192.168.100.13* enp125s0f0: *192.168.100.14* enp125s0f1: *192.168.100.15* IP addresses are assigned in descending order of the network port names (all nodes must comply with this rule): enp13s0f0: *192.168.100.15* enp13s0f1: *192.168.100.14* enp125s0f0: *192.168.100.13* enp125s0f1: *192.168.100.12* **NOTE** The storage network cannot use the same subnet as the external management network or service network. The control network and storage network (the internal management network and storage network share the same IP address) can use the same subnet (recommended) or different subnets. If they use the same subnet, they must use different IP address segments. IPV6_AUTOCONF=no BOOTPROTO=static PHYSDEV=*enp125s0f0* ONBOOT=yes USERCTL=no VLAN=yes VID=XXX /***VID** is the specified VLAN ID.*/ NM_CONTROLLED=no

 Copyright © Huawei Technologies Co., Ltd.

Name	Content
ifcfg-*vlan.12*:0 **NOTE** • When multiple IP addresses are used for networking, you need to set this parameter to configure the control network IP address of the node. • You can select any storage network port on the storage node to configure the control network IP address.	DEVICE=*vlan.12*:0 **NOTE** • The value of **DEVICE** consists of a user-defined prefix, a period (.), VLAN ID, and **:0**. • The value of **DEVICE** can contain a maximum of 15 characters. • The value of **DEVICE** must be unique in the OS. • The user-defined prefix can contain only letters and digits and must start with a letter. IPv4 configuration: IPADDR=*IPv4 address* NETMASK=*subnet mask* DEFROUTE=no GATEWAY=*gateway* **NOTE** • The control network and the storage network can be in the same subnet (recommended) or different subnets. If they are in the same subnet, they must use different IP address segments. • A control network gateway needs to be configured in any of the following scenarios: – The control network crosses subnets. – The control network does not cross subnets currently but needs to cross subnets due to subsequent capacity expansion. In this case, you are advised to configure the gateway first. – The control network and storage network use the same subnet. • The gateway configuration fields are as follows: – If an IPv4 address is used, configure **GATEWAY**. – If an IPv6 address is used, configure **IPV6_DEFAULTGW**. NO_ALIASROUTING=yes IPV6_AUTOCONF=no BOOTPROTO=static PHYSDEV=*enp125s0f0* ONBOOT=yes USERCTL=no VLAN=yes VID=XXX /***VID** is the specified VLAN ID, which must be the same as the VLAN ID of the storage network.*/ NM_CONTROLLED=no

Step 6 After editing the configuration file, press **Esc** and enter **:wq** to save the settings and exit.

Step 7 Modify the permission on the network port configuration file.

```
chmod 644 /etc/sysconfig/network-scripts/ifcfg-Network port name
chown -h root:root /etc/sysconfig/network-scripts/ifcfg-Network port name
```

NOTE

All network port configuration files need to be modified.

 Copyright © Huawei Technologies Co., Ltd.

Step 8 Run the following command to restart the network service:

```
service network restart
```

NOTE

After restarting the network service, you are advised to wait for 2 to 3 minutes to ensure that the network communication is recovered.

Step 9 Configure storage IP addresses for all storage nodes by following the instructions provided in **Step 1** to **Step 8**.

----End

5.5.17 Configuring a Temporary IP Address

Procedure

Step 1 Log in to the iBMC system of a node.

Step 2 Go to the **Home** page of the iBMC system. In the **Virtual Console** area, click **Start** and select **HTML5 Integrated Remote Console (Shared)**. The KVM page is displayed.

Step 3 Log in to the node as user **root**.

Step 4 Configure a temporary management IP address for the node.

- To configure an IPv4 address:

  Run the following commands:

  ifconfig *Management plane NIC name Temporary IPv4 address/Number of subnet mask bits* **up**
  route add default gw *Default gateway*

  The following is an example:

  ifconfig enp125s0f0 192.168.40.15/24 up

  route add default gw 192.168.40.1

- To configure an IPv6 address:

  Run the following commands:

  ifconfig *Management plane NIC name* **add** *Temporary IPv6 address/Prefix* **up**
  route -A inet6 add default gw *Default gateway*

  The following is an example:

  ifconfig enp2s0f0:3 add FC00::102/64 up

  route -A inet6 add default gw FC00::101

----End

5.5.18 Formatting an NVMe SSD

If a node uses NVMe SSDs, perform the following steps to format them.

Prerequisites

- You have obtained the management IP address of the host where NVMe SSDs reside.
- You have obtained PuTTY.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to a node as user **fsadmin** and enter the cliportal view.

NOTE

To obtain the default user password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)* or *OceanStor Pacific Series 8.2.1 Account List (Block Service)*. You need to change the default password upon the first login. After the password is changed, log in to the node again. If the default password has been changed, use the new password to log in.

Step 2 Run the **minisystem** command and enter the password of user **root** as prompted to enter the minisystem view.

Step 3 Run the **nvme list** command to query the NVMe SSD information. The following is an example. If the value in the **Format** column is **512**, you do not need to format the NVMe SSD. Otherwise, go to **Step 4**.

```
minisystem> nvme list
Node                  SN                   Model                                    Namespace Usage
Format         FW Rev
--------------------- -------------------- ---------------------------------------- --------- --------------------------
---------------- --------
/dev/nvme0n1          2102313VGR10NB100090 HSSD-D7B84PP1T6N                         1          1.60  TB /
1.60  TB    512   B +  8 B   7306
/dev/nvme1n1          2102313VGR10NB100083 HSSD-D7B84PP1T6N                         1          1.60  TB /
1.60  TB    512   B +  8 B   7306
```

Step 4 Run the **format_ssd.sh format_minisystem** *disksn* command to format the NVMe SSD. The following is an example.

```
minisystem> format_ssd.sh format_minisystem 2102313VGR10NB100090
You are about to format nvme0n1, namespace 0xffffffff(ALL namespaces).
Namespace nvme0n1 has parent controller(s):nvme0
WARNING: Format may irrevocably delete this device's data.
You have 10 seconds to press Ctrl-C to cancel this operation.
Use the force [--force|-f] option to suppress this warning.
Sending format operation ...
Success formatting namespace:ffffffff
result=1;value=no;
```

NOTE

- In the command, *disksn* is the SN of the NVMe SSD displayed in the **SN** column in **Step 3**.
- If **Success formatting namespace:ffffffff** is displayed in the command output, the formatting is successful. Otherwise, contact technical support.
- If multiple NVMe SSDs on a node need to be formatted, run this command for each NVMe SSD.

Step 5 Repeat the preceding steps to format NVMe SSDs on other nodes.

----End

5.5.19 Uninstalling OceanStor Pacific Series Software

Context

This section describes how to uninstall OceanStor Pacific series software from a single node. To uninstall the software from the entire cluster, perform this operation on each node in the cluster.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

If a maintenance terminal runs the Windows OS, the Secure Shell (SSH) client software has been obtained.

Procedure

Step 1 Disable the security sandbox by referring to **Routine Management** > **Managing a Cluster System** > **Managing Hardware Information** > **Disabling Security Sandbox** in *OceanStor Pacific Series 8.2.1 Administrator Guide*.

NOTE

- During the software installation of OceanStor Pacific series, the security sandbox is automatically enabled after the "Install Storage Node" step is complete.
- The security sandbox supports only the standard storage OS. Other non-standard OSs do not support the security sandbox function.
- You can also run the **closesandbox** command in the cliportal view to disable the security sandbox. When the security sandbox is enabled, use an SSH tool to log in to a node as user **fsadmin** and directly enter the cliportal view. To obtain the default account password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)*. You need to change the default password upon the first login.

Step 2 Close the DeviceManager GUI and clear the browser cache.

Step 3 Use SSH to log in to a node as user **fsadmin**.

Step 4 Run the **su - root** command and enter the password of user **root** as prompted to switch to user **root**.

Step 5 Run the software uninstallation script.

- When the management and storage nodes are deployed on the same server, if storage nodes fail to be added, you only need to uninstall software related to the storage nodes (excluding software related to the management nodes).

  Run the following command to uninstall the software and enter **yes** as prompted to confirm the operation.

  ```
  cd /opt/fusionstorage/deploymanager/clouda;\
  bash clear_extension_for_fsm_node.sh
  ```

- Other scenarios:

  Run the following command to uninstall the software and enter **yes** as prompted to confirm the operation.

  ```
  clear_script='/opt/fusionstorage/deploymanager/clouda/clear_all_for_fs_manual.sh';\
  [ ! -f "${clear_script}" ] && clear_script='/opt/fusionstorage/repository/deploymanager_pkg/
  DSwareSoft/clear_all_for_fs_manual.sh';\
  [ ! -f "${clear_script}" ] && clear_script='/opt/fusionstorage/repository/deploymanager_pkg/
  dfvmanager/clear_all_for_fs_manual.sh';\
  [ ! -f "${clear_script}" ] && clear_script='/opt/fusionstorage/deploymanager/clouda/
  clear_all_for_fs_node.sh all';\
  bash ${clear_script}
  ```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- After the uninstallation script is executed on a storage node, the iBMA component will be uninstalled. After the iBMA component is uninstalled, the network port name information of the node cannot be viewed in the iBMC system.
- After the script is executed, the last line in the command output indicates the processing result. If the execution fails, rectify the fault as prompted.
- If the uninstallation fails, restart the node and run the uninstallation script again.
- If no response is returned after you run the script, press **Ctrl+C** to stop and then run the script again. If the uninstallation still fails, contact Huawei technical support engineers. To contact technical support:

  For carrier users, log in to **https://support.huawei.com**.

  For enterprise users, log in to **https://e.huawei.com**.

  After logging in to the preceding website, you can select an area to obtain the technical support contact information of the area.

Step 6 Run the **cat /sys/fs/cgroup/cpuset/system.slice/cpuset.cpus** command to check CPU binding information.

If the file exists and the command output is not empty, residual CPU binding information exists. Run the **reboot** command to restart the node to clear the residual information. The following is an example:

```
[root@localhost ~]# cat /sys/fs/cgroup/cpuset/system.slice/cpuset.cpus
93-95
[root@localhost ~]# reboot
```

----End

5.5.20 Installing the iBMA Component

Context

This section describes how to install the iBMA component. After the iBMA component is installed, you can view the network port name information of nodes in the iBMC system.

Prerequisites

You have obtained software package **OceanStor-Pacific_8.2.1RC1.tar.gz**.

Procedure

Step 1 Use SSH to log in to a node as user **fsadmin**. To obtain the default user password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)* or *OceanStor Pacific Series 8.2.1 Account List (Block Service)*. You need to change the default password upon the first login.

Step 2 Run the **su - root** command and enter the password of user **root** as prompted to switch to user **root**.

Step 3 Run the **uname -r** command to check the system architecture. If *xxx*.**aarch64** is displayed in the command output, the system architecture is Arm. If *xxx*.**x86_64** is displayed in the command output, the system architecture is x86.

An example of the Arm system architecture is as follows:

 Copyright © Huawei Technologies Co., Ltd.

```
uname -r
xxx.aarch64
```

An example of the x86 system architecture is as follows:

```
uname -r
xxx.86_64
```

Step 4 Obtain the iBMA component package.

1. Use a decompression tool to open the directory where **OceanStor-Pacific_8.2.1RC1.tar.gz** is saved.
2. Obtain the hwmgt component package.
   a. Open **OceanStor-Pacific_8.2.1RC1.tar.gz\OceanStor-Pacific_8.2.1RC1.tar\OceanStor-Pacific_8.2.1RC1\packages** to obtain software package **FusionStorage_hwmgt**_*System architecture*_**1.0.0.release.***xxx***.tar.gz**.
   b. Determine the software package based on the system architecture. The software package for the Arm system architecture is **FusionStorage_hwmgt_aarch64_1.0.0.release.***xxx***.tar.gz**, and that for the x86 system architecture is **FusionStorage_hwmgt_x86_64_1.0.0.release.***xxx***.tar.gz**.
   c. Open **FusionStorage_hwmgt**_*System architecture*_**1.0.0.release.***xxx***.tar.gz\FusionStorage_hwmgt**_*System architecture*_**1.0.0.release.***xxx***.tar\FusionStorage_hwmgt**_*System architecture*_**1.0.0.release.***xxx***\packages** to obtain hwmgt component package **hwmgt_1.0.0.release.***xxx***.tar.gz**.

Step 5 Upload hwmgt component package **hwmgt_1.0.0.release.***xxx***.tar.gz** to a directory (not **/tmp**) on the node where the iBMA component is to be installed.

Step 6 Install the iBMA component.

1. Go to the path where the hwmgt component package is saved.
   ```
   cd /Save path
   ```
2. Decompress the hwmgt component package.
   ```
   tar zxf hwmgt_1.0.0.release.*.tar.gz
   ```
3. Go to the directory where the installation script is saved.
   ```
   cd hwmgt_1.0.0.release.*/action/ibma_script
   ```
4. Execute the script to install and start the iBMA component.
   ```
   sh appctl.sh install
   sh appctl.sh start
   ```

Step 7 Wait for three minutes and run the **systemctl status iBMA | grep running** command to check the iBMA component status.

If the command output is not empty, the iBMA component is normal. Otherwise, contact Huawei technical support engineers.

Step 8 Delete the iBMA component package and decompression directory.

```
cd /Save path
rm -rf hwmgt_1.0.0.release.*.tar.gz hwmgt_1.0.0.release.*
```

----End

 Copyright © Huawei Technologies Co., Ltd.

5.5.21 Identifying the Installation Mode

Procedure

Step 1 Obtain the installation information.

1. Use SSH to log in to a management node as user **fsadmin**. To obtain the default user password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)* or *OceanStor Pacific Series 8.2.1 Account List (Block Service)*. You need to change the default password upon the first login.
2. Run the **su - root** command to switch to user **root**.
3. Check whether the node is a pre-installed node. If yes, go to **Step 1.4**. Otherwise, go to **Step 1.5**.

   Run the **ls -l** *File name* command to check whether the **/home/.preinstall**, **/opt/fusionstorage/.preinstall**, and **/opt/fusionstorage/.production_preinstall** files exist. If any of the files exists, the node is a pre-installed node.

   The following example indicates that the **/home/.preinstall** file exists:

   ```
   [root@FSM1 ~]# ls -l /opt/fusionstorage/.production_preinstall
   ls: cannot access '/opt/fusionstorage/.production_preinstall': No such file or directory
   [root@FSM1 ~]# ls -l /opt/fusionstorage/.preinstall
   ls: cannot access '/opt/fusionstorage/.preinstall': No such file or directory
   [root@FSM1 ~]# ls -l /home/.preinstall
   -rw------- 1 root root 0 Feb 21 15:32 /home/.preinstall
   ```
4. Run the **cat /etc/dfv/product.ini | grep product_version | awk -F '= ' '{print $2}'** command to check the node version.
5. Repeat **Step 1.1** to **Step 1.4** to check whether the other management node is a pre-installed node.

Step 2 Identify the installation mode according to the obtained installation information.

- If both management nodes are pre-installed nodes and the pre-installed version is the target version, the pre-installation mode is used.
- In other scenarios, the regular installation mode is used. If either or both of the two management nodes are pre-installed nodes, uninstall the storage software from each pre-installed node by referring to **5.5.19 Uninstalling OceanStor Pacific Series Software**.

----End

5.5.22 Importing the OS Certificate of a DPC Node

Context

The OS installed on a DPC node supports two boot modes: Legacy BIOS and UEFI. In UEFI boot mode, the Secure Boot function is added to improve OS security. If this function is enabled and the signature of the kernel module is not imported when the kernel module is loaded, the loading will fail.

For compute nodes that support Secure Boot, perform the following operations to import the certificate of Huawei storage software package **OceanStor-Pacific_8.2.1RC1.tar.gz**.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

Before importing a certificate, ensure that the **mokutil** command is available.

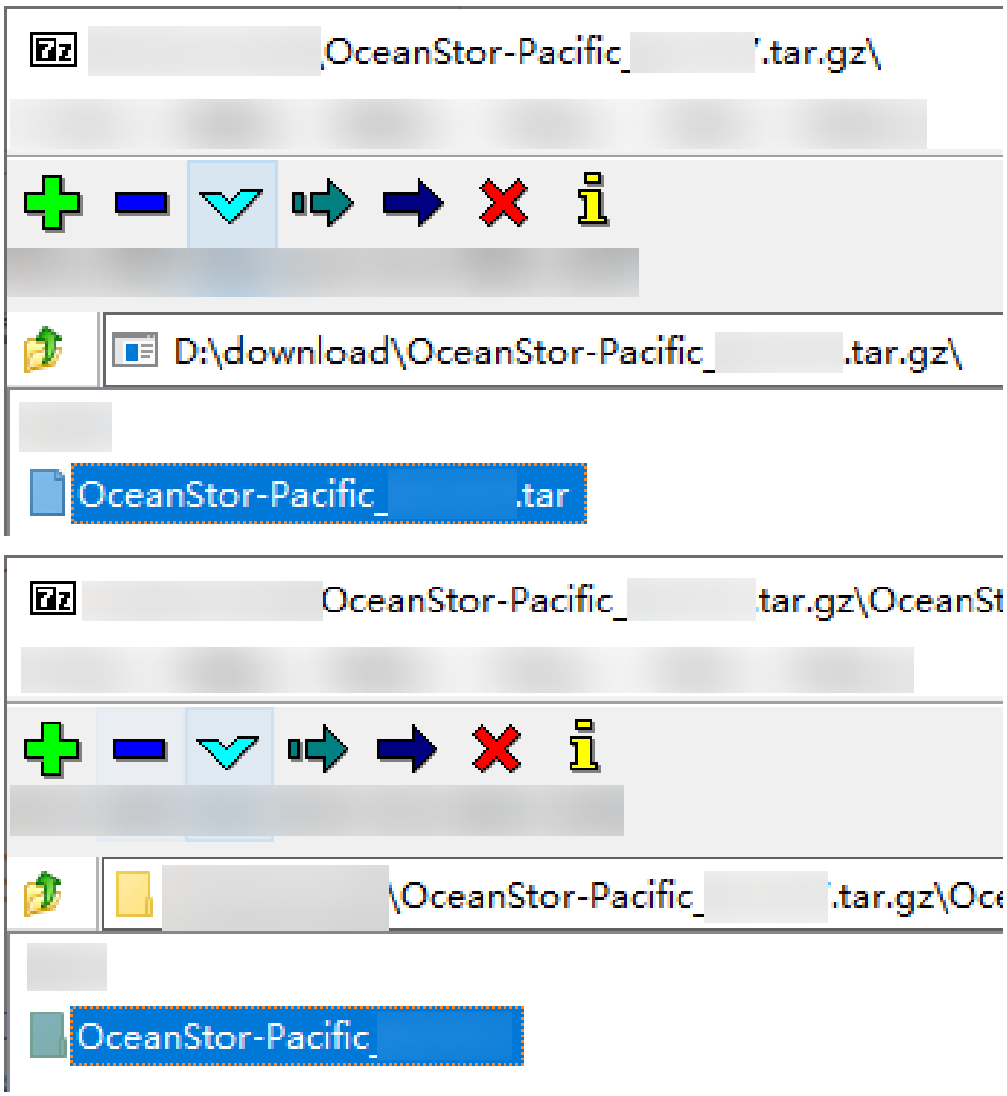
Procedure

Step 1 Obtain the certificate file from the OceanStor Pacific series storage software package downloaded from the Huawei support website.

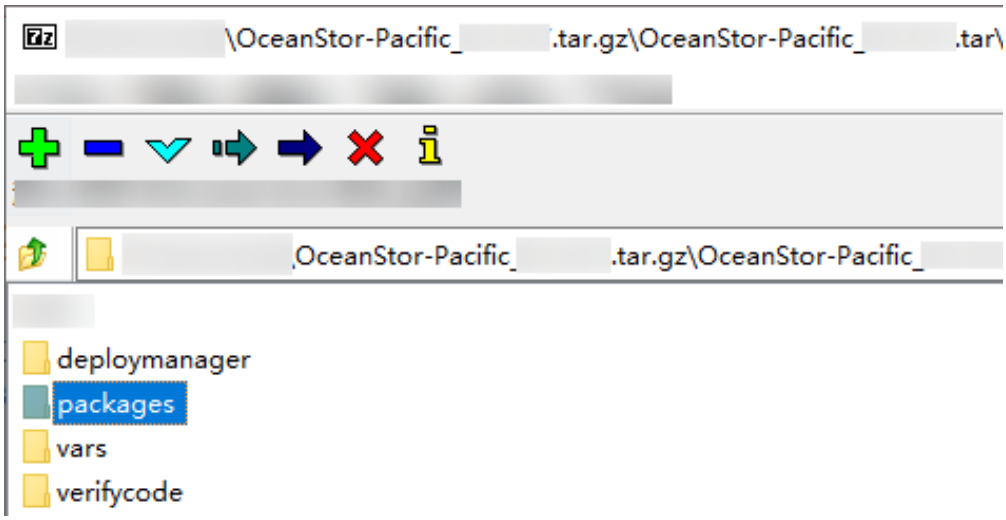
NOTE

For enterprise users, log in to **https://support.huawei.com/enterprise**. For carrier users, log in to **https://support.huawei.com**. In the search box, enter **OceanStor Pacific** and click the suggested path to enter the corresponding product page. For enterprise users, click **Software Download**. For carrier users, click **Software**. Search for and download the software package of the desired version.

1. Use the decompression tool to open the **OceanStor-Pacific_8.2.1RC1.tar.gz** storage software package and then the **OceanStor-Pacific_8.2.1RC1.tar** package, and go to the **OceanStor-Pacific_8.2.1RC1** > **packages** directory.



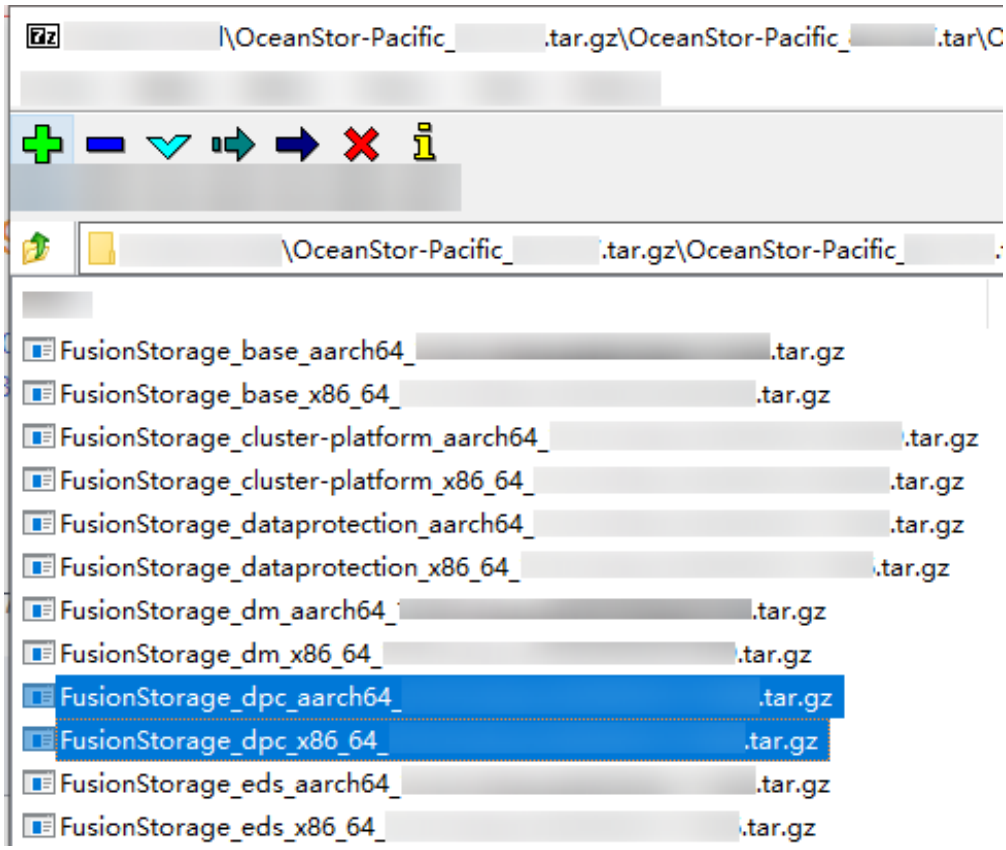
 Copyright © Huawei Technologies Co., Ltd.



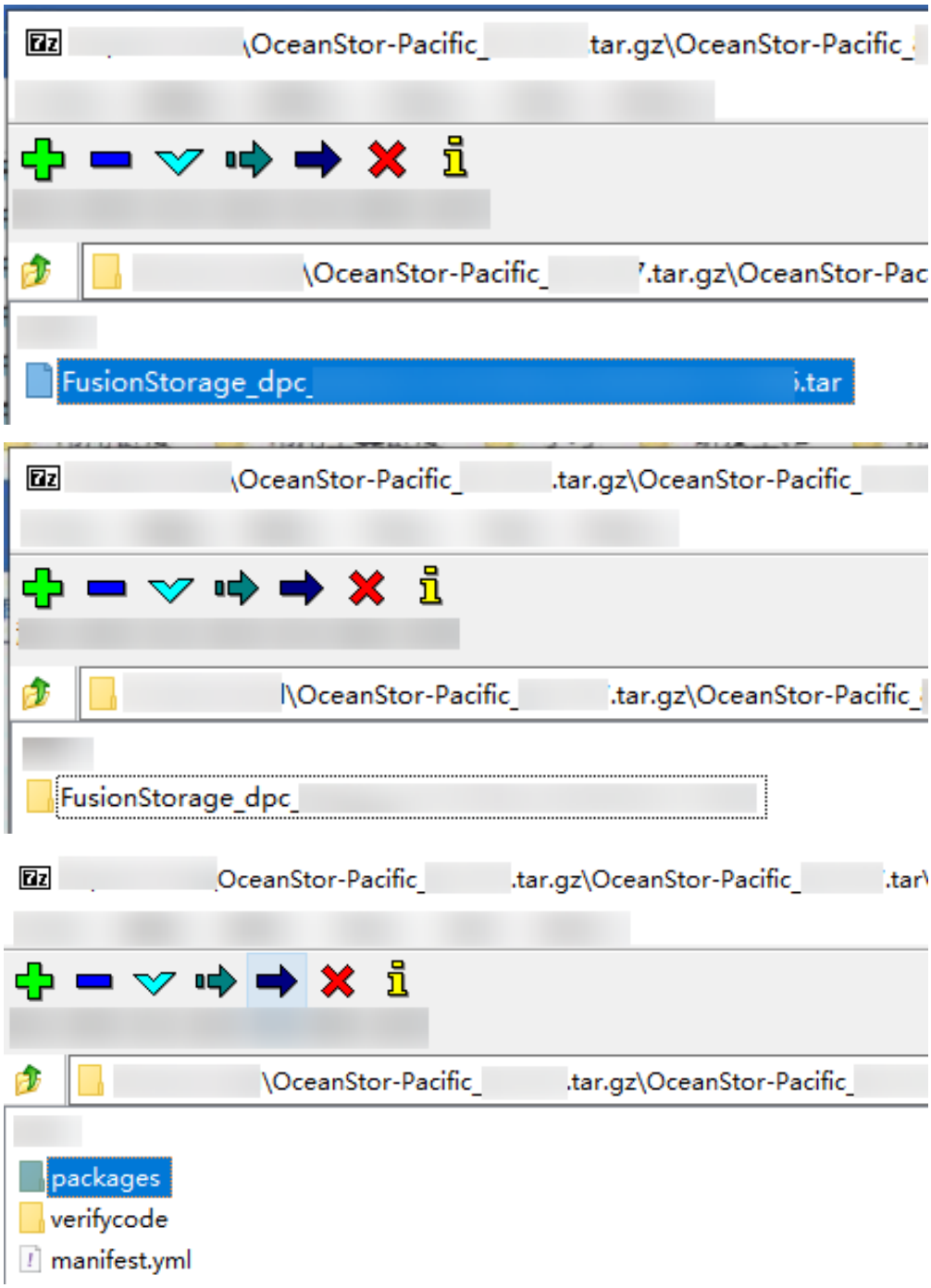
2. Open the **FusionStorage_dpc**_*xxx.xxx*.**tar.gz** package and then the **FusionStorage_dpc**_*xxx.xxx*.**tar** package, and go to the **FusionStorage_dpc**_*xxx.xxx* > **packages** directory.

   NOTE

   - For an x86-based node, open the **FusionStorage_dpc_x86_64.***xxx*.**tar.gz** package.
   - For an Arm-based node, open the **FusionStorage_dpc_aarch64.***xxx*.**tar.gz** package.

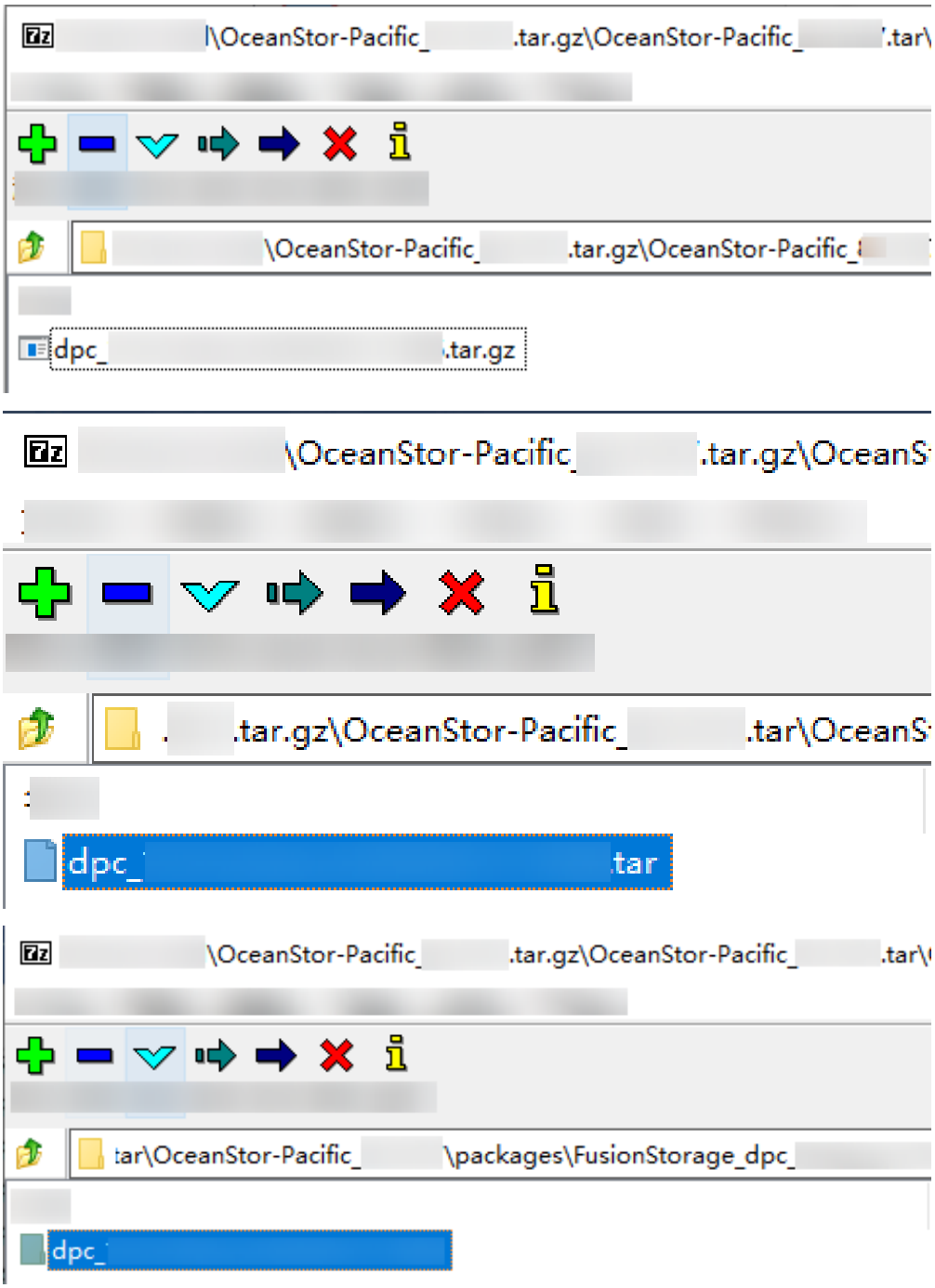


 Copyright © Huawei Technologies Co., Ltd.

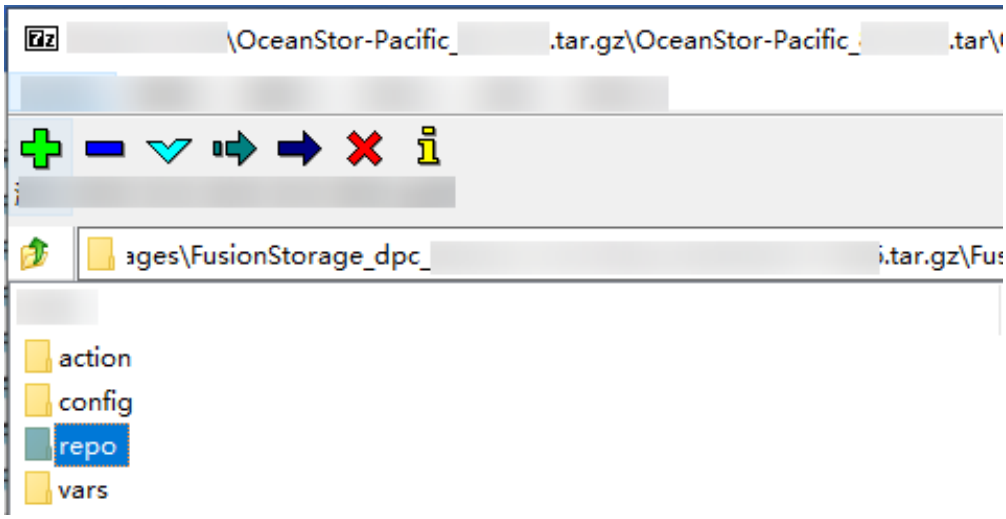


3. Open the **dpc**_*xxx*.**tar.gz** package and then the **dpc**_*xxx*.**tar** package, and go to the **dpc**_*xxx* > **repo** directory.

 Copyright © Huawei Technologies Co., Ltd.



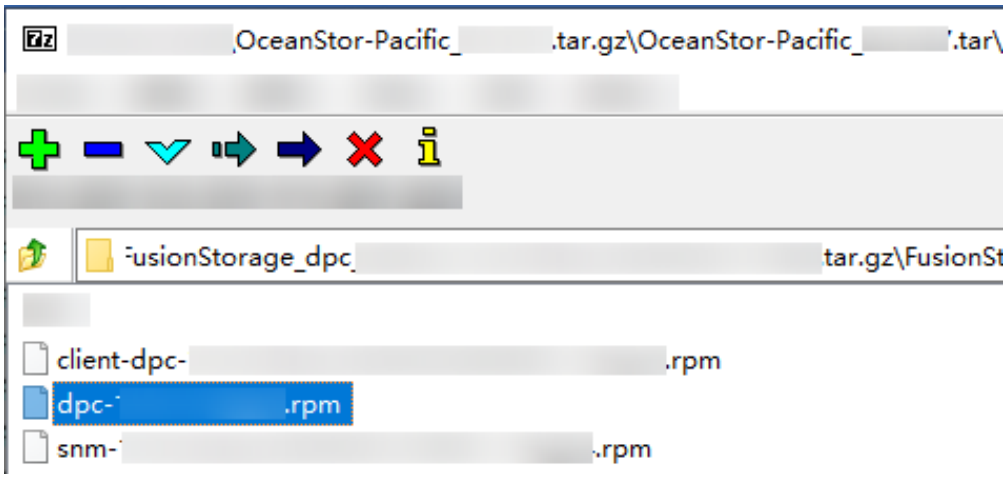
 Copyright © Huawei Technologies Co., Ltd.

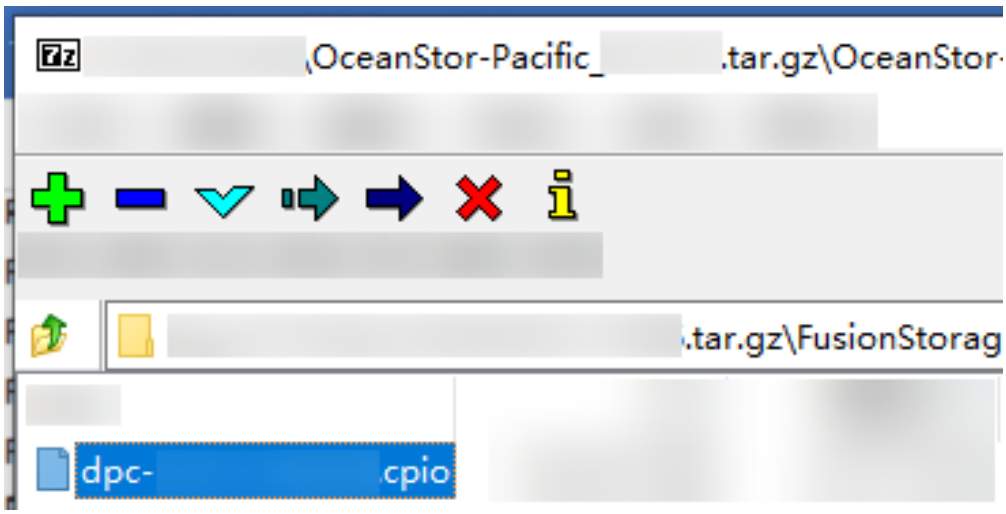


4. Open the **dpc-*xxx*.rpm** package and then the **dpc-*xxx*.cpio** package.

   NOTE

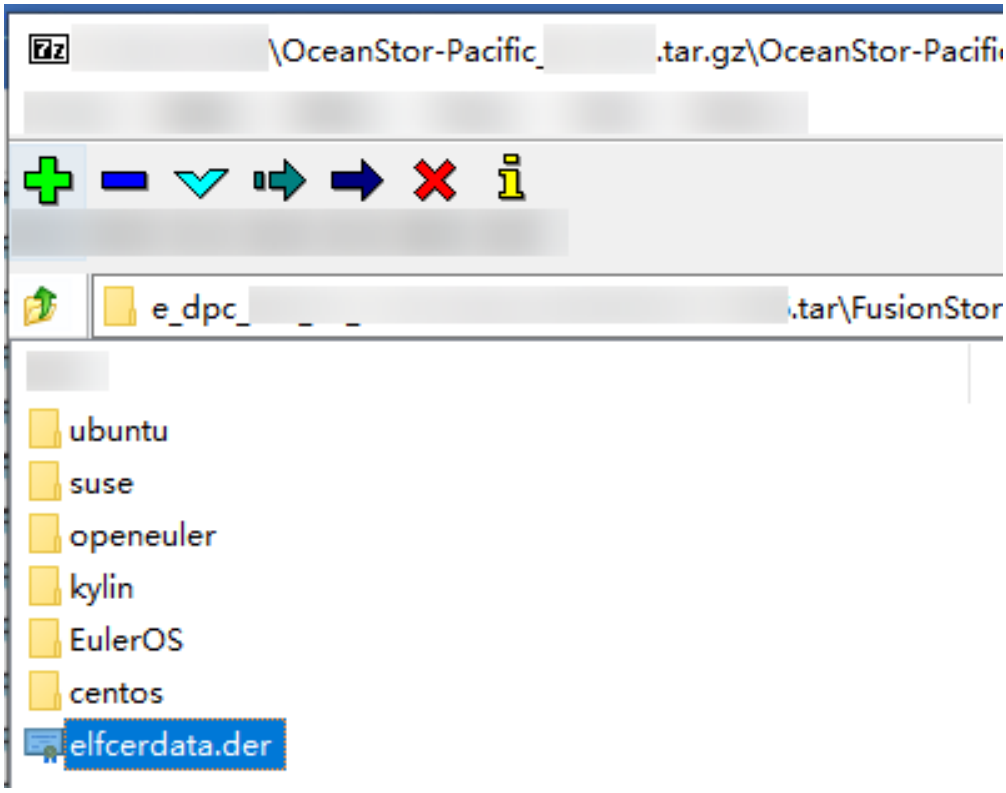
   - For an x86-based node, open the **dpc-*xxx*.x86_64.rpm** and **dpc-*xxx*.x86_64.cpio** packages.
   - For an Arm-based node, open the **dpc-*xxx*.aarch64.rpm** and **dpc-*xxx*.aarch64.cpio** packages.





 Copyright © Huawei Technologies Co., Ltd.

5. Go to the **opt** > **fusionstorage** > **dpc** > **ko** directory in sequence, and locate the **elfcerdata.der** certificate file.



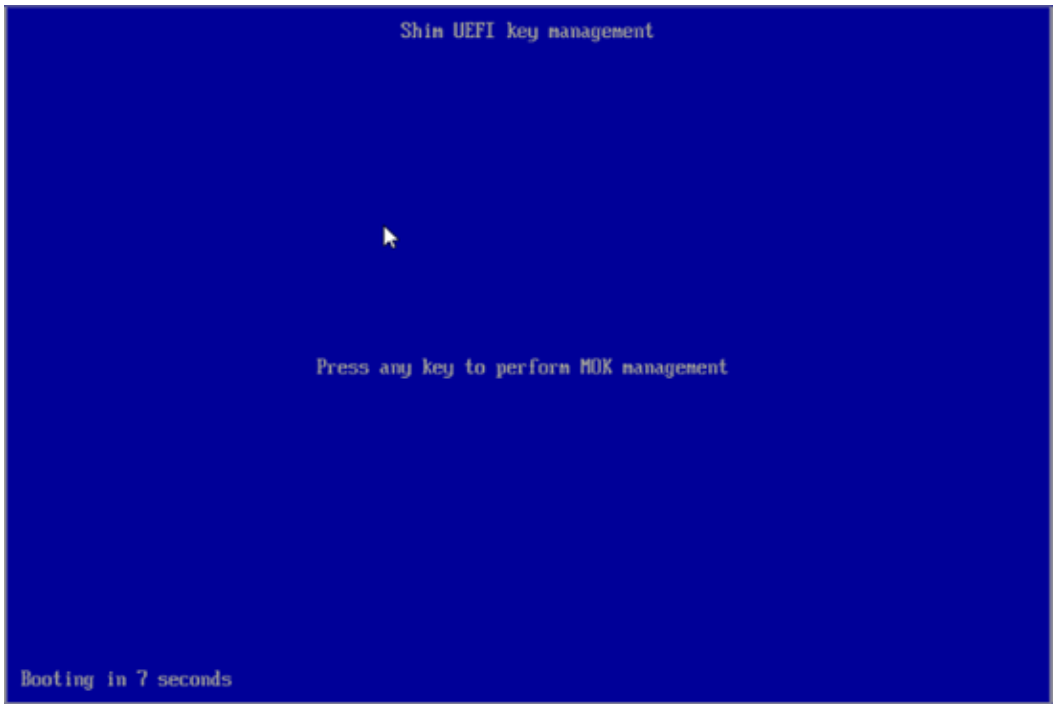
Step 2 Upload the certificate file to the **/tmp** directory on each compute node.

Step 3 Run the **mokutil --import /tmp/elfcerdata.der** command as user **root** to import the certificate. You will be prompted to set a password, which will be used in subsequent steps. You can set a password as required. Then run the **reboot** command to restart the node.

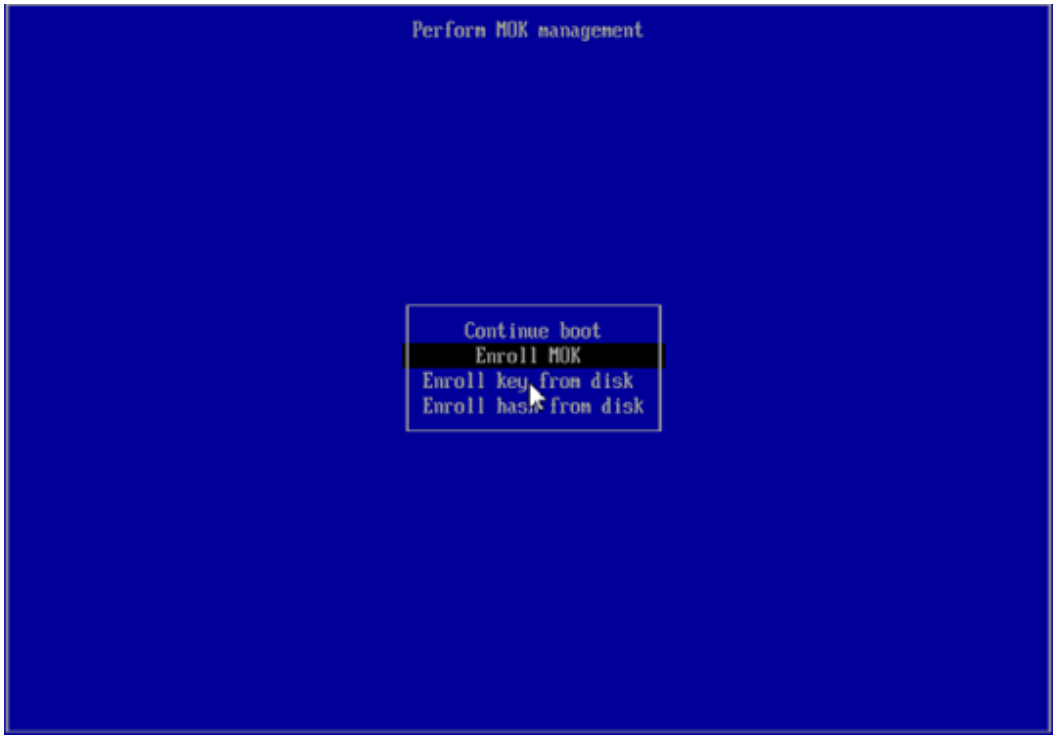
```
localhost:~# mokutil --import /tmp/elfcerdata.der
input password:
input password again:
localhost:~# reboot
```

Step 4 After the node is restarted, go to the UEFI certificate setting wizard and press **Enter**.

 Copyright © Huawei Technologies Co., Ltd.



Step 5 On the **Perform MOK management** page, select **Enroll MOK**, and then press **Enter**.



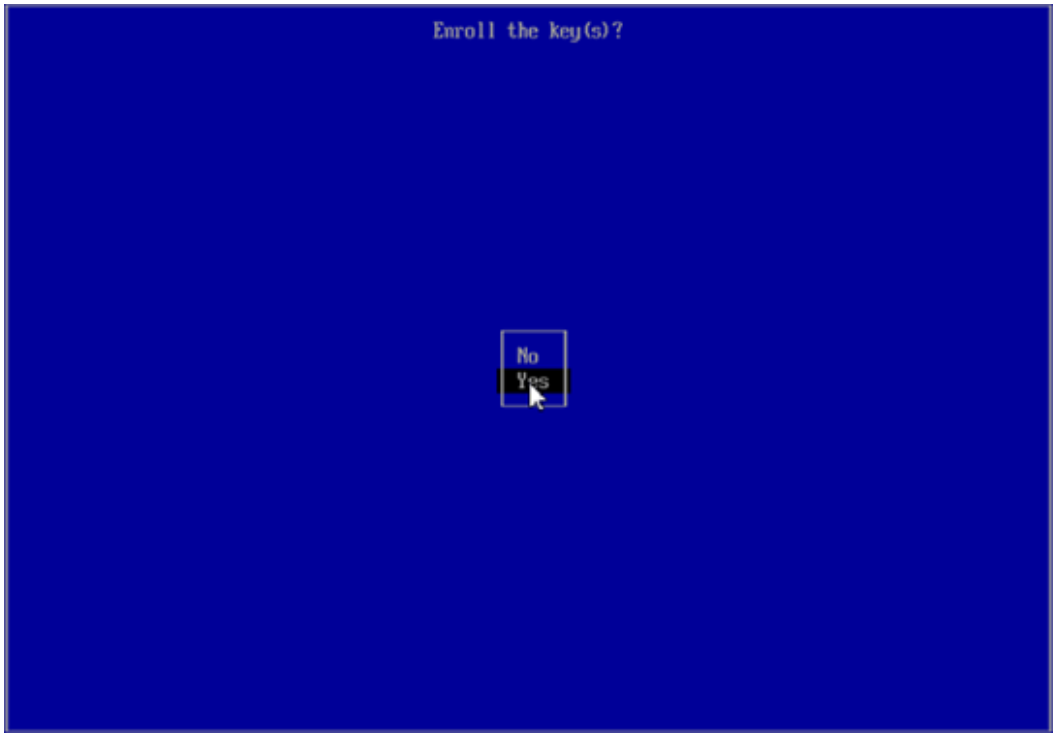
Step 6 On the **Enroll MOK** page, you can select **View key 0** to view the current certificate.

 Copyright © Huawei Technologies Co., Ltd.

Step 7 Press **Esc** to return to the **Enroll MOK** page. Select **Continue** and press **Enter**.

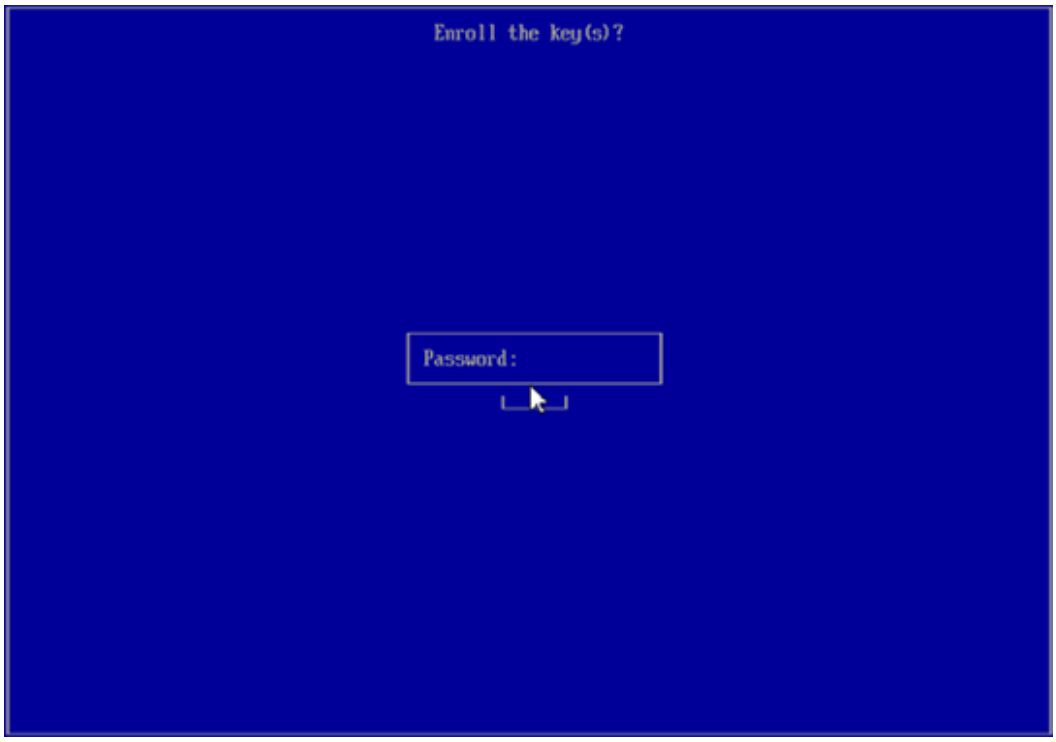
 Copyright © Huawei Technologies Co., Ltd.

Step 8 On the **Enroll the key(s)?** page, select **Yes** and press **Enter**.

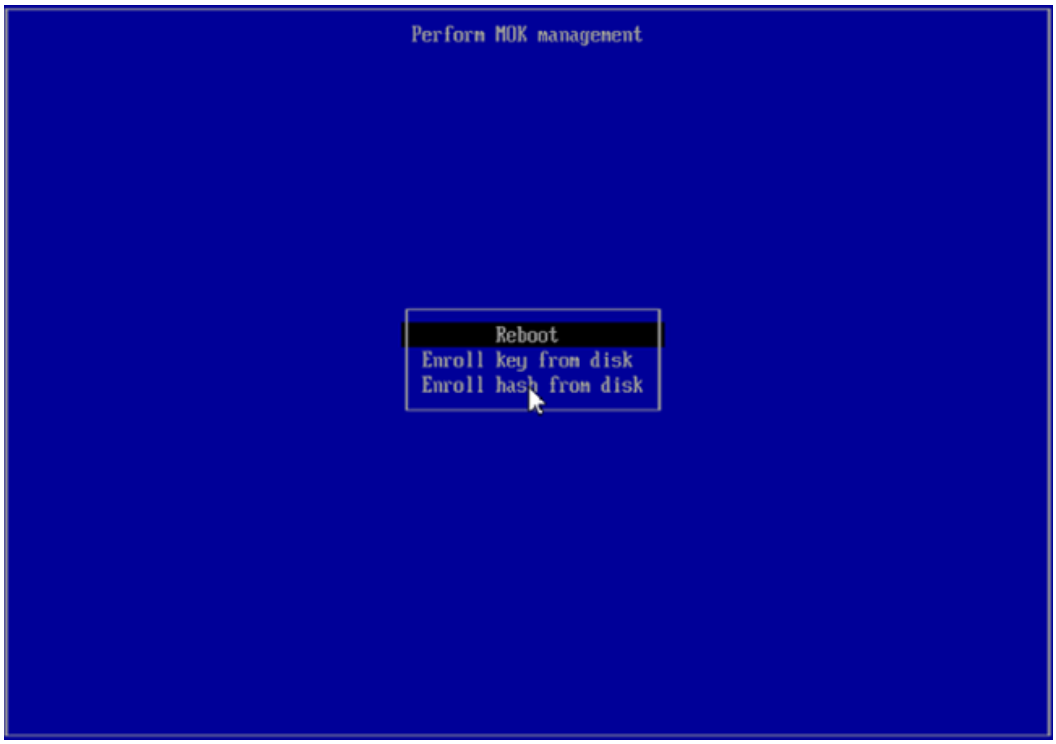


Step 9 Enter the password set in **Step 3** and press **Enter**.

 Copyright © Huawei Technologies Co., Ltd.



Step 10 Return to the **Perform MOK management** page, select **Reboot**, and press **Enter** to restart the system.



----End

5.5.23 Obtaining the Node Installation Resource Package

This section describes how to export the resource package required for node installation.

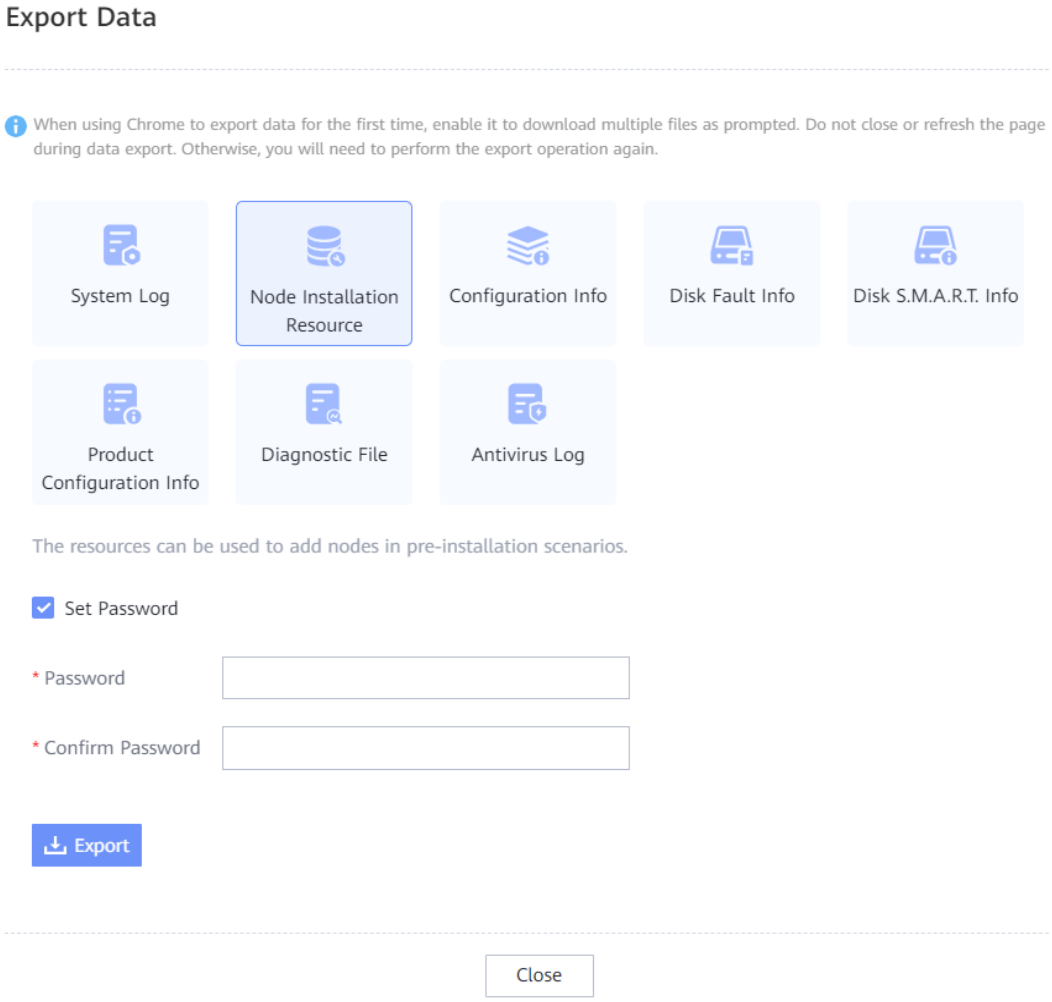
 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Go to the page for obtaining node installation resources.

Log in to DeviceManager, click on the right of the menu bar, and select **Export Data**.

On the **Export Data** page that is displayed on the right, select **Node Installation Resource**.

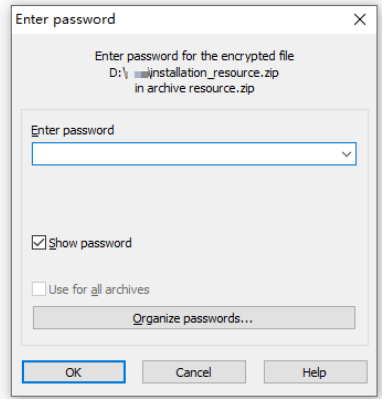


Step 2 Export the resource package.

- Select **Set Password**. This option is selected by default.
  a. Set a password for decompressing the resource package in the **Password** and **Confirm Password** text boxes.
  b. Click **Export** to obtain resource package **resource.zip**.
  c. Decompress resource package **resource.zip** to obtain installation resource package **installation_resource.zip**.
     - Windows:

       Use a local decompression software to decompress the package and enter the decompression password set in **Step 2.a** as prompted. The following is an example.

 Copyright © Huawei Technologies Co., Ltd.



  - Linux:
    1) Upload resource package **resource.zip** to the node.
    2) Log in to the node and go to the directory where resource package **resource.zip** is stored.
    3) Run the **unzip resource.zip** command to decompress the package and enter the decompression password set in **Step 2.a** as prompted. The following is an example.

```
unzip resource.zip
Archive:  resource.zip
[resource.zip] installation_resource.zip password:
inflating: installation_resource.zip
```

- Deselect **Set Password**.

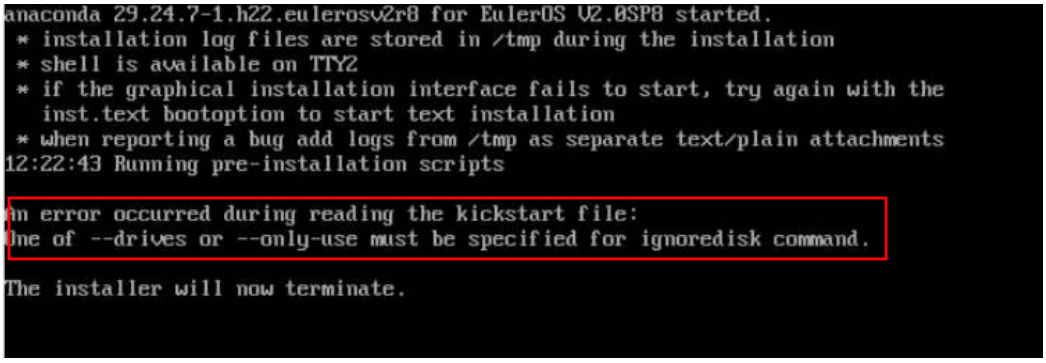
  Click **Export** to obtain installation resource package **installation_resource.zip**.

----End

5.5.24 FAQs

5.5.24.1 Failed to Install the Scale-Out Storage OS Using the 3108 or 3416 RAID Controller Card

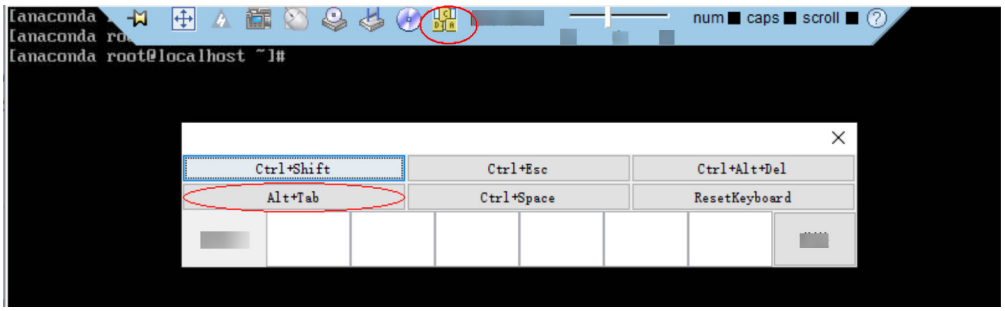
The scale-out storage OS cannot identify the 3108 or 3416 RAID controller cards. As a result, the following error message is displayed during the installation of the scale-out storage OS:



 Copyright © Huawei Technologies Co., Ltd.

Perform the following operations:

Step 1 On the iBMC WebUI, press **Alt+Tab** to switch to the minisystem mode.



Step 2 In minisystem mode, open image installation file **vi /run/install/ks.cfg**.

Step 3 Modify the RAID controller card configuration. Search for keyword **raid_card_flag=** and modify configuration item **raid_card_flag=`lspci | grep -E 'SAS3508|SAS3408|SAS3008|Smart Storage PQI'**.

- For the 3108 RAID controller card, change it to **raid_card_flag=`lspci | grep -E 'SAS3508|SAS3408|SAS3008|3108|Smart Storage PQI'**.
- For the 3416 RAID controller card, change it to **raid_card_flag=`lspci | grep -E 'SAS3508|SAS3408|SAS3008|3416|Smart Storage PQI'**.
- Search for keyword **raid_flag=`** and change the following configuration

  raid_flag=`udevadm info ${cur_disk} | grep -E "ID_VENDOR=AVAGO|ID_VENDOR=LSI|ID_VENDOR=MSCC|ID_VENDOR=Adaptec"`

  to

  raid_flag=`udevadm info ${cur_disk} | grep -E "ID_VENDOR=AVAGO|ID_VENDOR=LSI|ID_VENDOR=MSCC|ID_VENDOR=Adaptec|ID_VENDOR=BROADCOM"`

  NOTE

  For x86 servers, only the raid_flag=`udevadm info ${cur_disk} | grep -E "ID_VENDOR=AVAGO|ID_VENDOR=LSI|ID_VENDOR=MSCC|ID_VENDOR=Adaptec"` configuration item needs to be modified.

Step 4 Save the file and exit to the minisystem. Then, run the **systemctl restart anaconda** command to restart the installation service. If the installation fails again, contact technical support engineers.

----End

5.5.24.2 How Do I Solve the Problem That the Number of PFC-enabled Queues Exceeds the Upper Limit?

Scenarios

If the following error message is displayed when PFC is enabled globally, delete all PFC priority configurations and reconfigure them.

```
[~HUAWEI-dcb-pfc-default]priority 2 4
Error: The number of PFC-enabled queues exceeds the upper limit (2).
```

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run the **display this** command to view the PFC configurations. In the following example, PFC priority "2 3" has been configured.

```
[~HUAWEI-dcb-pfc-default]display this
#
dcb pfc
priority 2 3
priority 2 error-down threshold 20
priority 2 turn-off threshold 10
priority 3 error-down threshold 20
priority 3 turn-off threshold 10
#
```

- If the command output is not empty, run **undo** commands to delete all PFC priority configurations. For example, to delete PFC priority "2 3", run the following commands:

  ```
  [~HUAWEI-dcb-pfc-default]undo priority 2 error-down threshold 20
  [*HUAWEI-dcb-pfc-default]undo priority 2 turn-off threshold 10
  [*HUAWEI-dcb-pfc-default]undo priority 3 error-down threshold 20
  [*HUAWEI-dcb-pfc-default]undo priority 3 turn-off threshold 10
  [*HUAWEI-dcb-pfc-default]undo priority 2 3
  ```

- If the command output is empty, delete PFC priority "3".

  ```
  [*HUAWEI-dcb-pfc-default]undo priority 3
  ```

Step 2 Configure PFC priority "2 4".

```
[*HUAWEI-dcb-pfc-default]priority 2 4
[~HUAWEI-dcb-pfc-default]commit
```

----End

5.5.25 Other Operations

5.5.25.1 Uploading Files to a Node Using FileZilla

Prerequisites

The network between the installation PC and node is normal.

Procedure

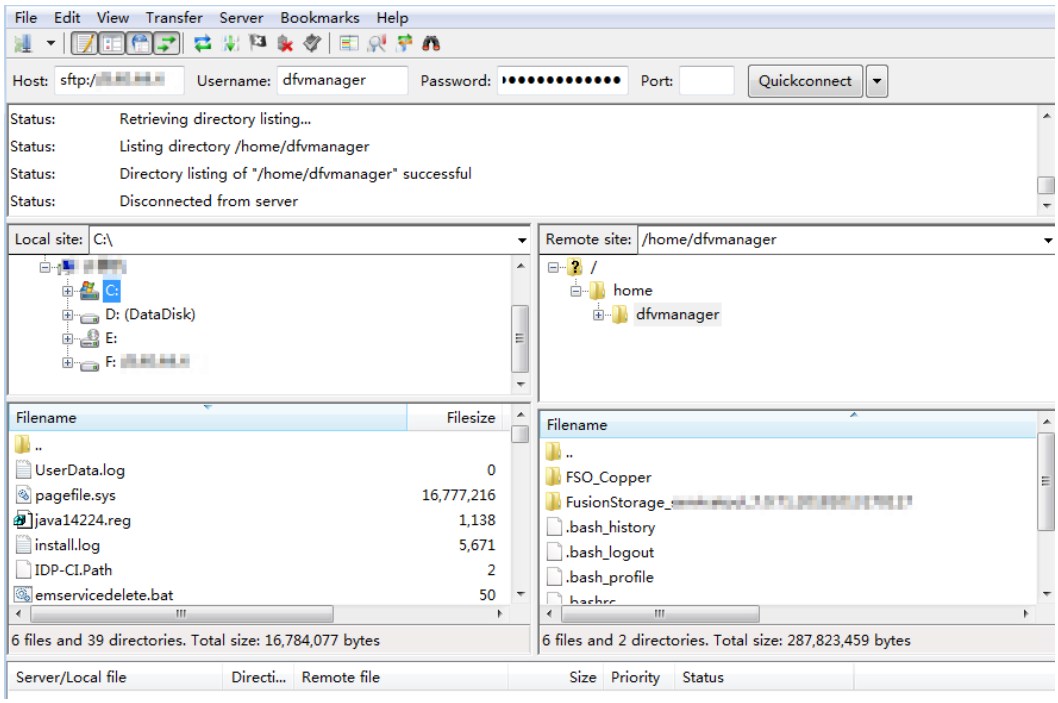
Step 1 Double-click the program file in the installation PC.

Enter **sftp://***xxx.xxx.xxx.xxx* in the **Host** text box, set **Username** and **Password**, and click **Quickconnect**, as shown in **Figure 5-43**.

xxx.xxx.xxx.xxx indicates the management plane IP address of a node.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-43 FileZilla page



Step 2 Upload the software package to be uploaded to the specified directory on the target node.

NOTE

If you want to download a file from a node to the local host, drag the file to be downloaded from the right to the left.

----End

5.5.25.2 Importing Environmental Variables

Scenarios

After the system is installed, the authentication mode is enabled by default. You need to import environment variables before executing CPS and OpenStack commands.

Procedure

Step 1 Run the following command to import the environment variables:

source set_env

Information similar to the following is displayed:

```
please choose environment variable which you want to import:
(1) openstack environment variable (keystone v3)
(2) cps environment variable
(3) openstack environment variable legacy (keystone v2)
please choose:[1|2|3]
```

Step 2 Select an authentication mode.

 Copyright © Huawei Technologies Co., Ltd.

- To enable Keystone V3 authentication, enter **1**, press **Enter**, and enter the password of **OS_USERNAME** as prompted. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)* or *OceanStor Pacific Series 8.2.1 Account List (Block Service)*. You need to change the default password upon the first login.

  The environment variables are imported successfully if the command outputs of **cps host-list** and **nova list** are automatically displayed. After the environment variables are imported, the system uses Keystone V3 authentication, and you can run both CPS and OpenStack commands.

  Keystone V3 authentication is recommended after FusionSphere OpenStack is installed and deployed.

- To enable CPS authentication, enter **2**, press **Enter**, and enter the user name and password of **CPS_USERNAME** as prompted.

  The user name is **cps_admin**.

  The environment variables are imported successfully if the command output of **cps host-list** is automatically displayed. After using CPS authentication to import the environment variables, you can run only CPS commands. Therefore, the **ERROR...** message is displayed after running the **nova list** command.

  CPS authentication is recommended only when the FusionSphere OpenStack deployment is incomplete, OpenStack authentication is unavailable, or an exception occurs in Keystone authentication.

- To enable Keystone V2 authentication of OpenStack, enter **3**, press **Enter**, and enter the password of **OS_USERNAME** as prompted.

  The environment variables are imported successfully if the command outputs of **cps host-list** and **nova list** are automatically displayed. After the environment variables are imported, the system uses Keystone V2 authentication, and you can run both CPS and OpenStack commands.

Step 3 **Optional:** In multi-DC scenarios, if glance is separately deployed in each DC, run the following command to import **OS_IMAGE_URL** to the DC when importing environment variables to the DC:

export OS_IMAGE_URL=https://image.*az.dc.domainname.com:443*

In the preceding command, *az.dc.domainname.com:443* is the glance domain name configured in the DC.

----End

5.5.25.3 Installing LFTP

Scenarios

If a third-party backup node is planned for a management node, install the LFTP software on the management node.

Prerequisites

You have obtained the LFTP software package from the LFTP official website.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Upload LFTP software package **lftp-8.2.1RC1.rpm** to the **home** directory of the management node.

For details, see **5.5.25.1 Uploading Files to a Node Using FileZilla**.

Step 2 Log in to the management node as user **fsadmin**. To obtain the default password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)* or *OceanStor Pacific Series 8.2.1 Account List (Block Service)*. You need to change the default password upon the first login.

Step 3 Run the **su - root** command to switch to user **root**.

Step 4 Run the **rpm -ivh lftp-8.2.1RC1.rpm** command to install the LFTP software.

Step 5 If management nodes are deployed in active/standby mode, repeat **Step 1** to **Step 4** to install the LFTP software on the other management node.

----End

5.5.25.4 Modifying the Management Node Network

Scenarios

If the External OM network is modified on FusionSphere OpenStack, the management node network must be modified accordingly.

Procedure

Step 1 Log in to the FusionSphere OpenStack controller node.

Step 2 Import environment variables. For details, see **5.5.25.2 Importing Environmental Variables**.

Step 3 Run the following command to query the External OM network IP address and management node VM ID allocated by the management node VM:

nova list | grep FusionStorageManager

Information similar to the following is displayed:

```
| b3edce1e-48fe-451f-821b-b8a3f57e2cf0| FusionStorageManager_dsware-server1_01 | ACTIVE | - |
Running | internal_base=172.28.12.142; external_om=192.168.92.66|
| 70eb3520-80d4-4930-a12d-609e98b165a8| FusionStorageManager_dsware-server1_02 | ACTIVE | - |
Running | internal_base=172.28.12.143; external_om=192.168.92.68|
```

Step 4 Run the following command to update the IP address of the management node VM in **metadata**:

nova meta *Management node VM ID* **set om-fixip=***Local IP address of the management node VM* **om-remote-ip=***Peer IP address of the management node VM* **om-netmask=***Subnet mask*

ID and IP address of the management node VM are those queried in **Step 3**.

Step 5 Log in to the FusionSphere OpenStack web client via the External API network.

The format of the login address is **https://***FusionSphere OpenStack reverse proxy IP address***:8890**, for example, **https://192.168.211.90:8890**.

 Copyright © Huawei Technologies Co., Ltd.

Login user name: **admin**. To obtain the default password, go to the "Type A (Portal)" sheet in *Huawei Cloud Stack 8.x.x Account List*. Then search for **FusionSphere OpenStack** in the **Product Name** column and find the **admin** account.

Step 6 Choose **Cloud Service** > **Huawei Distributed Block Storage**.

Step 7 Log in to the active management node using VNC.

Step 8 Run the following command to delete the HA configuration flag file.

rm -f /opt/dsware/manager/openstack/iscpsconfig

Step 9 Run the following command to restart the active management node VM:

reboot

Step 10 If management nodes are deployed in active/standby mode, configure the standby management node by repeating **Step 7** to **Step 9**.

----End

5.5.25.5 Obtaining the Compatibility Information Using Huawei Storage Interoperability Navigator

You can use Huawei Storage Interoperability Navigator to obtain the OceanStor Pacific series product compatibility information.

NOTICE

After obtaining the compatibility information of OceanStor Pacific series, visit the official websites of the nodes you plan to use and ensure that they are compatible with the components of OceanStor Pacific series, including OSs, SSD cards, and NICs. All components must meet the compatibility requirements of both OceanStor Pacific series and the nodes.

1. Log in to **Huawei Storage Interoperability Navigator**.
2. In **Compatible With**, select the type to be queried.
3. In **Storage Type**, select a service type.

5.5.25.6 Configuring Switch Ports in a Batch

To perform the same configuration on multiple Ethernet interfaces, you can use the port group function to add the Ethernet interfaces to the same port group in a batch. In the port group view, you need to run the configuration commands only once. Then, the configuration takes effect on all the Ethernet interfaces in the port group, reducing repeated configuration. The following is an example of port group configuration.

```
<HUAWEI> system-view
[~HUAWEI] port-group portgroup1
[*HUAWEI-port-group-portgroup1] group-member 25ge 1/0/e to 25ge 1/0/f  #e or f indicates a number.
[*HUAWEI-port-group-portgroup1] #Perform operations related to switch port commands.
[*HUAWEI-port-group-portgroup1] commit
[*HUAWEI-port-group-portgroup1] quit
[~HUAWEI] undo port-group portgroup1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[~HUAWEI] commit
[~HUAWEI] quit
<HUAWEI> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: Y
```

5.5.25.7 Changing the System Time of a Node

Prerequisites

- If a maintenance terminal runs the Windows OS, the Secure Shell (SSH) client software has been obtained.
- The security sandbox function is disabled for a node.

Procedure

Step 1 Use SSH to log in to a node as user **fsadmin**.

NOTE

To obtain the default user password, see *OceanStor Pacific Series 8.2.1 Account List (File, Object, and HDFS Service)* or *OceanStor Pacific Series 8.2.1 Account List (Block Service)*. You need to change the default password upon the first login. After the password is changed, log in to the node again. If the default password has been changed, use the new password to log in.

Step 2 Run the **su - root** command and enter the password of user **root** as prompted to switch to user **root**.

Step 3 Run the **date -s** *"Target date Target time"* command to change the system time. The following is an example.

```
[root@FSM1 ~]# date -s "2023-2-21 17:34"
Tue Feb 21 17:34:00 CST 2023
```

Step 4 Run the **hwclock -w** command to make the new date and time take effect permanently.

----End

 Copyright © Huawei Technologies Co., Ltd.

6 Basic Service Configuration

6.1 Before You Start
6.2 Installation Overview
6.3 Installation PC Requirements
6.4 Configuring Basic Services
6.5 Managing Basic Services

6.1 Before You Start

Instructions on Using the Security Sandbox

- Enabling the security sandbox function can improve system security and prevent untrusted users or attackers from logging in to the storage operating system (OS) through SSH to perform malicious operations. When the OceanStor Pacific Series 8.2.1RC1 software or later is installed for the first time, the security sandbox is automatically enabled on the added storage nodes.
- After the security sandbox is enabled, users can only use the **cli_portal** command after logging in to the OS. The **cli_portal** command can be used to run the CLI, **minisystem**, and **diagnose** (only for FSA nodes) commands. All commands or scripts that are directly executed on the OS cannot be executed, including common **ls**, **rm**, and **cat** commands, as shown in the following figure:

```
FSMA:cliportal> cat /etc/passwd
Error : Command 'cat' does not exist or has an incorrect format.
Try 'help' for more information.
```

- Before executing OS commands, disable the security sandbox by referring to **Routine Management** > **Managing a Cluster System** > **Managing Hardware Information** > **Disabling Security Sandbox** in *OceanStor Pacific Series 8.2.1 Administrator Guide*. After the OS commands are executed, enable the security sandbox by referring to **Routine Management** > **Managing a Cluster System** > **Managing Hardware Information** > **Enabling Security Sandbox** in *OceanStor Pacific Series 8.2.1 Administrator Guide*.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- You can also run the **closesandbox** command on the cli_portal to disable the security sandbox.
- The security sandbox supports only the standard storage OS. Other non-standard OSs do not support the security sandbox function.
- After the security sandbox function is disabled, the system is no longer protected by any security sandbox.
- After the security sandbox is disabled, you need to restart the session for the setting to take effect. After the security sandbox is disabled, you can enable it as required.
- The security sandbox is applicable to OceanStor Pacific series 8.1.3 and later versions.

6.2 Installation Overview

This chapter describes the key points of the installation solution, helping you quickly understand how to install OceanStor Pacific series software.

Select the desired installation process in the following sections according to the scenario of the file service to be installed (standard protocol scenario, DPC scenario, or DPC and standard protocol hybrid scenario) and the installation mode (LLD-based or wizard-based configuration mode). During software installation, configure management and service switches first (service switches are not required in the DPC scenario). Then configure or install other software:

- In LLD-based configuration mode, you need to prepare an LLD configuration file, import the LLD configuration file to SmartKit to initialize nodes, and import the LLD configuration file to DeviceManager Client to complete one-click installation.
- In wizard-based configuration mode, you need to check the OS, firmware, and drivers of each storage node, configure networks for each node, use the DeviceManager Client tool to install all management nodes, and then use the management nodes to install storage nodes.

  NOTE

  The OS and related firmware and drivers have been installed before the delivery of OceanStor Pacific series. If the versions of the OS and related firmware and drivers are the same as those in the version mapping, you do not need to install them separately and you can use the DeviceManager Client tool to install OceanStor Pacific series software. If the versions of the OS and related firmware and drivers are different from those in the version mapping, reinstall the OS and related firmware and drivers on each node.

6.3 Installation PC Requirements

OceanStor-Pacific_8.2.1RC1_DeviceManagerClient.zip is run on the installation PC and used to install and deploy OceanStor Pacific series software. **Table 6-1** lists the requirements.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-1 Installation PC requirements

Item	Requirements
OS	For details about DeviceManager Client's requirements for the OS and browser, visit **Huawei Storage Interoperability Navigator**.
Browser	
Available capacity of the disk where DeviceManager Client is installed	8 GB or more
Memory	1 GB or more
OS time	Set the value to the current time zone and time.
PuTTY	Indicates a cross-platform remote access tool, used to access each node in the Windows OS during software installation.
FileZilla	Indicates a cross-platform file transfer tool, used to transfer files between Windows and Linux OSs.

6.4 Configuring Basic Services

6.4.1 Configuring Basic File Services (Standard Protocol Scenario)

6.4.1.1 Configuring Basic Services (Standard Protocol Scenario-NFS Share)

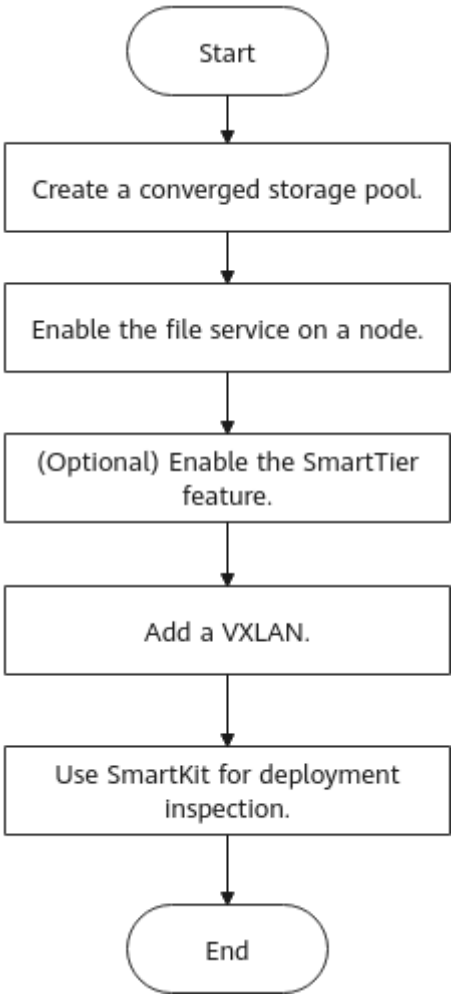
6.4.1.1.1 Configuration Process

By configuring the basic storage services, you can divide the storage space provided by the storage system into namespaces and configure shares. The storage space can be used by accessing shares.

Figure 6-1 shows the process for configuring the file service.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-1 Configuring an NFS share



6.4.1.1.2 Creating a Converged Storage Pool

This section describes how to create a storage pool from which application servers can use storage space.

Context

- You have installed storage nodes.
- You are advised to configure no more than 32 nodes for each disk pool. If the number of nodes exceeds 32, divide them into multiple disk pools. In this case, it is recommended that the number of nodes in each disk pool be the same. For example, if there are 90 nodes, you are advised to divide them into three disk pools. Each disk pool contains 30 nodes.
- HDD 4KN disks cannot be added to the same disk pool as other types of disks.
- The total capacity of cache disks on a single storage node to be added to a storage pool must be greater than **Max. Main Storage Media per Node** x 40 GB.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

Currently, only one converged storage pool can be created. Skip this operation if a converged storage pool has been created using the LLD during initialization.

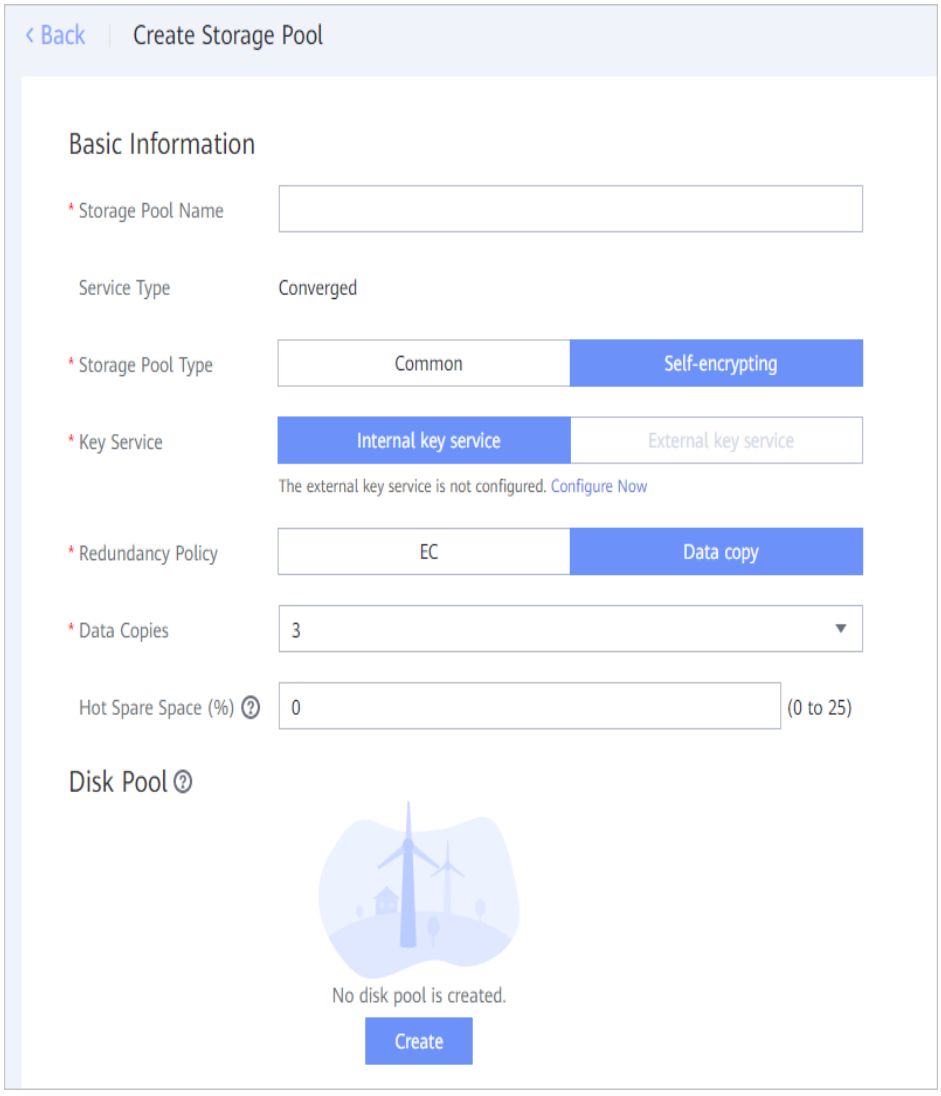
Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Resources** > **Storage Pool**.

Step 3 Click **Create**.

The **Create Storage Pool** page is displayed.



Step 4 Configure basic information for the storage pool.

Table 6-2 describes related parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-2 Storage pool parameters

Parameter	Description
Storage Pool Name	Name of the storage pool. **NOTE** • The name must be unique. • The name can contain only letters, digits, underscores (_), and hyphens (-). • The name contains 1 to 64 characters.
Service Type	Service type of the storage pool. In this example, the value is **Converged**.
Storage Pool Type	Type of the storage pool. Possible options are **Common** and **Self-encrypting**. You are advised to select **Common**. If you have high requirements on data security, select **Self-encrypting**. • **Common**: This type of storage pools does not support data encryption. • **Self-encrypting**: This type of storage pools supports data encryption. **NOTE** • Currently, converged storage pools do not support self-encrypting SATA disks. • A self-encrypting storage pool can be created only when all the following conditions are met: 1. OceanStor Pacific series 8.1.2 or a later version is deployed, and self-encrypting disks have been configured. 2. An advanced license has been imported. 3. Self-encrypting 4K SAS disks are used if **Main Storage** is set to **Self-encrypting SAS**.
Key Service	When creating a self-encrypting storage pool, you need to select a key management service. • **Internal key service**: The built-in key management function of the system is used. • **External key service**: An external key management server is used. If you select this option, you need to configure the external key service first. For details, see **6.5.6 Managing the External Key Service**.
Redundancy Policy	Redundancy policy of the storage pool. Possible options are **EC** and **Data copy**. Considering performance and reliability, **EC** is recommended. • **EC**: Data redundancy protection is implemented by calculating parity fragments. • **Data copy**: Multiple copies of the same data are stored on different nodes for data protection.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Data Copies	Number of redundant data copies allowed by the storage pool. When **Data Copies** is set to **3**, if the number of storage nodes is greater than 3, a maximum of two faulty nodes are allowed; if the number of storage nodes is 3, only one faulty node is allowed. **NOTE** • This parameter is available only when **Redundancy Policy** is set to **Data copy**. • If **Service Type** is set to **Intelligent video and image**, three-copy storage pools cannot be created.
Hot Spare Space (%)	Hot spare space is the space reserved in the system to take over data from faulty disks. This improves reliability and avoids system redundancy reduction. To support data rebuilding after single-disk failure at high capacity usage, the recommended value is (1/Number of disks on a single node) x 100%. **NOTE** Reserving too much hot spare space will occupy excessive available system capacity, causing the available capacity obtained by users to decrease. Configure the hot spare space properly. [Value range] 0 to 25 [Default value] **0**
Storage Pool Mode	If EC redundancy level of the storage pool is +3:1 or higher, you need to set the storage pool mode. If the reliability mode is selected, write cache acceleration cannot be enabled.

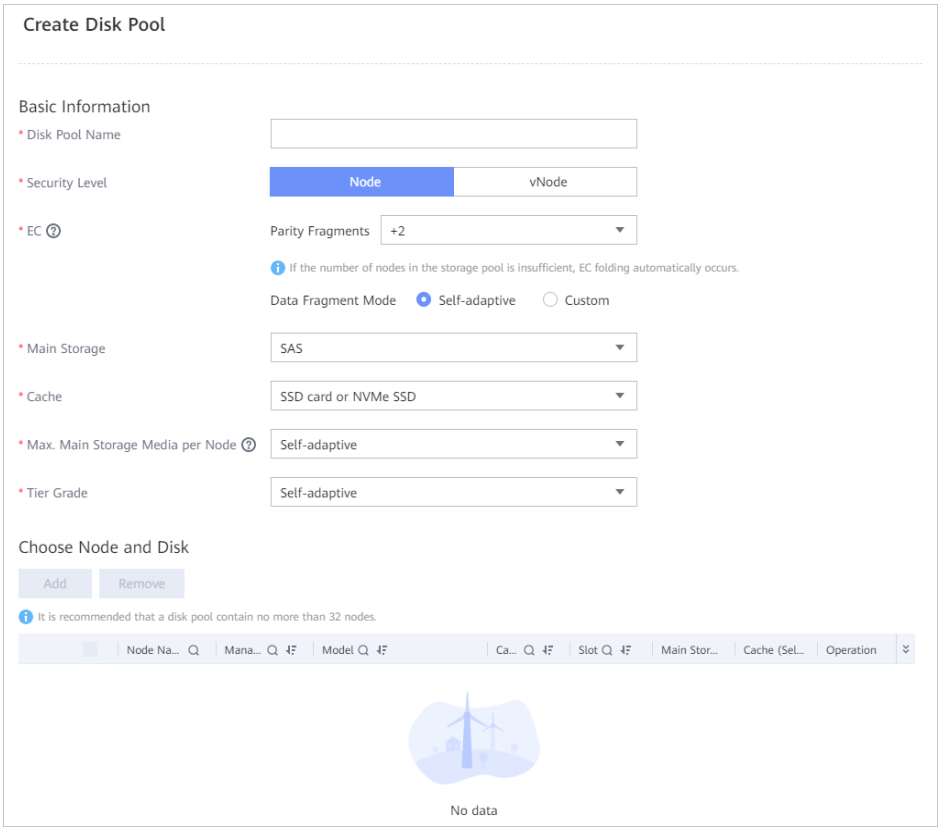
Step 5 Create a disk pool.

NOTE

For details about how to configure disk pools, see the plan in the BOQ.

1. In the **Disk Pool** area, click **Create**.
   The **Create Disk Pool** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



2. Set basic parameters for the disk pool.
   Table 6-3 describes related parameters.

Table 6-3 Disk pool parameters

Parameter	Description
Disk Pool Name	Name of the disk pool. **NOTE** – The name must be unique. – The name can contain only letters, digits, underscores (_), and hyphens (-). – The name contains 1 to 64 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Security Level	Security level of the disk pool. – **Node**: ▪ *N*+*M*: *N* data fragments and *M* parity fragments are randomly stored on different nodes. (The number of storage nodes is greater than *N* + *M*. To ensure reliability, data fragments are stored on different nodes.) In this case, the disk pool can tolerate simultaneous failures of *M* disks or *M* nodes. ▪ *N*+*M*:1 (folded): *N* data fragments and *M* parity fragments are randomly distributed on all nodes. Any node may store *M* fragments. In this case, the disk pool can tolerate simultaneous failures of *M* disks or one node. – **vNode**: A vNode is a logical area consisting of multiple disks on a node. In OceanStor Pacific 9546, a node contains two vNodes. In OceanStor Pacific 9550, a node contains four vNodes. *N* data fragments and *M* parity fragments are stored on different vNodes, and EC redundancy calculation is performed by vNode. A larger EC ratio indicates higher storage utilization. If a node is faulty, its disks can be taken over by the other node in the same chassis and main storage disks will not be degraded or rebuilt by virtue of the dedicated hardware design of OceanStor Pacific 9546 and OceanStor Pacific 9550. **NOTE** **vNode** is supported only when **Redundancy Policy** is set to **EC**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
EC	EC redundancy policy of the disk pool. Select the EC redundancy ratio planned in the Bill of Quotation (BOQ). **NOTE** – This parameter is available only when **Redundancy Policy** is set to **EC**. – When creating multiple disk pools, ensure that the settings of **Parity Fragments** for the disk pools are the same. – The data fragment mode can be **Self-adaptive** or **Custom**. ■ When you select **Self-adaptive**, the system automatically sets the number of data fragments based on the EC redundancy ratio tables and the selected nodes or cabinets and parity fragments. For details about the EC redundancy ratio tables, see **Functions and Features** > **Key Features** > **File/Object/HDFS Service** > **Elastic EC** in the *OceanStor Pacific Series 8.2.1 Product Description*. ■ When you select **Custom**, the number of data fragments is an even number ranging from 4 to 22. The number of nodes that can be contained in a disk pool and the disk pool utilization vary depending on the number of data fragments selected. For details, refer to the actual page.
Main Storage	Main storage type of the disk pool. – When **Storage Pool Type** is set to **Common**, the value of this parameter can be **SAS**, **Self-encrypting SAS**, **SATA**, **Self-encrypting SATA**, **SSD**, and **SSD card or NVMe SSD**. In this case, self-encrypting drives function as common disks and do not use the encryption function. – When **Storage Pool Type** is set to **Self-encrypting**, the value of this parameter can be **Self-encrypting SAS**, **Self-encrypting SATA**, **Self-encrypting SSD card or NVMe SSD (with Chinese cryptographic algorithms)**, or **Self-encrypting SSD card or NVMe SSD (with international cryptographic algorithms)**. – Each node must be configured with at least four disks of the same type. **NOTE** Meanings of the values are: – **SAS**: SAS HDDs – **SATA**: SATA HDDs – **SSD card or NVMe SSD**: NVMe SSDs – **SSD**: SAS SSDs

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Cache	Cache type of the disk pool. **NOTE** – This parameter is not required when **Main Storage** is set to **SSD** or **SSD card or NVMe SSD**. – Meanings of the values are: ■ **SSD card or NVMe SSD**: NVMe SSDs ■ **SSD**: SAS SSDs
Max. Main Storage Media per Node	Maximum number of main storage disks that can be used on a single storage node to store user data. The value of this parameter determines the allocation of cache and compute resources on the node. Set this parameter based on site requirements. To ensure that cache resources can be allocated to newly added main storage disks in the case of capacity expansion, you are advised to set this parameter based on the total number of main storage disks after capacity expansion. – If the value is too small, newly added main storage disks cannot be allocated with cache resources. Cache resources can be allocated to newly-added main storage disks only after both main storage disks and cache disks are added. – If the value is too large, extra cache resources are reserved. As a result, cache resources cannot be fully utilized to improve read/write performance. If you select **Self-adaptive**, the system automatically determines the value based on the number of selected main storage disks. Assume that the number of selected main storage disks is N: – If $4 \leq N \leq 12$, a single node supports a maximum of 12 main storage disks. – If $12 < N \leq 36$, a single node supports a maximum of 36 main storage disks. – If the type of nodes in the disk pool is OceanStor Pacific 9550, a single node supports a maximum of 60 main storage disks. Ensure that the total capacity of the cache disks on selected storage nodes is greater than the maximum number of main storage disks on a single node multiplied by 40 GB. If you select **Custom**, set the value based on site requirements. The value ranges from 4 to 60.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Tier Grade	Tier grade of the disk pool, which is defined based on the type of main storage disks in the disk pool. Possible values are **Hot**, **Warm**, **Cold**, and **Self-adaptive**. You can choose **Resources** > **Tuning** > **SmartTier** and set tiering policies to store different files to disk pools of different tier grades. **NOTE** – If you select **Self-adaptive**: When **Main Storage** is set to **SSD** or **SSD card or NVMe SSD**, **Self-adaptive** equals to tier grade **Hot**. When **Main Storage** is set to **SAS**, **Self-adaptive** equals to tier grade **Warm**. When **Main Storage** is set to **SATA**, **Self-adaptive** equals to tier grade **Cold**. – If you select a tier grade, you are advised to configure the storage tiers based on the self-adaptive rules.

3. In the **Choose Node and Disk** area, select the nodes and disks that are used to create the disk pool.

   NOTE

   – You can click **Add** and add nodes and disks in the cluster to the disk pool on the **Choose Node and Disk** page that is displayed.
   – You can select one or more added nodes or disks and click **Remove** to remove them.

4. Click **OK** and confirm your operation as prompted.

Step 6 Click **Create**.

Step 7 Confirm your operation as prompted.

----End

6.4.1.1.3 Enabling the File Service on a Node

This section describes how to enable the file service for nodes in a storage pool.

Prerequisites

- A storage pool has been created.
- This operation can be performed only when no node with the file service enabled exists in the storage pool. Otherwise, add nodes for the file service by referring to **6.5.8 Adding a Node for an Enabled Service**.

Procedure

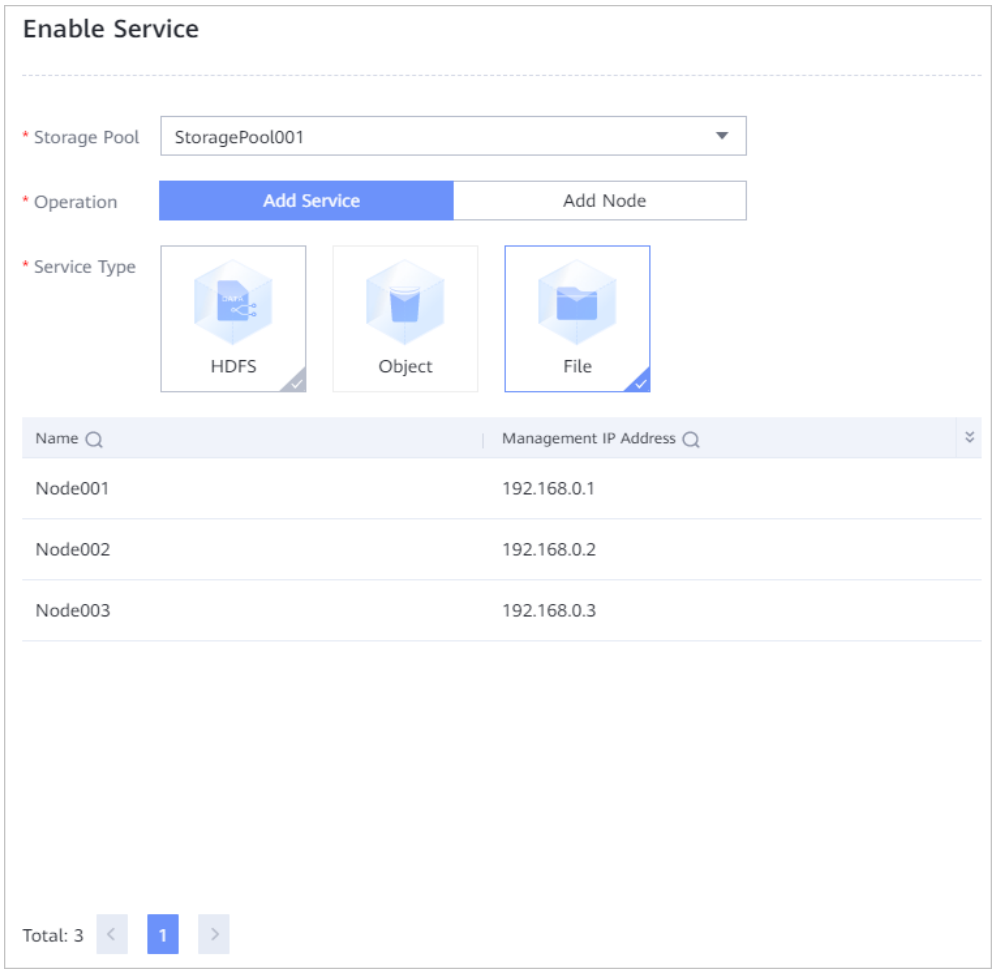
Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Resources** > **Services** > **Basic Service**.

Step 3 Click **Enable Service**.

The **Enable Service** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



Step 4 Select the storage pool for which you want to enable the file service.

Step 5 Select **Add Service** in **Operation**.

NOTE

This parameter is displayed only when at least one service is enabled on the nodes in the storage pool.

Step 6 Select **File** in **Service Type**.

Step 7 Based on service requirements, select at least three nodes in the **Available Nodes** area on the left. They will be automatically added to the **Selected Nodes** area on the right.

NOTE

You need to select nodes only when all services (file, object, and HDFS services) of the storage pool are disabled. Otherwise, the system enables the file service for all nodes where other services have been enabled by default.

Step 8 Click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

6.4.1.1.4 (Optional) Enabling the SmartTier Feature

If a cluster contains two or more types of media, you can perform this operation to enable the SmartTier feature and write files based on the default placement policy.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Tuning** > **SmartTier**.

Step 3 By default, the SmartTier feature is disabled by the storage system. When you go to the **SmartTier** page for the first time, you need to click **Enable** to enable the SmartTier feature.

----End

6.4.1.1.5 Adding a VXLAN

When the storage system needs to connect to the VPC network, you need to configure a VXLAN.

You do not need to configure a VXLAN for OceanStor Pacific 9950.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Access** > **VXLAN**.

Step 3 Click **Add**.

The **Add VXLAN** page is displayed.

Step 4 Click **Batch Import** or **Manually Add** to add nodes to which VXLANs can be added.

NOTE

Add VXLANs for each storage node separately.

- Batch import nodes.
  a. Click **Batch Import**.
  b. Click **Download the template** to download the template locally. Fill the information in the template, click ··· and select the template, and then click **Upload**. The nodes are imported to the system in a batch.
- Manually add nodes.
  a. Set VXLAN parameters. **Table 6-4** describes related parameters.

Table 6-4 VXLAN parameters

Parameter	Description
Management IP Address	Management IP address of a storage node.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Health Check IP Address/ Mask	IP address and mask configured on a storage node for checking the health status of the node. The IP address and mask are used for VPC EP2.0 load balancing.
Health Check Gateway	Gateway of the health check IP address.
VXLAN Tunnel IP Address/ Mask	VTEP IP address used to establish a VXLAN tunnel between nodes. The VTEP IP addresses of the nodes can communicate with each other.
VXLAN Tunnel Gateway	Gateway corresponding to the VXLAN tunnel IP address.
VXLAN Tunnel VLAN ID	VLAN ID of the service plane.
Destack Networking	Select this option when switches are not stacked. Do not select this option when switches are stacked.

b. Click **OK** to add the VXLAN to the list.

NOTE

You can click **More** on the right of a VXLAN and select **Modify** or **Delete** to manage it.

Step 5 Click **OK**.

----End

6.4.1.1.6 Using SmartKit to Perform Deployment Inspection

After hardware installation, software installation, and subsequent service configuration are complete, use SmartKit on the maintenance terminal to check the status of the storage cluster and the version mapping of storage nodes.

Prerequisites

The management IP address, user name, and password for logging in to the storage device have been obtained.

Context

The GUI may vary with the version.

Procedure

Step 1 Prepare SmartKit. If it has been installed, skip this step.

1. Download and install SmartKit.
   - For enterprise users: Log in to **https://support.huawei.com/enterprise**, enter **SmartKit** in the search box, and select **Distributed Storage > Tools**

 Copyright © Huawei Technologies Co., Ltd.

and Platform > SmartKit from the suggested paths. The SmartKit page is displayed.

i. On the SmartKit page, click **Software Download**, and select and download SmartKit of the latest version according to the publication date.

ii. On the SmartKit page, click **Documentation**, find the user guide of the corresponding version, and install and run SmartKit respectively by following the instructions provided in sections "Installing SmartKit" and "Running SmartKit".

– For carrier users: Log in to **https://support.huawei.com**, enter **SmartKit** in the search box, and select **Carrier IT > Data Storage > Storage Common > SmartKit** from the suggested paths. The SmartKit page is displayed.

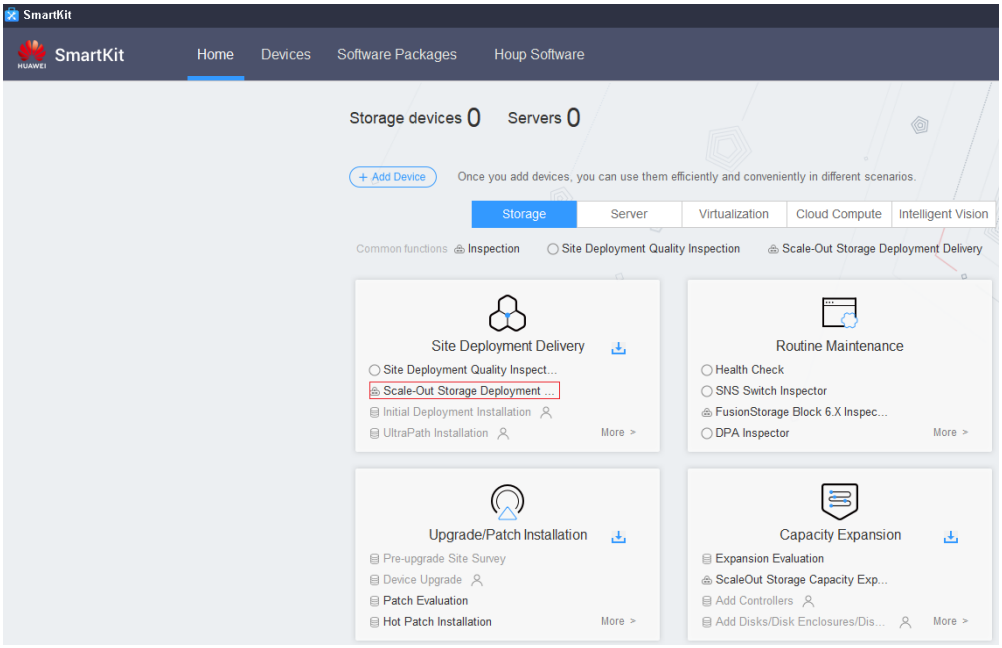
i. On the SmartKit page, click **Software**, and select and download SmartKit of the latest version according to the publication date.

ii. On the SmartKit page, click **Product Documentation**, find the user guide of the corresponding version, and install and run SmartKit respectively by following the instructions provided in sections "Installing SmartKit" and "Running SmartKit".

2. Install the Scale-Out Storage Deployment Delivery tool by referring to section "Installing Functions" in the SmartKit user guide.

Step 2 Go to the **Site Deployment Delivery** page.

1. On the home page of SmartKit, choose **Site Deployment Delivery** > **Scale-Out Storage Deployment Delivery**. The **Scale-Out Storage Deployment Delivery** page is displayed.

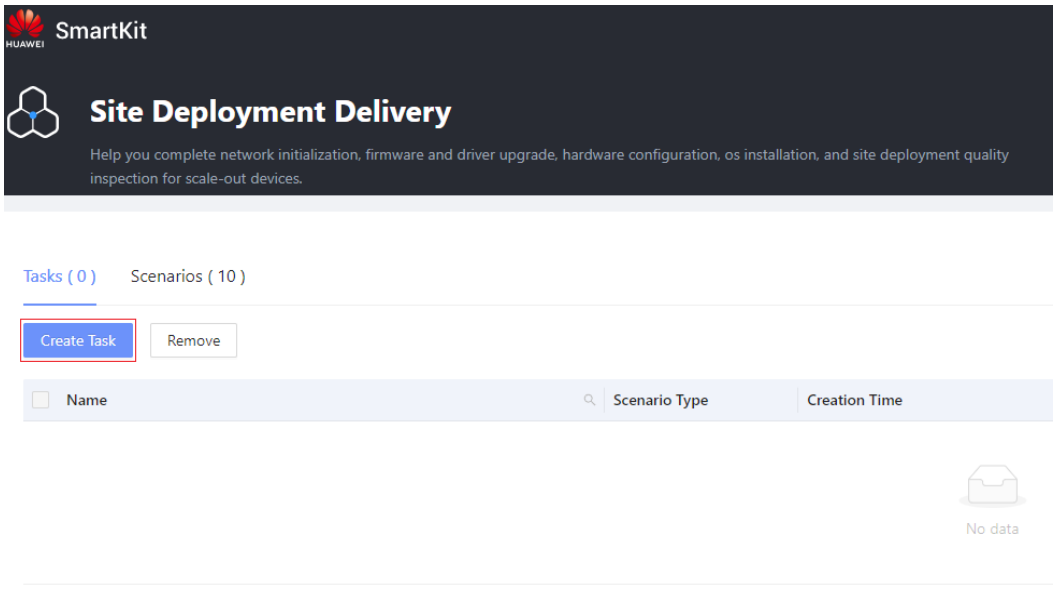


2. On the **Scale-Out Storage Deployment Delivery** page, click **Scale-Out Storage Deployment Delivery**. The **Site Deployment Delivery** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Click **New**. The **Select Scenario** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

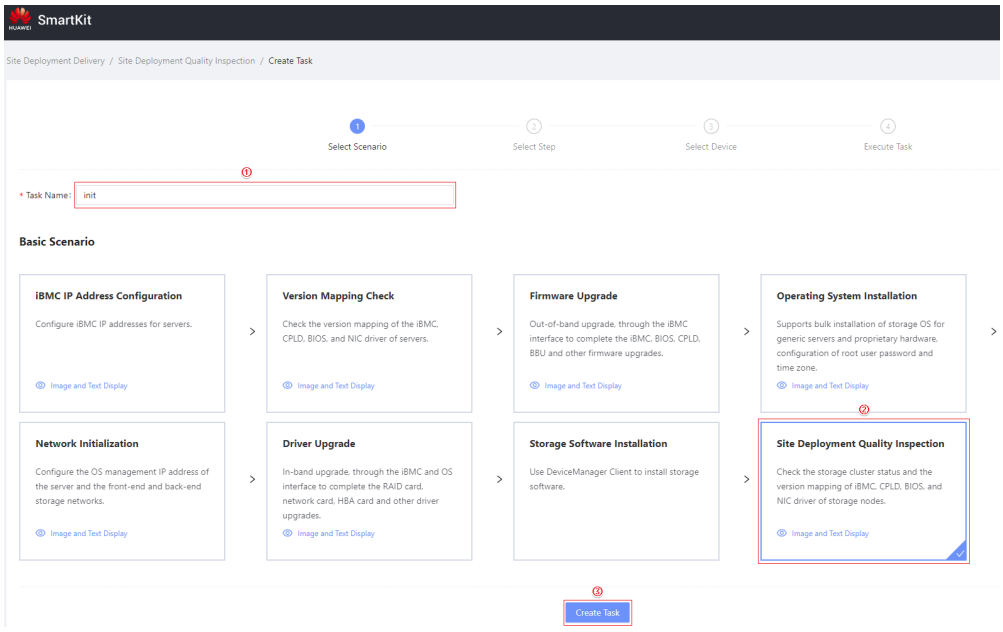


Step 4 Select a scenario.

1. Set **Task Name**, select **Site Deployment Quality Inspection**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).



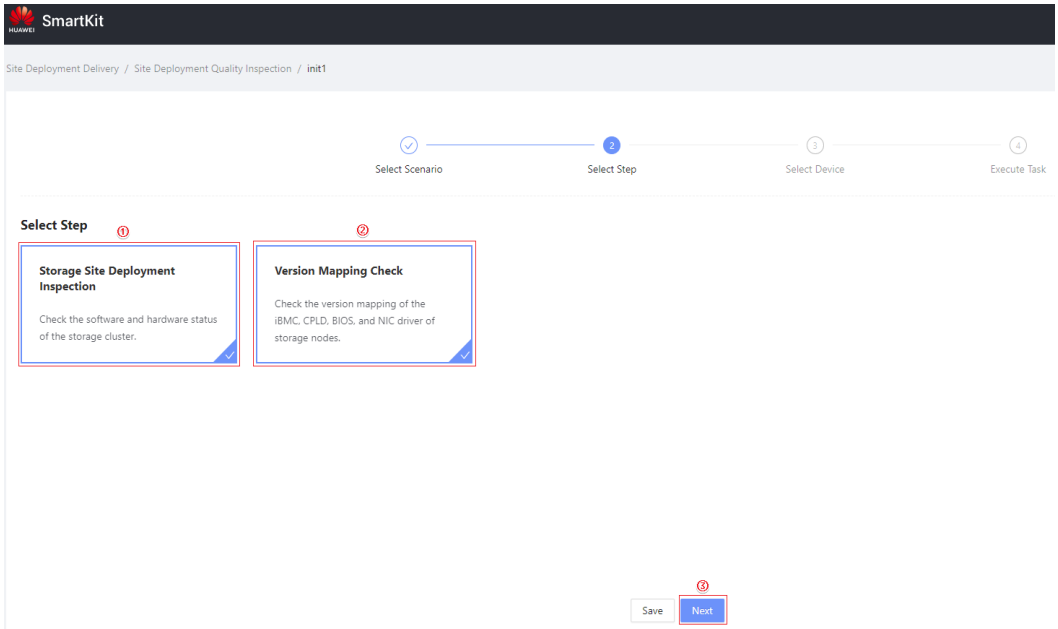
2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

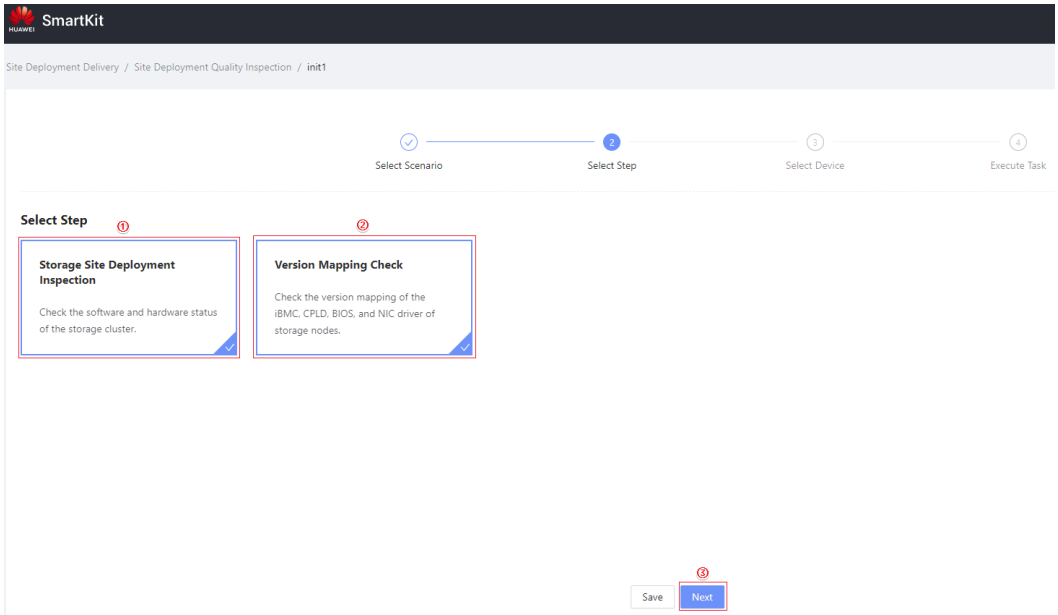
   NOTE

   If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Select **Storage Site Deployment Inspection** and **Version Mapping Check**, and click **Next**.

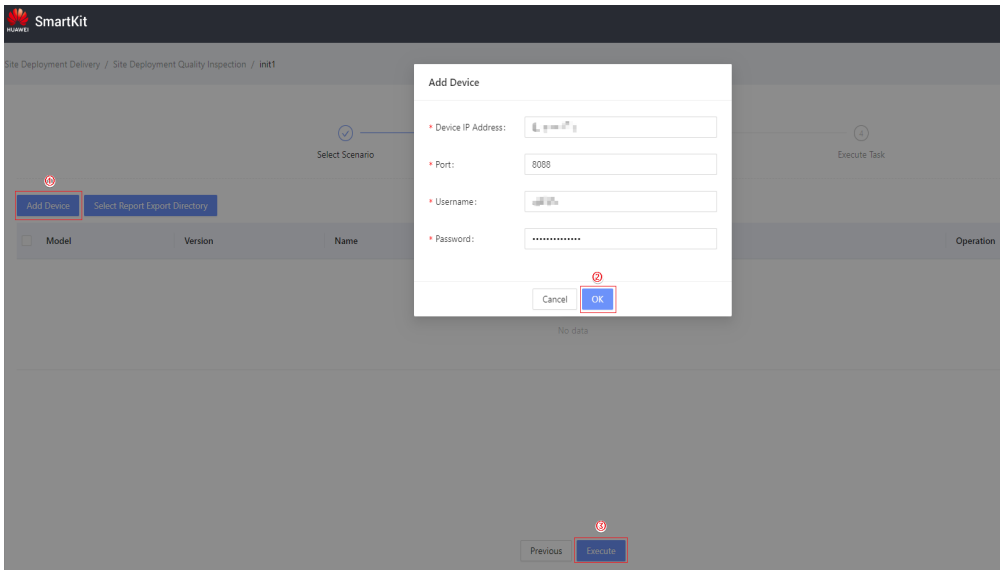




Step 6 Select a device.

1. Add a device.

 Copyright © Huawei Technologies Co., Ltd.



a. Click **Add Device**. The **Add Device** dialog box is displayed.

b. Enter device information as prompted and click **OK**.

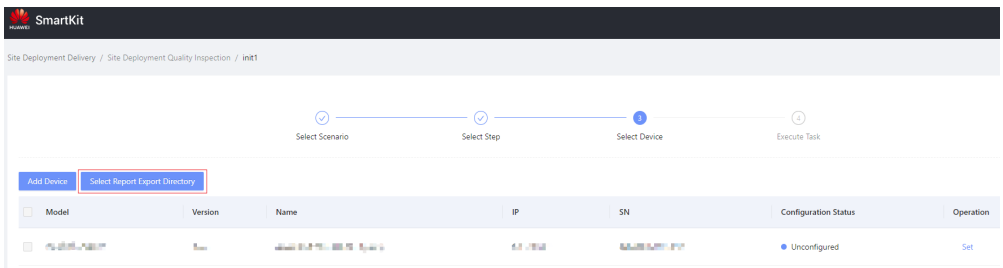
Table 6-5 Device information

Name	Description
Device IP Address	DeviceManager management IP address
Port	Port of DeviceManager. Use default port **8088**.
Username	DeviceManager login account
Password	Password for logging in to DeviceManager

NOTE

If the device has been added, it is displayed in the list by default. You do not need to add it again.

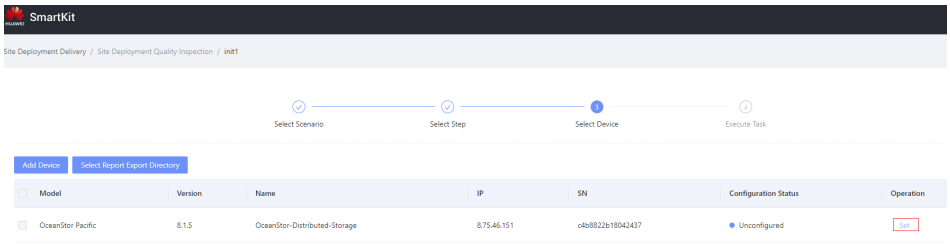
2. Click **Select Report Export Directory** and specify a save path for the report.



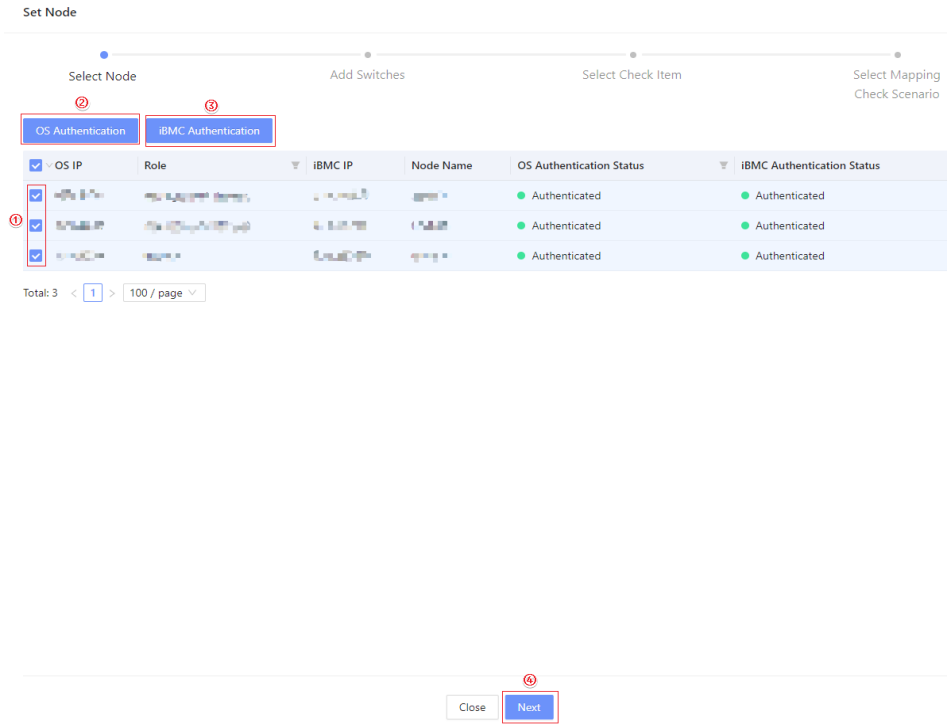
3. Set a check policy.

a. Click **Set** in the **Operation** column of a device. The **Set Node** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



b. Select a node and authenticate it.



i. Select the nodes to be checked.

ii. Click **OS Authentication** and enter related information as prompted to complete the authentication.

iii. Click **iBMC Authentication** and enter related information as prompted to complete the authentication.

iv. Click **Next**. The **Add Switches** page is displayed.

c. (Optional) Add switches.

NOTE

This step applies only to access switches whose storage network uses RoCE networking. In other scenarios, click **Skipped** to skip this step.

i. Click **Add Switch** and enter information about all storage switches.

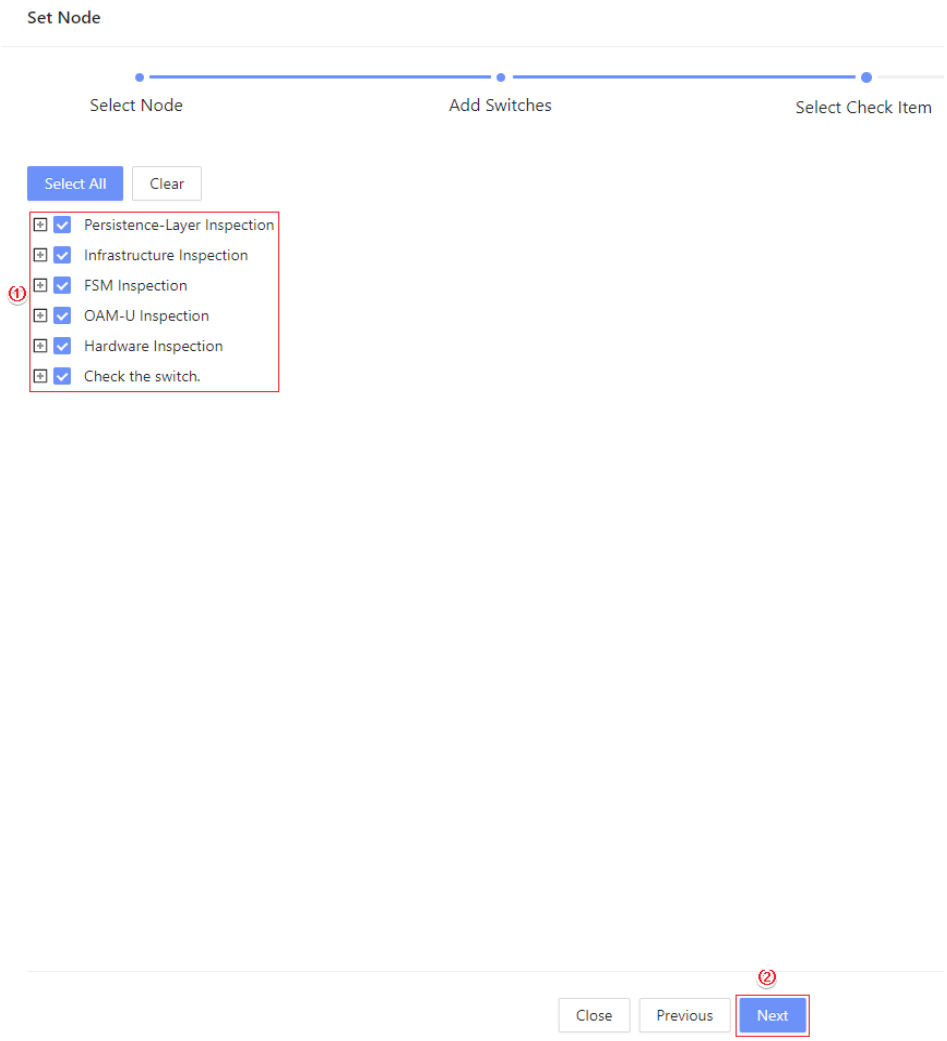
NOTE

You can also click **Download Template** to download the switch information template, enter login information, and click **Batch Import**.

ii. Click **Next**. The **Select Check Item** page is displayed.

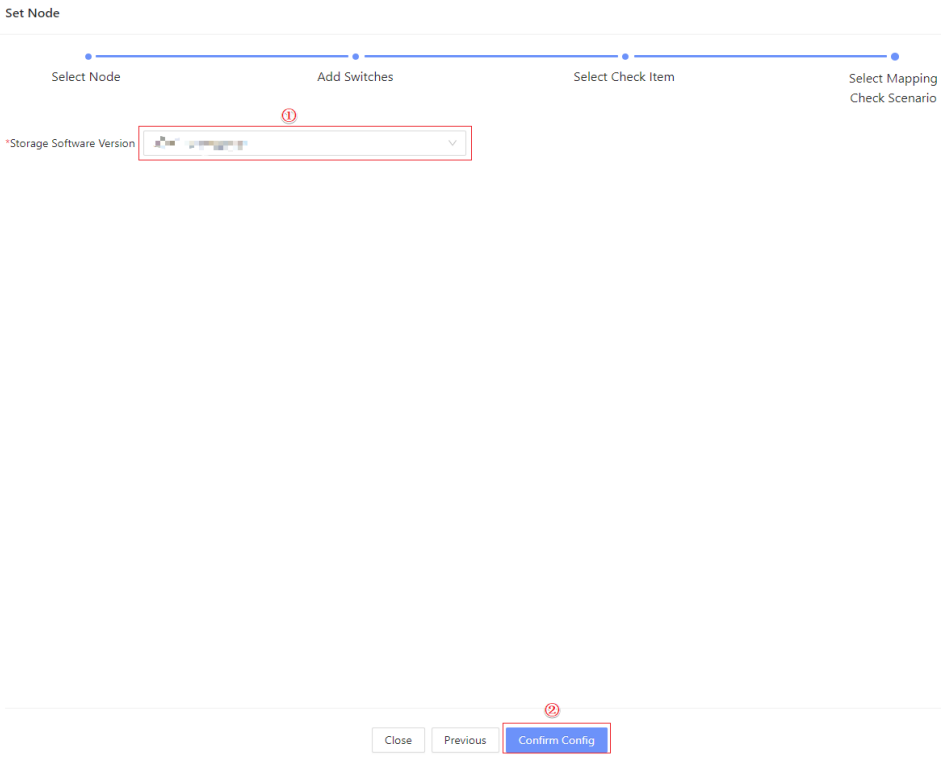
d. Select the items to be checked and click **Next**. The **Select Mapping Check Scenario** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



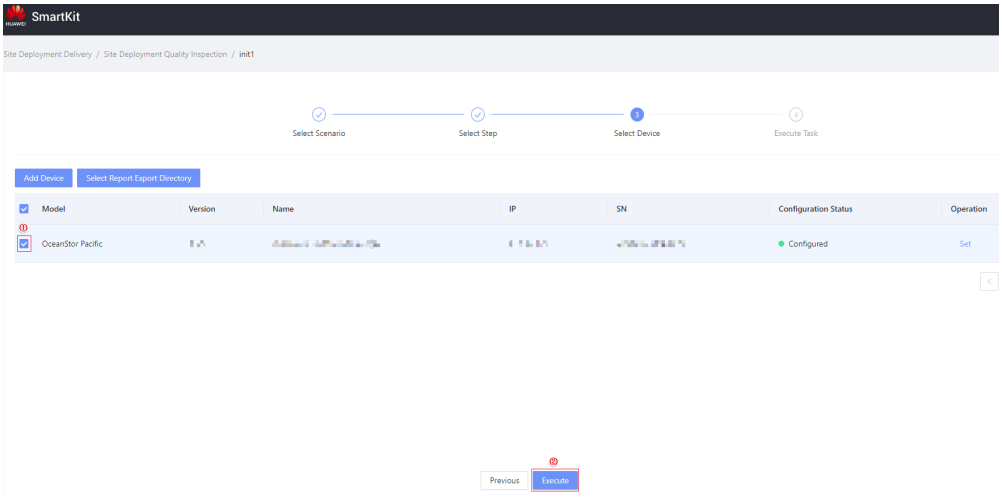
e. Select a storage software version and click **Confirm Config**.

 Copyright © Huawei Technologies Co., Ltd.



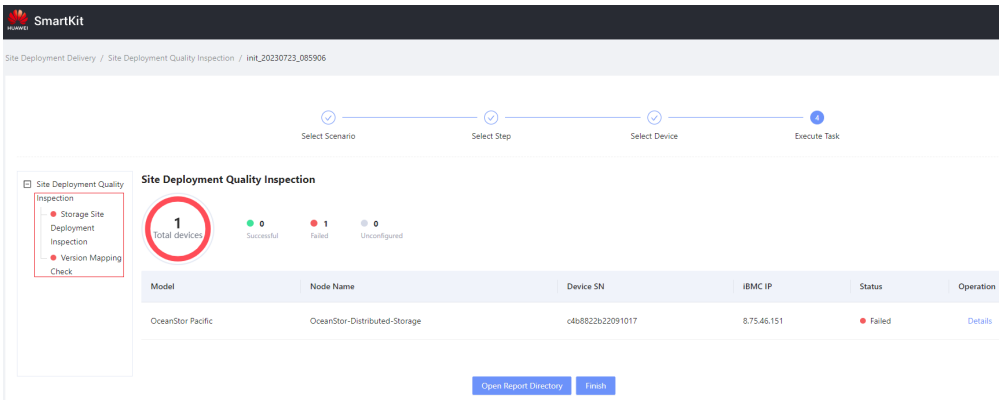
Step 7 Execute the task.

1. Select a device, click **Execute**, and enter the information about the inspection report personnel as prompted.



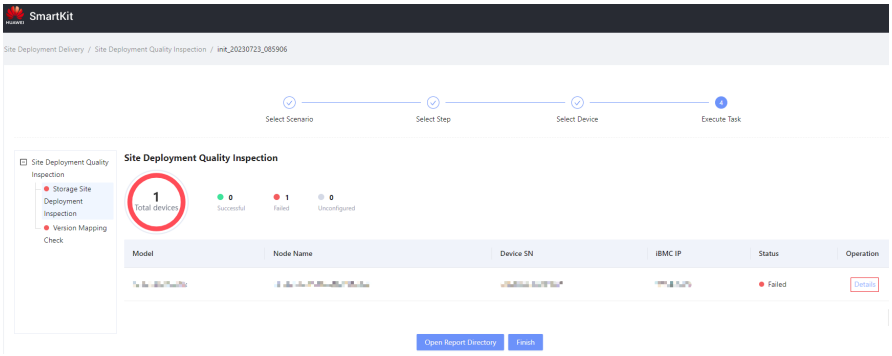
2. After the task is complete, check whether the **Storage Site Deployment Inspection** and **Version Mapping Check** items pass the check (marked in green).

 Copyright © Huawei Technologies Co., Ltd.



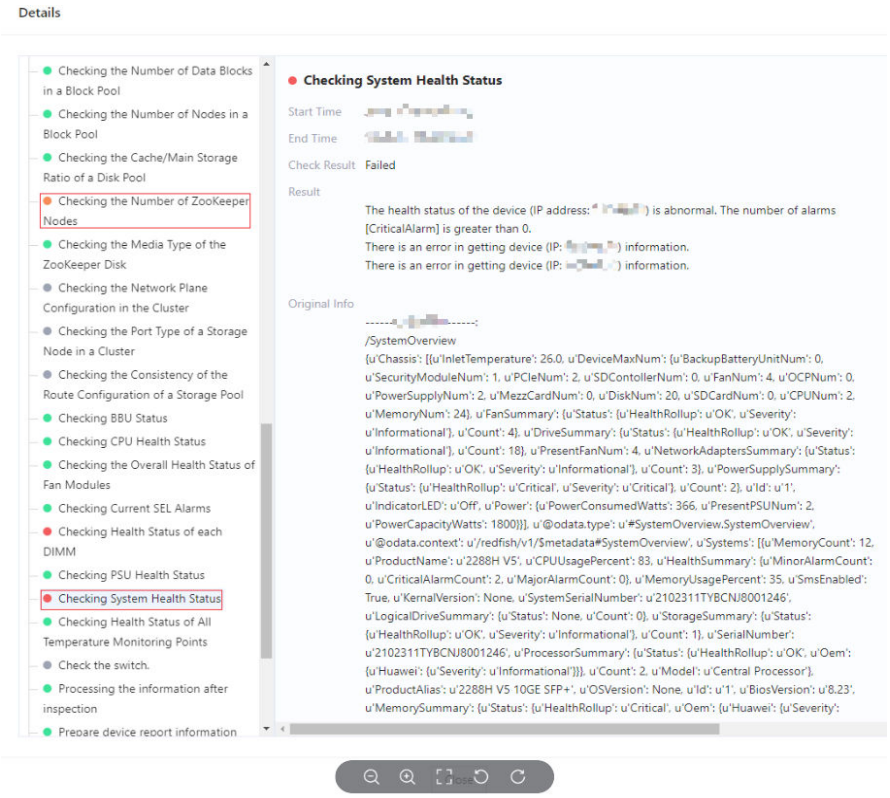
- If yes, click **Finish**.
- If no, perform the following steps for the two check items (after the troubleshooting is complete, click **Finish**):

  i. Click **Details** in the **Operation** column of the corresponding device.



  ii. Click the check items that fail to pass the check (marked in red) and the check items that need to be optimized (marked in orange) in sequence, and handle the problems according to the description in **Result**. The following uses **Storage Site Deployment Inspection** as an example:

 Copyright © Huawei Technologies Co., Ltd.



----End

6.4.1.2 Configuring Basic Services (Standard Protocol Scenario-CIFS Share)

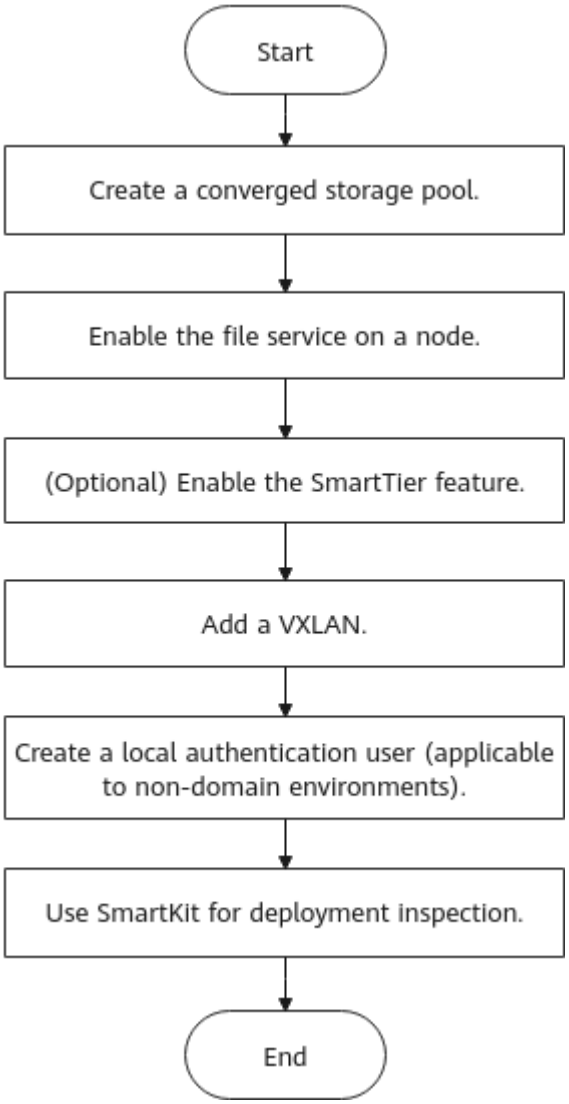
6.4.1.2.1 Configuration Process

By configuring the basic storage services, you can divide the storage space provided by the storage system into namespaces and configure shares. The storage space can be used by accessing shares.

Figure 6-2 shows the process for configuring the file service.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-2 Configuring a CIFS share



6.4.1.2.2 Creating a Converged Storage Pool

This section describes how to create a storage pool from which application servers can use storage space.

Context

- You have installed storage nodes.
- You are advised to configure no more than 32 nodes for each disk pool. If the number of nodes exceeds 32, divide them into multiple disk pools. In this case, it is recommended that the number of nodes in each disk pool be the same. For example, if there are 90 nodes, you are advised to divide them into three disk pools. Each disk pool contains 30 nodes.
- HDD 4KN disks cannot be added to the same disk pool as other types of disks.
- The total capacity of cache disks on a single storage node to be added to a storage pool must be greater than **Max. Main Storage Media per Node** x 40 GB.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

Currently, only one converged storage pool can be created. Skip this operation if a converged storage pool has been created using the LLD during initialization.

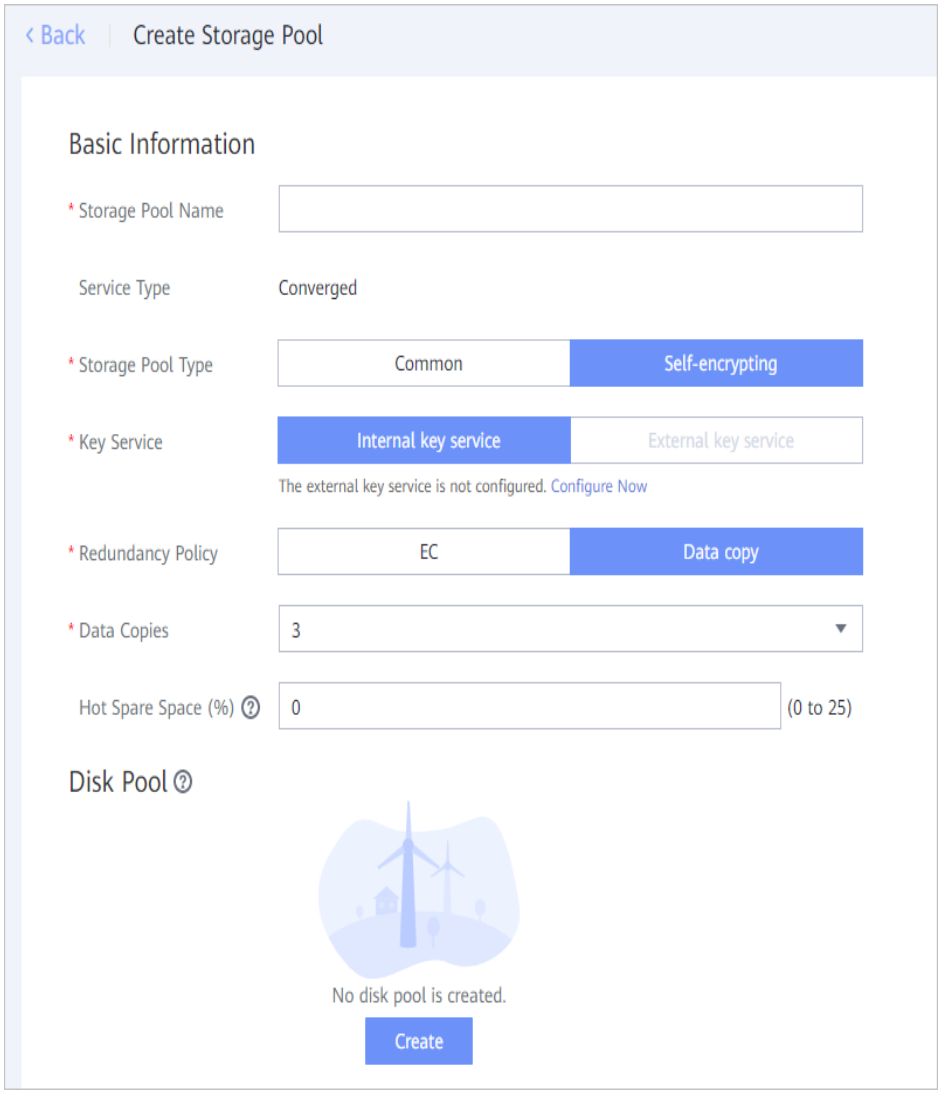
Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Resources** > **Storage Pool**.

Step 3 Click **Create**.

The **Create Storage Pool** page is displayed.



Step 4 Configure basic information for the storage pool.

Table 6-6 describes related parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-6 Storage pool parameters

Parameter	Description
Storage Pool Name	Name of the storage pool. **NOTE** • The name must be unique. • The name can contain only letters, digits, underscores (_), and hyphens (-). • The name contains 1 to 64 characters.
Service Type	Service type of the storage pool. In this example, the value is **Converged**.
Storage Pool Type	Type of the storage pool. Possible options are **Common** and **Self-encrypting**. You are advised to select **Common**. If you have high requirements on data security, select **Self-encrypting**. • **Common**: This type of storage pools does not support data encryption. • **Self-encrypting**: This type of storage pools supports data encryption. **NOTE** • Currently, converged storage pools do not support self-encrypting SATA disks. • A self-encrypting storage pool can be created only when all the following conditions are met: 1. OceanStor Pacific series 8.1.2 or a later version is deployed, and self-encrypting disks have been configured. 2. An advanced license has been imported. 3. Self-encrypting 4K SAS disks are used if **Main Storage** is set to **Self-encrypting SAS**.
Key Service	When creating a self-encrypting storage pool, you need to select a key management service. • **Internal key service**: The built-in key management function of the system is used. • **External key service**: An external key management server is used. If you select this option, you need to configure the external key service first. For details, see **6.5.6 Managing the External Key Service**.
Redundancy Policy	Redundancy policy of the storage pool. Possible options are **EC** and **Data copy**. Considering performance and reliability, **EC** is recommended. • **EC**: Data redundancy protection is implemented by calculating parity fragments. • **Data copy**: Multiple copies of the same data are stored on different nodes for data protection.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Data Copies	Number of redundant data copies allowed by the storage pool. When **Data Copies** is set to **3**, if the number of storage nodes is greater than 3, a maximum of two faulty nodes are allowed; if the number of storage nodes is 3, only one faulty node is allowed. **NOTE** • This parameter is available only when **Redundancy Policy** is set to **Data copy**. • If **Service Type** is set to **Intelligent video and image**, three-copy storage pools cannot be created.
Hot Spare Space (%)	Hot spare space is the space reserved in the system to take over data from faulty disks. This improves reliability and avoids system redundancy reduction. To support data rebuilding after single-disk failure at high capacity usage, the recommended value is (1/Number of disks on a single node) x 100%. **NOTE** Reserving too much hot spare space will occupy excessive available system capacity, causing the available capacity obtained by users to decrease. Configure the hot spare space properly. [Value range] 0 to 25 [Default value] **0**
Storage Pool Mode	If EC redundancy level of the storage pool is +3:1 or higher, you need to set the storage pool mode. If the reliability mode is selected, write cache acceleration cannot be enabled.

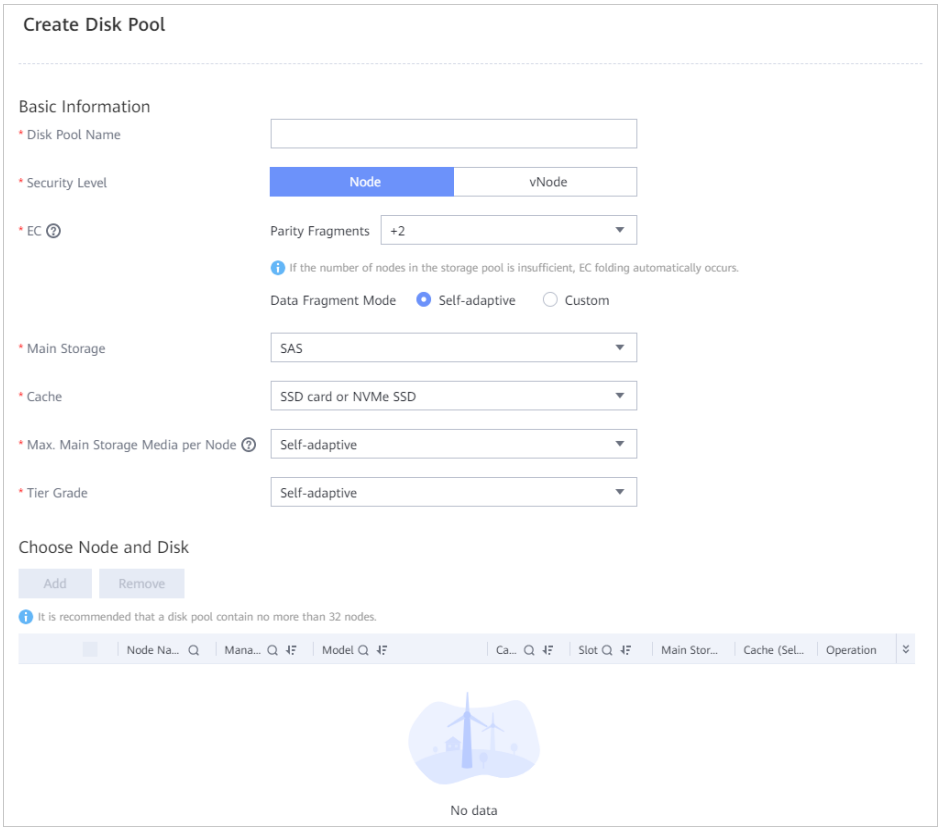
Step 5 Create a disk pool.

NOTE

For details about how to configure disk pools, see the plan in the BOQ.

1. In the **Disk Pool** area, click **Create**.
   The **Create Disk Pool** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



2. Set basic parameters for the disk pool.
   Table 6-7 describes related parameters.

Table 6-7 Disk pool parameters

Parameter	Description
Disk Pool Name	Name of the disk pool. **NOTE** – The name must be unique. – The name can contain only letters, digits, underscores (_), and hyphens (-). – The name contains 1 to 64 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Security Level	Security level of the disk pool. – **Node**: ▪ *N*+*M*: *N* data fragments and *M* parity fragments are randomly stored on different nodes. (The number of storage nodes is greater than *N* + *M*. To ensure reliability, data fragments are stored on different nodes.) In this case, the disk pool can tolerate simultaneous failures of *M* disks or *M* nodes. ▪ *N*+*M*:1 (folded): *N* data fragments and *M* parity fragments are randomly distributed on all nodes. Any node may store *M* fragments. In this case, the disk pool can tolerate simultaneous failures of *M* disks or one node. – **vNode**: A vNode is a logical area consisting of multiple disks on a node. In OceanStor Pacific 9546, a node contains two vNodes. In OceanStor Pacific 9550, a node contains four vNodes. *N* data fragments and *M* parity fragments are stored on different vNodes, and EC redundancy calculation is performed by vNode. A larger EC ratio indicates higher storage utilization. If a node is faulty, its disks can be taken over by the other node in the same chassis and main storage disks will not be degraded or rebuilt by virtue of the dedicated hardware design of OceanStor Pacific 9546 and OceanStor Pacific 9550. **NOTE** **vNode** is supported only when **Redundancy Policy** is set to **EC**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
EC	EC redundancy policy of the disk pool. Select the EC redundancy ratio planned in the Bill of Quotation (BOQ). **NOTE** – This parameter is available only when **Redundancy Policy** is set to **EC**. – When creating multiple disk pools, ensure that the settings of **Parity Fragments** for the disk pools are the same. – The data fragment mode can be **Self-adaptive** or **Custom**. ■ When you select **Self-adaptive**, the system automatically sets the number of data fragments based on the EC redundancy ratio tables and the selected nodes or cabinets and parity fragments. For details about the EC redundancy ratio tables, see **Functions and Features** > **Key Features** > **File/Object/HDFS Service** > **Elastic EC** in the *OceanStor Pacific Series 8.2.1 Product Description*. ■ When you select **Custom**, the number of data fragments is an even number ranging from 4 to 22. The number of nodes that can be contained in a disk pool and the disk pool utilization vary depending on the number of data fragments selected. For details, refer to the actual page.
Main Storage	Main storage type of the disk pool. – When **Storage Pool Type** is set to **Common**, the value of this parameter can be **SAS**, **Self-encrypting SAS**, **SATA**, **Self-encrypting SATA**, **SSD**, and **SSD card or NVMe SSD**. In this case, self-encrypting drives function as common disks and do not use the encryption function. – When **Storage Pool Type** is set to **Self-encrypting**, the value of this parameter can be **Self-encrypting SAS**, **Self-encrypting SATA**, **Self-encrypting SSD card or NVMe SSD (with Chinese cryptographic algorithms)**, or **Self-encrypting SSD card or NVMe SSD (with international cryptographic algorithms)**. – Each node must be configured with at least four disks of the same type. **NOTE** Meanings of the values are: – **SAS**: SAS HDDs – **SATA**: SATA HDDs – **SSD card or NVMe SSD**: NVMe SSDs – **SSD**: SAS SSDs

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Cache	Cache type of the disk pool. **NOTE** – This parameter is not required when **Main Storage** is set to **SSD** or **SSD card or NVMe SSD**. – Meanings of the values are: ▪ **SSD card or NVMe SSD**: NVMe SSDs ▪ **SSD**: SAS SSDs
Max. Main Storage Media per Node	Maximum number of main storage disks that can be used on a single storage node to store user data. The value of this parameter determines the allocation of cache and compute resources on the node. Set this parameter based on site requirements. To ensure that cache resources can be allocated to newly added main storage disks in the case of capacity expansion, you are advised to set this parameter based on the total number of main storage disks after capacity expansion. – If the value is too small, newly added main storage disks cannot be allocated with cache resources. Cache resources can be allocated to newly-added main storage disks only after both main storage disks and cache disks are added. – If the value is too large, extra cache resources are reserved. As a result, cache resources cannot be fully utilized to improve read/write performance. If you select **Self-adaptive**, the system automatically determines the value based on the number of selected main storage disks. Assume that the number of selected main storage disks is *N*: – If $4 \leq N \leq 12$, a single node supports a maximum of 12 main storage disks. – If $12 < N \leq 36$, a single node supports a maximum of 36 main storage disks. – If the type of nodes in the disk pool is OceanStor Pacific 9550, a single node supports a maximum of 60 main storage disks. Ensure that the total capacity of the cache disks on selected storage nodes is greater than the maximum number of main storage disks on a single node multiplied by 40 GB. If you select **Custom**, set the value based on site requirements. The value ranges from 4 to 60.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Tier Grade	Tier grade of the disk pool, which is defined based on the type of main storage disks in the disk pool. Possible values are **Hot**, **Warm**, **Cold**, and **Self-adaptive**. You can choose **Resources** > **Tuning** > **SmartTier** and set tiering policies to store different files to disk pools of different tier grades. **NOTE** – If you select **Self-adaptive**: When **Main Storage** is set to **SSD** or **SSD card or NVMe SSD**, **Self-adaptive** equals to tier grade **Hot**. When **Main Storage** is set to **SAS**, **Self-adaptive** equals to tier grade **Warm**. When **Main Storage** is set to **SATA**, **Self-adaptive** equals to tier grade **Cold**. – If you select a tier grade, you are advised to configure the storage tiers based on the self-adaptive rules.

3. In the **Choose Node and Disk** area, select the nodes and disks that are used to create the disk pool.

   NOTE

   – You can click **Add** and add nodes and disks in the cluster to the disk pool on the **Choose Node and Disk** page that is displayed.
   – You can select one or more added nodes or disks and click **Remove** to remove them.

4. Click **OK** and confirm your operation as prompted.

Step 6 Click **Create**.

Step 7 Confirm your operation as prompted.

----End

6.4.1.2.3 Enabling the File Service on a Node

This section describes how to enable the file service for nodes in a storage pool.

Prerequisites

- A storage pool has been created.
- This operation can be performed only when no node with the file service enabled exists in the storage pool. Otherwise, add nodes for the file service by referring to **6.5.8 Adding a Node for an Enabled Service**.

Procedure

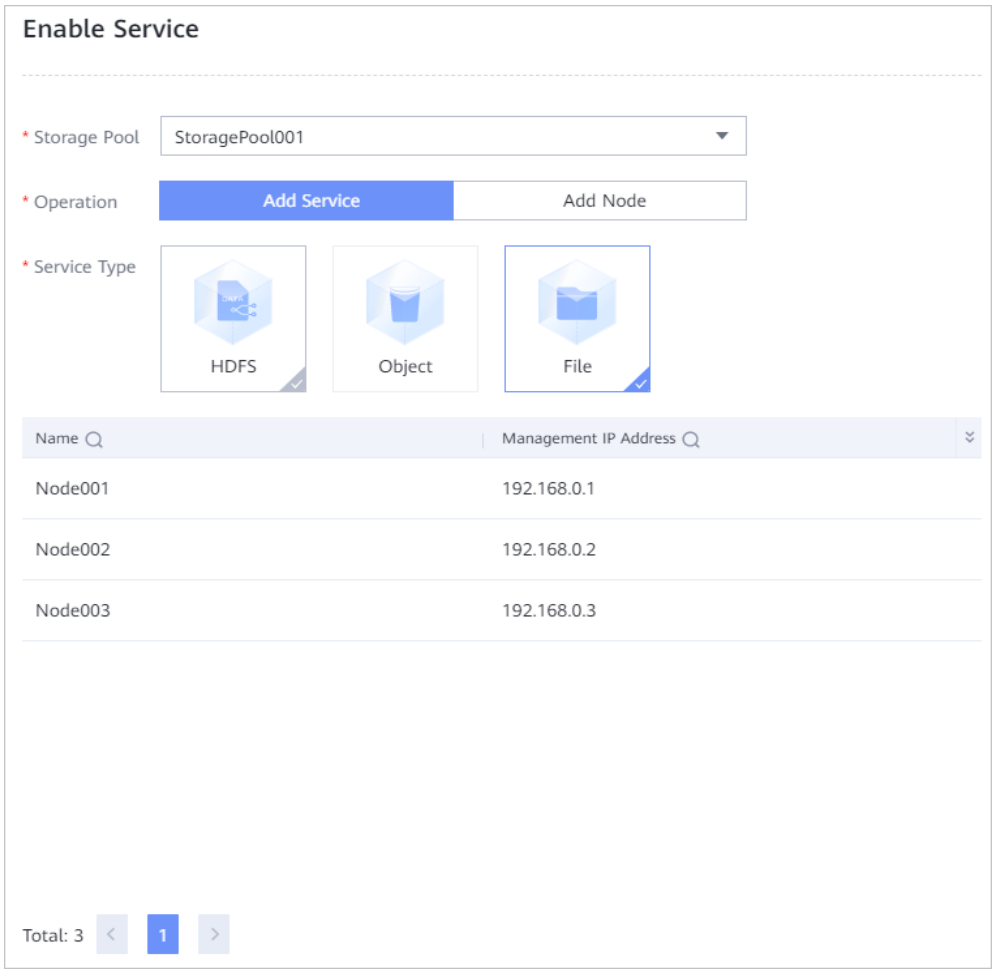
Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Resources** > **Services** > **Basic Service**.

Step 3 Click **Enable Service**.

The **Enable Service** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



Step 4 Select the storage pool for which you want to enable the file service.

Step 5 Select **Add Service** in **Operation**.

NOTE

This parameter is displayed only when at least one service is enabled on the nodes in the storage pool.

Step 6 Select **File** in **Service Type**.

Step 7 Based on service requirements, select at least three nodes in the **Available Nodes** area on the left. They will be automatically added to the **Selected Nodes** area on the right.

NOTE

You need to select nodes only when all services (file, object, and HDFS services) of the storage pool are disabled. Otherwise, the system enables the file service for all nodes where other services have been enabled by default.

Step 8 Click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

6.4.1.2.4 (Optional) Enabling the SmartTier Feature

If a cluster contains two or more types of media, you can perform this operation to enable the SmartTier feature and write files based on the default placement policy.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Tuning** > **SmartTier**.

Step 3 By default, the SmartTier feature is disabled by the storage system. When you go to the **SmartTier** page for the first time, you need to click **Enable** to enable the SmartTier feature.

----End

6.4.1.2.5 Adding a VXLAN

When the storage system needs to connect to the VPC network, you need to configure a VXLAN.

You do not need to configure a VXLAN for OceanStor Pacific 9950.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Access** > **VXLAN**.

Step 3 Click **Add**.

The **Add VXLAN** page is displayed.

Step 4 Click **Batch Import** or **Manually Add** to add nodes to which VXLANs can be added.

NOTE

Add VXLANs for each storage node separately.

- Batch import nodes.
  a. Click **Batch Import**.
  b. Click **Download the template** to download the template locally. Fill the information in the template, click ··· and select the template, and then click **Upload**. The nodes are imported to the system in a batch.
- Manually add nodes.
  a. Set VXLAN parameters. **Table 6-8** describes related parameters.

Table 6-8 VXLAN parameters

Parameter	Description
Management IP Address	Management IP address of a storage node.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Health Check IP Address/ Mask	IP address and mask configured on a storage node for checking the health status of the node. The IP address and mask are used for VPC EP2.0 load balancing.
Health Check Gateway	Gateway of the health check IP address.
VXLAN Tunnel IP Address/ Mask	VTEP IP address used to establish a VXLAN tunnel between nodes. The VTEP IP addresses of the nodes can communicate with each other.
VXLAN Tunnel Gateway	Gateway corresponding to the VXLAN tunnel IP address.
VXLAN Tunnel VLAN ID	VLAN ID of the service plane.
Destack Networking	Select this option when switches are not stacked. Do not select this option when switches are stacked.

b. Click **OK** to add the VXLAN to the list.

NOTE

You can click **More** on the right of a VXLAN and select **Modify** or **Delete** to manage it.

Step 5 Click **OK**.

----End

6.4.1.2.6 Creating a Local Authentication User (Applicable to Non-Domain Environments)

This operation enables you to create a local authentication user. For applications that use local authentication, local users are used to access shares. You can add a local user to a local user group for authentication and access a share as the user group.

Procedure

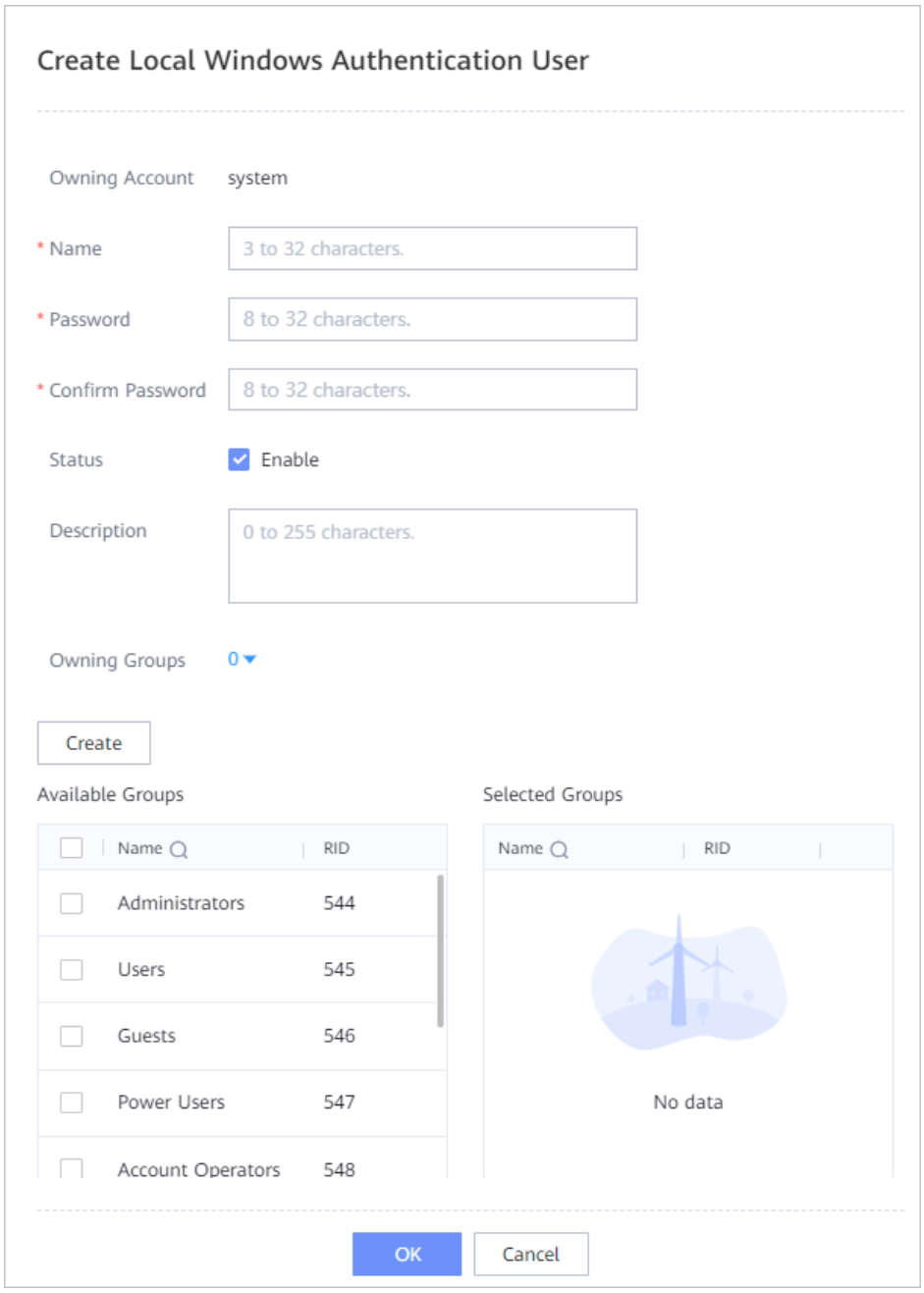
Step 1 Choose **Resources** > **Access** > **Authentication User** > **Windows Users** > **Local Authentication User**.

Step 2 Select a desired account from the **Account** drop-down list in the upper left corner.

Step 3 Click **Create**.

The **Create Local Windows Authentication User** page is displayed on the right.

 Copyright © Huawei Technologies Co., Ltd.



Step 4 Set basic parameters for the local authentication user.

Table 6-9 describes related parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-9 Local authentication user parameters

Parameter	Description
Name	Name of the local authentication user. [Value range] • The name must be unique. • The name cannot contain "/\][:;|=,+*?<>@ or spaces, or end with a period (.). • The name can contain case-insensitive letters. For example, **aaaaaaaa** and **AAAAAAAA** cannot be created at the same time. • The name cannot be the same as the name of a local authentication user group. • The name contains 3 to 32 characters. **NOTE** You can modify the minimum length of the user name on the **Set Security Policy** page.
Password	Password of the local authentication user. [Value range] The default password rules are as follows: • The password contains 8 to 32 characters. • The password must contain at least two of the following types: special characters, uppercase letters, lowercase letters, and digits. Special characters include !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces. • The password cannot contain three consecutive identical characters. • The password cannot be the same as the user name or the user name spelled backward. **NOTE** You can set security policies for the password of a local authentication user on the **Set Security Policy** page. If **Password Validity Period** is **0**, the password will never expire. For the security purpose, you are advised to set a specific password validity period. After the password expires, you cannot access shares, but you can set a password again or modify the password security policy on the **Set Security Policy** page.
Confirm Password	Confirm the password for consistency.
Status	Whether to enable the user.
Description	Description of the local authentication user. [Value range] The description can be left blank or contain up to 255 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Owning Groups	Group to which the local authentication user belongs. Click ▸ on the right of **Owning Groups**. In the **Available Groups** list, select desired groups. They will be automatically added to the **Selected Groups** list. **NOTE** Click **Create** to create a local authentication user group.

Step 5 Click **OK**.

----End

6.4.1.2.7 Using SmartKit to Perform Deployment Inspection

After hardware installation, software installation, and subsequent service configuration are complete, use SmartKit on the maintenance terminal to check the status of the storage cluster and the version mapping of storage nodes.

Prerequisites

The management IP address, user name, and password for logging in to the storage device have been obtained.

Context

The GUI may vary with the version.

Procedure

Step 1 Prepare SmartKit. If it has been installed, skip this step.

1. Download and install SmartKit.
   - For enterprise users: Log in to **https://support.huawei.com/enterprise**, enter **SmartKit** in the search box, and select **Distributed Storage > Tools and Platform > SmartKit** from the suggested paths. The SmartKit page is displayed.
     i. On the SmartKit page, click **Software Download**, and select and download SmartKit of the latest version according to the publication date.
     ii. On the SmartKit page, click **Documentation**, find the user guide of the corresponding version, and install and run SmartKit respectively by following the instructions provided in sections "Installing SmartKit" and "Running SmartKit".
   - For carrier users: Log in to **https://support.huawei.com**, enter **SmartKit** in the search box, and select **Carrier IT > Data Storage > Storage Common > SmartKit** from the suggested paths. The SmartKit page is displayed.
     i. On the SmartKit page, click **Software**, and select and download SmartKit of the latest version according to the publication date.

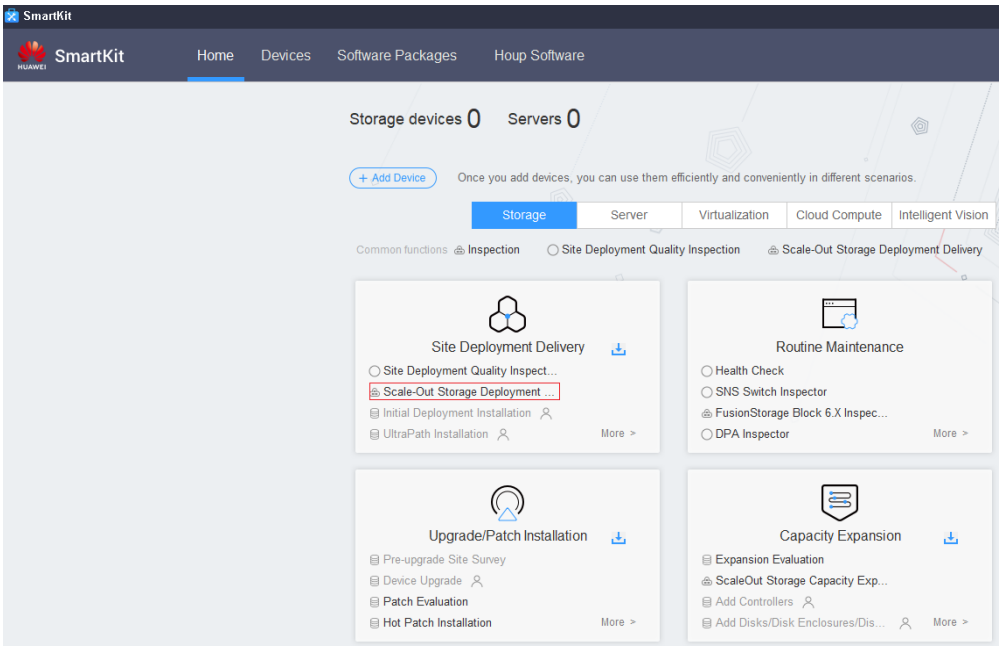
 Copyright © Huawei Technologies Co., Ltd.

ii. On the SmartKit page, click **Product Documentation**, find the user guide of the corresponding version, and install and run SmartKit respectively by following the instructions provided in sections "Installing SmartKit" and "Running SmartKit".

2. Install the Scale-Out Storage Deployment Delivery tool by referring to section "Installing Functions" in the SmartKit user guide.

Step 2 Go to the **Site Deployment Delivery** page.

1. On the home page of SmartKit, choose **Site Deployment Delivery** > **Scale-Out Storage Deployment Delivery**. The **Scale-Out Storage Deployment Delivery** page is displayed.

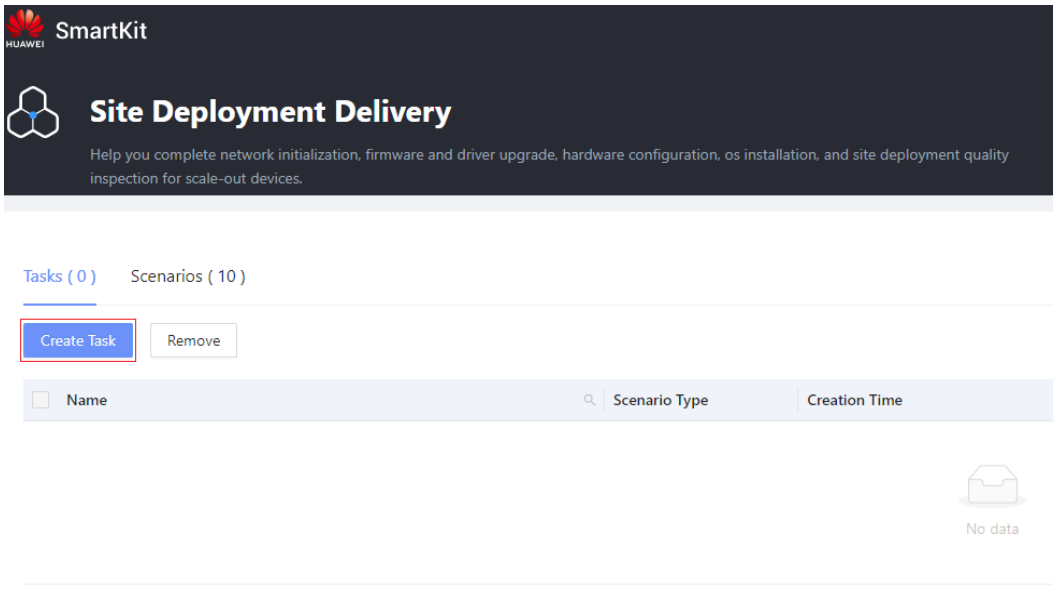


2. On the **Scale-Out Storage Deployment Delivery** page, click **Scale-Out Storage Deployment Delivery**. The **Site Deployment Delivery** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Click **New**. The **Select Scenario** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

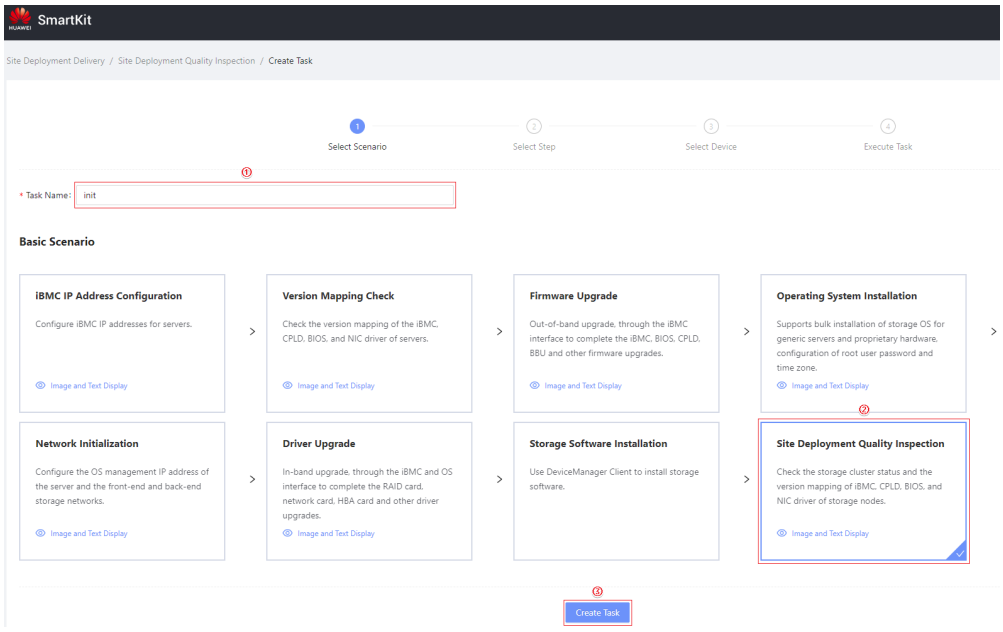


Step 4 Select a scenario.

1. Set **Task Name**, select **Site Deployment Quality Inspection**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).



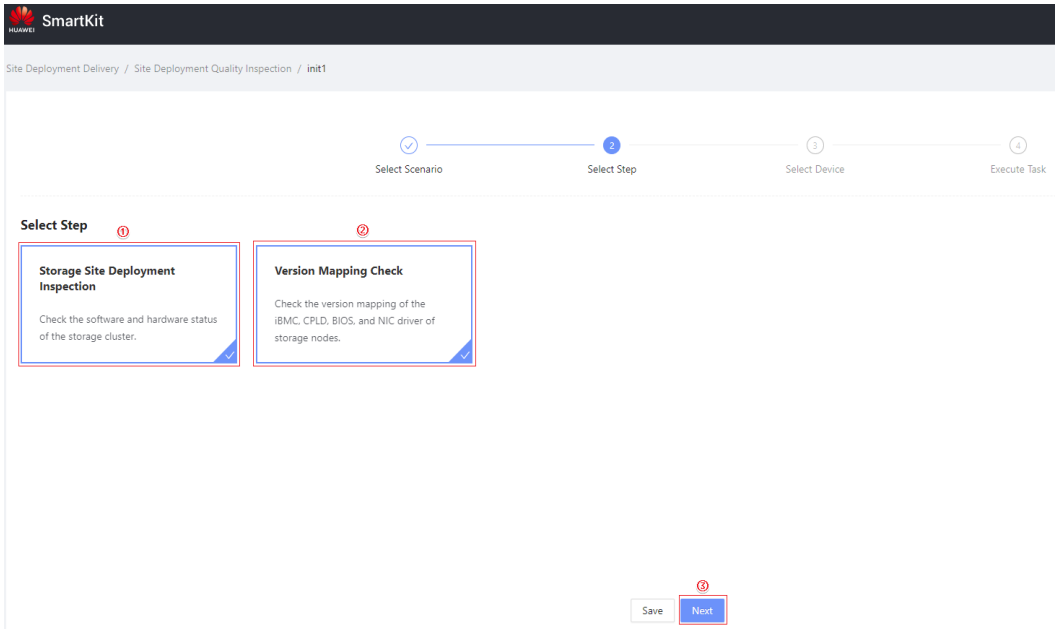
2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

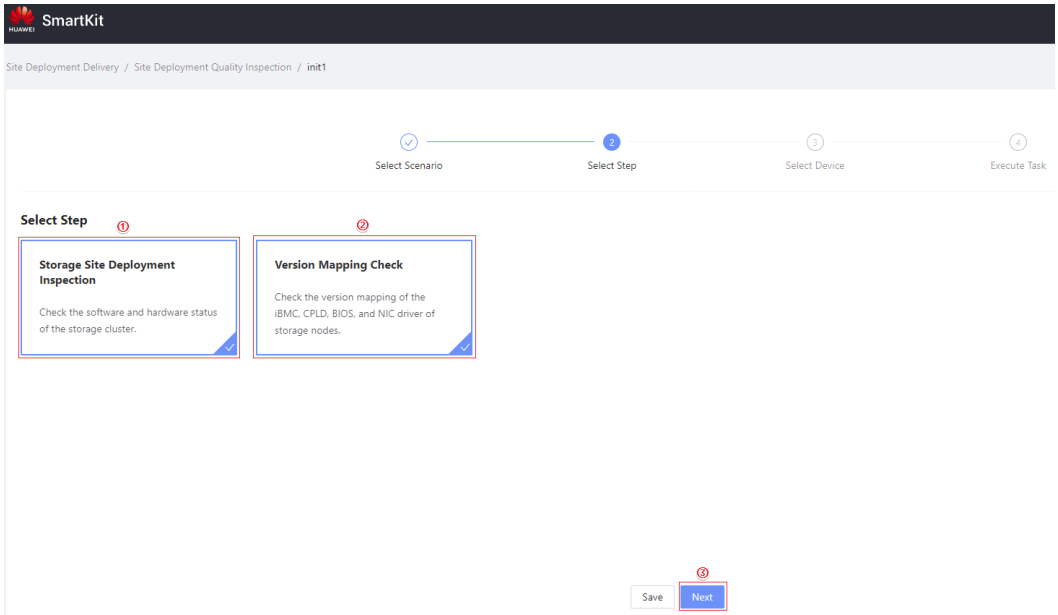
   NOTE

   If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Select **Storage Site Deployment Inspection** and **Version Mapping Check**, and click **Next**.

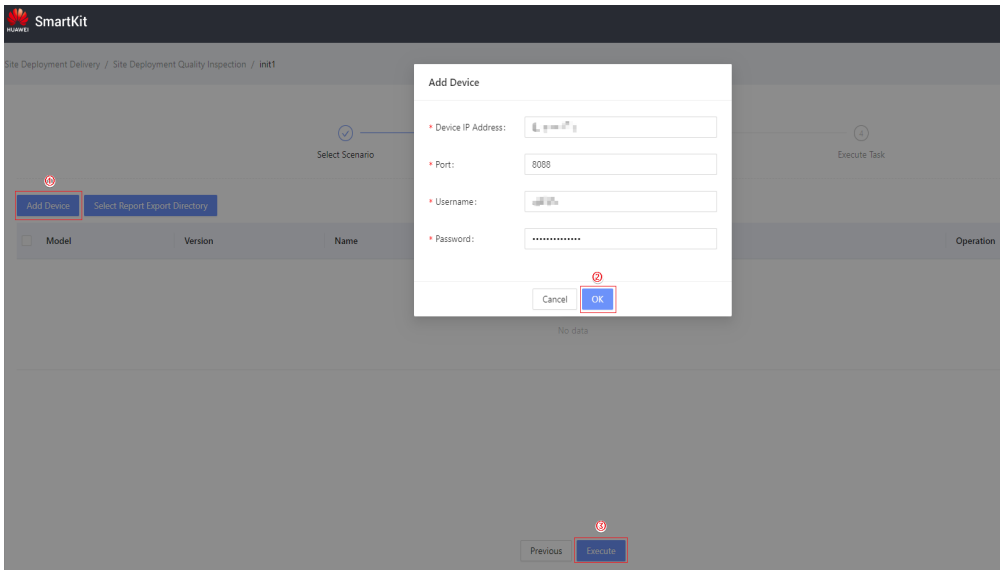




Step 6 Select a device.

1. Add a device.

 Copyright © Huawei Technologies Co., Ltd.



a. Click **Add Device**. The **Add Device** dialog box is displayed.

b. Enter device information as prompted and click **OK**.

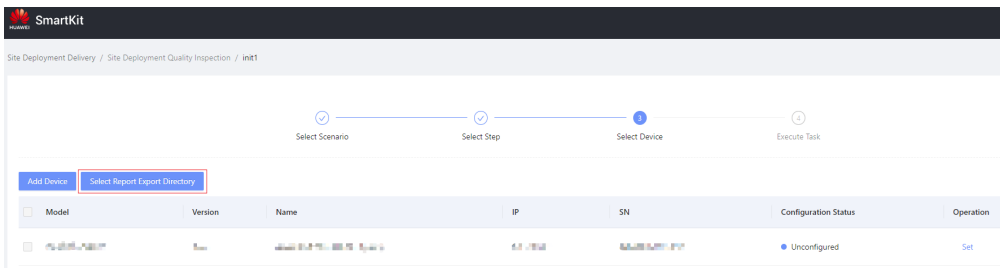
Table 6-10 Device information

Name	Description
Device IP Address	DeviceManager management IP address
Port	Port of DeviceManager. Use default port **8088**.
Username	DeviceManager login account
Password	Password for logging in to DeviceManager

NOTE

If the device has been added, it is displayed in the list by default. You do not need to add it again.

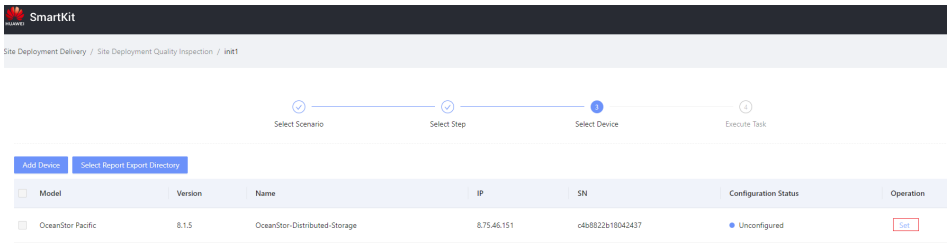
2. Click **Select Report Export Directory** and specify a save path for the report.



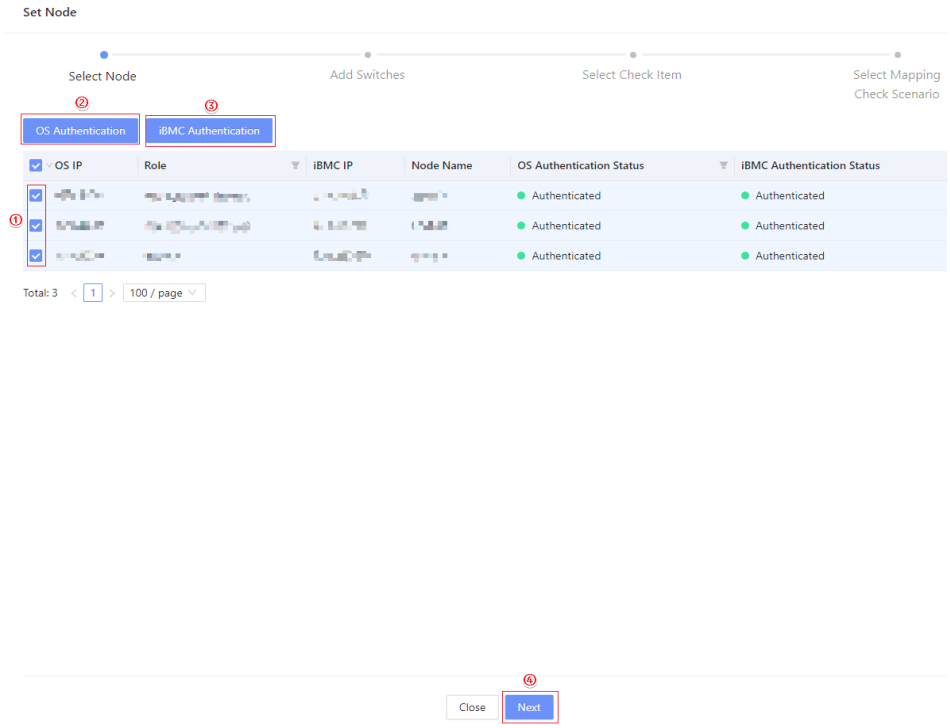
3. Set a check policy.

a. Click **Set** in the **Operation** column of a device. The **Set Node** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



b. Select a node and authenticate it.



i. Select the nodes to be checked.

ii. Click **OS Authentication** and enter related information as prompted to complete the authentication.

iii. Click **iBMC Authentication** and enter related information as prompted to complete the authentication.

iv. Click **Next**. The **Add Switches** page is displayed.

c. (Optional) Add switches.

NOTE

This step applies only to access switches whose storage network uses RoCE networking. In other scenarios, click **Skipped** to skip this step.

i. Click **Add Switch** and enter information about all storage switches.

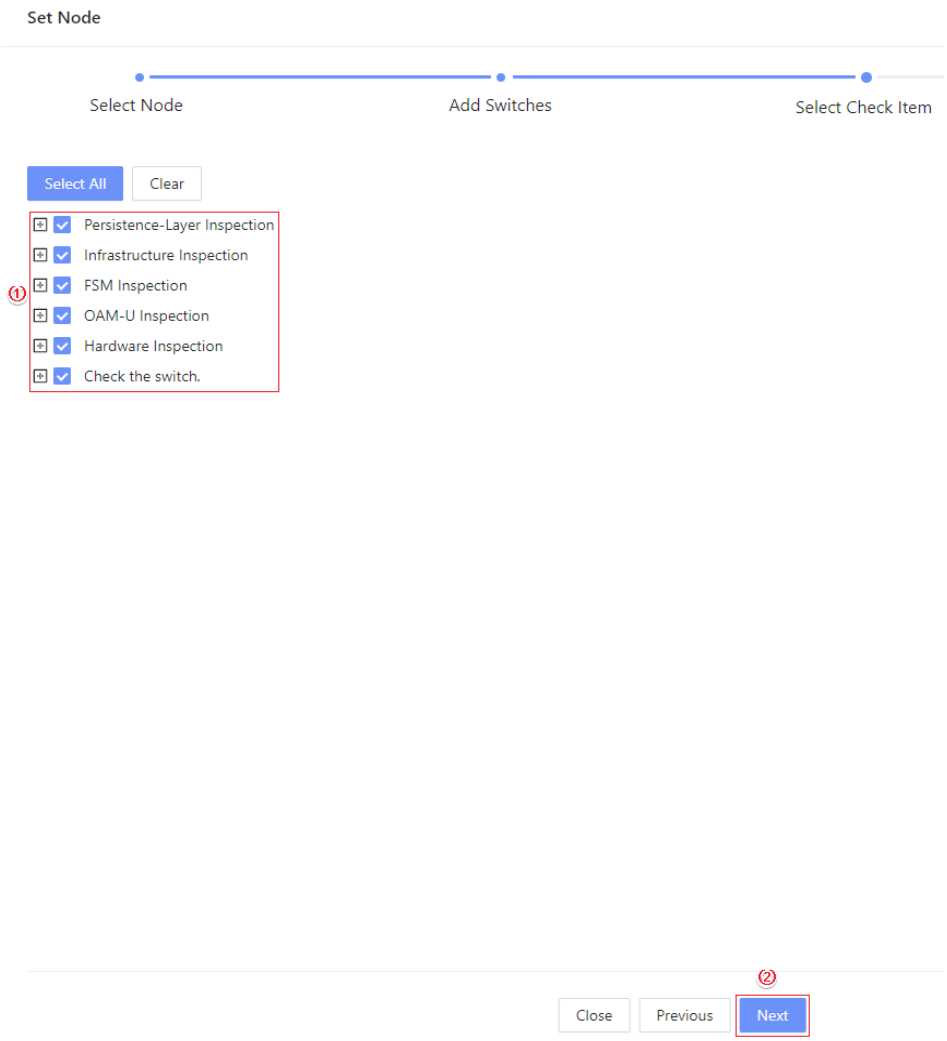
NOTE

You can also click **Download Template** to download the switch information template, enter login information, and click **Batch Import**.

ii. Click **Next**. The **Select Check Item** page is displayed.

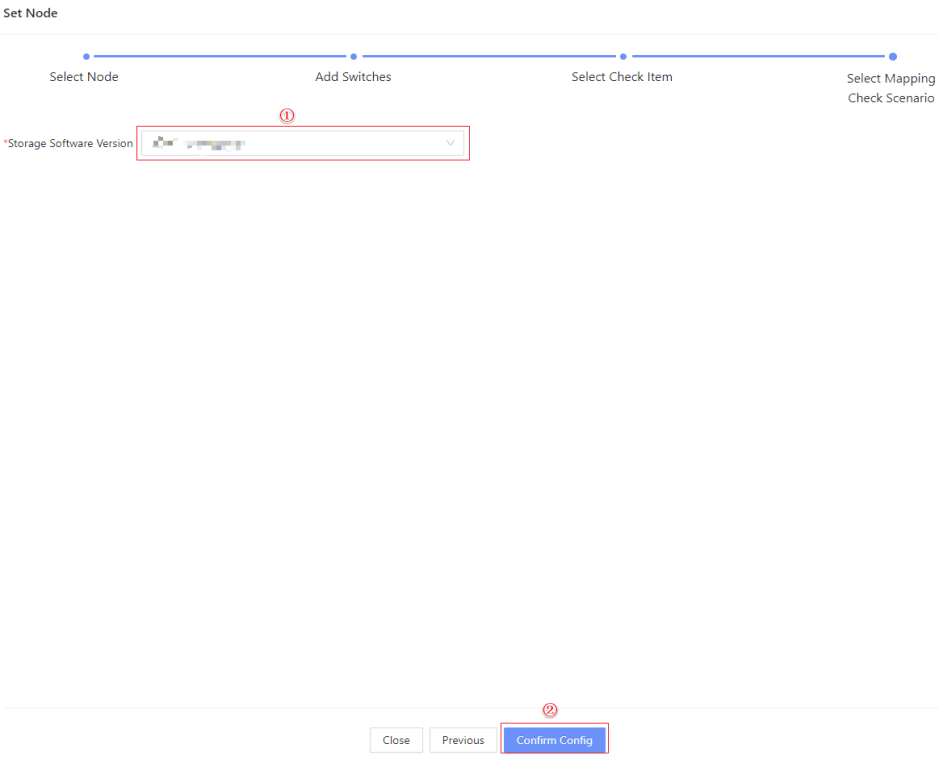
d. Select the items to be checked and click **Next**. The **Select Mapping Check Scenario** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



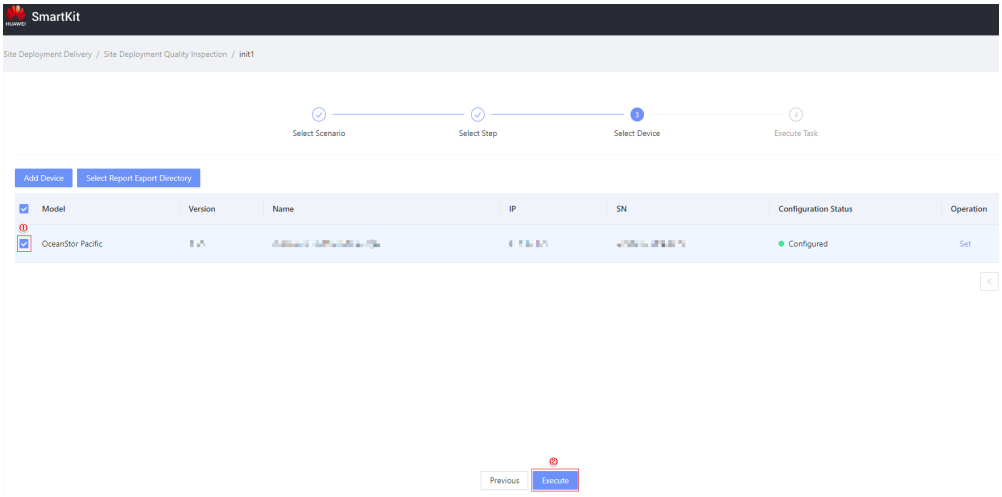
e. Select a storage software version and click **Confirm Config**.

 Copyright © Huawei Technologies Co., Ltd.



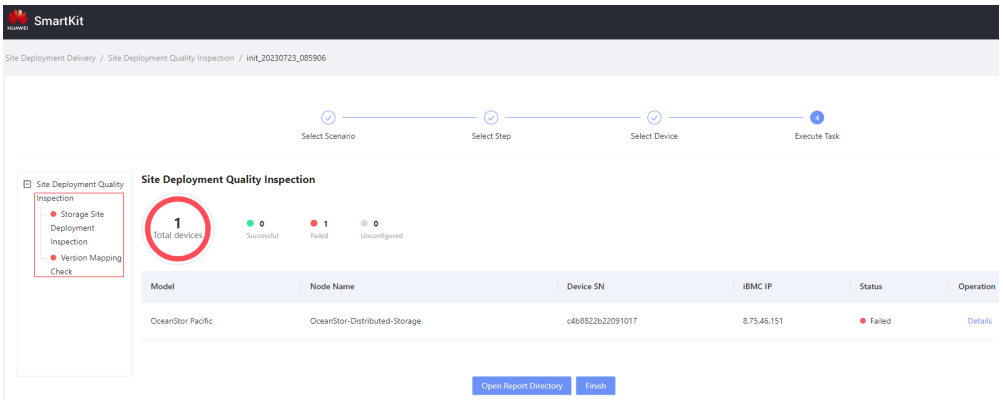
Step 7 Execute the task.

1. Select a device, click **Execute**, and enter the information about the inspection report personnel as prompted.



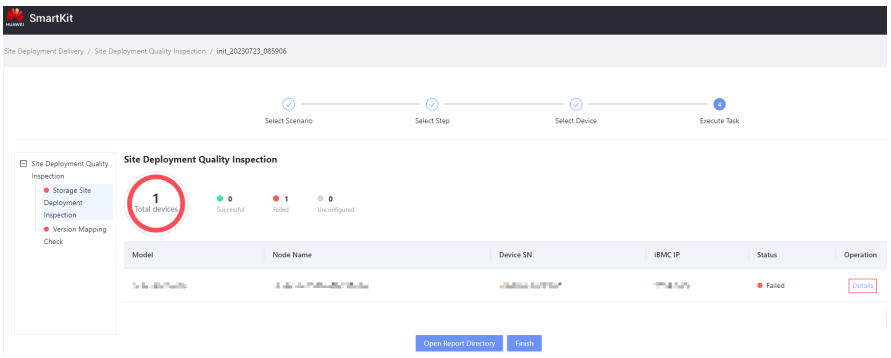
2. After the task is complete, check whether the **Storage Site Deployment Inspection** and **Version Mapping Check** items pass the check (marked in green).

 Copyright © Huawei Technologies Co., Ltd.



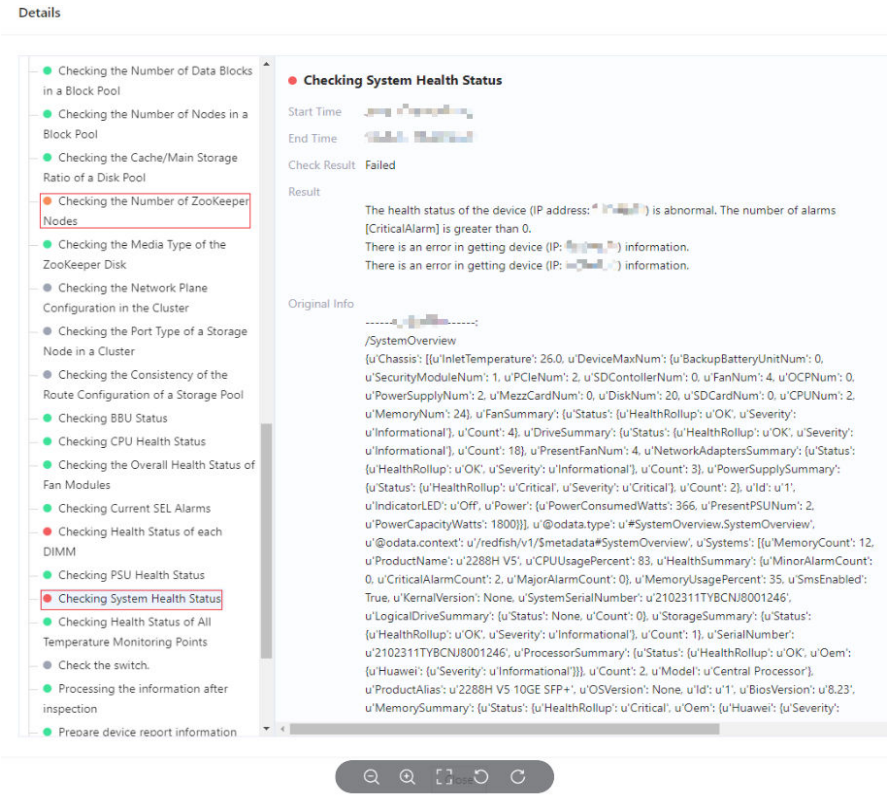
- If yes, click **Finish**.
- If no, perform the following steps for the two check items (after the troubleshooting is complete, click **Finish**):

  i. Click **Details** in the **Operation** column of the corresponding device.

  ii. Click the check items that fail to pass the check (marked in red) and the check items that need to be optimized (marked in orange) in sequence, and handle the problems according to the description in **Result**. The following uses **Storage Site Deployment Inspection** as an example:

 Copyright © Huawei Technologies Co., Ltd.



----End

6.4.2 Configuring Basic File Services (DPC Scenario)

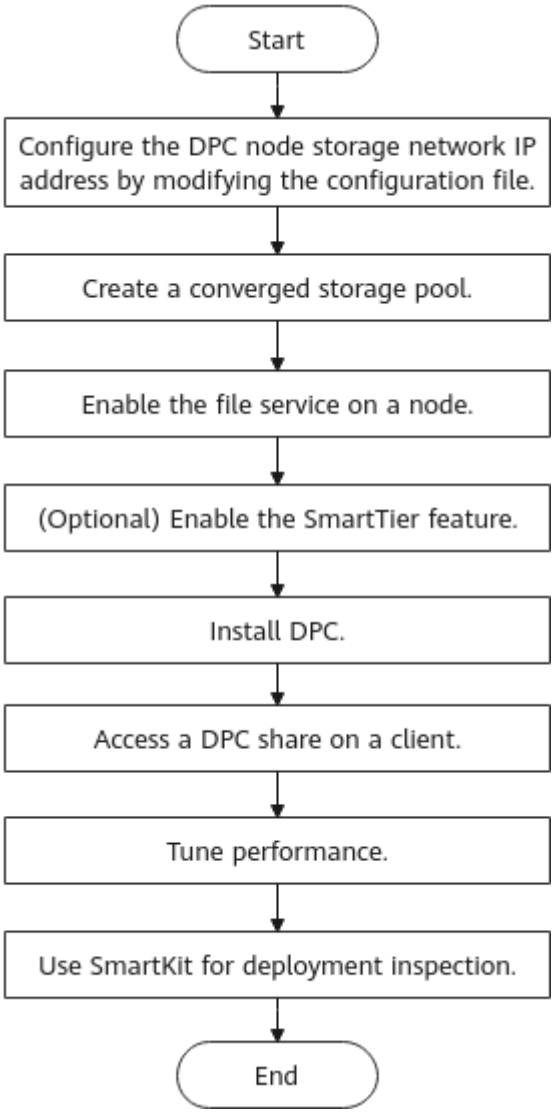
6.4.2.1 Configuration Process

By configuring the basic storage services, you can divide the storage space provided by the storage system into name spaces and mount them to the DPC client. The storage space can be accessed on the DPC client.

Figure 6-3 shows the process for configuring the file service.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-3 Configuration process in the DPC scenario



6.4.2.2 Configuring the DPC Node Storage Network IP Address by Modifying the Configuration File

For details about how to configure the DPC node storage network, see the *OceanStor Pacific Series DPC Storage Network Configuration Guide*.

6.4.2.3 Creating a Converged Storage Pool

This section describes how to create a storage pool from which application servers can use storage space.

Context

- You have installed storage nodes.
- You are advised to configure no more than 32 nodes for each disk pool. If the number of nodes exceeds 32, divide them into multiple disk pools. In this case, it is recommended that the number of nodes in each disk pool be the

 Copyright © Huawei Technologies Co., Ltd.

same. For example, if there are 90 nodes, you are advised to divide them into three disk pools. Each disk pool contains 30 nodes.

- HDD 4KN disks cannot be added to the same disk pool as other types of disks.
- The total capacity of cache disks on a single storage node to be added to a storage pool must be greater than **Max. Main Storage Media per Node** x 40 GB.

Precautions

Currently, only one converged storage pool can be created. Skip this operation if a converged storage pool has been created using the LLD during initialization.

Procedure

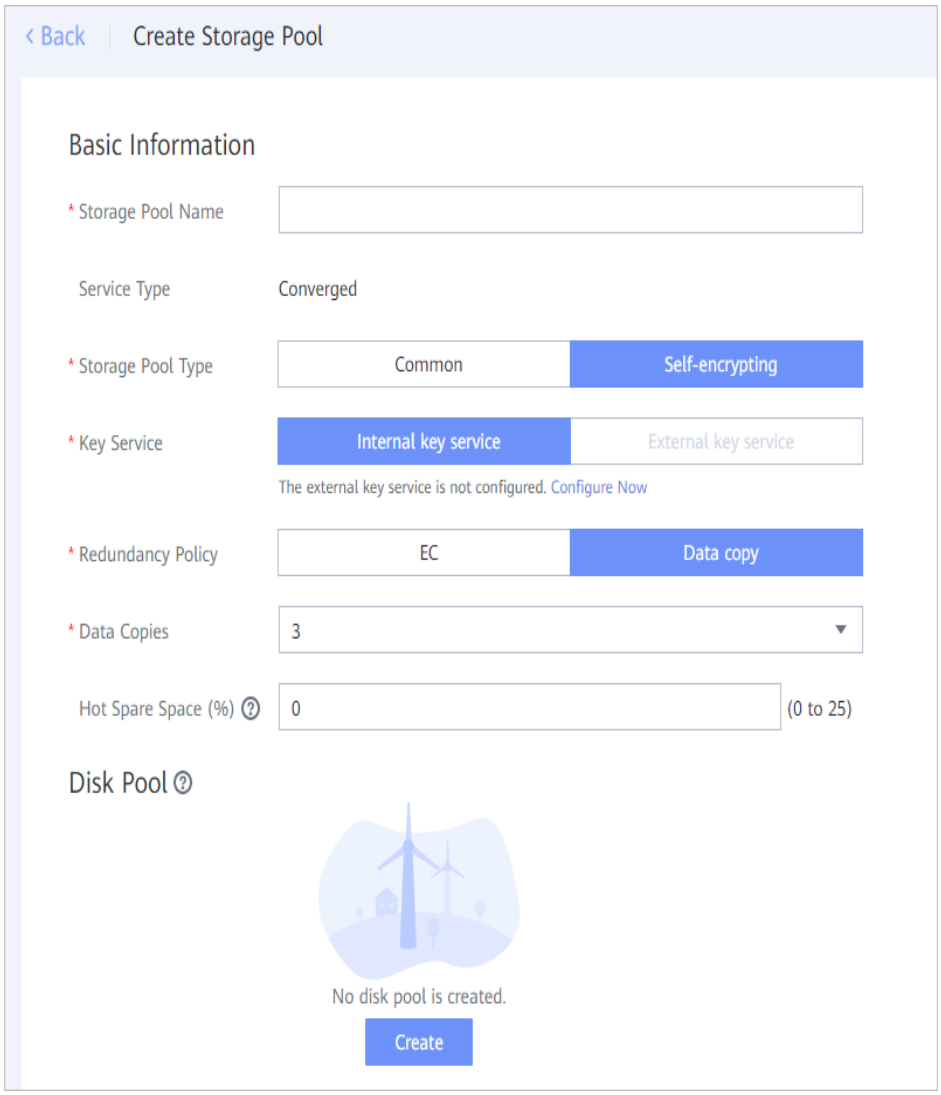
Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Resources** > **Storage Pool**.

Step 3 Click **Create**.

The **Create Storage Pool** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



Step 4 Configure basic information for the storage pool.

Table 6-11 describes related parameters.

Table 6-11 Storage pool parameters

Parameter	Description
Storage Pool Name	Name of the storage pool. **NOTE** • The name must be unique. • The name can contain only letters, digits, underscores (_), and hyphens (-). • The name contains 1 to 64 characters.
Service Type	Service type of the storage pool. In this example, the value is **Converged**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Storage Pool Type	Type of the storage pool. Possible options are **Common** and **Self-encrypting**. You are advised to select **Common**. If you have high requirements on data security, select **Self-encrypting**. • **Common**: This type of storage pools does not support data encryption. • **Self-encrypting**: This type of storage pools supports data encryption. **NOTE** • Currently, converged storage pools do not support self-encrypting SATA disks. • A self-encrypting storage pool can be created only when all the following conditions are met: 1. OceanStor Pacific series 8.1.2 or a later version is deployed, and self-encrypting disks have been configured. 2. An advanced license has been imported. 3. Self-encrypting 4K SAS disks are used if **Main Storage** is set to **Self-encrypting SAS**.
Key Service	When creating a self-encrypting storage pool, you need to select a key management service. • **Internal key service**: The built-in key management function of the system is used. • **External key service**: An external key management server is used. If you select this option, you need to configure the external key service first. For details, see **6.5.6 Managing the External Key Service**.
Redundancy Policy	Redundancy policy of the storage pool. Possible options are **EC** and **Data copy**. Considering performance and reliability, **EC** is recommended. • **EC**: Data redundancy protection is implemented by calculating parity fragments. • **Data copy**: Multiple copies of the same data are stored on different nodes for data protection.
Data Copies	Number of redundant data copies allowed by the storage pool. When **Data Copies** is set to **3**, if the number of storage nodes is greater than 3, a maximum of two faulty nodes are allowed; if the number of storage nodes is 3, only one faulty node is allowed. **NOTE** • This parameter is available only when **Redundancy Policy** is set to **Data copy**. • If **Service Type** is set to **Intelligent video and image**, three-copy storage pools cannot be created.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Hot Spare Space (%)	Hot spare space is the space reserved in the system to take over data from faulty disks. This improves reliability and avoids system redundancy reduction. To support data rebuilding after single-disk failure at high capacity usage, the recommended value is (1/Number of disks on a single node) x 100%. **NOTE** Reserving too much hot spare space will occupy excessive available system capacity, causing the available capacity obtained by users to decrease. Configure the hot spare space properly. [Value range] 0 to 25 [Default value] **0**
Storage Pool Mode	If EC redundancy level of the storage pool is +3:1 or higher, you need to set the storage pool mode. If the reliability mode is selected, write cache acceleration cannot be enabled.

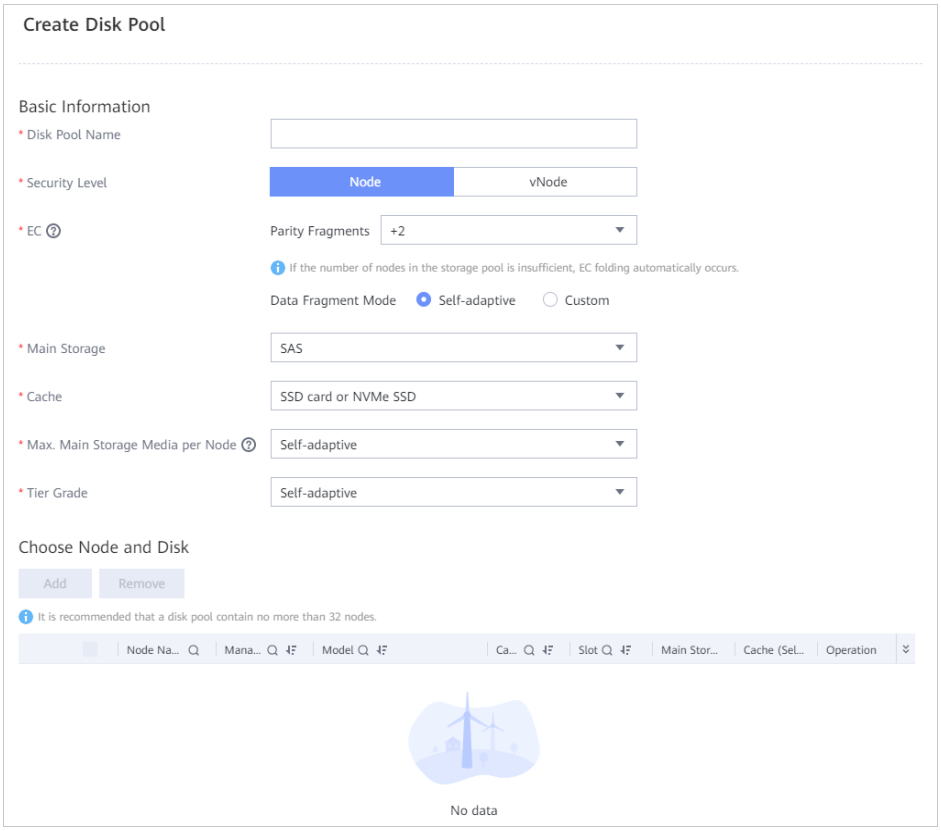
Step 5 Create a disk pool.

NOTE

For details about how to configure disk pools, see the plan in the BOQ.

1. In the **Disk Pool** area, click **Create**.
   The **Create Disk Pool** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



2. Set basic parameters for the disk pool.
   Table 6-12 describes related parameters.

Table 6-12 Disk pool parameters

Parameter	Description
Disk Pool Name	Name of the disk pool. **NOTE** – The name must be unique. – The name can contain only letters, digits, underscores (_), and hyphens (-). – The name contains 1 to 64 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Security Level	Security level of the disk pool. – **Node**: ▪ *N*+*M*: *N* data fragments and *M* parity fragments are randomly stored on different nodes. (The number of storage nodes is greater than *N* + *M*. To ensure reliability, data fragments are stored on different nodes.) In this case, the disk pool can tolerate simultaneous failures of *M* disks or *M* nodes. ▪ *N*+*M*:1 (folded): *N* data fragments and *M* parity fragments are randomly distributed on all nodes. Any node may store *M* fragments. In this case, the disk pool can tolerate simultaneous failures of *M* disks or one node. – **vNode**: A vNode is a logical area consisting of multiple disks on a node. In OceanStor Pacific 9546, a node contains two vNodes. In OceanStor Pacific 9550, a node contains four vNodes. *N* data fragments and *M* parity fragments are stored on different vNodes, and EC redundancy calculation is performed by vNode. A larger EC ratio indicates higher storage utilization. If a node is faulty, its disks can be taken over by the other node in the same chassis and main storage disks will not be degraded or rebuilt by virtue of the dedicated hardware design of OceanStor Pacific 9546 and OceanStor Pacific 9550. **NOTE** **vNode** is supported only when **Redundancy Policy** is set to **EC**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
EC	EC redundancy policy of the disk pool. Select the EC redundancy ratio planned in the Bill of Quotation (BOQ). **NOTE** – This parameter is available only when **Redundancy Policy** is set to **EC**. – When creating multiple disk pools, ensure that the settings of **Parity Fragments** for the disk pools are the same. – The data fragment mode can be **Self-adaptive** or **Custom**. ■ When you select **Self-adaptive**, the system automatically sets the number of data fragments based on the EC redundancy ratio tables and the selected nodes or cabinets and parity fragments. For details about the EC redundancy ratio tables, see **Functions and Features** > **Key Features** > **File/Object/HDFS Service** > **Elastic EC** in the *OceanStor Pacific Series 8.2.1 Product Description*. ■ When you select **Custom**, the number of data fragments is an even number ranging from 4 to 22. The number of nodes that can be contained in a disk pool and the disk pool utilization vary depending on the number of data fragments selected. For details, refer to the actual page.
Main Storage	Main storage type of the disk pool. – When **Storage Pool Type** is set to **Common**, the value of this parameter can be **SAS**, **Self-encrypting SAS**, **SATA**, **Self-encrypting SATA**, **SSD**, and **SSD card or NVMe SSD**. In this case, self-encrypting drives function as common disks and do not use the encryption function. – When **Storage Pool Type** is set to **Self-encrypting**, the value of this parameter can be **Self-encrypting SAS**, **Self-encrypting SATA**, **Self-encrypting SSD card or NVMe SSD (with Chinese cryptographic algorithms)**, or **Self-encrypting SSD card or NVMe SSD (with international cryptographic algorithms)**. – Each node must be configured with at least four disks of the same type. **NOTE** Meanings of the values are: – **SAS**: SAS HDDs – **SATA**: SATA HDDs – **SSD card or NVMe SSD**: NVMe SSDs – **SSD**: SAS SSDs

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Cache	Cache type of the disk pool. **NOTE** – This parameter is not required when **Main Storage** is set to **SSD** or **SSD card or NVMe SSD**. – Meanings of the values are: ■ **SSD card or NVMe SSD**: NVMe SSDs ■ **SSD**: SAS SSDs
Max. Main Storage Media per Node	Maximum number of main storage disks that can be used on a single storage node to store user data. The value of this parameter determines the allocation of cache and compute resources on the node. Set this parameter based on site requirements. To ensure that cache resources can be allocated to newly added main storage disks in the case of capacity expansion, you are advised to set this parameter based on the total number of main storage disks after capacity expansion. – If the value is too small, newly added main storage disks cannot be allocated with cache resources. Cache resources can be allocated to newly-added main storage disks only after both main storage disks and cache disks are added. – If the value is too large, extra cache resources are reserved. As a result, cache resources cannot be fully utilized to improve read/write performance. If you select **Self-adaptive**, the system automatically determines the value based on the number of selected main storage disks. Assume that the number of selected main storage disks is N: – If $4 \leq N \leq 12$, a single node supports a maximum of 12 main storage disks. – If $12 < N \leq 36$, a single node supports a maximum of 36 main storage disks. – If the type of nodes in the disk pool is OceanStor Pacific 9550, a single node supports a maximum of 60 main storage disks. Ensure that the total capacity of the cache disks on selected storage nodes is greater than the maximum number of main storage disks on a single node multiplied by 40 GB. If you select **Custom**, set the value based on site requirements. The value ranges from 4 to 60.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Tier Grade	Tier grade of the disk pool, which is defined based on the type of main storage disks in the disk pool. Possible values are **Hot**, **Warm**, **Cold**, and **Self-adaptive**. You can choose **Resources** > **Tuning** > **SmartTier** and set tiering policies to store different files to disk pools of different tier grades. **NOTE** – If you select **Self-adaptive**: When **Main Storage** is set to **SSD** or **SSD card or NVMe SSD**, **Self-adaptive** equals to tier grade **Hot**. When **Main Storage** is set to **SAS**, **Self-adaptive** equals to tier grade **Warm**. When **Main Storage** is set to **SATA**, **Self-adaptive** equals to tier grade **Cold**. – If you select a tier grade, you are advised to configure the storage tiers based on the self-adaptive rules.

3. In the **Choose Node and Disk** area, select the nodes and disks that are used to create the disk pool.

   NOTE

   – You can click **Add** and add nodes and disks in the cluster to the disk pool on the **Choose Node and Disk** page that is displayed.
   – You can select one or more added nodes or disks and click **Remove** to remove them.

4. Click **OK** and confirm your operation as prompted.

Step 6 Click **Create**.

Step 7 Confirm your operation as prompted.

----End

6.4.2.4 Enabling the File Service on a Node

This section describes how to enable the file service for nodes in a storage pool.

Prerequisites

- A storage pool has been created.
- This operation can be performed only when no node with the file service enabled exists in the storage pool. Otherwise, add nodes for the file service by referring to **6.5.8 Adding a Node for an Enabled Service**.

Procedure

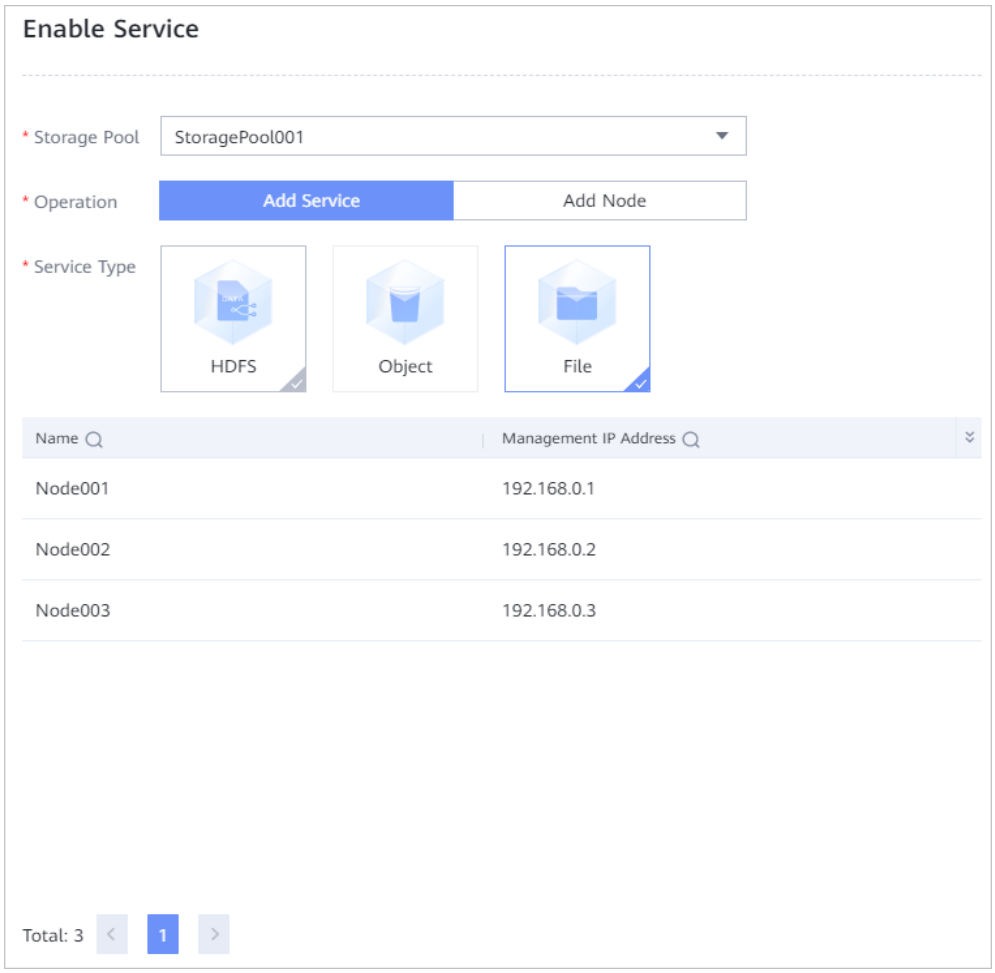
Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Resources** > **Services** > **Basic Service**.

Step 3 Click **Enable Service**.

The **Enable Service** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



Step 4 Select the storage pool for which you want to enable the file service.

Step 5 Select **Add Service** in **Operation**.

NOTE

This parameter is displayed only when at least one service is enabled on the nodes in the storage pool.

Step 6 Select **File** in **Service Type**.

Step 7 Based on service requirements, select at least three nodes in the **Available Nodes** area on the left. They will be automatically added to the **Selected Nodes** area on the right.

NOTE

You need to select nodes only when all services (file, object, and HDFS services) of the storage pool are disabled. Otherwise, the system enables the file service for all nodes where other services have been enabled by default.

Step 8 Click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

6.4.2.5 (Optional) Enabling the SmartTier Feature

If a cluster contains two or more types of media, you can perform this operation to enable the SmartTier feature and write files based on the default placement policy.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Tuning** > **SmartTier**.

Step 3 By default, the SmartTier feature is disabled by the storage system. When you go to the **SmartTier** page for the first time, you need to click **Enable** to enable the SmartTier feature.

----End

6.4.2.6 Installing DPC

6.4.2.6.1 Checking the Connectivity Between the Internal Management Networks of a Management Node and a DPC Node Before Installation

A DPC node can be successfully added only when its internal management network is properly connected to the internal management networks of management nodes.

You can run the **ping [-6]** *Destination IP address* command on a management node to check the connectivity. If their internal management networks are not properly connected, perform the following steps to configure a route.

Procedure

NOTE

A route must be configured for both management nodes.

Step 1 Check whether management nodes and storage nodes are deployed on the same servers.

If yes, configure a route from the management nodes to the DPC node by referring to **6.4.2.9.1 Configuring a Static Route**.

If no, configure a route from the management nodes to the DPC node by referring to **Step 2** to **Step 4**.

Step 2 Use an external management IP address to remotely log in to a management node as user **fsadmin** through a remote connection tool.

Step 3 Run the following command to switch to user **root**.

```
su - root
```

Step 4 Run the following commands to configure a route from the management node to the DPC node. If the configuration file does not exist in the current directory, run the following commands to create and edit the configuration file.

 Copyright © Huawei Technologies Co., Ltd.

```
vi /etc/sysconfig/static-routes
any net Internal management IP address segment of the DPC node/Subnet prefix gw Internal management IP address gateway of the management node
```

The following is an example:

```
vi /etc/sysconfig/static-routes
any net 192.168.4.0/24 gw 192.168.3.254
```

----End

6.4.2.6.2 Creating DPC

This section describes how to create DPC on a new node, that is, install DPC on a compute node.

Installation Requirements

- The available disk space of the compute node meets the following requirements:
  - DPC software installation directory (**/opt**): ≥ 8 GB. If there is an upgrade plan, the space must be greater than or equal to 15 GB.
  - **/var/log**: ≥ 5 GB
  - **/dev/shm**: ≥ 2 GB
  - **/tmp**: ≥ 2 GB if there is an upgrade plan
- The memory required for running DPC software on the compute node is greater than or equal to 16 GB, and the memory reserved for the OS is greater than or equal to 8 GB.
- For details about the requirements on the OS and NIC driver version of the compute node, visit **OceanStor Pacific Compatibility Query**. (Click the link, set **Compatible With** to **DPC Basic Connectivity**, and select related configurations based on the actual environment.)

NOTICE

If Secure Boot is enabled on the compute node, check whether the OS corresponding to DPC supports Secure Boot by referring to **OceanStor Pacific Compatibility Query**. (Click the link, set **Compatible With** to **DPC Basic Connectivity**, and check whether the function is supported as prompted.)

- If the OS corresponding to DPC supports Secure Boot, you need to import the certificate corresponding to Huawei OceanStor Pacific series 8.2.1RC1 storage software. Otherwise, the software installation will fail. For details, see **6.4.2.9.2 Importing the OS Certificate of a DPC Node**.
- If the OS corresponding to DPC does not support Secure Boot, disable Secure Boot on the compute node. Otherwise, the software installation will fail.

- To maximize the performance of the compute node, you are advised to disable firewall software. If the firewall needs to be enabled for security purposes, ensure that correct firewall rules are configured for all ports on the DPC compute node by referring to *OceanStor Pacific Series 8.2.1 Communication Matrix*.

Copyright © Huawei Technologies Co., Ltd.

- To improve performance, the DPC kernel-mode module binds threads to cores. Therefore, do not directly isolate CPU cores from applications on compute nodes. Otherwise, file system mounting fails and DPC is unavailable.
- The OS time of the compute node must be the same as that (local time) of a storage node.
- DPC software cannot be installed in a container.
- The script interpreter of the compute node must be sh or bash. To view the script interpreter of a node, run the following command (the command output indicates that the script interpreter is bash):
  ```
  cat /etc/passwd|grep root:/root|awk -F ":" '{print $NF}'
  /bin/bash
  ```
- If the compute node runs the Ubuntu OS, disable the automatic system update function. To to so, log in to the node and change the values of all configuration items in the **10periodic** and **20auto-upgrades** files (only one of the two files may exist) from **1** to **0**.
  a. Run the **vi /etc/apt/apt.conf.d/10periodic** command and change the values of all configuration items from **1** to **0**.
  b. Run the **vi /etc/apt/apt.conf.d/20auto-upgrades** command and change the values of all configuration items from **1** to **0**.

  ```
  root@ubuntu:/home/testTools/vdbench# cat /etc/apt/apt.conf.d/10periodic
  APT::Periodic::Update-Package-Lists "0";
  APT::Periodic::Download-Upgradeable-Packages "0";
  APT::Periodic::AutocleanInterval "0";
  root@ubuntu:/home/testTools/vdbench# cat /etc/apt/apt.conf.d/20auto-upgrades
  APT::Periodic::Update-Package-Lists "0";
  APT::Periodic::Unattended-Upgrade "0";
  root@ubuntu:/home/testTools/vdbench#
  ```
- If the storage network uses RoCE, the lldpad service must be disabled. Otherwise, nodes will be isolated and services will be interrupted. To disable the lldpad service, run the following command:
  ```
  systemctl stop lldpad.service
  ```
- You have configured a management IP address and a storage IP address for the compute node.
- You have obtained the software package **OceanStor-Pacific_8.2.1RC1_DPC_MULTI.tar.gz** for installing DPC on the compute node in container-based deployment mode.
- If the compute node uses a third-party OS, install the OS dependency package by referring to **6.4.2.9.3 Installing the OS Dependency Package**.

Procedure

Step 1 If the compute node uses a third-party OS, install the OS dependency package by referring to **6.4.2.9.3 Installing the OS Dependency Package**. If you have installed the OS dependency package, skip this step.

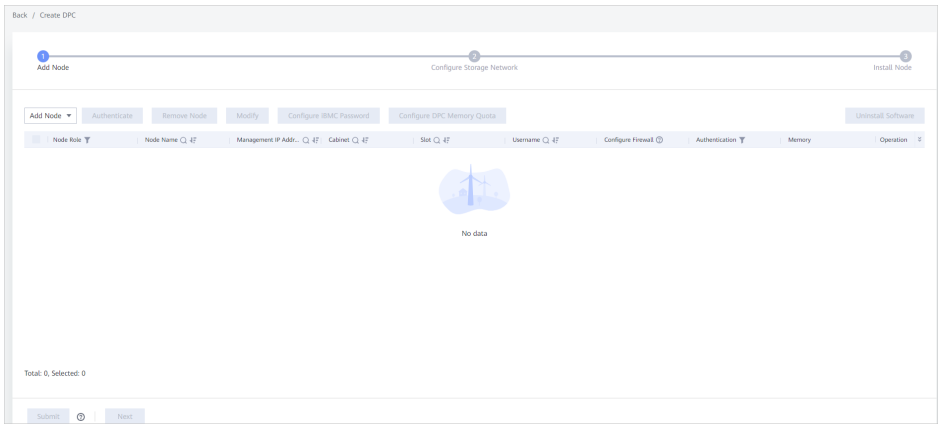
Step 2 Log in to DeviceManager.

Step 3 Choose **Resources** > **Access** > **DPC**.

Step 4 Click **Create DPC** and select **New Node**.

The **Create DPC** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



NOTE

If no DPC node has been created in the system, clicking **Create DPC** directly enters the **Create DPC** page.

Step 5 Click **Batch Import Node** or **Manually Add Node** to add nodes.

NOTE

- The total number of nodes imported in batches and manually added nodes cannot exceed 512. The total number of DPC nodes in the system cannot exceed 6000.
- If the number of DPC nodes exceeds 1024, upgrade the OFED driver. For details, see the *OceanStor Pacific Series 8.2.1RC1 Firmware Installation and Upgrade Guide*.

- **Batch Import Node**
  a. Choose **Add Node** > **Batch Import Node**.
  b. Click **Download the template** to download the template locally. Fill the information in the template, click ··· and select the template, and then click **Upload**. The nodes are imported to the system in a batch.
  c. Select the newly imported nodes and click **Authenticate**.
     On the **Authentication** page, select an installation mode for the nodes. Possible options are **Regular installation** and **Pre-installation**. If you select **Regular installation**, set **Username**, **Password**, and **Password of root** for authentication.

     NOTE

     Select **Pre-installation** when the DPC software has been pre-installed for compute nodes during the file service installation.

- **Manually Add Node**
  a. Choose **Add Node** > **Manually Add Node**.
     The **Add Node** page is displayed on the right.
  b. Set parameters for a node. **Table 6-13** describes related parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-13 Node parameters

Parameter	Description
Management IP Address	Management IP address of the node. **NOTE** ■ The management IP address cannot use the same subnet as the storage, control, service, or replication network. ■ When the management network is isolated, the management IP address must be able to communicate with the internal management network. ■ When the management network is isolated and the internal management networks of management nodes and compute nodes are in different subnets: If the internal management networks and the storage network do not share IP addresses, you need to configure static routes on the management nodes to the internal management network of the compute nodes. Otherwise, you can use storage network routes instead of configuring separate static routes.
Cabinet	Cabinet where the node resides. [Value range] ■ The value contains 1 to 256 characters. ■ The value can contain only letters, digits, underscores (_), and hyphens (-). ■ The value cannot start or end with a space.
Node Name	Name of the node. [Value range] ■ The name contains 1 to 64 characters. ■ The name can contain only letters, digits, hyphens (-), underscores (_), and periods (.), and must start and end with a letter or digit. A period (.) cannot be adjacent to a period (.), hyphen (-), or underscore (_).
Chassis	Chassis where the node resides.
Slot	Serial number of the slot where the node resides.
Node Role	Role of the node. **DPC compute** is automatically selected.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Configure Firewall	Whether to automatically configure the node firewall. This function is enabled by default. If the firewall is disabled, manually enable it. For details, see the *OceanStor Pacific Series 8.2.1 Communication Matrix* to ensure that all ports of compute nodes are configured with correct firewall rules. **NOTE** This parameter is available only when **Installation Mode** is set to **Regular installation**. If firewall has been enabled on the node, enable **Configure Firewall** when adding the node.
Installation Mode	Installation mode of the node. Possible options are **Regular installation** and **Pre-installation**. If you select **Regular installation**, set **Username**, **Password**, and **Password of root** for authentication. **NOTE** Select **Pre-installation** when the DPC software has been pre-installed for compute nodes during the file service installation.
Username	User name used for logging in to the DPC node. **NOTE** This parameter needs to be specified only when **Installation Mode** is set to **Regular installation**.
Password	Password used for logging in to the DPC node. **NOTE** This parameter needs to be specified only when **Installation Mode** is set to **Regular installation**.
Password of root	Password of user **root** of the DPC node. **NOTE** ■ If you log in to the DPC node not as user **root**, you need to enter the password of user **root**. ■ This parameter needs to be specified only when **Installation Mode** is set to **Regular installation**.

c. Click **OK** to add the node to the list.

Step 6 Click **Submit** to configure the nodes and install the network management components.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- You can select a newly added node and click **Authenticate** to authenticate the node again.
- You can select a node to be removed and click **Remove Node** to remove the node and uninstall the storage software on the node, or click **More** on the right of the node and select **Remove Node** to remove the node. After the node is removed, it is no longer managed by the cluster.
  - Nodes that have not been configured and installed can be directly removed. Perform the operations as prompted.
  - Nodes that have been configured and installed can be removed only after being authenticated. Perform the operations as prompted.
- You can select a node to be modified and click **Modify** to modify the node, or click **More** on the right of the node and select **Modify** to modify the node.
- You can select a newly added node that contains the **Storage** role and click **Set iBMC Password** to configure the user name and password for authenticating the iBMC server.
- If the newly added nodes include a DPC compute node, you can click **Configure DPC Memory Quota**. On the **Configure DPC Memory Quota** page that is displayed, select the maximum memory that can be occupied by the DPC process of the node. The value can be 32 GB, 64 GB, 128 GB, 256 GB, or 512 GB. The default value is 32 GB. The DPC memory quota must be less than or equal to 70% of the remaining physical memory of the node. Set this parameter as required.
- You can click **Uninstall Software** to clear the configurations and data related to the storage software on all nodes. Perform the operations as prompted.
- After the operation is successful, you can click **More** on the right of a node and select **Log Details** to view its operation logs.
- If **Network Management Component Installation** is **Waiting for completion**, the progress of installing network management components on the node is 100%. However, you need to wait until the installation is complete on all nodes and a notification is sent to related components. After the notification is sent to the related components, the installation process ends and the status changes to **Successful**.

----End

6.4.2.6.3 Configuring the Storage Network

This section describes how to configure the storage network for a DPC node and install the DPC node.

Prerequisites

- The storage network of the DPC nodes is properly connected.
- The management network IP addresses of the DPC nodes have been configured.
- The storage network of the DPC node must be able to communicate with the front-end storage network of the storage node.
- Modify the network port configuration file to configure the storage/control network in advance (for details, see **6.4.2.2 Configuring the DPC Node Storage Network IP Address by Modifying the Configuration File**). When the control network is in different network segments, the gateway must be configured. Then, read the existing storage/control network IP address by following the instructions in this section.
- When the storage network is a multi-IP network or the storage network is on different network segments, you need to configure policy-based routes for DPC nodes.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure the storage network for the DPC node by referring to **6.4.2.2 Configuring the DPC Node Storage Network IP Address by Modifying the Configuration File**. If the storage network has been configured, skip this step.

Step 2 Configure the storage network.

1. The **Configure Storage Network** page varies depending on the selected transmission protocol. Configure the storage network as prompted. **Table 6-14** describes related parameters.

   NOTE

   - The values of **Transmission Protocol**, **Network Flow Classification**, **Congestion Control Algorithm**, and **Multiple IP Addresses** must be the same as those of the front-end storage network configured during cluster initialization.
   - The system allocates only the IP addresses that have been configured in the specified IP address range to nodes. The IP addresses of all nodes must be configured in advance.

   Table 6-14 Storage network parameters

Parameter	Description
Shared IP Address on DPC Compute Node	This parameter is mandatory when **Transmission Protocol** is set to **RoCE** and **Multiple IP Addresses** is set to **Yes**. When a DPC compute node has only one front-end storage IP address and you select **Yes**, the control IP address must be the same as the front-end storage IP address. **NOTE** – This parameter is used only when Huawei Cloud Stack Online is connected. – This parameter can be configured only when a DPC compute node is added for the first time. For adding DPC compute nodes subsequently, the value of this parameter will be the same as that configured for the first time and cannot be changed.

2. Click **Add Control IP Address Range** to configure control IP addresses.
   Table 6-15 describes related parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-15 Control IP address configuration

Parameter	Description
IP Address Range	IP address range of the control network. **NOTE** – The control and management networks cannot use the same subnet. The control, front-, and back-end storage networks can use the same (recommended) or different subnets. When using the same subnet, they must use different IP address ranges. – A control network gateway needs to be configured in either of the following scenarios: ■ The control network crosses subnets. ■ The control network does not cross subnets currently but needs to cross subnets due to subsequent capacity expansion.
Subnet Mask/Prefix	Subnet mask or prefix of the control network. **NOTE** When IP addresses of the storage network are IPv4 addresses, enter the subnet mask. When IP addresses of the storage network are IPv6 addresses, enter the prefix.
Gateway	In cross-network segment scenarios, enter the gateway of the actually used control IP addresses. **NOTE** If **Shared IP Address on DPC Compute Node** is set to **Yes**, you do not need to configure the gateway.

NOTE

- You can click **Add Control IP Address Range** to configure multiple control IP address ranges across network segments.
- IP address ranges must contain the IP addresses of all nodes in a cluster.
- The control network needs to be configured only in the RoCE multi-IP scenario.

3. Click **Add Storage IP Address Range** to configure storage IP addresses.

   Table 6-16 describes related parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-16 Storage IP address configuration

Parameter	Description
IP Address Range	IP address range of the storage network. **NOTE** – The start IP address and end IP address of each IP address range must be in the same network segment. – In the multi-IP scenario, the storage network can use the same subnet as the control network, but cannot use the same subnet as the internal management, external management, service, and replication networks. The IP address range of the storage network cannot use the same subnet as the IP addresses of other ports on the nodes. – In non-multi-IP scenarios, the storage network cannot use the same subnet as the internal management, external management, service, and replication networks. The IP address range of the storage network cannot use the same subnet as the IP addresses of other ports on the nodes. IPv4 and IPv6 addresses are supported.
Subnet Mask/Prefix	Subnet mask or prefix of the storage network. **NOTE** When IP addresses of the storage network are IPv4 addresses, enter the subnet mask. When IP addresses of the storage network are IPv6 addresses, enter the prefix.

NOTE

You can click **Add Storage IP Address Range** to configure multiple storage IP address ranges. A maximum of 300 storage IP address ranges can be configured.

IP address ranges must contain the IP addresses of all nodes in a cluster.

4. Click **Preview**.

   The system displays the storage IP address of each node and refreshes the table.

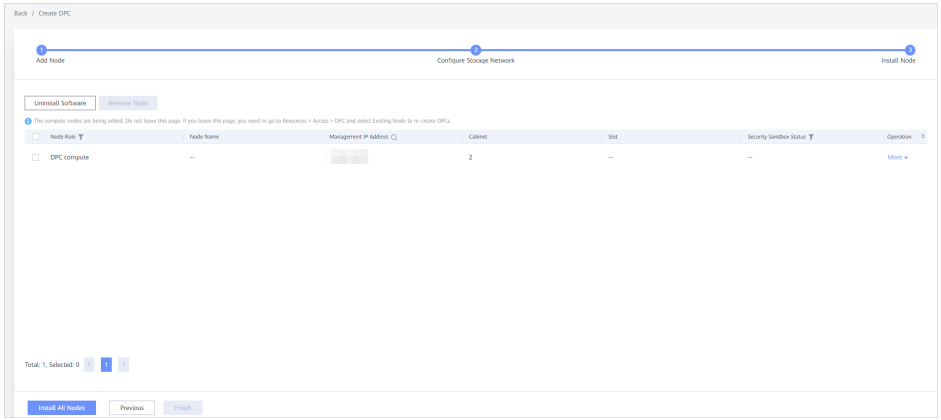
NOTE

- After modifying the network configurations, if you do not click **Preview**, you can click **Reset** to restore to the previous previewed network information.
- You can click **More** on the right of a node and select **Manage Bond Port** to manage bond ports of the node.
- You can select a node to be removed and click **Remove Node** to remove the node and uninstall the storage software on the node. You can also click **More** > **Remove Node** to remove the node. After the node is removed, it is no longer managed by the cluster.
  - Nodes that have not been configured and installed can be directly removed. Perform the operations as prompted.
  - Nodes that have been configured and installed can be removed only after being authenticated. Perform the operations as prompted.

 Copyright © Huawei Technologies Co., Ltd.

5. Click **Submit**.
6. After the storage network is configured successfully, click **Next**.

Step 3 Install nodes.



1. Click **Install**.

   NOTE

   - If the installation fails, you can click **Uninstall Software** to reconfigure the nodes. Perform the operations as prompted.
   - You can select a node to be removed and click **Remove Node** to remove the node and uninstall the storage software on the node. You can also click **More** > **Remove Node** to remove the node. After the node is removed, it is no longer managed by the cluster.
     - Nodes that have not been configured and installed can be directly removed. Perform the operations as prompted.
     - Nodes that have been configured and installed can be removed only after being authenticated. Perform the operations as prompted.
2. Click **Finish**.

Step 4 After the installation is complete, click **Close**.

----End

Related Operations

If the storage network transmission protocol of the DPC node is RoCE, you need to configure flow control for the DPC node. The configuration method is as follows:

Step 1 Log in to a DPC node as user **root**.

Step 2 Run the following command to check flow control parameters and whether the value of **result** is **1**:

```
/opt/fusionstorage/agent/script/check_roce_config.sh
```

- If no, the flow control parameters are correctly configured. No further action is required.
- If yes, the flow control parameters are incorrectly configured. In this case, reconfigure the parameters by referring to **Step 3** to **Step 4**.

Step 3 Run the following command to obtain the flow control parameter settings of the DPC node:

 Copyright © Huawei Technologies Co., Ltd.

```
cat /opt/fusionstorage/agent/conf/network.cfg |grep g_rdma_service_level
```

NOTE

Check the value of **g_rdma_service_level** for subsequent flow control parameter configuration.

Step 4 Run the following command to modify the flow control parameter settings:

```
/opt/fusionstorage/agent/script/RoCE_monitor.sh g_rdma_service_level 0
```

The following is an example:

```
[root@HN00 ~]# /opt/fusionstorage/agent/script/check_roce_config.sh
result=1;value=Pfc enabled level for port(enp129s0f1) is wrong, level 3 is expected.
[root@HN00 ~]# cat /opt/fusionstorage/agent/conf/network.cfg |grep g_rdma_service_level
g_rdma_service_level="3"
[root@HN00 ~]# /opt/fusionstorage/agent/script/RoCE_monitor.sh 3 0
result=0;value=no;
[root@HN00 ~]#
```

----End

6.4.2.7 Performance Tuning

6.4.2.7.1 Scenario 1

Scenario

4 MB **fs blocksize** is recommended for large files in high-bandwidth scenarios.

Prerequisites

When creating or modifying a file system, set **fs blocksize** to the power of 2 and greater than or equal to 4096 bytes, for example, 4096, 8192, or 16384 bytes. Currently, the default size is 1 MB.

Procedure

Step 1 Unmount the mount point.

```
umount DPC mount point
```

NOTE

- No DPC mount point can be unmounted in a container.
- Mount operations cannot be performed in a container.

Step 2 Set **fs blocksize**. The following is an example of setting **fs blocksize** to 4 MB.

```
mount -t dpc -o blocksize=4096 /fsname /directory
```

----End

6.4.2.7.2 Scenario 2

Scenario

DPC provides the NUMA affinity tuning feature. After this feature is enabled on fat compute nodes of the NUMA architecture and works with the service tuning of

 Copyright © Huawei Technologies Co., Ltd.

upper-layer applications, the NUMA hardware performance can be leveraged, further improving the performance of DPC.

- Service tuning suggestions for upper-layer applications in bandwidth-intensive scenarios:
  - Each NUMA of an upper-layer application is bound with a process.
  - Each instance of an upper-layer application independently operates its own directories or files.
- Service tuning suggestions for upper-layer applications in single-stream scenarios:
  - Upper-layer applications are bound to one NUMA.
  - Each instance of an upper-layer application independently operates its own directories and files.

If you need to enable the NUMA function to optimize the DPC performance, you are advised to enable the NUMA function before upper-layer applications deliver services.

Prerequisites

The NUMA affinity tuning feature provided by DPC requires the collaboration with storage nodes. To achieve the optimal performance, both DPC nodes and storage nodes must be of the OceanStor Pacific series 8.1.2 version or later.

Impacts and Constraints

Enabling or disabling the NUMA function causes the DPC process to restart. During the restart, the process cannot carry upper-layer services. If services are still delivered, an error is reported in the service process.

Method 1: Manual Change

NOTE

Perform the following operations on each DPC node.

Step 1 Log in to a DPC node as user **root**.

Step 2 Run the following command to check whether the DPC node uses the NUMA architecture. If the value of **NUMA node(s)** is greater than or equal to 2, the DPC node uses the NUMA architecture. In this case, you can enable the NUMA feature to further improve the performance of DPC.

```
[root@client81 ~]# lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                40
On-line CPU(s) list:   0-39
Thread(s) per core:    1
Core(s) per socket:    20
Socket(s):             2
NUMA node(s):          2
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 85
Model name:            Intel(R) Xeon(R) Gold 6138 CPU @ 2.00GHz
Stepping:              4
```

 Copyright © Huawei Technologies Co., Ltd.

```
CPU MHz:               2000.000
BogoMIPS:              4000.00
Virtualization:        VT-x
L1d cache:             32K
L1i cache:             32K
L2 cache:              1024K
L3 cache:              28160K
NUMA node0 CPU(s):     0-19
NUMA node1 CPU(s):     20-39
```

Step 3 Enable NUMA.

NOTICE

If NUMA is enabled, the DPC process is stopped and then started.

```
/opt/fusionstorage/dpc/script/dpcctl set_param numa_optimize true
```

Step 4 (Optional) If the service performance is not improved after NUMA is enabled, you can disable NUMA on the DPC node.

NOTICE

If NUMA is disabled, the DPC process is stopped and then started.

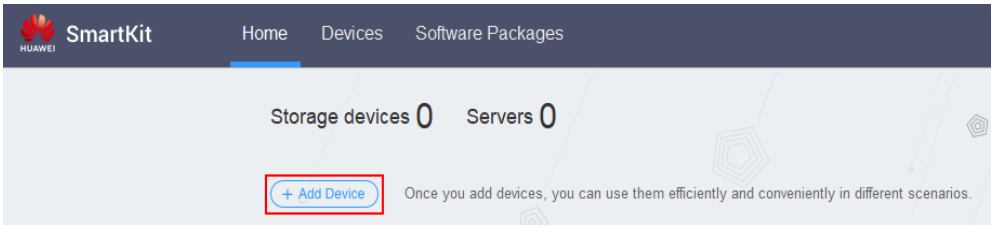
```
/opt/fusionstorage/dpc/script/dpcctl set_param numa_optimize false
```

----End

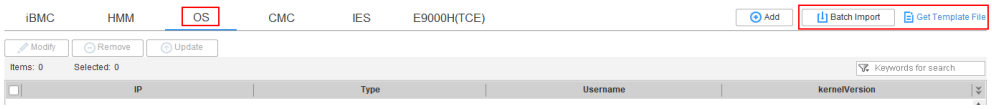
Method 2: Batch Change Using SmartKit

Step 1 If there are a large number of DPC nodes, you can use SmartKit to enable NUMA in batches as follows.

1. On SmartKit, choose **Home** > **Add Device**.



2. Select **OS**, click **Get Template File** to download the template file, and enter related information in the template.



   - Set the start and end IP addresses to the management IP address of the DPC node OS.
   - Set the user name to **fsadmin**. To obtain the password, see section "Account and Password Management" in *OceanStor Pacific Series 8.2.1 Security Configuration Guide*.

 Copyright © Huawei Technologies Co., Ltd.

- To obtain the password of user **root**, see section "Account and Password Management" in *OceanStor Pacific Series 8.2.1 Security Configuration Guide*.

3. Click **Batch Import** to import the template.
4. On the SmartKit home page, choose **Server** > **Upgrade/Patch Installation** > **Batch Distribution**.
5. Click **Device Selection**. On the **OS** tab page, select the device for which the service flow needs to be configured, and click **OK**.
6. Click **Batch Distribution**.
7. Select the device IP address and click **Config Service**.
8. Configure the file transfer service flow. Set **Select Configuration Mode** to **Custom**.
9. Click **Next**, select **Command Execution**, click **Add a Task**, set parameters related to command execution, and click **Save**.

   Table 6-17 describes the parameters.

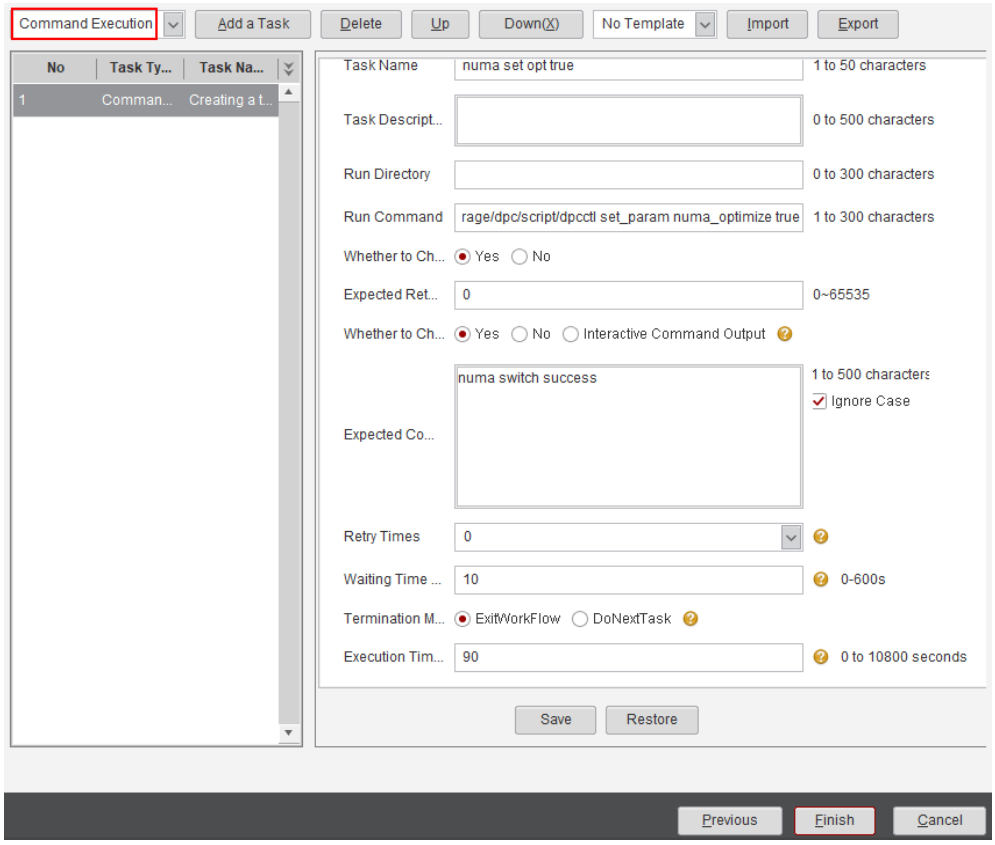


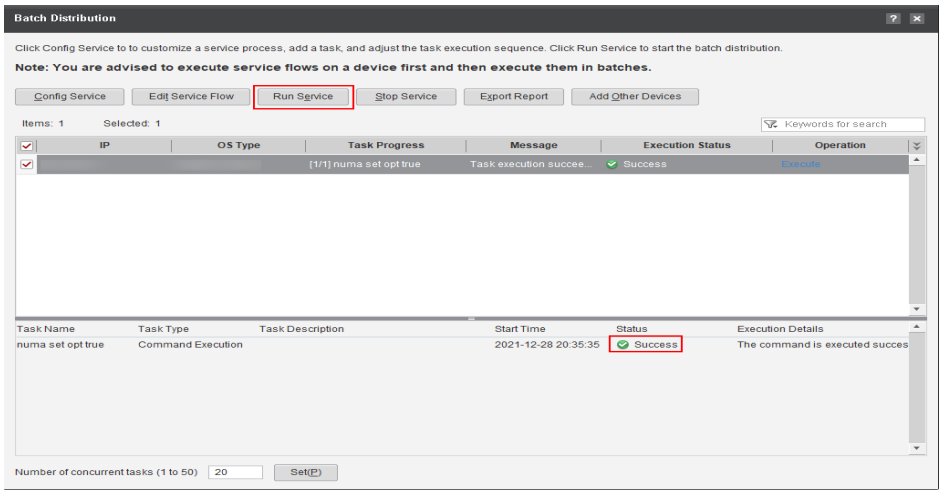
Table 6-17 Command execution parameters

Parameter	Description
Task Name	Enter **numa set opt true**.
Run Command	Enter **/opt/fusionstorage/dpc/script/dpcctl set_param numa_optimize true**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Whether to Check the Return Code	Select **Yes**.
Expected Return Code	Enter **0**.
Whether to Check the Command Output	Select **Yes**.
Expected Command Output	Enter **numa switch success**.
Execution Timeout Interval	90

10. Click **Run Service** and wait until the command execution is complete.
    - If **Success** is displayed, the command is executed successfully and the task is complete.



    - If **Fail** is displayed, contact technical support.
      - For carrier users, log in to **https://support.huawei.com**.
      - For enterprise users, log in to **https://e.huawei.com**.

      After logging in to the preceding website, you can select an area to obtain the technical support contact information of the area.

----End

6.4.2.7.3 Scenario 3

Scenario

DPC provides the eventual consistency mode. In this mode, distributed lock operations on files are not required, and file data and metadata can be protected using timeout, further improving DPC performance. In scenarios with a large number of small files (such as AI scenarios), the read and write performance can be significantly improved.

 Copyright © Huawei Technologies Co., Ltd.

Impacts and Constraints

1. The eventual consistency mode provided by DPC requires the collaboration with storage nodes. To achieve the optimal performance, both DPC nodes and storage nodes must be of the OceanStor Pacific series 8.2.0 version or later.
2. In eventual consistency mode, the cache policy is the same as that of the standard NFS protocol.
3. The same file system on a single client must be mounted using the same consistency mode and timeout.

Procedure

Step 1 Unmount the mount point.

umount *DPC mount point*

NOTE

- No DPC mount point can be unmounted in a container.
- Mount operations cannot be performed in a container.

Step 2 Use the eventual consistency mode for mounting.

mount -t dpc -o eventual */fsname /localdirectory*

NOTE

- **-o eventual** indicates the eventual consistency mode.
- *fsname* indicates the name of the namespace to be shared.
- *localdirectory* indicates the local mounting directory of a DPC node.

----End

6.4.2.7.4 Scenario 4

Scenario

If services running on DPC require higher performance, you can set a CPU to work in performance mode.

Impacts and Constraints

Perform the following operations on each DPC node.

Procedure

Step 1 Check whether the current CPU works in performance mode.

Log in to a DPC node as user **root** and run the **cpupower frequency-info** command. If the command output contains **performance**, the performance mode has been enabled and you do not need to enable it again.

```
[root@arm182 ~]# cpupower frequency-info
analyzing CPU 0:
  driver: cppc_cpufreq
  CPUs which run at the same hardware frequency: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
22 23
  CPUs which need to have their frequency coordinated by software: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
16 17 18 19 20 21 22 23
```

 Copyright © Huawei Technologies Co., Ltd.

```
maximum transition latency:  Cannot determine or is not supported.
hardware limits: 200 MHz - 2.60 GHz
available cpufreq governors: conservative ondemand userspace powersave performance schedutil
current policy: frequency should be within 200 MHz and 2.60 GHz.
                The governor "performance" may decide which speed to use
                within this range.
current CPU frequency: 2.60 GHz (asserted by call to hardware)
```

Step 2 Enable the CPU performance mode.

Method 1: enabling the CPU performance mode by running a CLI command

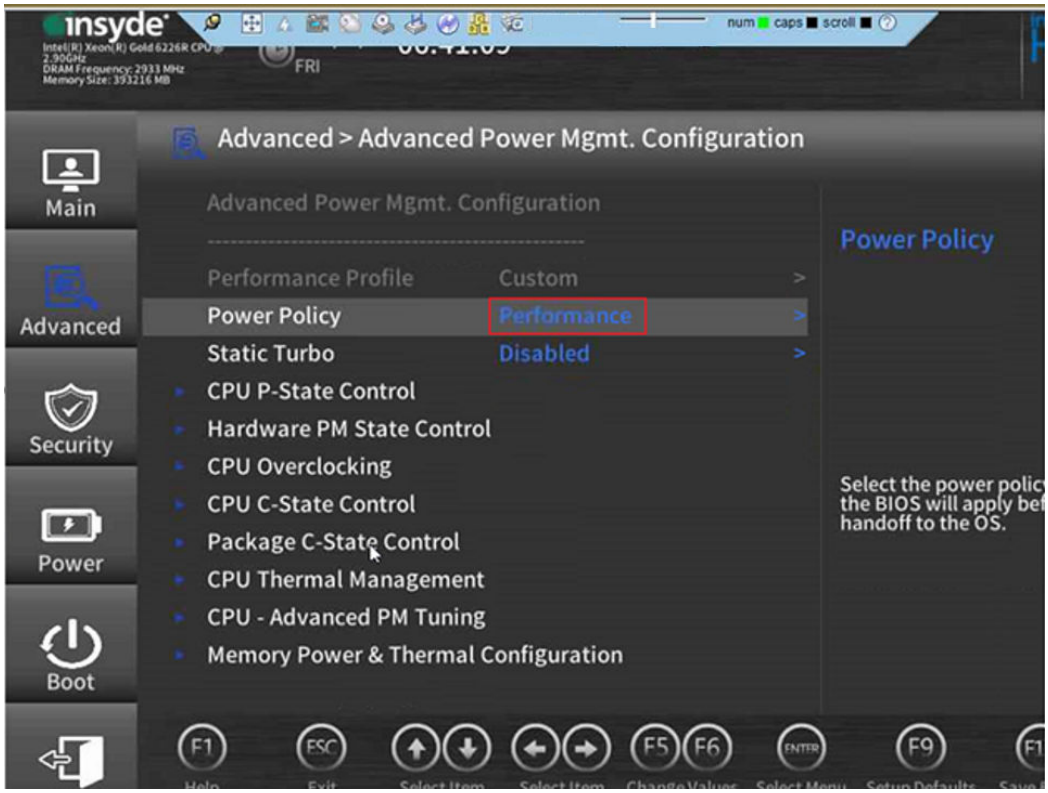
1. Run the following command to enable the CPU performance mode.

```
[root@arm182 ~]# cpupower frequency-set -g performance
Setting cpu: 0
Setting cpu: 1
Setting cpu: 2
Setting cpu: 3
Setting cpu: 4
Setting cpu: 5
```

2. Check whether the mode is successfully enabled by referring to **Step 1**.

Method 2: enabling the CPU performance mode by setting BIOS

1. Take Intel(R) Xeon(R) Gold 6226R CPU @ 2.90GHz as an example. On the **Advanced** page, set **Power Policy** to **Performance**.



----End

6.4.2.8 Using SmartKit to Perform Deployment Inspection

After hardware installation, software installation, and subsequent service configuration are complete, use SmartKit on the maintenance terminal to check the status of the storage cluster and the version mapping of storage nodes.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The management IP address, user name, and password for logging in to the storage device have been obtained.

Context

The GUI may vary with the version.

Procedure

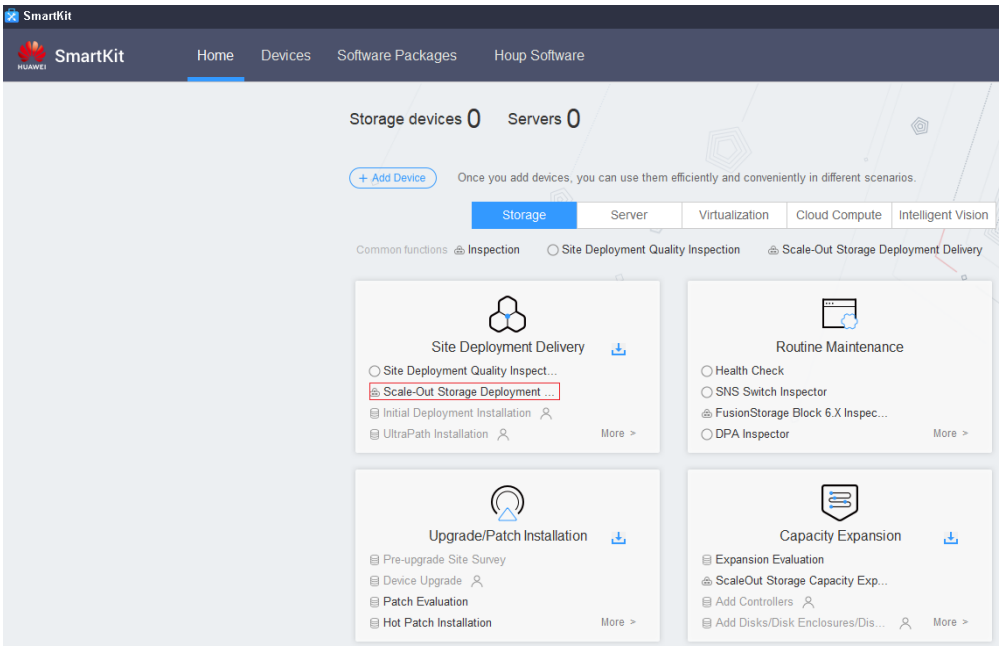
Step 1 Prepare SmartKit. If it has been installed, skip this step.

1. Download and install SmartKit.
   - For enterprise users: Log in to **https://support.huawei.com/enterprise**, enter **SmartKit** in the search box, and select **Distributed Storage > Tools and Platform > SmartKit** from the suggested paths. The SmartKit page is displayed.
     i. On the SmartKit page, click **Software Download**, and select and download SmartKit of the latest version according to the publication date.
     ii. On the SmartKit page, click **Documentation**, find the user guide of the corresponding version, and install and run SmartKit respectively by following the instructions provided in sections "Installing SmartKit" and "Running SmartKit".
   - For carrier users: Log in to **https://support.huawei.com**, enter **SmartKit** in the search box, and select **Carrier IT > Data Storage > Storage Common > SmartKit** from the suggested paths. The SmartKit page is displayed.
     i. On the SmartKit page, click **Software**, and select and download SmartKit of the latest version according to the publication date.
     ii. On the SmartKit page, click **Product Documentation**, find the user guide of the corresponding version, and install and run SmartKit respectively by following the instructions provided in sections "Installing SmartKit" and "Running SmartKit".
2. Install the Scale-Out Storage Deployment Delivery tool by referring to section "Installing Functions" in the SmartKit user guide.

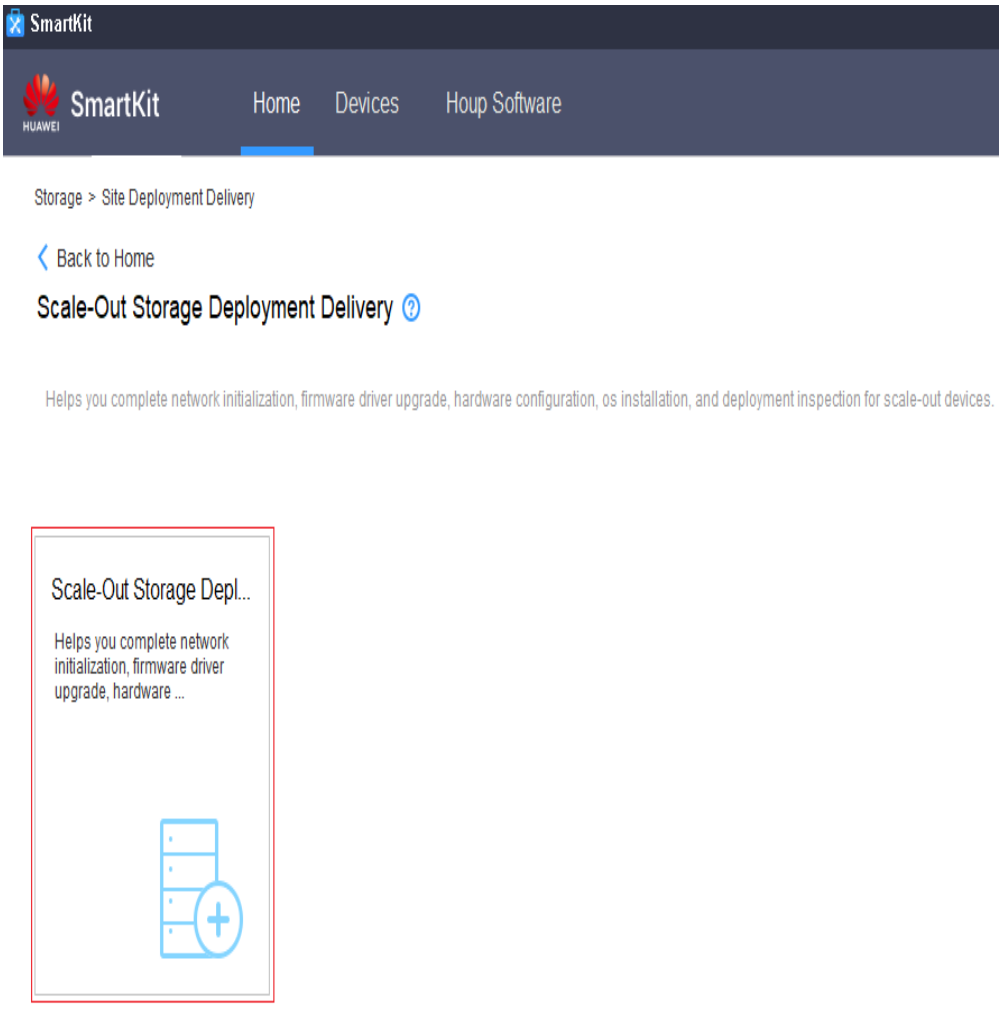
Step 2 Go to the **Site Deployment Delivery** page.

1. On the home page of SmartKit, choose **Site Deployment Delivery** > **Scale-Out Storage Deployment Delivery**. The **Scale-Out Storage Deployment Delivery** page is displayed.

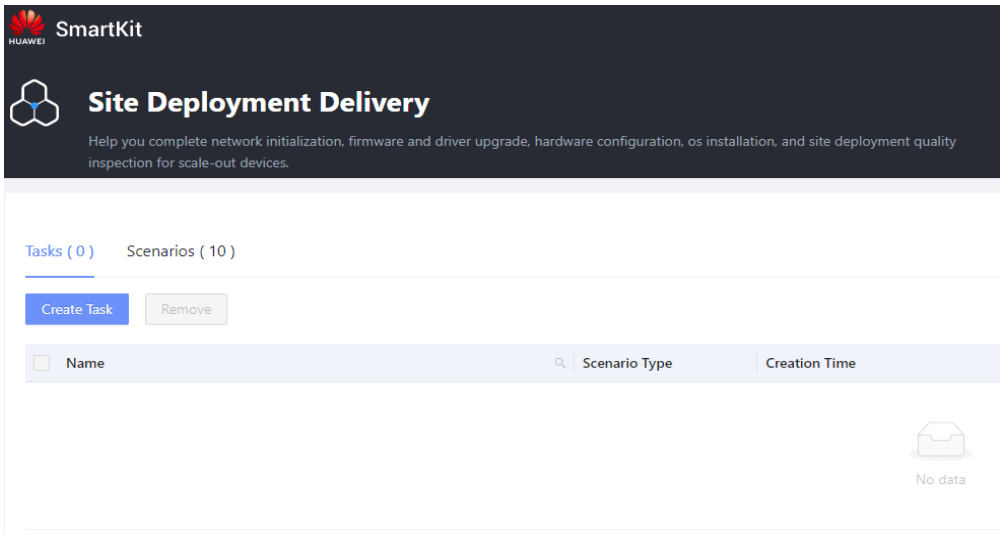
 Copyright © Huawei Technologies Co., Ltd.



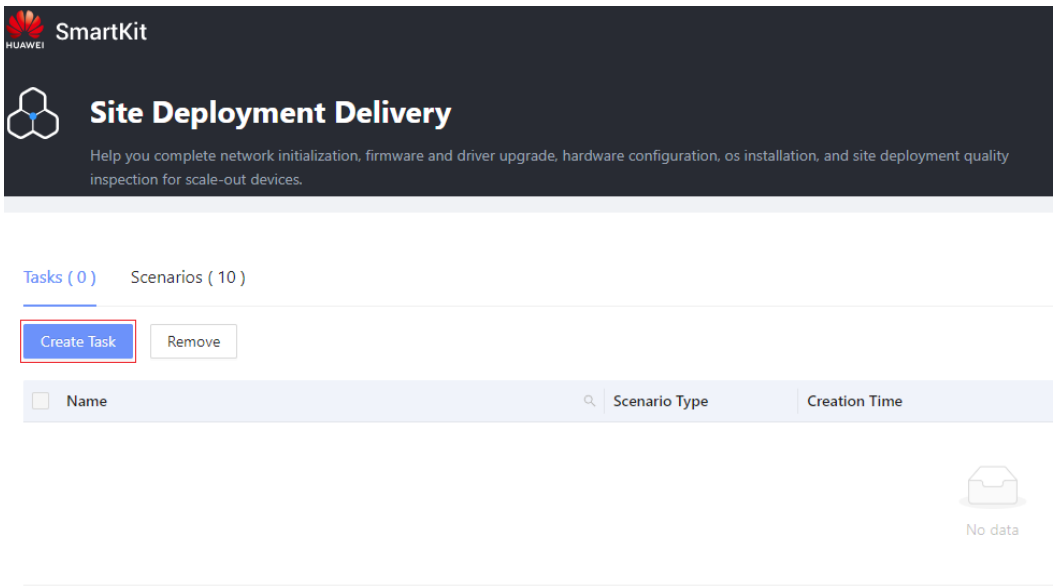
2. On the **Scale-Out Storage Deployment Delivery** page, click **Scale-Out Storage Deployment Delivery**. The **Site Deployment Delivery** page is displayed.



 Copyright © Huawei Technologies Co., Ltd.



Step 3 Click **New**. The **Select Scenario** page is displayed.



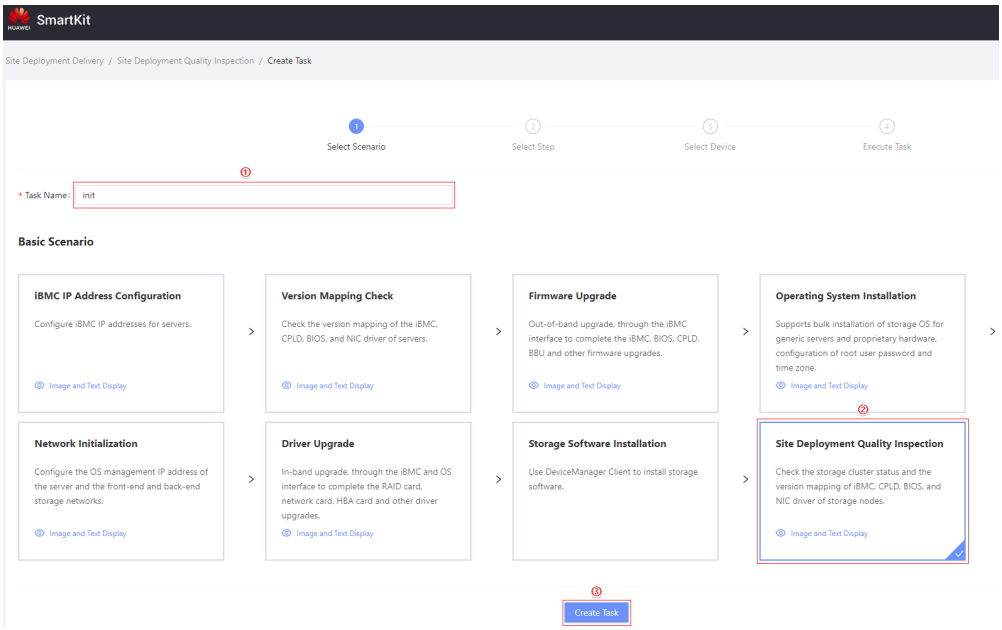
Step 4 Select a scenario.

1. Set **Task Name**, select **Site Deployment Quality Inspection**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).

 Copyright © Huawei Technologies Co., Ltd.

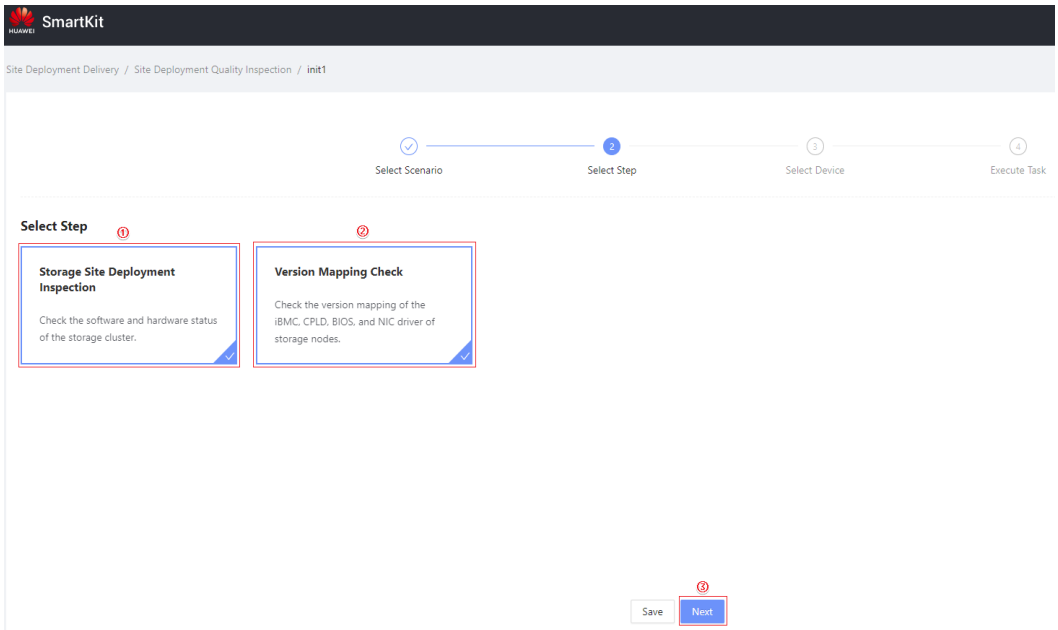


2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

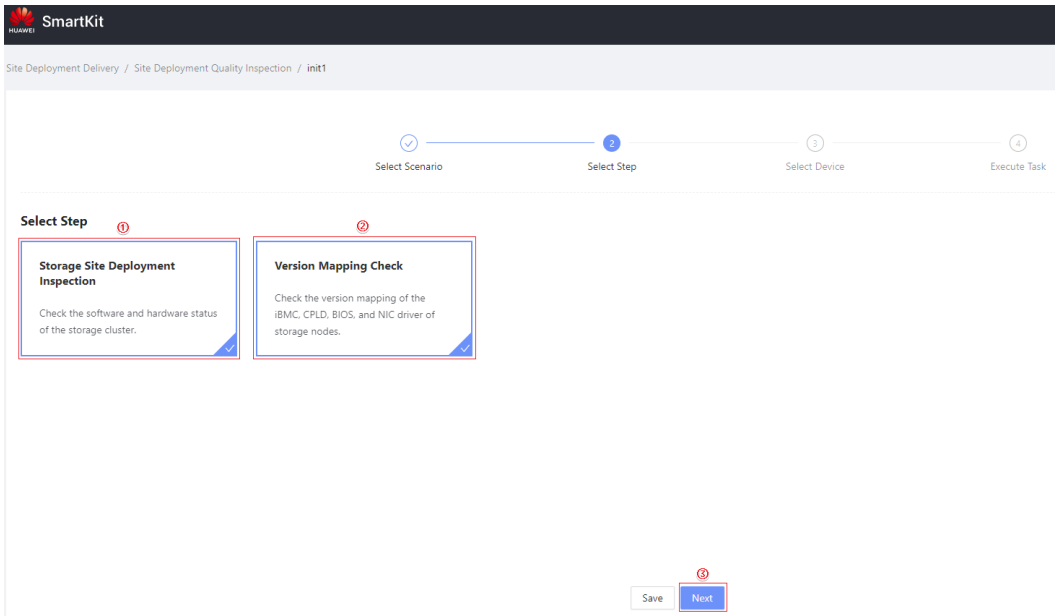
   NOTE

   If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

Step 5 Select **Storage Site Deployment Inspection** and **Version Mapping Check**, and click **Next**.

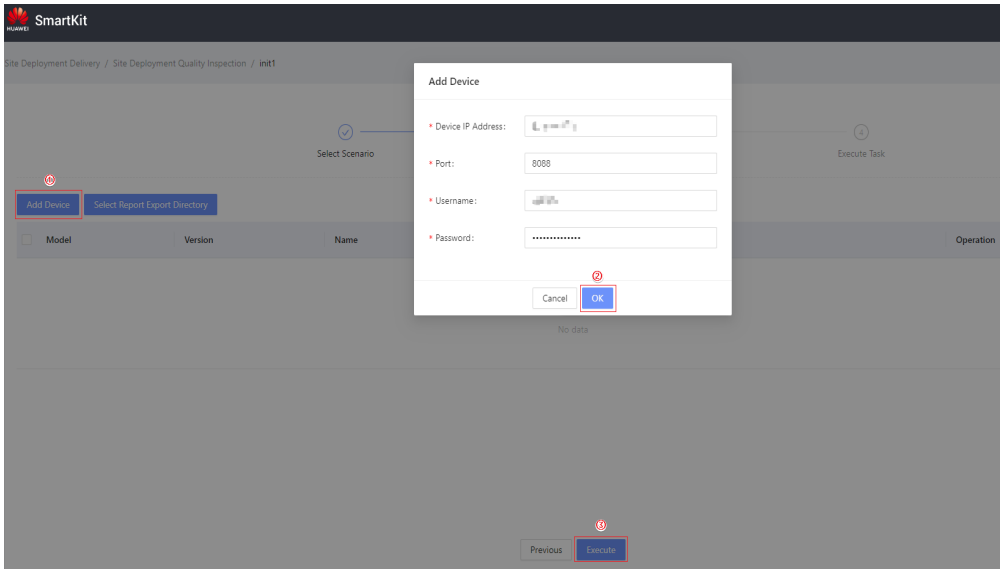


 Copyright © Huawei Technologies Co., Ltd.



Step 6 Select a device.

1. Add a device.



a. Click **Add Device**. The **Add Device** dialog box is displayed.

b. Enter device information as prompted and click **OK**.

Table 6-18 Device information

Name	Description
Device IP Address	DeviceManager management IP address
Port	Port of DeviceManager. Use default port **8088**.
Username	DeviceManager login account

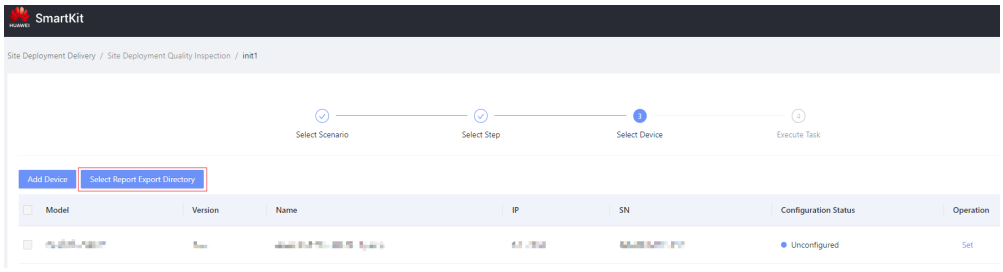
 Copyright © Huawei Technologies Co., Ltd.

Name	Description
Password	Password for logging in to DeviceManager

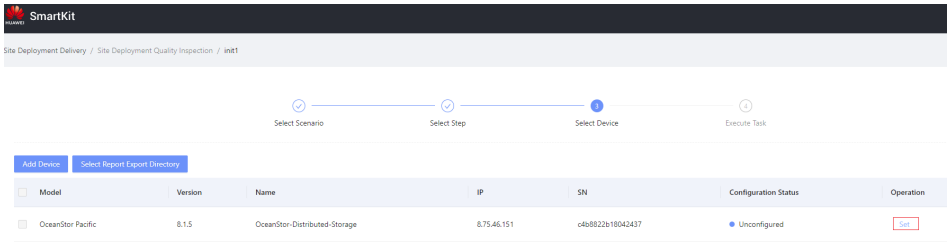
NOTE

If the device has been added, it is displayed in the list by default. You do not need to add it again.

2. Click **Select Report Export Directory** and specify a save path for the report.

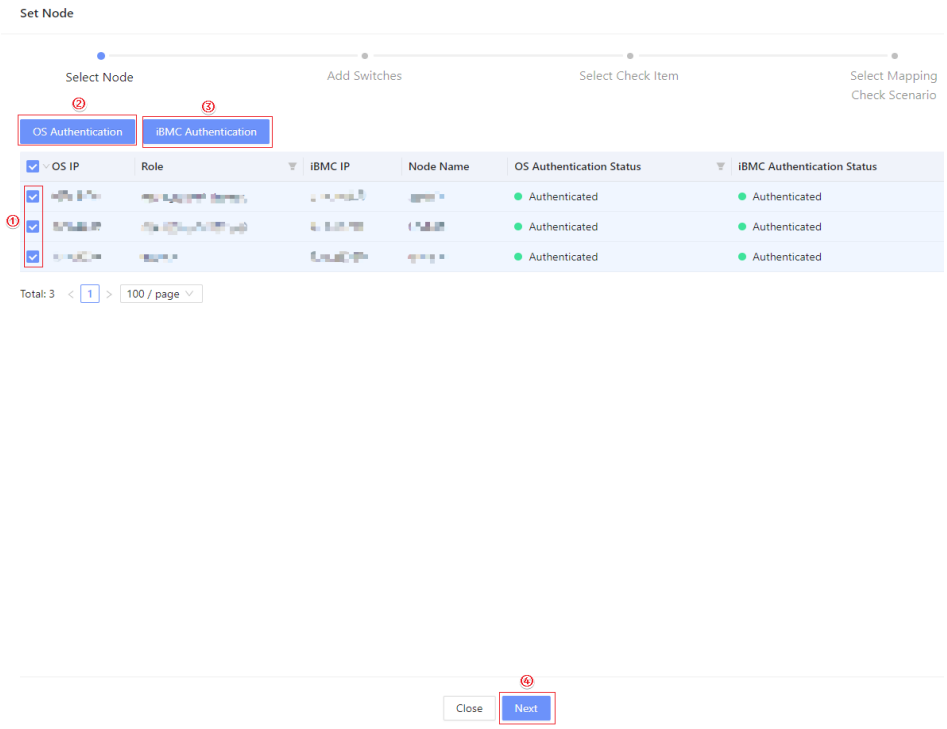


3. Set a check policy.
   a. Click **Set** in the **Operation** column of a device. The **Set Node** page is displayed.



   b. Select a node and authenticate it.

 Copyright © Huawei Technologies Co., Ltd.



i. Select the nodes to be checked.

ii. Click **OS Authentication** and enter related information as prompted to complete the authentication.

iii. Click **iBMC Authentication** and enter related information as prompted to complete the authentication.

iv. Click **Next**. The **Add Switches** page is displayed.

c. (Optional) Add switches.

NOTE

This step applies only to access switches whose storage network uses RoCE networking. In other scenarios, click **Skipped** to skip this step.

i. Click **Add Switch** and enter information about all storage switches.

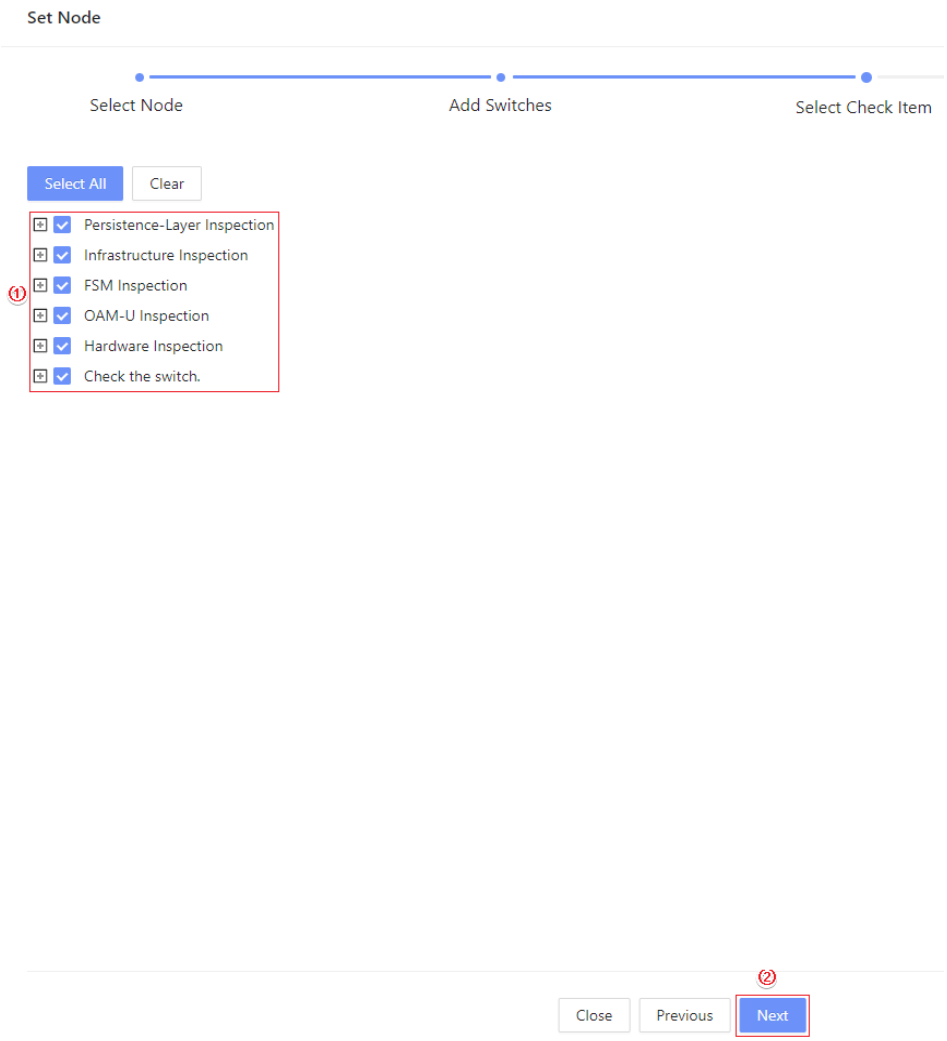
NOTE

You can also click **Download Template** to download the switch information template, enter login information, and click **Batch Import**.

ii. Click **Next**. The **Select Check Item** page is displayed.

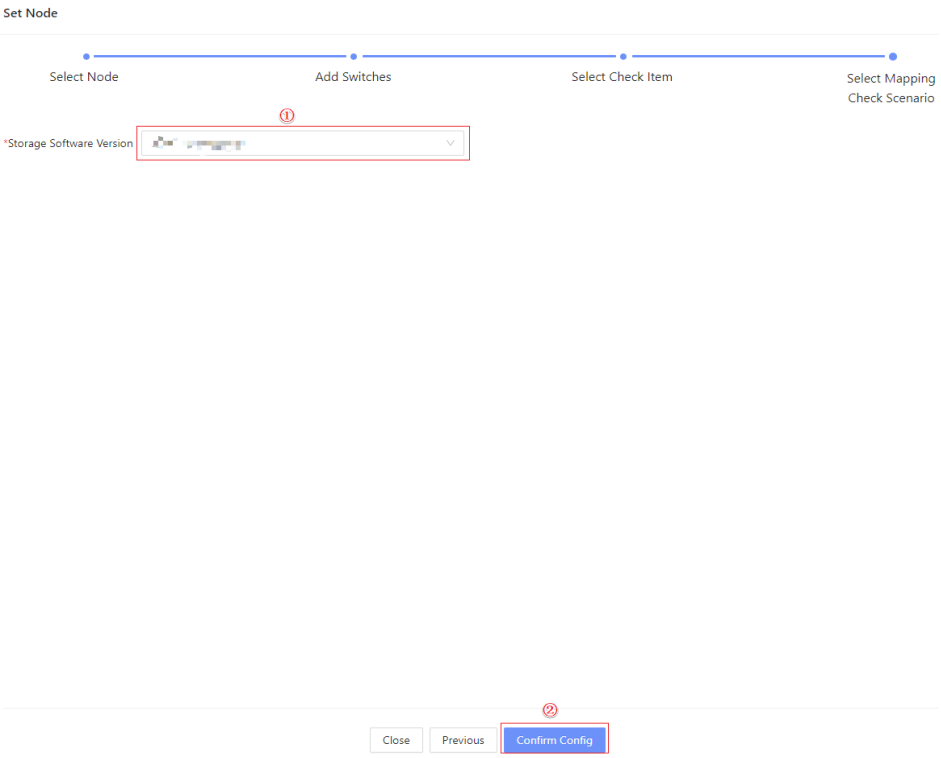
d. Select the items to be checked and click **Next**. The **Select Mapping Check Scenario** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



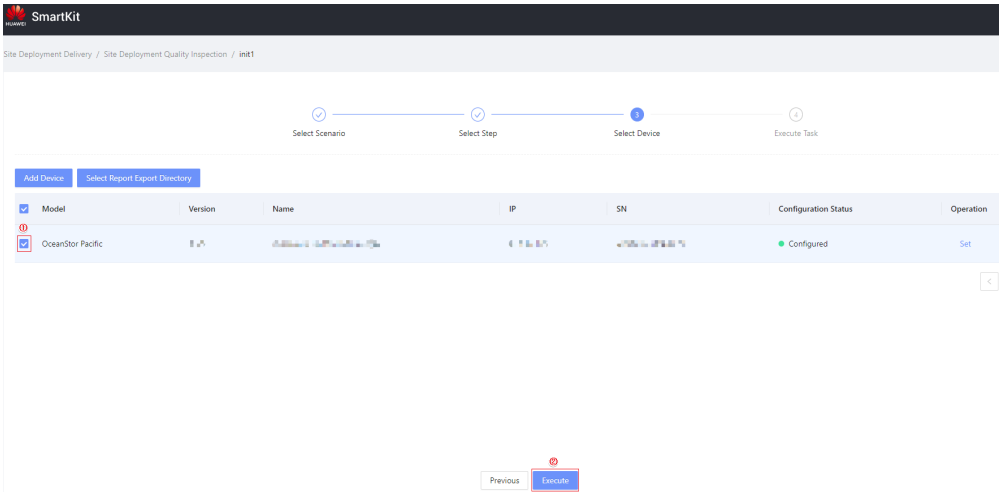
e. Select a storage software version and click **Confirm Config**.

 Copyright © Huawei Technologies Co., Ltd.



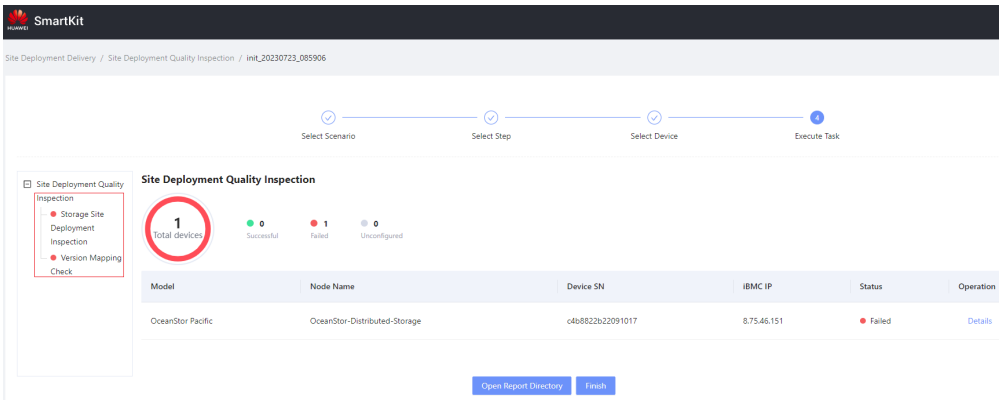
Step 7 Execute the task.

1. Select a device, click **Execute**, and enter the information about the inspection report personnel as prompted.



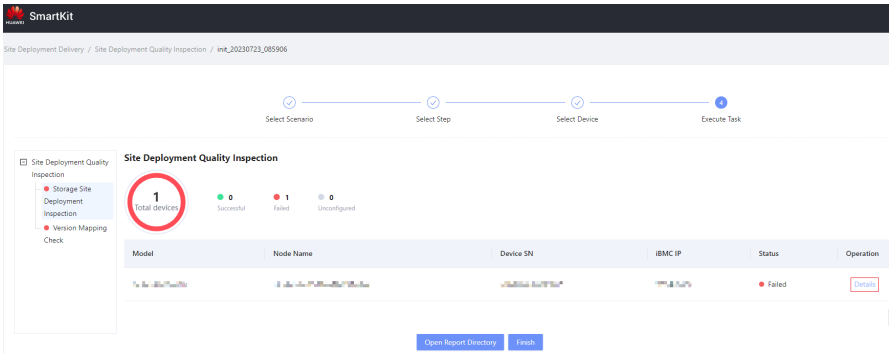
2. After the task is complete, check whether the **Storage Site Deployment Inspection** and **Version Mapping Check** items pass the check (marked in green).

 Copyright © Huawei Technologies Co., Ltd.



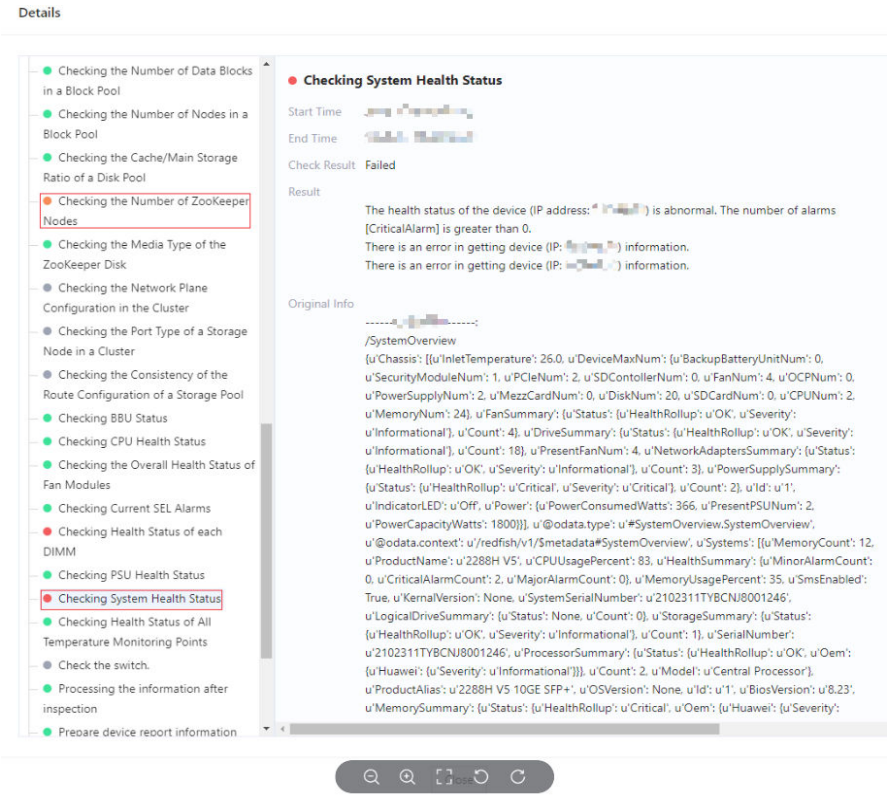
- If yes, click **Finish**.
- If no, perform the following steps for the two check items (after the troubleshooting is complete, click **Finish**):

  i. Click **Details** in the **Operation** column of the corresponding device.



  ii. Click the check items that fail to pass the check (marked in red) and the check items that need to be optimized (marked in orange) in sequence, and handle the problems according to the description in **Result**. The following uses **Storage Site Deployment Inspection** as an example:

 Copyright © Huawei Technologies Co., Ltd.



----End

6.4.2.9 Appendix

6.4.2.9.1 Configuring a Static Route

6.4.2.9.1.1 Configuring a Static Route for a Physical Port

This section describes how to configure static route information for a physical port.

Procedure

Step 1 Select one or more desired ports and click **Configure Static Route**.

The **Configure Static Route** page is displayed.

NOTE

You can also click **More** on the right of a desired port and select **Manage Static Route**. On the **Manage Static Route** page that is displayed, click **Add** to configure a static route.

Step 2 Configure static route information for the physical port.

- Selecting **New** in **Configuration Mode**
  a. Set the parameters listed in **Table 6-19**.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-19 Route parameters

Parameter	Description
Destination IP Address	IP address or network segment of the target node network port connected to the physical port.
Subnet Mask/ Prefix	Subnet mask or prefix of the network segment where the target node network port connected to the physical port resides.
Gateway	Gateway where the local physical port's IP address resides.

b. (Optional) Click **Add** to add another static route.

- Selecting **Copy from** in **Configuration Mode**

a. In **Node**, click **Choose** to select a node.

b. In **Port**, click **Choose** to select a port.

c. In the **Available Static Routes** list, select one or more required static routes.

d. (Optional) Click **More** on the right of a desired route and select **Modify** to modify it.

NOTE

This operation does not change the route information of the source node.

Step 3 Click **OK**.

----End

6.4.2.9.1.2 Configuring a Static Route for a Bond Port

This section describes how to configure static route information for a bond port.

Procedure

Step 1 Select one or more desired ports and click **Configure Static Route**.

The **Configure Static Route** page is displayed.

NOTE

You can also click **More** on the right of a desired port and select **Manage Static Route**. On the **Manage Static Route** page that is displayed, click **Add** to configure a static route.

Step 2 Configure the static route information for a bond port.

- Selecting **New** in **Configuration Mode**

a. Set the parameters listed in **Table 6-20**.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-20 Route parameters

Parameter	Description
Destination IP Address	IP address or network segment of the target node network port connected to the bond port.
Subnet Mask/ Prefix	Subnet mask or prefix of the network segment where the target node network port connected to the bond port resides.
Gateway	Gateway where the local bond port's IP address resides.

b. (Optional) Click **Add** to add another static route.

- Selecting **Copy from** in **Configuration Mode**

a. In **Node**, click **Choose** to select a node.

b. In **Port**, click **Choose** to select a port.

c. In the **Available Static Routes** list, select one or more required static routes.

d. (Optional) Click **More** on the right of a desired route and select **Modify** to modify it.

NOTE

This operation does not change the route information of the source node.

Step 3 Click **OK**.

----End

6.4.2.9.1.3 Configuring a Static Route for a VLAN Port

This section describes how to configure a static route for a VLAN port.

Procedure

Step 1 Select one or more desired VLAN ports and click **Configure Static Route**.

The **Configure Static Route** page is displayed.

NOTE

You can also click **More** on the right of a desired VLAN port and select **Manage Static Route**. On the **Manage Static Route** page that is displayed, click **Add** to configure a static route.

Step 2 Configure the static route information for a VLAN port.

- Selecting **New** in **Configuration Mode**

a. Set the parameters listed in **Table 6-21**.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-21 Route parameters

Parameter	Description
Destination IP Address	IP address or network segment of the target node network port connected to the VLAN port.
Subnet Mask/ Prefix	Subnet mask or prefix of the target network segment where the node network port connected to the VLAN port resides.
Gateway	Gateway where the local VLAN port's IP address resides.

b. (Optional) Click **Add** to add another static route.

- Selecting **Copy from** in **Configuration Mode**
  a. In **Node**, click **Choose** to select a node.
  b. In **Port**, click **Choose** to select a port.
  c. In the **Available Static Routes** list, select one or more required static routes.
  d. (Optional) Click **More** on the right of a desired route and select **Modify** to modify it.

  NOTE

  This operation does not change the route information of the source node.

Step 3 Click **OK**.

----End

6.4.2.9.2 Importing the OS Certificate of a DPC Node

Context

The OS installed on a DPC node supports two boot modes: Legacy BIOS and UEFI. In UEFI boot mode, the Secure Boot function is added to improve OS security. If this function is enabled and the signature of the kernel module is not imported when the kernel module is loaded, the loading will fail.

For compute nodes that support Secure Boot, perform the following operations to import the certificate of Huawei storage software package **OceanStor-Pacific_8.2.1RC1.tar.gz**.

Prerequisites

Before importing a certificate, ensure that the **mokutil** command is available.

Procedure

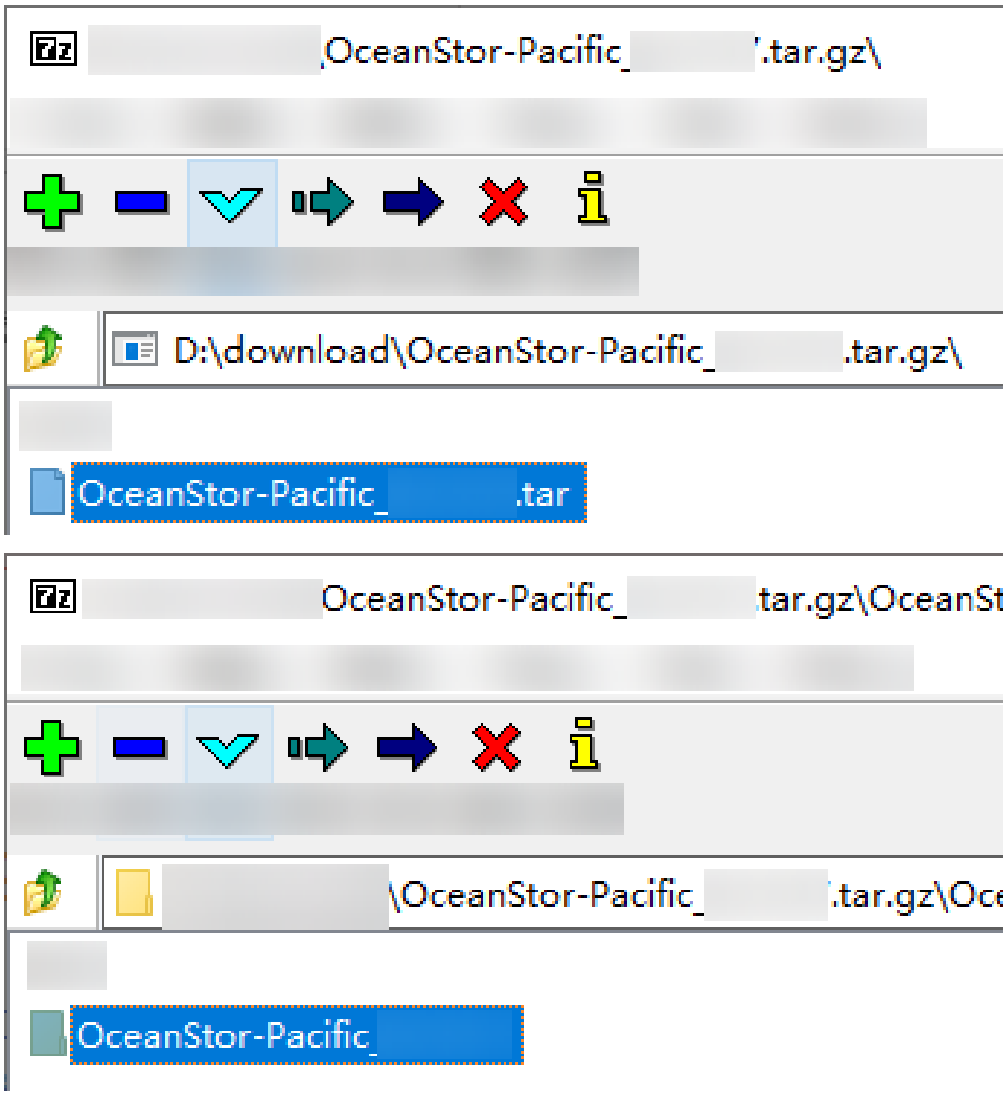
Step 1 Obtain the certificate file from the OceanStor Pacific series storage software package downloaded from the Huawei support website.

 Copyright © Huawei Technologies Co., Ltd.

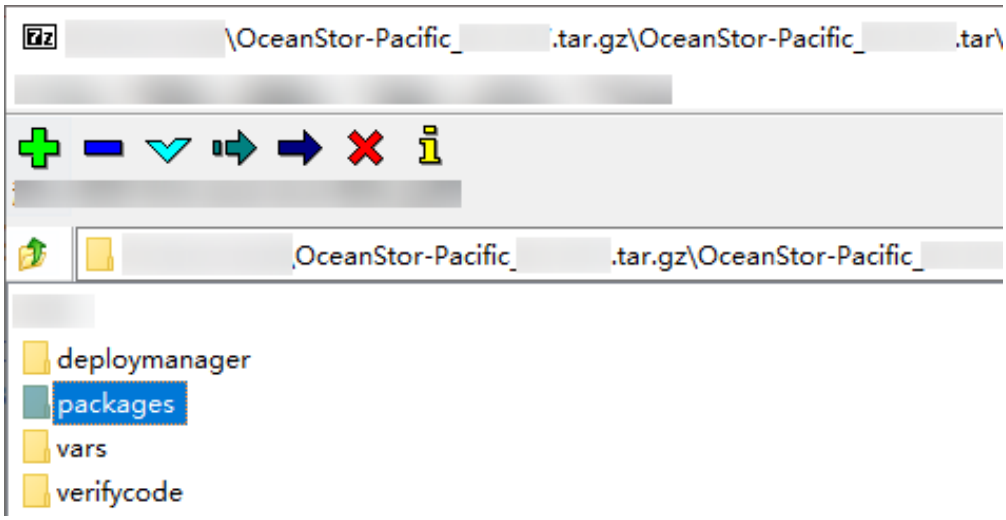
NOTE

For enterprise users, log in to **https://support.huawei.com/enterprise**. For carrier users, log in to **https://support.huawei.com**. In the search box, enter **OceanStor Pacific** and click the suggested path to enter the corresponding product page. For enterprise users, click **Software Download**. For carrier users, click **Software**. Search for and download the software package of the desired version.

1. Use the decompression tool to open the **OceanStor-Pacific_8.2.1RC1.tar.gz** storage software package and then the **OceanStor-Pacific_8.2.1RC1.tar** package, and go to the **OceanStor-Pacific_8.2.1RC1** > **packages** directory.



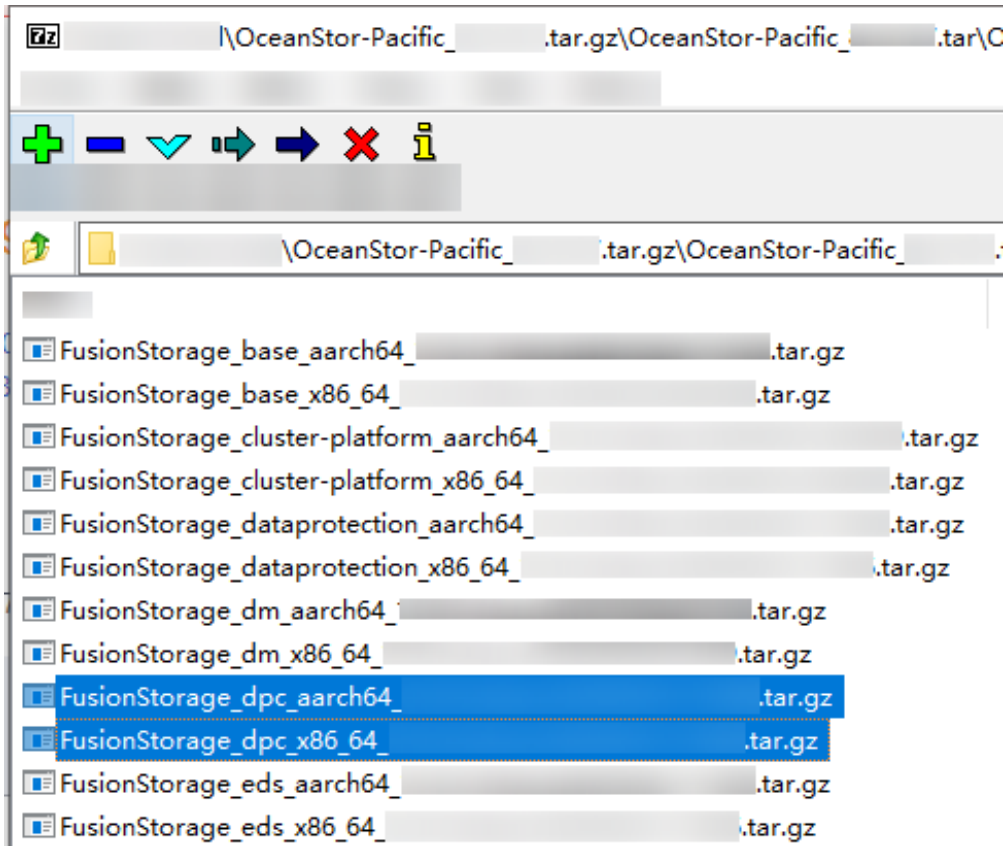
 Copyright © Huawei Technologies Co., Ltd.



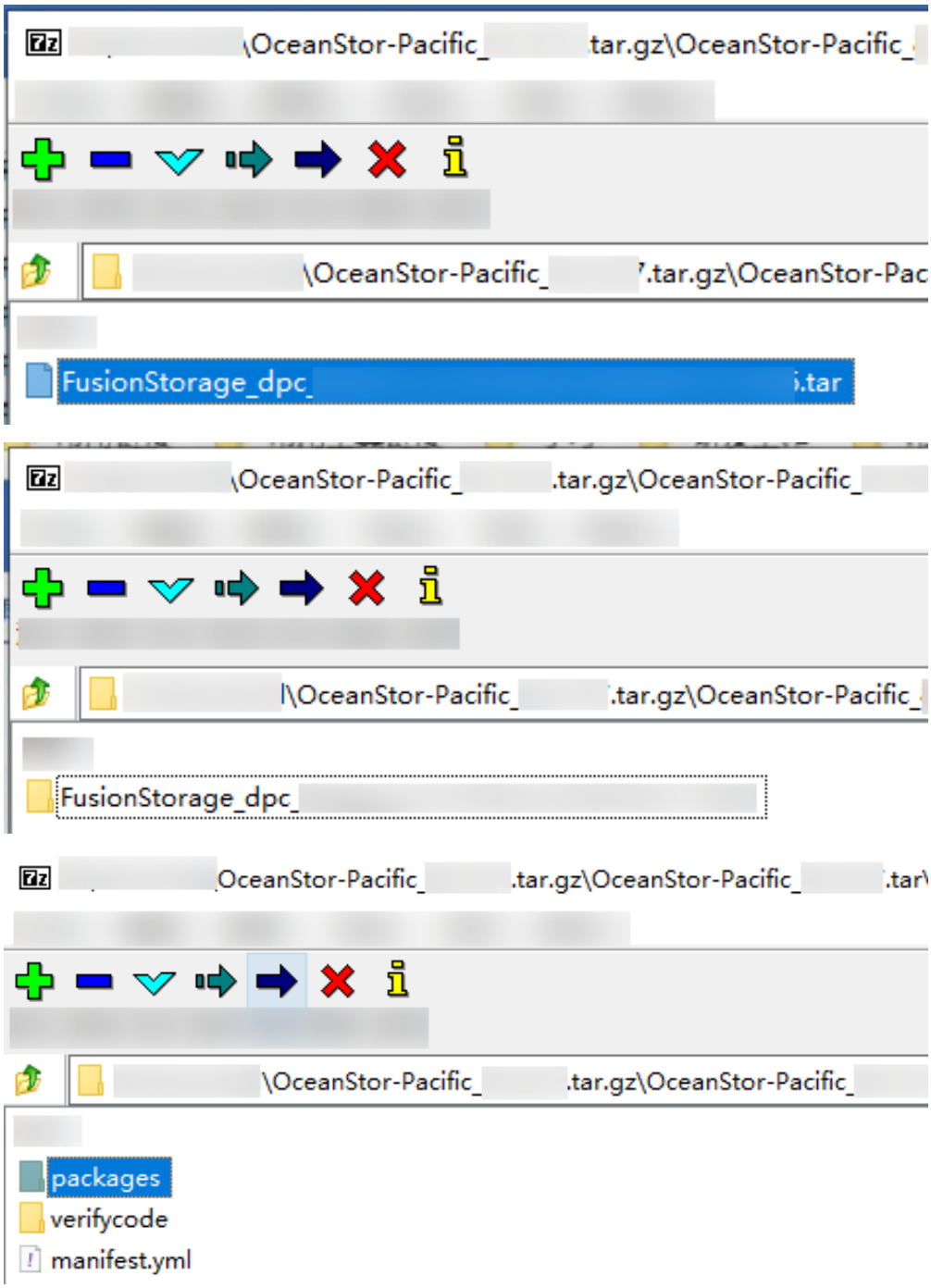
2. Open the **FusionStorage_dpc**_*xxx.xxx*.**tar.gz** package and then the **FusionStorage_dpc**_*xxx.xxx*.**tar** package, and go to the **FusionStorage_dpc**_*xxx.xxx* > **packages** directory.

   NOTE

   - For an x86-based node, open the **FusionStorage_dpc_x86_64.***xxx*.**tar.gz** package.
   - For an Arm-based node, open the **FusionStorage_dpc_aarch64.***xxx*.**tar.gz** package.

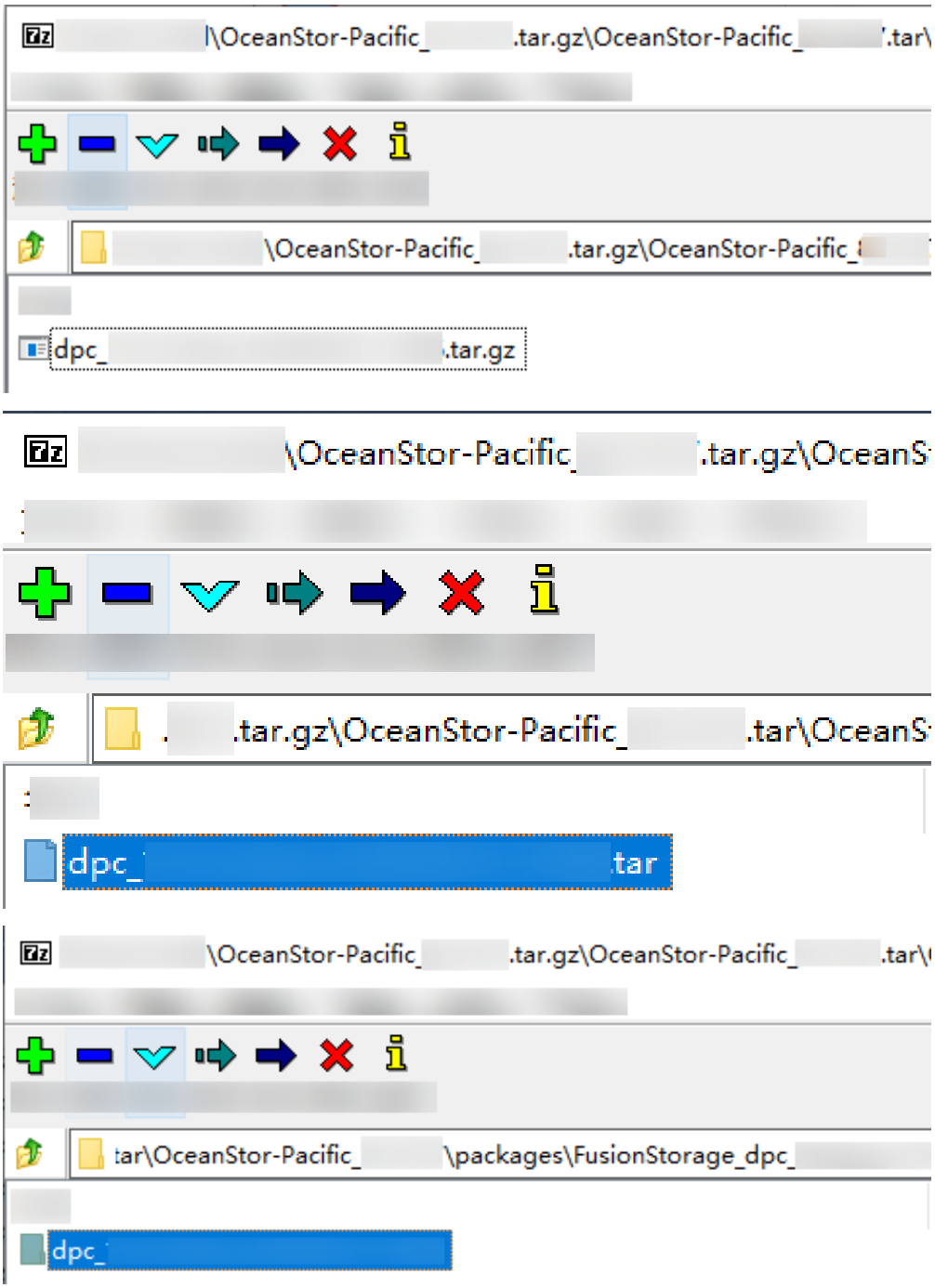


 Copyright © Huawei Technologies Co., Ltd.

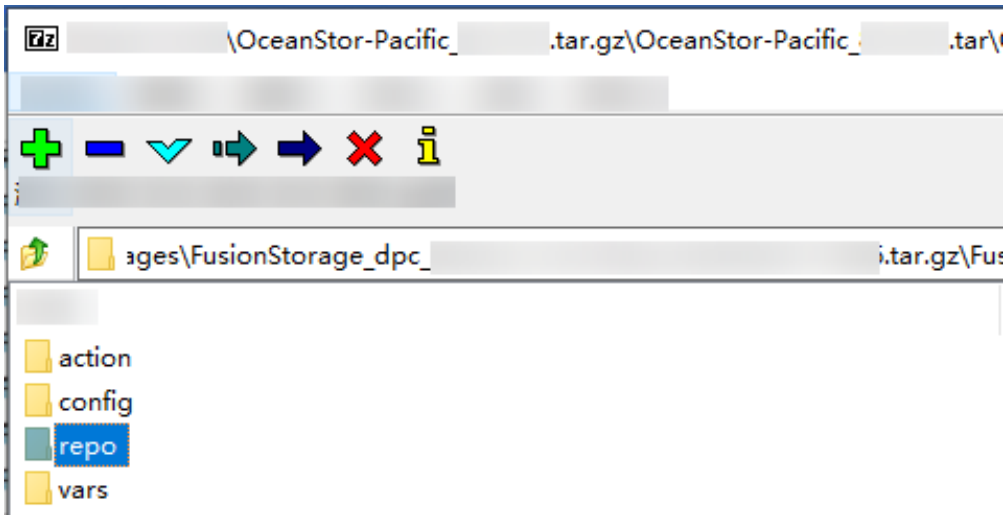


3. Open the **dpc**_*xxx*.**tar.gz** package and then the **dpc**_*xxx*.**tar** package, and go to the **dpc**_*xxx* > **repo** directory.

 Copyright © Huawei Technologies Co., Ltd.



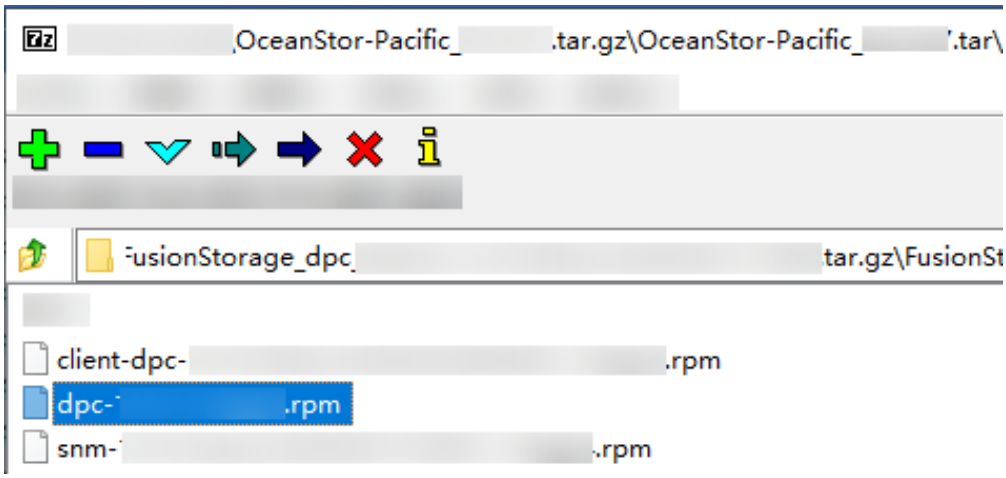
 Copyright © Huawei Technologies Co., Ltd.

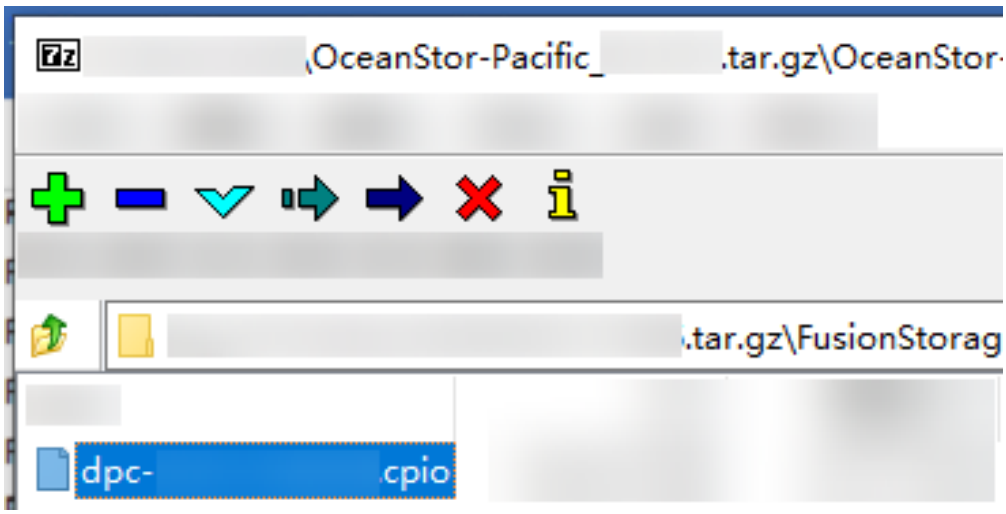


4. Open the **dpc-*xxx*.rpm** package and then the **dpc-*xxx*.cpio** package.

   NOTE

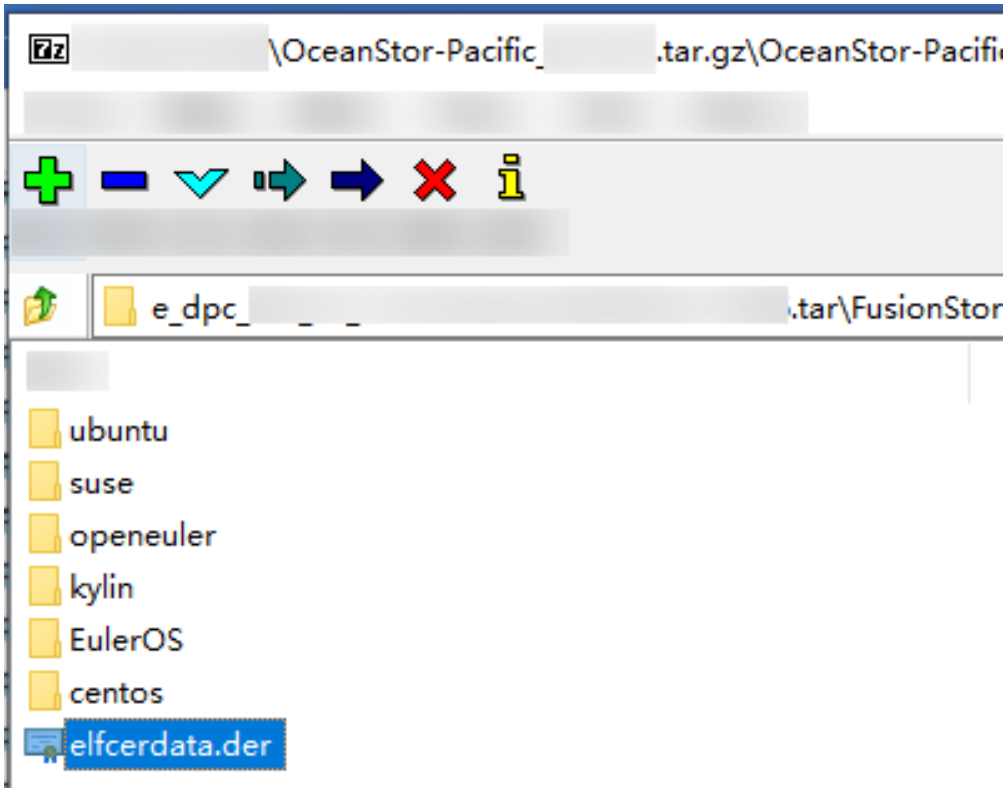
   - For an x86-based node, open the **dpc-*xxx*.x86_64.rpm** and **dpc-*xxx*.x86_64.cpio** packages.
   - For an Arm-based node, open the **dpc-*xxx*.aarch64.rpm** and **dpc-*xxx*.aarch64.cpio** packages.





 Copyright © Huawei Technologies Co., Ltd.

5. Go to the **opt** > **fusionstorage** > **dpc** > **ko** directory in sequence, and locate the **elfcerdata.der** certificate file.



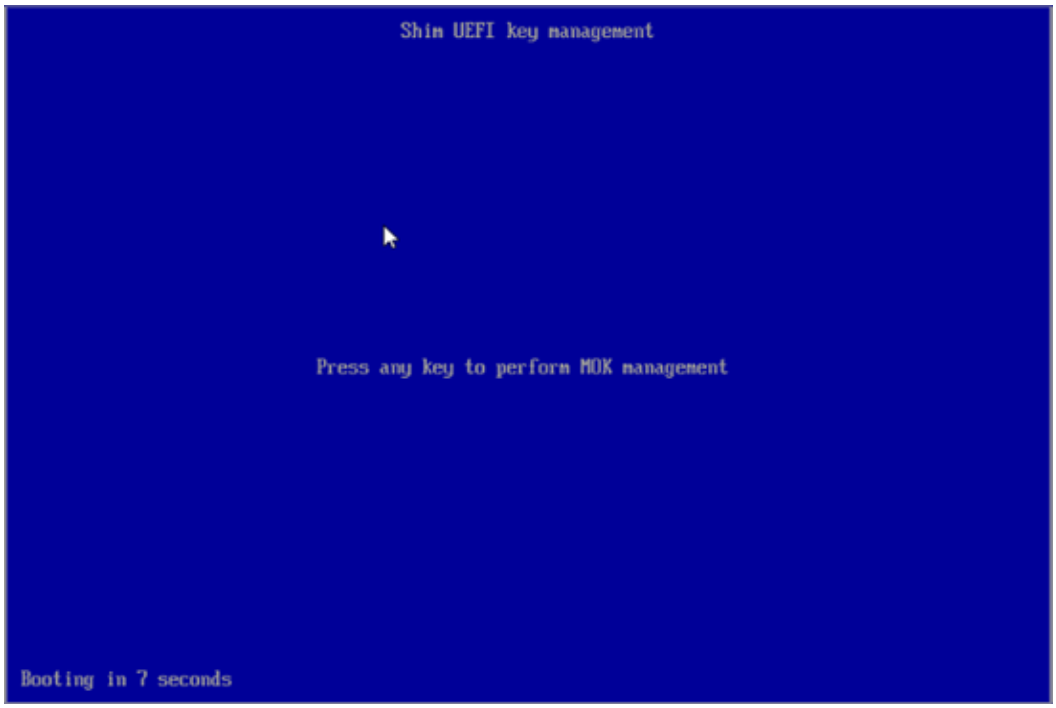
Step 2 Upload the certificate file to the **/tmp** directory on each compute node.

Step 3 Run the **mokutil --import /tmp/elfcerdata.der** command as user **root** to import the certificate. You will be prompted to set a password, which will be used in subsequent steps. You can set a password as required. Then run the **reboot** command to restart the node.

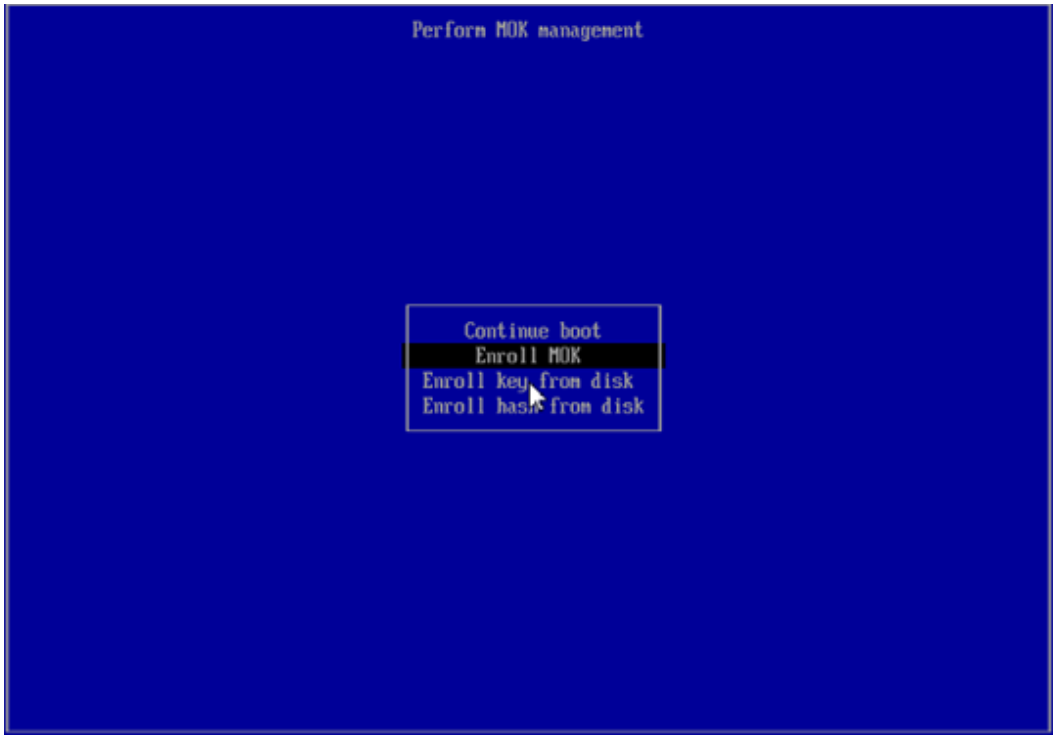
```
localhost:~# mokutil --import /tmp/elfcerdata.der
input password:
input password again:
localhost:~# reboot
```

Step 4 After the node is restarted, go to the UEFI certificate setting wizard and press **Enter**.

 Copyright © Huawei Technologies Co., Ltd.



Step 5 On the **Perform MOK management** page, select **Enroll MOK**, and then press **Enter**.



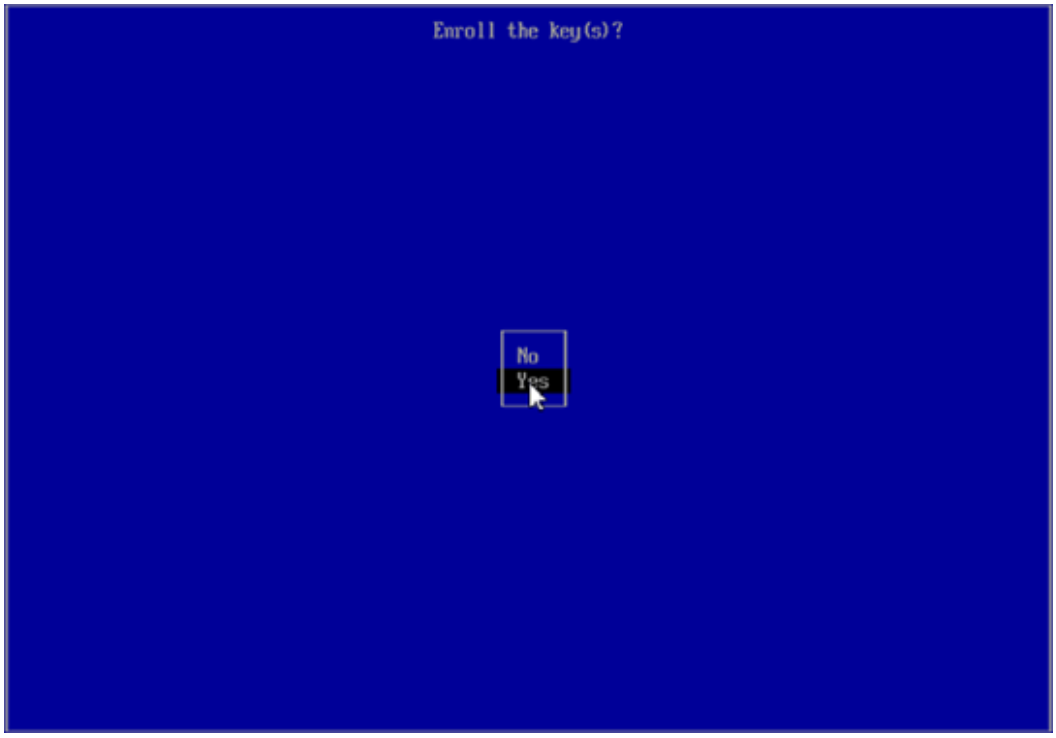
Step 6 On the **Enroll MOK** page, you can select **View key 0** to view the current certificate.

 Copyright © Huawei Technologies Co., Ltd.

Step 7 Press **Esc** to return to the **Enroll MOK** page. Select **Continue** and press **Enter**.

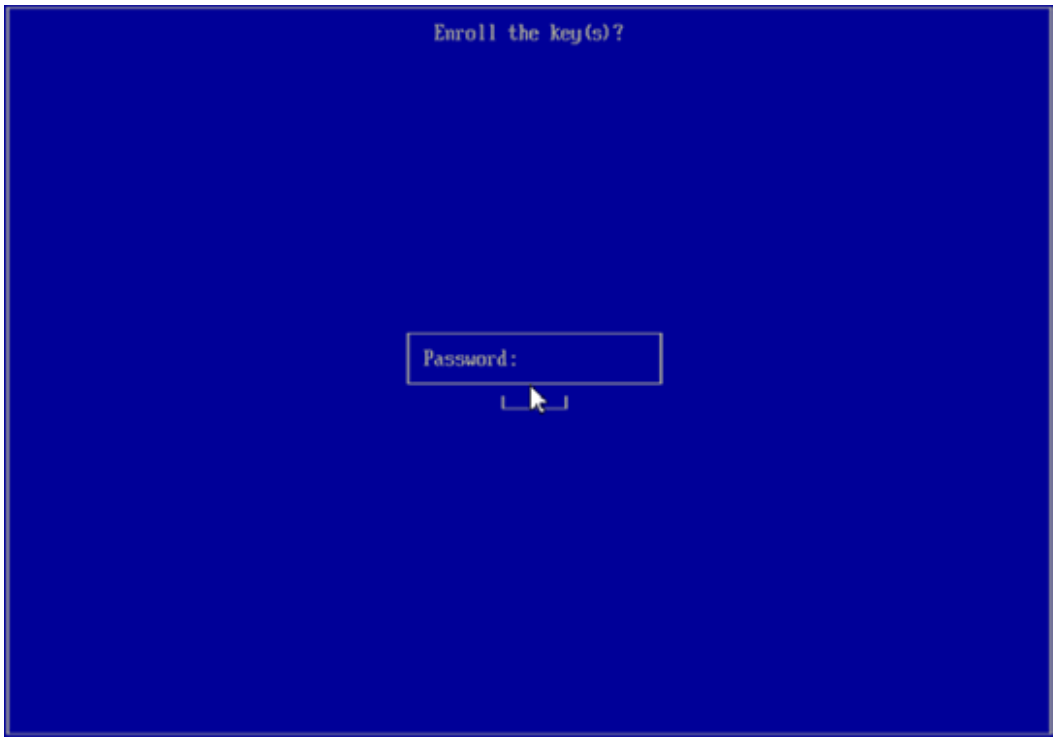
 Copyright © Huawei Technologies Co., Ltd.

Step 8 On the **Enroll the key(s)?** page, select **Yes** and press **Enter**.

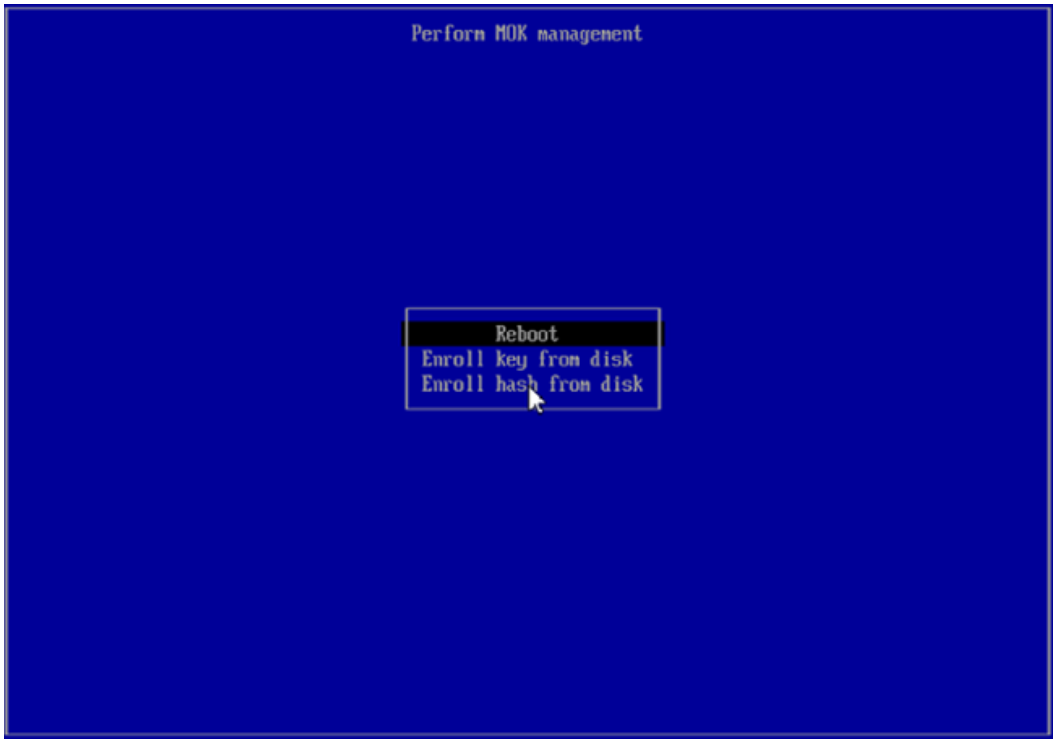


Step 9 Enter the password set in **Step 3** and press **Enter**.

 Copyright © Huawei Technologies Co., Ltd.



Step 10 Return to the **Perform MOK management** page, select **Reboot**, and press **Enter** to restart the system.



----End

6.4.2.9.3 Installing the OS Dependency Package

If a third-party OS is installed on a compute node, the OS dependency package must be installed.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- You have obtained software package **OceanStor-Pacific_8.2.1RC1_Tools.tar.gz** for installing DPC/VBS on a compute node.
- You have configured a management IP address for the compute node.

Procedure

Step 1 Log in to a target compute node through the management IP address as user **root**. If you have logged in as another user, run the **su - root** command to switch to user **root**.

Step 2 Upload the **OceanStor-Pacific_8.2.1RC1_Tools.tar.gz** software package to the compute node and run the following command to decompress the software package.

```
tar -xzf OceanStor-Pacific_8.2.1RC1_Tools.tar.gz
```

NOTE

If error message "-bash: tar: command not found" is displayed, the .tar software package is not installed on the OS. In this case, you need to manually install the .tar software package.

Step 3 Install the OS dependency package.

1. Obtain the script for installing the OS dependency package in the **install_lib** directory.
   - VBS node:

     For the OS dependency package script, see **Table 6-22**. To query the supported OSs, see **Huawei Storage Interoperability Navigator**. For details about the query path, see **Figure 6-4**.

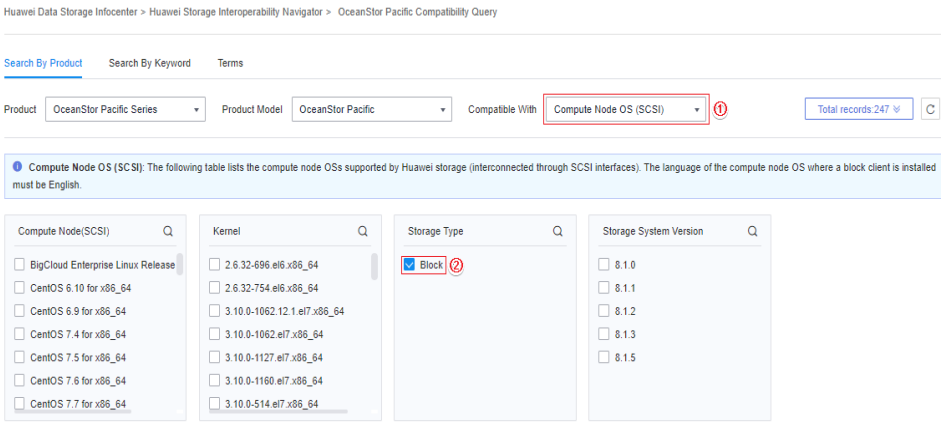
     Table 6-22 OS dependency package scripts of a VBS node

OS and Its Version	Node Role	OS Dependency Package Script Name
Red Hat Enterprise Linux	compute	install_lib_for_rhel.sh
CentOS	compute	install_lib_for_centos.sh
BigCloud Enterprise Linux	compute	install_lib_for_bclinux.sh
Oracle Linux	compute	install_lib_for_oel.sh
Ubuntu	compute	install_lib_for_ubuntu.sh
SUSE Linux Enterprise Server	compute	install_lib_for_suse.sh

 Copyright © Huawei Technologies Co., Ltd.

OS and Its Version	Node Role	OS Dependency Package Script Name
NeoKylin Linux Advanced Server	compute	install_lib_for_neokylin.sh
Kylin Linux Advanced Server	compute	install_lib_for_kylin.sh
UnionTech OS Server	compute	install_lib_for_untech.sh
openEuler	compute	install_lib_for_openeuler.sh
Rocky Linux	compute	install_lib_for_rocky.sh
AlmaLinux	compute	install_lib_for_alma.sh

Figure 6-4 Path for querying the OSs supported by VBS nodes



– DPC node:

  For the OS dependency package script, see **Table 6-23**. To query the supported OSs, see **Huawei Storage Interoperability Navigator** and set **Compatible With** to **DPC Basic Connectivity**, as shown in **Figure 6-5**.

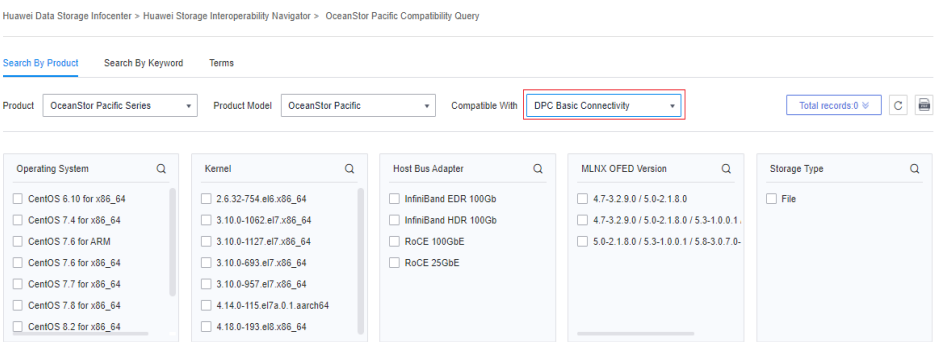
Table 6-23 OS dependency package scripts of a DPC node

OS	Node Role	OS Dependency Package Script Name
Red Hat Enterprise Linux	compute	install_lib_for_rhel.sh

Copyright © Huawei Technologies Co., Ltd.

OS	Node Role	OS Dependency Package Script Name
CentOS	compute	install_lib_for_centos.sh
SUSE Linux Enterprise Server	compute	install_lib_for_suse.sh
Ubuntu	compute	install_lib_for_ubuntu.sh
Kylin Linux Advanced Server	compute	install_lib_for_kylin.sh
KylinSecOS	compute	install_lib_for_kylinsec.sh
AlmaLinux	compute	install_lib_for_alma.sh
Rocky Linux	compute	install_lib_for_rocky.sh
openEuler	compute	install_lib_for_openeuler.sh
EulerOS	compute	install_lib_for_euler.sh
BigCloud Enterprise Linux	compute	install_lib_for_bclinux.sh
Debian GNU/Linux	compute	install_lib_for_debian.sh
CULinux	compute	install_lib_for_culinux.sh

Figure 6-5 Path for querying the OSs supported by DPC nodes



2. Use the script to install the OS dependency package.

 Copyright © Huawei Technologies Co., Ltd.

Check whether a software repository is configured onsite.

- If yes, perform the following operations:
  i. Edit OS dependency package script **install_lib_for**_*xxx*.**sh** and change the value of **YUM_REPO_IS_EXIST** to **1**.

     NOTE

     - Skip this operation if Ubuntu is used.
     - For the SUSE OS, change the value of **ZYPPER_REPO_IS_EXIST** to **1**.

  ii. Copy the OS dependency package script upon modification to the **/tmp** directory on the compute node.
  ```
  cp install_lib_for_xxx.sh /tmp
  ```
  iii. Run the following command to go to the directory where the script for installing the dependency package is stored.
  ```
  cd /tmp
  ```
  iv. Run the following command to install the OS dependency package.
  ```
  bash install_lib_for_xxx.sh node_type
  ```
- If no, perform the following operations:
  i. Upload the OS dependency package script to the **/tmp** directory on the compute node.
  ii. Run the following command to go to the directory where the script for installing the dependency package is stored.
  ```
  cd /tmp
  ```
  iii. Obtain the OS image file. Upload the local OS ISO image file to the compute node.
  iv. Run the following command to install the OS dependency package.
  ```
  bash install_lib_for_xxx.sh node_type /Directory for storing the OS ISO image file/OS ISO image file name
  ```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- When installing the dependency package of the Ubuntu OS, configure the software repository to configure the software installation source and run the following commands.
  ```
  apt-get update
  bash install_lib_for_ubuntu.sh node_type
  ```
- In the commands, *node_type* indicates the role of a node, such as **compute**, **storage**, and **manager**. For details about the node roles supported by the OS, see **Table 6-22** and **Table 6-23**. If a node has multiple roles, use a hyphen (-) to connect the roles, for example:
  - compute-manager
  - compute-storage
  - manager-storage
  - compute-manager-storage
- The installation takes about 10 minutes. The required time depends on the hardware configuration and whether a software repository is used.
- The automatic update of the Ubuntu OS must be disabled. You can run the following commands on a supported OS to change all configuration items in the **10periodic** and **20auto-upgrades** files (only one of the two files may exist) from **1** to **0**. For details about the supported OSs, see **Huawei Storage Interoperability Navigator**.
  - **vi /etc/apt/apt.conf.d/10periodic**

    Change all configuration items from **1** to **0**.
  - **vi /etc/apt/apt.conf.d/20auto-upgrades**

    Change all configuration items from **1** to **0**.

  ```
  root@ubuntu:/home/testTools/vdbench# cat /etc/apt/apt.conf.d/10periodic
  APT::Periodic::Update-Package-Lists "0";
  APT::Periodic::Download-Upgradeable-Packages "0";
  APT::Periodic::AutocleanInterval "0";
  root@ubuntu:/home/testTools/vdbench# cat /etc/apt/apt.conf.d/20auto-upgrades
  APT::Periodic::Update-Package-Lists "0";
  APT::Periodic::Unattended-Upgrade "0";
  root@ubuntu:/home/testTools/vdbench#
  ```
- Hardware Enablement (HWE) cannot be installed on Ubuntu Server.

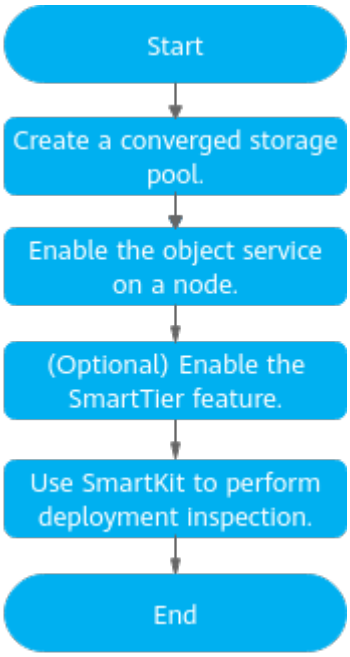
Step 4 Repeat **Step 1** to **Step 3** to install the OS dependency package on other compute nodes.

----End

6.4.3 Configuring Basic Object Services

Figure 6-6 shows the basic service configuration process of object.

Figure 6-6 Configuration process



6.4.3.1 Creating a Converged Storage Pool

This section describes how to create a storage pool from which application servers can use storage space.

Context

- You have installed storage nodes.
- You are advised to configure no more than 32 nodes for each disk pool. If the number of nodes exceeds 32, divide them into multiple disk pools. In this case, it is recommended that the number of nodes in each disk pool be the same. For example, if there are 90 nodes, you are advised to divide them into three disk pools. Each disk pool contains 30 nodes.
- HDD 4KN disks cannot be added to the same disk pool as other types of disks.
- The total capacity of cache disks on a single storage node to be added to a storage pool must be greater than **Max. Main Storage Media per Node** x 40 GB.

Procedure

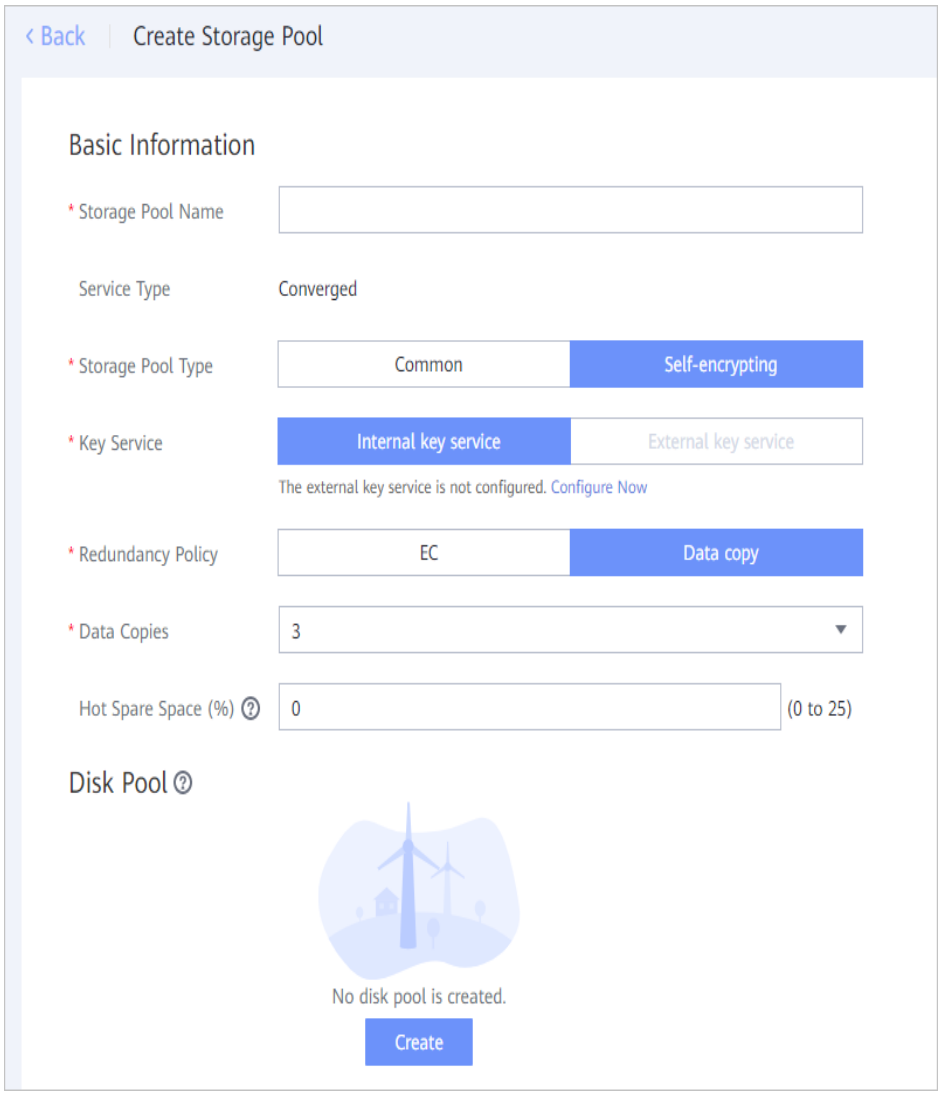
Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Resources** > **Storage Pool**.

Step 3 Click **Create**.

The **Create Storage Pool** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



Step 4 Configure basic information for the storage pool.

Table 6-24 describes related parameters.

Table 6-24 Storage pool parameters

Parameter	Description
Storage Pool Name	Name of the storage pool. **NOTE** • The name must be unique. • The name can contain only letters, digits, underscores (_), and hyphens (-). • The name contains 1 to 64 characters.
Service Type	Service type of the storage pool. In this example, the value is **Converged**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Storage Pool Type	Type of the storage pool. Possible options are **Common** and **Self-encrypting**. You are advised to select **Common**. If you have high requirements on data security, select **Self-encrypting**. • **Common**: This type of storage pools does not support data encryption. • **Self-encrypting**: This type of storage pools supports data encryption. **NOTE** • Currently, converged storage pools do not support self-encrypting SATA disks. • A self-encrypting storage pool can be created only when all the following conditions are met: 1. OceanStor Pacific series 8.1.2 or a later version is deployed, and self-encrypting disks have been configured. 2. An advanced license has been imported. 3. Self-encrypting 4K SAS disks are used if **Main Storage** is set to **Self-encrypting SAS**.
Key Service	When creating a self-encrypting storage pool, you need to select a key management service. • **Internal key service**: The built-in key management function of the system is used. • **External key service**: An external key management server is used. If you select this option, you need to configure the external key service first. For details, see **6.5.6 Managing the External Key Service**.
Redundancy Policy	Redundancy policy of the storage pool. Possible options are **EC** and **Data copy**. Considering performance and reliability, **EC** is recommended. • **EC**: Data redundancy protection is implemented by calculating parity fragments. • **Data copy**: Multiple copies of the same data are stored on different nodes for data protection.
Data Copies	Number of redundant data copies allowed by the storage pool. When **Data Copies** is set to **3**, if the number of storage nodes is greater than 3, a maximum of two faulty nodes are allowed; if the number of storage nodes is 3, only one faulty node is allowed. **NOTE** • This parameter is available only when **Redundancy Policy** is set to **Data copy**. • If **Service Type** is set to **Intelligent video and image**, three-copy storage pools cannot be created.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Hot Spare Space (%)	Hot spare space is the space reserved in the system to take over data from faulty disks. This improves reliability and avoids system redundancy reduction. To support data rebuilding after single-disk failure at high capacity usage, the recommended value is (1/ Number of disks on a single node) x 100%. **NOTE** Reserving too much hot spare space will occupy excessive available system capacity, causing the available capacity obtained by users to decrease. Configure the hot spare space properly. [Value range] 0 to 25 [Default value] **0**
Storage Pool Mode	If EC redundancy level of the storage pool is +3:1 or higher, you need to set the storage pool mode. If the reliability mode is selected, write cache acceleration cannot be enabled.

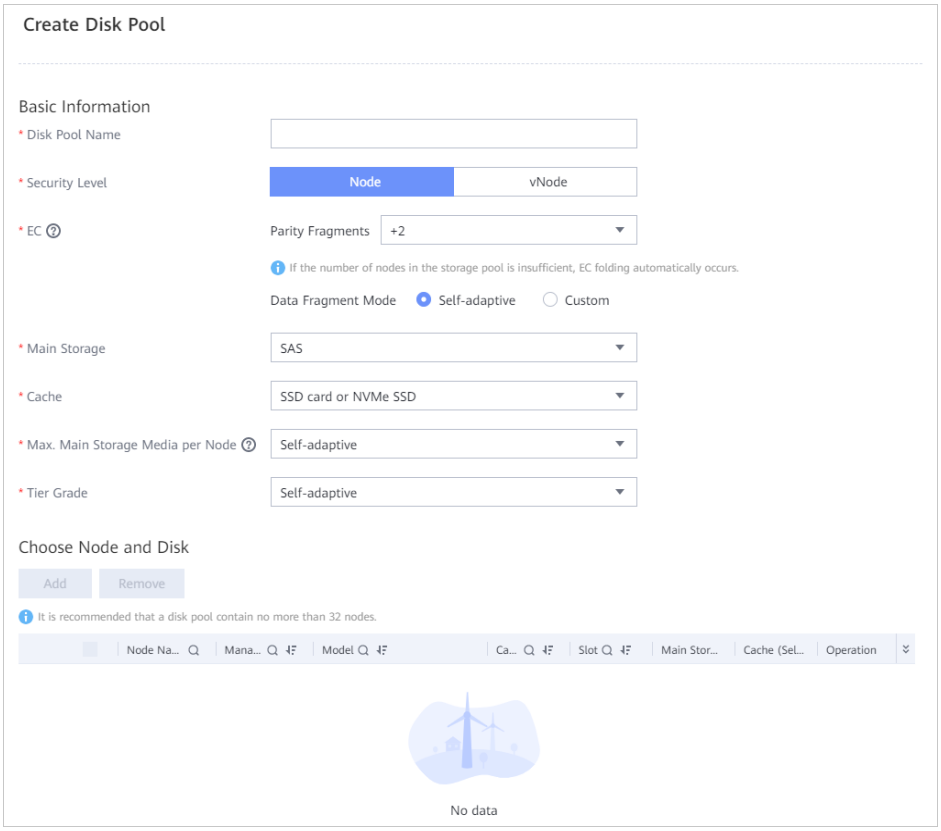
Step 5 Create a disk pool.

NOTE

For details about how to configure disk pools, see the plan in the BOQ.

1. In the **Disk Pool** area, click **Create**.
   The **Create Disk Pool** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



2. Set basic parameters for the disk pool.
   Table 6-25 describes related parameters.

Table 6-25 Disk pool parameters

Parameter	Description
Disk Pool Name	Name of the disk pool. **NOTE** – The name must be unique. – The name can contain only letters, digits, underscores (_), and hyphens (-). – The name contains 1 to 64 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Security Level	Security level of the disk pool. – **Node**: ▪ *N*+*M*: *N* data fragments and *M* parity fragments are randomly stored on different nodes. (The number of storage nodes is greater than *N* + *M*. To ensure reliability, data fragments are stored on different nodes.) In this case, the disk pool can tolerate simultaneous failures of *M* disks or *M* nodes. ▪ *N*+*M*:1 (folded): *N* data fragments and *M* parity fragments are randomly distributed on all nodes. Any node may store *M* fragments. In this case, the disk pool can tolerate simultaneous failures of *M* disks or one node. – **vNode**: A vNode is a logical area consisting of multiple disks on a node. In OceanStor Pacific 9546, a node contains two vNodes. In OceanStor Pacific 9550, a node contains four vNodes. *N* data fragments and *M* parity fragments are stored on different vNodes, and EC redundancy calculation is performed by vNode. A larger EC ratio indicates higher storage utilization. If a node is faulty, its disks can be taken over by the other node in the same chassis and main storage disks will not be degraded or rebuilt by virtue of the dedicated hardware design of OceanStor Pacific 9546 and OceanStor Pacific 9550. **NOTE** **vNode** is supported only when **Redundancy Policy** is set to **EC**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
EC	EC redundancy policy of the disk pool. Select the EC redundancy ratio planned in the Bill of Quotation (BOQ). **NOTE** – This parameter is available only when **Redundancy Policy** is set to **EC**. – When creating multiple disk pools, ensure that the settings of **Parity Fragments** for the disk pools are the same. – The data fragment mode can be **Self-adaptive** or **Custom**. ■ When you select **Self-adaptive**, the system automatically sets the number of data fragments based on the EC redundancy ratio tables and the selected nodes or cabinets and parity fragments. For details about the EC redundancy ratio tables, see **Functions and Features** > **Key Features** > **File/Object/ HDFS Service** > **Elastic EC** in the *OceanStor Pacific Series 8.2.1 Product Description*. ■ When you select **Custom**, the number of data fragments is an even number ranging from 4 to 22. The number of nodes that can be contained in a disk pool and the disk pool utilization vary depending on the number of data fragments selected. For details, refer to the actual page.
Main Storage	Main storage type of the disk pool. – When **Storage Pool Type** is set to **Common**, the value of this parameter can be **SAS**, **Self-encrypting SAS**, **SATA**, **Self-encrypting SATA**, **SSD**, and **SSD card or NVMe SSD**. In this case, self-encrypting drives function as common disks and do not use the encryption function. – When **Storage Pool Type** is set to **Self-encrypting**, the value of this parameter can be **Self-encrypting SAS**, **Self-encrypting SATA**, **Self-encrypting SSD card or NVMe SSD (with Chinese cryptographic algorithms)**, or **Self-encrypting SSD card or NVMe SSD (with international cryptographic algorithms)**. – Each node must be configured with at least four disks of the same type. **NOTE** Meanings of the values are: – **SAS**: SAS HDDs – **SATA**: SATA HDDs – **SSD card or NVMe SSD**: NVMe SSDs – **SSD**: SAS SSDs

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Cache	Cache type of the disk pool. **NOTE** – This parameter is not required when **Main Storage** is set to **SSD** or **SSD card or NVMe SSD**. – Meanings of the values are: ■ **SSD card or NVMe SSD**: NVMe SSDs ■ **SSD**: SAS SSDs
Max. Main Storage Media per Node	Maximum number of main storage disks that can be used on a single storage node to store user data. The value of this parameter determines the allocation of cache and compute resources on the node. Set this parameter as planned. To ensure that cache resources can be allocated to newly added main storage disks in the case of capacity expansion, you are advised to set this parameter based on the total number of main storage disks after capacity expansion. – If the value is too small, newly added main storage disks cannot be allocated with cache resources. Cache resources can be allocated to newly-added main storage disks only after both main storage disks and cache disks are added. – If the value is too large, extra cache resources are reserved. As a result, cache resources cannot be fully utilized to improve read/write performance. If you select **Self-adaptive**, the system automatically determines the value based on the number of selected main storage disks. Assume that the number of selected main storage disks is N: – If $4 \leq N \leq 12$, a single node supports a maximum of 12 main storage disks. – If $12 < N \leq 36$, a single node supports a maximum of 36 main storage disks. – If the type of nodes in the disk pool is OceanStor Pacific 9550, a single node supports a maximum of 60 main storage disks. Ensure that the total capacity of the cache disks on selected storage nodes is greater than the maximum number of main storage disks on a single node multiplied by 40 GB. If you select **Custom**, set this parameter as required. When **Service Type** is set to **Intelligent video and image**, the value ranges from 24 to 60. For other service types, the value ranges from 4 to 60.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Tier Grade	Tier grade of the disk pool, which is defined based on the type of main storage disks in the disk pool. Possible values are **Hot**, **Warm**, **Cold**, and **Self-adaptive**. You can choose **Resources** > **Dataflow** > **SmartTier** and set tiering policies to store different files to disk pools of different tier grades. **NOTE** – If you select **Self-adaptive**: When **Main Storage** is set to **SSD** or **SSD card or NVMe SSD**, **Self-adaptive** equals to tier grade **Hot**. When **Main Storage** is set to **SAS**, **Self-adaptive** equals to tier grade **Warm**. When **Main Storage** is set to **SATA**, **Self-adaptive** equals to tier grade **Cold**. – If you select **Self-adaptive**, you are advised to configure the storage tiers based on the self-adaptive rules.

3. In the **Choose Node and Disk** area, select the nodes and disks that are used to create the disk pool.

   NOTE

   – You can click **Add** and add nodes and disks in the cluster to the disk pool on the **Choose Node and Disk** page that is displayed.
   – When **Service Type** is set to **Intelligent video and image**, the number of selected disks must be greater than or equal to 24.
   – You can select one or more added nodes or disks and click **Remove** to remove them.

4. Click **OK** and confirm your operation as prompted.

Step 6 Click **Create**.

Step 7 Confirm your operation as prompted.

----End

6.4.3.2 Enabling the Object Service on a Node

Before using the object service, you need to enable the object service for storage nodes.

Prerequisites

- A storage pool has been created.
- This operation can be performed only when no node with the object service enabled exists in the storage pool. Otherwise, add nodes for the object service by referring to **6.5.8 Adding a Node for an Enabled Service**.
- NTP synchronization must be configured for each cluster. You are advised to use the same NTP time source. For details, see **Routine Management** > **Managing Storage System Settings** > **Configuring the System Time** in the *OceanStor Pacific Series 8.2.1 Administrator Guide*. The configuration item is **Synchronize with NTP server time**. Administrators are not allowed to manually adjust the time of cluster nodes. Otherwise, conflict processing may be different, causing data inconsistency.

Copyright © Huawei Technologies Co., Ltd.

- The NTP clock in the storage cluster must be the same as the clock of the object service access client.

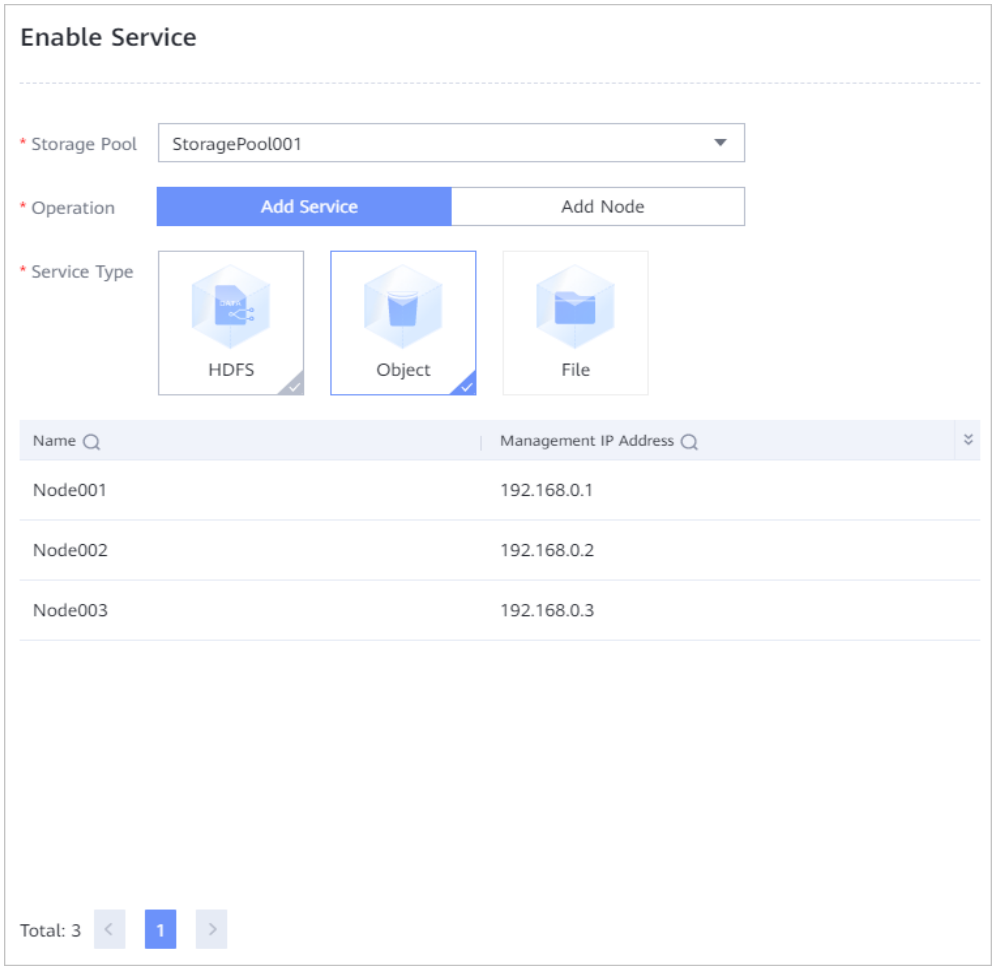
Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Resources** > **Services** > **Basic Service**.

Step 3 Click **Enable Service**.

The **Enable Service** page is displayed.



Step 4 Select the storage pool for which you want to enable the object service.

Step 5 Select **Add Service** in **Operation**.

NOTE

This parameter is displayed only when at least one service is enabled on the nodes in the storage pool.

Step 6 Select **Object** in **Service Type**.

Step 7 Based on service requirements, select at least three nodes in the **Available Nodes** area on the left. They will be automatically added to the **Selected Nodes** area on the right.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

You need to select nodes only when all services (file, object, and HDFS services) of the storage pool are disabled. Otherwise, the system enables the object service for all nodes where other services have been enabled by default.

----End

6.4.3.3 (Optional) Enabling the SmartTier Feature

If a cluster contains two or more types of media, you can perform this operation to enable the SmartTier feature and write files based on the default placement policy.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Tuning** > **SmartTier**.

Step 3 By default, the SmartTier feature is disabled by the storage system. When you go to the **SmartTier** page for the first time, you need to click **Enable** to enable the SmartTier feature.

----End

6.4.3.4 Adding a VXLAN

When the storage system needs to connect to the VPC network, you need to configure a VXLAN.

You do not need to configure a VXLAN for OceanStor Pacific 9950.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Access** > **VXLAN**.

Step 3 Click **Add**.

The **Add VXLAN** page is displayed.

Step 4 Click **Batch Import** or **Manually Add** to add nodes to which VXLANs can be added.

NOTE

Add VXLANs for each storage node separately.

- Batch import nodes.
  a. Click **Batch Import**.
  b. Click **Download the template** to download the template locally. Fill the information in the template, click ··· and select the template, and then click **Upload**. The nodes are imported to the system in a batch.
- Manually add nodes.

 Copyright © Huawei Technologies Co., Ltd.

a. Set VXLAN parameters. **Table 6-26** describes related parameters.

Table 6-26 VXLAN parameters

Parameter	Description
Management IP Address	Management IP address of a storage node.
Health Check IP Address/ Mask	IP address and mask configured on a storage node for checking the health status of the node. The IP address and mask are used for VPC EP2.0 load balancing.
Health Check Gateway	Gateway of the health check IP address.
VXLAN Tunnel IP Address/ Mask	VTEP IP address used to establish a VXLAN tunnel between nodes. The VTEP IP addresses of the nodes can communicate with each other.
VXLAN Tunnel Gateway	Gateway corresponding to the VXLAN tunnel IP address.
VXLAN Tunnel VLAN ID	VLAN ID of the service plane.
Destack Networking	Select this option when switches are not stacked. Do not select this option when switches are stacked.

b. Click **OK** to add the VXLAN to the list.

NOTE

You can click **More** on the right of a VXLAN and select **Modify** or **Delete** to manage it.

Step 5 Click **OK**.

----End

6.4.3.5 Using SmartKit to Perform Deployment Inspection

After hardware installation, software installation, and subsequent service configuration are complete, use SmartKit on the maintenance terminal to check the status of the storage cluster and the version mapping of storage nodes.

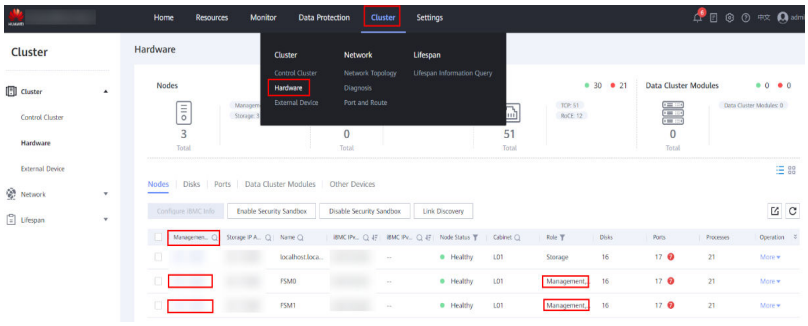
Prerequisites

1. A local PC is properly communicating with the scale-out storage devices and server OS/BMC, the SSH and HTTPS communication ports are enabled, and the floating IP addresses of the scale-out storage devices and server OS/BMC IP addresses can be pinged from the local PC. You have obtained the following data:
   - Floating IP addresses, user names, and passwords of the scale-out storage devices

 Copyright © Huawei Technologies Co., Ltd.

- SSH login user name and password of the server OS. The password of user **root** must be provided for a non-root user. If you do not customize the account and password, you are advised to use the **fsadmin** account and its password.
- External management IP addresses of management nodes
- Server BMC user name and password

2. When the management network of the storage cluster is isolated, you need to configure the SSH proxy for the two management nodes (FSM) in each cluster:
   a. Disable the security sandbox by referring to **Routine Management** > **Managing a Cluster System** > **Managing Hardware Information** > **Disabling Security Sandbox** in the *Administrator Guide* of the corresponding version.
   b. Log in to DeviceManager, choose **Cluster** > **Hardware**, view the nodes whose roles include **Management**, and record the management IP addresses of all management nodes.



   c. Use the SSH tool to log in to each management node as user **fsadmin** through the management IP address. Run the **su - root** command and enter the password of user **root** to switch to user **root**.
   d. Run the **vi /etc/ssh/sshd_config** command to open the configuration file and set **AllowTcpForwarding** to **yes**.
   e. After editing the configuration files, press **Esc** and enter **:wq** to save the settings and exit.
   f. Run the **sudo service sshd restart** command to restart the sshd service.

NOTICE

After the deployment inspection is completed, you need to disable the SSH proxy mode by referring to **Follow-up Procedure** and enable the security sandbox again.

Context

The GUI may vary with the version.

Procedure

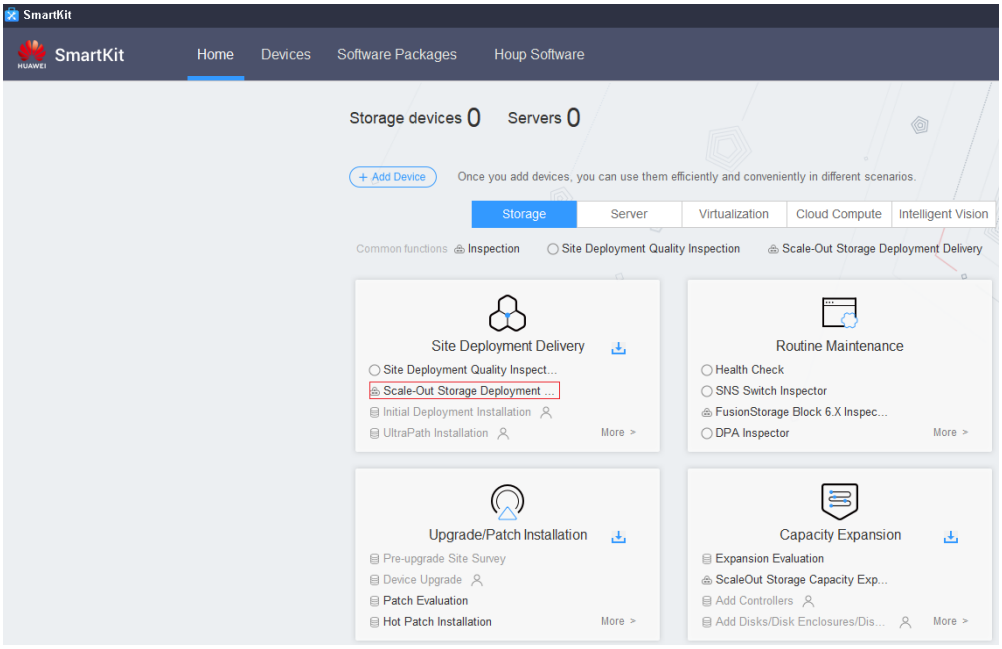
Step 1 Prepare SmartKit. If it has been installed, skip this step.

 Copyright © Huawei Technologies Co., Ltd.

1. Download and install SmartKit.
   - For enterprise users: Log in to **https://support.huawei.com/enterprise**, enter **SmartKit** in the search box, and select **Distributed Storage > Tools and Platform > SmartKit** from the suggested paths.
     i. On the displayed SmartKit page, click **Software Download**, and select and download SmartKit of the latest version according to the publication date.
     ii. On the SmartKit page, click **Documentation**, find the user guide of the corresponding version, and install and run SmartKit respectively by following the instructions provided in sections "Installing SmartKit" and "Running SmartKit".
   - For carrier users: Log in to **https://support.huawei.com**, enter **SmartKit** in the search box, and select **Data Storage > Scale out Storage > Storage Common > SmartKit** from the suggested paths.
     i. On the displayed SmartKit page, click **Software**, and select and download SmartKit of the latest version according to the release date.
     ii. On the SmartKit page, click **Product Documentation**, find the user guide of the corresponding version, and install and run SmartKit respectively by following the instructions provided in sections "Installing SmartKit" and "Running SmartKit".
2. Install the Scale-Out Storage Deployment Delivery tool by referring to section "Installing Functions" in the SmartKit user guide.

Step 2 Go to the **Site Deployment Delivery** page.

1. On the home page of SmartKit, choose **Site Deployment Delivery** > **Scale-Out Storage Deployment Delivery**.

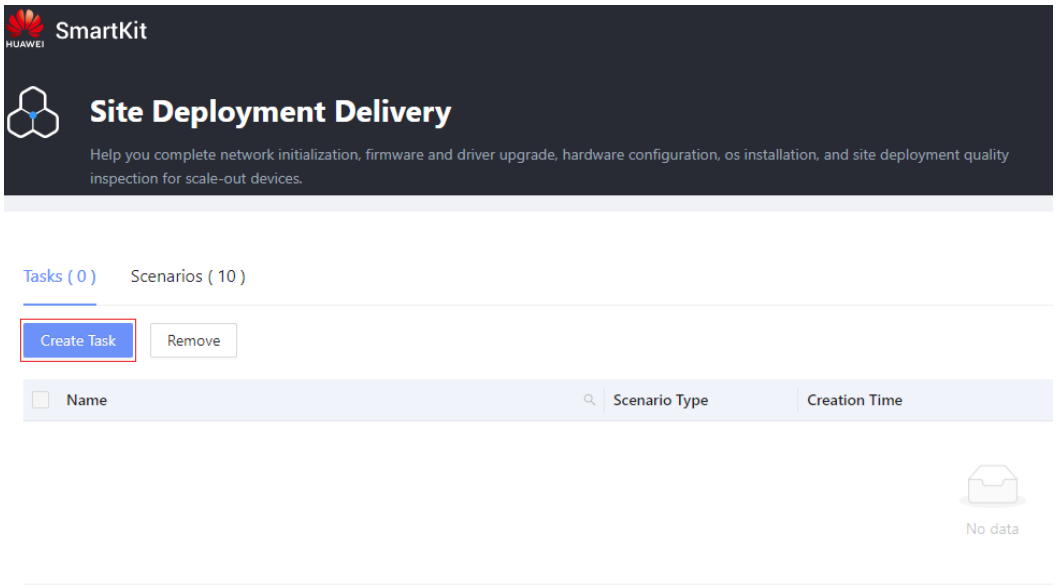


2. On the **Scale-Out Storage Deployment Delivery** page, click **Scale-Out Storage Deployment Delivery**. The **Site Deployment Delivery** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Click **Create Task**. The **Select Scenario** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

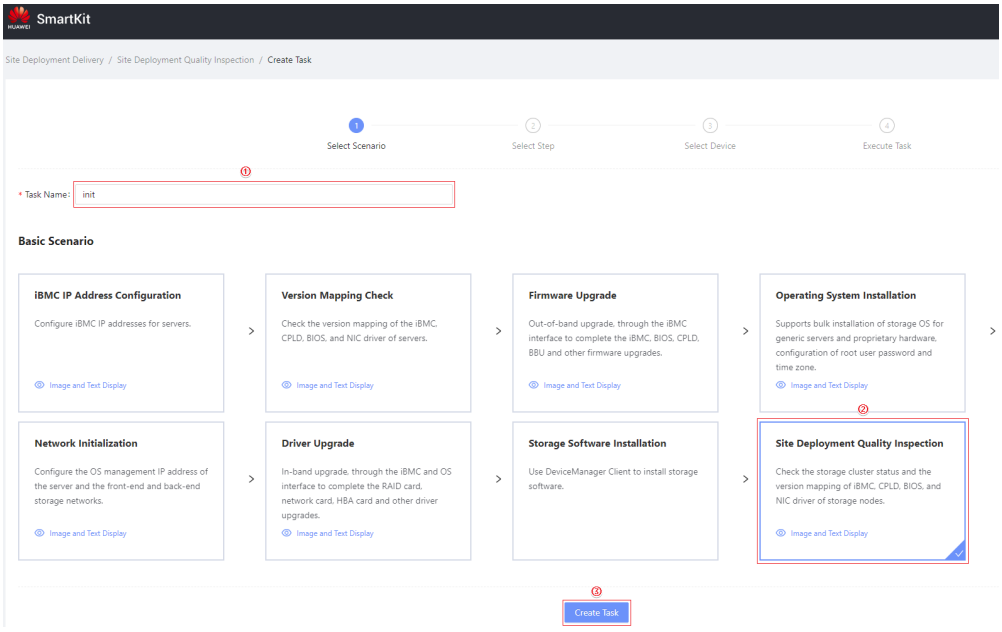


Step 4 Select a scenario.

1. Set **Task Name**, select **Site Deployment Quality Inspection**, and click **Create Task**.

   NOTE

   The task name contains 2 to 128 characters, including digits, letters, spaces, hyphens (-), and underscores (_). It cannot start or end with a space, hyphen (-), or underscore (_).



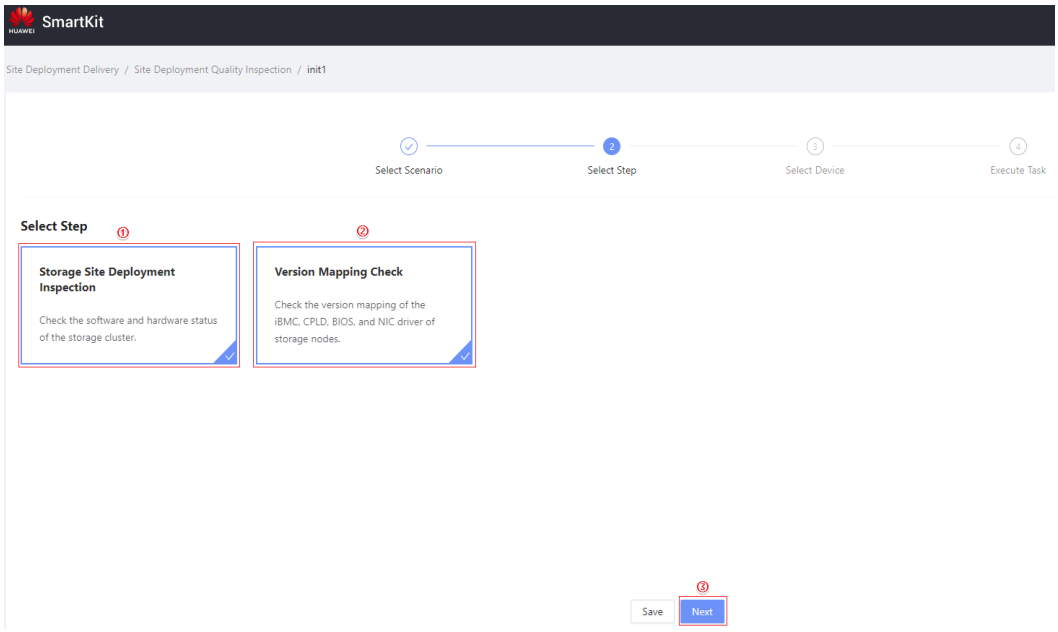
2. The **Confirm Message** dialog box is displayed. Confirm the information and click **Continue**.

   NOTE

   If you select **Do not show again**, the dialog box will not be displayed when you create a task again.

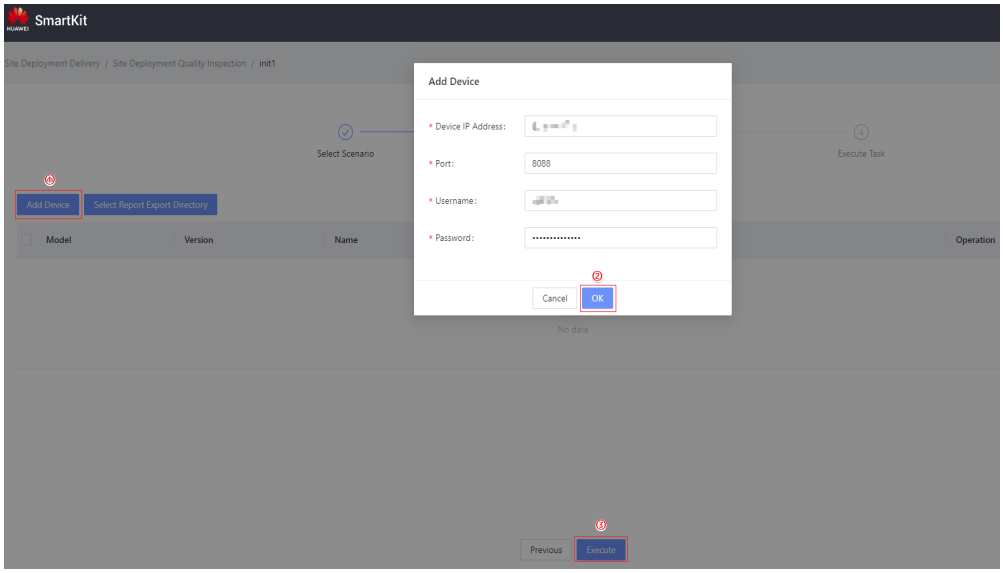
 Copyright © Huawei Technologies Co., Ltd.

Step 5 Select **Storage Site Deployment Inspection** and **Version Mapping Check**, and click **Next**.



Step 6 Select a device.

1. Add a device.



a. Click **Add Device**. The **Add Device** dialog box is displayed.

b. Enter device information as prompted and click **OK**.

Table 6-27 Device information

Name	Description
Device IP Address	DeviceManager management IP address

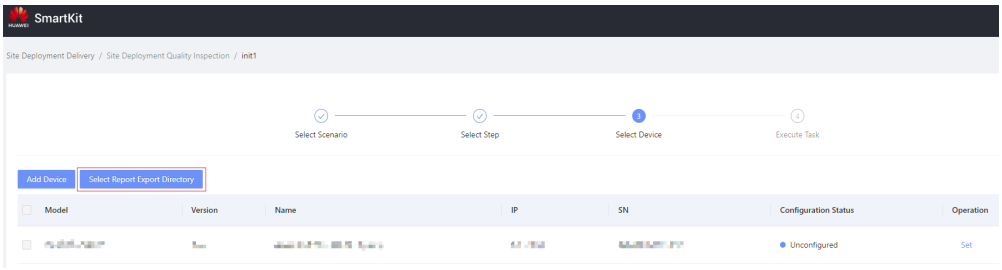
 Copyright © Huawei Technologies Co., Ltd.

Name	Description
Port	Port of DeviceManager. Use default port **8088**.
Username	DeviceManager login account
Password	Password for logging in to DeviceManager

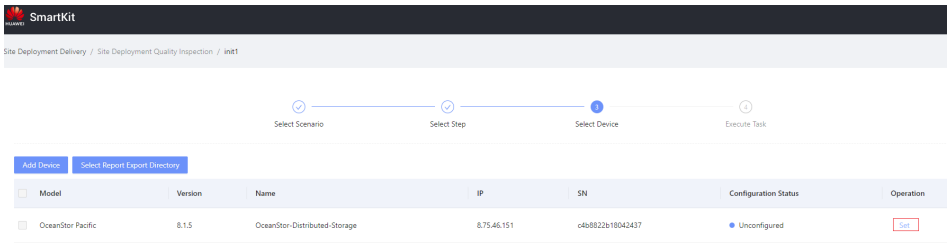
NOTE

If the device has been added, it is displayed in the list by default. You do not need to add it again.

2. Click **Select Report Export Directory** and specify a save path for the report.



3. Set a check policy.
   a. Click **Set** in the **Operation** column of a device. The **Set Node** page is displayed.



   b. Select a node and authenticate it.

      i. Select the nodes to be checked.

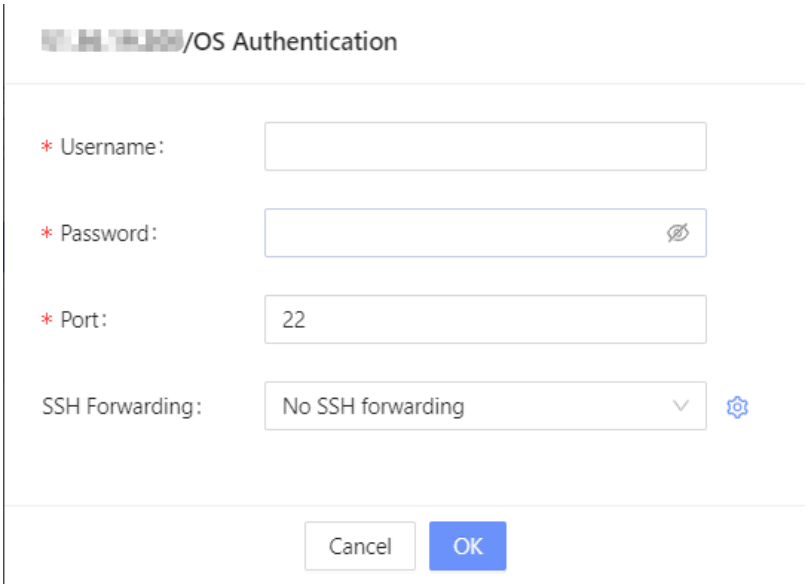
      ii. Click **OS Authentication**. In the node authentication dialog box that is displayed, perform OS authentication and BMC authentication on the node as prompted.

      You do not need to configure SSH forwarding for BMC authentication. To configure SSH forwarding for OS authentication, perform the following steps:

      1) Select the node to be authenticated and click **OS Authentication**. In the dialog box that is displayed, enter the SSH login user name and password of the server OS and port. If the user name and password are not customized, you are advised to use the **fsadmin** account and password. If a non-**root** user is used, you need to provide the password of the **root** user.

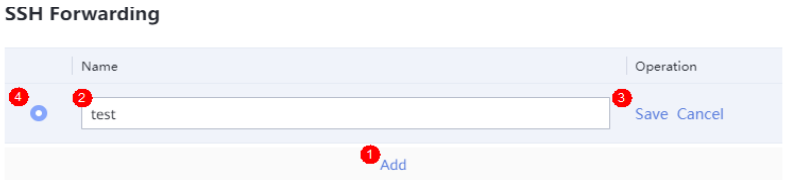
 Copyright © Huawei Technologies Co., Ltd.

2) Click ⚙ in the **SSH Forwarding** column.

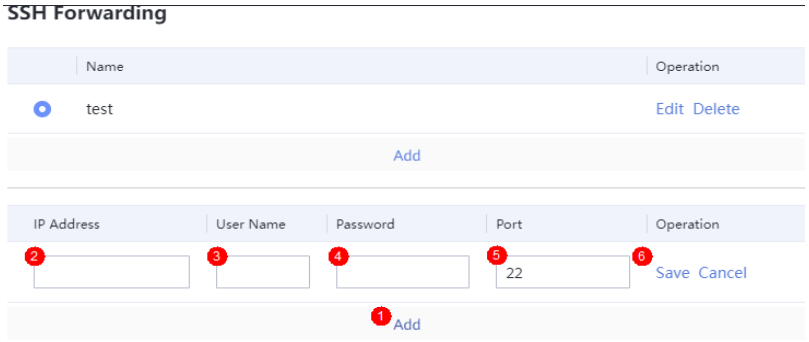


3) Click **Add** in the **Name** column, name the configured SSH forwarding, and click **Save**.

4) Click the check box next to **Name** to select the newly added SSH forwarding.



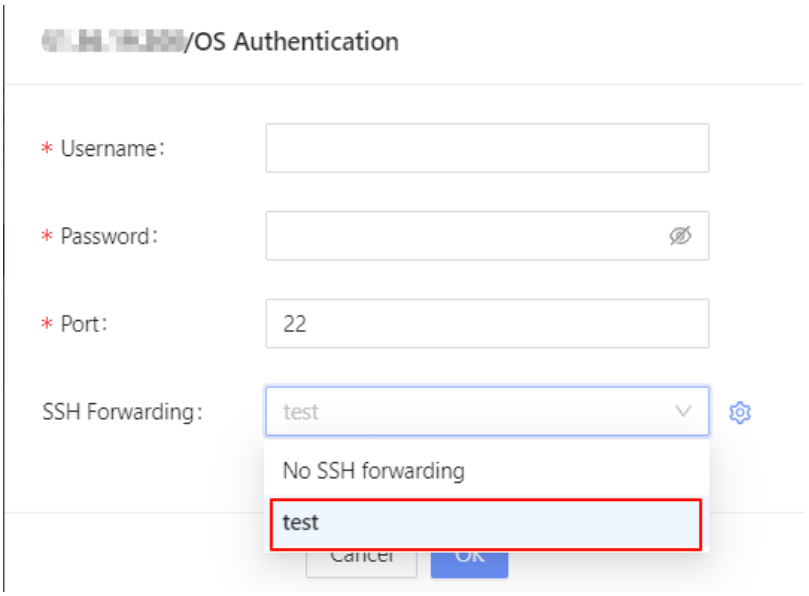
5) Click **Add** in the **IP Address** column to add the IP address, user name, password, and port for SSH forwarding. IP address indicates the external management IP address of any management node, user name and password indicate the **root** user and password of user **root** of the server OS, and port is 22 by default. Click **Save**.



6) Click **OK** to return to the authentication page.

7) In the **SSH Forwarding** area, select the created SSH forwarding.

 Copyright © Huawei Technologies Co., Ltd.



8) Click **OK**.

iii. Click **iBMC Authentication** and enter related information as prompted to complete the authentication.

iv. Click **Next**. The **Add Switches** page is displayed.

c. (Optional) Add switches.

NOTE

This step applies only to access switches whose storage network uses RoCE networking. In other scenarios, click **Skipped** to skip this step.

i. Click **Add Switch** and enter information about all storage switches.

NOTE

You can also click **Download Template** to download the switch information template, enter login information, and click **Batch Import**.

ii. Click **Next**. The **Select Check Item** page is displayed.

d. Select the items to be checked and click **Next**. The **Select Mapping Check Scenario** page is displayed.

e. Select a mapping check scenario.

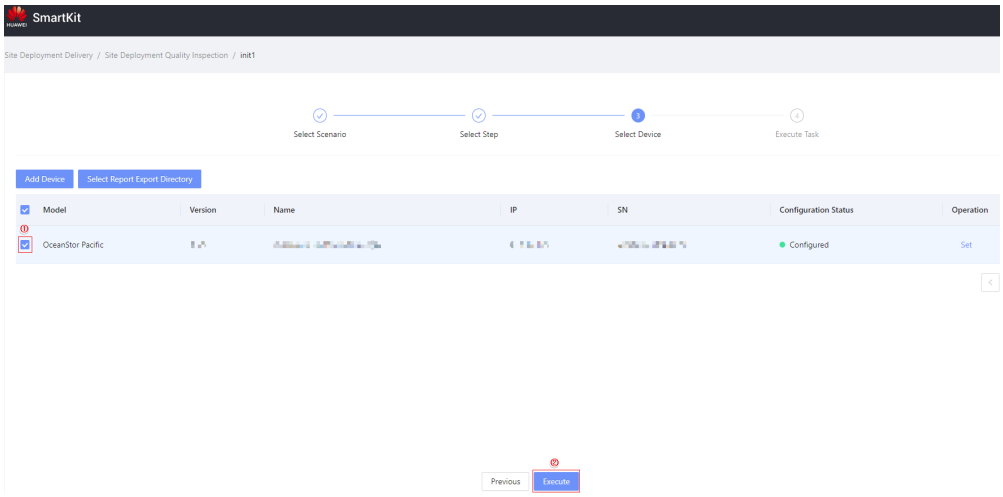
i. Set **Storage Software Version**.

ii. Click **Confirm Config**.

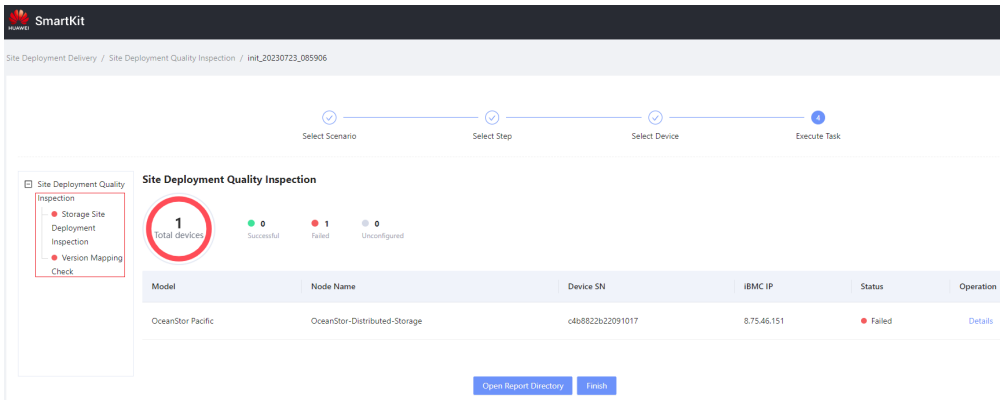
Step 7 Execute the task.

1. Select a device, click **Execute**, and enter the information about the inspection report personnel as prompted.

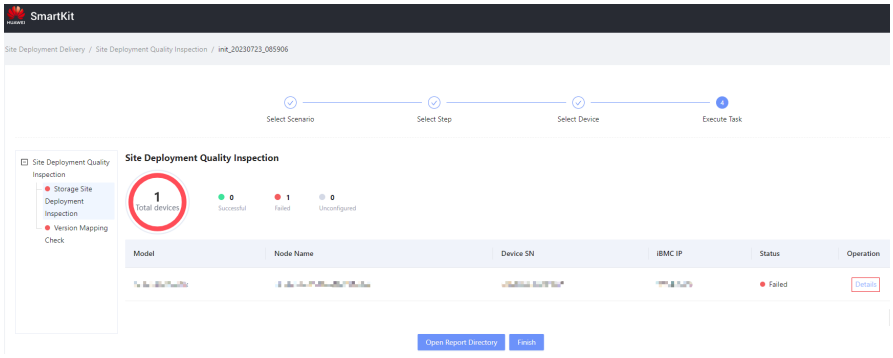
 Copyright © Huawei Technologies Co., Ltd.



2. After the task is complete, check whether the **Storage Site Deployment Inspection** and **Version Mapping Check** items pass the check (marked in green).

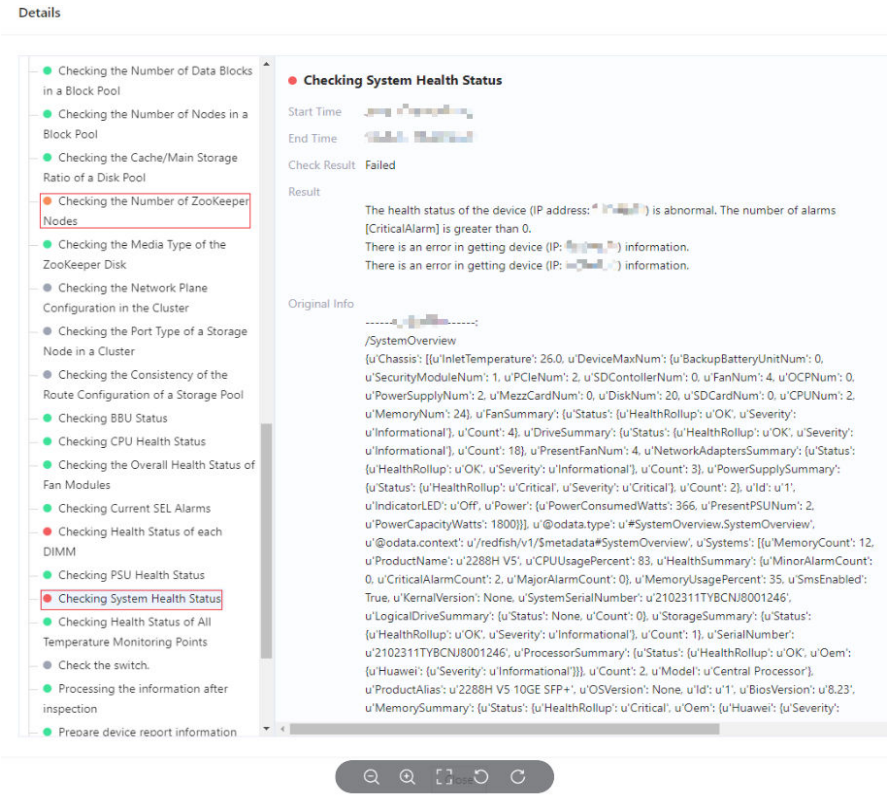


- If yes, click **Finish**.
- If no, perform the following steps for the two check items (after the troubleshooting is complete, click **Finish**):
  i. Click **Details** in the **Operation** column of the corresponding device.



  ii. Click the check items that fail to pass the check (marked in red) and the check items that need to be optimized (marked in orange) in sequence, and handle the problems according to the description in **Result**. The following uses **Storage Site Deployment Inspection** as an example:

 Copyright © Huawei Technologies Co., Ltd.



----End

Follow-up Procedure

When the management network of the storage cluster is isolated, you need to disable the SSH proxy configured for the management nodes (FSM) and enable the security sandbox after the deployment inspection operation is completed.

1. Use the SSH tool to log in to each management node as user **fsadmin** through the management IP address. Run the **su - root** command and enter the password of user **root** to switch to user **root**.
2. Run the **vi /etc/ssh/sshd_config** command to open the configuration file and set **AllowTcpForwarding** to **no**.
3. After editing the configuration file, press **Esc** and enter **:wq** to save the settings and exit.
4. Run the **sudo service sshd restart** command to restart the sshd service.
5. Enable the security sandbox again by referring to **Routine Management** > **Managing a Cluster System** > **Managing Hardware Information** > **Enabling Security Sandbox** in the *Administrator Guide* of the corresponding version.

6.5 Managing Basic Services

 Copyright © Huawei Technologies Co., Ltd.

6.5.1 Managing a Converged Storage Pool

A storage pool consolidates the storage space of different nodes for centralized management.

6.5.1.1 Viewing Storage Pool Information

This section describes how to view information about storage pools.

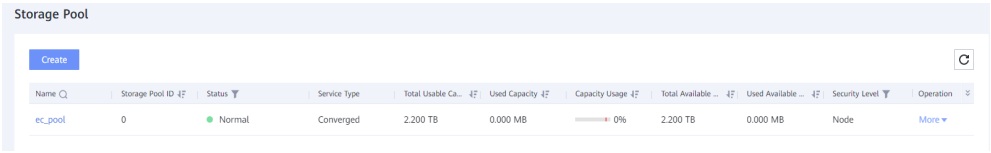
Context

- On the storage pool management page, click to refresh storage pools.
- On the storage pool management page, click to export a list of storage pools.
- On the storage pool management page, click or next to a parameter and enter a keyword or select a parameter value to search for desired storage pools.
- On the storage pool management page, click and select desired storage pool parameters to be viewed.
- On the storage pool management page, click or next to a parameter to change the display order of storage pools.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Resources** > **Storage Pool**.



Step 3 View information about the storage pools in the function pane. **Table 6-28** describes related parameters.

Table 6-28 Storage pool parameters

Parameter	Description
Name	Name of a storage pool.
Storage Pool ID	ID of a storage pool.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Status	Status of a storage pool. Possible values are **Normal**, **Faulty**, **Write-protected**, **Stopped**, **Faulty and write-protected**, **Migrating data**, **Degraded**, **Rebuilding data**, **Migrating services**, and **Unknown**. **NOTE** When expanding or reducing the capacity of a storage pool on DeviceManager, the task is at the **Notify EDS scale out** or **Clear EDS on the storage node** step, and the storage pool is in normal status, **Status** of the storage pool will be displayed as **Migrating services**. On the CLI, **Migrating services** is not a possible value of storage pool status. A storage pool in such status will be displayed as **Normal**.
Service Type	Service type of a storage pool.
Key Service	• **Internal key service**: The built-in key management function of the system is used. • **External key service**: An external key management server is used for management.
Total Usable Capacity	Actual usable physical disk space of a storage pool (Total physical disk capacity – Capacity consumed by EC redundancy – Capacity lost due to hardware faults).
Used Capacity	Used physical disk space of a storage pool.
Capacity Usage	Ratio of **Used Capacity** to **Total Usable Capacity** of a storage pool.
Total Available Capacity	Total amount of data that can be written into a storage pool.
Used Available Capacity	Total amount of data that has been written into a storage pool.
Hot Spare Space	Percentage of the hot spare space in the storage pool space.

NOTE

- In the event of a node or disk fault, the system is degraded and reconstructed. **Total Usable Capacity** and **Total Available Capacity** decrease and change dynamically. After the fault is rectified, the capacity recovers.
- After the node or disk recovers from the fault, the system recycles the data written during EC reduction upon the fault. Before the recycle is complete, **Total Usable Capacity** and **Total Available Capacity** change dynamically in a small range.
- You can click the name of a storage pool to view its summary and disk pool information. **Table 6-29** describes related disk pool parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-29 Disk pool parameters

Parameter	Description
Disk Pool	Name of a disk pool.
ID	ID of a disk pool.
Status	Status of a disk pool. Possible values are **Normal**, **Faulty**, **Stopped**, **Migrating data**, **Degraded**, **Rebuilding data**, and **Unknown**.
Nodes	Number of nodes in a disk pool.
Redundancy Policy	Redundancy policy of a disk pool.
Main Storage	Main storage type of a disk pool.
Main Storage Disks	Number of main storage disks in a disk pool.
Cache Disks	Number of cache disks in a disk pool.
Tier Grade	Tier grade of a disk pool.
Security Level	Security level of the disk pool.
Remaining Data for Increasing Fragments	Amount of data for which data fragments are to be increased to meet the current redundancy policy of a disk pool.

----End

6.5.1.2 Modifying a Storage Pool

This section describes how to modify basic information about a storage pool.

Procedure

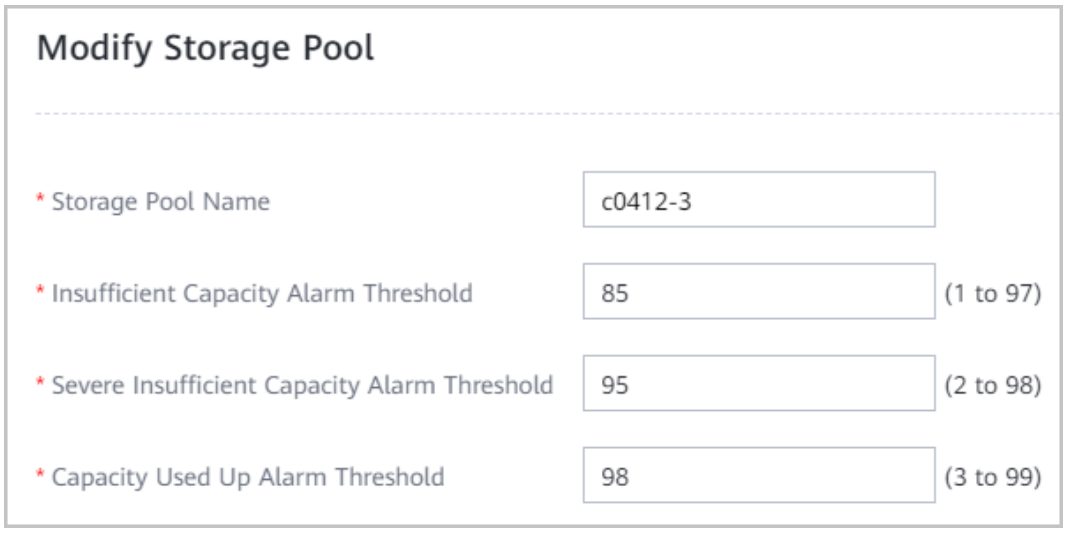
Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Resources** > **Storage Pool**.

Step 3 Click **More** on the right of the desired storage pool and select **Modify**.

The **Modify Storage Pool** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



Step 4 Change the name of the storage pool.

NOTE

- The name must be unique.
- The name can contain only letters, digits, underscores (_), and hyphens (-).
- The name contains 1 to 64 characters.

Step 5 Set **Insufficient Capacity Alarm Threshold**, **Severe Insufficient Capacity Alarm Threshold**, and **Capacity Used Up Alarm Threshold**.

NOTE

When the percentage of the used capacity in the total capacity (used capacity for short) of a storage pool reaches the capacity alarm threshold, the system generates an alarm. An alarm is generated in the following circumstances:

- When the used capacity of a storage pool reaches **Insufficient Capacity Alarm Threshold**, the system generates an alarm indicating that the storage pool capacity is insufficient.
- When the used capacity of a storage pool reaches **Severe Insufficient Capacity Alarm Threshold**, the system generates an alarm indicating that the storage pool capacity is severely insufficient.
- When the used capacity of a storage pool reaches **Capacity Used Up Alarm Threshold**, the system generates an alarm indicating that the storage pool capacity is about to be used up.

Step 6 Click **OK**.

Step 7 Confirm your operation as prompted.

----End

6.5.1.3 Modifying a Disk Pool

This section describes how to change the name of a disk pool.

Procedure

Step 1 Log in to DeviceManager.

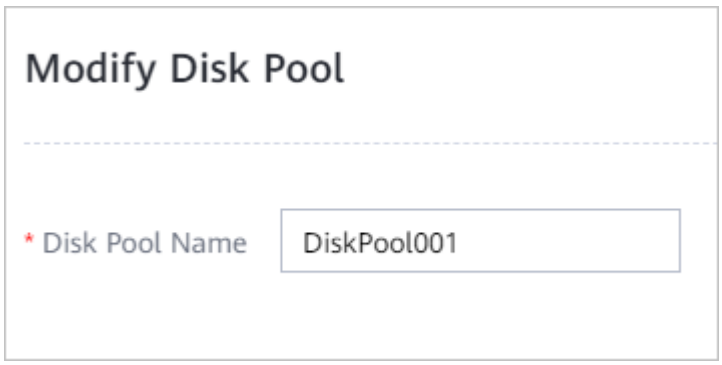
 Copyright © Huawei Technologies Co., Ltd.

Step 2 Choose **Resources** > **Resources** > **Storage Pool**.

Step 3 Click the name of the desired storage pool. On the page that is displayed, click the **Disk Pool** tab.

Step 4 Click **More** on the right of the desired disk pool and select **Modify**.

The **Modify Disk Pool** page is displayed.



Step 5 Change the disk pool name in **Disk Pool Name**.

NOTE

- The name must be unique.
- The name can contain only letters, digits, underscores (_), and hyphens (-).
- The name contains 1 to 64 characters.

Step 6 Click **OK**.

Step 7 Confirm your operation as prompted.

----End

6.5.1.4 Deleting a Storage Pool

This section describes how to delete a storage pool when it is no longer used.

Prerequisites

Before deleting a storage pool, check its status. If the storage pool status is **Migrating services**, the storage pool is being scaled in or out and cannot be deleted.

Before deleting a storage pool, ensure that you have disabled services in the storage pool. Before disabling any service:

- Uninstall the SmartIndexing service. For details, see **SmartIndexing Feature Guide for File/Object/HDFS** in the *OceanStor Pacific Series 8.2.1 Feature Guide*.
- Check whether the system is in upgrade mode. No service can be disabled in upgrade mode.
- Disable per-second performance monitoring and delete the configuration information. For details, see **6.5.7 Setting Per-Second Performance Monitoring for Converged Services**.

To disable services:

 Copyright © Huawei Technologies Co., Ltd.

1. Log in to the CLI and run the following command to stop the service:
   delete converged_eds_service general storage_pool_id=*Storage pool ID*
2. Run the following command to check whether the task is successfully stopped.
   show task info task_id=*Task ID*

   NOTE

   Storage pool ID can be obtained in **6.5.1.1 Viewing Storage Pool Information**, and *Task ID* can be obtained from the command output in **1**.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Resources** > **Storage Pool**.

Step 3 Click **More** on the right of the desired storage pool and select **Delete**.

Step 4 (Optional) In the displayed dialog box, click **Advanced** and select **Erase Data**.

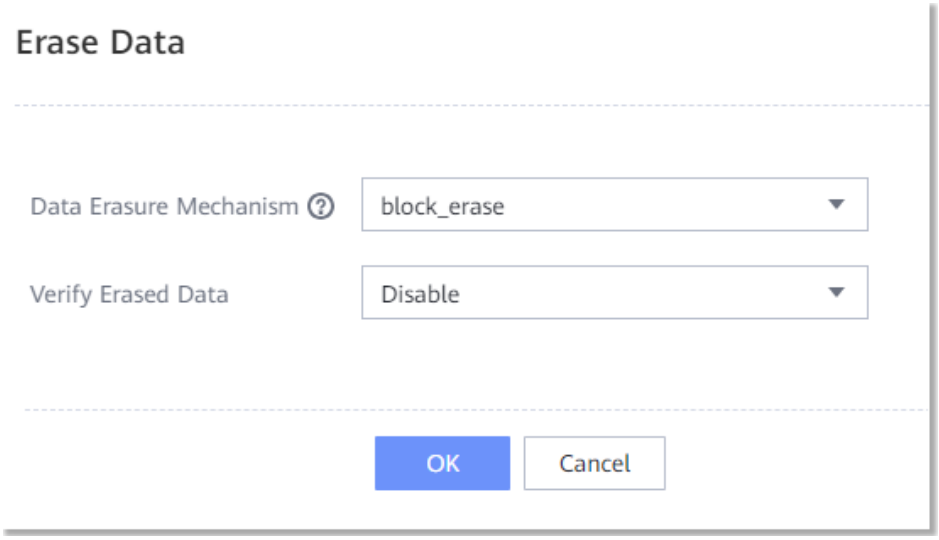
NOTICE

- You are about to delete the storage pool, and destroy data on disks in the storage pool. This operation will permanently destroy the data on the disks and the data cannot be restored. If you select **Erase Data**, the system will delete the storage pool and then erase data from all disks in the storage pool. Do not perform operations on involved disks during data erasing. If you do not select this option, the system will only delete the storage pool.
- Data erasure takes a long time. The time required with data erasure mechanisms **block_erase** and **cryptographic_erase** used is about 10 minutes, and that with data erasure mechanism **overwrite** used varies according to the configured parameters and disk capacity, which ranges from several to dozens of hours. During data erasure, you can choose **Cluster** > **Cluster** > **Hardware**, click the **Disks** tab in the lower part of the function pane, and view the data erasure progress in the **Data Erasure Progress** column of the disk in the disk information table.
- Do not clear the environment during data erasure. In case of an emergency, you can run the **clear_all_for_fsm_node.sh all forceClear** command to clear the environment. After the environment is forcibly cleared, if you restart the environment, the data erasure task will be lost. Therefore, exercise caution when determine whether to clear the environment.

1. Select **I have read and understand the consequences associated with performing this operation** and click **OK**.

   The **Erase Data** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.



2. Set data erasure parameters.
   Table 6-30 describes related parameters.

Table 6-30 Data erasure parameters

Parameter	Description
Data Erasure Mechanism	Disk data erasure method. Possible options are: – **cryptographic_erase**: erases security keys. This parameter is available only when the data encryption feature is enabled for the storage pool. – **block_erase**: erases disk data by block. User data and mappings are erased at the same time. – **overwrite**: overwrites disk data with specific pattern data. The erasure durations of the three data erasure mechanisms are different. For details, see **Data Security Feature** > **Secure Disk Data Erasure** in the *OceanStor Pacific Series 8.2.1 Security Configuration Guide*.
Data Erasure Standard	Standard for overwriting disk data. Possible options are **DoD 5220.22-M (E)**, **DoD 5220.22-M (ECE)**, **VSITR**, and **Custom**. This parameter is available only when **Data Erasure Mechanism** is set to **overwrite**. **NOTE** When **Data Erasure Standard** is set to **Custom**, the system will overwrite disk data according to the values of **Pattern** and **Overwrites**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Pattern	Pattern value used to overwrite disk data. The value is **r** or a one-byte hexadecimal number starting with **0x**. You can enter at most three values separated with commas (,). **NOTE** – This parameter is available only when **Data Erasure Standard** is set to **Custom**. – Value **r** indicates a random number.
Overwrites	Number of times the disk data is overwritten using the pattern value. The value ranges from 1 to 15. The default value is 1.
Verify Erased Data	Whether to enable function of verifying erased data. If this function is enabled, the system checks whether the data has been erased after the data erasure operation is complete. **NOTE** This parameter is unavailable when **Data Erasure Mechanism** is set to **cryptographic_erase**.
Data to Be Verified (%)	Percentage of the data to be verified to the total disk capacity. The value ranges from 1 to 100. The default value is 10. **NOTE** This parameter is available only when **Verify Erased Data** is set to **Enable**.

Step 5 Confirm your operation as prompted.

----End

6.5.2 Managing Certificates

When the storage system is communicating with an , you are advised to use the certificate verification mode to improve service security. This chapter describes how to generate and export certificate request files, and import and activate signed certificates.

6.5.2.1 Viewing Certificates

This section describes how to view the certificates of the current storage device.

Context

- On the certificate management page, you can click to refresh certificate information.
- On the certificate management page, click next to **Scenario** and enter a keyword to search for the required certificate information.

 Copyright © Huawei Technologies Co., Ltd.

- On the snapshot management page, you can click or next to a parameter to change the display order of snapshots.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Certificate** > **Certificate Management**.

Step 3 View imported certificate information. **Table 6-31** describes related parameters.

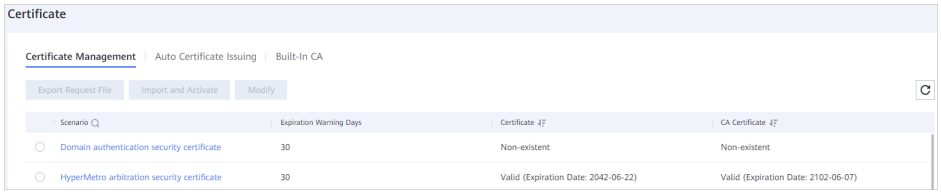


Table 6-31 Certificate parameters

Parameter	Description
Scenario	Scenario where a certificate is used.
Expiration Warning Days	Number of days before certificate expiration. When the period starts, the system sends warning to users about the expiration. The value ranges from 7 to 180, in unit of days.
Certificate	Validity and expiration date of a certificate. Possible values are **Valid**, **Non-existent**, and **Invalid**.
CA Certificate	Validity and expiration date of a CA certificate. Possible values are **Valid**, **Non-existent**, and **Invalid**.

Step 4 Click the desired certificate scenario. You can view the certificate details on the displayed **Certificate Details** page.

Table 6-32 describes related parameters.

Table 6-32 Certificate parameters

Parameter	Description
Auto Certificate Issuing	Whether to enable the automatic certificate issuing function.
Certificate Validity Period	Valid period of a certificate.
Common Name	Common name of a certificate.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Subject Alternative Name	Alternative name of a certificate.
Used By	User of a certificate.
Issued By	Issuer of a certificate.
Certificate Status	Validity and expiration date of a certificate.
Start Time	Start time of the certificate validity period.
SN	Serial number of a certificate.
Key Algorithm	Key algorithm of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Key Length	Key length of a certificate.
Fingerprint	Hashed value of the certificate content. This value is unique for every certificate. The certificate fingerprint is required to obtain the certificate, ensuring that content in the certificate has not been modified illegally. If the certificate fingerprint is different from that configured in the PKI domain, the device will refuse the certificate.

NOTE

The details page varies depending on the scenario. Refer to the actual page.

----End

6.5.2.2 Viewing Built-In CA Certificates

This section describes how to view details about built-in CA certificates.

Context

- On the built-in CA certificate management page, click to refresh the built-in CA certificate information.
- On the built-in CA certificate management page, click or next to a parameter and enter a keyword or select a parameter value to search for desired built-in CA certificates.
- On the built-in CA certificate management page, click and select specified built-in CA certificate parameters to be viewed.
- On the built-in CA certificate management page, click or next to a parameter to change the sequence of the parameter.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Certificate** > **Built-in CA**.

Step 3 View the built-in CA certificate information. **Table 6-33** describes related parameters.

Table 6-33 Built-in CA certificate parameters

Parameter	Description
Name	Name of a built-in CA certificate. The value of this parameter can be **RootCA**, **Web**, **Service**, **MicroService**, and **External**.
Type	Type of a built-in CA certificate. The value of this parameter can be **Root CA certificate** or **Subordinate CA certificate**. **NOTE** Only subordinate CA certificates can be used to issue digital certificates.
Issuer Certificate Name	Name of the issuer certificate. Subordinate CA certificates are issued by the root CA certificate.
Used By	User of a built-in CA certificate.
Key Algorithm	Key algorithm of a built-in CA certificate.
Start Time	Start time of the validity period of a built-in CA certificate.
Expiration Time	Expiration time of a built-in CA certificate.
SN	Serial number of a built-in CA certificate.
Signature Hash Algorithm	Signature algorithm used by a built-in CA certificate.
Status	Status of a built-in CA certificate.
Expiration Warning Days	Number of days before a CA certificate expires. When the period starts, the system sends warning to users about the expiration. The value ranges from 7 to 180, in unit of days.
Issued By	Issuer of a built-in CA certificate.
Fingerprint	Hashed value of the content of a built-in CA certificate. This value is unique for every certificate. When a device obtains a certificate, the certificate fingerprint is required to ensure that the certificate content is not tampered with by unauthorized users. If the certificate fingerprint is different from that configured in the PKI domain, the device will refuse the certificate.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Parameters **Expiration Warning Days**, **Issued By**, and **Fingerprint** are displayed only after you click the name of a built-in CA to go to the details page.

Step 4 Click the name of a built-in CA certificate to view its basic information and the digital certificates issued by it.

NOTE

The Root CA cannot issue digital certificates. Therefore, you will see no issued digital certificates after clicking the name of the Root CA.

----End

6.5.2.3 Exporting a Certificate Signing Request (CSR) File

This section describes how to export a certificate request file. After signing the file, you can import a new certificate.

Context

Only super administrators can export certificate request files.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Certificate** > **Certificate Management**.

Step 3 Select a desired certificate and click **Export Request File**.

The **Export Request File** page is displayed on the right.

NOTE

Request files cannot be exported for **SSO security certificate**, **DSwareTool security certificate**, **Object storage service maintenance API security certificate**, **Internal KMS certificate**, **Grafana service security certificate**, and **IAM security certificate**.

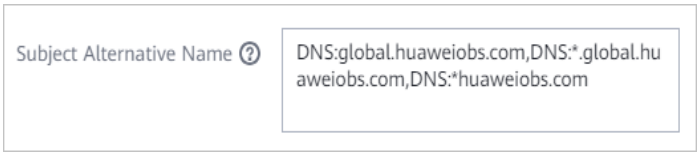
Step 4 Select a certificate key algorithm from the **Certificate Key Algorithm** drop-down list to encrypt the request file to be exported.

Step 5 Select **Advanced** in the upper right corner and set advanced parameters for exporting the certificate request file.

Table 6-34 describes related parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-34 Advanced request file parameters

Parameter	Description
Country	Value of the **country** parameter in the **subject** field when a CSR file is generated.
State or Province	Value of the **state or province name** parameter in the **subject** field when a CSR file is generated.
City or Locality	Value of the **locality** parameter in the **subject** field when a CSR file is generated.
Organization	Value of the **organization** parameter in the **subject** field when a CSR file is generated.
Organization Unit	Value of the **organizational unit** parameter in the **subject** field when a CSR file is generated.
Common Name	Value of the **common name** parameter in the **subject** field when a CSR file is generated. **NOTE** If the exported certificate is **Object storage service security certificate**, the value of **common name** in the **subject** field is the global domain name of the object storage service.
Subject Alternative Name	Subject Alternative Name (SAN) is an extensible field (defined in the SSL standard X.509) during CSR file generation. The SSL certificate that uses the **Subject Alternative Name** field can extend the domain names supported by the certificate so that one certificate can support the resolution of multiple domain names. In the scenario where multiple clusters are deployed for the object service, you can configure global, region, and cluster domain names at the same time, or use wildcards (*). Use commas (,) to separate multiple domain names. For example: 

Step 6 Click **OK**.

----End

6.5.2.4 Using Built-In CA to Issue Digital Certificates

This section describes how to use built-in CA certificates to issue digital certificates.

Prerequisites

You can only use subordinate CA certificates to issue digital certificates.

 Copyright © Huawei Technologies Co., Ltd.

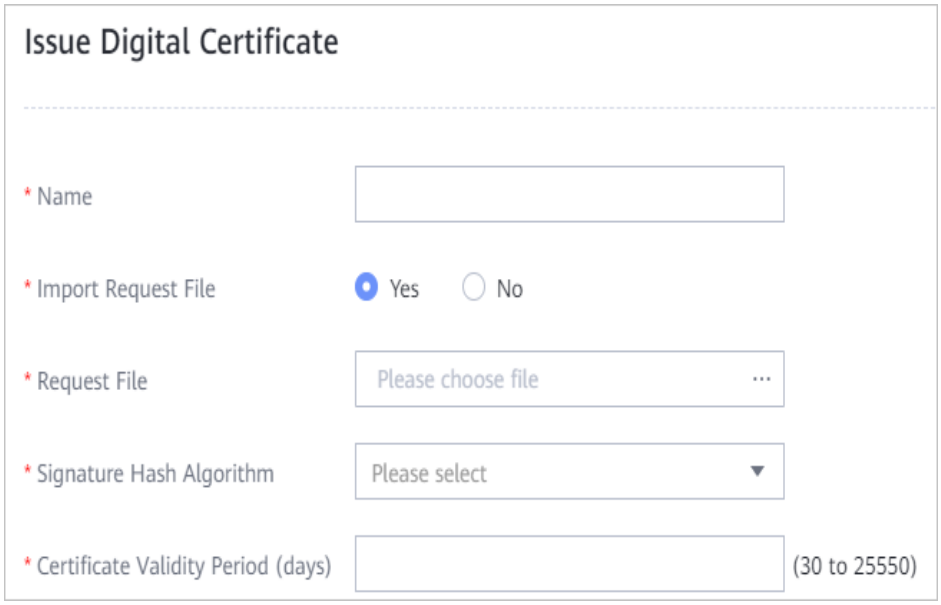
Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Certificate** > **Built-In CA**.

Step 3 Select a subordinate CA certificate that you want to use to issue a digital certificate and click **Issue Digital Certificate**.

The **Issue Digital Certificate** page is displayed on the right.



Step 4 Set the certificate parameters. **Table 6-35** describes related parameters.

Table 6-35 Parameters for issuing a certificate

Parameter	Description
Name	Name of the digital certificate to be issued. **NOTE** • The name consists of 4 to 63 characters. • The name can contain only letters, digits, underscores (_), and hyphens (-).
Import Request File	Select whether to import the request file as required.
Request File	If **Yes** is selected in **Import Request File**, you need to select and import a request file.
Request Content	If **No** is selected in **Import Request File**, you need to enter the request file content.
Signature Hash Algorithm	Select the signature algorithm to be used by the digital certificate. The options include **SHA256** or **SHA512**.
Certificate Validity Period (days)	Set the validity period of the digital certificate. The value ranges from 30 to 25,550 days.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Click **OK**.

Step 6 Click **Export Issued Certificate** to download the certificate.

Step 7 Click **Close**.

----End

6.5.2.5 Exporting Issued Digital Certificates

This section describes how to export digital certificates issued by a built-in CA certificate.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Certificate** > **Built-In CA**.

Step 3 Click the name of a CA certificate. The CA certificate details page is displayed.

Step 4 In the **List of Issued Certificates** area, select the certificates to be exported and click **Export Issued Certificate**.

----End

6.5.2.6 Exporting a Built-In CA Certificate

This section describes how to export a specified built-in CA certificate.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Certificate** > **Built-In CA**.

Step 3 Select a CA certificate to be exported and click **Export CA Certificate**.

----End

6.5.2.7 Importing and Activating a Certificate

When the storage system is communicating with an , you are advised to use the certificate verification mode to improve service security. It is recommended that you replace the default security certificate with a certificate applied from an official authority and replace the certificate that has expired or is about to expire in a timely manner. This section describes how to import and activate a certificate.

Context

- Only super administrators can import and activate certificates.
- In the multi-cluster scenario, when importing security certificates of the same type to different clusters, ensure that the certificate file, CA certificate file, and private key file imported to each cluster are the same.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

- When updating the security certificate of an internal service, wait until the certificate update is complete (that is, until the system records a log indicating that the certificate update is successful or failed) before updating certificates in other scenarios.
- During certificate update, you must not scale in or out a cluster, replace components, or power on or off a cluster.
- During certificate update, the module that uses the certificate will restart. As a result, some services may be unavailable for a short period of time in this process.
- If the OceanStor Pacific series storage system and data pilot service are upgraded from 8.1.2 to 8.1.3 or a later version at the same time or a new OceanStor Pacific series 8.1.3 storage system or a later version is deployed, data pilot service is unavailable when the internal system service security certificate is imported and activated.
- If the OceanStor Pacific series data pilot service is upgraded from 8.1.0 or 8.1.1 to 8.1.3 or a later version, you need to manually replace the Elasticsearch certificate. For details, see **Manually Replacing REST layer TLS** or **Manually Replacing Transport layer TLS** in the security configuration guide of the corresponding version.
- Before importing and activating the internal system service security certificate, FSM security certificate, and internal KMS certificate, ensure that the storage nodes and compute nodes have consistent software versions. For details, see **Appendix > Checking Software Version Consistency Between Storage Nodes and Compute Nodes** in the *Security Configuration Guide* of the corresponding version.

Prerequisites

1. You have obtained the request file. For details, see **6.5.2.3 Exporting a Certificate Signing Request (CSR) File**.
2. After exporting the request file, you have issued a certificate file through the CA and obtained the issued digital certificate and CA certificate of the CA:
   - Issue a certificate using the built-in CA of the storage system:
     i. Issue a certificate by following instructions in **6.5.2.4 Using Built-In CA to Issue Digital Certificates**.
     ii. Export the certificate file by following instructions in **6.5.2.5 Exporting Issued Digital Certificates**.
     iii. Export the CA certificate file by following instructions in **6.5.2.6 Exporting a Built-In CA Certificate**.
   - Use the customer's CA or a trusted third-party CA to issue a certificate: Send the request file to the customer's CA or a trusted third-party CA to generate a certificate file and obtain the CA certificate.

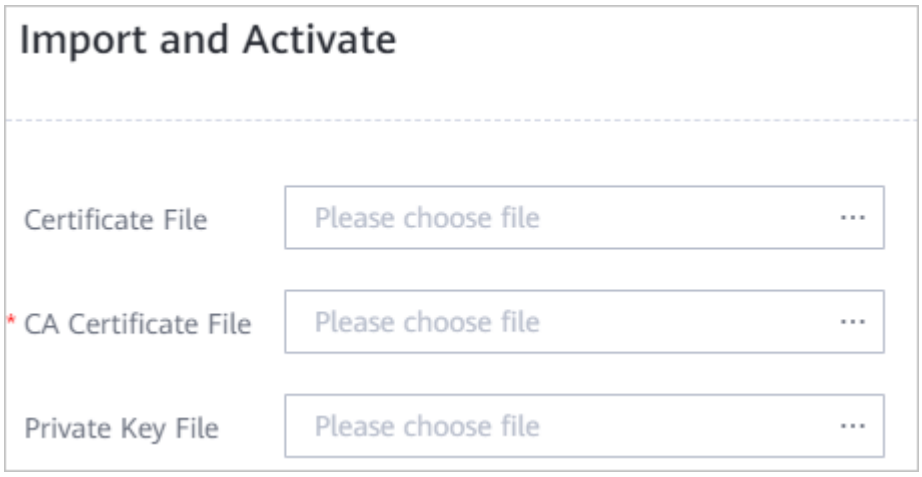
Procedure

Step 1 Log in to DeviceManager.

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Choose **Settings** > **Certificate** > **Certificate Management**.

Step 3 Select a desired certificate and click **Import and Activate**.



NOTE

- The prompt messages for importing and activating certificates vary in different scenarios. This online help uses importing and activating HyperMetro arbitration certificates as an example.
- When a customer updates the DeviceManager and DswareTool certificates, if a third-party NMS connects to the storage system through a RESTful API and the customer wants to obtain the complete certificate chain information during link negotiation, the imported certificate must contain the complete certificate chain information. To obtain the complete certificate chain file, perform the following steps:
  1. Use Notepad to open the server certificate, intermediate CA certificate, and root CA certificate.
  2. Add the intermediate CA certificate and root CA certificate to the server certificate file based on the SSL certificate chain format. Generally, an organization describes the complete certificate chain format when issuing a certificate. For details, see related rules. The common format is as follows (there is no blank line between certificates):

     -----BEGIN CERTIFICATE-----

     Server certificate

     -----END CERTIFICATE-----

     -----BEGIN CERTIFICATE-----

     Intermediate CA certificate

     -----END CERTIFICATE-----

     -----BEGIN CERTIFICATE-----

     Root CA certificate

     -----END CERTIFICATE-----
  3. Save the server certificate to obtain a certificate that contains a complete certificate chain.

Step 4 (Optional) Select when importing the CA certificates of the **access certificate** and **service certificate** scenarios.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

If you want to add multiple with the same management IP address, import the same access CA certificate for each . Otherwise, a verification exception may occur, and device details cannot be obtained.

NOTE

Click **Add Now**. The page for adding is displayed. You can add .

Step 5 Set **Certificate File**, **CA Certificate File**, and **Private Key File** as required.

NOTE

Only plaintext private keys are supported.

Step 6 Click **OK**.

NOTE

- After you import and activate a certificate in one scenario, choose **Monitor** > **Alarms and Events** > **Events**. Wait until certificate import success, certificate activation success, and certificate update success events are displayed in sequence, and then import and activate the certificate in the next scenario. Before a certificate is updated, related service operations may fail. Try again after the certificate is updated.
- HA-related alarms may be generated during the update of **Internal system service security certificate**. The alarms will be automatically cleared after the certificate is updated.

----End

6.5.2.8 Modifying a Certificate

This section describes how to change the expiration warning days or private key encryption password of a certificate.

Context

Only super administrators can modify certificates.

Prerequisites

A valid certificate or CA certificate can be modified.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Certificate** > **Certificate Management**.

Step 3 Select the desired certificate and click **Modify**.

The **Modify Certificate** dialog box is displayed on the right.

Step 4 Change the status of **Auto Certificate Issuing**. After this function is enabled, you need to set **Certificate Validity Period**, **Common Name**, and **Subject Alternative Name**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

This operation is supported only in some scenarios. Follow the actual page.

Step 5 Modify **Expiration Warning Days**, **New Private Key Encryption Password**, and **Confirm Password** as required.

Step 6 Click **OK**.

----End

6.5.2.9 Deleting an Issued Digital Certificate

This section describes how to delete a digital certificate that is no longer needed.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Certificate** > **Built-In CA**.

Step 3 Click the name of a CA certificate. The CA certificate details page is displayed.

Step 4 In the **List of Issued Certificates** area, select a certificate to be deleted and click **Delete**.

----End

6.5.2.10 Auto Certificate Issuing

After this function is enabled, the system automatically initiates a certificate update request to update a certificate when it is about to expire.

Precautions

Before initiating a certificate update request in a scenario, ensure that the **Auto Certificate Issuing** function has been enabled for both the system and the scenario.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Certificate** > **Auto Certificate Issuing**.

Step 3 Enable **Auto Certificate Issuing** and configure parameters.

NOTE

After **Auto Certificate Issuing** is disabled, the system does not initiate automatic certificate update requests.

Step 4 Click **Modify** to modify the configuration information.

NOTE

This operation is required if **Auto Certificate Issuing** is not enabled for the first time.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Set **Days Before Auto Update**. When the number of days that a certificate is about to expire reaches the value of this parameter, the system automatically triggers a certificate update.

Step 6 Configure the CA server that issues certificates. **Table 6-36** describes related parameters.

Table 6-36 CA server parameters

Parameter	Description
IP Address	IP address of the CA server. IPv4 and IPv6 addresses are supported.
Port	Port number of the CA server.
Path	Path of the CA server.

Step 7 Import the CA server certificate. Import **Certificate File**, **CA Certificate File**, and **Private Key File**.

NOTE

If a CA server certificate has been imported, you can select **Import New Certificate** to import a new one.

Step 8 If a CA server certificate has been imported, determine whether to change the private key encryption password of the certificate. If you need to change the password, select **Modify Private Key Encryption Password** and specify **New Private Key Encryption Password** and **Confirm Password**.

Step 9 Click **Save**.

----End

6.5.2.11 Replacing the HyperMetro Arbitration Security Certificate

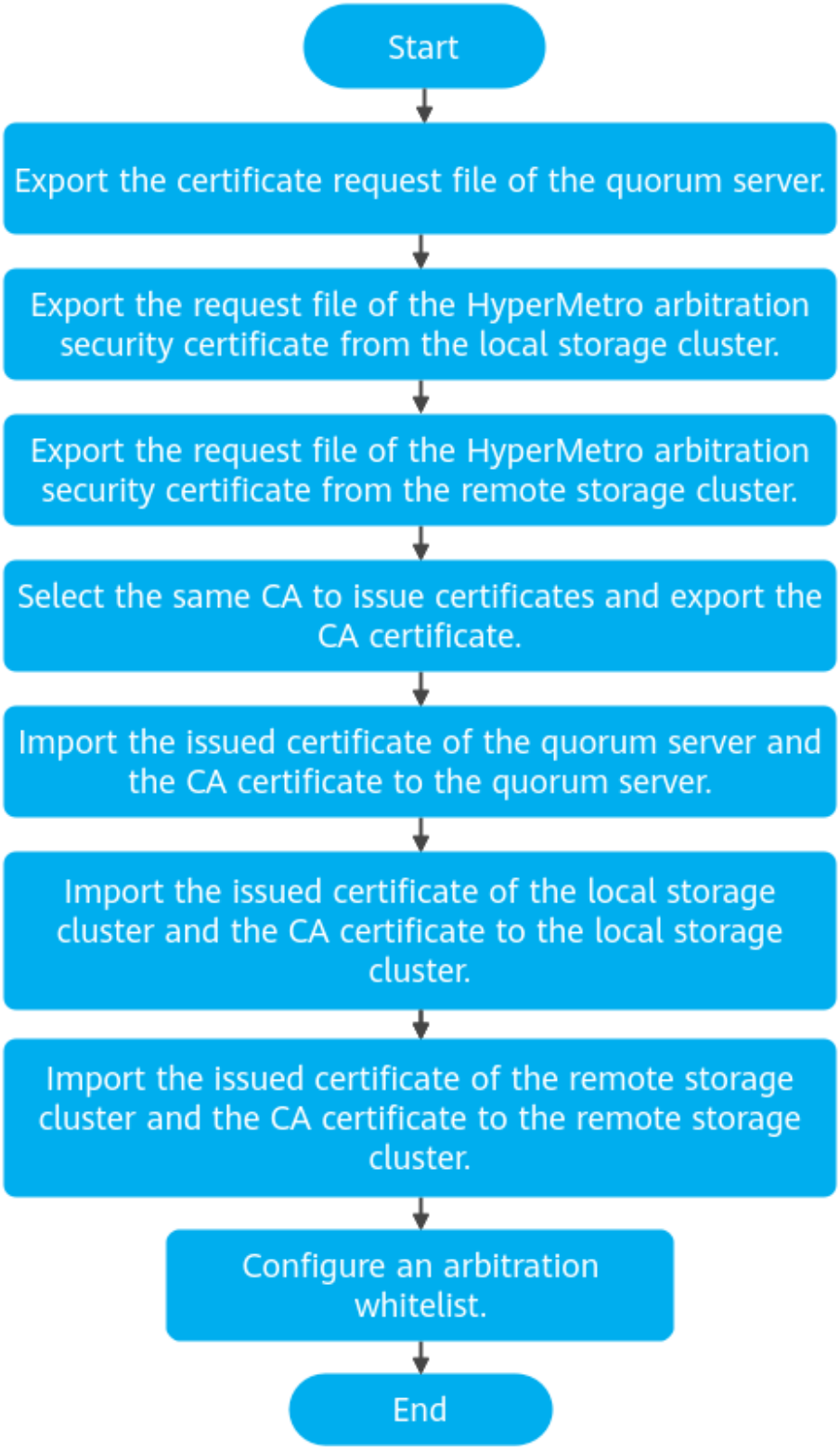
Prerequisites

- The quorum server software must be configured under the same user used to install it.
- If the quorum server or storage cluster is newly installed in OceanStor Pacific 8.1.3 or a later version, you must replace the HyperMetro arbitration security certificate. If the quorum server or storage cluster is upgraded from OceanStor Pacific 8.1.2 or an earlier version and the HyperMetro arbitration security certificate has never been replaced, replacing the HyperMetro arbitration security certificate is optional. If the quorum server or storage cluster is upgraded from OceanStor Pacific 8.1.2 or an earlier version and the HyperMetro arbitration security certificate has been replaced, you must update the certificate when the original certificate of the quorum server or storage cluster does not match the current version.

 Copyright © Huawei Technologies Co., Ltd.

Process Flow

Figure 6-7 Process flow of replacing the HyperMetro arbitration security certificate



 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Export the certificate request file of the quorum server.

In the CLI of the quorum server software, run the **export tls_cert** command to export the device information. The **qs_certreq.csr** file is generated in the **/opt/quorum_server/export_import** directory on the quorum server.

```
admin:/>export tls_cert
Command executed successfully.
```

NOTE

- The certificates must be replaced in user mode where the quorum server software is running.
- After installing the quorum server software, you are advised to grant the SFTP permission only to the **/opt/quorum_server/export_import/** directory. This allows the security certificates to be imported and exported.

Step 2 Log in to DeviceManager of the local storage cluster and export the certificate request file of the local storage cluster in the **HyperMetro arbitration security certificate** scenario. For details, see **6.5.2.3 Exporting a Certificate Signing Request (CSR) File**.

Step 3 Log in to DeviceManager of the remote storage cluster and export the certificate request file of the remote storage cluster in the **HyperMetro arbitration security certificate** scenario. For details, see **6.5.2.3 Exporting a Certificate Signing Request (CSR) File**.

Step 4 Select a certificate authority (CA) and use the certificate request files to generate certificates.

NOTICE

- To ensure normal and secure communication between devices, the quorum server and the storage clusters must use the same CA to issue certificates.
- This section describes three methods for issuing certificates. You are advised to use the customer's CA or a trusted third-party CA. If no CA is available, use the built-in CA of the quorum server or the built-in CA of a storage cluster.

- When using the customer's CA or a third-party CA to issue certificates:
  a. Send certificate request file **qs_certreq.csr** of the quorum server to the customer's CA or the third-party CA to generate the certificate of the quorum server.
  b. Send the certificate request file of the local storage cluster to the customer's CA or the third-party CA to generate the certificate of the local storage cluster.
  c. Send the certificate request file of the remote storage cluster to the customer's CA or the third-party CA to generate the certificate of the remote storage cluster.
- When using the built-in CA of the quorum server to issue certificates:
  – To issue certificates one by one, perform steps **a** to **c** to issue the certificates of the quorum server, local storage cluster, and remote storage cluster, respectively:

 Copyright © Huawei Technologies Co., Ltd.

i. Copy the certificate request file (for example, **qs_certreq.csr**) to the **/opt/quorum_server/export_import** directory on the quorum server, change the owner and owner group of the certificate request file to the installation user and owner group of the quorum server software, and ensure that the certificate request file can be read.

```
chown quorumsvr:quorumsvr qs_certreq.csr
```

NOTE

In this example, **quorumsvr** is the default installation user of the quorum server software. Change it to the actual user and user group you use to install the quorum server software.

ii. Run the **generate tls_cert csr=***qs_certreq.csr* **[days=***1095***] [cert_name=***qs_certreq.crt***] [sign_algorithm=***0***]** command to issue the certificate.

NOTE

- **csr** (mandatory): specifies the name of the certificate request file. The file needs to be stored in a specified location. Its name can contain letters, digits, periods (.), hyphens (-), and underscores (_), and must start with a letter or digit and end with **.csr**.
- **days** (optional): specifies the validity period of the certificate. The value can only contain digits.
- **cert_name** (optional): specifies the name of the certificate file to be issued. The file needs to be stored in a specified location. Its name can contain letters, digits, periods (.), hyphens (-), and underscores (_), and must start with a letter or digit and end with **.crt**.
- **sign_algorithm** (optional): specifies the signature algorithm suite required by users. This parameter is related to the generation of the CA private key. The value can be **SHA256RSA** or **SHA256ECDSA**.

  0. **SHA256RSA**

  1. **SHA256ECDSA**

```
admin:/>generate tls_cert csr=qs_certreq.csr cert_name=qs_certreq.crt
Command executed successfully.
```

iii. Obtain the issued certificate and CA certificate file from the **/opt/quorum_server/export_import** directory on the quorum server. In this example, **qs_certreq.crt** (or a specified name) is the certificate file, and **cps_ca.crt** is the CA certificate file.

– To issue certificates in batches:

i. Copy certificate request files (for example, **qs_certreq.csr**, **qs_certreq_1.csr**, and **qs_certreq_2.csr**) of the quorum server, local storage cluster, and remote storage cluster to the **/opt/quorum_server/export_import** directory on the quorum server. Change the owner and owner group of the certificate request files to the installation user and owner group of the quorum server software, and ensure that the certificate request files can be read.

```
chown quorumsvr:quorumsvr *.csr
```

NOTE

In this example, **quorumsvr** is the default installation user of the quorum server software. Change it to the actual user and user group you use to install the quorum server software.

 Copyright © Huawei Technologies Co., Ltd.

ii. Run the **generate tls_cert_multi [days=*1095*] [sign_algorithm=*0*]** command to issue certificates in batches.

NOTE

- A certificate request file can be issued successfully only when its name meets the following requirements: The file needs to be stored in a specified location. Its name can contain letters, digits, periods (.), hyphens (-), and underscores (_), and must start with a letter or digit and end with **.csr**.
- **days** (optional): specifies the validity period of the certificate. The value can only contain digits.
- **sign_algorithm** (optional): specifies the signature algorithm suite required by users. This parameter is related to the generation of the CA private key. The value can be **SHA256RSA** or **SHA256ECDSA**.

  0. **SHA256RSA**

  1. **SHA256ECDSA**

```
admin:/>generate tls_cert_multi
[SUCCEED]generate cert for csr file:[qs_certreq.csr] succeed!
[SUCCEED]generate cert for csr file:[qs_certreq_1.csr] succeed!
[SUCCEED]generate cert for csr file:[qs_certreq_2.csr] succeed!
------all 3 csr files<succeed 3 files and failed 0 files>------
Command executed successfully.
```

iii. Obtain the issued certificates and CA certificate file from the **/opt/quorum_server/export_import** directory on the quorum server. In this example, **qs_certreq.crt**, **qs_certreq_1.crt**, and **qs_certreq_2.crt** are the certificate files (with the same names as the request files), and **cps_ca.crt** is the CA certificate file.

```
ll /opt/quorum_server/export_import
total 28
-rw-r--r--. 1 quorumsvr quorumsvr 1927 Jun  3 09:03 cps_ca.crt
-rw-r--r--. 1 quorumsvr quorumsvr 1476 Jun  3 09:03 qs_certreq_2.crt
-r--------. 1 quorumsvr quorumsvr  976 Jun  3 09:00 qs_certreq_2.csr
-rw-r--r--. 1 quorumsvr quorumsvr 1476 Jun  3 09:03 qs_certreq_1.crt
-r--------. 1 quorumsvr quorumsvr  976 Jun  3 09:00 qs_certreq_1.csr
-rw-r--r--. 1 quorumsvr quorumsvr 1476 Jun  3 09:03 qs_certreq.crt
-r--------. 1 quorumsvr quorumsvr  976 Jun  3 08:55 qs_certreq.csr
```

- When using the built-in CA of a storage cluster to issue certificates (the local storage cluster is used as an example):

  a. Log in to DeviceManager of the local storage cluster, choose **Settings** > **Certificate** > **Built-In CA**, and use the subordinate CA certificate named **External** to issue certificates of the quorum server, local storage cluster, and remote storage cluster. For details, see **6.5.2.4 Using Built-In CA to Issue Digital Certificates**.

  b. Export the issued digital certificates of the quorum server, local storage cluster, and remote storage cluster. For details, see **6.5.2.5 Exporting Issued Digital Certificates**.

  c. Export the subordinate CA certificate named **External** in the local storage cluster. For details, see **6.5.2.6 Exporting a Built-In CA Certificate**.

Step 5 Import the issued certificate of the quorum server and the CA certificate to the quorum server.

1. Copy the certificate of the quorum server to the quorum server.

   After the certificates are generated, copy the digital certificate of the quorum server (for example, **qs_cert.crt**) and the CA certificate (for example, **cps_ca.crt**) to the **/opt/quorum_server/export_import** directory.

 Copyright © Huawei Technologies Co., Ltd.

2. Import the certificate of the quorum server to the quorum server software.

   In the CLI of the quorum server software, run the **import tls_cert cert_name=hm_third_cert ca=***cps_ca.crt* **cert=***qs_cert.crt* **[private_key=***privateKeyFileName***] class=hm** command to import the certificate to the quorum server software.

   ```
   admin:/>import tls_cert cert_name=hm_third_cert ca=cps_ca.crt cert=qs_cert.crt class=hm
   Command executed successfully.
   ```

   NOTE

   When importing a HyperMetro certificate, you must set **cert_name** to **hm_third_cert** and **class** to **hm**.

Step 6 Log in to DeviceManager of the local storage cluster, select the **HyperMetro arbitration security certificate** scenario, and import the issued certificate of the local storage cluster and the CA certificate. For details, see **6.5.2.7 Importing and Activating a Certificate**.

Step 7 Log in to DeviceManager of the remote storage cluster, select the **HyperMetro arbitration security certificate** scenario, and import the issued certificate of the remote storage cluster and the CA certificate. For details, see **6.5.2.7 Importing and Activating a Certificate**.

Step 8 After certificate replacement is complete, you need to reconfigure an arbitration whitelist. For details, see **Configuring an Arbitration Whitelist** in the product documentation of the corresponding version.

----End

6.5.2.12 Deleting the CA Certificate of

This section describes how to delete the access and service CA certificates of .

Prerequisites

- A CA certificate has been imported for the **access certificate** or **service certificate** scenario.
- Do not delete the CA certificate when the is providing services.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Certificate** > **Certificate Management**.

Step 3 Click the name of the **access certificate** or **service certificate** scenario.

The **Certificate Details** page is displayed on the right.

Step 4 On the **CA Certificate** tab page, select one or more CA certificates to be deleted and click **Delete**.

NOTE

You can also click **More** on the right of a desired CA certificate and select **Delete**.

Step 5 Confirm your operation as prompted.

----End

 Copyright © Huawei Technologies Co., Ltd.

6.5.3 Managing DPC Nodes

This section describes how to manage DPC compute nodes.

6.5.3.1 Viewing Nodes

This section describes how to view node information.

Context

- On the node management page, click to refresh nodes.
- On the Node Management page, you can click to export a list of nodes.
- On the node management page, click or next to a parameter and enter a keyword or select a parameter value to search for desired nodes.
- On the storage pool management page, click or next to a parameter to change the display order of storage pools.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Access** > **DPC**.

Step 3 View the DPC compute nodes in the function pane. **Table 6-37** describes related parameters.

Table 6-37 DPC node parameters

Parameter	Description
IP Address	IP address of a node.
Status	Status of a node. • Normal
FSA	Whether to enable the FSA process.
Memory	Memory of a DPC node.

----End

6.5.3.2 Enabling FSA

This section describes how to start the FSA process on a DPC node for DPC node configuration.

Precautions

Enabling the FSA process compromises system performance. Therefore, you are advised to enable the FSA process when configuring a DPC node and disable the FSA process after the configuration is complete.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Resources** > **Access** > **DPC**.

Step 2 Select one or more desired DPC nodes and click **Enable FSA**.

NOTE

You can also click **More** on the right of a desired node and select **Enable FSA**.

Step 3 Confirm your operation as prompted.

----End

6.5.3.3 Disabling FSA

If you do not need to configure a DPC node, you can perform this operation to stop the FSA process on the node.

Procedure

Step 1 Choose **Resources** > **Access** > **DPC**.

Step 2 Select one or more desired DPC nodes and click **Disable FSA**.

NOTE

You can also click **More** on the right of a desired node and select **Disable FSA**.

Step 3 Confirm your operation as prompted.

----End

6.5.3.4 Deleting DPC

This section describes how to stop the DPC process on a node.

Prerequisites

The FSA process on the node has been started or **Status** of the node is .

Procedure

Step 1 (Optional) If a namespace is mounted to the node where the DPC process resides, you need to unmount it from the node first.

1. Log in to the desired compute node where the DPC process resides as a common user and switch to user **root**.

   NOTE

   - Stop services before performing the unmount operation.
   - No DPC mount point can be unmounted in a container.

2. Run the following command to query the directories to be unmounted. In the command output, if **type** of a directory is **dpc**, the directory needs to be unmounted.

 Copyright © Huawei Technologies Co., Ltd.

mount |grep dpc

```
[root@kwephdfs00522 ~]# mount |grep dpc
/dpcfs on /mnt/fs1 type dpc (rw,relatime)
```

3. Unmount the mounted directory.

umount */mnt/fs1*

```
[root@kwephdfs00522 ~]#umount /mnt/fs1
```

NOTE

- If the unmount operation fails, try again or contact technical support engineers. You must not run the **umount -l** or **umount -f** command to forcibly unmount a DPC mount point.
- To obtain contact information of Huawei technical support center, visit **https://support.huawei.com** (for carrier users) or **https://support.huawei.com/enterprise** (for enterprise users). After logging in to the preceding website, you can select an area to obtain the technical support contact information of the area.

Step 2 Log in to DeviceManager.

Step 3 Choose **Resources** > **Access** > **DPC**.

Step 4 Select one or more desired nodes from which you want to delete the DPC process and click **Delete DPC**.

NOTE

- You can also click **More** on the right of a desired node and select **Delete DPC** to delete the DPC process.
- After unmounting the namespace from the node where the DPC process resides, wait for about 5 minutes before performing the deletion. Otherwise, the DPC process may fail to be deleted.

Step 5 Confirm your operation as prompted.

NOTE

- If the status of a node where the DPC process resides is , you can select to forcibly delete the DPC process.
- After deleting a DPC node whose status is , you need to clear the related alarms manually.
- You can click **Create DPC** and select **Existing Node** to add a deleted DPC node again.
- Deleting a DPC node only stops the DPC process on the node. For details about how to remove the node, see **6.5.4 Removing a Node**.

----End

6.5.4 Removing a Node

This section describes how to remove a node from the cluster.

Prerequisites

If the node to be removed is used in a storage pool, VBS, DR service, DPC, management cluster, or service network, you need to remove the node from all related modules first, ensuring that all services on the node have been cleared.

Procedure

Step 1 On the menu bar, click and select **Remove Node**.

The **Remove Node** page is displayed.

Step 2 Authenticate the nodes to be removed.

1. Select the desired nodes and click **Authenticate**.

   The **Authentication** dialog box is displayed.

2. Set **Username**, **Password**, and **Password of root** as required.

   NOTE

   The user name, password, and root password must be the same as those for authentication when you add a node.

3. Click **OK**.

NOTE

When removing a pre-installed DPC compute node, you can choose not to perform authentication. If authentication is not required, you are advised to perform the following operations to clear the DPC node:

1. Log in to a compute node through the management IP address as user **root**. If you have logged in as another user, run the **su - root** command to switch to user **root**.
2. Run the following command to check whether the **clear_all_for_fs_manual.sh** script exists. The following example indicates that the script exists.
   ```
   [root@localhost ~]# ls -l /opt/fusionstorage/deploymanager/clouda/clear_all_for_fs_manual.sh
   -r-x------. 1 root root 258 Apr 21 10:46 /opt/fusionstorage/deploymanager/clouda/
   clear_all_for_fs_manual.sh
   ```
3. If the script exists, run the following commands to uninstall the node.
   ```
   cd /opt/fusionstorage/deploymanager/clouda
   bash clear_all_for_fs_manual.sh
   ```
4. If the script does not exist, run the following commands to uninstall the node.
   ```
   cd /opt/fusionstorage/deploymanager/clouda
   bash clear_all_for_fs_node.sh all
   ```

Step 3 Click **Remove**.

Step 4 Confirm your operation as prompted.

NOTE

If the duration for removing multiple nodes exceeds the session timeout duration set in the security policy and the user does not perform any operation (for example, moving the mouse) on DeviceManager, the security policy is triggered and DeviceManager automatically exits to the login page. In this case, log in to DeviceManager and remove the nodes that are not removed.

----End

6.5.5 Viewing VXLAN Information

This section describes how to view basic information about created VXLANs.

 Copyright © Huawei Technologies Co., Ltd.

Context

- On the VXLAN management page, click to refresh VXLANs.
- On the VXLAN management page, click next to a parameter and enter a keyword to search for desired VXLANs.
- On the VXLAN management page, click and select desired VXLAN parameters to be viewed.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Access** > **VXLAN**.

Step 3 View the VXLANs in the function pane. **Table 6-38** describes related parameters.

Table 6-38 VXLAN parameters

Parameter	Description
Management IP Address	Management IP address of a storage node.
Status	VXLAN status. The value can be **Running**, **Starting**, **Stopping**, or **Start/Stop failed**. **NOTE** If the status is **Start/Stop failed**, check the VXLAN configuration of the node, remove the VXLAN, and add it again.
Health Check IP Address/Mask	IP address and mask configured on a storage node for checking the health status of the node. The IP address and mask are used for VPC EP2.0 load balancing.
Health Check Gateway	Gateway of the health check IP address.
Service IP Address/ Mask	Service IP address and mask, to be used by an NFS/CIFS client to mount the file service.
VXLAN Tunnel IP Address/Mask	VTEP IP address used to establish a VXLAN tunnel between nodes. The VTEP IP addresses of the nodes can communicate with each other.
VXLAN Tunnel Gateway	Gateway corresponding to the VXLAN tunnel IP address.
VXLAN Tunnel VLAN ID	VLAN ID of the service plane.
Destack Networking	If the value is **Yes**, switches are not stacked. If the value is **No**, switches are stacked.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Click the management IP address of a storage node to view its basic VXLAN information.

----End

6.5.5.1 Viewing VXLAN Information

This section describes how to view basic information about created VXLANs.

Context

- On the VXLAN management page, click to refresh VXLANs.
- On the VXLAN management page, click next to a parameter and enter a keyword to search for desired VXLANs.
- On the VXLAN management page, click and select desired VXLAN parameters to be viewed.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Access** > **VXLAN**.

Step 3 View the VXLANs in the function pane. **Table 6-39** describes related parameters.

Table 6-39 VXLAN parameters

Parameter	Description
Management IP Address	Management IP address of a storage node.
Status	VXLAN status. The value can be **Running**, **Starting**, **Stopping**, or **Start/Stop failed**. **NOTE** If the status is **Start/Stop failed**, check the VXLAN configuration of the node, remove the VXLAN, and add it again.
Health Check IP Address/Mask	IP address and mask configured on a storage node for checking the health status of the node. The IP address and mask are used for VPC EP2.0 load balancing.
Health Check Gateway	Gateway of the health check IP address.
Service IP Address/ Mask	Service IP address and mask, to be used by an NFS/CIFS client to mount the file service.
VXLAN Tunnel IP Address/Mask	VTEP IP address used to establish a VXLAN tunnel between nodes. The VTEP IP addresses of the nodes can communicate with each other.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
VXLAN Tunnel Gateway	Gateway corresponding to the VXLAN tunnel IP address.
VXLAN Tunnel VLAN ID	VLAN ID of the service plane.
Destack Networking	If the value is **Yes**, switches are not stacked. If the value is **No**, switches are stacked.

NOTE

Click the management IP address of a storage node to view its basic VXLAN information.

----End

6.5.5.2 Removing a VXLAN

This section describes how to remove a VXLAN.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Access** > **VXLAN**.

Step 3 Select one or more desired VXLANs and click **Remove**.

NOTE

You can also click **More** on the right of a desired VXLAN and select **Remove**.

Step 4 Confirm your operation as prompted.

Step 5 Click **Close**.

----End

6.5.6 Managing the External Key Service

After the external key service is configured, you can select an external key management server to manage keys when creating a self-encrypting storage pool or enabling data encryption for an account.

Prerequisites

The external key service is supported only when an advanced license is imported.

Procedure

Step 1 Log in to DeviceManager.

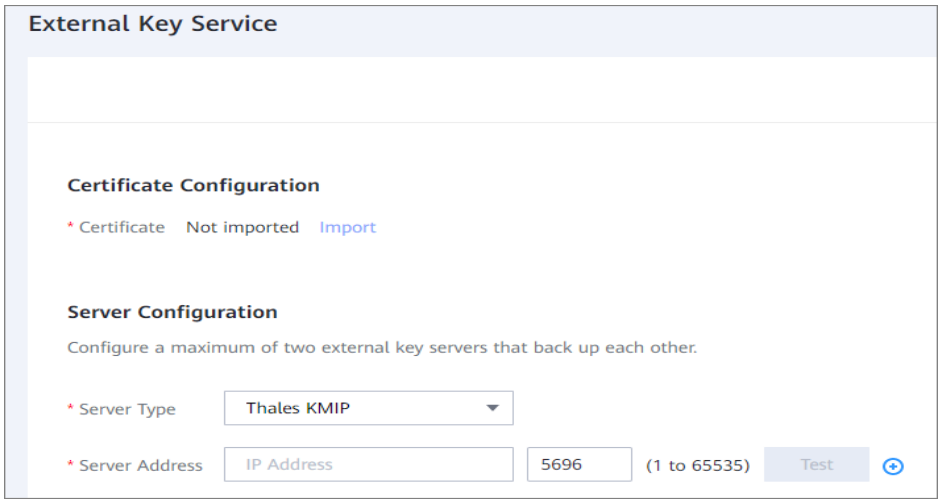
 Copyright © Huawei Technologies Co., Ltd.

Step 2 Choose **Settings** > **External Key Service**.

Step 3 Click **Edit**.

The **External Key Service** page is displayed, as shown in **Figure 6-8**.

Figure 6-8 External key service



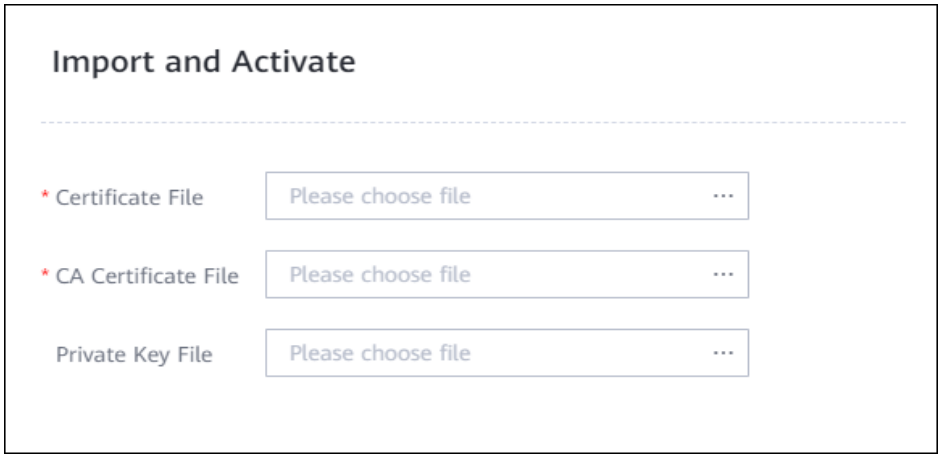
NOTE

If an external key management server has been configured, you can click **Modify** to modify its settings.

To modify a configured external key management server, delete it and then add a new one.

Step 4 Click **Import**. The **Import and Activate** page is displayed, as shown in **Figure 6-9**. Set **Certificate File**, **CA Certificate File**, and **Private Key File** of the external key service and click **OK**.

Figure 6-9 Importing and activating certificates



NOTE

If the external key service certificates have been imported, click **Re-import** to update the certificates.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Select the type of the external key management server and enter its IP address and port number. **Table 6-40** describes the parameters of an external key management server.

NOTE

- Click to configure a second external key management server. The two servers back up each other.
- Click to remove an external key management server. When modifying or removing an external key management server, ensure that the IP address of the other server is connected, or modify or remove the server whose IP address is disconnected.

Table 6-40 Parameters of an external key management server

Parameter	Description	Example
Server Type	Type of an external key management server.	SafeNet KMIP **NOTE** • **Thales KMIP**: Thales CipherTrust Manager key management server. • **SafeNet KMIP**: SafeNet KeySecure key management server. • **Sansec KMIP**: Sansec SecKMS key management server. • **Utimaco KMIP**: Utimaco vESKM key management server. • **Thales DSM KMIP**: Thales Vormetric Data Security Manager key management server.
Server Address	Service network port IP address of an external key management server.	192.168.141.128
Port	Port of an external key management server IP address.	Value range: 1 to 65535. Default value: 5696. **NOTE** If **Thales DSM KMIP** is selected, the port number can only be set to **5696**.

Step 6 Click **Test** to check whether the external key management server is configured successfully.

Step 7 Click **Save**.

Step 8 (Optional) To delete a configured server, click **Initialize Server** and confirm the operation as prompted.

Copyright © Huawei Technologies Co., Ltd.

NOTE

Before initializing a server, ensure that the self-encrypting storage pool or encrypted account that uses the external key service has been deleted and the configured external key management servers are connected. If either server is disconnected, remove it and try again.

----End

6.5.7 Setting Per-Second Performance Monitoring for Converged Services

This section describes how to enable or disable per-second performance monitoring.

Prerequisites

- A storage pool has been created.
- If per-second performance monitoring is enabled, you need to disable the function and delete the configuration information by referring to **Step 3** before modifying parameters.

Context

Before per-second performance monitoring is enabled, there is limited space for storing performance monitoring data. As a result, the data can only be stored for a short period of time at a coarse granularity. After this function is enabled, performance monitoring data is written to the mounted namespace and can be stored for a longer time at a finer granularity.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Monitoring Settings** > **Per-Second Performance Monitoring**.

Step 3 **(Optional)** If per-second performance monitoring is enabled, disable it and delete the configuration information before modifying parameters.

1. Click **Modify** in the upper right corner of the page.
2. Set **Per-Second Performance Monitoring** to **Disable** and click **Save**.
3. In the dialog box that is displayed, select **Delete per-second performance monitoring configurations and performance data** and click **OK**.
4. Confirm your operation as prompted.

Step 4 Click **Modify** in the upper right corner of the page.

Step 5 Set per-second performance monitoring.

Set basic information about per-second performance monitoring. **Table 6-41** describes related parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-41 Per-second performance monitoring parameters

Parameter	Description
Per-Second Performance Monitoring	Select whether to enable per-second performance monitoring. • **Enable**: Performance monitoring data is written to a specified namespace. • **Disable**: Performance monitoring data will no longer be written to the namespace. If you select **Delete per-second performance monitoring configurations and performance data**, the per-second performance monitoring data that has been saved to the namespace will be deleted (unable to be restored) and can no longer be viewed. Otherwise, the data that has been saved to the namespace will not be deleted. **NOTE** If per-second performance monitoring has never been enabled, a message will be displayed on the top of DeviceManager: "The system detects that per-second performance monitoring is not enabled. Enabling this function helps you analyze performance more accurately. Do you want to enable the function? After enablement, this prompt will be automatically cleared."
Storage Pool	Select a storage pool where the per-second performance monitoring data is to be stored.
Namespace	Determine a name for the namespace to be mounted for the storage of per-second performance monitoring data. **NOTE** The character string provided in the text box is the prefix of the namespace.

Step 6 Click **Save**.

Step 7 Confirm your operation as prompted.

----End

6.5.8 Adding a Node for an Enabled Service

This section describes how to add a node for a service that has been enabled in a storage pool.

Prerequisites

- At least one service is enabled for nodes in the storage pool.
- Some nodes in the storage pool do not have services enabled.
- The object service is supported only when **Service Type** is set to **Intelligent video and image** and a license that supports SmartInterworking is imported.
- When **Service Type** is set to **Intelligent video and image** or **Backup and archiving**, the HDFS service is not supported.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Resources** > **Services** > **Basic Service**.

Step 3 Click **Enable Service**.

The **Enable Service** page is displayed.

Step 4 Select a storage pool to which you want to add a service node.

Step 5 Set **Operation** to **Add Node**.

Step 6 In the **Available Nodes** area on the left, select one or more desired nodes. They will be automatically added to the **Selected Nodes** area on the right.

NOTE

In the **Service Type** area, view the services to be enabled for the new node. The selected services are those enabled in the storage pool. All enabled services in the storage pool must also be enabled on the new node.

Step 7 Click **OK**.

----End

6.5.9 Deleting a Subnet

This section describes how to delete a subnet.

Prerequisites

Zones in the subnet have been deleted.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Resources** > **Access** > **Service Network** > **Subnet**.

Step 3 Select one or more desired subnets and click **Delete**.

NOTE

You can also click **More** on the right of a desired subnet and select **Delete**.

Step 4 Confirm your operation as prompted.

Step 5 Click **Close**.

----End

 Copyright © Huawei Technologies Co., Ltd.

7 Maintenance and Fault Management

Table 7-1 Maintenance and fault management

Operation	Reference Document
Security configuration	*OceanStor Pacific Series 8.2.1 Security Configuration Guide*
Administrator operations	*OceanStor Pacific Series 8.2.1 Administrator Guide*
Parts replacement	*OceanStor Pacific Series 8.2.1 Parts Replacement*
Troubleshooting	*OceanStor Pacific Series 8.2.1 Troubleshooting*

 Copyright © Huawei Technologies Co., Ltd.