

SAP S/4HANA

HA Deployment Guide

Issue 01
Date 2019-06-30



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. 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 Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property 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 Cloud 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

1 Overview	1
2 Deployment Scheme	3
3 Resource Planning	8
3.1 Node Planning	8
3.2 Network Plane Planning	11
3.3 Security Group Planning	13
4 Resource Preparation	17
4.1 Software and Tools	17
4.2 Creating a Subnet and Configuring a Security Group	19
4.3 Creating an SFS Turbo File System	20
4.4 Creating an SAP S/4HANA Instance	22
5 Configuration Before Installation	26
5.1 Configuring SSH Switching Permissions	26
5.2 Modifying OS Configurations	27
5.3 Binding to a Shared Disk and Floating IP Address	28
5.4 Formatting a Disk	29
5.5 Attaching an SFS Turbo File System to an ECS	30
6 SAP S/4HANA Installation	32
6.1 Installing the SAP S/4HANA Software	32
6.2 Installing SAP GUI	32
6.3 Configuring the HA Function of SAP S/4HANA	33
6.4 Configuring iSCSI (Cross-AZ HA Deployment)	37
7 Backup and Restoration	41
8 FAQs	42
8.1 What Should I Do If a SAP Application on an ECS Cannot Be Started?	42
A Change History	44

1 Overview

The document conventions are as follows:

- This document provides instructions to prepare resources (such as ECSs and network resources) on the public cloud platform, and install SAP S/4HANA in high availability (HA) mode. SAP S/4HANA is authorized in Bring Your Own License (BYOL) mode. In this mode, you must log in at [SAP Support Portal Home](#) and apply for a license.
- This document cannot replace the standard SAP document. If you have any trouble in installing and using SAP S/4HANA due to its own problems, contact the SAP technical support.
- This document is written based on the SUSE Linux OS. The deployment modes mentioned in the document are only for reference. Install SAP S/4HANA by referring to the standard SAP installation manual or based on sizing results and site requirements.
- You have installed the SAP HANA database and the SAP HANA database is used as the background database to install SAP S/4HANA. For details about how to install SAP HANA, see the [SAP HANA User Guide \(Single Node\)](#).
- For details about the official SAP installation guide and related notes, see the following documents:
 - [SAP Installation Guides](#)
 - [SAP Notes](#)
 - [SAP Library](#)

Version Mapping

The following table lists the mappings between application versions and operating systems.

Table 1-1 Version mappings

Application Version	SLES 12 SP1	SLES 12 SP2	SLES 12 SP3	SLES 15
S/4HANA 1610	Supported	Supported	Supported	Supported
S/4HANA 1709	Supported	Supported	Supported	Supported

Application Version	SLES 12 SP1	SLES 12 SP2	SLES 12 SP3	SLES 15
S/4HANA 1809	Not supported	Supported	Supported	Supported

The following table describes the mappings between versions of the OSs and Resource Agents as well as the OSs and SAP Connector.

Table 1-2 Version mappings

OS Version	Resource Agents Version	SAP Connector Version
SLES 12 SP1	SUSE-SLE-HA-12-SP1-2017-885	3.1.0
SLES 12 SP2	SUSE-SLE-HA-12-SP2-2018-1923	3.1.0
SLES 12 SP3	SUSE-SLE-HA-12-SP3-2018-1922	3.1.0
SLES 15	SUSE-SLE-Product-HA-15-2018-1855	3.1.0

Required Cloud Services

Table 1-3 lists the required cloud services for deploying SAP S/4HANA in HA mode.

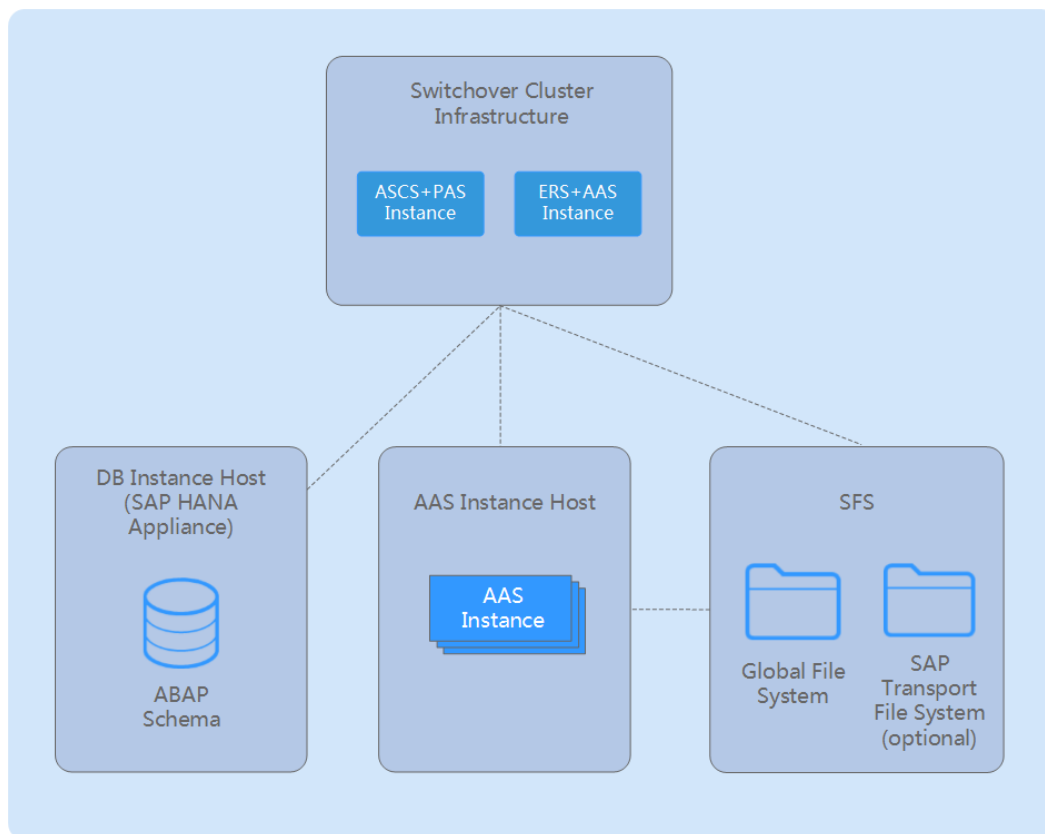
Table 1-3 Required cloud services

Cloud Service Name	Description
Elastic Cloud Server (ECS)	SAP S/4HANA is deployed on ECSs.
Elastic Volume Service (EVS)	All the SAP S/4HANA ECSs have EVS disks attached.
Virtual Private Cloud (VPC)	All SAP S/4HANA ECSs belong to the same VPC. They are isolated using subnets and security groups in the VPC for network security.
Image Management Service (IMS)	When creating an SAP S/4HANA ECS, select a proper public image, for example, SUSE Linux Enterprise Server (SLES) 12 SP1 for SAP .
Volume Backup Service (VBS)	VBS backs up EVS disks and uses the backups to restore original EVS disks, ensuring user data accuracy and security.
Scalable File Service (SFS)	SFS provides high-performance file storage that is scalable on demand. It can be accessed by multiple ECSs.

2 Deployment Scheme

Figure 2-1 shows the processes of deploying SAP S/4HANA in HA mode.

Figure 2-1 SAP S/4HANA HA deployment flowchart



In this deployment mode, the SAP S/4HANA system consists of multiple SAP instances. An SAP instance is a group of processes that are simultaneously started or stopped. In the SAP S/4HANA system, each SAP instance is deployed on an ECS. The SAP instances include:

- ASCS instance
- Enqueue Replication Server instance (ERS instance)

- Database instance (DB instance)
- Primary Application Server instance (PAS instance)
- Additional Application Server instance (AAS instance)

Table 2-1 describes the feature of each SAP S/4HANA component.

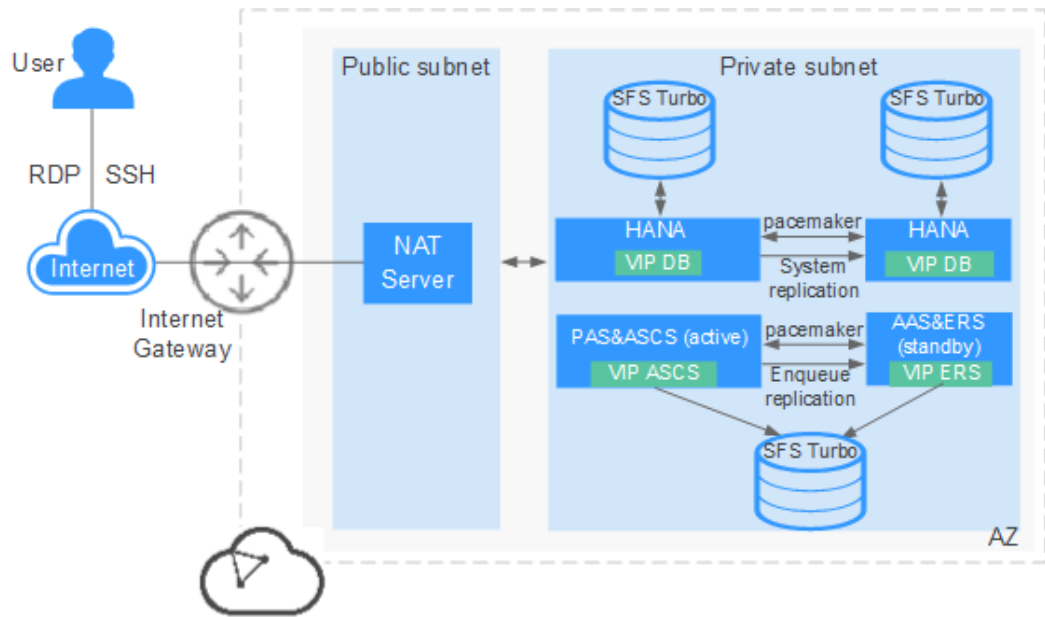
Table 2-1 Features of SAP S/4HANA components

SAP S/4HANA Component	Reliability Assurance
<ul style="list-style-type: none"> • ASCS instance (including the Message server and Enqueue server) • Database instance 	The cloud platform capabilities protect instances from an SPOF. For example, the active and standby ASCS node switchover is configured to ensure HA.
<ul style="list-style-type: none"> • Central instance and Dialog instance include: <ul style="list-style-type: none"> - ABAP Dialog and Batch work process - Update work process - Gateway work process - Spool work process - J2EE cluster nodes 	With the HA of SAP S/4HANA, install Dialog instance in distributed mode to ensure HA.

Customers can install SAP S/4HANA as required and formulate deployment modes based on its component features to ensure HA. To avoid SPOF and ensure HA, the ASCS instance (including the Message server and Enqueue server) requires the cloud platform and the database is configured with the active and standby switchover. Central instance and Dialog instance (including the ABAP Dialog and Batch work process) can be installed on multiple ECSs to ensure HA.

Figure 2-2 shows the recommended HA deployment mode on the public cloud.

Figure 2-2 Recommended SAP S/4HANA HA deployment mode



The preceding describes an example of the SAP S/4HANA HA deployment mode. You can install SAP S/4HANA as required.

- ASCS instance (including the Message server and Enqueue server) is a system that may have an SPOF. With the help of the cloud platform, ASCS instance is protected from an SPOF. Two ASCS ECSs need to be created and attached with a shared disk. The ASCS and PAS instances are installed on the active ECS, and the ERS and AAS instances are installed on the standby ECS. The time synchronization and disk formatting must be performed on the two ECSs.
- For details about how to deploy SAP HANA in active/standby mode, see the [Single-Node Scenario Where HA Is Required](#).
- The security group and elastic NICs are used to protect SAP S/4HANA Central instance, ASCS instance, and DB instance to avoid communication errors and isolate failed resources.
- [Table 2-2](#) and [Table 2-3](#) show the file system planning for the active and standby ASCS nodes.

Table 2-2 File system planning for the active ASCS node

Mount Point	File System Type	Description
/usr/sap/<SID>/ ASCS<##>	xfs NOTE In the cross-AZ or cross-region scenario, this file system type is sfs.	Shared disk, which is used to install the ASCS instance. For details, see section Node Planning . In the cross-AZ/Region scenario, SFS Turbo provides shared disks.

Mount Point	File System Type	Description
/sapmnt	sfs	SFS Turbo file system, which provides the shared storage. For details, see section Node Planning .
/usr/sap/<SID>/SYS	sfs	SFS Turbo file system, which provides the shared storage. For details, see section Node Planning .
/sapcd	sfs	SFS Turbo file system, which provides the shared storage. The SAP S/4HANA installation package is uploaded to this directory.

Table 2-3 File system planning for the standby ASCS node

Mount Point	File System Type	Description
/usr/sap/<SID>/ERS<##>	xfs NOTE In the cross-AZ or cross-region scenario, this file system type is sfs.	Shared disk, which is used to install the ERS instance. For details, see section Node Planning . In the cross-AZ/Region scenario, SFS Turbo provides shared disks.
/sapmnt	sfs	SFS Turbo file system, which provides the shared storage. For details, see section Node Planning .
/usr/sap/<SID>/SYS	sfs	SFS Turbo file system, which provides the shared storage. For details, see section Node Planning .

Mount Point	File System Type	Description
/sapcd	sfs	SFS Turbo file system, which provides the shared storage. The SAP S/4HANA installation package is uploaded to this directory.

3 Resource Planning

3.1 Node Planning

Before applying for SAP S/4HANA ECSs, 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 S/4HANA, see SAP note: [1953429](#) and [SAP Installation Guides](#).

SAP S/4HANA Node Planning

Follow the descriptions in [Table 3-1](#) to conduct SAP S/4HANA node planning. HUAWEI CLOUD provides SAP-certified ECSs with various specifications. Configure the actual hardware usage based on the SAP Sizing result.

Table 3-1 Recommended SAP S/4HANA node planning

Item	Specification
OS	<ul style="list-style-type: none">• SUSE Linux Enterprise Server for SAP Applications 12 SP3• SUSE Linux Enterprise Server for SAP Applications 12 SP4• SUSE Linux Enterprise Server for SAP Applications 12 SP5• SUSE Linux Enterprise Server for SAP Applications 15• SUSE Linux Enterprise Server for SAP Applications 15 SP1
Specification	m6.2xlarge.8 (8 vCPUs and 64 GB memory)

Item	Specification
Disk	<ul style="list-style-type: none"> System disk: ultra-high I/O, 100 GB Following the descriptions in Table 3-3 to plan the data disk created on the ASCS node. After a data disk is created, bind it to the ERS node. Only one system disk needs to be created for the ERS node. <p>NOTE In the cross-AZ HA scenario, you do not need to create the data disk. EVS disks cannot be shared across AZs. For details about how to create and configure a shared disk in a cross-AZ HA scenario, see Configuring iSCSI (Cross-AZ HA Deployment).</p>

[Table 3-2](#) describes the specifications of SAP-certified ECSs.

Table 3-2 Recommended ECS specifications

ECS Type	Flavor	vCPUs	Memory (GB)
Memory-optimized	m6.large.8	2	16
	m6.xlarge.8	4	32
	m6.2xlarge.8	8	64
	m6.4xlarge.8	16	128
	m6.8xlarge.8	32	256
General computing-plus	c6.large.4	2	8
	c6.xlarge.4	4	16
	c6.2xlarge.4	8	32
	c6.3xlarge.4	12	48
	c6.4xlarge.4	16	64
	c6.6xlarge.4	24	96
	c6.8xlarge.4	32	128

File System Planning

[Table 3-3](#), [Table 3-4](#), and [Table 3-5](#) describe the file system planning.

Table 3-3 File system planning

Parti tion	Capac ity (GB)	Mounted To	Description
sda	10	N/A	Used as the SBD disk.
sdb	80	/usr/sap/<SID>/ASCS<##>	Partition of the active node, which is used to install the ASCS instance.
sdc	80	/usr/sap/<SID>/ERS<##>	Partition of the standby node, which is used to install the ERS instance.

 **NOTE**

In the cross-AZ HA scenario, three ECSs are required and Internet Small Computer System Interface (iSCSI) is used to create a shared disk for Split Brain Detection (SBD). For details, see [Configuring iSCSI \(Cross-AZ HA Deployment\)](#). The disks used to install the ASCS instance and the ERS instance are provided by the SFS Turbo file system. [Table 3-5](#) describes the planning of the SFS Turbo file system in the cross-AZ HA scenario.

Table 3-4 Planning of the SFS Turbo file system

Name	Total Capac ity (GB)	Mounted To	Description
sapmnt	100GB	/sapmnt	Shared to all nodes in the SAP S/4HANA system
usrsapsy s	10	/usr/sap/ <SID>/SYS	Shared to all nodes in the SAP S/4HANA system
sapmedi a	100	/sapcd	Shared to all nodes in the SAP S/4HANA system

Table 3-5 Planning of the SFS Turbo file system in the cross-AZ HA scenario

Name	Total Capac ity (GB)	Mounted To	Description
sapmnt	100GB	/sapmnt	Shared to all nodes in the SAP S/4HANA system
usrsapsy s	10	/usr/sap/ <SID>/SYS	Shared to all nodes in the SAP S/4HANA system

Name	Total Capacity (GB)	Mounted To	Description
sapmedia	100	/sapcd	Shared to all nodes in the SAP S/4HANA system
ASCS	80GB	/usr/sap/<SID>/ASCS<##>	Shared to the active node, which is used to install the ASCS instance.
ERS	80GB	/usr/sap/<SID>/ERS<##>	Shared to the standby node, which is used to install the ERS instance.

3.2 Network Plane Planning

The network information needs to be planned based on application scenarios and SAP S/4HANA planning. The network segments and IP addresses are for reference only. You can configure it based on site requirements.

In HA scenario, the ASCS node uses two NICs for the server/client network communication plane and internal communication plane, respectively.

NOTE

The IP addresses of the server/client plane and internal heartbeat communication plane must belong to different subnets.

Figure 3-1 shows the network planning in HA scenario.

Figure 3-1 Network planning in HA scenario

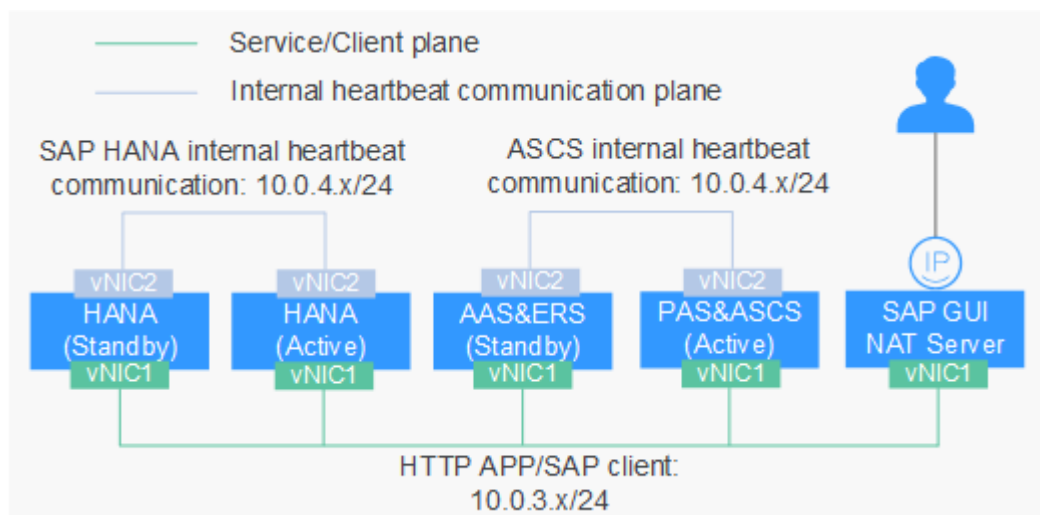


Table 3-6 Network planning

Parameter	Description	Example Value
IP address of the server/client plane	Specifies the IP address of the primary NIC plane. The ASCS and ERS nodes communicate with NAT Server and SAP HANA using this IP address.	PAS & ASCS node: 10.0.3.12 AAS & ERS node: 10.0.3.13 NAT Server: 10.0.3.4 Active SAP HANA node: 10.0.3.5 Standby SAP HANA node: 10.0.3.6
IP address of the internal heartbeat communication plane	The ASCS and ERS nodes use this network plane to communicate with each other. The active and standby SAP HANA databases use this network plane to communicate with each other.	PAS & ASCS node: 10.0.4.2 AAS & ERS node: 10.0.4.3 Active SAP HANA node: 10.0.4.6 Standby SAP HANA node: 10.0.4.7

VPC and Subnet Planning

The VPC and subnet planning is the same as that for SAP HANA. For details, see [Single-Node Scenario Where HA Is Required](#).

Host Planning

SAP application system ID (SID): PRD

SAP HANA SID: HAP

Table 3-7 describes the SAP host planning.

Table 3-7 SAP host planning

Host Name	IP Address	Active Heart beat	Virtual IP Address	Type	Instance number	SID
hana01	10.0.3.5	10.0.4.6	10.0.3.7	DB Server 01	00	HAP
hana02	10.0.3.6	10.0.4.7		DB Server 02		

Host Name	IP Address	Active Heart beat	Virtual IP Address	Type	Instance number	SID
S/4HANA-0001	10.0.3.12	10.0.4.2	10.0.3.14	ASCS Instance/PAS Instance	01	PRD
S/4HANA-0002	10.0.3.13	10.0.4.3		ERS Instance/AAS Instance	02	

3.3 Security Group Planning

The security group planning needs to meet the requirements for communication between SAP nodes, management plane, and internal communication plane. You need to configure the security group together with the network department. For details about SAP's requirements for security group rules, see [TCP/IP ports used by SAP Applications](#).

You can configure the security group by referring to [Table 3-8](#), [Table 3-9](#), and [Table 3-10](#).

 **NOTE**

The network segments and IP addresses are for reference only. The following security group rules are recommended best practices. You can configure your own security group rules as you need.

In the following table, ## stands for the SAP S/4HANA instance ID. Ensure that this ID is the same as that specified when you installed the SAP S/4HANA software.

Table 3-8 Security group rules (SAP Application Server nodes)

Source	Protocol	Port range	Description
Inbound			
10.0.3.0/24	TCP	32##	Allows SAP GUI to access SAP S/4HANA.
10.0.3.0/24	TCP	5##13 to 5##14	Allows ASCS to access SAP application server.
10.0.3.0/24	TCP	33## and 48##	The ports are used by CPIC and RFC.

Source	Protocol	Port range	Description
10.0.3.0/24	TCP	22	Allows SAP S/4HANA to be accessed using SSH.
10.0.3.0/24	UDP	123	Allows other servers to synchronize time with SAP S/4HANA.
Determined by the public cloud	ANY	ANY	The security group rule is created by the system by default. Allows ECSs in the same security group to communicate with each other.
Outbound			
0.0.0.0/0	ANY	ANY	The security group rule is created by the system by default. Allows SAP S/4HANA to access all peers.

Table 3-9 Security group rules (SAP ASCS nodes)

Source	Protocol	Port range	Description
Inbound			
10.0.3.0/24	TCP	36##	Message Port with profile parameter rdisp/msserv
10.0.3.0/24	TCP	5##13 to 5##14	Allows ASCS to access SAP Application Server.
10.0.3.0/24	TCP	33## and 38##	The ports are used by CPIC and RFC.

Source	Protocol	Port range	Description
10.0.3.0/24	TCP	22	Allows SAP S/4HANA to be accessed using SSH.
10.0.3.0/24	UDP	123	Allows other servers to synchronize time with SAP S/4HANA.
Determined by the public cloud	ANY	ANY	The security group rule is created by the system by default. Allows ECSs in the same security group to communicate with each other.
Outbound			
0.0.0.0/0	ANY	ANY	The security group rule is created by the system by default. Allows SAP S/4HANA to access all peers.

Table 3-10 Security group rules (NAT Server nodes)

Source	Protocol	Port range	Description
Inbound			
0.0.0.0/0	TCP	22	Allows users to access the NAT server using SSH.
Determined by the public cloud	ANY	ANY	The security group rule is created by the system by default. Allows ECSs in the same security group to communicate with each other.

Source	Protocol	Port range	Description
Outbound			
0.0.0.0/0	ANY	ANY	The security group rule is created by the system by default. Allows the NAT server to access all peers.

4 Resource Preparation

4.1 Software and Tools

Table 1 Required software and tools lists the required software and tools.

Table 4-1 Required software and tools

Item	Description	How to Obtain
Local computer	Runs a Windows OS which is Windows 7 or later.	-
WinSCP	Uploads key files to ECSs.	https://www.winscp.net
PuTTY and PuTTYgen	Used for logging in to an ECS and running commands.	https://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
OBS Browser+	Used for uploading the SAP S/4HANA and SAP HANA installation packages to the public ECS. You can run the wget command to download the uploaded files to the nodes where SAP S/4HANA is to be installed. For details, see Installing the SAP S/4HANA Software .	Downloading OBS Browser+

Item	Description	How to Obtain
VNC Viewer for Windows	Used for providing the GUI on the local computer for installing SAP S/4HANA	https://www.realvnc.com/download/viewer/
SAPCAR	Compression and decompression software used by SAP. The patch packages and small software downloaded from the SAP website in .car or .sar format can be decompressed using SAPCAR.	Log in to the SAP official website to download the installation media: https://support.sap.com/en/my-support/software-downloads.html
SAP GUI 7.4	SAP system application client SAP GUI 7.4 or higher version is recommended.	
SWPM	Used for upgrading, migrating, and installing SAP systems The latest version released by SAP is recommended.	
SAP S/4HANA installation package NOTE Install the required SAP S/4HANA version based on version mapping.	The SAP S/4HANA installation package mainly includes Kernel, export, and HDB files. For details about the Kernel version, see SAP note: 1680045 and Product Availability Matrix (PAM) by visiting https://support.sap.com/pam .	
sap-suse-cluster-connector	SUSE HAE software	Visit the SUSE official website https://www.suse.com/ to download and install it.


4.2 Creating a Subnet and Configuring a Security Group

Scenarios

To ensure proper communication between all SAP S/4HANA ECSs, create subnet for the ECSs and configure a proper security group.

Procedure

Step 1 Create a subnet.

1. Log in to the public cloud management console.
2. In the navigation pane on the left, click  and choose **Virtual Private Cloud** under **Network**.
3. Choose **Subnets** in the left navigation pane.
4. In the upper right corner of the displayed page, click **Create Subnet**.
5. In the **Create Subnet** pane, configure parameters as prompted.
 - **VPC**: Select the VPC where SAP HANA is located.
 - **AZ**: specifies the AZ of the subnet.
 - **Name**: Configure the subnet name that is easy to identify, for example, **service_subnet**.
 - **CIDR Block**: Configure the subnet segment based on [Network Plane Planning](#) and [Security Group Planning](#).
 - **Advanced Settings**: Use the default settings.
6. Click **OK** to complete the subnet configuration.
7. Repeat [Step 1.1](#) to [Step 1.6](#) to create all required subnets according to the requirements specified in sections [Network Plane Planning](#) and [Security Group Planning](#).

Step 2 Set security groups.

SAP S/4HANA, NAT Server, and SAP HANA require security groups.

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. In the displayed dialog box, add the rule based on the requirements specified in section **Security Group Planning**.
The default security group rules cannot be deleted.
 - 8. Repeat **Step 2.5** to **Step 2.7** to configure all security groups.
- End

4.3 Creating an SFS Turbo File System

Scenarios

In the HA deployment scenario, create an SFS Turbo file system to provide the file sharing capability. Create an SFS Turbo file system on the public cloud platform based on **Table 4-2**.

Creating an SFS Turbo File System



- 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**. The **Create File System** page is displayed.
- Step 5** Configure the parameters listed in **Table 4-2**.

Table 4-2 Parameters

Parameter	Description	Example Value
File System Type	File system type. Select SFS Turbo .	SFS Turbo

Parameter	Description	Example Value
Billing Mode	Select a mode based on the site requirements.	Yearly/Monthly
Region	Select the target region.	CN-Hong Kong
AZ	Specifies the AZ where the file system is located. Select an AZ as required.	AZ1
Protocol Type	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
VPC	Select the VPC and subnet used by the ECS. For details, see Creating a Subnet and Configuring a Security Group .	N/A
Security Group	Select the security group where the ECSs belong. For details, see Creating a Subnet and Configuring a Security Group .	N/A
Enterprise Project	Select the project you need.	SAP
Cloud Backup and Recovery	To use this service, you need to buy server backup vault that is used for storing the backup of disks. Set this parameter as required.	Not required
Name	Specifies the file system name.	sfs-turbo-backup
Required Duration	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 On the displayed **SFS** 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 the 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

4.4 Creating an SAP S/4HANA Instance

Scenarios

SAP S/4HANA runs on ECSs. Create one or more ECSs based on the deployment mode.

Determine the number of ECSs and related planning information based on sections "Solution Introduction" and "Data Planning".

Procedure


- Step 1** On the public cloud management console, click  in the upper left corner and choose **Computing > Elastic Cloud Server** to switch to the **Elastic Cloud Server** page.
- Step 2** Click **Buy ECS** in the upper right corner. A page for creating ECSs is displayed.
- Step 3** Configure basic information about the SAP S/4HANA ECS as prompted. [Table 4-3](#) describes the parameters.

Table 4-3 SAP S/4HANA ECS basic configuration

Parameter	Description
Billing Mode	Select a billing mode based on the site requirements. The recommended billing mode is Yearly/Monthly .
AZ	Specifies the AZ where the ECS is located.
CPU Architecture	Select x86 .
Specifications	Set the type of SAP S/4HANA ECSs to High-performance computing . Set the ECS specifications based on Node Planning or site requirements.
Image	Select Public image and SUSE Linux Enterprise Server (SLES) 12 SP1 for SAP or configure them based on site requirements.
System Disk	Plan the system disk and data disk by referring to section Node Planning .

- Step 4** Click **Next: Configure Network**.
- Step 5** Configure network information for the SAP S/4HANA ECS as prompted. [Table 4-4](#) describes the parameters.

Table 4-4 SAP S/4HANA ECS network configuration

Parameter	Description
Network	Choose the VPC and subnet in specified in Creating a Subnet and Configuring a Security Group .
Extension NIC	Create an NIC by referring to section Network Plane Planning .
Security Group	Use the security group in section Creating a Subnet and Configuring a Security Group .
EIP	If you select Not required , the SAP S/4HANA ECS on the private subnet can be accessed through the NAT server.

Step 6 Click **Next: Configure Advanced Settings**.

Step 7 Configure advanced settings about the SAP S/4HANA ECS as prompted. [Table 4-5](#) describes the parameters.

Table 4-5 SAP S/4HANA ECS advanced settings

Parameter	Description
ECS Name	When you create ECSs in batches, the number in the ECS Name is generated automatically in ascending order based on the Quantity value that you filled in. For example, if you fill SAP-Dev in ECS Name , the first ECS is SAP-Dev-0001 , and the second ECS is SAP-Dev-0002 .
Login Mode	Select Key pair .
Key Pair	<p>Key Pair is recommended. A Secure Shell (SSH) key certificate is used for authenticating users who attempt to log in to SAP S/4HANA ECSs. Ensure that the ECSs where SAP S/4HANA and NAT server are to be deployed use the same key. Otherwise, SAP S/4HANA installation will fail.</p> <ul style="list-style-type: none"> • 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 ECS. • Click Create Key Pair. On the Key Pair page that is displayed, 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 query and save the private key as prompted.

Parameter	Description
Cloud Backup and Recovery	<p>Cloud Backup and Recovery (CBR) provides backup protection for EVS disks and ECSs, and uses backups to restore the EVS disks and ECSs. After you set Cloud Backup and Recovery, the system binds the target ECS to the cloud backup vault and associates the ECS with the selected backup policy to periodically back up the ECS.</p> <p>The following options are provided:</p> <ul style="list-style-type: none"> • Auto assign <ol style="list-style-type: none"> 1. Set the name of the cloud backup vault, which is a character string consisting of 1 to 64 characters, including letters, digits, underscores (_), and hyphens (-). For example, vault-f61e. The default naming rule is vault_XXXX. 2. Enter the vault capacity, which is required for backing up the ECS. The vault capacity cannot be smaller than that of the ECS to be backed up. Its value ranges from the total capacity of the ECS to 10,485,760 in the unit of GB. 3. Select a backup policy from the drop-down list, or log in to the CBR console and configure a desired one. • Use existing <ol style="list-style-type: none"> 1. Select an existing cloud backup vault from the drop-down list. 2. Select a backup policy from the drop-down list, or log in to the CBR console and configure a desired one. • Not required: This function is not required. If you require this function after purchasing the ECS, log in to the CBR console and bind the desired cloud backup vault to your ECS.
ECS Group	<p>This parameter is displayed only after you click Configure now behind Advanced Options.</p> <p>Specify an SAP S/4HANA ECS group. When you create ECSs, the system will allocate the ECSs in the same server group to different physical servers to ensure the running reliability of these ECSs.</p> <p>Determine the policy of an SAP S/4HANA ECS group based on the deployment mode:</p> <ul style="list-style-type: none"> • Standardized deployment: You do not need to specify an ECS group. • HA deployment: All SAP S/4HANA ECSs must belong to the same ECS group. <p>NOTE Perform the following operations to create an ECS group: Click Create ECS Group. On the displayed page, click Create ECS Group, specify the ECS group name, and click OK.</p>
Advanced Options	Select Configure now .

Parameter	Description
Agency	<p>After the agency is specified, the delegated domain can obtain the credentials from the agency to temporarily access the public cloud.</p> <p>You need to specify the DataproviderAccess agency for the SAP S/4HANA ECS to interconnect with Data Provider.</p> <p>Log in to the management console as the tenant administrator and create the agency. For details, see Data Provider for SAP User Guide.</p>

Step 8 Click **Next: Confirm**.

Step 9 Confirm the information about SAP S/4HANA ECSs as prompted.

Table 4-6 SAP S/4HANA ECS information

Parameter	Description
Enterprise Project	Select the name of a created enterprise project, for example, SAP.
Required Duration	Set the duration based on your requirements.
Quantity	Set this parameter as required.
Agreement	Select I have read and agree to Huawei Image Disclaimer .

Step 10 Click **Next** and complete the payment as prompted.

Step 11 The system returns to the **Elastic Cloud Server** page. Check the status of the created task in **Task Status** on the right of the page.

Step 12 After the SAP S/4HANA ECS is created, you can view the ECS from the ECS list on the right of the page.

Step 13 Create other SAP S/4HANA ECSs as required.

Step 14 Change the **root** password for logging in to all SAP S/4HANA ECSs.

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

1. Use the key to log in to the SAP S/4HANA ECSs.
2. Run the following command to change the password for user **root**:

```
passwd
```

Enter the password as prompted for confirmation.

----End

5 Configuration Before Installation

5.1 Configuring SSH Switching Permissions

Scenarios

To allow SSH switchovers between SAP S/4HANA ECSs and NAT servers, you must configure the ECSs and servers to be trusty.

Procedure

Step 1 Upload the key file to the NAT server.

1. On the local computer, generate the key file for logging in to the NAT server. When creating the NAT server, you specify the certificate key file (.pem file) for the NAT server.

The .pem file generates the .ppk file using PuTTYgen.

2. On the local computer, install the WinSCP software.
3. Upload the certificate private key file (.pem file) to the NAT server. Use WinSCP to upload the certificate private key file (.pem file) to the **/usr** directory on the NAT server using an elastic IP address. Ensure that user **root** and the key file (.ppk file) are used for authentication.
4. Use PuTTY to log in to the NAT server. Ensure that user **root** and the key file (.ppk file) are used for authentication.
5. Copy the certificate private key file (.pem 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 command 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 locally stored private key file and **authorized_keys** file to all SAP S/4HANA ECSs.

The command is 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/
```

For example, if the peer IP address is **10.0.3.52**, run the following commands:

```
scp /root/.ssh/id_rsa 10.0.3.52:/root/.ssh/id_rsa  
scp /root/.ssh/authorized_keys 10.0.3.52:/root/.ssh/
```

Step 3 Verify the switching.

Use SSH to switch from the NAT server to all SAP S/4HANA ECSs for verification.

The following command is used to switch to the active ASCS node. For example, the IP address of the server/client plane of the active ASCS node is 10.0.3.52.

```
ssh 10.0.3.52
```

 **NOTE**

After the switching, you must switch back to the NAT server. Then, verify the switching from the NAT server to other nodes.

During the first switching, the system displays the fingerprint as well as the message "Are you sure you want to continue connecting (yes/no)?" In such a case, enter **yes** and continue the switching.

----End

5.2 Modifying OS Configurations

Scenarios

To ensure the proper installation of the SAP S/4HANA system, disable the OS firewalls of all nodes before the installation.

Procedure

Step 1 Log in to the NAT server as user **root** using the key file. Then, use SSH to switch to the ASCS node.

Step 2 Disable the automatic startup of the firewall, and disable the firewall.

- If the OS is SUSE Linux Enterprise Server 12, run the following commands to disable automatic firewall startup 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
```

- If the OS is SUSE Linux Enterprise Server 15, run the following commands to disable automatic firewall startup and disable the firewall:

```
systemctl stop firewalld
systemctl disable firewalld
```

Step 3 Repeat step [Step 1](#) and [Step 2](#) to disable the firewalls of all SAP S/4HANA nodes.

----End

5.3 Binding to a Shared Disk and Floating IP Address

Scenarios

In the 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 disk of the active ASCS node to the standby ASCS node and bind the floating IP address to the active and standby ASCS nodes.

Prerequisites

The SSH switching between the active and standby SAP ASCS nodes has been allowed.

Procedure

Binding to a Shared Disk

Step 1

Step 2 Click the name of the active ASCS ECS.

Step 3

Step 4

Step 5

Creating a Floating IP Address and Binding it to the ECS

Step 6 On the ECS list page, click the name of the active ASCS ECS.

Step 7

Step 8

Step 9 After virtual IP addresses are assigned, bind each virtual IP address to both the active and standby ASCS ECSs.

Step 10 Log in to the active ASCS ECS and write the mapping between all IP addresses and hostnames of all SAP S/4HANA ECSs to the `/etc/hosts` file. The following uses the active and standby ASCS nodes as an example.

```
10.0.3.52 S/4HANA-0001
10.0.3.196 S/4HANA-0002
10.0.3.52 ascsha
10.0.3.196 ersha
```

 NOTE

- **ascsha** indicates the virtual hostname of the active ASCS node and **ersha** indicates the virtual hostname of the standby ASCS node. The virtual hostname can be customized.
- You do not need to write the mapping between the virtual IP addresses and virtual hostnames. The virtual IP addresses take effect only after the 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 11 Copy the hosts file to other SAP S/4HANA ECSs.

----End

5.4 Formatting a Disk

Scenarios

The data disks of SAP S/4HANA nodes can be used only after they are formatted and attached to required directories. This section describes how to format the data disk on the active ASCS node within an AZ in the HA deployment. The shared disk of the active ASCS node needs to be formatted based on [Table 3-3](#).

 NOTE

- On the ECS homepage, choose to view the hard disk initialization information.
- In the cross-AZ scenario, create three ECSs and attach a SCSI disk to each ECS. Use Internet Small Computer System Interface (iSCSI) to create a shared disk. In this scenario, disks do not need to be formatted. The SAP S/4HANA deployment scenarios are diversified. You need to format disks based on the actual deployment scenario.

Procedure

Step 1 Use PuTTY to log in to the NAT server with an EIP bound. Ensure that user **root** and the key file (.ppk file) are used for authentication. Then, use SSH to switch to the active ASCS node from the NAT server.

Step 2 Based on [Table 3-3](#), run the following commands to format disks:

```
mkfs.xfs /dev/sdb
```

```
mkfs.xfs /dev/sdc
```

Do not format the partition **sda**.

The formatting takes a period of time. Observe the system running status and do not exit.

Step 3 Attach the disks to the required directory.

Create the **/usr/sap/A01/ASCS00** directory on the active ASCS node and run the following command:

```
mount /dev/sdb /usr/sap/A01/ASCS00
```

Create the **/usr/sap/A01/ERS10** directory on the standby ASCS node and run the following command:


```
mount /dev/sdc /usr/sap/A01/ERS10
```

 NOTE

A01 is the **SID** of SAP S/4HANA, **00** is the **Instance Number** of ASCS, and **10** is the **Instance Number** of ERS.

Step 4 Save the changes and exit.

----End

5.5 Attaching an SFS Turbo File System to an ECS

Scenarios

In the HA deployment scenario, you need to mount the created SFS Turbo file system to an ECS. For details, see [Table 3-4](#).

Prerequisites

- You have created a file system and have obtained the shared path of the file system.
- The IP addresses of the DNS server used to resolve the file system domain name have been configured on the ECS.

Procedure

Step 1 Use PuTTY to log in to the NAT server with an EIP bound. Ensure that user **root** and the key file (.ppk file) are used for authentication. Then, use SSH to switch to the active ASCS node.

Step 2 Run the following command to check whether the NFS software package has been installed:

```
rpm -qalgrep nfs
```

Step 3 If the package has not been installed, run the following command:

```
zypper install nfs-client
```

Step 4 Run the following command to check whether the domain name in the file system shared path can be resolved:

```
nslookup File system domain name
```

Step 5 Run the following command to create a local path for attaching the file system based on [Table 3-4](#):

```
mkdir Local path
```

For example, run the command **mkdir /sapmnt**.

Step 6 Run the following command to attach the file system to the active ASCS node. Repeat this operation to attach three file systems to the active ASCS node.

```
mount -t nfs Shared path Local path
```

Step 7 Run the following command to view the attached file systems:

```
mount -l
```

Step 8 Log in to the standby ASCS node as user **root**. Repeat steps [Step 2](#) to [Step 7](#) to attach the three file systems to the standby ASCS node.

Step 9 Write the disk attaching information to the **/etc/fstab** file so that disks can be automatically attached when the VM is restarted.

```
vi /etc/fstab
```

Step 10 Enter the path information.

Enter the path based on the actual condition.

 **NOTE**

- The **/etc/fstab** format is **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.
- Do not write the attaching information of partitions **sdb** and **sd c** to the **fstab** file because the two partitions will be automatically attached when the HA function of SAP S/4HANA is configured. Otherwise, the VM may fail to be restarted. Write the attaching information of other partitions to the **fstab** file.

An example is provided as follows:

```
Shared path /sapmnt      nfs defaults 0 0
Shared path /usr/sap/A01/SYS  nfs defaults 0 0
Shared path /sapcd       nfs defaults 0 0
```

Save the changes and exit.

----End

6 SAP S/4HANA Installation

6.1 Installing the SAP S/4HANA Software

Before installing SAP S/4HANA, modify the configuration file on the ECS where SAP S/4HANA is to be deployed. For details, see [What Should I Do If a SAP Application on an ECS Cannot Be Started?](#)

Install SAP S/4HANA on ECSs based on information provided in section "2.1 Overview" and SAP installation guides.

To obtain the SAP installation guides and notes, visit the following websites:

- SAP Installation Guides: <https://service.sap.com/instguides>
- SAP Notes: <https://service.sap.com/notes>
- SAP Help Center: <https://help.sap.com/>

6.2 Installing SAP GUI

The SAP GUI is a graphical user interface that allows SAP users to access the SAP system.

Download the SAP GUI software package **51032986_6.rar** from the [SAP Support portal](#).

SAP GUI needs to be installed to allow users to access and manage SAP S/4HANA.

NOTE

SAP GUI can be deployed on a Windows computer or an NAT server.

Follow-up Operations

After installing SAP GUI, configure the SAP GUI, interconnect it with SAP S/4HANA, and then log in to the SAP GUI to process routine services. For details, see the official SAP documentation.

6.3 Configuring the HA Function of SAP S/4HANA

Scenarios

To prevent SAP S/4HANA from being affected by a single point of failure and improve the availability of SAP S/4HANA, configure the HA mechanism for both the active and standby ASCS nodes. If the active and standby nodes are located in the same AZ, you can directly configure the HA function of SAP S/4HANA. If the active and standby node are located in different AZs, another three ECSs are required and iSCSI is used to create a shared disk for SBD before the HA function is configured. For details, see section [Configuring iSCSI \(Cross-AZ HA Deployment\)](#).

Prerequisites

- The mutual trust relationship has been established between the active and standby ASCS nodes.
- You have disabled the firewall of the OS. For details, see section [Modifying OS Configurations](#).
- To ensure that the communication between the active and standby ASCS nodes is normal, add the mapping between the virtual IP addresses and virtual hostnames to the hosts file after installing the SAP S/4HANA instance.

- a. Log in to the active and standby ASCS nodes one by one and modify the `/etc/hosts` file:

vi /etc/hosts

- b. Change the IP addresses corresponding to the virtual hostnames to the virtual IP addresses.

```
10.0.3.52 S/4HANA-0001
10.0.3.196 S/4HANA-0002
10.0.3.220 ascsha
10.0.3.2 ersha
```

NOTE

ascsha indicates the virtual hostname of the active ASCS node and **ersha** indicates the virtual hostname of the standby ASCS node. Virtual hostnames can be customized.

- Check that both the active and standby ASCS nodes have the `/var/log/cluster` directory. If the directory does not exist, create one.
- Update the SAP **resource-agents** package on the active and standby ASCS nodes.
 - a. Run the following command to check whether the **resource-agents** package has been installed:
sudo grep 'parameter name="IS_ERS"' /usr/lib/ocf/resource.d/heartbeat/SAPInstance
 - If the following information is displayed, the patch package has been installed. No further action is required.
 - If the following information is not displayed, install the patch package. Go to **b**.

```
<parameter name="IS_ERS" unique="0" required="0">
```

- b. Install the **resource-agents** package.
If the image is SLES 12 SP1, run the following command:
sudo zypper in -t patch SUSE-SLE-HA-12-SP1-2017-885=1
If the image is SLES 12 SP2, run the following command:
sudo zypper in -t patch SUSE-SLE-HA-12-SP2-2018-1923=1
If the image is SLES 12 SP3, run the following command:
sudo zypper in -t patch SUSE-SLE-HA-12-SP3-2018-1922=1
- Update the **sap_suse_cluster_connector** package on the active and standby ASCS nodes.
 - a. Run the following command to uninstall the old package. Note that the software package name uses underscores (_).
zypper remove sap_suse_cluster_connector
 - b. Run the following command to install the new package. Note that the software package name uses hyphens (-):
zypper install sap-suse-cluster-connector
 - c. Run the following command to obtain the version information about the newly installed **sap-suse-cluster-connector** package:
/usr/bin/sap_suse_cluster_connector gvi --out version
 - d. View the version file to check the version is 3.1.0 or later.

Procedure

Step 1 Log in to the ASCS instance node, obtain the **ha_auto_script.zip** package, and decompress it to any directory.

1. Obtain the **ha_auto_script.zip** package.
2. Run the following commands to decompress the package:

```
cd /sapmnt
unzip ha_auto_script.zip
```

Step 2 Set parameters in the **ascs_ha.cfg** file based on the site requirements. [Table 6-1](#) describes the parameters in the file.

Table 6-1 Parameters in the **ascs_ha.cfg** file

Type	Name	Description
masterNode	masterName	ASCS instance node name
	masterHeartbeatIP1	Heartbeat plane IP address 1 of the ASCS instance node
	masterHeartbeatIP2	Service plane IP address of the ASCS instance node

Type	Name	Description
slaveNode	slaveName	ERS instance node name
	slaveHeartbeatIP1	Heartbeat plane IP address 1 of the ERS instance node
	slaveHeartbeatIP2	Service plane IP address of the ERS instance node
ASCSInstance	ASCSFloatIP	Service IP address of the ASCS instance node
	ASCSInstanceDir	Directory of the ASCS instance
	ASCSDevice	Disk partition used by the ASCS instance directory
	ASCSProfile	Profile file of the ASCS instance
ERSInstance NOTE You need to log in to the ERS instance node to obtain the information about ERSInstanceDir, ERSDevice, and ERSProfile parameters.	ERSFloatIP	Service IP address of the ERS instance node
	ERSInstanceDir	Directory of the ERS instance
	ERSDevice	Disk partition used by the ERS instance directory
	ERSProfile	Profile file of the ERS instance
trunkInfo	SBDDDevice	Disk partition used by the SBD. One or three disk partitions are supported. Every two partitions are separated by a comma (,), for example, /dev/sda, /dev/sdb, /dev/sdc .

Step 3 Run the following command to perform automatic HA deployment:

```
sh ascs_auto_ha.sh
```

Step 4 Run the **crm status** command to check the resource status.

```
clusternode0:~/ascs_hae # crm status
Last updated: Fri Aug 24 11:06:47 2018      Last change: Thu Aug 23 10:28:02 2018 by root via cibadmin on clusternode0
Stack: corosync
Current DC: clusternode0 (version 1.1.13-10.4-6f22ad7) - partition with quorum
2 nodes and 7 resources configured

Online: [ clusternode0 clusternode1 ]

Full list of resources:

stonith-sbd (stonith:external/sbd): Started clusternode0
Resource Group: grp_ASCS
  rsc_ip_ASCS (ocf::heartbeat:IPaddr2): Started clusternode0
  rsc_fs_ASCS (ocf::heartbeat:Filesystem): Started clusternode0
  rsc_sap_ASCS (ocf::heartbeat:SAPInstance): Started clusternode0
Resource Group: grp_ERS
  rsc_ip_ERS (ocf::heartbeat:IPaddr2): Started clusternode1
  rsc_fs_ERS (ocf::heartbeat:Filesystem): Started clusternode1
  rsc_sap_ERS (ocf::heartbeat:SAPInstance): Started clusternode1
```

NOTE

After the HA function is configured, HAE manages resources. Do not start or stop resources in other modes. If you need to manually perform test or modification operations, switch the cluster to the maintenance mode first.

crm configure property maintenance-mode=true

Exit the maintenance mode after the modification is complete.

crm configure property maintenance-mode=false

If you need to stop or restart the node, manually stop the cluster service.

systemctl stop pacemaker

After the ECS is started or restarted, run the following command to start the cluster service:

systemctl start pacemaker

To clear the HA configuration, run the following command on the active node for which the HA mechanism is configured (Roll back to the initial status if the active and standby nodes are switched over.):

sh ascs_auto_ha.sh unconf

----End

Verifying the Configuration

Step 1 Open a browser and ensure that JavaScript and Cookie are enabled.

Step 2 Enter the IP address or host name of the active or standby node as the URL. The login port is 7630.

https://HOSTNAME_OR_IP_ADDRESS:7630/

NOTE

If a certificate warning is displayed when you attempt to access the URL for the first time, it indicates that a self-signed certificate is used. By default, the self-signed certificate is not considered as a trusted certificate.

Click **Continue to this website (not recommended)** or add an exception in the browser to eliminate the warning message.

Step 3 On the login page, enter the username and password of user **hacluster** or any other user who belongs to the hacluster group.

NOTE

The username is **hacluster** and the password is **linux**. Change the password after the first login.

Step 4 Click **Login**. You can view the cluster node and resource status on the displayed page.

----End

6.4 Configuring iSCSI (Cross-AZ HA Deployment)

Scenarios

This operation is required only in the cross-AZ HA scenario.

EVS disks cannot be shared across AZs. Therefore, three ECSs are required in the cross-AZ HA scenario. Each ECS is bound to a SCSI disk and iSCSI configuration is required for SBD. SAP S/4HANA and SAP HANA can be deployed on the same ECS. [Table 6-2](#) lists the ECS specifications.

If SAP S/4HANA is deployed across three AZs, create an ECS in each AZ. If SAP S/4HANA is deployed across two AZs, create an ECS in an AZ and two ECSs in the other AZ. The three ECSs must belong to the same ECS group.

Table 6-2 ECS specifications

OS	SUSE Linux Enterprise Server (SLES) 12 SP1
Specification	s1.medium (1 vCPU and 4 GB memory)
Disk	System disk: high I/O Data disk: High I/O, 10 GB, SCSI, non-shared disk

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
```

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

```
zypper in open-iscsi yast2-iscsi-lilo-server targetcli
```

Step 2 Run the following command to install open-iscsi on the client side (SAP S/4HANA 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 lblock 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 disk. 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:

```
server:~ # targetcli /iscsi create
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 an 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 lblock 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:

```
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 S/4HANA node (client side) and attach the iSCSI disk of a server side ECS to the SAP S/4HANA 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 S/4HANA 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 S/4HANA 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 S/4HANA nodes and repeat [Step 14](#) and [Step 15](#) to configure all SAP S/4HANA nodes of the client side.

----End

7 Backup and Restoration

The SAP S/4HANA backup consists of two parts. One is the backup and restoration of disk snapshots and related file directories in SAP S/4HANA ASCS instance. The other is the backup and restoration of the SAP HANA database. The details are as follows:

- SAP S/4HANA ASCS backup and restoration
Prepare backup policies and regularly create snapshots for or back up disks of the ASCS instance. Ensure that the file directory (which is `/usr/sap/<SID>/SYS/profile` by default) containing Kernel and profile files on ASCS instance are covered by the backup policies. This is because these files contain configurations of **Kernel**, **Start profile**, **Default profile**, and **Instance profile**. When an AZ is faulty, you can use backup files or snapshots to restore the SAP S/4HANA system using VBS in the standby AZ.
To implement DR restoration, you need to install SAP S/4HANA in the other AZ and use the backup directory to overwrite files in the original directory to restore the system. Then, restore the disks using disk backups through VBS.
- SAP HANA database backup and restoration:
The HANA system or storage replication function is used to ensure HA and remote DR and restoration for SAP HANA databases. For more SAP HANA information, see the section **Backup and Restoration** in the *SAP HANA User Guide (Single-Node Deployment)* and *SAP HANA User Guide (Cluster Deployment)*. For details about HA and DR of SAP HANA data (including data and log volumes), see [SAP HANA Database Backup and Recovery](#).
- For details about how to back up and restore EVS, see sections **Data Backup Using a Backup Policy** and **Data Restoration Using a VBS Backup** in the *Volume Backup Service User Guide*.

8 FAQs

8.1 What Should I Do If a SAP Application on an ECS Cannot Be Started?

Symptom

The `/etc/hosts` file contains "`127.0.0.1 host name host name`". As a result, the SAP application installed on the ECS cannot be started. You need to log in to the ECS where the SAP application is deployed to modify the configurations.

NOTE

You only need to perform this operation on the ECS where the SAP application software is deployed.

Procedure

Step 1 Log in to the ECS where the SAP application software is deployed as user **root**.

Step 2 Comment out **manage_etc_hosts: localhost** in the configuration file.

1. Run the following command to open the Cloud-Init configuration file `/etc/cloud/cloud.cfg`:

```
vi /etc/cloud/cloud.cfg
```

2. Comment out **manage_etc_hosts: localhost** in the configuration file and save the modification.

Example: `#manage_etc_hosts: localhost`

```
datasource_list: ['OpenStack']
manage_etc_hosts: localhost

datasource:
  OpenStack:
    # timeout: the timeout value for a request at metadata service
    timeout : 50
    # The length in seconds to wait before giving up on the metadata
    # service. The actual total wait could be up to
    # len(resolvable_metadata_urls)*timeout
    max_wait : 120
```

Step 3 Delete "**127.0.0.1** *host name host name*" from the **/etc/hosts** file.

1. Run the following command to open the **/etc/hosts** file:

```
vi /etc/hosts
```

2. Delete "**127.0.0.1** *host name host name*" from the **/etc/hosts** file and save the modification.

```
#
# hosts          This file describes a number of hostname-to-address
#                mappings for the TCP/IP subsystem.  It is mostly
#                used at boot time, when no name servers are running.
#                On small systems, this file can be used instead of a
#                "named" name server.
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#
# special IPv6 addresses
::1          localhost          ipv6-localhost  ipv6-loopback
fe00::0     ipv6-localnet
ff00::0     ipv6-mcastprefix
ff02::1     ipv6-allnodes
ff02::2     ipv6-allrouters
ff02::3     ipv6-allhosts

127.0.0.1   localhost
127.0.0.1   localhost          localhost
127.0.0.1   test-xiongp          test-xiongp
~
```

Step 4 Restart the SAP application on the ECS where the SAP application has been installed. If the SAP application has not been installed on the ECS, perform the preceding operations and install the SAP software.

----End

A Change History

Released On	What's New
2019-06-30	This issue is the first official release.