SAP

Deployment Guide (DeC)

Issue	07
Date	2019-09-30

HUAWEI TECHNOLOGIES CO., LTD.

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

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

Trademarks and Permissions


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

Notice

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

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

Contents

 Copyright © Huawei Technologies Co., Ltd.

 Copyright © Huawei Technologies Co., Ltd.

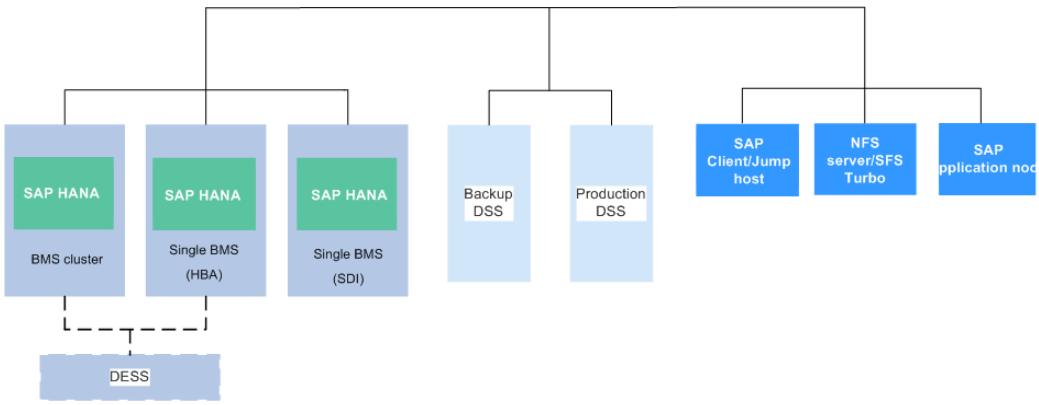
 Copyright © Huawei Technologies Co., Ltd.

1 Scheme

1.1 DeC Scheme Overview

This section describes the deployment scheme of the DeC.

Figure 1-1 Dedicated Cloud (DeC) scheme



- Production (PRD): indicates the production system where SAP applications are formally used.
- Quality Assure (QAS): indicates the quality assurance system where the functions, performance, and reliability of SAP applications are fully verified.
- Development (DEV): indicates the development system where development engineers configure and verify the compatibility between application software and SAP applications and continuously optimize the application software.
- Test (TST): indicates the test system where the development engineers test application software and SAP applications to verify the functions of application software after the application software development is complete.

SAP DeC consists of the following parts:

- SAP applications are stored in virtual resource pools.
  - SAP applications and NFS servers are deployed on Elastic Cloud Servers (ECSs).

 Copyright © Huawei Technologies Co., Ltd.

  - The NFS servers can be deployed in the active/standby mode. You can use SFS Turbo to provide shared file storage.
  - SAP application ECSs can be deployed in the high availability (HA) mode.
- Databases are deployed in Bare Metal Server (BMS) resource pools.
  - BMS (single-node deployment): Local disks are used as log volumes, data volumes, or shared volumes. Backup volumes are provided by NFS servers or SFS Turbo.
  - BMS (cluster deployment): Dedicated Enterprise Storage Service (DESS) provides log volumes and data volumes, while NFS servers or SFS Turbo provide backup volumes and shared volumes.
- Storage uses two isolated storage pools.
  - Production storage pool: is used as data volumes and SBD volumes of SAP applications.
  - Backup storage pool: is used as backup volumes of the NFS servers or SFS Turbo for the SAP system (SAP applications and SAP HANA databases).

DeC allows SAP DR systems to be deployed across AZs or regions, including cross-AZ or cross-region DR for SAP HANA and cross-AZ or cross-region DR for SAP applications.

- In the cross-AZ or cross-region DR scenario, the standby SAP HANA system is deployed in a different AZ of the same region or in a different AZ of a different region, and Multitier System Replication is configured to implement multi-layer data replication. The Preload function of System Replication is enabled to preload data to the memory of the standby system, reducing the switchover time and lowering Recovery Time Objective (RTO). For details, see **SAP HANA HA and DR Guide** and **SAP HANA User Guide (Single-Node Deployment)**.
- In the cross-AZ or cross-region DR scenario, the standby SAP application system is deployed in a different AZ of the same region or in a different AZ of a different region, and snapshots are periodically created for servers and storage resources in the active AZ. If a disaster occurs in the active AZ, a private image can be used to quickly provision cloud servers in the standby AZ. In addition, a snapshot file can be used to restore the SAP applications in the standby AZ through Volume Backup Service (VBS). For details, see the **SAP NetWeaver User Guide**.

1.2 Related Cloud Services

- **DeC**

  DeC is used as virtual resource pools. You have exclusive use of all physical devices, computing and network resources, and reliable distributed storage in a DeC.
- **Dedicated Distributed Storage Service (DSS)**

  DSS provides you with dedicated, physical storage resources. With advanced data redundancy and cache acceleration capabilities, DSS offers high availability and durability with an extremely low latency. By flexibly interconnecting with various computing services, such as ECS, BMS, and DeC, DSS offers first-class performance in a wide-range of scenarios, including, HPC, OLAP, and hybrid loads.

 Copyright © Huawei Technologies Co., Ltd.

- **BMS**

  SAP HANA software is deployed on BMSs.

- **ECS**

  Network File System (NFS) servers, SAP HANA Studio, and jump host use ECSs.

  NOTE

  In the SAP system deployment mode, the NFS server shares its shared and backup volumes with all SAP nodes.

- **Elastic Volume Service (EVS)**

  All cloud servers in the SAP system have EVS disks attached.

- **Virtual Private Cloud (VPC)**

  All cloud servers in the SAP system locate in the same VPC. They are isolated using VPC subnets and security groups for network security.

- **Image Management Service (IMS)**

  Images are required for creating ECSs and BMSs.

- **Direct Connect**

  Direct Connect is a high-speed, stable, and secure dedicated network connection that connects your data center to DeC. You can use a Direct Connect connection to connect computers in your local data center to cloud servers or hosting servers in DeC. It maximizes cloud computing capacities and existing IT facilities to build a flexible, scalable hybrid cloud computing environment.

- **Virtual Private Network (VPN)**

  VPN establishes a secure, encrypted communication tunnel between your local data center and your DeC and quickly extends services from the data center to the cloud.

- **DESS**

  DESS provides dedicated storage services to enterprises based on Huawei storage devices. DESS provides the same superb performance and reliability as enterprise private cloud and simplifies service deployment on public cloud for enterprise users.

  NOTE

  After you have purchased DESS, create disks and then attach disks as required.

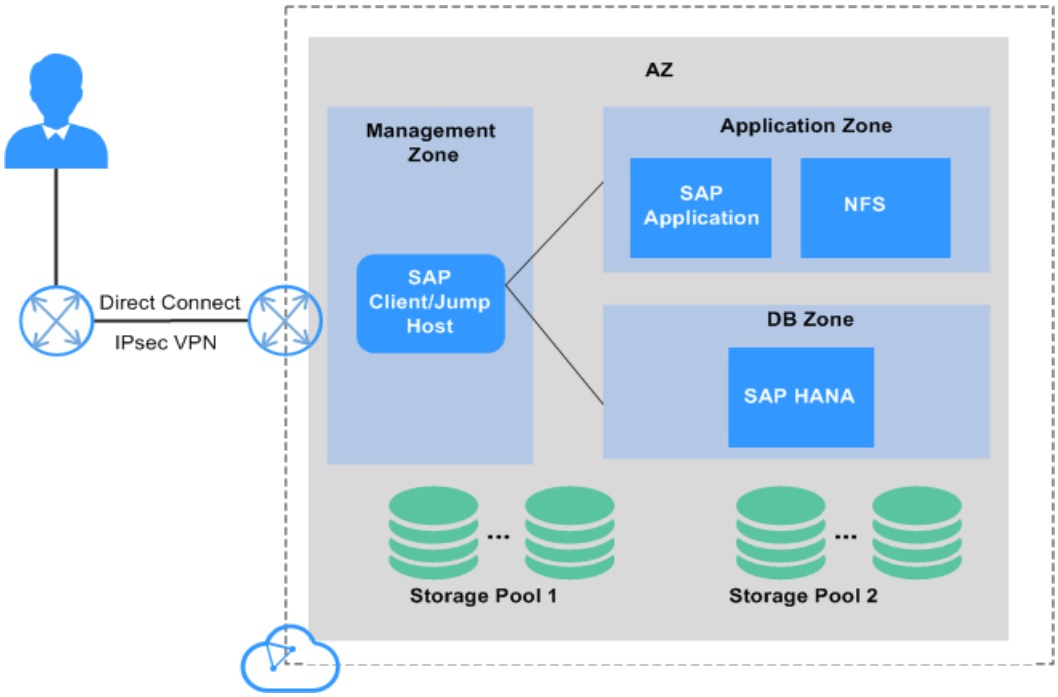
 Copyright © Huawei Technologies Co., Ltd.

2 Deployment of Development and Test Systems

2.1 Deployment Scheme

Figure 2-1 shows the deployment scheme of the SAP (DeC) development and test system.

Figure 2-1 Deployment scheme



The concepts involved in the preceding figure are as follows:

- VPC network: All nodes in the SAP system are deployed within a VPC and belong to the same availability zone (AZ) to ensure network security. The VPC network consists of three subnets in the management zone, application zone, and database zone, respectively.

 Copyright © Huawei Technologies Co., Ltd.

- Storage pool 1 is a data storage pool for SAP application nodes and the jump host, and storage pool 2 is a backup data storage pool for SAP application nodes and database nodes.
- Management zone:
  - Jump host node: ECS

    A tenant accesses the jump host node and uses SSH to navigate to the application nodes and database nodes. It is also used to deploy SAP Client software, such as SAP GUI and SAP HANA Studio.
- Database zone:

  SAP HANA node: BMS

  SAP HANA nodes are used to deploy the SAP HANA software. A BMS has the following disks attached:
  - OS disk: provides the directory for installing the OS.
  - Data volume: periodically stores the data transmitted from the SAP HANA IMDB (a database running in high-performance memory). The period is 5 minutes by default.
  - Log volume: stores the data triggered by an event. If an event, for example, a record or a batch of records are updated, is triggered for the server IMDB, the system will write the latest IMDB data into the log volume.
  - Shared volume: stores the SAP HANA installation software and SAP HANA database log files.
- Application zone
  - SAP application node: ECS

    SAP application nodes are used to deploy SAP applications.
  - NFS server: ECS

    NFS servers provide backup volumes and share them with SAP application nodes and database nodes. You can use SFS Turbo to provide shared file storage.

NOTICE

If you use SFS Turbo, you do not need to perform operations related to NFS servers in this document.

2.2 Data Planning

2.2.1 Network Planning

Networking Description

Figure 2-2 shows the network planning of the SAP (DeC) development and test system.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The network segments and IP addresses are for reference only.

Figure 2-2 Network plane planning

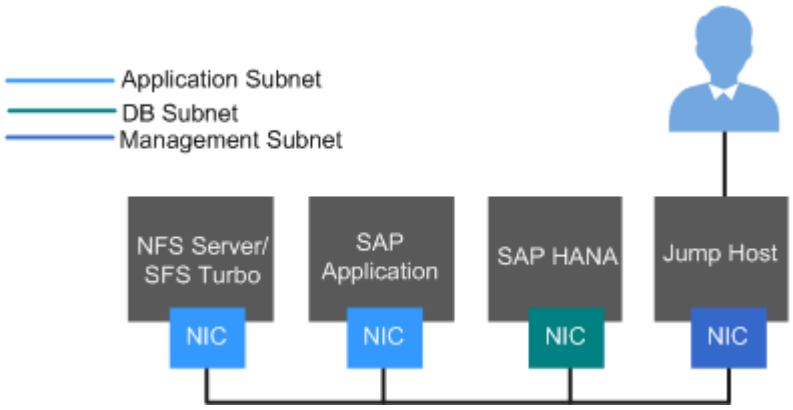


Table 2-1 shows the planned network information.

Table 2-1 Network planning information

Parameter	Description	Example Value
IP address	Allows an SAP HANA node to communicate with SAP application nodes or SAP HANA Studio client. Allows the backup volume on the NFS server to be shared with all SAP application nodes and database nodes.	SAP HANA node: 10.0.3.2 SAP application node: 10.0.5.4 NFS server: 10.0.5.101 Jump host: 10.0.0.202

Security Group Rule

The following security group rules are recommended practices. You can configure your own security group rules as you need.

For details about SAP HANA security group rules, see section "Network Planning" in the **SAP HANA User Guide (Single BMS Node Deployment)**.

For details about SAP NetWeaver security group rules, see section "Security Group Planning" in the *SAP NetWeaver User Guide*.

For more information about specific ports and security group rules to be accessed by SAP, see **SAP official documents**.

2.2.2 SAP HANA Nodes

Table 2-2 lists the planning of SAP HANA nodes.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-2 SAP HANA node planning

Flavor	CPU Number and Model	Memory	OS and Disk
physical.m2.large	4 x Broadwell EX 8890 v4	3 TB	OS: SUSE Linux Enterprise Server 12 SP2 for SAP Local disk: • OS volume: 2 x 600 GB, SAS disk, hardware RAID 1 • Log volume: 2 x 1.6 TB ES3600, SSD disk, software RAID 1 • Data volume: 9 TB • Shared volume: 3 TB Use Logical Volume Manager (LVM) to logically divide the local disk (14 x 1.8 TB 10K 2.5 SAS HDD, hardware RAID 50) into a data volume and a shared volume.

2.2.3 SAP Application Nodes

Table 2-3 SAP application ECS specifications

Flavor	vCPUs	Memory (GB)
h1.8xlarge.4	32	128
h1.4xlarge.4	16	64
h1.2xlarge.4	8	32
h1.xlarge.4	4	16
m3.large.8	2	16
m3.xlarge.8	4	32
m3.2xlarge.8	8	64
m3.3xlarge.8	12	96
m3.4xlarge.8	16	128
m3.6xlarge.8	24	192
m3.8xlarge.8	32	256

Table 2-4 lists the planning of SAP application nodes.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-4 SAP application node planning

Node	Specifications
SAP application node	• OS: SUSE Linux Enterprise Server 12 SP2 for SAP or SUSE Linux Enterprise Server 12 SP1 for SAP • Disk: Configure it as required.

Before applying for cloud services for SAP applications, evaluate the SAP Application Performance Standard (SAPS) value based on the standard SAP Sizing method. Then apply for the ECSs based on the evaluation results. For details, see **SAP Quick Sizer**.

For details about the minimum hard disk space, RAM, and minimum software requirements on each component of SAP applications, see SAP note: **1953429** and **SAP Installation Guides**.

2.2.4 Other Nodes

Table 2-5 lists the planning of other nodes.

Table 2-5 Other node planning

Node	Specifications
NFS server	• OS: SUSE Linux Enterprise Server 12 SP2 for SAP • Flavor: h1.xlarge.4 (4 vCPUs and 16 GB memory capacity) • Disk: – System disk: 60 GB, high I/O, non-shared disk – Backup volume: Configure it as required. **NOTE** HUAWEI CLOUD supports two types of shared disks: NFS and SFS Turbo. Optionally, you can also create an SFS Turbo file system to provide backup volumes.
Jump host	• OS: SUSE Linux Enterprise Server 12 SP2 for SAP • Flavor: h1.xlarge.4 (4 vCPUs and 16 GB memory capacity) • System disk: 60 GB, high I/O, non-shared disk

2.3 Software and Tools

Table 2-6 lists the software and tools to be obtained.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-6 Required software and tools

Item	Description	How to Obtain
WinSCP	Uploads key files to cloud servers.	www.winscp.net
PuTTY and PuTTYgen	Used for logging in to a cloud server and running commands.	https://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
SAP HANA 1.0 SAP HANA 2.0 **NOTE** Install the required SAP HANA version based on version mapping relationship between SAP HANA software version and SUSE OS version on the SAP official website.	SAP HANA installation package. You can visit the SAP official website or access the OBS bucket to download the installation package.	For detailed paths where the files can be downloaded, see the sections describing how to install SAP HANA.
SAP HANA Studio **NOTE** Install the required SAP HANA Studio version based on version mapping.	SAP HANA Studio installation package	
Configuration script	Contains the script and configuration file used for installing and configuring SAP HANA.	

2.4 Purchasing Cloud Services

2.4.1 Purchasing DeC

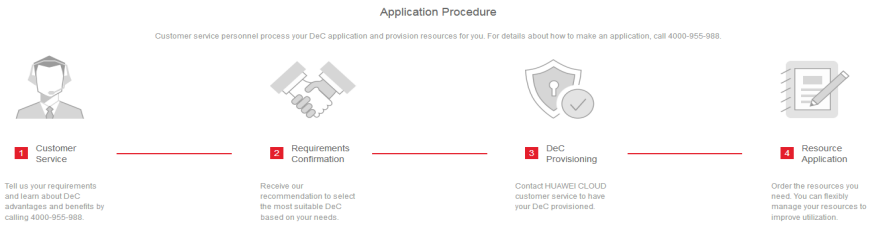
This section describes how to purchase a DeC. For details, see **Dedicated Cloud Purchase Guide**.

Provisioning DeC

Before purchasing the Huawei DeC service, you must apply for and provision the DeC service. Apply for and provision the DeC service offline. If necessary, contact HUAWEI CLOUD customer service at 4000-955-988 or 950808. Therefore, reserve sufficient time for each process so that you can use the DeC service in a timely manner as expected.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-3 DeC service application process



Purchasing DeC

Step 1 Log in to the management console.

Step 2 In the upper right corner of the page, choose **Billing** > **Renewal**.

Step 3 In the navigation pane on the left, choose **Funds Management** > **Top Up** and top up your account as prompted.

Step 4 Click in the upper left corner of the management console to switch to the region where the DeC is enabled.

Step 5 In the navigation pane on the left, click and choose **Dedicated Cloud** under **Computing**. On the displayed page, click **Apply for Resources**.

Step 6 Click **Next**. After confirming that the configurations are correct, click **Submit**.

----End

2.4.2 Purchasing Dedicated Storage

Scenarios

To ensure the service reliability of an SAP system, you need to create two dedicated storage pools on a DeC. One is used to back up data of all nodes in the SAP system and the other is used to store data of all SAP applications.

Procedure

Step 1 Log in to the management console. In the navigation pane on the left, click and choose **Dedicated Cloud** under **Computing**. On the displayed **Dedicated Cloud Console** page, choose **Dedicated Distributed Storage Service** in the navigation pane.

Step 2 On the displayed page, click **Apply for Storage Pool**.

Step 3 Set the parameters as prompted.

Note the following:

- The storage pool name can contain a maximum of 255 characters. It is recommended that the name contains identifiable words, such as production and backup.
- Set **Type** to **High I/O**.

 Copyright © Huawei Technologies Co., Ltd.

Step 4 Click **Apply Now**.

----End

2.4.3 Applying for a VPC

Procedure

Step 1 Log in to the management console.

Step 2 In the navigation pane on the left, click ☰ and choose **Network** > **Virtual Private Cloud**.

Step 3 Click **Create VPC**.

Step 4 On the displayed page, configure VPC parameters.

Set the parameters as follows:

- **CIDR Block**: specifies the IP address range for the VPC. Configure this parameter based on the planned subnet information.
- **CIDR Block**: specifies the IP address range for the default VPC subnet. Ensure that the IP address range for the default VPC subnet is within the IP address range for the VPC subnet. Configure this parameter based on the planned information.
- **DNS Server Address**: The external DNS server address is used by default. If you need to change the DNS server address, ensure that the DNS server addresses are available.

Step 5 Complete the VPC creation.

----End

2.4.4 Creating a Subnet and Configuring a Security Group

To ensure proper communication between the ECSs in an SAP HANA system, create a subnet for the ECSs and configure a proper security group.

Procedure

Step 1 Create a subnet.

1. Log in to the management console.
2. Click ⌖ in the upper left corner and select a region and project.
3. In the navigation pane on the left, click ☰ and choose **Network > Virtual Private Cloud**.
4. Click the VPC to which the SAP HANA system belongs.
5. Click the **Subnets** tab and then **Create Subnet**.
6. In the **Create Subnet** pane, configure parameters as prompted.
   - **AZ**: specifies the AZ of the subnet.
   - **Name**: Configure the subnet name that is easy to identify, for example, **service_subnet**.

 Copyright © Huawei Technologies Co., Ltd.

- **CIDR Block**: Configure this parameter according to the deployment plan described in section **Network Planning**.
- **Advanced Settings**: Set it to **Default**.

7. Click **OK** to complete the subnet configuration.
8. Repeat **Step 1.5** to **Step 1.7** to create all required subnets according to the requirements specified in section **Network Planning**.

Step 2 Configure a security group.

You need to create a security group for all nodes in the SAP HANA system.

1. Choose **Access Control > Security Groups** on the left and then click **Create Security Group** in the upper right corner. The **Create Security Group** dialog box is displayed.
2. Set the following parameters as prompted:
   - **Template**: The template contains security group rules, which help you quickly create a security group. The following templates are provided:
     - **Custom**: This template allows you to create security groups with custom security group rules.
     - **General-purpose web server**: The security group that will be created using this template is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and allow inbound traffic on ports 22, 80, 443, and 3389.
     - **All ports open**: The security group that will be created using this template includes default rules that allow inbound traffic on any port. Allowing inbound traffic on any port may pose security risks. Exercise caution when using this template.
   - **Name**: specifies the name of the security group. Name the security group that is easy to identify, for example, **studio_security_group**.
   - **Enterprise Project**: You can add the security group to an enabled enterprise project. You can select an enterprise project from the drop-down list.
3. Click **OK**.
4. Repeat **Step 2.1** to **Step 2.3** to create other security groups.
5. In the navigation pane on the left, choose **Access Control** > **Security Groups**. In the security group list, click the security group to which you want to add an access rule.
6. Click **Add Rule** on the **Inbound Rules** or **Outbound Rules** tab as planned.
7. On the displayed page, add the rule according to the requirements specified in section **Network Planning**.

   The default security group rules cannot be deleted.
8. Repeat **Step 2.5** to **Step 2.7** to configure all security groups.

----End

 Copyright © Huawei Technologies Co., Ltd.

2.4.5 (Optional) Creating an SFS Turbo File System

If you want to use SFS Turbo instead of the NFS to provide shared file storage, such as HANA database backup volume and shared volume, you need to create an SFS Turbo file system to offer the shared path to SAP nodes.

NOTICE

If you use SFS Turbo, you do not need to perform operations related to the NFS server in this document.

Prerequisites

Ensure that the dedicated computing and storage resources are in the same DeC.

Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the console, and select a region and project.

Step 3 In the navigation pane on the left, click and choose **Scalable File Service** under **Storage**. The **Scalable File Service** page is displayed.

Step 4 Click **Create File System**.

Step 5 Configure the parameters listed in **Table 2-7**.

Table 2-7 Configuration parameters

Parameter	Description	Example Value
File System Type	Specifies the file system type. Select **SFS Turbo**.	SFS Turbo
Billing Mode	Select a mode based on your need.	Yearly/Monthly
Region	Select the target region.	CN North-Beijing4
AZ	Specifies the AZ where the file system is located. Select an AZ as needed.	AZ1
Protocol Type	Specifies the file service type. Set this parameter to **NFS**.	NFS
Storage Class	Select a storage class as required.	Standard
Capacity	Specifies the maximum capacity of a single file system. When the used capacity of a file system reaches this value, no more data can be written to the file system. You need to expand the file system.	5TB

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
VPC	Select the VPC and subnet used by the ECS. For details, see **Applying for a VPC** and **Creating a Subnet and Configuring a Security Group**.	N/A
Security Group	Select the security group where the ECS belongs. For details, see **Creating a Subnet and Configuring a Security Group**.	N/A
Enterprise Project	Select the project you need.	SAP
Automatic Backup	This parameter is optional. SFS Turbo provides the automatic backup function. You can back up data of the file system by setting the backup policy. After a backup policy is enabled, the system automatically backs up file system data at the specified time. Select **Enable automatic backup**. After a backup policy is enabled, you need to set the backup start time and backup cycle. You can create backup policies based on service requirements. For details, see **Table 3** in section "Creating a File System" of the *Scalable File Service Getting Started*.	N/A
Name	Specifies the file system name.	sfs-turbo-backup
Quantity	Select the quantity according to the site requirements.	1 year

Step 6 Click **Create Now**. On the displayed page, confirm the configuration information and click **Submit**.

Step 7 Go back to the file system list. On the displayed page, locate the new file system by its name in the file system list on the right. In the **Shared Path** column, query the shared path.

Step 8 Log in to an SAP HANA ECS and check whether the IP address of the DNS server is configured in the **/etc/resolv.conf** file. If not, write the IP address of the DNS server into the **/etc/resolv.conf** file.

----End

2.4.6 Purchasing a BMS

Scenarios

SAP HANA runs on BMSs. Thus, you need to apply for BMSs on the DeC. BMSs use local disks.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the management console.

Step 2 In the navigation pane on the left, click  and choose **Dedicated Cloud** under **Computing**. On the displayed **Dedicated Cloud Console** page, choose **Dedicated Bare Metal Server** in the navigation pane.

Step 3 On the displayed page, click **Provision BMS in DeC**.

Step 4 Configure the parameters based on **SAP HANA Nodes**.

Note the following:

- The BMS name contains a maximum of 13 characters.
- An EIP has not been bound to the target BMS.
- Select **Key pair** for **Login Mode**. Ensure that all nodes in the SAP system use the same key. Otherwise, the SAP software installation will fail.

Step 5 Click **Buy Now**. Switch to the BMS management page and check the status of the created BMS.

After the BMS is created, you can view the BMS from the BMS list on the right of the page.

Step 6 Change the password of user **root** for logging in to all BMSs.

Securely keep the **root** password. In addition, ensure that all ECSs and BMSs in the SAP system use the same **root** password.

1. Log in to a BMS.
2. Run the following command to switch to user **root**:

   sudo su -
3. Run the following command to change the password of user **root**:

   passwd

   Enter the password as prompted for confirmation.

----End

2.4.7 Purchasing an ECS

Scenarios

In the SAP system, SAP HANA is deployed on BMSs while other software systems are deployed on ECSs.

- Jump host uses an ECS. You can access the jump host and use SSH to navigate to SAP HANA nodes and SAP application nodes. An ECS is also used to deploy SAP Client software, such as SAP GUI and SAP HANA Studio.
- NFS servers use ECSs. NFS servers provide backup volumes and share them with SAP application nodes and database nodes.
- SAP applications are deployed on ECSs.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the management console.

Step 2 In the navigation pane on the left, click ☰ and choose **Computing** > **Elastic Cloud Server**.

Step 3 On the displayed page, click **Buy ECS**.

Step 4 Configure the parameters based on sections **SAP Application Nodes** and **Other Nodes**.

Note the following:

- The ECS name contains a maximum of 13 characters.
- Select **DSS** for **Disk** and select the storage pool to which the disk belongs based on the deployment scheme.
- An EIP has not been bound to the target ECS.
- Select **Key pair** for **Login Mode**. Ensure that all nodes in the SAP system use the same key. Otherwise, the SAP software installation will fail.

Step 5 Create other ECSs as required.

Step 6 Change the password of user **root** for logging in to all ECSs.

Securely keep the **root** password. In addition, ensure that all ECSs use the same **root** password.

1. Log in to an ECS.
2. Run the following command to switch to user **root**:

   sudo su -
3. Run the following command to change the password of user **root**:

   passwd

   Enter the password as prompted for confirmation.

----End

2.5 Configuring Switching Permissions

2.5.1 Configuring the Switching Between the Jump Host and Other Nodes

Scenarios

To switch to an SAP node from the jump host and to allow SSH switchovers between SAP nodes and the jump host, you must configure the them to be trusty.

Procedure

Step 1 Upload the key file to the jump host.

 Copyright © Huawei Technologies Co., Ltd.

1. Use WinSCP to log in to the jump host. Ensure that user **root** and the key file are used for authentication. Upload the certificate private key file (.pem file) to the directory **/usr** on the jump host.
2. Log in to the jump host. Copy the certificate private key file to the **/root/.ssh** directory and rename the file **id_rsa**.

   For example, if the original file name is **private.pem**, run the following commands to rename it:

   cp /usr/private.pem /root/.ssh/id_rsa

   cd /root/.ssh/

   chmod 600 id_rsa

Step 2 Use the server/client plane IP address to allocate the private key file and **authorized_keys** file to all nodes excepting the SAP HANA Studio node.

The commands are in the following format:

scp /root/.ssh/id_rsa *Peer IP address*:/root/.ssh/id_rsa

scp /root/.ssh/authorized_keys *Peer IP address*:/root/.ssh/

Step 3 Verify the switching.

Use SSH to switch from the jump host to all nodes excepting the SAP HANA Studio node for verification.

For example, the server/client plane IP address of the NFS server is 10.0.3.101. To switch from the jump host to the NFS server, run the following command:

ssh 10.0.3.101

----End

2.5.2 Configuring Mapping Between Hostnames and IP Addresses

Scenarios

During the SAP installation, installation programs use hostnames for communication. Therefore, you must configure the mapping between hostnames and IP addresses.

Procedure

Step 1 Log in to the jump host. Ensure that user **root** and the key file are used for authentication. Then, use SSH to switch to the node on which the SAP HANA is to be installed.

Step 2 Run the following command to open the **hosts** file:

vi /etc/hosts

Step 3 Write the hostnames and IP addresses of all SAP nodes into the **hosts** file.

- In the following format, **IP-Address** is the IP address of the server/client plane for the SAP node.

 Copyright © Huawei Technologies Co., Ltd.

- Both **Full-Qualified-Hostname** and **Short-Hostname** are the node name, for example, **hana001**.

The format is **IP-Address Full-Qualified-Hostname Short-Hostname**.

NOTICE

In an SAP system, you must write the mapping between all SAP node IP addresses and node names into the **hosts** file.

----End

2.5.3 Modifying OS Configurations

Scenarios

To ensure the proper installation of the SAP system, disable the OS firewalls of all nodes before the installation.

Procedure

Step 1 Log in to the jump host. Ensure that user **root** and the key file are used for authentication. Then, use SSH to switch to SAP HANA nodes.

Step 2 Run the following commands on the SAP HANA node to disable automatic firewall enabling and disable the firewall:

SuSEfirewall2 off

SuSEfirewall2 stop

systemctl disable SuSEfirewall2_init.service

systemctl disable SuSEfirewall2.service

systemctl stop SuSEfirewall2_init.service

systemctl stop SuSEfirewall2.service

Step 3 Repeat the preceding step to disable the firewalls of all nodes in the SAP system.

----End

2.6 Formatting a Disk

2.6.1 Formatting the Disks Attached to an NFS Server

NOTICE

If you use SFS Turbo to provide shared file storage, skip this section. For details about how to mount the backup volumes, see section **Formatting a Disk** in the *SAP HANA User Guide*.

 Copyright © Huawei Technologies Co., Ltd.

The NFS server disks are available only after they are formatted and mounted to the required directory.

Procedure

Step 1 Format the disks attached to an NFS server.

1. Log in to an NFS server.
2. Run the following command to view the disks that are not formatted:

   fdisk -l
3. Run the following commands to partition the disk:

   parted */dev/xvdd* **mklabel gpt y**

   parted */dev/xvdd* **mkpart primarty 0% 100%**
4. Set the file system of the created partition. Run the following command to set the file system format of the created partition to **ext3**:

   mkfs -t ext3 */dev/xvdd1*

Step 2 Attach the disk to the **/backup** directory.

1. Run the following command to create the **/backup** directory:

   mkdir /backup
2. Run the following command to attach the disk to the required directory:

   mount */dev/xvdd1* **/backup**
3. Write disk attaching relationships into the **/etc/fstab** file.

   Perform this operation so that the disk can be automatically attached to the NFS server when the NFS server restarts.
4. Run the following command to check the UUID of the disk:

   ll /dev/disk/by-uuid/
5. Open the file, enter the editing mode, and add an empty row.

   vi /etc/fstab
6. Replace the empty row with the following content:

   UUID=*8cbc7aa5-9110-4ff2-a15e-7170d9c45b8f* **/backup ext3 defaults 0 0**

Step 3 Configure and restart the NFS server.

1. Open the **/etc/sysconfig/nfs** file and enter the editing mode to set the ports of the NFS server.

   vi /etc/sysconfig/nfs
2. Configure the data as follows:

   ....

   MOUNTD_PORT="4002"

   ....

   STATD_PORT="4000"

   ....

   LOCKD_TCPPORT="4001"

   ....

   LOCKD_UDPPORT="4001"

 Copyright © Huawei Technologies Co., Ltd.

3. Open the **/etc/exports** file.

   The purpose of editing the file is to share the disks on the NFS server to all SAP HANA nodes.

   vi /etc/exports

4. Add the sharing record.

   The format is ***Shared directoryHosts that can access the shared directory (option)***.

   Take the IP address 10.0.1.2 of the cloud management/backup plane for the BMS as an example.

   /backup 10.0.1.2(rw,sync,no_root_squash,no_subtree_check)

   NOTE

   You need to add the sharing records of the SAP application instance nodes and SAP application nodes.

5. Run the following command to make the configuration in the **/etc/exports** file take effect:

   exportfs -a

6. Run the following command to restart the NFS server:

   systemctl restart nfsserver

7. Run the following command to check whether the shared directory is successfully set. If the directory information is displayed in the command output, the setting is successful.

   showmount -e

8. Run the following command to set the automatic startup of the NFS server:

   systemctl enable nfsserver

9. Run the following command to check the NFS server status:

   If the status of **Active** is active, the NFS server is started normally.

   systemctl status nfsserver

Step 4 Log in to the BMS and SAP application nodes and attach the backup volume to the SAP application nodes.

1. Run the following command to create the **/hana/backup** directory:

   mkdir -p /hana/backup

2. Run the following command to assign permissions to **/backup**:

   chmod -R 777 /hana/backup

3. Attach the backup volume to the **/hana/backup** directory on the SAP node.

   Take the NFS server with IP address 10.0.1.101 as an example.

   mount -t nfs -o vers=3 10.0.1.101:/backup /hana/backup

4. Write disk attaching relationships into the **/etc/fstab** file.

   Open the file and add the following content:

   10.0.1.101:/backup /hana/backup nfs defaults 0 0

----End

 Copyright © Huawei Technologies Co., Ltd.

2.6.2 Formatting a BMS Disk

Scenarios

The data volumes of SAP HANA nodes can be used only after they are formatted and then attached to required directories.

Procedure

Step 1 Log in to the jump host. Ensure that user **root** and the key file are used for authentication. Then, use SSH to switch to SAP HANA nodes.

Step 2 Use SSD disks to form RAID 1.

1. View the disk information.

   fdisk -l

2. Locate the drive letters of the SSD disks, such as **/dev/nvme0n1** and **/dev/nvme1n1**.
3. Form RAID 1 and specify the drive letter.

   For example, if the drive letter is **/dev/md0**, run the following command:

   mdadm --create */dev/md0* **--level=1 --raid-devices=2** */dev/nvme0n1 /dev/nvme1n1*
4. Enter **y** when the system displays **Continue creating array?**.
5. Save the RAID configuration.

   mdadm -Ds >> /etc/mdadm.conf

   NOTE

   If one SSD card is damaged and the damaged drive letter is **/dev/nvme1n1**, perform the following operations to restore data:

   1. Run the **mdadm --manage** */dev/md0* **--remove** */dev/nvme1n1* command to remove the drive letter.
   2. Stop the node, replace the SSD card, and then start the node.
   3. Run the **mdadm --manage** */dev/md0* **--add** */dev/nvme*n1* command to add a new drive letter to restore data. Replace *** with the drive letter based on the actual situation.
6. Create the **/hana/log/** directory.

   mkdir -p /hana/log/
7. Create a file system.

   mkfs -t xfs -f */dev/md0*
8. Attach a disk.

   mount */dev/md0* **/hana/log/**

Step 3 Use LVM to logically divide the disk into a data volume and a shared volume.

Run the following commands to partition the disk:

parted */dev/sda* **mklabel gpt y**

parted */dev/sda* **mkpart primarty 0% 100%**

 Copyright © Huawei Technologies Co., Ltd.

Step 4 Run the following command to create a physical volume:

pvcreate */dev/sda1*

Step 5 Run the following command to create a volume group:

vgcreate vghana */dev/sda1*

Step 6 Run the following command to query the available capacity of the volume group:

vgdisplay vghana

Step 7 Run the following commands to create logical volumes:

lvcreate -n lvhanashared -L *3T* **vghana**

lvcreate -n lvhanadata -L *9T* **vghana**

Step 8 Run the following commands to format the logical volumes and attach them to the corresponding directories:

mkfs -t xfs /dev/mapper/vghana-lvhanadata

mkfs -t xfs /dev/mapper/vghana-lvhanashared

mkdir -p /hana/data

mkdir -p /hana/shared

mount /dev/mapper/vghana-lvhanadata /hana/data

mount /dev/mapper/vghana-lvhanashared /hana/shared

Step 9 Run the following commands to write disk attaching relationships into the **/etc/fstab** file:

/dev/mapper/vghana-lvhanadata /hana/data xfs defaults 0 0

/dev/mapper/vghana-lvhanashared /hana/shared xfs defaults 0 0

/dev/md0 **/hana/log xfs defaults 0 0**

----End

2.6.3 Formatting Disks Attached to an SAP Application Node

Scenarios

The data disks of SAP application nodes can be used only after they are formatted and attached to required directories. The section describes how to initialize the hard disks of an SAP NetWeaver node in the standard deployment mode. **Table 2-8** lists the file system planning.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-8 File systems planned for the standard deployment mode of SAP NetWeaver nodes

Mount Point	File System Type	Description
/usr/sap	ext3	Specifies the directory which is used to store SAP application files. The directory capacity is at least 30 GB.
/sapmnt	ext3	Specifies the SAPMNT directory. The directory capacity is at least 10 GB.

NOTE

On the ECS homepage, choose **Learn more** > **Quick Start** > **Initializing an EVS Disk (Linux)** and you can view the hard disk initialization information.

Procedure

Step 1 Log in to an SAP NetWeaver node.

Step 2 Format the disk.

1. Run the following command to query the disk to be formatted:

   fdisk -l

   Information similar to the following is displayed:

   ```
   ... Disk /dev/sde doesn't contain a valid partition table
   ```

2. Format the disk and attach it to the specified directory based on information provided in **Table 2-8**.

   Run the following command to format the disk (taking the **dev/sde** disk as an example):

   fdisk /dev/sde

3. Enter **n** and press **Enter** to create partitions.
4. Enter **P** and press **Enter**.

   Creating a primary partition is used as an example.

   Information similar to the following is displayed:

   ```
   Partition number (1-4, default 1):
   ```

5. Enter the primary partition ID and press **Enter**.

   Primary partition ID 1 is used as an example.

   Information similar to the following is displayed:

   ```
   ... First sector (2048-259715199, default 2048):
   ```

6. Press **Enter**.

   The default start cylinder number is used as an example.

   Information similar to the following is displayed:

 Copyright © Huawei Technologies Co., Ltd.

```
... Using default value 2048 Last sector, +sectors or +sizeM or +size{K,M,G}(2048-259715199, default 2048):
```

Press **Enter**.

The default end cylinder number is used as an example.

Information similar to the following is displayed:

```
.... Using default value 209715199  Command (m for help):
```

7. Enter **w** and press **Enter**.

   Enter the partition result into the partition table to complete partition creation.

8. Format the new partition based on the disk format.

   The command for formatting a disk in the ext3 format is **mkfs.ext3**. For example, to format **/dev/sde1** in ext3 format, run the following command:

   mkfs -t ext3 /dev/sde1

   Formatting the partition requires a period of time. During this time, observe the system running status and do not exit the system.

9. Run the **mkdir /sapmnt** command to create the **/sapmnt** directory.

10. Attach the disk to the **/sapmnt** directory.

    mount -t ext3 /dev/sde1 /sapmnt

11. Run the following command to modify the **fstab** file:

    vi /etc/fstab

12. Enter the path information.

    Enter the path based on site requirements. In the distributed deployment mode, the NFS server is used. You need to configure the shared directory on the NFS server to **/etc/fstab**, as shown in **Figure 2-4**.

    NOTE

    The information configured in the **/etc/fstab** file is in the following format:

    Disk ID or partition Attached directory Disk format defaults 0 0

    In the preceding format, the recommended value of the last field **fs_passno** is **0**. In this case, the disk can be attached to the other instance if required.

Figure 2-4 Modifying the **fstab** file

```
UUID=1851e23f-1c57-40ab-86bb-5fc5fc606ffa /mnt/sdc      ext4 defaults     0   2
```

After you complete editing, press **Esc**, enter **:x**, and press **Enter** to exit the file.

Step 3 After formatting the disk, run the following commands to check the disk status:

mount -a (Mount all disks configured in **/etc/fstab** to the specified directory.)

df -h (displays the attachment point directories.)

Run the following command to assign permissions to **/sapmnt**:

chmod -R 777 /sapmnt

----End

 Copyright © Huawei Technologies Co., Ltd.

2.7 Installing SAP HANA

For details about how to install SAP HANA, see section "Installing SAP HANA" in the **SAP HANA User Guide (Single BMS Node Deployment)**.

2.8 Installing SAP Applications

For details about how to install SAP applications, visit the following website to refer to the specific SAP application software installation guide.

SAP Help Center: **https://help.sap.com/viewer/index**

For details about how to install SAP NetWeaver, see section "Installing SAP NetWeaver" in the **SAP NetWeaver User Guide**.

 Copyright © Huawei Technologies Co., Ltd.

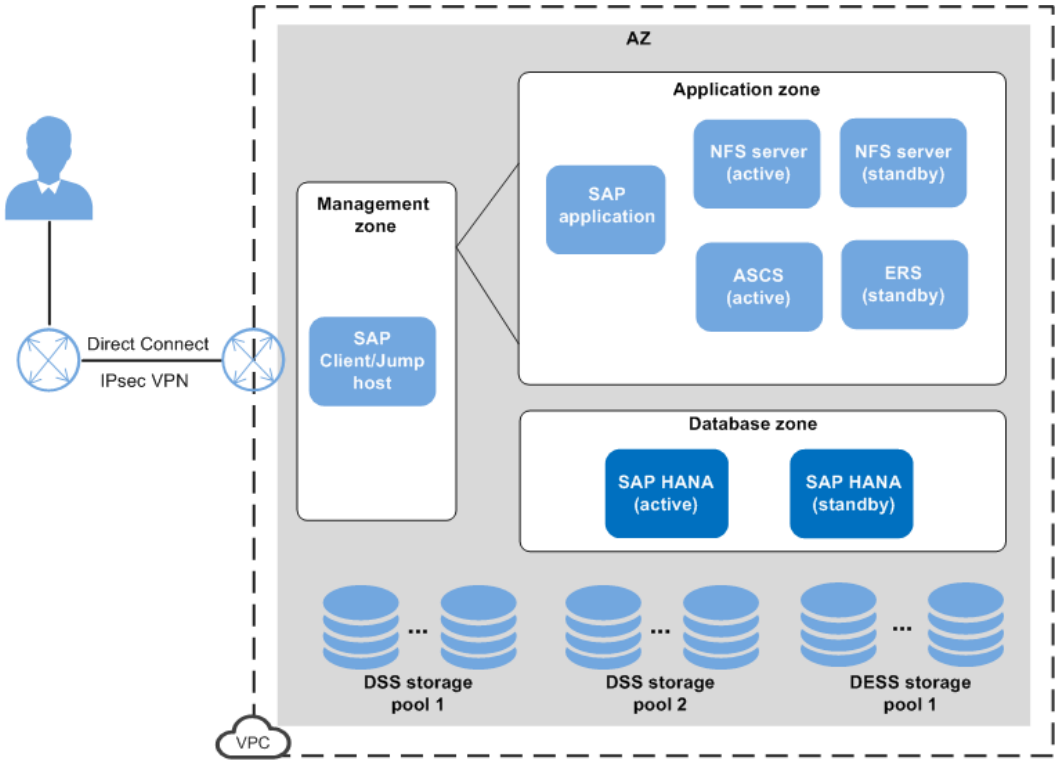
3 Production System Deployment

3.1 Deployment Scheme (DESS)

This scheme uses DESS for storage. KunLun servers only allow DESS to provide SBD volumes. To reduce costs, you can function iSCSI disks as SBD volumes when KunLun servers are deployed in the HA mode. For details, see section **Deployment Scheme (iSCSI)**.

Figure 3-1 illustrates the single-node deployment mode.

Figure 3-1 Single-node deployment



The concepts involved in the preceding figure are as follows:

 Copyright © Huawei Technologies Co., Ltd.

- VPC network: All nodes in the SAP system are deployed within a VPC and belong to the same AZ to ensure network security. The VPC network consists of three subnets in the management zone, application zone, and database zone, respectively.
- DSS storage pool 1 is a data production storage pool for SAP application nodes and the jump host, and DSS storage pool 2 is a data backup storage pool for SAP application nodes and database nodes. DESS storage pool 1 is a data production pool for SAP HANA nodes.
- Management zone:
  - Jump host: ECS

    A tenant accesses the jump host and uses SSH to navigate to application nodes and database nodes. It is also used to deploy SAP Client software, such as SAP GUI and SAP HANA Studio.
- Database zone:

  SAP HANA node: Two BMSs are required for deploying SAP HANA. A BMS has the following disks attached:
  - OS disk: provides the directory for installing the OS.
  - Data volume: periodically stores the data transmitted from the SAP HANA IMDB (a database running in high-performance memory). The period is 5 minutes by default.
  - Log volume: stores the data triggered by an event. When an event, for example, a record or a batch of records are updated, is triggered for the server IMDB, the system will write the latest IMDB data into the log volume.
  - Shared volume: stores the SAP HANA installation software and SAP HANA database log files.
  - Backup volume: stores the SAP HANA database backup files.
- Application zone:
  - SAP application node: ECS

    SAP application nodes are used to deploy SAP applications.
  - NFS servers: ECSs

    Two ECSs are required to work in the active/standby mode. SAP HANA and SAP NetWeaver share the NFS server. The backup volume of an SAP HANA node is provided by the NFS server. You can use SFS Turbo to provide shared file storage.

    NOTICE

    If you use SFS Turbo, you do not need to perform operations related to NFS servers in this document.
  - ASCS node: ECS

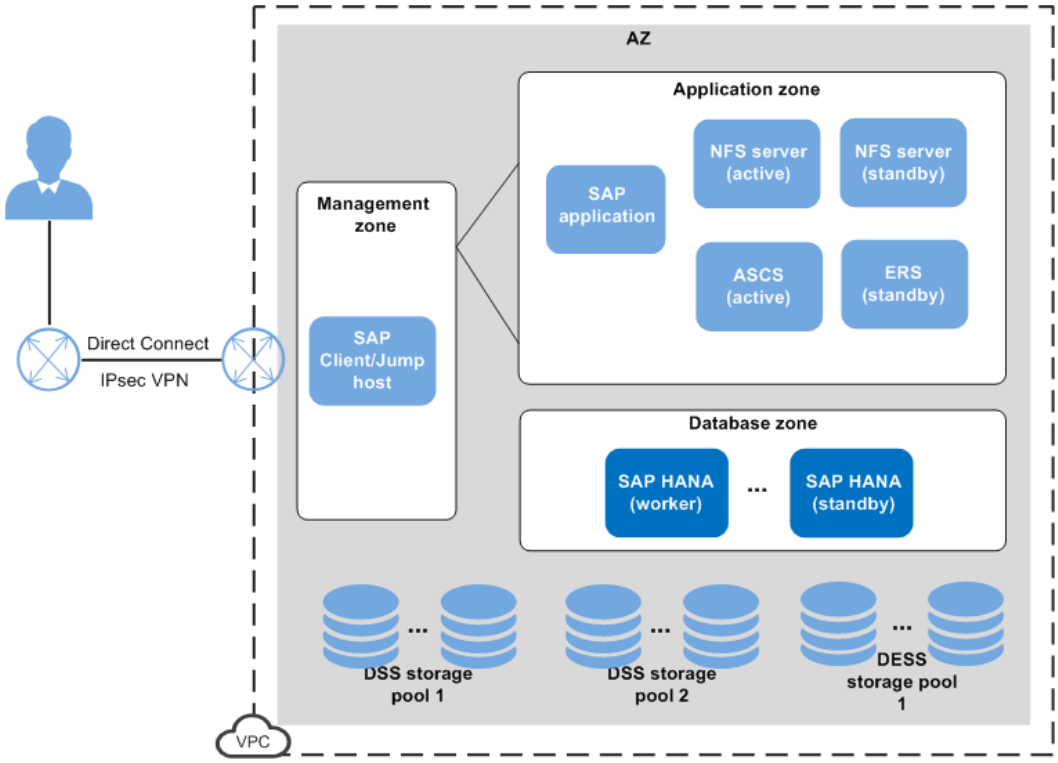
    The ASCS node works as the active node in the ASCS HA cluster, which is used to deploy the SAP NetWeaver ASCS instance.
  - ERS node: ECS

    The ERS node works as the standby node in the ASCS HA cluster, which is used to deploy the SAP NetWeaver ERS instance.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-2 shows the cluster deployment plan.

Figure 3-2 Cluster deployment



The concepts involved in this scenario are the same as those involved in the single-node deployment scenario in addition to the following remarks:

NFS server: The shared volume and the backup volume of an SAP HANA node are provided by the NFS server.

Cluster deployment: Three BMSs are required to constitute a cluster. Among these servers, one functions as the standby node, and the others are worker nodes.

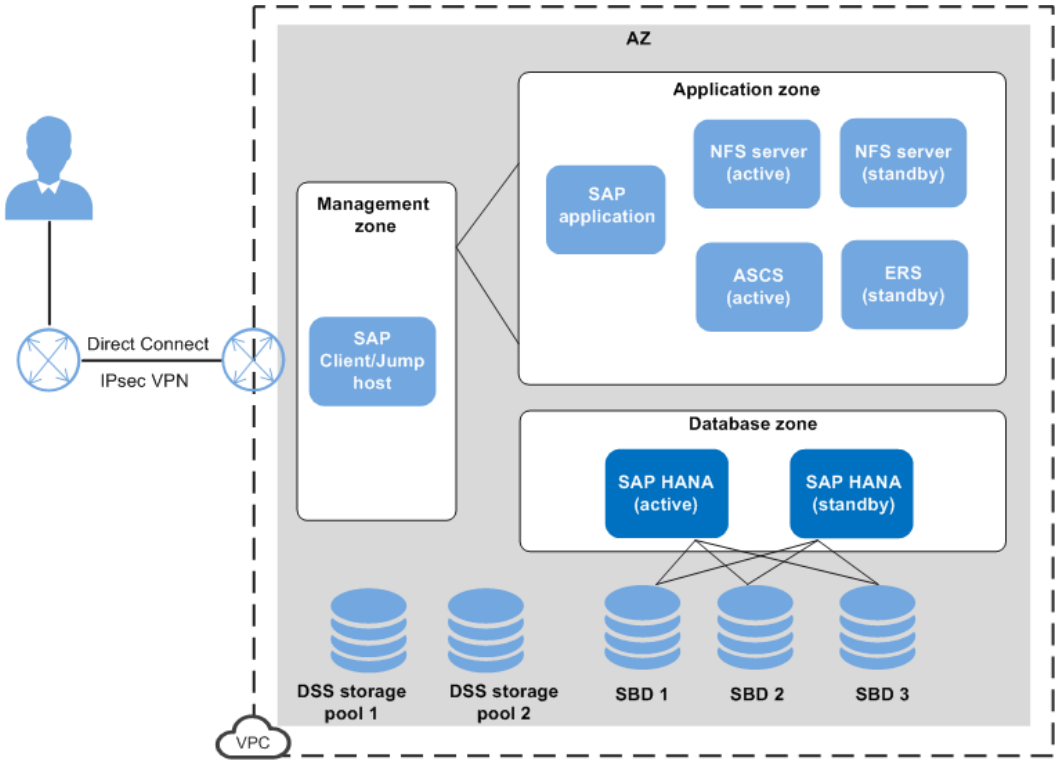
3.2 Deployment Scheme (iSCSI)

In HA scenarios where KunLun servers are used, iSCSI disks are used as SBD volumes for storage. In this scheme, skip the steps related to DESS. You can also use DESS for storage. For details, see section **Deployment Scheme (DESS)**.

Figure 3-3 shows the deployment scheme.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-3 KunLun servers in the HA deployment mode



The concepts involved in the preceding figure are as follows:

- VPC network: All nodes in the SAP system are deployed within a VPC and belong to the same AZ to ensure network security. The VPC network consists of three subnets in the management zone, application zone, and database zone, respectively.
- DSS storage pool 1 is a data production storage pool for SAP application nodes and the jump host, and DSS storage pool 2 is a data backup storage pool for SAP application nodes and database nodes. SBD 1, SBD 2, and SBD 3 are three SBD volumes of SAP HANA nodes.
- Management zone:
  - Jump host: ECS

    A tenant accesses the jump host and uses SSH to navigate to application nodes and database nodes. It is also used to deploy SAP Client software, such as SAP GUI and SAP HANA Studio.
- Database zone:

  SAP HANA node: Two KunLun servers are required for deploying SAP HANA. A BMS has the following disks attached:
  - OS disk: provides the directory for installing the OS.
  - Data volume: periodically stores the data transmitted from the SAP HANA IMDB (a database running in high-performance memory). The period is 5 minutes by default.
  - Log volume: stores the data triggered by an event. When an event, for example, a record or a batch of records are updated, is triggered for the server IMDB, the system will write the latest IMDB data into the log volume.

 Copyright © Huawei Technologies Co., Ltd.

  - Shared volume: stores the SAP HANA installation software and SAP HANA database log files.
  - Backup volume: stores the SAP HANA database backup files.
- Application zone:
  - SAP application node: ECS

    SAP application nodes are used to deploy SAP applications.
  - NFS servers: ECSs

    Two ECSs are required to work in the active/standby mode. SAP HANA and SAP NetWeaver share the NFS server. The backup volume of an SAP HANA node is provided by the NFS server. You can use SFS Turbo to provide shared file storage.

    NOTICE

    If you use SFS Turbo, you do not need to perform operations related to NFS servers in this document.
  - ASCS node: ECS

    The ASCS node works as the active node in the ASCS HA cluster, which is used to deploy the SAP NetWeaver ASCS instance.
  - ERS node: ECS

    The ERS node works as the standby node in the ASCS HA cluster, which is used to deploy the SAP NetWeaver ERS instance.

3.3 Data Planning

3.3.1 Network Planning

Networking Description

NOTE

- The network segments and IP addresses are for reference only. When iSCSI is used, three ECSs need to be connected to the server or backup plane. SBD volumes are attached to the ECSs.
- Application subnet: The IP addresses of the server/backup plane and heartbeat plane must belong to different subnets.
- Database subnet: The IP addresses of the server/backup plane and heartbeat plane must belong to different subnets.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-4 Network plane planning in the single-node deployment mode

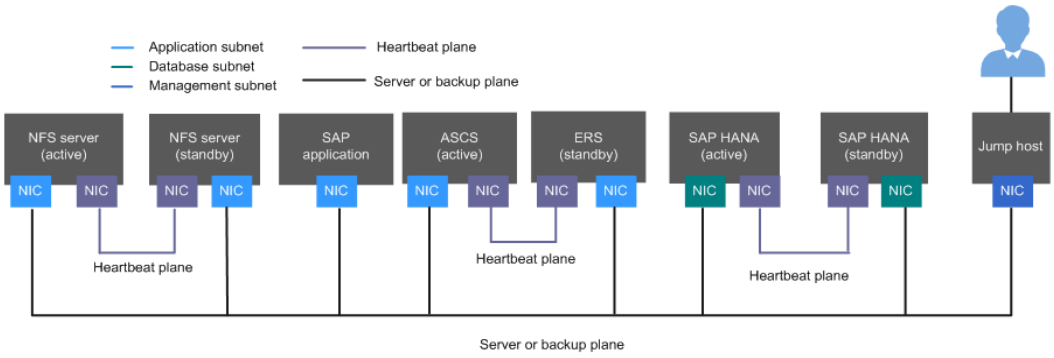


Table 3-1 shows the planned network information.

Table 3-1 Network planning information

Subnet	Plane	Description	Example Value
Application subnet	Server/backup plane	Specifies the IP address of the primary NIC plane. Allows SAP application nodes to communicate with the SAP HANA database nodes or the SAP GUI client nodes. Allows the backup volume on the NFS server to be shared with all SAP application nodes and database nodes.	ASCS node: 10.0.5.11 ERS node: 10.0.5.12 SAP application node: 10.0.5.4 NFS server: 10.0.5.101 to 10.0.5.102 NFS server floating IP address: 10.0.5.103
	Heartbeat plane	Allows SAP NetWeaver nodes to communicate with each other. Specifies the IP address of the plane that SAP application nodes and NFS server use to transmit heartbeat signals to perform automatic active/standby switchovers when a node is faulty.	ASCS node: 10.0.4.11 ERS node: 10.0.4.12 NFS server: 10.0.4.101 to 10.0.4.102

 Copyright © Huawei Technologies Co., Ltd.

Subnet	Plane	Description	Example Value
Database subnet	Server/backup plane	Allows an SAP HANA node to communicate with service software (such as ERP) or SAP HANA Studio client software.	SAP HANA node: 10.0.3.2 to 10.0.3.3 SAP HANA node floating IP address: 10.0.3.103
	Heartbeat plane	Specifies the IP address of the plane that SAP HANA nodes use to implement System Replication and transmit heartbeat signals to perform automatic active/standby switchovers when a node is faulty.	SAP HANA node: 10.0.4.2 to 10.0.4.3
Management subnet	Server/backup plane	Allows the jump host to switch to application nodes and database nodes.	Jump host: 10.0.0.202

Figure 3-5 Network plane planning in the cluster deployment mode

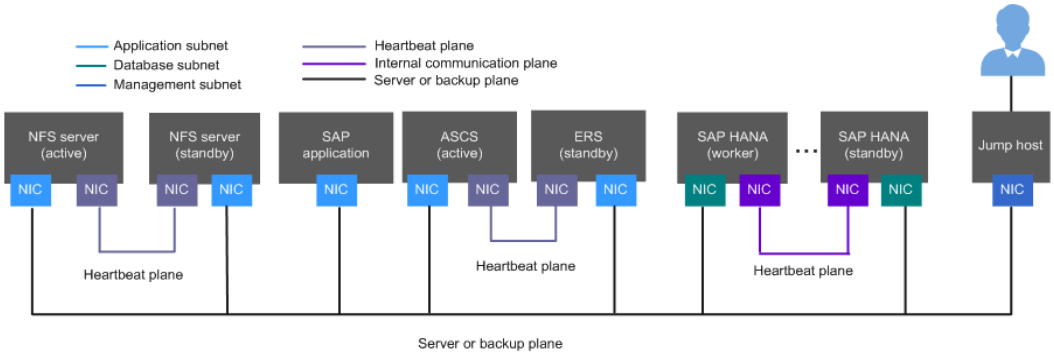


Table 3-2 shows the planned network information.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-2 Network planning information

Subnet	Plane	Description	Example Value
Application subnet	Server/ backup plane	Specifies the IP address of the primary NIC plane. Allows SAP application nodes to communicate with the SAP HANA database nodes or the SAP GUI client nodes. Allows the backup volume on the NFS server to be shared with all SAP application nodes and database nodes.	ASCS node: 10.0.5.11 ERS node: 10.0.5.12 SAP application node: 10.0.5.4 NFS server: 10.0.5.101 to 10.0.5.102 NFS server floating IP address: 10.0.5.103
	Heartbeat plane	Allows SAP NetWeaver nodes to communicate with each other. Specifies the IP address of the plane that SAP application nodes and NFS server use to transmit heartbeat signals to perform automatic active/ standby switchovers when a node is faulty.	ASCS node: 10.0.4.11 ERS node: 10.0.4.12 NFS server: 10.0.4.101 to 10.0.4.102
Database subnet	Server/ backup plane	Allows an SAP HANA node to communicate with service software (such as ERP) or SAP HANA Studio client software.	SAP HANA node: 10.0.3.2 to 10.0.3.4
	Internal communicati on plane:	Allows SAP HANA nodes to communicate with each other.	SAP HANA node: 10.0.2.2 to 10.0.2.4
Manageme nt subnet	Server/ backup plane	Allows the jump host to switch to application nodes and database nodes.	Jump host: 10.0.0.202

Security Group Rule

The following security group rules are recommended practices. You can configure your own security group rules as you need.

For details about SAP HANA security group rules, see section "Network Planning" in the *SAP HANA User Guide (BMS Cluster Deployment)*.

 Copyright © Huawei Technologies Co., Ltd.

For details about SAP NetWeaver security group rules, see section "Network Planning" in the *SAP NetWeaver User Guide*.

For more information about specific ports and security group rules to be accessed by SAP, see **SAP official documents**.

3.3.2 SAP HANA Node Planning

Single-Node Planning

Table 3-3 SAP HANA node planning

Flavor	CPU Number and Model	Memory	OS and Disk
physical.m2.medium	4 x Broadwell EX 8890 v4	2 TB	OS: SUSE Linux Enterprise Server 12 SP2 for SAP Local disk: • OS volume: 2 x 600 GB, SAS disk, hardware RAID 1 • Log volume: 2 x 1.6 TB ES3600, SSD disk, software RAID 1 • Data volume: 6 TB • Shared volume: 2 TB • SBD volume: 10 GB, DSS production storage pool, high I/O, SCSI, shared disk Use LVM to logically divide the local disk (7 x 1.8 TB 10K 2.5 SAS HDD, hardware RAID 5) into a data volume and a shared volume.

 Copyright © Huawei Technologies Co., Ltd.

Flavor	CPU Number and Model	Memory	OS and Disk
physical.kl1.2xlarge.hba	8*Broadwell EX 8880 v4	4 TB	OS: SUSE Linux Enterprise Server 12 SP2 for SAP Local disk: • OS volume: 2 x 600 GB, SAS disk, hardware RAID 1 • Log volume: 512 GB • Data volume: 12 TB • Shared volume: 4 TB • SBD volume (DESS scheme): 10 GB, DESS storage pool, ultra-high I/O, SCSI, shared disk • SBD volume (iSCSI scheme): 10 GB, SCSI Use LVM to logically divide the local disk (13 x 3.2 TB SAS disk, hardware RAID 50) into a log volume, a data volume, and a shared volume.

Clustered Node Planning

Table 3-4 SAP HANA node planning

Flavor	CPU Number and Model	Memory	OS and Disk
physical.m2.medium.hba	4 x Broadwell EX 8890 v4	2 TB	OS: SUSE Linux Enterprise Server 12 SP2 for SAP Local disk: • OS volume: 2 x 600 GB, SAS disk, hardware RAID 1 • Log volume: 512 GB, DESS storage pool, ultra-high I/O, SCSI, shared disk • Data volume: 512 GB, DESS storage pool, ultra-high I/O, SCSI, shared disk **NOTE** In the cluster deployment mode, a standby node only requires an OS volume.

 Copyright © Huawei Technologies Co., Ltd.

3.3.3 SAP NetWeaver Node Planning

This section describes SAP NetWeaver node planning in the distributed HA deployment mode. For details about node planning in other deployment modes, see the **SAP NetWeaver User Guide**.

NOTE

The flavors are only for reference. The ECS specifications are recommended examples. Choose one based on the SAP Sizing results.

Table 3-5 ECS specifications for SAP NetWeaver

Flavor	vCPUs	Memory (GB)
h1.8xlarge.4	32	128
h1.4xlarge.4	16	64
h1.2xlarge.4	8	32
h1.xlarge.4	4	16
m3.large.8	2	16
m3.xlarge.8	4	32
m3.2xlarge.8	8	64
m3.4xlarge.8	16	128
m3.8xlarge.8	32	256

For details about data planning, see **Table 3-6**. For the actual hardware usage, evaluate the SAP Application Performance Standard (SAPS) value based on the standard SAP Sizing method. Then apply for the ECSs based on the evaluation results. For details, see **SAP Quick Sizer**.

For details about the minimum hard disk space, RAM, and minimum software requirements of each component in SAP NetWeaver, see the SAP note **1953429** and **SAP Installation Guides**.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-6 Recommended ECS node planning

Node	Specifications
SAP NetWeaver ECS planning in the distributed HA deployment mode	Recommended configurations: • OS: SUSE Linux Enterprise Server 12 SP2 for SAP • Flavor: h1.2xlarge.4 (8 vCPUs and 32 GB memory) • Disk: – System disk: ultra-high I/O, 100 GB – Data disk (created on the active node): ultra-high I/O, SCSI, shared disk, 170 GB. After a data disk is created, bind it to the standby node. Only create a system disk for the standby node.

Table 3-7 lists the file system planning of the data disk in the distributed HA deployment mode.

Table 3-7 Planning of the data disk file system

Partition	Capacity (GB)	Mounting Directory	Description
sda1	10 GB	-	Used as the SBD volume.
sda2	80 GB	/usr/sap/<SID>/ASCS<##>	Partition of the active ASCS node, which is used to install the ASCS node.
sda3	80 GB	/usr/sap/<SID>/ERS<##>	Partition of the standby ASCS node, which is used to install the ERS node.

In the distributed HA deployment scenario, shared files are provided by the NFS server. Table 3-8 lists the file system planning.

Table 3-8 Planning of the shared file system

Partition	Capacity (GB)	Mounting Directory	Description
sde1	100 GB	/sapmnt	Shared to all nodes in the SAP NetWeaver system

 Copyright © Huawei Technologies Co., Ltd.

Partition	Capacity (GB)	Mounting Directory	Description
sde2	10 GB	/usr/sap/A01/SYS	Shared to all nodes in the SAP NetWeaver system **NOTE** **A01** in the mounting directory is the **SID** of SAP NetWeaver. Create a directory based on the actual condition.
sde3	100 GB	/sapcd	Shared to all nodes in the SAP NetWeaver system

3.3.4 SAP Application Node Planning

Table 3-9 SAP application ECS specifications

Flavor	vCPUs	Memory (GB)
h1.8xlarge.4	32	128
h1.4xlarge.4	16	64
h1.2xlarge.4	8	32
h1.xlarge.4	4	16
m3.large.8	2	16
m3.xlarge.8	4	32
m3.2xlarge.8	8	64
m3.4xlarge.8	16	128
m3.8xlarge.8	32	256

Table 3-10 lists the planning of SAP application nodes.

Table 3-10 SAP application node planning

Node	Specifications
SAP application node	• OS: SUSE Linux Enterprise Server 12 SP2 for SAP or SUSE Linux Enterprise Server 12 SP1 for SAP • Disk: Configure it as required.

Before applying for cloud services for SAP applications, evaluate the SAP Application Performance Standard (SAPS) value based on the standard SAP Sizing

 Copyright © Huawei Technologies Co., Ltd.

method. Then apply for the ECSs based on the evaluation results. For details, see **SAP Quick Sizer**.

For details about the minimum hard disk space, RAM, and minimum software requirements on each component of SAP applications, see SAP note **1953429** and **SAP Installation Guides**.

3.3.5 Other Node Planning

Table 3-11 lists the planning of other nodes.

Table 3-11 Other node planning

Node	OS and Specifications
NFS server	The active and standby NFS servers need to be deployed for the production system. • OS: SUSE Linux Enterprise Server 12 SP2 for SAP • Flavor: h1.xlarge.4 (4 vCPUs and 16 GB memory capacity) • Disk: **NOTE** If two NFS servers are required to work in active/standby mode, each type of the shared, backup, and SBD volumes requires one for the two NFS servers. – System disk: 60 GB, DSS production storage pool, high I/O, non-shared disk – Shared volume: Number of worker nodes/4 x Memory size. The value of number of worker nodes/4 is rounded up for decimal places. This volume is required only in the cluster deployment mode. DSS production storage pool, high I/O, SCSI, shared disk – Backup volume: DSS production storage pool, **high I/O**, SCSI, shared disk The recommended size is at least three times that of the memory size. – SBD volume: 10 GB, DSS production storage pool, high I/O, SCSI, shared disk – Data volume: 210 GB, DSS production storage pool, high I/O, SCSI, shared disk This volume is used for SAP NetWeaver system file sharing.

 Copyright © Huawei Technologies Co., Ltd.

Node	OS and Specifications
Jump host	• OS: **NOTE** Windows ECSs are available for deploying SAP HANA Studio. Select a Windows or Linux ECS as required to deploy SAP HANA Studio. – Windows: Windows Server 2008 – Linux: SUSE Linux Enterprise Server 12 SP2 for SAP • Flavor: h1.xlarge.4 (4 vCPUs and 16 GB memory capacity) • System disk: 60 GB, high I/O, non-shared disk

3.4 Software and Tools

Table 3-12 lists the software and tools to be obtained.

NOTE

On the local computer, download the **readme.txt** file at **https://obs-sap.obs.myhwclouds.com/readme.txt**. Then, obtain the paths where the software and configuration scripts are stored.

Table 3-12 Required software and tools

Item	Description
WinSCP	Uploads key files to cloud servers.
PuTTY and PuTTYgen	Used for logging in to a cloud server and running commands.
SAP HANA 1.0 SAP HANA 2.0	SAP HANA installation package
SAP HANA Studio	SAP HANA Studio installation package
VNC Viewer for Windows	Used for providing the GUI on the local computer for installing SAP NetWeaver
SAP GUI 7.4	SAP system client The SAP GUI 7.4 or a latter version is recommended.
SWPM	Used for upgrading, migrating, and installing SAP systems The latest version released by SAP is recommended.
SAP NetWeaver	SAP NetWeaver installation package
Configuration script	Contains the script and configuration file used for installing and configuring the SAP system.

 Copyright © Huawei Technologies Co., Ltd.

3.5 Preparing Network Resources

3.5.1 Creating a VPC

Creating a VPC

Step 1 Log in to the management console.

Step 2 In the navigation pane on the left, click ☰ and choose **Network** > **Virtual Private Cloud**.

Step 3 Click **Create VPC**.

Step 4 On the displayed page, configure VPC parameters.

Set the parameters as follows:

- **CIDR Block**: specifies the IP address range for the VPC. Configure this parameter based on the planned subnet information.
- **CIDR Block**: specifies the IP address range for the default VPC subnet. Ensure that the IP address range for the default VPC subnet is within the IP address range for the VPC subnet. Configure this parameter based on the planned information.
- **DNS Server Address**: The external DNS server address is used by default. If you need to change the DNS server address, ensure that the DNS server addresses are available.

Step 5 Complete the VPC creation.

----End

3.5.2 Creating a Subnet and Configuring a Security Group

To ensure proper communication between the ECSs in an SAP HANA system, create a subnet for the ECSs and configure a proper security group.

Procedure

Step 1 Create a subnet.

1. Log in to the management console.
2. Click 📍 in the upper left corner and select a region and project.
3. In the navigation pane on the left, click ☰ and choose **Network > Virtual Private Cloud**.
4. Click the VPC to which the SAP HANA system belongs.
5. Click the **Subnets** tab and then **Create Subnet**.
6. In the **Create Subnet** pane, configure parameters as prompted.
   - **AZ**: specifies the AZ of the subnet.
   - **Name**: Configure the subnet name that is easy to identify, for example, **service_subnet**.

 Copyright © Huawei Technologies Co., Ltd.

- **CIDR Block**: Configure this parameter according to the deployment plan described in section **Network Planning**.
- **Advanced Settings**: Set it to **Default**.

7. Click **OK** to complete the subnet configuration.
8. Repeat **Step 1.5** to **Step 1.7** to create all required subnets according to the requirements specified in section **Network Planning**.

Step 2 Configure a security group.

You need to create a security group for all nodes in the SAP HANA system.

1. Choose **Access Control > Security Groups** on the left and then click **Create Security Group** in the upper right corner. The **Create Security Group** dialog box is displayed.
2. Set the following parameters as prompted:
   - **Template**: The template contains security group rules, which help you quickly create a security group. The following templates are provided:
     - **Custom**: This template allows you to create security groups with custom security group rules.
     - **General-purpose web server**: The security group that will be created using this template is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and allow inbound traffic on ports 22, 80, 443, and 3389.
     - **All ports open**: The security group that will be created using this template includes default rules that allow inbound traffic on any port. Allowing inbound traffic on any port may pose security risks. Exercise caution when using this template.
   - **Name**: specifies the name of the security group. Name the security group that is easy to identify, for example, **studio_security_group**.
   - **Enterprise Project**: You can add the security group to an enabled enterprise project. You can select an enterprise project from the drop-down list.
3. Click **OK**.
4. Repeat **Step 2.1** to **Step 2.3** to create other security groups.
5. In the navigation pane on the left, choose **Access Control** > **Security Groups**. In the security group list, click the security group to which you want to add an access rule.
6. Click **Add Rule** on the **Inbound Rules** or **Outbound Rules** tab as planned.
7. On the displayed page, add the rule according to the requirements specified in section **Network Planning**.

   The default security group rules cannot be deleted.
8. Repeat **Step 2.5** to **Step 2.7** to configure all security groups.

----End

 Copyright © Huawei Technologies Co., Ltd.

3.5.3 (Optional) Creating an SFS Turbo File System

If you want to use SFS Turbo instead of the NFS to provide shared file storage, such as HANA database backup volume and shared volume, you need to create an SFS Turbo file system to offer the shared path to SAP nodes.

NOTICE

If you use SFS Turbo, you do not need to perform operations related to NFS servers in this document.

Prerequisites

Ensure that the dedicated computing and storage resources are in the same DeC.

Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the console, and select a region and project.

Step 3 In the navigation pane on the left, click and choose **Scalable File Service** under **Storage**. The **Scalable File Service** page is displayed.

Step 4 Click **Create File System**.

Step 5 Configure the parameters listed in **Table 3-13**.

Table 3-13 Configuration parameters

Parameter	Description	Example Value
File System Type	Specifies the file system type. Select **SFS Turbo**.	SFS Turbo
Billing Mode	Select a mode based on your need.	Yearly/Monthly
Region	Select the target region.	CN North-Beijing4
AZ	Specifies the AZ where the file system is located. Select an AZ as needed.	AZ1
Protocol Type	Specifies the file service type. Set this parameter to **NFS**.	NFS
Storage Class	Select a storage class as required.	Standard
Capacity	Specifies the maximum capacity of a single file system. When the used capacity of a file system reaches this value, no more data can be written to the file system. You need to expand the file system.	5 TB

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
VPC	Select the VPC and subnet used by the ECS. For details, see **Creating a VPC** and **Creating a Subnet and Configuring a Security Group**.	N/A
Security Group	Select the security group where the ECS belongs. For details, see **Creating a Subnet and Configuring a Security Group**.	N/A
Enterprise Project	Select the project you need.	SAP
Automatic Backup	This parameter is optional. SFS Turbo provides the automatic backup function. You can back up data of the file system by setting the backup policy. After a backup policy is enabled, the system automatically backs up file system data at the specified time. Select **Enable automatic backup**. After a backup policy is enabled, you need to set the backup start time and backup cycle. You can create backup policies based on service requirements. For details, see **Table 3** in section "Creating a File System" of the *Scalable File Service Getting Started*.	N/A
Name	Specifies the file system name.	sfs-turbo-backup
Quantity	Select the quantity according to the site requirements.	1 year

Step 6 Click **Create Now**. On the displayed page, confirm the configuration information and click **Submit**.

Step 7 Go back to the file system list. On the displayed page, locate the new file system by its name in the file system list on the right. In the **Shared Path** column, query the shared path.

Step 8 Log in to an SAP HANA ECS and check whether the IP address of the DNS server is configured in the **/etc/resolv.conf** file. If not, write the IP address of the DNS server into the **/etc/resolv.conf** file.

----End

 Copyright © Huawei Technologies Co., Ltd.

3.5.4 Applying for Dedicated Storage Pools

Scenarios

To ensure the service reliability of an SAP system, you need to create two dedicated storage pools on a DeC. One is used to back up data of all nodes in the SAP system and the other is used to store data of all SAP applications.

Procedure

Step 1 Log in to the management console. In the navigation pane on the left, click ☰ and choose **Dedicated Cloud** under **Computing**. On the displayed **Dedicated Cloud Console** page, choose **Dedicated Distributed Storage Service** in the navigation pane.

Step 2 On the displayed page, click **Apply for Storage Pool**.

Step 3 Configure the parameters as planned.

Note the following:

- The storage pool name can contain a maximum of 255 characters. It is recommended that the name contains identifiable words, such as production and backup.
- Set **Type** to **High I/O**.

Step 4 Click **Apply Now**.

----End

3.5.5 Creating an SAP HANA BMS

Scenarios

SAP HANA runs on BMSs. Thus, you need to apply for BMSs on the DeC. BMSs use local disks.

Procedure

Step 1 Log in to the management console. In the navigation pane on the left, click ☰ and choose **Computing** > **Bare Metal Server**.

Step 2 On the displayed page, click **Provision BMS in DeC**.

Step 3 Configure the parameters based on section **SAP HANA Node Planning**.

Note the following:

- The BMS name contains a maximum of 13 characters.
- An EIP has not been bound to the target BMS.
- Select **Key pair** for **Login Mode**. Ensure that all nodes in the SAP system use the same key. Otherwise, the SAP software installation will fail.

 Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> If you choose an existing SSH key certificate from the drop-down list, make sure that you have saved the certificate locally. Otherwise, you may fail to log in to the BMS.
>
> To create a key, do as follows:
>
> Click **View Key Pair**. On the displayed **Key Pair** page, click **Create Key Pair**, specify the key pair name, and click **OK**. In the **Information** dialog box that is displayed, click **OK**. Then, you can view and save the private key as prompted.

Step 4 Click **Buy Now**. Switch to the BMS management page and check the status of the created BMS.

After the BMS is created, you can view the BMS from the BMS list on the right of the page.

Step 5 Change the password of user **root** for logging in to all BMSs.

Securely keep the **root** password. In addition, ensure that all ECSs and BMSs in the SAP system use the same **root** password.

1. Log in to a BMS.
2. Run the following command to switch to user **root**:

   sudo su -
3. Run the following command to change the password of user **root**:

   passwd

   Enter the password as prompted for confirmation.

Step 6 Open the **/etc/fstab** file and add the parameter **nofail** to the end of the **/usr/sap** directory.

An example is provided as follows:

```
/dev/vg_os/lv_usrsap /usr/sap           ext4    acl,user_xattr      1 2
```

Add the parameter **nofail** to the file as follows:

```
/dev/vg_os/lv_usrsap /usr/sap           ext4    acl,user_xattr,nofail      1 2
```

----End

3.5.6 Creating Other Nodes

Scenarios

In the SAP system, SAP HANA is deployed on BMSs while other software systems are deployed on ECSs.

- Jump host uses an ECS. You can access the jump host and use SSH to navigate to SAP HANA nodes and SAP application nodes. It is also used to deploy SAP Client software, such as SAP GUI and SAP HANA Studio.
- Two ECSs are required for NFS servers to provide shared and backup volumes and share them with the SAP nodes.
- SAP applications are deployed on ECSs.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the management console. In the navigation pane on the left, click and choose **Computing** > **Elastic Cloud Server**.

Step 2 On the displayed page, click **Buy ECS**.

Step 3 Configure the parameters based on section **Other Node Planning**.

Note the following:

- The ECS name contains a maximum of 13 characters.
- Select **DSS** for **Disk** and select the storage pool to which the disk belongs based on the deployment scheme.
- An EIP has not been bound to the target ECS.

  NOTE

  When you create a jump host, you can determine whether to bind an EIP based on actual requirements.
- Select **Key pair** for **Login Mode**. Ensure that all nodes in the SAP system use the same key. Otherwise, the SAP software installation will fail.
- The active and standby ASCS nodes must belong to the same ECS group, which must be different from the ECS group to which the SAP HANA nodes and NFS servers belong.
- The active and standby NFS servers must belong to the same ECS group, which must be different from the ECS group to which SAP HANA nodes and SAP NetWeaver nodes belong.

Step 4 Create other ECSs as required.

Step 5 Change the password of user **root** for logging in to all ECSs.

Securely keep the **root** password. In addition, ensure that all ECSs use the same **root** password.

1. Log in to an ECS.
2. Run the following command to switch to user **root**:

   sudo su -
3. Run the following command to change the password of user **root**:

   passwd

   Enter the password as prompted for confirmation.

----End

3.5.7 Configuring SSH Switching Permissions

Scenarios

To switch to an SAP node from the jump host and to allow SSH switchovers between SAP nodes, you must configure the nodes to be trusty.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Upload the key file to the jump host.

1. Use WinSCP to log in to the jump host. Ensure that user **root** and the key file are used for authentication. Upload the certificate private key file (.pem file) to the directory **/usr** on the jump host.
2. Copy the certificate private key file to the **/root/.ssh** directory and rename the file **id_rsa**.

   For example, if the original file name is **private.pem**, run the following commands to rename it:

   cp /usr/private.pem /root/.ssh/id_rsa

   cd /root/.ssh/

   chmod 600 id_rsa
3. Run the following command to generate a public key file:

   cat authorized_keys >>id_rsa.pub

Step 2 Use the server/backup plane IP address to allocate the locally stored public key file to an SAP HANA node.

Ensure that the SAP HANA node cannot be the planned standby node and the subsequent operations to manually install SAP HANA must be performed on this node.

The command is in the following format:

scp /root/.ssh/id_rsa.pub *Peer IP address*:**/root/.ssh/**

Step 3 Use the server/backup plane IP address to allocate the private key file and **authorized_keys** file to all nodes excepting the SAP HANA Studio node.

The commands are in the following format:

scp /root/.ssh/id_rsa *Peer IP address*:**/root/.ssh/id_rsa**

scp /root/.ssh/authorized_keys *Peer IP address*:**/root/.ssh/**

Step 4 Verify the switching.

Use SSH to switch from the jump host to all nodes excepting the SAP HANA Studio node for verification.

For example, the server/backup plane IP address of the NFS server is 10.0.5.101. To switch from the jump host to the NFS server, run the following command:

ssh 10.0.5.101

----End

 Copyright © Huawei Technologies Co., Ltd.

3.5.8 Configuring an IP Address for a BMS NIC (Cluster Deployment)

Scenarios

After applying for a BMS for an SAP HANA cluster, you must manually configure an IP address for the BMS NIC on the internal communication plane to meet SAP system deployment requirements.

Procedure

Step 1 Use a key to log in to the BMS as user **root**.

Step 2 Run the following command to check the NIC information:

ip link

Information similar to the following is displayed:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group
default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 8888 qdisc mq master bond0 state UP mode
DEFAULT group default qlen 1000
    link/ether fa:16:3e:3d:1c:e0 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 8888 qdisc mq master bond0 state UP mode
DEFAULT group default qlen 1000
    link/ether fa:16:3e:3d:1c:e0 brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state DOWN mode DEFAULT group
default qlen 1000
    link/ether 38:4c:4f:89:55:8d brd ff:ff:ff:ff:ff:ff
5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state DOWN mode DEFAULT group
default qlen 1000
    link/ether 38:4c:4f:89:55:8e brd ff:ff:ff:ff:ff:ff
6: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 8888 qdisc noqueue state UP mode
DEFAULT group default
    link/ether fa:16:3e:3d:1c:e0 brd ff:ff:ff:ff:ff:ff
```

Step 3 Configure the udev rules.

Run the following command to create the **80-persistent-net.rules** file:

cp /etc/udev/rules.d/70-persistent-net.rules /etc/udev/rules.d/80-persistent-net.rules

Write the NIC MAC address and name that are queried in **Step 2** and that are not displayed in **80-persistent-net.rules** to the file. In this way, after the BMS is restarted, the NIC name and sequence will not change.

NOTE

Ensure that NIC MAC address and name are lowercase letters.

vim /etc/udev/rules.d/80-persistent-net.rules

The modification result is as follows:

```
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="38:4c:4f:29:0b:e0", NAME="eth0"
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="38:4c:4f:29:0b:e1", NAME="eth1"
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="38:4c:4f:89:55:8d", NAME="eth2"
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="38:4c:4f:89:55:8e", NAME="eth3"
```

 Copyright © Huawei Technologies Co., Ltd.

After the modification, save the change and exit.

Step 4 Run the following command to check the NIC IP address:

ifconfig

Information similar to the following is displayed, where **bond0** shows the NIC IP address automatically allocated by the system when you apply for the BMS:

```
bond0     Link encap:Ethernet  HWaddr FA:16:3E:3D:1C:E0
          inet addr:10.0.3.2  Bcast:10.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::f816:3eff:fe3d:1ce0/64 Scope:Link
          UP BROADCAST RUNNING MASTER MULTICAST  MTU:8888  Metric:1
          RX packets:852 errors:0 dropped:160 overruns:0 frame:0
          TX packets:1121 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:125429 (122.4 Kb)  TX bytes:107221 (104.7 Kb)

eth0      Link encap:Ethernet  HWaddr FA:16:3E:3D:1C:E0
          UP BROADCAST RUNNING SLAVE MULTICAST  MTU:8888  Metric:1
          RX packets:428 errors:0 dropped:10 overruns:0 frame:0
          TX packets:547 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:64670 (63.1 Kb)  TX bytes:50132 (48.9 Kb)

eth1      Link encap:Ethernet  HWaddr FA:16:3E:3D:1C:E0
          UP BROADCAST RUNNING SLAVE MULTICAST  MTU:8888  Metric:1
          RX packets:424 errors:0 dropped:7 overruns:0 frame:0
          TX packets:574 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:60759 (59.3 Kb)  TX bytes:57089 (55.7 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:520 (520.0 b)  TX bytes:520 (520.0 b)
```

Step 5 View the names of bonded NICs.

The in-service bonded NICs cannot be used on the internal communication plane. Therefore, you must obtain them by name.

cd /etc/sysconfig/network

vi ifcfg-*bond0*

Information similar to the following is displayed, where **bond0** is composed of NICs **eth0** and **eth1**:

```
BONDING_MASTER=yes
TYPE=Bond
STARTMODE=auto
BONDING_MODULE_OPTS="mode=4 xmit_hash_policy=layer3+4 miimon=100"
NM_CONTROLLED=no
BOOTPROTO=dhcp
DEVICE=bond0
USERCONTRL=no
LLADDR=fa:16:3e:3d:1c:e0
BONDING_SLAVE1=eth1
BONDING_SLAVE0=eth0
```

After the query, exit.

 Copyright © Huawei Technologies Co., Ltd.

Step 6 Run the following command to check the statuses of all NICs:

ip link

Information similar to the following is displayed:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group
default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 8888 qdisc mq master bond0 state UP mode
DEFAULT group default qlen 1000
    link/ether fa:16:3e:3d:1c:e0 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 8888 qdisc mq master bond0 state UP mode
DEFAULT group default qlen 1000
    link/ether fa:16:3e:3d:1c:e0 brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state DOWN mode DEFAULT group
default qlen 1000
    link/ether 38:4c:4f:89:55:8d brd ff:ff:ff:ff:ff:ff
5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state DOWN mode DEFAULT group
default qlen 1000
    link/ether 38:4c:4f:89:55:8e brd ff:ff:ff:ff:ff:ff
6: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 8888 qdisc noqueue state UP mode
DEFAULT group default
    link/ether fa:16:3e:3d:1c:e0 brd ff:ff:ff:ff:ff:ff
```

Step 7 Change the NIC status **qdisc mq state DOWN** to **qdisc mq state UP**. The following commands use NICs **eth2** and **eth3** as examples.

ip link set *eth2* **up**

ip link set *eth3* **up**

Step 8 Run the following command to check the statuses of all NICs again:

ip link

Information similar to the following is displayed:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group
default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 8888 qdisc mq master bond0 state UP mode
DEFAULT group default qlen 1000
    link/ether fa:16:3e:3d:1c:e0 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 8888 qdisc mq master bond0 state UP mode
DEFAULT group default qlen 1000
    link/ether fa:16:3e:3d:1c:e0 brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group
default qlen 1000
    link/ether 38:4c:4f:89:55:8d brd ff:ff:ff:ff:ff:ff
5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group
default qlen 1000
    link/ether 38:4c:4f:89:55:8e brd ff:ff:ff:ff:ff:ff
6: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 8888 qdisc noqueue state UP mode
DEFAULT group default
    link/ether fa:16:3e:3d:1c:e0 brd ff:ff:ff:ff:ff:ff
```

Step 9 Check the statuses of the NICs in **Step 8** and obtain the names of the NICs in **qdisc mq state UP** status.

Only the NICs that are in **qdisc mq state UP** status and have not been used can be bonded. In this example, such NICs are **eth2** and **eth3**.

The LLADR values of NICs **eth2** and **eth3** are **38:4c:4f:89:55:8d** and **38:4c:4f:89:55:8e**, respectively.

Step 10 Run the following commands to create the configuration files of NICs **eth2** and **eth3**:

 Copyright © Huawei Technologies Co., Ltd.

You can copy an existing NIC configuration file and modify it to improve the creation efficiency.

cp *ifcfg-eth0 ifcfg-eth2*

cp *ifcfg-eth1 ifcfg-eth3*

Step 11 Run the following commands to modify the configuration files of NICs **eth2** and **eth3**:

vi *ifcfg-eth2*

vi *ifcfg-eth3*

Modified configuration file of NIC **eth2** is as follows.

In this configuration file, set **MTU** to **8888**, **BOOTPROTO** to **STATIC**, and configure **DEVICE** and **LLADDR** as required.

```
STARTMODE=auto
MTU=8888
NM_CONTROLLED=no
BOOTPROTO=STATIC
DEVICE=eth2
USERCONTRL=no
LLADDR=38:4c:4f:89:55:8d
TYPE=Ethernet
```

Modified configuration file of NIC **eth3** is as follows:

```
STARTMODE=auto
MTU=8888
NM_CONTROLLED=no
BOOTPROTO=STATIC
DEVICE=eth3
USERCONTRL=no
LLADDR=38:4c:4f:89:55:8e
TYPE=Ethernet
```

After the modification, save the change and exit.

Step 12 Bond NICs **eth2** and **eth3** to form, for example, **bond1**.

Run the following commands to create the **ifcfg-bond1** file and modify the configuration file:

cp *ifcfg-bond0 ifcfg-bond1*

vi *ifcfg-bond1*

Modified configuration file of NIC **bond1** is as follows.

In this configuration file, **MTU** is set to **8888**, **BONDING_MODULE_OPTS** is set to **mode=1 miimon=100**, **BOOTPROTO** is set to **STATIC**. **DEVICE**, **BONDING_SLAVE1**, **BONDING_SLAVE0**, **IPADDR**, **NETMASK**, and **NETWORK** are configured as required. **LLADDR** is set to the LLADDR value of the **BONDING_SLAVE1** NIC.

```
BONDING_MASTER=yes
TYPE=Bond
MTU=8888
STARTMODE=auto
BONDING_MODULE_OPTS="mode=1 miimon=100"
NM_CONTROLLED=no
BOOTPROTO=STATIC
```

 Copyright © Huawei Technologies Co., Ltd.

```
DEVICE=bond1
USERCONTRL=no
LLADDR=38:4c:4f:89:55:8d
BONDING_SLAVE1=eth2
BONDING_SLAVE0=eth3
IPADDR=10.0.2.2
NETMASK=255.255.255.0
NETWORK=10.0.2.0
```

After the modification, save the change and exit.

Step 13 Make the configuration file take effect.

1. Run the following commands to create a temporary directory and copy the NIC configuration file to this directory:

   mkdir /opt*/tmp/*

   mkdir /opt/tmp/*xml*

   cp /etc/sysconfig/network/ifcfg* /opt/tmp/

   cp /etc/sysconfig/network/config /opt/tmp/

   cp /etc/sysconfig/network/dhcp /opt/tmp/

2. Run the following commands to stop NICs to form **bond1**:

   ip link set *eth2* **down**

   ip link set *eth3* **down**

3. Run the following command to convert the NIC configuration file to a configuration file that can be recognized by the OS:

   /usr/sbin/wicked --log-target=stderr --log-level=debug3 --debug all convert --output /opt/tmp/xml /opt/tmp/

4. Run the following commands to restart the NICs to form **bond1**:

   ip link set *eth2* **up**

   /usr/sbin/wicked --log-target=stderr --log-level=debug3 --debug all ifup --ifconfig /opt/tmp/xml/*eth2***.xml** *eth2*

   ip link set *eth3* **up**

   /usr/sbin/wicked --log-target=stderr --log-level=debug3 --debug all ifup --ifconfig /opt/tmp/xml/*eth3***.xml** *eth3*

   /usr/sbin/wicked --log-target=stderr --log-level=debug3 --debug all ifup --ifconfig /opt/tmp/xml/bond1.xml *bond1*

Step 14 Run the following command to check IP addresses:

ip addr show

An example is provided as follows:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 8888 qdisc mq master bond0 state UP group default qlen 1000
    link/ether fa:16:3e:3d:1c:e0 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 8888 qdisc mq master bond0 state UP group default qlen 1000
    link/ether fa:16:3e:3d:1c:e0 brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 8888 qdisc mq master bond1 state UP group
```

 Copyright © Huawei Technologies Co., Ltd.

```
default qlen 1000
    link/ether 38:4c:4f:89:55:8d brd ff:ff:ff:ff:ff:ff
5: eth3: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 8888 qdisc mq master bond1 state UP group
default qlen 1000
    link/ether 38:4c:4f:89:55:8d brd ff:ff:ff:ff:ff:ff
6: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 8888 qdisc noqueue state UP group
default
    link/ether fa:16:3e:3d:1c:e0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.2/24 brd 10.0.3.255 scope global bond0
       valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fe3d:1ce0/64 scope link
       valid_lft forever preferred_lft forever
7: bond1: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 8888 qdisc noqueue state UP group
default
    link/ether 38:4c:4f:89:55:8d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.2/24 brd 10.0.2.255 scope global bond1
       valid_lft forever preferred_lft forever
    inet6 fe80::3a4c:4fff:fe29:b36/64 scope link
       valid_lft forever preferred_lft forever
```

Step 15 Run the following commands to delete the temporary directory:

cd /opt

rm -rf tmp/

Step 16 Perform the preceding operations to configure other BMSs.

----End

3.5.9 Configuring Mapping Between Hostnames and IP Addresses

Scenarios

During the SAP installation, installation programs use hostnames for communication. Therefore, you must configure the mapping between hostnames and IP addresses.

Procedure

Step 1 Log in to the jump host. Ensure that user **root** and the key file are used for authentication. Then, use SSH to switch to the BMS on which the SAP HANA is to be installed.

NOTE

In the cluster deployment scenario, you will switch to the first SAP HANA BMS. Then, you will perform operations on this BMS when installing SAP HANA.

Step 2 Run the following command to open the **hosts** file:

vi /etc/hosts

Step 3 Write the hostnames and IP addresses of all SAP nodes into the **hosts** file.

- In the single-node deployment mode, **IP-Address** is the IP address of the heartbeat plane for SAP HANA nodes. In the cluster deployment mode, **IP-Address** is the IP address of the internal communication plane for SAP HANA nodes.

 Copyright © Huawei Technologies Co., Ltd.

- Both **Full-Qualified-Hostname** and **Short-Hostname** are the node name, for example, **hana001**.

The format is **IP-Address Full-Qualified-Hostname Short-Hostname**.

NOTICE

In an SAP system, you must write the mapping between all SAP node IP addresses and node names into the **hosts** file.

You need to first bind the virtual IP addresses in the SAP NetWeaver system to the active and standby ASCS node names. The virtual IP addresses take effect only after the ASCS HA is configured. Do not bind virtual IP addresses to virtual hostnames before the virtual IP addresses take effect. After the ASCS and ERS instances are installed, write the mapping between the virtual IP addresses and virtual hostnames to the hosts file.

Step 4 Transfer the configured **/etc/hosts** file to other SAP HANA nodes:

The command is in the following format:

scp /etc/hosts *Peer IP address*:**/etc/hosts**

Step 5 Verify the SSH switching between SAP HANA nodes.

Use SSH to switch from one SAP HANA node to all SAP HANA nodes (including the current node) to ensure that the switching is correct.

For example, if the name of the peer SAP HANA node is **hana002**, run the following command:

ssh hana002

----End

3.5.10 Preparing for Storage Resources (iSCSI)

Scenarios

In the scenario where KunLun servers are highly available, iSCSI disks can be used as SBD volumes for storage. Perform operations in this section only in this scenario. In this scenario, three ECSs are required and must belong to the same ECS group. Each ECS is bound to a SCSI disk and iSCSI configuration is required for SBD. **Table 3-14** lists the ECS specifications.

Table 3-14 ECS specifications

OS	SUSE Linux Enterprise Server (SLES) 12 SP1
Specifications	s3.small.1 (1 vCPU and 1 GB memory) or higher specifications
Disk	System disk: high I/O (40 GB) Data disk: 10 GB, SCSI

 Copyright © Huawei Technologies Co., Ltd.

Network	Same as the SAP HANA server or backup plane

Prerequisites

You have created three ECSs.

Procedure

Software installation

NOTE

Before installing the software, update the software source. To do so, run the following command:

zypper ar --refresh *Software source network address*

The **open-iscsi** version must be **2.0.873-46.10.1**, the **yast2-iscsi-lio-server** version must be **3.1.19-4.5**, and the **targetcli** version must be **2.1-17.1**.

Step 1 Run the following command to install open-iscsi on the server side (three ECSs):

zypper in open-iscsi yast2-iscsi-lio-server targetcli

Step 2 Run the following command to install open-iscsi on the client side (SAP HANA node):

zypper in open-iscsi

Server side configuration

Step 3 Log in to a server side ECS.

Step 4 Run the following commands to configure automatic service startup:

systemctl enable targetcli

systemctl enable target

Step 5 Run the following command to create an Iblock device named **stonith_bd** using the drive letter **/dev/sda**:

targetcli /backstores/iblock create *stonith_bd /dev/sda*

NOTE

/dev/sda is the drive letter of the data volume. Set it based on the actual condition.

Step 6 Query the iSCSI IQN.

iscsi-iname

Information similar to the following is displayed:

```
iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5
```

Step 7 Create a target using the queried IQN.

targetcli /iscsi create *Queried IQN*

Information similar to the following is displayed:

 Copyright © Huawei Technologies Co., Ltd.

```
server:~ # targetcli /iscsi create iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5
Created target iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5.
Selected TPG Tag 1.
Created TPG 1.
```

Step 8 Run the following command to create a LUN:

targetcli /iscsi/*iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5***/tpg1/luns create** */backstores/iblock/stonith_bd*

Information similar to the following is displayed:

```
server:~ # targetcli /iscsi/iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5/tpg1/luns create /
backstores/fileio/stonith_bd
Selected LUN 0.
Created LUN 0.
```

NOTE

- *iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5* is the ID of **iqn**, which can be queried by running the **targetcli ls** command.
- */backstores/iblock/stonith_bd* is the Iblock device created in **Step 5**.

Step 9 Run the following command to create a portal:

targetcli /iscsi/*iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5***/tpg1/portals create**

Information similar to the following is displayed:

```
server:~ # targetcli /iscsi/iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5/tpg1/portals create
Using default IP port 3260
Automatically selected IP address 192.168.124.10.
Created network portal 192.168.124.10:3260.
```

NOTE

/*iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5* is the ID of **iqn**.

Step 10 Create an ACL.

1. Run the following command to view the **initiatorname.iscsi** file and obtain value of **InitiatorName**:

   cat /etc/iscsi/initiatorname.iscsi

   ```
   server:~ #cat /etc/iscsi/initiatorname.iscsi
   InitiatorName=iqn.1996-04.de.suse:01:f3cdb3b6ea6a
   ```

2. Run the following command to create an ACL using the value of **InitiatorName**:

   targetcli /iscsi/*iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5***/tpg1/acls create** *iqn.1996-04.de.suse:01:f3cdb3b6ea6a*

   Information similar to the following is displayed:

   ```
   server:~ # targetcli /iscsi/iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5/tpg1/acls create
   iqn.1996-04.de.suse:01:f3cdb3b6ea6a
   Created Node ACL for iqn.1996-04.de.suse:01:f3cdb3b6ea6a
   Created mapped LUN 0.
   ```

Step 11 Run the following command to disable the authentication:

targetcli /iscsi/*iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5***/tpg1 set attribute authentication=0**

Information similar to the following is displayed:

 Copyright © Huawei Technologies Co., Ltd.

```
server:~ # targetcli /iscsi/iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5/tpg1 set attribute
authentication=0
Parameter authentication is now '0'.
```

Step 12 Run the following command to save the configuration:

targetcli saveconfig

NOTE

If an error is reported, locate the error, delete **.aslist ()**, and save the configuration.

Step 13 Log in to the other two ECSs of the server side one by one and repeat **Step 4** to **Step 12** to configure the server side.

Client side configuration

Step 14 Log in to an SAP HANA node (client side) and attach the iSCSI disk of a server side ECS to the SAP HANA node.

iscsiadm -m discovery -t sendtargets -p *10.0.3.250*:**3260**

iscsiadm -m node -p *10.0.3.250*:**3260 --login**

NOTE

- *10.0.3.250* is the IP address of the server side ECS and 3260 is the default port number of iSCSI.
- Attach three iSCSI disks of three server side ECSs to the SAP HANA node.
- You can run the **fdisk –l** command to view the newly attached disks.

Step 15 Run the following command to attach iSCSI disks automatically once the SAP HANA node starts:

iscsiadm -m node -T *iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5* **-p** *10.0.3.250* **--op update -n node.startup -v automatic**

NOTE

- *iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5* is the ID of **iqn**
- *10.0.3.250* is the IP address of a server side ECS.

Step 16 Log in to other SAP HANA nodes and repeat **Step 14** to **Step 15** to configure all SAP HANA nodes of the client side.

----End

3.5.11 Preparing for Storage Resources (DESS)

Scenarios

To ensure service reliability of the SAP system, you need to prepare a DESS storage pool, create disks in the DESS storage pool, and attach disks to BMSs to store data of all SAP nodes. For details about the required disk specifications, see **Table 3-15**.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-15 DESS disks required by SAP nodes

Flavor	Disk	Disk Specifications
physical.kl1.2xlarge.hba	SBD volume	10 GB, ultra-high I/O (low latency), SCSI, shared disk
physical.m2.medium.hba	Log volume	512 GB, ultra-high I/O (low latency), SCSI, shared disk
	Data volume	6 TB, ultra-high I/O (low latency), SCSI, shared disk

Procedure

Buy DESS.

Step 1 Log in to the management console, click **Service List** and choose **Storage** > **Dedicated Enterprise Storage Service**.

Step 2 Click **Enable DeC**.

Step 3 Enable DeC offline as prompted. If necessary, dial 4000-955-988 or 950808 to contact HUAWEI CLOUD customer service.

Create a disk.

Step 4 Log in to the management console, click **Service List** and choose **Storage** > **Dedicated Enterprise Storage Service**.

Step 5 Create a disk in either of the following methods:

- Click **Create Disk** close to the DESS name to go to the disk creation page.
- Click the target DESS name. On the details page that is displayed, click **Create Disk** in the upper left corner to go to the page for creating a disk.

Step 6 View the displayed information and set required parameters for the disk to be created. For details, see **Table 3-16**.

Table 3-16 Parameter description

Parameter	Description
AZ	Specifies the AZ of the DESS where the disk resides.
Type	Specifies the type of the DESS where the disk resides.
Name	Specifies the disk name. When multiple disks are created, the system automatically adds suffixes. For example, **disk-0001** and **disk-0002**. A disk name cannot start or end with a space and can contain a maximum of 255 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Capacity (GB)	The disk capacity cannot exceed the DECC capacity. The available storage capacity cannot exceed the purchased storage capacity. **NOTE** The disk capacity ranges from 10 GB to 64 TB.
Quantity	Specifies the number of disks to be created. You can create a maximum of 512 disks.

Step 7 Click **OK**.

Attach a disk to a BMS.

Step 8 Log in to the management console, click **Service List** and choose **Storage** > **Dedicated Enterprise Storage Service**.

Step 9 Click the name of the target DESS to go to the details page.

Step 10 Attach a disk in either of the following methods:

- Click **Attach** in the row where the target disk locates to go to the page for attaching the disk.
- Click the name of the target disk to go to the details page. Click **Attach** in the upper left corner to go to the page for attaching the disk.

Step 11 Select the BMS that the disk is to be attached to.

The page automatically queries the BMS that the disks can be attached to. The displayed information includes **Name/ID**, **Status**, **Flavor**, **Image**, **Private IP Address**, and **AZ**.

Step 12 Click **OK**. A message is displayed indicating that the command for attaching the disk is successfully delivered.

----End

3.5.12 Scanning for DESS Disks

Scenarios

The attached DESS disks can be configured only after being scanned.

Procedure

Step 1 Log in to the jump host. Ensure that user **root** and the key file are used for authentication. Then, use SSH to switch to SAP HANA nodes.

Step 2 Run the following command to scan attached DESS disks:

hot_add

Step 3 Run the following command to check the attached DESS disk information:

fdisk -l

 Copyright © Huawei Technologies Co., Ltd.

Step 4 Scan the disks attached to other BMSs.

----End

3.5.13 Modifying OS Configurations

Scenarios

To ensure the proper installation of the SAP system, disable the OS firewalls of all nodes before the installation.

Procedure

Step 1 Log in to the jump host. Ensure that user **root** and the key file are used for authentication. Then, use SSH to switch to SAP HANA nodes.

Step 2 Run the following commands on the SAP HANA node to disable automatic firewall enabling and disable the firewall:

SuSEfirewall2 off

SuSEfirewall2 stop

systemctl disable SuSEfirewall2_init.service

systemctl disable SuSEfirewall2.service

systemctl stop SuSEfirewall2_init.service

systemctl stop SuSEfirewall2.service

Step 3 Repeat the preceding steps to disable the firewalls of all nodes in the SAP system.

----End

3.5.14 Configuring NFS Servers to Be Trusty to Each Other

Scenarios

NOTICE

If you use SFS Turbo to provide shared file storage, skip this section.

Two NFS servers use HAE for active/standby deployment. HAE requires that the two NFS servers be trusty to each other.

The two NFS servers have been configured to be trusty in section **Configuring SSH Switching Permissions**. In this section, you only need to configure the mapping between the hostnames of the ECSs where the NFS servers are deployed and the cloud management or backup plane IP addresses.

Procedure

Step 1 Log in to the jump host. Ensure that user **root** and the key file are used for authentication. Then, use SSH to switch to another NFS server.

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Modify the **/etc/hosts** file on the NFS server. Specifically, write the mapping between the server or backup plane IP addresses (for example, **10.0.5.x**) of the two NFS servers and the names of the HANA ECSs where the two NFS servers are deployed into this file.

Step 3 Upload the local hosts file to the other NFS server.

The command is in the following format:

scp /etc/hosts Peer IP address:/etc/hosts

The following is a command example:

scp /etc/hosts 10.0.5.102:/etc/hosts

Step 4 Verify the trusty relationship.

For example, if the local NFS server is **nfs01**, and the name of the other NFS server is **nfs02**, run the following commands:

ssh nfs02

ssh nfs01

NOTE

When an SSH connection is set up between two ECSs (where the two NFS servers are deployed) for the first time, the system displays the message "Are you sure you want to continue connecting (yes/no)?" on the CLI. In such a case, you only need to select **yes** and press **Enter**.

----End

3.6 Installing SAP HANA (Single-Node Deployment)

3.6.1 Formatting the Disks Attached to an NFS Server

Scenarios

NOTICE

If you use SFS Turbo to provide shared file storage, skip this section.

The disks attached to an NFS server must be formatted to comply with the SAP system installation requirements.

This section uses the formatting of backup and SBD volumes as an example. The shared volume on the active NFS server planned for the SAP NetWeaver system needs to be bound to the standby NFS server and then be formatted. For details about how to format disks, see section **Formatting the Disks Attached to an NFS Server**.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Bind the shared disk to the standby NFS server.

This operation is performed only when two NFS servers are deployed to work in active/standby mode. The reason is as follows: When one NFS server is created, the shared volume is attached to it. The volume must be attached to the other NFS server.

1. Log in to the management console, click **Service List** and choose **Computing** > **Elastic Cloud Server**.
2. According to the ECS name, locate the ECS where the NFS server with disks attached is deployed and click the ECS name.
3. On the page displayed for the ECS details, click the **Disks** tab and then the first data disk.
4. In the expanded data disk pane, take note of the **Device Name** and click the link following the data disk **ID**.
5. On the displayed page, click **Attach**. The **Attach Disk** page is displayed.
6. On the page, select the ECS used by the NFS server to be bound, and ensure that **Mount Point** bound to the ECS is the same as **Device Name** in **Step 1.4**.
7. Repeat **Step 1.2** to **Step 1.6** to attach all disks to the NFS server.

Step 2 Format the disks attached to the active NFS server.

1. Log in to the active NFS server.
2. Run the following command to check the disks that are not formatted:

   Determine the backup volume based on the disk size.

   fdisk -l
3. Create partitions for the SBD volume.

   Assume that **/dev/sdd** is the drive letter of the SBD volume.

   fdisk */dev/sdd*

   The following information is displayed:

   Command (m for help):

   a. Enter **n** and press **Enter** to create partitions.

   b. Press **Enter** until the following information is displayed:

   ```
   ....
   Using default value 209715199

   Command (m for help):
   ```

   c. Enter **w** and press **Enter**.
4. Create partitions for the backup volume.

   The following commands assume that **/dev/sdb** is the drive letter of the backup volume.

   parted */dev/sdb* **mklabel gpt y**

   parted */dev/sdb* **mkpart primarty 0% 100%**
5. Set the file system of the created partition. Run the following command to set the file system format of the created partition to **ext3**:

   mkfs -t ext3 */dev/sdb1*

 Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> Run the **partprobe** command on the standby NFS server to update its partition table.

Step 3 Run the following command to create the **/backup** directory:

mkdir /backup

> **NOTE**
>
> You also need to create the **/backup** directory on the standby NFS server.

Step 4 Configure both the active and standby NFS servers and restart them.

1. Open the **/etc/sysconfig/nfs** file and enter the editing mode to configure the ports of the NFS servers.

   vi /etc/sysconfig/nfs

2. Configure the ports as follows.

   ....

   MOUNTD_PORT="4002"

   ....

   STATD_PORT="4000"

   ....

   LOCKD_TCPPORT="4001"

   ....

   LOCKD_UDPPORT="4001"

3. Open the **/etc/exports** file.

   The purpose of editing the file is to share the disks on NFS servers to all SAP HANA nodes.

   vi /etc/exports

4. Add shared records of all SAP HANA nodes.

   The format is ***Shared directoryHosts that can access the shared directory (option)***.

   Assume that the IP address of the server or backup plane of SAP HANA nodes is **10.0.3.2**.

   /backup 10.0.3.2(rw,sync,no_root_squash,no_subtree_check)

5. Run the following command to restart the NFS server:

   systemctl restart nfsserver

6. Run the following command to make the configuration in the **/etc/exports** file take effect:

   exportfs -a

7. Run the following command to check whether the shared directory is successfully set. If the directory information is displayed in the command output, the setting is successful.

   showmount -e

8. Run the following command to disable the automatic startup of the NFS server. Perform this operation on both the active and standby NFS servers.

 Copyright © Huawei Technologies Co., Ltd.

systemctl disable nfsserver

----End

3.6.2 Configuring HA on NFS Servers

Scenarios

NOTICE

If you use SFS Turbo to provide shared file storage, skip this section.

When NFS servers are deployed to work in active/standby mode, you must enable data synchronization on the NFS servers so that they can properly support the SAP system.

Prerequisites

You have configured NFS servers to be trusty to each other and formatted the disks attached to NFS servers. For details, see sections **Configuring NFS Servers to Be Trusty to Each Other** and **Formatting the Disks Attached to an NFS Server**.

Procedure

Step 1 Initialize the cluster.

1. Log in to the jump host. Ensure that user **root** and key file are used for authentication. Then, use SSH to switch to the active NFS server. The name of the NFS server is assumed to **nfs01**.
2. Run the following command on the active NFS server to enter the cluster configuration page:

   ha-cluster-init
3. When the system displays the following information, enter **y** and press **Enter**:

   ```
   WARNING: NTP is not configured to start at system boot.
   WARNING: No watchdog device found. If SBD is used, the cluster will be unable to start without a watchdog.
   Do you want to continue anyway? [y/N]
   ```
4. When the system displays the following information, enter **n** and press **Enter**:

   ```
   /root/.ssh/id_rsa already exists - overwrite? [y/N]
   ```
5. Enter the heartbeat network segment of the NFS server and press **Enter**.

   Take network segment **10.0.4.0** as an example:

   ```
   Network address to bind to (e.g.: 192.168.1.0) []
   ```
6. When the system displays the following information, retain the default settings and press **Enter**:

   ```
   Multicast address (e.g.: 239.x.x.x) [239.97.171.218]
   ```
7. When the system displays the following information, retain the default settings and press **Enter**:

   ```
   Multicast port [5405]
   ```
8. When the system displays the following information, enter **n** and press **Enter**:

   ```
   Do you wish to use SBD? [y/N]
   ```

 Copyright © Huawei Technologies Co., Ltd.

9. When the system displays the following information, enter **n** and press **Enter**:

   NOTE

   To ensure system security, change the **hacluster** password after configuring HA.

   ```
   ...
     Log in with username 'hacluster', password 'linux'
   WARNING: You should change the hacluster password to something more secure!
    Enabling pacemaker.service
    Waiting for cluster.....done
    Loading initial configuration
   ...
   Do you wish to configure an administration IP? [y/N]
   ```

10. During the cluster initialization, the system displays the following information:

    ```
    Done (log saved to /var/log/ha-cluster-bootstrap.log)
    ```

Step 2 Add the standby NFS server to the cluster.

1. On the active NFS server **nfs01**, synchronize the **corosync.conf** configuration file to the standby NFS server.

   The command is in the following format:

   scp /etc/corosync/corosync.conf *Name of the standby NFS server*:**/etc/corosync/**

   The following command is used as an example:

   scp /etc/corosync/corosync.conf nfs02:/etc/corosync/

2. Log in to the standby NFS server from the active one using SSH.

   ssh nfs02

3. Run the following command to add the standby NFS server to the cluster:

   ha-cluster-join

4. When the system displays the following information, enter **y** and press **Enter**:

   ```
   WARNING: NTP is not configured to start at system boot.
   WARNING: No watchdog device found. If SBD is used, the cluster will be unable to start without a watchdog.
   Do you want to continue anyway? [y/N]
   ```

5. When the system displays the following information, enter the heartbeat plane IP address of the active NFS server, for example, **10.0.4.101**, and press **Enter**:

   ```
   IP address or hostname of existing node (e.g.: 192.168.1.1) []
   ```

6. When the system displays the following information, enter **n** and press **Enter**:

   ```
   /root/.ssh/id_rsa already exists - overwrite? [y/N]
   ```

7. During the cluster initialization after the standby NFS server is added to the cluster, the system displays the following information:

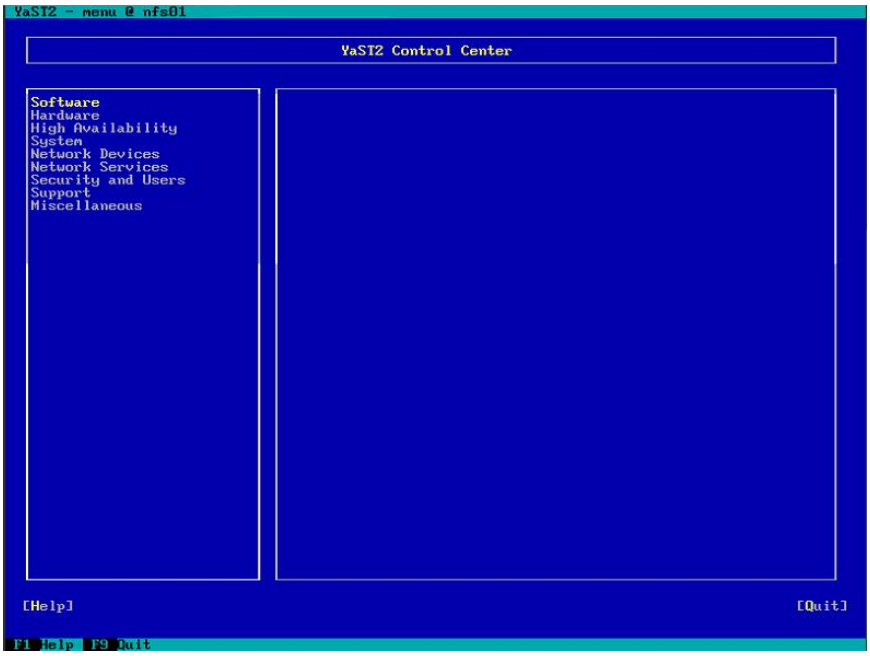
   ```
   ......
   WARNING: You should change the hacluster password to something more secure!
   Enabling pacemaker.service
   Waiting for cluster.....done
   Done (log saved to /var/log/ha-cluster-bootstrap.log)
   ```

Step 3 Configure basic cluster parameters.

1. Use VNC and user **root** password to log in to the active NFS server as user **root** and switch to the CLI mode.
2. Run the **yast2** command to enter the **YaST2 Control Center** page.

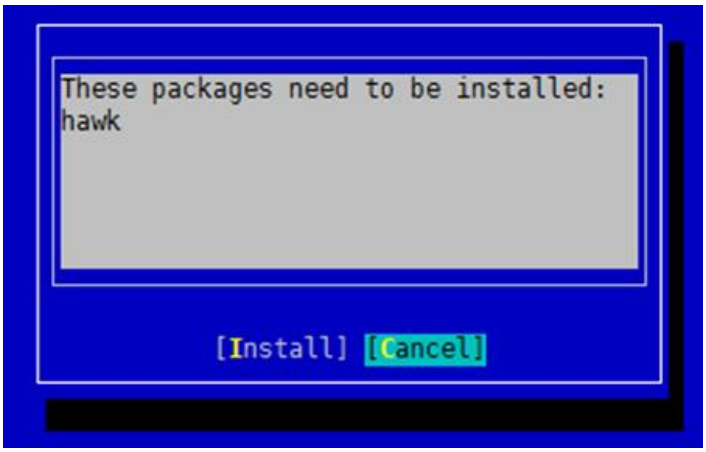
 Copyright © Huawei Technologies Co., Ltd.

Figure 3-6 YaST2 Control Center page



3. Choose **High Availability** > **Cluster**. The system displays a message, asking you to install the **hawk** software package, as shown in **Figure 3-7**. Select **Cancel** and press **Enter**.

Figure 3-7 Installing the **hawk** software package



4. The system displays the message "If you continue without installing required packages, YaST may not work properly." Select **Continue** and press **Enter**. The configuration information page of the cluster is displayed.
5. On the left side of the page, choose **Communication Channels**. Then, configure parameters on the right side of the page. **Figure 3-8** shows an example.

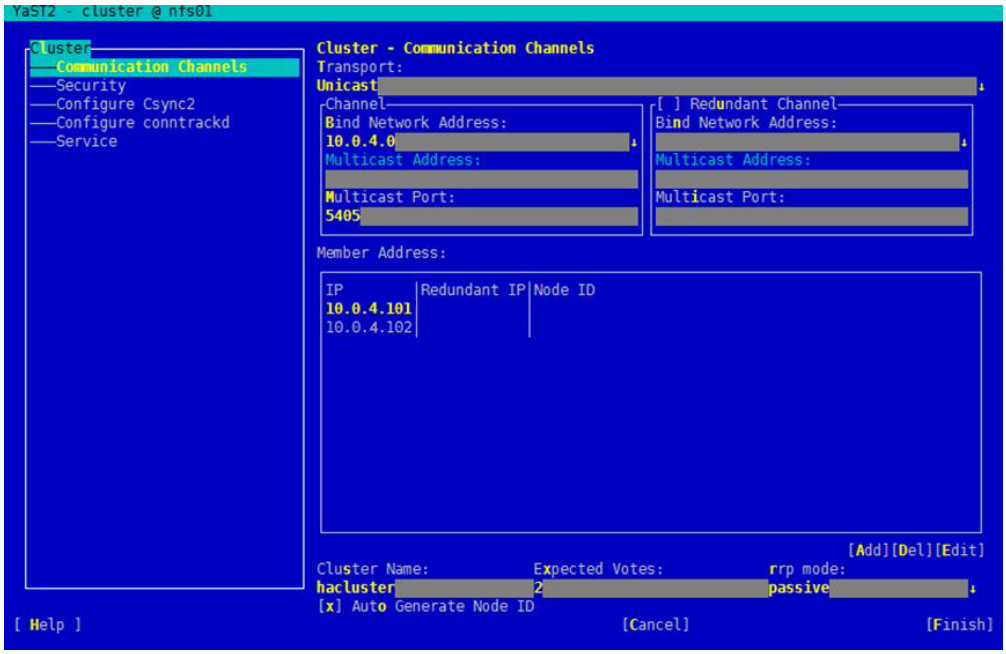
   Set the parameters as follows:

   - **Transport**: Set this parameter to **Unicast**.
   - In the **Channel** pane, select the network segment for the NFS server heartbeat link, which is the network segment of the heartbeat plane, for example, 10.0.4.0, for **Bind Network Address**; retain the default setting of **Multicast Port**.

 Copyright © Huawei Technologies Co., Ltd.

- **Auto Generate Node ID**: Select this parameter.
- **Redundant Channel**: You do not need to configure this parameter.
- **Member Address**: Select **Add** to add the heartbeat plane IP addresses of the active and standby NFS servers to **Member Address**.

Figure 3-8 Communication Channels page



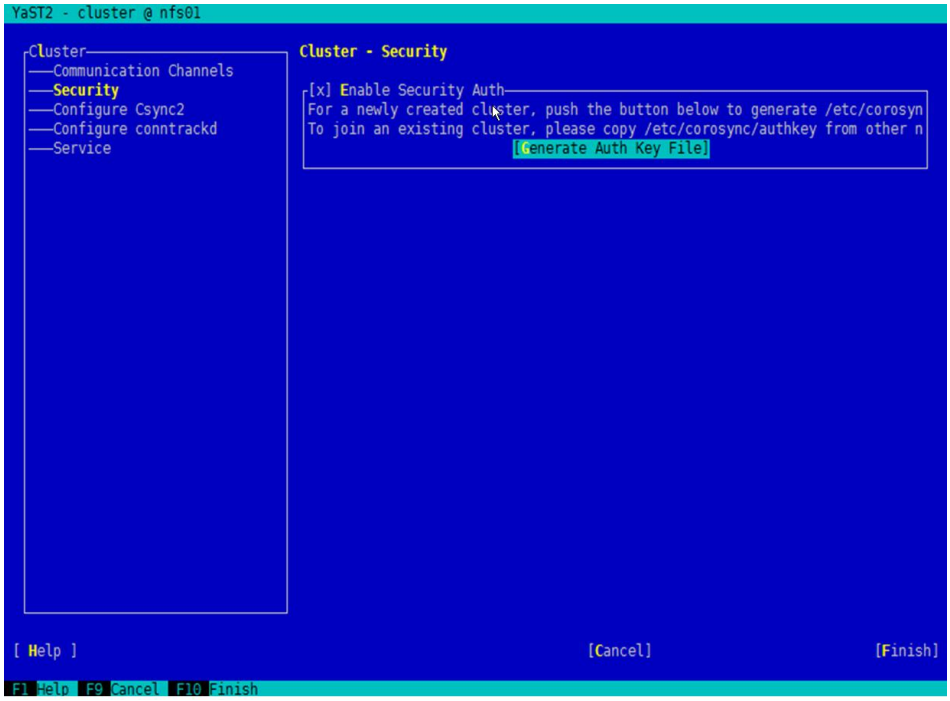
6. On the left side of the page, choose **Security**. Then, configure parameters on the right side of the page.

   Enable Security Auth: Select this parameter.

   Select **Generate Auth Key File** and press **Enter**. In the dialog box showing the file generation message, select **OK** and press **Enter** to generate the authentication key file.

 Copyright © Huawei Technologies Co., Ltd.

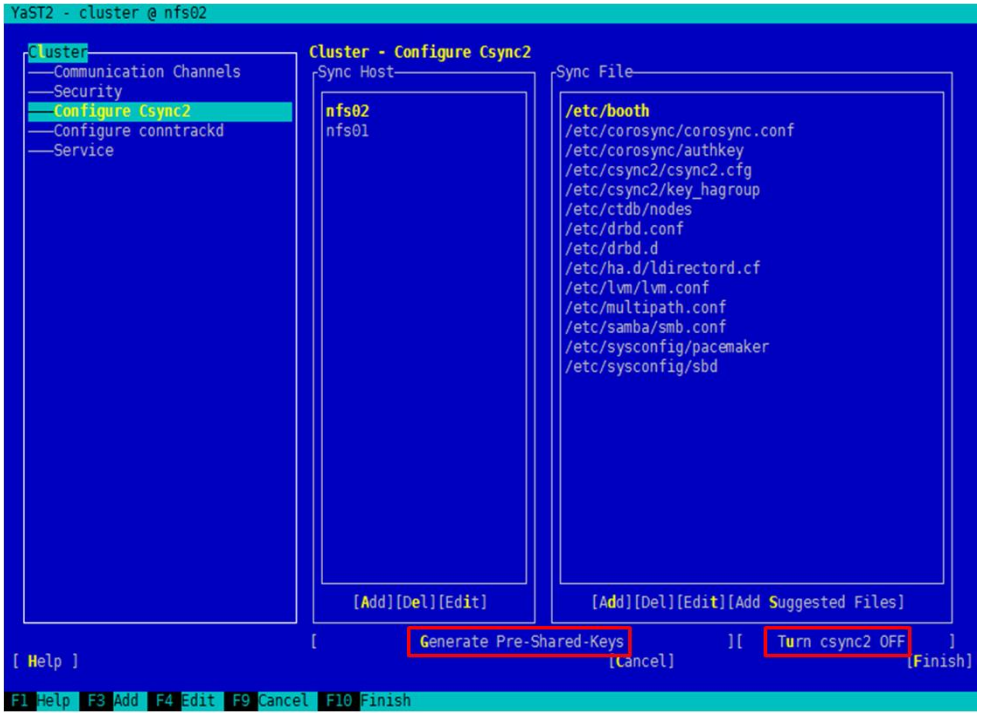
Figure 3-9 Security page



7. On the left side of the page, choose **Configure Csync2**. Then, configure parameters on the right side of the page.

   Select a **Sync Host** node and **Generate Pre-Shared-Keys** and press **Enter** to generate the file. In addition, ensure that **Turn csync2 OFF** in the lower right corner of the page is displayed, indicating that Csync2 has been enabled.

Figure 3-10 Configure Csync2 page



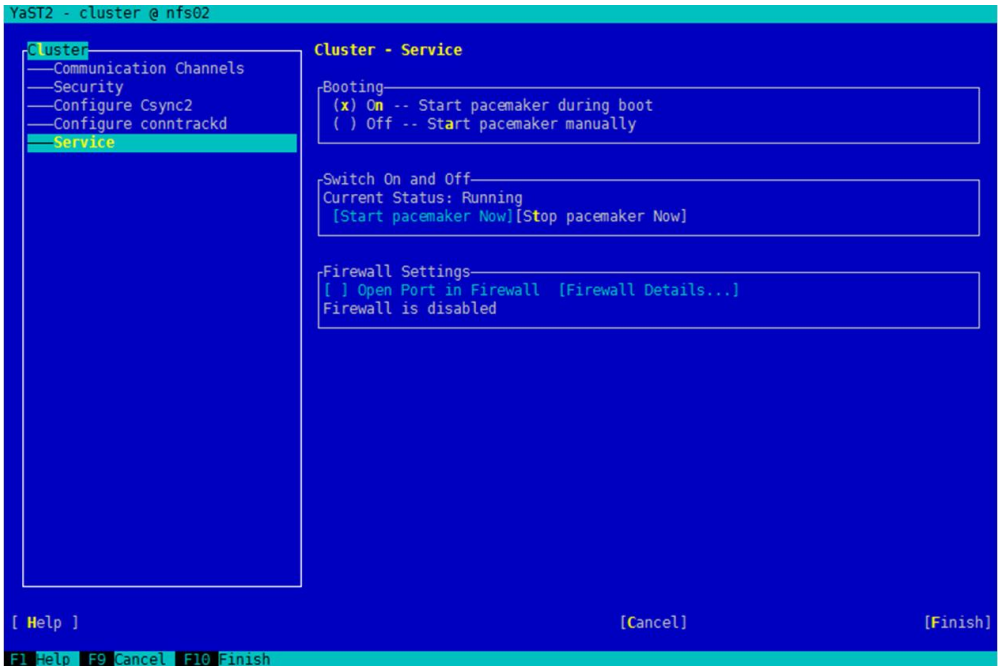
 Copyright © Huawei Technologies Co., Ltd.

8. On the left side of the page, choose **Service**. Then, configure parameters on the right side of the page.

   Set the parameters as follows:

   - **Booting**: **On** is selected by default, which indicates that the cluster is automatically started when the server starts.
   - **Switch on and off**: Ensure that the cluster has been started.
   - **Firewall Settings**: Ensure that **Firewall is disabled** is selected.

   Figure 3-11 Service page



9. Select **Finish** and press **Enter** to complete the configuration.
10. Copy the **key_hagroup** and **csync2.cfg** files on the active NFS server to the standby NFS server.

    Log in to the active NFS server as user **root** and run the following command:

    scp /etc/csync2/key_hagroup /etc/csync2/csync2.cfg *Name of the standby NFS server*:**/etc/csync2**

    The following command is used as an example:

    scp /etc/csync2/key_hagroup /etc/csync2/csync2.cfg nfs02:/etc/csync2
11. Run the following commands on the active NFS server:

    systemctl enable csync2.socket

    systemctl enable xinetd

    systemctl restart xinetd
12. Log in to the standby NFS server as user **root** and

    run the following commands:

    systemctl enable csync2.socket

    systemctl enable xinetd

    systemctl restart xinetd

 Copyright © Huawei Technologies Co., Ltd.

13. Run the following command on the active NFS server to synchronize the configuration file:

    csync2 -xv

14. Run the following command on the active NFS server to check the cluster status:

    Ensure that the cluster status is **active (running)**.

    NOTE

    If the command output indicating that the STONITH disk has not been configured, this is normal. The STONITH disk will be configured in the subsequent steps.

    systemctl status pacemaker

15. Run the following commands on the active NFS server to restart the cluster:

    systemctl stop pacemaker

    systemctl start pacemaker

16. Run the following command on the standby NFS server to check the cluster status:

    Ensure that the cluster status is **active (running)**.

    NOTE

    If the command output indicating that the STONITH disk has not been configured, this is normal. The STONITH disk will be configured in the subsequent steps.

    systemctl status pacemaker

17. Run the following commands on the standby NFS server to restart the cluster:

    systemctl stop pacemaker

    systemctl start pacemaker

18. Run the following command on the active NFS server to check the cluster heartbeat status:

    corosync-cfgtool -s

    The system displays the heartbeats of the active and standby links. Ensure that the configurations are correct.

19. Run the following command to check the cluster status on the active NFS server:

    crm_mon -r1

    The terminal display is as follows, where two NFS servers are in **Online** state, indicating that the cluster is functional:

```
Last updated: Wed Oct 19 17:40:31 2016
Last change: Tue Oct 18 15:32:00 2016 by root via cibadmin on hana01
Stack: classic openais (with plugin)
Current DC: nfs01 - partition with quorum
Version: 1.1.12-f47ea56
2 Nodes configured, 2 expected votes
0 Resources configured


Online: [ nfs01 nfs02 ]
```

Step 4 Configure the softdog.

1. Run the following command on the active NFS server to open the file and enter **i** to enter editing mode:

 Copyright © Huawei Technologies Co., Ltd.

vi /etc/init.d/boot.local

2. Add the following information to the last line of the file:
```
modprobe softdog >/dev/null 2>&1
```
3. Press **Esc**, enter **:x!**, and press **Enter** to exit the configuration.
4. On the CLI, run the following command:

   modprobe softdog
5. Repeat steps **Step 4.1** to **Step 4.4** to configure the softdog on the standby NFS server.

Step 5 Configure SBD on the Fence devices.

1. Run the following command on the active and standby NFS servers to start the SBD service automatically once the active and standby NFS servers start:

   systemctl enable sbd
2. Run the following command on the active NFS server to create an SBD partition:

   The command is in the following format:

   sbd -d /dev/disk/by-id/*Partition ID* **create**

   NOTE

   To query an SDB disk ID, run the **ll /dev/disk/by-id |grep** *Partition name*|**grep scsi-3** command. For example, if the partition name is **/dev/sdb1**, run the **ll /dev/disk/by-id |grep sdb|grep scsi-3** command to query the ID corresponding to **sdb1**.

   The following command is used as an example:

   sbd -d /dev/disk/by-id/scsi-36888603000000db7fa179ea56210049-part1 create
3. Run the following command to allocate the partition to the active NFS server:

   The command is in the following format:

   sbd -d /dev/disk/by-id/*Partition ID* **allocate** *Active node host name*

   The following command is used as an example:

   sbd -d /dev/disk/by-id/scsi-36888603000000db7fa179ea56210049-part1 allocate nfs01
4. Run the following command to allocate the partition to the standby NFS server:

   The command is in the following format:

   sbd -d /dev/disk/by-id/*Partition ID* **allocate** *Standby node host name*

   The following command is used as an example:

   sbd -d /dev/disk/by-id/scsi-36888603000000db7fa179ea56210049-part1 allocate nfs02
5. Run the following command to query the allocated partition:

   The command is in the following format:

   sbd -d /dev/disk/by-id/*Partition ID* **list**

   The following command is used as an example:

   sbd -d /dev/disk/by-id/scsi-36888603000000db7fa179ea56210049-part1 list

   The command output is as follows:

 Copyright © Huawei Technologies Co., Ltd.

```
0  nfs01 clear
1  nfs02 clear
```

6. Run the following command to dump the partition:

   sbd -d /dev/disk/by-id/*Partition ID* **dump**

   The following command is used as an example:

   sbd -d /dev/disk/by-id/scsi-36888603000000db7fa179ea56210049-part1 dump

7. Open the **sbd** file and add data to the file.

   Run the **vi /etc/sysconfig/sbd** command to open the file and add data to the file.

   An example is provided as follows:

   NOTE

   Enter the path of the partition for SBD in **SBD_DEVICE**. The partition in the following terminal display is for reference only.

```
SBD_DEVICE="/dev/disk/by-id/scsi-36888603000000db7fa179ea56210049-part1"
SBD_OPTS="-W"
```

8. On active NFS server, synchronize the configuration file to the standby NFS server.

   scp /etc/sysconfig/sbd *Standby node host name*:**/etc/sysconfig**

   The following command is used as an example:

   scp /etc/sysconfig/sbd nfs02:/etc/sysconfig

9. Run the following commands on the active NFS server to restart the cluster:

   systemctl stop pacemaker

   systemctl start pacemaker

10. Run the following commands on the standby NFS server to restart the cluster:

    systemctl stop pacemaker

    systemctl start pacemaker

11. Check cluster configurations.

    crm_mon -r1

    The terminal display is as follows, where two NFS servers are in **Online** state, indicating that the cluster is functional:

```
Last updated: Wed Oct 19 17:40:31 2016
Last change: Tue Oct 18 15:32:00 2016 by root via cibadmin on hana01
Stack: classic openais (with plugin)
Current DC: nfs01 - partition with quorum
Version: 1.1.12-f47ea56
2 Nodes configured, 2 expected votes
0 Resources configured


Online: [ nfs01 nfs02 ]
```

Step 6 Add Fence SBD resources.

1. Run the following command on the active NFS server to switch to the CRM configuration mode:

   crm

   Information similar to the following is displayed:

```
crm(live)#
```

 Copyright © Huawei Technologies Co., Ltd.

2. Run the following command to switch to the configuration mode:

   configure

3. Run the following commands to add SBD resources:

   primitive r_sbd stonith:external/sbd params pcmk_delay_max=40

   commit

Step 7 Assign a virtual service IP address.

1. On the management console, click **Service List** and choose **Computing** > **Elastic Cloud Server** to switch to the **Elastic Cloud Server** page.
2. Locate the ECS on which an NFS server is deployed and click the ECS name. Then, the page for the ECS details is displayed.
3. Click the **NIC** tab and then **Manage Private IP** in the row of the server or management plane NIC. Then, the system displays the **Virtual IP Address** page.
4. Click **Assign Virtual IP Address** to assign a floating IP address. Locate the row that contains the target IP address, click **Bind to Server** to bind the IP address to the target ECS, and repeat this operation to bind the IP address to other ECSs.
5. Run the following commands on the active NFS server in CRM configuration mode:

   In the preceding commands, **params ip** is the virtual service IP address of the NFS server. This value is for reference only.

   primitive nfs_vip ocf:heartbeat:IPaddr2 params ip=*10.0.1.103* op monitor interval="10" timeout="20" on-fail=restart

   commit

Step 8 Create cluster shared volume file systems.

Run the following commands on the active NFS server to create the cluster shared disk file system for the backup volume:

In the commands, **params device** and **directory** specify the ID and path of the backup volume, and the values provided are for reference only. For instructions about how to query a disk ID, see **Step 5.2**.

primitive nfs_bak ocf:heartbeat:Filesystem params device="*/dev/disk/by-id/Volume ID*" directory="/backup" fstype=ext3 op monitor interval="10" timeout="40" on-fail=restart

primitive nfs_sapmnt ocf:heartbeat:Filesystem params device="*/dev/disk/by-id/Volume ID*" directory="/sapmnt " fstype=ext3 op monitor interval="10" timeout="40" on-fail=restart

primitive nfs_sys ocf:heartbeat:Filesystem params device="*/dev/disk/by-id/Volume ID*" directory="/usr/sap/A01/SYS" fstype=ext3 op monitor interval="10" timeout="40" on-fail=restart

primitive nfs_sapcd ocf:heartbeat:Filesystem params device="*/dev/disk/by-id/Volume ID*" directory="/sapcd" fstype=ext3 op monitor interval="10" timeout="40" on-fail=restart

commit

 Copyright © Huawei Technologies Co., Ltd.

Step 9 Create the **nfsserver** resource.

In the CRM configuration mode on the active NFS server, create the **nfsserver** resource.

If the floating IP address (specified by **nfs_ip**) of the NFS server is 10.0.1.103, run the following commands:

primitive nfsserver nfsserver params nfs_ip=*10.0.5.103* nfs_shared_infodir="/backup" nfs_shared_infodir="/sapmnt" nfs_shared_infodir="/usr/sap/A01/SYS" nfs_shared_infodir="/sapcd" operations $id=nfsserver-operations op monitor interval="10" timeout="20" on-fail=restart

commit

Step 10 Create the resource group **nfs_group**.

Run the following commands on the active NFS server in the CRM configuration mode to create resource group **nfs_group** for the resource created from **Step 7.5** to **Step 9**:

group nfs_group nfs_vip nfs_bak nfs_sapmnt nfs_sys nfs_sapcd nfsserver

commit

Step 11 Create Clone Ping.

Run the following commands on the active NFS server in the CRM configuration mode to create Clone Ping:

primitive r_ping ocf:pacemaker:ping params multiplier="100" dampen="5" host_list="*10.0.5.1*" op monitor interval="15" timeout="60" start="60" op start interval="0" timeout="60"

clone PING r_ping

commit

Set the parameters as follows:

- **r_ping**: specifies the Clone Ping resource name.
- **Multiplier**: an efficiency enhancer that uses the benchmark of 100. When packet loss occurs during the ping operation between two nodes, the multiplier decreases a certain value from 100 to determine the service NIC communication status of the nodes.
- **dampen**: indicates that the ping operation is performed once every 5s.
- **10.0.5.1**: indicates the gateway IP address of the server or backup plane network segment for the NFS servers.
- **monitor**: indicates monitoring resources. **interval**: indicates that if pinging the upper-layer switch fails within 15s, the system will migrate resources at most 60s (timeout) later.

Step 12 Create restraint **nfs_conn**.

Run the following commands on the active NFS server in the CRM configuration mode to create restraint **nfs_conn** on resource group **nfs_group**:

location nfs_conn nfs_group rule -inf: not_defined pingd or pingd lte 0

 Copyright © Huawei Technologies Co., Ltd.

commit

Step 13 Configure other information.

1. Configure the **stonith** parameter:
   property startup-fencing=true
   property stonith-enabled=true
   property stonith-action=off
   commit
2. Configure the failure timeout duration:
   rsc_defaults failure-timeout=600
   commit
3. Press **Ctrl+C** on the active NFS server to exit the CRM configuration mode.

----End

3.6.3 Attaching the Backup Volume

Scenarios

Attach the backup volume on NFS servers to SAP HANA nodes. If you use SFS Turbo to provide shared file storage, skip this section. For details about how to mount the backup volumes, see section **Formatting a Disk** in the *SAP HANA User Guide*.

Procedure

Step 1 Log in to the active SAP HANA node and attach the backup volume to the active SAP HANA node.

1. Run the following command to create the **/hana/backup** directory:
   mkdir -p /hana/backup
2. Run the following command to assign permissions to **/backup**:
   chmod -R 777 /hana/backup
3. Add the following content to the end of the **/etc/auto.master** file:
   ```
   /- /etc/hananfs.direct
   ```
4. Create and edit the **/etc/hananfs.direct** file.
   vi /etc/hananfs.direct
   Add a sharing record. In this example, the floating IP address of the NFS server is **10.0.5.103**.
   /hana/backup -rw,intr,rsize=32768,wsize=32768,timeo=14,vers=3 10.0.5.103:/backup
5. Check whether **autofs** has been attached to the backup directory.
   systemctl restart autofs
   Run the following commands to check whether the **/hana/backup** directory has been attached properly:
   ls /hana/backup
   df -h

 Copyright © Huawei Technologies Co., Ltd.

6. Enable automatic start of the **autofs** service during system startup.

   systemctl enable autofs

Step 2 Log in to the standby SAP HANA node, repeat the preceding steps, and attach the backup volume to the standby SAP HANA node.

----End

3.6.4 Formatting a BMS (physical.m2.medium) Disk

Scenarios

The data volumes of SAP HANA nodes can be used only after they are formatted and then attached to required directories.

This section describes how to format a BMS (physical.m2.medium) disk.

Procedure

Step 1 Log in to the jump host. Ensure that user **root** and the key file are used for authentication. Then, use SSH to switch to SAP HANA nodes.

Step 2 Use local disks (2 x 1.6 TB ES3600 SSD) to form RAID 1 and allocate the RAID 1 to the log volume.

1. View the disk information.

   fdisk -l

2. In the displayed information, locate the drive letters of the SSD disks, such as **/dev/nvme0n1** and **/dev/nvme1n1**.
3. Form RAID 1 and specify the drive letter.

   For example, if the drive letter is **/dev/md0**, run the following command:

   mdadm --create */dev/md0* **--level=1 --raid-devices=2** */dev/nvme0n1 /dev/nvme1n1*

   Enter **y** when the system displays **Continue creating array?**.
4. Save the RAID configuration.

   mdadm -Ds >> /etc/mdadm.conf

   NOTE

   If any SSD card is faulty, you can perform the following operations to restore data after the card is replaced with a normal one.

   1. Install the hioadm tool. Run the **hioadm info -d** */dev/nvme1n1* command to locate the faulty SSD card, and replace the faulty SSD card with a normal one. Assume that the drive letter of the faulty disk is **/dev/nvme1n1**.
   2. Run the **mdadm --manage** */dev/md0* **--remove** */dev/nvme1n1* command to remove the drive letter of the faulty disk.
   3. Run the **mdadm --manage** */dev/md0* **--add** */dev/nvme2n1* command to add a new drive letter to restore data.
5. Create the **/hana/log/** directory.

   mkdir -p /hana/log/
6. Create a file system.

   mkfs -t xfs -f */dev/md0*

 Copyright © Huawei Technologies Co., Ltd.

7. Attach a disk.

   mount */dev/md0* **/hana/log/**

Step 3 Use LVM to logically divide local disks (7 x 1.8 TB 10K 2.5 SAS HDD) into a data volume and a shared volume.

View the disk information and find the drive letter, for example, **/dev/sdb**.

Run the following commands to partition the disk:

parted */dev/sdb* **mklabel gpt y**

parted */dev/sdb* **mkpart primarty 0% 100%**

Step 4 Run the following command to create a physical volume:

pvcreate */dev/sdb1*

Step 5 Run the following command to create a volume group:

vgcreate vghana */dev/sdb1*

Step 6 Run the following command to query the available capacity of the volume group:

vgdisplay vghana

Step 7 Run the following commands to create logical volumes:

lvcreate -n lvhanashared -L *2T* **vghana**

lvcreate -n lvhanadata -L *6T* **vghana**

Step 8 Run the following commands to format the logical volumes and attach them to the corresponding directories:

mkfs -t xfs /dev/mapper/vghana-lvhanadata

mkfs -t xfs /dev/mapper/vghana-lvhanashared

mkdir -p /hana/data

mkdir -p /hana/shared

mount /dev/mapper/vghana-lvhanadata /hana/data

mount /dev/mapper/vghana-lvhanashared /hana/shared

Step 9 Run the following commands to write disk attaching relationships into the **/etc/fstab** file:

/dev/mapper/vghana-lvhanadata /hana/data xfs defaults 0 0

/dev/mapper/vghana-lvhanashared /hana/shared xfs defaults 0 0

/dev/md0 **/hana/log xfs defaults 0 0**

Step 10 Format the data volume of the other BMS.

----End

 Copyright © Huawei Technologies Co., Ltd.

3.6.5 Formatting a BMS (physical.kl1.2xlarge.hba) Disk

Scenarios

The data volumes of SAP HANA nodes can be used only after they are formatted and then attached to required directories.

This section describes how to format a BMS (physical.kl1.2xlarge.hba) disk.

Procedure

Step 1 Log in to the jump host. Ensure that user **root** and the key file are used for authentication. Then, use SSH to switch to SAP HANA nodes.

Step 2 Use LVM to logically divide local data disks (13 x 3.2 TB SAS) into a log volume, a data volume, and a shared volume.

View the disk information and find the drive letter, for example, **/dev/sdb**.

Run the following commands to partition the disk:

parted */dev/sdb* **mklabel gpt y**

parted */dev/sdb* **mkpart primarty 0% 100%**

Step 3 Run the following command to create a physical volume:

pvcreate */dev/sdb1*

Step 4 Run the following command to create a volume group:

vgcreate vghana */dev/sdb1*

Step 5 Run the following command to query the available capacity of the volume group:

vgdisplay vghana

Step 6 Run the following commands to create logical volumes:

lvcreate -n lvhanalog -L *512G* **vghana**

lvcreate -n lvhanadata -L *12T* **vghana**

lvcreate -n lvhanashared -L *4T* **vghana**

Step 7 Run the following commands to format the logical volumes and attach them to the corresponding directories:

mkfs -t xfs /dev/mapper/vghana-lvhanalog

mkfs -t xfs /dev/mapper/vghana-lvhanadata

mkfs -t xfs /dev/mapper/vghana-lvhanashared

mkdir -p /hana/log

mkdir -p /hana/data

mkdir -p /hana/shared

mount /dev/mapper/vghana-lvhanalog /hana/log

 Copyright © Huawei Technologies Co., Ltd.

mount /dev/mapper/vghana-lvhanadata /hana/data

mount /dev/mapper/vghana-lvhanashared /hana/shared

Step 8 Run the following commands to write disk attaching relationships into the **/etc/fstab** file:

/dev/mapper/vghana-lvhanalog /hana/log xfs defaults 0 0

/dev/mapper/vghana-lvhanadata /hana/data xfs defaults 0 0

/dev/mapper/vghana-lvhanashared /hana/shared xfs defaults 0 0

Step 9 Format the data volume of the other BMS.

----End

3.6.6 Installing SAP HANA

For details about how to install SAP HANA in the single-node deployment mode, see section "Installing SAP HANA (Single-Node Deployment with HA Required)" in the **SAP HANA User Guide (Single BMS Node Deployment)**.

For details about how to configure the backup path, System Replication, the HA function of SAP HANA nodes, and storage parameters, see section "Installing SAP HANA (Single-Node Deployment with HA Required)" in the **SAP HANA User Guide (Single BMS Node Deployment)**.

NOTE

If SAP HANA has been installed on a BMS whose flavor is physical.kl1.2xlarge.hba, you need to modify the **sysctl.conf** configuration in the operating system before configuring the HA function for the SAP HANA nodes.

Procedure

Step 1 Log in to the jump host. Ensure that user **root** and the key file are used for authentication. Then, use SSH to switch to the active SAP HANA node.

Step 2 Open the **sysctl.conf** file and change the value of **aio-max-nr** to **200000**.

vi /etc/sysctl.conf

An example is provided as follows:

```
fs.aio-max-nr=200000
```

Step 3 Run the following command to make the configuration take effect:

sysctl –p

Step 4 Repeat the preceding steps to switch to the standby SAP HANA node and modify the **sysctl.conf** file.

----End

3.7 Installing SAP HANA (Cluster Deployment)

 Copyright © Huawei Technologies Co., Ltd.

3.7.1 Formatting the Disks Attached to an NFS Server

Scenarios

NOTICE

If you use SFS Turbo to provide shared file storage, skip this section.

The disks attached to an NFS server must be formatted to comply with the SAP system installation requirements.

This section uses the formatting of shared, backup, and SBD volumes as an example. The shared volume on the active NFS server planned for the SAP NetWeaver system needs to be bound to the standby NFS server and then be formatted. For details about how to format disks, see section **Formatting the Disks Attached to an NFS Server**.

Procedure

Step 1 Bind the shared disk to the standby NFS server.

This operation is performed only when two NFS servers are deployed to work in active/standby mode. The reason is as follows: When one NFS server is created, the shared volume is attached to it. The volume must be attached to the other NFS server.

1. Log in to the management console, click **Service List** and choose **Computing** > **Elastic Cloud Server**.
2. According to the ECS name, locate the ECS where the NFS server with disks attached is deployed and click the ECS name.
3. On the page displayed for the ECS details, click the **Disks** tab and then the first data disk.
4. In the expanded data disk pane, take note of the **Device Name** and click the link following the data disk **ID**.
5. On the displayed page, click **Attach**. The **Attach Disk** page is displayed.
6. On the page, select the ECS used by the NFS server to be bound, and ensure that **Mount Point** bound to the ECS is the same as **Device Name** in **Step 1.4**.
7. Repeat **Step 1.2** to **Step 1.6** to attach all disks to the NFS server.

Step 2 Format the disks attached to an NFS server.

1. Log in to the active NFS server.
2. Run the following command to check the disks that are not formatted:

   Determine the disk type (shared, backup, or SBD volume) according to the disk size.

   fdisk -l
3. Create partitions for the SBD volume.

   Assume that **/dev/sdd** is the drive letter of the SBD volume.

   fdisk */dev/sdd*

 Copyright © Huawei Technologies Co., Ltd.

The following information is displayed:

Command (m for help):

a. Enter **n** and press **Enter** to create partitions.

b. Press **Enter** until the following information is displayed:

....

Using default value 209715199

Command (m for help):

c. Enter **w** and press **Enter**.

4. Create partitions for the shared and backup volumes.

The following commands assume that **/dev/sdb** and **/dev/sdc** are the drive letters of shared and backup volumes, respectively.

parted */dev/sdb* **mklabel gpt y**

parted */dev/sdb* **mkpart primarty 0% 100%**

parted */dev/sdc* **mklabel gpt y**

parted */dev/sdc* **mkpart primarty 0% 100%**

5. Set the file system of the created partition. The file system format of the shared volume is **xfs**, and that of the backup volume is **ext3**.

mkfs -t xfs */dev/sdb1*

mkfs -t ext3 */dev/sdc1*

NOTE

Run the **partprobe** command on the standby NFS server to update its partition table.

Step 3 Create the **/shared** and **/backup** directories.

mkdir /backup

mkdir /shared

NOTE

You also need to create the **/shared** and **/backup** directories on the standby NFS server.

Step 4 Configure both the active and standby NFS servers and restart them.

1. Open the **/etc/sysconfig/nfs** file and enter the editing mode to configure the ports of the NFS servers.

vi /etc/sysconfig/nfs

2. Configure the ports as follows.

....

MOUNTD_PORT="4002"

....

STATD_PORT="4000"

....

LOCKD_TCPPORT="4001"

....

LOCKD_UDPPORT="4001"

 Copyright © Huawei Technologies Co., Ltd.

3. Open the **/etc/exports** file.

   The purpose of editing the file is to share the disks on NFS servers to all SAP HANA nodes.

   vi /etc/exports

4. Add shared records of all SAP HANA nodes.

   The format is ***Shared directoryHosts that can access the shared directory (option)***.

   Assume that the IP address of the server or backup plane of SAP HANA nodes is **10.0.3.2**.

   /shared 10.0.3.2(rw,sync,no_root_squash,no_subtree_check)

   /backup 10.0.3.2(rw,sync,no_root_squash,no_subtree_check)

5. Run the following command to restart the NFS server:

   systemctl restart nfsserver

6. Run the following command to make the configuration in the **/etc/exports** file take effect:

   exportfs -a

7. Run the following command to check whether the shared directory is successfully set. If the directory information is displayed in the command output, the setting is successful.

   showmount -e

8. Run the following command to disable the automatic startup of the NFS server. Perform this operation on both the active and standby NFS servers.

   systemctl disable nfsserver

----End

3.7.2 Configuring HA on NFS Servers

Scenarios

NOTICE

If you use SFS Turbo to provide shared file storage, skip this section.

When NFS servers are deployed to work in active/standby mode, you must enable data synchronization on the NFS servers so that they can properly support SAP HANA.

Prerequisites

You have configured NFS servers to be trusty to each other and formatted the disks attached to NFS servers. For details, see sections **Configuring NFS Servers to Be Trusty to Each Other** and **Formatting the Disks Attached to an NFS Server**.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Initialize the cluster.

1. Log in to the jump host. Ensure that user **root** and key file are used for authentication. Then, use SSH to switch to the active NFS server. The name of the NFS server is assumed to **nfs01**.
2. Run the following command on the active NFS server to enter the cluster configuration page:

   ha-cluster-init
3. When the system displays the following information, enter **y** and press **Enter**:
   ```
   WARNING: NTP is not configured to start at system boot.
   WARNING: No watchdog device found. If SBD is used, the cluster will be unable to start without a watchdog.
   Do you want to continue anyway? [y/N]
   ```
4. When the system displays the following information, enter **n** and press **Enter**:
   ```
   /root/.ssh/id_rsa already exists - overwrite? [y/N]
   ```
5. Enter the heartbeat network segment of the NFS server and press **Enter**.

   Take network segment **10.0.4.0** as an example:
   ```
   Network address to bind to (e.g.: 192.168.1.0) []
   ```
6. When the system displays the following information, retain the default settings and press **Enter**:
   ```
   Multicast address (e.g.: 239.x.x.x) [239.97.171.218]
   ```
7. When the system displays the following information, retain the default settings and press **Enter**:
   ```
   Multicast port [5405]
   ```
8. When the system displays the following information, enter **n** and press **Enter**:
   ```
   Do you wish to use SBD? [y/N]
   ```
9. When the system displays the following information, enter **n** and press **Enter**:

   NOTE

   To ensure system security, change the **hacluster** password after configuring HA.

   ```
   ...
     Log in with username 'hacluster', password 'linux'
   WARNING: You should change the hacluster password to something more secure!
    Enabling pacemaker.service
    Waiting for cluster.....done
    Loading initial configuration
   ...
   Do you wish to configure an administration IP? [y/N]
   ```
10. During the cluster initialization, the system displays the following information:
    ```
    Done (log saved to /var/log/ha-cluster-bootstrap.log)
    ```

Step 2 Add the standby NFS server to the cluster.

1. On the active NFS server **nfs01**, synchronize the **corosync.conf** configuration file to the standby NFS server.

   The command is in the following format:

   scp /etc/corosync/corosync.conf *Name of the standby NFS server*:**/etc/corosync/**

   The following command is used as an example:

   scp /etc/corosync/corosync.conf nfs02:/etc/corosync/

 Copyright © Huawei Technologies Co., Ltd.

2. Log in to the standby NFS server from the active one using SSH.

   ssh nfs02

3. Run the following command to add the standby NFS server to the cluster:

   ha-cluster-join

4. When the system displays the following information, enter **y** and press **Enter**:

   ```
   WARNING: NTP is not configured to start at system boot.
   WARNING: No watchdog device found. If SBD is used, the cluster will be unable to start without a watchdog.
   Do you want to continue anyway? [y/N]
   ```

5. When the system displays the following information, enter the heartbeat plane IP address of the active NFS server, for example, **10.0.4.101**, and press **Enter**:

   ```
   IP address or hostname of existing node (e.g.: 192.168.1.1) []
   ```

6. When the system displays the following information, enter **n** and press **Enter**:

   ```
   /root/.ssh/id_rsa already exists - overwrite? [y/N]
   ```

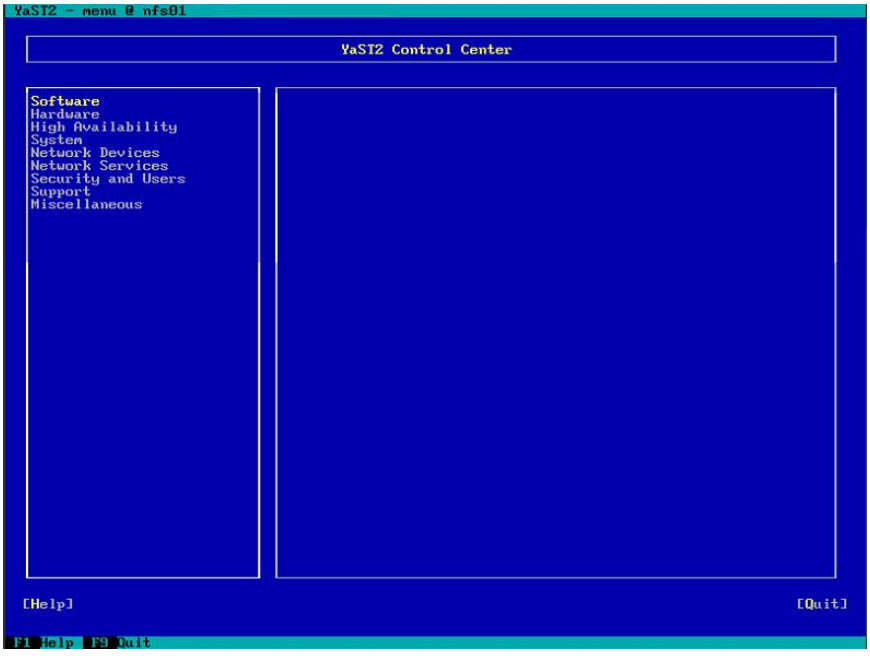
7. During the cluster initialization after the standby NFS server is added to the cluster, the system displays the following information:

   ```
   ......
   WARNING: You should change the hacluster password to something more secure!
   Enabling pacemaker.service
   Waiting for cluster.....done
   Done (log saved to /var/log/ha-cluster-bootstrap.log)
   ```

Step 3 Configure basic cluster parameters.

1. Use VNC and user **root** password to log in to the active NFS server as user **root** and switch to the CLI mode.
2. Run the **yast2** command to enter the **YaST2 Control Center** page.

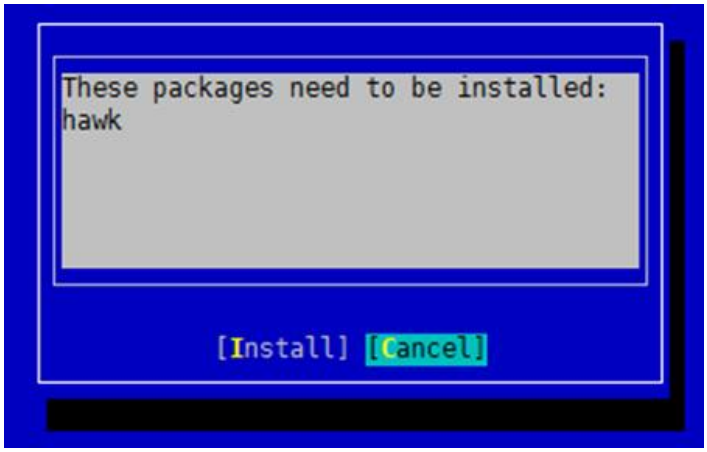
   Figure 3-12 YaST2 Control Center page



3. Choose **High Availability** > **Cluster**. The system displays a message, asking you to install the **hawk** software package, as shown in **Figure 3-13**. Select **Cancel** and press **Enter**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-13 Installing the **hawk** software package



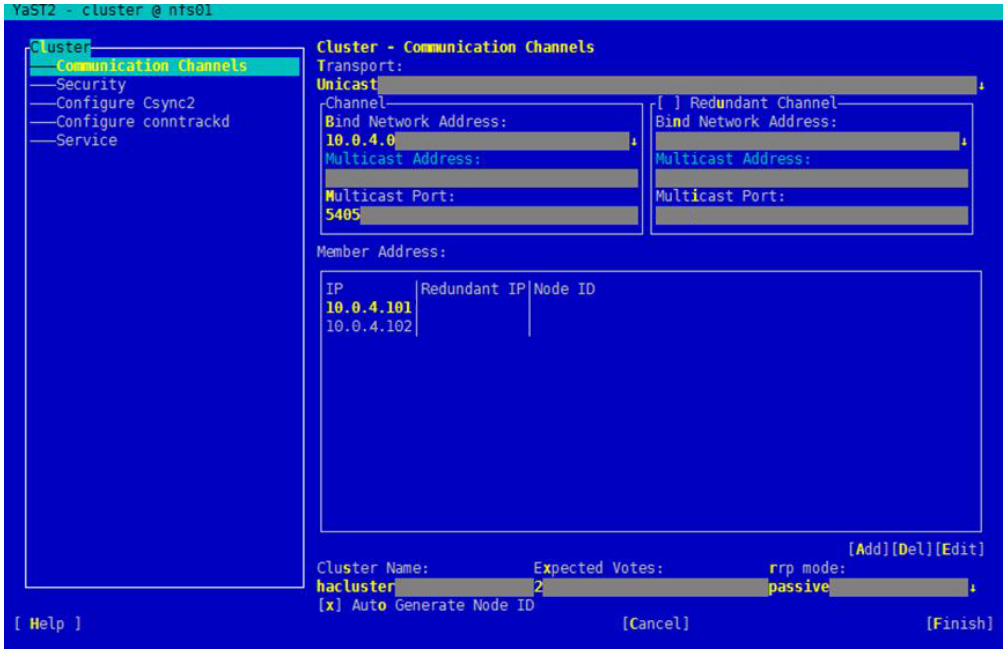
4. The system displays the message "If you continue without installing required packages, YaST may not work properly." Select **Continue** and press **Enter**. The configuration information page of the cluster is displayed.
5. On the left side of the page, choose **Communication Channels**. Then, configure parameters on the right side of the page. **Figure 3-14** shows an example.

   Set the parameters as follows:

   - **Transport**: Set this parameter to **Unicast**.
   - In the **Channel** pane, select the network segment for the NFS server heartbeat link, which is the network segment of the heartbeat plane, for example, 10.0.4.0, for **Bind Network Address**; retain the default setting of **Multicast Port**.
   - **Auto Generate Node ID**: Select this parameter.
   - **Redundant Channel**: You do not need to configure this parameter.
   - **Member Address**: Use **Add** to add the heartbeat plane IP addresses as well as the server or backup plane IP addresses of the active and standby NFS servers to **Member Address**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-14 Communication Channels page

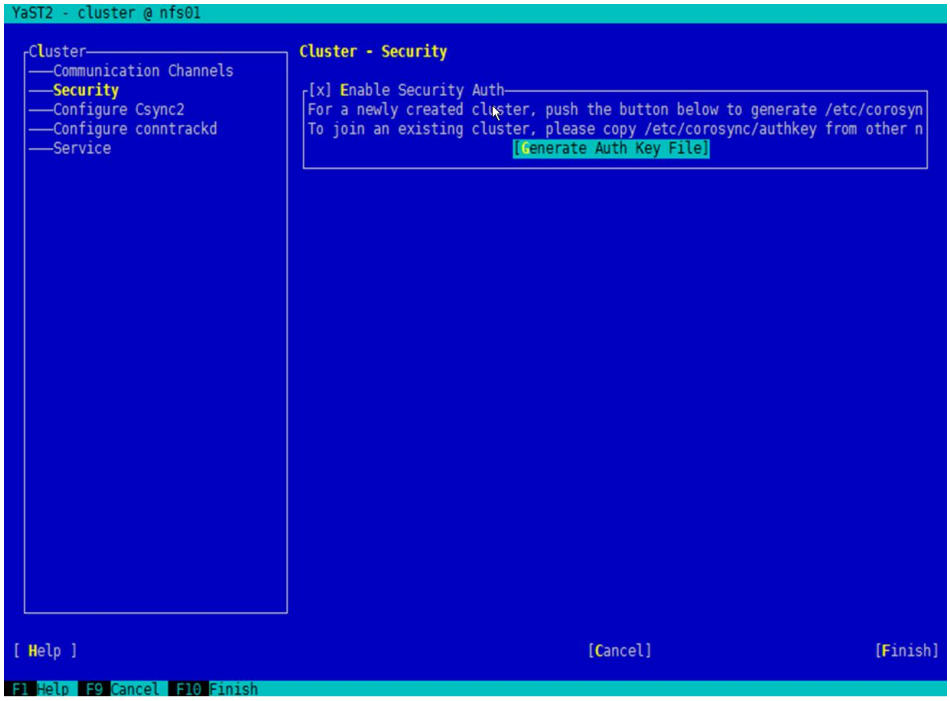


6. On the left side of the page, choose **Security**. Then, configure parameters on the right side of the page.

   Enable Security Auth: Select this parameter.

   Select **Generate Auth Key File** and press **Enter**. In the dialog box showing the file generation message, select **OK** and press **Enter** to generate the authentication key file.

Figure 3-15 Security page

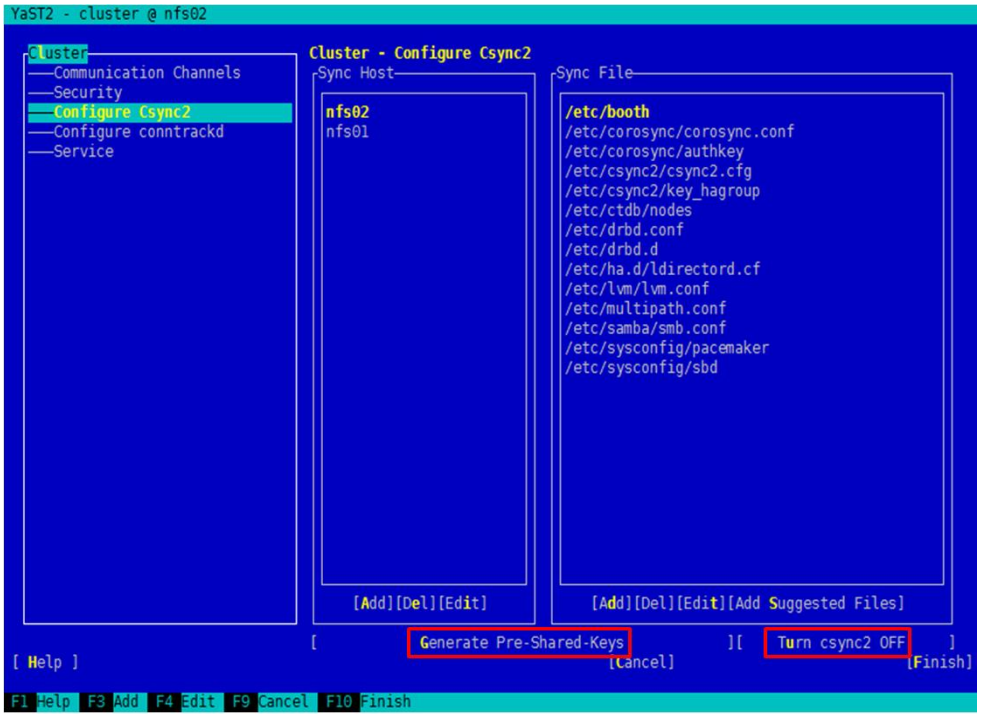


7. On the left side of the page, choose **Configure Csync2**. Then, configure parameters on the right side of the page.

 Copyright © Huawei Technologies Co., Ltd.

Select a **Sync Host** node and **Generate Pre-Shared-Keys** and press **Enter** to generate the file. In addition, ensure that **Turn csync2 OFF** in the lower right corner of the page is displayed, indicating that Csync2 has been enabled.

Figure 3-16 Configure Csync2 page



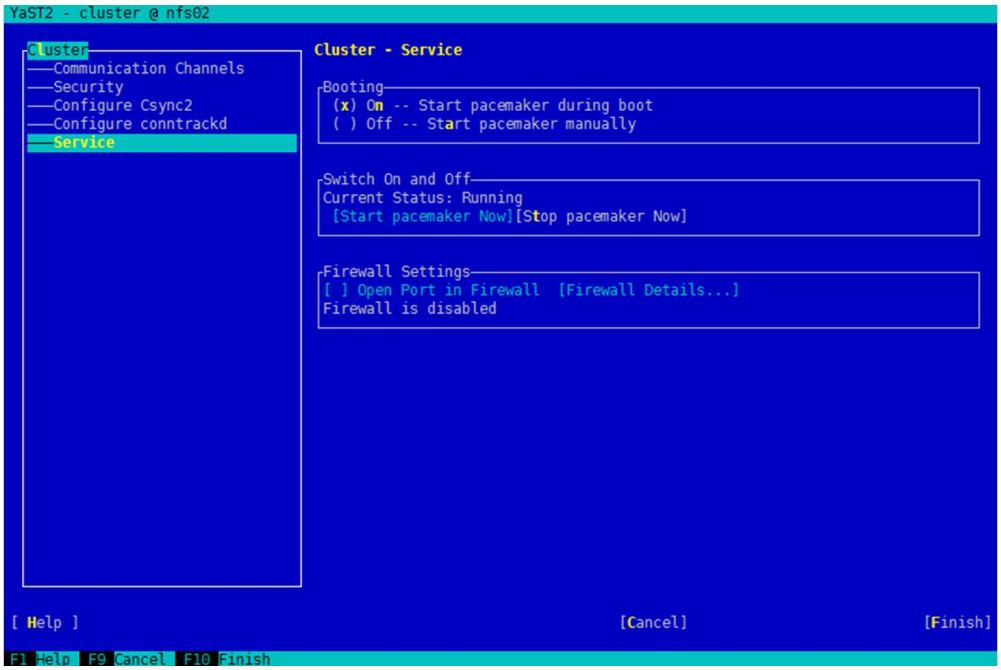
8. On the left side of the page, choose **Service**. Then, configure parameters on the right side of the page.

   Set the parameters as follows:

   - **Booting**: **On** is selected by default, which indicates that the cluster is automatically started when the server starts.
   - **Switch on and off**: Ensure that the cluster has been started.
   - **Firewall Settings**: Ensure that **Firewall is disabled** is selected.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-17 Service page



9. Select **Finish** and press **Enter** to complete the configuration.
10. Copy the **key_hagroup** and **csync2.cfg** files on the active NFS server to the standby NFS server.

    Log in to the active NFS server as user **root** and run the following command:

    scp /etc/csync2/key_hagroup /etc/csync2/csync2.cfg *Name of the standby NFS server*:**/etc/csync2**

    The following command is used as an example:

    scp /etc/csync2/key_hagroup /etc/csync2/csync2.cfg nfs02:/etc/csync2
11. Run the following commands on the active NFS server:

    systemctl enable csync2.socket

    systemctl enable xinetd

    systemctl restart xinetd
12. Run the following commands on the standby NFS server.

    Log in to the standby NFS server as user **root** and run the following commands:

    systemctl enable csync2.socket

    systemctl enable xinetd

    systemctl restart xinetd
13. Run the following command on the active NFS server to synchronize the configuration file:

    csync2 -xv
14. Run the following command on the active NFS server to check the cluster status:

    Ensure that the cluster status is **active (running)**.

 Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> If the command output indicating that the STONITH disk has not been configured, this is normal. The STONITH disk will be configured in the subsequent steps.

systemctl status pacemaker

15. Run the following commands on the active NFS server to restart the cluster:

    systemctl stop pacemaker

    systemctl start pacemaker

16. Run the following command on the standby NFS server to check the cluster status:

    Ensure that the cluster status is **active (running)**.

    > **NOTE**
    >
    > If the command output indicating that the STONITH disk has not been configured, this is normal. The STONITH disk will be configured in the subsequent steps.

    systemctl status pacemaker

17. Run the following commands on the standby NFS server to restart the cluster:

    systemctl stop pacemaker

    systemctl start pacemaker

18. Run the following command on the active NFS server to check the cluster heartbeat status:

    corosync-cfgtool -s

    The system displays the heartbeats of the active and standby links. Ensure that the configurations are correct. An example is provided as follows:

    ```
    Printing ring status.
    Local node ID 167772739
    RING ID 0
    id= 10.0.4.101
    status= ring 0 active with no faults
    RING ID 1
    id= 10.0.5.101
    status= ring 1 active with no faults
    ```

19. Run the following command to check the cluster status on the active NFS server:

    crm_mon -r1

    The terminal display is as follows, where two NFS servers are in **Online** state, indicating that the cluster is functional:

    ```
    Last updated: Wed Oct 19 17:40:31 2016
    Last change: Tue Oct 18 15:32:00 2016 by root via cibadmin on hana01
    Stack: classic openais (with plugin)
    Current DC: nfs01 - partition with quorum
    Version: 1.1.12-f47ea56
    2 Nodes configured, 2 expected votes
    0 Resources configured


    Online: [ nfs01 nfs02 ]
    ```

Step 4 Configure the softdog.

1. Run the following command on the active NFS server to open the file and enter **i** to enter editing mode:

 Copyright © Huawei Technologies Co., Ltd.

vi /etc/init.d/boot.local

2. Add the following information to the last line of the file:
```
modprobe softdog >/dev/null 2>&1
```
3. Press **Esc**, enter **:x!**, and press **Enter** to exit the configuration.
4. On the CLI, run the following command:

   modprobe softdog
5. Repeat steps **Step 4.1** to **Step 4.4** to configure the softdog on the standby NFS server.

Step 5 Configure SBD on the Fence devices.

1. Run the following command on the active and standby NFS servers to start the SBD service automatically once the active and standby NFS servers start:

   systemctl enable sbd
2. Run the following command on the active NFS server to create an SBD partition:

   The command is in the following format:

   sbd -d /dev/disk/by-id/*Partition ID* **create**

   NOTE

   To query an SDB disk ID, run the **ll /dev/disk/by-id |grep** *Partition name*|**grep scsi-3** command. For example, if the partition name is **/dev/sdb1**, run the **ll /dev/disk/by-id |grep sdb|grep scsi-3** command to query the ID corresponding to **sdb1**.

   The following command is used as an example:

   sbd -d /dev/disk/by-id/scsi-36888603000000db7fa179ea56210049-part1 create
3. Run the following command to allocate the partition to the active NFS server:

   The command is in the following format:

   sbd -d /dev/disk/by-id/*Partition ID* **allocate** *Active node host name*

   The following command is used as an example:

   sbd -d /dev/disk/by-id/scsi-36888603000000db7fa179ea56210049-part1 allocate nfs01
4. Run the following command to allocate the partition to the standby NFS server:

   The command is in the following format:

   sbd -d /dev/disk/by-id/*Partition ID* **allocate** *Standby node host name*

   The following command is used as an example:

   sbd -d /dev/disk/by-id/scsi-36888603000000db7fa179ea56210049-part1 allocate nfs02
5. Run the following command to query the allocated partition:

   The command is in the following format:

   sbd -d /dev/disk/by-id/*Partition ID* **list**

   The following command is used as an example:

   sbd -d /dev/disk/by-id/scsi-36888603000000db7fa179ea56210049-part1 list

   The command output is as follows:

 Copyright © Huawei Technologies Co., Ltd.

```
0  nfs01 clear
1  nfs02 clear
```

6. Run the following command to dump the partition:

   sbd -d /dev/disk/by-id/*Partition ID* **dump**

   The following command is used as an example:

   sbd -d /dev/disk/by-id/scsi-36888603000000db7fa179ea56210049-part1 dump

7. Open the **sbd** file and add data to the file.

   Run the **vi /etc/sysconfig/sbd** command to open the file and add data to the file.

   An example is provided as follows:

   NOTE

   Enter the path of the partition for SBD in **SBD_DEVICE**. The partition in the following terminal display is for reference only.

   ```
   SBD_DEVICE="/dev/disk/by-id/scsi-36888603000000db7fa179ea56210049-part1"
   SBD_OPTS="-W"
   ```

8. On active NFS server, synchronize the configuration file to the standby NFS server.

   scp /etc/sysconfig/sbd *Standby node host name*:**/etc/sysconfig**

   The following command is used as an example:

   scp /etc/sysconfig/sbd nfs02:/etc/sysconfig

9. Run the following commands on the active NFS server to restart the cluster:

   systemctl stop pacemaker

   systemctl start pacemaker

10. Run the following commands on the standby NFS server to restart the cluster:

    systemctl stop pacemaker

    systemctl start pacemaker

11. Check cluster configurations.

    crm_mon -r1

    The terminal display is as follows, where two NFS servers are in **Online** state, indicating that the cluster is functional:

    ```
    Last updated: Wed Oct 19 17:40:31 2016
    Last change: Tue Oct 18 15:32:00 2016 by root via cibadmin on hana01
    Stack: classic openais (with plugin)
    Current DC: nfs01 - partition with quorum
    Version: 1.1.12-f47ea56
    2 Nodes configured, 2 expected votes
    0 Resources configured


    Online: [ nfs01 nfs02 ]
    ```

Step 6 Add Fence SBD resources.

1. Run the following command on the active NFS server to switch to the CRM configuration mode:

   crm

   Information similar to the following is displayed:

 Copyright © Huawei Technologies Co., Ltd.

```
crm(live)#
```

2. Run the following command to switch to the configuration mode:

   configure

3. Run the following commands to add SBD resources:

   primitive r_sbd stonith:external/sbd params pcmk_delay_max=40

   commit

Step 7 Assign a virtual service IP address.

1. On the management console, click **Service List** and choose **Computing** > **Elastic Cloud Server** to switch to the **Elastic Cloud Server** page.
2. Locate the ECS on which an NFS server is deployed and click the ECS name. Then, the page for the ECS details is displayed.
3. Click the **NIC** tab and then **Manage Private IP** in the row of the server or management plane NIC. Then, the system displays the **Virtual IP Address** page.
4. Click **Assign Virtual IP Address** to assign a floating IP address. Locate the row that contains the target IP address, click **Bind to Server** to bind the IP address to the target ECS, and repeat this operation to bind the IP address to other ECSs.
5. Run the following commands on the active NFS server in CRM configuration mode.

   In the commands, **params ip** is the virtual service IP address of the NFS server. This value is for reference only.

   primitive nfs_vip ocf:heartbeat:IPaddr2 params ip=*10.0.1.103* op monitor interval="10" timeout="20" on-fail=restart

   commit

Step 8 Create cluster shared volume file systems.

Run the following commands on the active NFS server to create the cluster shared disk file system for the shared and backup volumes, respectively:

In the commands, **params device** and **directory** specify the volume ID and path, and the values provided are for reference only. For instructions about how to query a volume ID, see **Step 5.2**.

primitive nfs_shared ocf:heartbeat:Filesystem params device="*/dev/disk/by-id/Volume ID*" directory="/shared" fstype=xfs op monitor interval="10" timeout="40" on-fail=restart

primitive nfs_bak ocf:heartbeat:Filesystem params device="*/dev/disk/by-id/Volume ID*" directory="/backup" fstype=ext3 op monitor interval="10" timeout="40" on-fail=restart

primitive nfs_sapmnt ocf:heartbeat:Filesystem params device="*/dev/disk/by-id/Volume ID*" directory="/sapmnt " fstype=ext3 op monitor interval="10" timeout="40" on-fail=restart

primitive nfs_sys ocf:heartbeat:Filesystem params device="*/dev/disk/by-id/Volume ID*" directory="/usr/sap/A01/SYS" fstype=ext3 op monitor interval="10" timeout="40" on-fail=restart

 Copyright © Huawei Technologies Co., Ltd.

primitive nfs_sapcd ocf:heartbeat:Filesystem params device="*/dev/disk/by-id/Volume ID*" directory="/sapcd" fstype=ext3 op monitor interval="10" timeout="40" on-fail=restart

commit

Step 9 Create the **nfsserver** resource.

In the CRM configuration mode on the active NFS server, create the **nfsserver** resource.

If the floating IP address (specified by **nfs_ip**) of the NFS server is 10.0.1.103, run the following commands:

primitive nfsserver nfsserver params nfs_ip=*10.0.5.103* nfs_shared_infodir="/shared" nfs_shared_infodir="/backup" nfs_shared_infodir="/sapmnt" nfs_shared_infodir="/usr/sap/A01/SYS" nfs_shared_infodir="/sapcd" operations $id=nfsserver-operations op monitor interval="10" timeout="20" on-fail=restart

commit

Step 10 Create the resource group **nfs_group**.

Run the following commands on the active NFS server in CRM configuration mode to create resource group **nfs_group** for the resource created from **Step 7.5** to **Step 9**:

group nfs_group nfs_vip nfs_shared nfs_bak nfs_sapmnt nfs_sys nfs_sapcd nfsserver

commit

Step 11 Create Clone Ping.

Run the following commands on the active NFS server in the CRM configuration mode to create Clone Ping:

primitive r_ping ocf:pacemaker:ping params multiplier="100" dampen="5" host_list="*10.0.5.1*" op monitor interval="15" timeout="60" start="60" op start interval="0" timeout="60"

clone PING r_ping

commit

Set the parameters as follows:

- **r_ping**: specifies the Clone Ping resource name.
- **Multiplier**: an efficiency enhancer that uses the benchmark of 100. When packet loss occurs during the ping operation between two nodes, the multiplier decreases a certain value from 100 to determine the service NIC communication status of the nodes.
- **dampen**: indicates that the ping operation is performed once every 5s.
- **10.0.5.1**: indicates the gateway IP address of the server or backup plane network segment for the NFS servers.
- **monitor**: monitors resources; **interval**: indicates that if pinging the upper-layer switch fails within 15s, the system will migrate resources at most 60s (timeout) later.

 Copyright © Huawei Technologies Co., Ltd.

Step 12 Create restraint **nfs_conn**.

Run the following commands on the active NFS server in the CRM configuration mode to create restraint **nfs_conn** on resource group **nfs_group**:

location nfs_conn nfs_group rule -inf: not_defined pingd or pingd lte 0

commit

Step 13 Configure other information.

1. Configure the **stonith** parameter:
   property startup-fencing=true
   property stonith-enabled=true
   property stonith-action=off
   commit
2. Configure the failure timeout duration:
   rsc_defaults failure-timeout=600
   commit
3. Press **Ctrl+C** on the active NFS server to exit the CRM configuration mode.

----End

3.7.3 Attaching the Shared and Backup Volumes

Scenarios

Attach the shared and backup volumes on NFS servers to SAP HANA nodes. If you use SFS Turbo to provide shared file storage, skip this section. For details about how to mount the backup volumes, see section **Formatting a Disk** in the *SAP HANA User Guide*.

Procedure

Step 1 Log in to all SAP HANA nodes to attach shared and backup volumes to them.

1. Run the following commands to create the **/hana/shared** and **/hana/backup** directories:
   mkdir -p /hana/shared
   mkdir -p /hana/backup
2. Run the following commands to assign permissions to **/shared** and **/backup**:
   chmod -R 777 /hana/shared
   chmod -R 777 /hana/backup
3. Add the following content to the end of the **/etc/auto.master** file:
   ```
   /- /etc/hananfs.direct
   ```
4. Create and edit the **/etc/hananfs.direct** file.
   vi /etc/hananfs.direct
   Add a sharing record. In this example, the floating IP address of the NFS server is **10.0.5.103**.
   /hana/shared -rw,intr,nolock,rsize=32768,wsize=32768,timeo=14,vers=3 10.0.5.103:/shared

 Copyright © Huawei Technologies Co., Ltd.

/hana/backup -rw,intr,nolock,rsize=32768,wsize=32768,timeo=14,vers=3 10.0.5.103:/backup

5. Check whether **autofs** has been attached to the shared and backup directories.

   systemctl restart autofs

   Run the following commands to check whether the **/hana/shared** and **/hana/backup** directories have been attached properly:

   ls /hana/shared

   ls /hana/backup

   df -h

6. Enable automatic start of the **autofs** service during system startup.

   systemctl enable autofs

----End

3.7.4 Formatting DESS Disks

Procedure

Step 1 Log in to the jump host and use SSH to switch to the active SAP HANA BMS.

Step 2 Create XFS file systems for the planned log and data volumes.

The following drive letters are for reference only. Set them based on the actual planning.

mkfs.xfs -f -d agcount=60 */dev/sdc*

mkfs.xfs -f -d agcount=60 */dev/sdd*

mkfs.xfs -f -d agcount=60 */dev/sde*

mkfs.xfs -f -d agcount=60 */dev/sdf*

----End

3.7.5 Configuring the global.ini File

Scenarios

Obtain the **global.ini** file from the **/hana/shared/** directory and modify the **Storage HA configuration**, **Persistence configuration**, and **Communication** parts in the file.

Procedure

Step 1 Log in to the jump host and use SSH to switch to the active SAP HANA BMS.

Step 2 View world wide names (WWNs) of volumes.

Run the following command to view the WWNs of the two log volumes (512 GB each) and the two data volumes (6 TB each):

upadmin show vlun

 Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> This operation also needs to be performed on other SAP HANA nodes to check WWNs of volumes. WWNs of the four volumes on all nodes should be the same.

Step 3 Download the SAP HANA installation package.

1. On the CLI, run the following commands to download SAP HANA installation packages:

   wget https://obs-sap.obs.myhwclouds.com/*hana/software/sps12/51052383_part1.exe* -P /hana/shared

   wget https://obs-sap.obs.myhwclouds.com/*hana/software/sps12/51052383_part2.rar* -P /hana/shared

   wget https://obs-sap.obs.myhwclouds.com/*hana/software/sps12/51052383_part3.rar* -P /hana/shared

2. Run the following command to decompress the installation package:

   unrar x *51052383_part1.exe*

Step 4 Prepare for the **fcV3Client.py** file.

1. Download the **fcV3Client.py** file.

   wget https://obs-sap.obs.myhwclouds.com/hana/cfgandscript/scale_out_script.zip -P /hana/shared

2. Switch to the **/hana/shared/** directory and decompress the package to obtain the **fcV3Client.py** file.

   cd /hana/shared

   unzip scale_out_script.zip

3. Copy the **fcV3Client.py** file to the **/hana/shared/** directory.
4. Copy the **client.py** file to the **/hana/shared/** directory.

   > **NOTE**
   >
   > Run the **find /hana/shared -name client.py** command to view the directory where the **client.py** file is stored.

Step 5 Configure the **global.ini** file.

1. Copy the **global.ini** file to the **/hana/shared/** directory.

   cp /hana/shared/scale_out_script/global.ini /hana/shared

2. Configure the **global.ini** file.

   vi /hana/shared/global.ini

3. Configure **Storage HA configuration**.

   Set **ha_provider** to **fcV3Client** and **wwid** of each partition to WWNs queried in **Step 2**. **partition_*_log__mountoptionspartition_*_log__mountoptions** is a **mount** parameter.

   An example is provided as follows:

```
################################################################################
# Storage HA configuration
################################################################################
# . short_desc
# storage HA configuration
[storage]
```

 Copyright © Huawei Technologies Co., Ltd.

```
# .short_desc
# name of python HA provider script
ha_provider = fcV3Client
ha_provider_path = /hana/shared/

# these parameters name the WWIDs of the devices for each partition/usage_type combination
# if you have more nodes, add your LUNs here.
# for proper usage, replace the '...' with specified WWID in your system.
partition_*_*__prType = 5
partition_*_data__mountoptions = -o noatime,nodiratime,wsync
partition_*_log__mountoptions = -o noatime,nodiratime,wsync
partition_1_data__wwid = 680d4a51008ea4d90f0948f90000002d
partition_1_log__wwid = 680d4a51008ea4d9023c87b400000018
partition_2_data__wwid = 680d4a51008ea4d90f09748c0000002e
partition_2_log__wwid = 680d4a51008ea4d9023d394400000019
```

4. Configure **Persistence configuration**.

   Change to the actual SID of the SAP HANA database, for example, **ANA**.

   An example is provided as follows:

```
#########################################################################
#####
# Persistence configuration
#########################################################################
#####
[persistence]
basepath_datavolumes=/hana/data/ANA/
basepath_logvolumes=/hana/log/ANA/

basepath_shared=yes
```

5. Configure **Communication**.

   Change the IP addresses and hostnames in the following information to the actual IP addresses and hostnames.

   An example is provided as follows:

```
#########################################################################
#####
# Communication
#########################################################################
#####
[communication]
listeninterface = .global

[internal_hostname_resolution]
10.0.2.2 = hana001
10.0.2.3 = hana002
10.0.2.4 = hana003
```

----End

3.7.6 Creating an SAP HANA Installation Path

Procedure

Step 1 Log in to the jump host and use SSH to switch to an SAP HANA BMS.

Step 2 Run the following commands to create a permanent database path. In the commands, **ANA** indicates the actual SID of the database.

mkdir -p */hana/data/ANA /hana/log/ANA*

chmod o+w */hana/data/ANA /hana/log/ANA*

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Repeat the preceding steps to create database paths on other SAP HANA BMSs.

----End

3.7.7 Installing SAP HANA

Scenarios

This section uses the SAP HANA 1.0 installation package as an example. You can download the package from the official website.

Prerequisites

- You have created BMSs, formatted disks attached to them, and completed required configurations.
- You have synchronized the time of the BMSs.

Procedure

Step 1 Log in to the jump host and use SSH to switch to the active SAP HANA BMS.

Step 2 Enter the directory where the installation file is stored.

For example, if the installation file is stored in **/51052383/DATA_UNITS/HDB_SERVER_LINUX_X86_64**, run the following command:

cd /51052383/DATA_UNITS/HDB_SERVER_LINUX_X86_64

Step 3 Run the following command to assign permissions to the directory:

chmod 777 -R /hana

Step 4 Run the following command to install SAP HANA:

Set the parameters based on the actual planning. **internal_network** is the planned internal communication network segment.

NOTE

When the SAP HANA 2.0 is used, the parameter **--db_mode=singledb** is not required.

For details, see section "Installing SAP HANA" in *SAP HANA User Guide (BMS Cluster Deployment)*.

./hdblcm --action=install --sid=ANA --number=00 --sapmnt=/hana/shared/ --storage_cfg=/hana/shared/ --root_user=root --autostart=on --restrict_max_mem=off --max_mem=0 --logpath=*/hana/log/ANA* **--nostart=off --datapath=***/hana/data/ANA* **--shell=/bin/sh --hostname=***hana001* **--remote_execution=ssh --install_hostagent=on --db_mode=singledb --install_ssh_key=on --addhosts=***hana002***:role=worker:group=default:storage_partition=2,***hana003***:role=standby:group=default --password=***Admin123* **--system_user_password=***Admin123* **--root_password=***Admin@123* **--internal_network=***10.0.2.0/24*

----End

 Copyright © Huawei Technologies Co., Ltd.

For details about how to configure backup paths and storage parameters, see section "Installing SAP HANA (Cluster Deployment and Two NFS Servers Deployed)" in *SAP HANA User Guide (BMS Cluster Deployment)*.

3.8 Installing SAP NetWeaver

3.8.1 Formatting the Disks Attached to an NFS Server

Scenarios

NOTICE

If you use SFS Turbo to provide shared file storage, skip this section.

Format the shared volume planned for SAP NetWeaver on the NFS server to meet the requirements for installing the SAP NetWeaver system.

Procedure

Step 1 Log in to the active NFS server.

Step 2 Run the following command to query the disk to be formatted:

fdisk -l

Information similar to the following is displayed:

```
... Disk /dev/sde doesn't contain a valid partition table
```

Step 3 Format the disk and attach it to the specified directory based on information provided in **Table 3-8**.

Run the following command to format the disk (taking the **dev/sde** disk as an example):

fdisk /dev/sde

The following information is displayed:

```
Command (m for help):
```

Step 4 Enter **n** and press **Enter** to create partitions.

Information similar to the following is displayed:

```
... Command action   e   extended   p   primary partition (1-4)
```

Step 5 Enter **p** and press **Enter**.

Creating a primary partition is used as an example.

Information similar to the following is displayed:

```
Partition number (1-4, default 1):
```

Step 6 Enter the primary partition ID and press **Enter**.

 Copyright © Huawei Technologies Co., Ltd.

Primary partition ID 1 is used as an example.

Information similar to the following is displayed:

```
... First sector (2048-259715199, default 2048):
```

Step 7 Press **Enter**.

The default start cylinder number is used as an example.

Information similar to the following is displayed:

```
... Using default value 2048 Last sector, +sectors or +sizeM or +size{K,M,G}(2048-259715199, default 2048):
```

Press **Enter**.

The default end cylinder number is used as an example.

Information similar to the following is displayed:

```
.... Using default value 209715199  Command (m for help):
```

Step 8 Enter **w** and press **Enter**.

Enter the partition result into the partition table to complete partition creation.

Step 9 Create partitions **sde2** and **sde3** as required.

NOTE

Run the **partprobe** command on the standby NFS server to update the partition table of the standby node.

1. Run the following commands to create file systems on partitions:

   mkfs.ext3 /dev/sde1

   mkfs.ext3 /dev/sde2

   mkfs.ext3 /dev/sde3

   Formatting the disk requires a period of time. During this time, observe the system running status and do not exit disk formatting.

1. Run the following commands to create directories:

   mkdir /sapmnt

   mkdir -p /usr/sap/A01/SYS

   mkdir /sapcd

   NOTE

   You also need to create directories on the standby NFS server.

2. Run the following commands to attach the volumes to corresponding directories:

   mount /dev/sde1 /sapmnt

   mount /dev/sde2 /usr/sap/A01/SYS

   mount /dev/sde3 /sapcd

Step 10 Open the **/etc/exports** file.

Edit the file to share the volumes on the NFS server to the active and standby ASCS nodes.

 Copyright © Huawei Technologies Co., Ltd.

vi /etc/exports

Add the shared records of the active and standby ASCS nodes.

```
/sapmnt 10.0.5.11(rw,sync,no_root_squash,no_subtree_check)
/usr/sap/A01/SYS 10.0.5.11(rw,sync,no_root_squash,no_subtree_check)
/sapcd 10.0.5.11(rw,sync,no_root_squash,no_subtree_check)
/sapmnt 10.0.5.12(rw,sync,no_root_squash,no_subtree_check)
/usr/sap/A01/SYS 10.0.5.12(rw,sync,no_root_squash,no_subtree_check)
/sapcd 10.0.5.12(rw,sync,no_root_squash,no_subtree_check)
```

Run the following command to make the **/etc/exports** configurations take effect:

exportfs -a

Run the following command to restart the NFS server:

systemctl restart nfsserver

Run the following command to check the NFS server status:

service nfsserver status

Run the following command to check whether the shared directory is successfully set. If the directory information is displayed in the command output, the setting is successful.

showmount -e

----End

3.8.2 Attaching NFS Server Volumes

Scenarios

NOTICE

If you use SFS Turbo to provide shared file storage, skip this section. To attach an SFS Turbo file system to an ECS, see related sections in the *SAP NetWeaver User Guide*.

After the HA mechanism of NFS servers has been configured, attach the corresponding volumes on NFS servers to both the active and the standby ASCS nodes.

NOTE

For details about the HA mechanism of NFS servers, see section **Configuring HA on NFS Servers**.

Procedure

Step 1 Log in to the active ASCS node.

1. Run the following commands to create directories:
   mkdir /sapmnt
   mkdir -p /usr/sap/A01/SYS

 Copyright © Huawei Technologies Co., Ltd.

mkdir /sapcd

2. Attach the shared volumes to corresponding directories on the active ASCS node.

   In this example, the floating IP address of the NFS server is **10.0.5.103**.

   mount -t nfs -o vers=3 10.0.5.103:/sapmnt /sapmnt

   mount -t nfs -o vers=3 10.0.5.103:/usr/sap/A01/SYS /usr/sap/A01/SYS

   mount -t nfs -o vers=3 10.0.5.103:/sapcd /sapcd

3. Write disk attaching relationships into the **/etc/fstab** file.

   Open the file and add the following content:

   ```
   10.0.5.103:/sapmnt /sapmnt nfs defaults 0 0
   10.0.5.103:/usr/sap/A01/SYS /usr/sap/A01/SYS nfs defaults 0 0
   10.0.5.103:/sapcd /sapcd nfs defaults 0 0
   ```

4. Log in to the standby ASCS node and repeat steps **Step 1.1** to **Step 1.3**.

----End

3.8.3 Attaching a Shared Disk and Binding a Floating IP Address

Scenarios

In the distributed HA deployment scenario, the active and standby ASCS nodes synchronize data using the shared disk. This section provides guidance for you to bind the data volume of the active ASCS node to the standby ASCS node and bind the floating IP address to both the active and the standby ASCS nodes. For details, see section "Attaching a Shared Disk and Binding a Floating IP Address" in the *SAP NetWeaver User Guide*.

3.8.4 Formatting the Shared Disk Attached to the Active and the Standby ASCS Nodes

Scenarios

The shared disks of ASCS nodes can be used only after they are formatted and attached to required directories. For details, see section "Formatting a Disk" in the *SAP NetWeaver User Guide*.

3.8.5 Installing SAP NetWeaver

For details about how to install SAP applications, visit the following website to refer to the specific SAP application software installation guide.

SAP Help Center: **https://help.sap.com/viewer/index**

You need to install the ASCS instance on the active ASCS node and the ERS instance on the standby ASCS node. For details, see section "Installing the SAP NetWeaver Software" in the **SAP NetWeaver User Guide**.

3.8.6 Configuring the HA Function for SAP NetWeaver

After the ASCS instance and the ERS instance have been installed, you need to configure the HA mechanism for the active and the standby ASCS nodes of SAP

 Copyright © Huawei Technologies Co., Ltd.

NetWeaver. For details, see section "Configuring the HA Function for SAP NetWeaver (Distributed HA Deployment)" in the *SAP NetWeaver User Guide*.

3.9 Installing SAP HANA Studio

3.9.1 Installing the SAP HANA Studio on a Windows ECS

SAP HANA Studio manages SAP HANA. After SAP HANA nodes are deployed, you need to install the SAP HANA Studio and use it to manage the SAP HANA nodes.

This section describes how to install the SAP HANA Studio on a Windows ECS.

Prerequisites

- You have prepared related resources. For details, see section "Preparing Resources".
- You have created ECSs, formatted disks attached to them, and installed the SAP HANA.
- The firewall on the target ECS has been disabled.
- Remote login to the target ECS has been enabled.

Procedure

Step 1 Use the Remote Desktop Protocol (RDP) and elastic IP address to log in to the SAP HANA Studio ECS.

Use the username **Administrator** and the password obtained in section **Obtaining the Password for Logging In to a Windows ECS** to log in to the SAP HANA Studio ECS.

Step 2 Upload the installation package obtained from the SAP official website to the SAP HANA Studio ECS.

Step 3 Decompress the installation package and navigate to the directory where SAP HANA Studio is stored.

Step 4 On the Windows page, switch to the directory where the SAP HANA Studio installation package is stored and double-click **hdbsetup.exe** to open the installation wizard page.

Step 5 Select the installation path and click **Next**.

Step 6 On the **Select Features** page, select the features to be installed and click **Next**.

You are advised to select all features.

Step 7 Confirm all information on the **Review & Confirm** page and click **Install**.

Step 8 An installation page is displayed. Continue the installation. When the installation is complete, the system displays the message "You have successfully installed the SAP HANA Studio."

Step 9 Click **Finish**.

----End

 Copyright © Huawei Technologies Co., Ltd.

3.9.2 Installing the SAP HANA Studio on a Linux ECS

SAP HANA Studio manages SAP HANA. After SAP HANA nodes are deployed, you need to install the SAP HANA Studio and use it to manage the SAP HANA nodes.

This section describes how to install the SAP HANA Studio on a Linux ECS.

Prerequisites

- You have prepared related resources. For details, see section "Preparing Resources".
- You have created ECSs, formatted disks attached to them, and installed the SAP HANA.
- The firewall on the target ECS has been disabled.

Procedure

Step 1 Log in to the SAP HANA Studio ECS with an elastic IP address bound as user **root** using the key file.

Step 2 Upload the obtained installation package to the **/hana/shared** directory on the ECS where the SAP HANA Studio is to be installed and decompress it.

Enter the directory where the installation file is stored. For example, if the installation file is stored in **/DATA_UNITS/HDB_STUDIO_LINUX_X86_64**, run the following command:

cd /DATA_UNITS/HDB_STUDIO_LINUX_X86_64

Step 3 Assign operation permissions to the directory where the installation packages are stored.

For example, if the directory is **HDB_STUDIO_LINUX_X86_64**, run the following command:

chmod 777 -R HDB_STUDIO_LINUX_X86_64

Step 4 Switch to the directory and perform the installation. The SAP HANA Studio installation page is displayed.

./hdbsetup

Step 5 Select the installation path and click **Next**.

Step 6 On the **Select Features** page, select the features to be installed and click **Next**.

You are advised to select all features.

Step 7 Confirm all information on the **Review & Confirm** page and click **Install**.

Step 8 An installation page is displayed. Continue the installation. When the installation is complete, the system displays the message "You have successfully installed the SAP HANA Studio."

Step 9 Click **Finish**.

Step 10 Go to **Step 5** to select the installation path, edit the **hdbstudio.ini** file, and add parameters to configure the GTK version.

 Copyright © Huawei Technologies Co., Ltd.

vi hdbstudio.ini

Add the following parameters:

--launcher.GTK_version

2

An example is provided as follows:

```
-startup
plugins/org.eclipse.equinox.launcher_1.3.201.v20161025-1711.jar
--launcher.library
plugins/org.eclipse.equinox.launcher.gtk.linux.x86_64_1.1.401.v20161122-1740
--launcher.GTK_version
2
--launcher.XXMaxPermSize
512m
```

Step 11 (Optional) If the version is not configured in **Step 10**, run the following commands before starting **hdbstudio** on the Linux OS:

export SWT_GTK3=0

./hdbstudio

----End

3.9.3 Connecting SAP HANA Nodes to SAP HANA Studio

Scenarios

SAP HANA nodes can be managed only after they are connected to the SAP HANA Studio.

This section uses a Windows ECS where SAP HANA Studio is deployed as an example.

Procedure

Step 1 Start SAP HANA Studio.

On the ECS where the SAP HANA Studio is deployed, choose **Start** > **SAP HANA** > **SAP HANA Studio**. Then, the system displays the SAP HANA Studio management page and the **Workspace Launcher** dialog box.

Step 2 Specify the **Workspace** directory, select **Use this as the default and do not ask me again**, and click **OK**.

Step 3 On the displayed **Security Storage** dialog box, click **No**.

Step 4 On the **Overview** page, click **Open Administration Console** to enter the **SAP HANA Administration Console** page.

Step 5 Right-click the blank area under **System**.

Step 6 Choose **Add System**. On the displayed **Specify System** page, configure parameters.

Key parameters are as follows:

 Copyright © Huawei Technologies Co., Ltd.

- **Host Name**: Enter the service or client plane IP address of the SAP HANA BMS. In the cluster scenarios, you only need to enter the IP address of the first SAP HANA node, on which installation has been performed.
- **Instance Number**: Enter the number of the instance on the SAP HANA node.
- **Mode**: Select a mode based on actual requirements. If SAP HANA 2.0 is used, select **Multiple containers**.

Step 7 Click **Next** to go to the **System** page. Choose **Authentication by database user** and enter the username and password.

The username and password are those configured during SAP HANA software installation. The username is consistently set to **SYSTEM**.

Step 8 Click **Next** and then **Finish**. Then, the SAP HANA Studio automatically connects to the database.

If the connection fails, check whether the database instance on the SAP HANA node is running.

Step 9 Under **System** of the **SAP HANA Administration Console** page, double-click the node to be checked.

Step 10 Click the **Landscape** tab on the right of the page and check the status of each process on the SAP HANA node.

Green indicates that the process is running properly.

----End

 Copyright © Huawei Technologies Co., Ltd.

4 Appendix

4.1 Handling the SSH Switching Failure Between Active and Standby Nodes

Question Description

On a Linux node, the SSH switching between the active and standby nodes fails. As a result, the HA function fails to be configured.

Possible Causes

Key pair is not selected for the **Login Mode** during node creation.

Handling Method

Upload the key file to the target node.

Step 1 Log in to the jump host, copy the certificate private key file to the **/root/.ssh** directory, and rename the file **id_rsa**.

NOTE

To create a key, do as follows:

On the cloud server creation page, click **View Key Pair**. On the displayed **Key Pair** page, click **Create Key Pair**, specify the key pair name, and click **OK**. In the **Information** dialog box that is displayed, click **OK**. Then, you can view and save the private key as prompted.

For example, if the private key file name is **private.pem**, run the following commands to rename it:

cp /usr/private.pem /root/.ssh/id_rsa

cd /root/.ssh/

chmod 600 id_rsa

Step 2 Run the following commands to generate the **id_rsa.pub** and **authorized_keys** files:

 Copyright © Huawei Technologies Co., Ltd.

ssh-keygen -y -f id_rsa > id_rsa.pub

cp id_rsa.pub authorized_keys

Step 3 Use the server/backup plane IP address to allocate the public key file, the private key file, and the **authorized_keys** file to all nodes excepting SAP HANA Studio nodes.

The command is in the following format:

scp /root/.ssh/id_rsa *Peer IP address*:**/root/.ssh/**

scp /root/.ssh/authorized_keys *Peer IP address*:**/root/.ssh/**

scp /root/.ssh/id_rsa.pub *Peer IP address*:**/root/.ssh/**

Step 4 Verify the switching.

Use SSH to switch from the jump host to all nodes excepting the SAP HANA Studio node for verification.

For example, the server/backup plane IP address of the NFS server is 10.0.5.101. To switch from the jump host to the NFS server, run the following command:

ssh 10.0.5.101

----End

4.2 Follow-up Procedure After DESS Disk Capacity Expansion (fdisk)

After the capacity expansion of a DESS disk has succeeded, the additional disk space needs to be allocated to an existing partition or a new partition of a BMS.

Prerequisites

- You have logged in to the BMS. For details about how to log in to a BMS, see section **Logging In to a BMS** in the *Bare Metal Server User Guide*.
- You have attached the disk to the BMS, and the additional disk space has not been allocated.

Background

This section uses SUSE Linux Enterprise Server 11 SP4 64bit to describe how to allocate the additional space of an attached SCSI data disk to a partition using fdisk.

Currently, a disk has been attached to the BMS, the original disk capacity is 10 GB. In addition, a 10-GB space has been added to the disk through the management console, and the total disk capacity should be 20 GB. However, the additional space cannot be viewed on the BMS. The following operations guide you to query the additional space and expand the partition.

The method for allocating the additional space varies depending on the BMS OS. This document is used for reference only. For detailed operations and differences, see the corresponding OS documents.

 Copyright © Huawei Technologies Co., Ltd.

Based on your service requirements and actual disk condition, you can choose either of the following ways to allocate the additional disk space:

- Create a new partition (services will not be interrupted).

  Creating a new partition for the expanded disk does not require the original partitions to be unmounted. Therefore, the impacts on services are minor than expanding an existing partition. This method is recommended for system disks or disks carrying services that cannot be interrupted.

  If the MBR partition style is used, the disk capacity cannot exceed 2 TB and the number of partitions cannot exceed the upper limit after the expansion completes.

- Expand an existing partition (services will be interrupted).

  If the MBR partition style is used and the number of partitions has reached the upper limit, the existing partition needs to be expanded. Expanding an existing partition does not delete its data, but requires the partition to unmount. Therefore, the services will be interrupted.

  If the MRB partition style is used and the disk capacity after expansion has exceeded 2 TB, the disk space besides 2 TB cannot be allocated to a partition with MBR. In this case, if you change the partition style from MBR to GPT, the original disk data will be cleared. Therefore, back up the disk data before you change the partition style.

Expanding the Existing Partition

The following example shows you how to make use of the additional capacity of a disk attached to a BMS by recreating the **/dev/sda1** partition and mounting the partition on **/mnt/sdc**. During this process, the services will be interrupted.

Step 1 Run the following command to view the disk partition information:

fdisk -l

Information similar to the following is displayed:

```
ecs-xen-02:/home/linux # fdisk -l

Disk /dev/xvda: 107.4 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13054 cylinders, total 209715200 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00065c40

   Device Boot      Start         End      Blocks   Id  System
/dev/xvda1            2048    41945087    20971520   82  Linux swap / Solaris
/dev/xvda2   *    41945088    83892223    20973568   83  Linux
/dev/xvda3        83892224   209715199    62911488   83  Linux

Disk /dev/sda: 10.7 GB, 10737418240 bytes
64 heads, 32 sectors/track, 10240 cylinders, total 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x2f1c057a

  Device Boot      Start         End      Blocks   Id  System
/dev/sda1            2048    20971519    10484736   83  Linux
```

In the command output, the 10 GB has been added to the **/dev/sda** data disk on the management console, and the total capacity should be 20 GB. However, the

 Copyright © Huawei Technologies Co., Ltd.

additional space is not included in the command output. In this case, run the desired command to update the disk capacity of the BMS.

Step 2 Run the following command to update the disk capacity of the BMS:

echo 1 > /sys/class/scsi_device/*%d:%d:%d:%d*/device/rescan &

In the command, **%d:%d:%d:%d** indicates a folder in the **/sys/class/scsi_device/** directory and can be obtained using **lsscsi**.

For example, run the following command:

echo 1 > /sys/class/scsi_device/2:0:0:0/device/rescan &

Step 3 After the update is complete, run the following command to view the disk partition information again:

fdisk -l

Information similar to the following is displayed:

```
ecs-xen-02:/sys/class/scsi_device # fdisk -l

Disk /dev/xvda: 107.4 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13054 cylinders, total 209715200 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00065c40

   Device Boot      Start         End      Blocks   Id  System
/dev/xvda1            2048    41945087    20971520   82  Linux swap / Solaris
/dev/xvda2   *    41945088    83892223    20973568   83  Linux
/dev/xvda3        83892224   209715199    62911488   83  Linux

Disk /dev/sda: 21.5 GB, 21474836480 bytes
64 heads, 32 sectors/track, 20480 cylinders, total 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x2f1c057a

  Device Boot      Start         End      Blocks   Id  System
/dev/sda1            2048    20971519    10484736   83  Linux
```

In the command output, the additional space has been added to the **/dev/sda** data disk, and the update is successful. The **/dev/sda** disk has only one partition, **/dev/sda1**. Take note of first and last sectors of the **/dev/sda1** partition. These values will be used during the partition recreation. The partition's first sector is **2048**, and its last sector is **20971519**.

Step 4 Run the following command to unmount the disk partition:

umount /mnt/sdc

Step 5 Run the following command to enter fdisk and enter **d** to delete the **/dev/sda1** partition:

fdisk /dev/sda

Information similar to the following is displayed:

```
[ecs-xen-02:/sys/class/scsi_device # fdisk /dev/sda

Command (m for help): d
Selected partition 1

Command (m for help):
```

 Copyright © Huawei Technologies Co., Ltd.

Step 6 Enter **n** and press **Enter** to create partitions.

Entering **n** creates a new partition.

Information similar to the following is displayed:

```
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
```

There are two types of disk partitions:

- Choosing **p** creates a primary partition.
- Choosing **e** creates an extended partition.

Step 7 Ensure that the entered partition type is the same as the partition had before. In this example, a primary partition is used. Therefore, enter **p** and press **Enter** to create a primary partition.

Information similar to the following is displayed:

```
p
Partition number (1-4, default 1):
```

In the command output, **Partition number** specifies the primary partition number.

Step 8 Ensure that entered partition number is the same as the partition had before. In this example, the partition number **1** is used. Therefore, enter **1** and press **Enter**.

Information similar to the following is displayed:

```
Partition number (1-4, default 1): 1
First sector (2048-41943039, default 2048):
```

In the command output, **First sector** specifies the first sector.

NOTE

Data will be lost if the following operations are performed:

- Select a first sector other than the partition had before.
- Select a last sector smaller than the partition had before.

Step 9 Ensure that the entered first sector is the same as the partition had before. In this example, first sector **2048** is recorded in **Step 3**. Therefore, enter **2048** and press **Enter**.

Information similar to the following is displayed:

```
First sector (2048-41943039, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-41943039, default 41943039):
```

In the command output, **Last sector** specifies the last sector.

Step 10 Ensure that the entered last sector is equal to or greater than the last sector recorded in **Step 3**. In this example, the recorded last sector is **20971519**, and the default last sector is used. Therefore, enter **41943039** and press **Enter**.

Information similar to the following is displayed:

```
Last sector, +sectors or +size{K,M,G} (2048-41943039, default 41943039):
Using default value 41943039

Command (m for help):
```

The primary partition is successfully created.

 Copyright © Huawei Technologies Co., Ltd.

Step 11 Enter **p** and press **Enter** to view the details about the created partition.

Information similar to the following is displayed: (Details about the **/dev/sda1** partition are displayed.)

```
CCommand (m for help): p

Disk /dev/sda: 21.5 GB, 21474836480 bytes
64 heads, 32 sectors/track, 20480 cylinders, total 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x2f1c057a

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1            2048    41943039    20970496   83  Linux
Command (m for help):
```

Step 12 Enter **w** and press **Enter** to write the changes into the partition table.

Information similar to the following is displayed. The partition is successfully created.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

NOTE

In case that you want to discard the changes made before, you can exit fdisk by entering **q**.

Step 13 Run the following command to check the correctness of the file system on **/dev/sda1**:

e2fsck -f /dev/sda1

Information similar to the following is displayed:

```
ecs-xen-02:/sys/class/scsi_device # e2fsck -f /dev/sda1
e2fsck 1.41.9 (22-Aug-2009)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/sda1: 11/655360 files (0.0% non-contiguous), 79663/2621184 blocks
```

Step 14 Run the following command to expand the size of the file system on **/dev/sda1**:

resize2fs /dev/sda1

Information similar to the following is displayed:

```
ecs-xen-02:/sys/class/scsi_device # resize2fs /dev/sda1
resize2fs 1.41.9 (22-Aug-2009)
Resizing the filesystem on /dev/sda1 to 5242624 (4k) blocks.
The filesystem on /dev/sda1 is now 5242624 blocks long.
```

Step 15 Run the following command to mount the created partition to the **/mnt/sdc** directory:

mount /dev/sda1 /mnt/sdc

Step 16 Run the following command to view the mount result for **/dev/sda1**:

df -TH

----End

 Copyright © Huawei Technologies Co., Ltd.

4.3 Adding or Deleting a BMS NIC

If service requirements change, you can add or delete NICs on a BMS.

WARNING

- A NIC cannot be added to or deleted from a BMS with two NICs.
- A NIC can be added to and then deleted from a BMS with one NIC.
- Currently, only two NICs can be attached to a BMS.

4.3.1 Managing NICs

Dependency

- Combined API 1.8.9 or later
- ECS UI 2.2.29 or later
- The IaaS OpenStack V100R006C20U20 or later is used as the BMS POD in the region.

Restrictions and Limitations

- Only VPC NICs can be added or deleted.
- The number of VPC NICs of a BMS is limited by **baremetal:net_num** in the BMS flavor.

Prerequisites

NICs can only be added to or deleted from a BMS in running or stopped state.

Configuring ECS UI

Add the following parameters in the **Configuration File** area and set their values by following the instructions in section "Upgrading ECS UI" in the *ECS UI Upgrade Guide*:

```
is_supported_bms_addnic: "true"  //specifies whether NICs can be added to or deleted from BMSs. If yes, set the value to true. If no, set the value to false.
 is_supported_bms_delete_auxiliary_nic: "true"  //specifies whether extended NICs added during BMS creation can be deleted. If yes, set the value to true. If no, set the value to false.
```

Adding a NIC

To add NICs to your BMS, perform the following operations:

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** and choose **Computing** > **Bare Metal Server**.

   The BMS console is displayed.

 Copyright © Huawei Technologies Co., Ltd.

4. Click the name of the target BMS.

   The page showing details of the BMS is displayed.
5. Click the **NIC** tab. Then, click **Add NIC**.
6. Select the security group and subnet to be added.

   NOTE

   If you want to add a NIC with a specified IP address, enter an IP address into the **Private IP Address** field.
7. Click **OK**.

Follow-up procedure

The BMS cannot identify the newly added NICs. You must manually activate the NICs by following the instructions in section **Configuring a NIC Added to or Deleted from a BMS**.

Deleting a NIC

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click **Service List** and choose **Computing** > **Bare Metal Server**.

   The BMS console is displayed.
4. Click the name of the target BMS.

   The page showing details of the BMS is displayed.
5. Click the **NIC** tab, expand the NIC details, and make a note of the VLAN and MAC address.

   NOTE

   After deleting a NIC on the console, you need to log in to the BMS OS and perform related operations to delete the device (the VLAN and MAC address recorded will be used).
6. Click **Delete**.
7. Click **OK**.

Follow-up procedure

Delete network devices by following the instructions in section **Configuring a NIC Added to or Deleted from a BMS**.

Managing Virtual IP Addresses

You can bind a virtual IP address to a BMS NIC to provide an additional IP address for the NIC, making the network more flexible.

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click **Service List** and choose **Computing** > **Bare Metal Server**.

   The BMS console is displayed.

 Copyright © Huawei Technologies Co., Ltd.

4. Click the name of the BMS to which a virtual IP address needs to be bound.

   The page showing details of the BMS is displayed.

5. Click the **NIC** tab. Then, click **Manage Virtual IP Address**.

   The page showing details of the particular VPC is displayed.

6. On the **Virtual IP Addresses** tab, select a desired one or click **Assign Virtual IP Address** for a new one.
7. Click **Bind to Server** in the **Operation** column and select the target BMS and the NIC to bind the virtual IP address to the NIC.

   For details about the virtual IP address, see *Virtual Private Cloud User Guide*.

Changing a Security Group

To change the security group of a BMS NIC, perform the following operations:

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** and choose **Computing** > **Bare Metal Server**.

   The BMS console is displayed.

4. Click the name of the target BMS.

   The page showing details of the BMS is displayed.

5. Click the **NIC** tab. Then, click **Change Security Group**.
6. In the displayed **Change Security Group** dialog box, select the target security group.
7. Click **OK**.

Setting the Source/Destination Check for a NIC

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** and choose **Computing** > **Bare Metal Server**.

   The BMS console is displayed.

4. Click the name of the target BMS.

   The page showing details of the BMS is displayed.

5. Select the **NIC** tab. On the displayed page, click the icon before the NIC to be configured.
6. Enable or disable the source/destination check function.

   By default, the source/destination check function is enabled. When this function is enabled, the system checks whether source IP addresses contained in the packets sent by BMSs are correct. If the IP addresses are incorrect, the system does not allow the BMSs to send the packets. This mechanism prevents packet spoofing, thereby improving system security. If the BMS functions as a NAT server, router, or firewall, you must disable the source/destination check for the BMS.

 Copyright © Huawei Technologies Co., Ltd.

4.3.2 Configuring a NIC Added to or Deleted from a BMS

This section uses SUSE Linux Enterprise Server 12 SP3 (x86_64) as an example to describe how to configure a NIC added to or deleted from a BMS.

Configuring a NIC Added to a BMS

1. Obtain information about the NIC to be added.

   Table 4-1 Information to be collected

Parameter	Description	Example Value
VLAN and MAC address	Specifies the VLAN information and MAC address. To obtain them, perform the following operations: 1. In the BMS list, click the name of the target BMS. 2. Click the **NIC** tab, locate the row that contains the NIC to be added, and click . 3. Obtain the values of **VLAN** and **MAC Address**.	2835 fa:16:3e:01:c3:2e
Gateway	Specifies the gateway address. To obtain it, perform the following operations: 1. On the NIC details page, obtain the subnet information. 2. On the BMS details page, click the link following **VPC** to switch to the VPC list. 3. Click the name of the VPC to which the BMS belongs to go to the VPC details page. 4. Click the **Subnets** tab and obtain the gateway address of the subnet in step **1.a**.	192.168.1.1

2. Use a key or password to log in to the BMS as user **root**.
3. Run the following command to copy network configuration file **/etc/sysconfig/network/ifcfg-bond0** to generate file **/etc/sysconfig/network/ifcfg-bond0.***vlan* (replace *vlan* with the VLAN obtained in step **1.a**, such as **2835**):

   cp -p /etc/sysconfig/network/ifcfg-bond0 /etc/sysconfig/network/ifcfg-bond0.*2835*
4. Run the following command to edit **/etc/sysconfig/network/ifcfg-bond0.***vlan* and configure the network configuration file of the newly added NIC, such as **ifcfg-bond0.***2835*:

   vim /etc/sysconfig/network/ifcfg-bond0.*2835*

   Edit the file as follows:

   ```
   STARTMODE=auto
   ETHERDEVICE=bond0
   ```

 Copyright © Huawei Technologies Co., Ltd.

```
LLADDR=fa:16:3e:01:c3:2e NM_CONTROLLED=no
BOOTPROTO=dhcp
DEVICE=bond0.2835 USERCONTRL=auto
TYPE=Ethernet VLAN_ID=2835
```

Where,

- **LLADDR**: indicates the MAC address of the NIC to be added. For its value, see step **1.a**.
- **DEVICE**: Set it to **bond0.***vlan*. *vlan* is the value obtained from step **1.a**, such as **2835**.
- **VLAN_ID**: indicates the VLAN ID, such as **2835**.

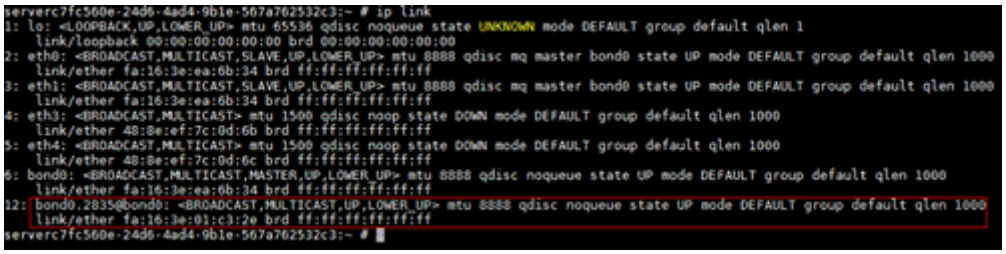
  After the modification, press **Esc** and enter **:wq** to save the change and exit.

5. Run the following command to start the added NIC:

   /usr/sbin/wicked ifup bond0.*vlan*

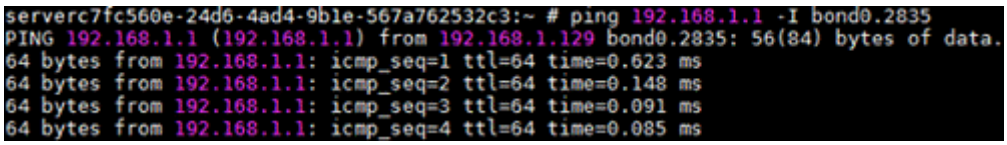
   For example, to start bond0.2835, run the command shown in the following figure.

6. Run the following command to check the status of the NIC device:



7. Ping the gateway from the new network device to check whether the network connectivity is normal.

   Use the gateway address obtained from step **1.a**.



Configuring a NIC Deleted from a BMS

1. Obtain the VLAN and MAC address of the NIC to be deleted.
2. Use a key or password to log in to the BMS as user **root**.
3. Locate the network device based on the VLAN information and run the **/usr/sbin/wicked ifdown band0.***vlan* command to delete the device.

```
serverc7fc560e-24d6-4ad4-9b1e-567a762532c3:~ # ip link | grep 2835 12: bond0.2835@bond0:
<BROADCAST,MULTICAST,UP,LOWER_UP> mtu 8888 qdisc noqueue state UP mode DEFAULT group
default qlen 1000 serverc7fc560e-24d6-4ad4-9b1e-567a762532c3:~ #
serverc7fc560e-24d6-4ad4-9b1e-567a762532c3:~ # /usr/sbin/wicked ifdown bond0.2835
serverc7fc560e-24d6-4ad4-9b1e-567a762532c3:~ #
```

4. Run the following command to delete network configuration file **/etc/sysconfig/network/ifcfg-bond0.***vlan* (replace *vlan* with the VLAN obtained from step **1**, such as **2835**):

rm /etc/sysconfig/network/ifcfg-bond0.*2835*

4.4 Obtaining the Password for Logging In to a Windows ECS

Scenarios

Password authentication mode is required to log in to a Windows ECS. Therefore, you must use the key file used when you created the ECS to obtain the administrator password generated when the ECS was initially installed. The administrator user is **Administrator** or the user configured using Cloudbase-Init. This password is randomly generated, offering high security.

You can obtain the initial password for logging in to a Windows ECS using either the management console or API. For details, see this section.

Obtaining the Password Using the Management Console

1. Obtain the private key file (.pem file) used when you created the ECS.
2. Log in to the management console.
3. Under **Computing**, click **Elastic Cloud Server**.
4. In the ECS list, select the ECS whose password you want to get.
5. In the **Operation** column, click **More** and choose **Get Password**.
6. Use either of the following methods to obtain the password through the key file:
   - Click **Select File** and upload the key file from a local directory.
   - Copy the key file content to the text field.
7. Click **Get Password** to obtain a random password.

Obtaining the Password Using APIs

1. Obtain the private key file (.pem file) used when you created the ECS.
2. Set up the API calling environment.
3. For details, see section "API Calling" in the *Elastic Cloud Server API Reference*.
4. Obtain the ciphertext password.

   Call the password obtaining APIs to obtain the ciphertext password of the public key encrypted using RSA. The API URI is in the format "GET /v2/{*tenant_id*}/servers/{*server_id*}/os-server-password".

   NOTE

   For instructions about how to call an API, see section "Retrieving the Password for Logging In to a Windows ECS (Native OpenStack API)" in *Elastic Cloud Server API Reference*.
5. Decrypt the ciphertext password.

   Use the private key file used when you created the ECS to decrypt the ciphertext password obtained in step **4**.

 Copyright © Huawei Technologies Co., Ltd.

a. Run the following command to convert the ciphertext password format to ".key -nocrypt" using OpenSSL:

   openssl pkcs8 -topk8 -inform PEM -outform DER -in rsa_pem.key -out pkcs8_der.key -nocrypt

b. Invoke the Java class library **org.bouncycastle.jce.provider.BouncyCastleProvider** and use the private key file to edit the code decryption ciphertext.

 Copyright © Huawei Technologies Co., Ltd.

A Change History

What's New	Released On
This issue is the seventh official release, which incorporates the following change: Updated the description about using an SFS Turbo file system as shared storage.	2019-09-30
This issue is the sixth official release, which incorporates the following change: Added ECS flavors.	2018-11-16
This issue is the fifth official release, which incorporates the following change: Updated the network planning information.	2018-08-20
This issue is the fourth official release, which incorporates the following change: Added the scheme that iSCSI disks can function as SBD volumes for storage in the HA deployment scenario where KunLun servers are used.	2018-06-15
This issue is the third official release, which incorporates the following changes: • Added the description of cross-AZ DR. • Added the description that DESS disks can be created and attached on the public cloud management console.	2018-03-30
This issue is the second official release, which incorporates the following change: Added the deployment of the production system.	2018-02-01
This issue is the first official release.	2018-01-08

 Copyright © Huawei Technologies Co., Ltd.