

SAP NetWeaver User Guide

SAP NetWeaver User Guide

Issue 01
Date 2022-12-23



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2022. 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.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

Contents

1 Overview.....	1
1.1 About This Document.....	1
1.2 Introduction to SAP NetWeaver.....	2
1.3 SAP NetWeaver and Public Cloud.....	3
1.4 Common Concepts.....	4
1.4.1 Node and Role.....	4
1.4.2 SAP NetWeaver Instances.....	5
1.5 Technical Support.....	7
2 Solution.....	8
2.1 Solution Introduction.....	8
2.1.1 Solution Overview.....	8
2.1.2 License.....	9
2.1.3 SAP Indicator Collector.....	9
2.1.4 Standard Deployment.....	9
2.1.5 Distributed Deployment.....	12
2.1.6 Distributed HA Deployment Mode.....	14
2.2 Data Planning.....	18
2.2.1 SAP NetWeaver ECS Hardware Evaluation (SAP Sizing).....	18
2.2.2 Region and AZ.....	18
2.2.3 IAM Requirements.....	19
2.2.4 Recommended ECS Planning.....	19
2.2.5 Network Planning.....	22
2.2.5.1 Network Plane Planning.....	22
2.2.5.2 Security Group Planning.....	25
3 Deploying SAP NetWeaver.....	29
3.1 Resource Preparation.....	29
3.1.1 Software and Tools.....	29
3.1.2 Applying for a VPC.....	31
3.1.3 Creating a Subnet and Configuring a Security Group.....	32
3.1.4 Creating an SFS Turbo File System.....	33
3.2 Creating ECSs.....	35
3.2.1 Creating ECSs for SAP NetWeaver	35

3.2.2 Creating an ECS Used as an NAT Server.....	40
3.3 Configuration Before Installation.....	44
3.3.1 Configuring SSH Switching Permissions.....	44
3.3.2 Modifying OS Configurations.....	45
3.3.3 Attaching a Shared Disk and Binding a Floating IP Address (Distributed HA Deployment).....	46
3.4 Installing SAP NetWeaver.....	47
3.4.1 Formatting a Disk.....	47
3.4.2 Attaching an SFS Turbo File System to an ECS.....	48
3.4.3 Installing the SAP NetWeaver Software.....	49
3.4.4 Installing SAP GUI.....	50
3.4.5 Interconnecting SAP GUI with SAP NetWeaver.....	50
3.4.6 Configuring the HA Function for SAP NetWeaver (Distributed HA Deployment).....	50
3.4.7 Installing Data Provider.....	54
3.5 Configuring iSCSI (Cross-AZ HA Deployment).....	54
4 Backup and Restoration.....	59
5 FAQs.....	60
5.1 What Should I Do If a SAP Application on an ECS Cannot Be Started?.....	60
A Change History.....	62

1 Overview

- [1.1 About This Document](#)
- [1.2 Introduction to SAP NetWeaver](#)
- [1.3 SAP NetWeaver and Public Cloud](#)
- [1.4 Common Concepts](#)
- [1.5 Technical Support](#)

1.1 About This Document

The document conventions are as follows:

- This document provides instructions for you to prepare resources (such as ECSs and network resources) on the public cloud platform, and install SAP NetWeaver.
- This document cannot replace the standard SAP document. If you have any trouble in installing and using SAP NetWeaver 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 NetWeaver 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 NetWeaver.
- For details about the official SAP installation guide and related notes, see the following documents:
 - [SAP Installation Guides](#)
 - [SAP Notes](#)
 - [SAP Library](#)

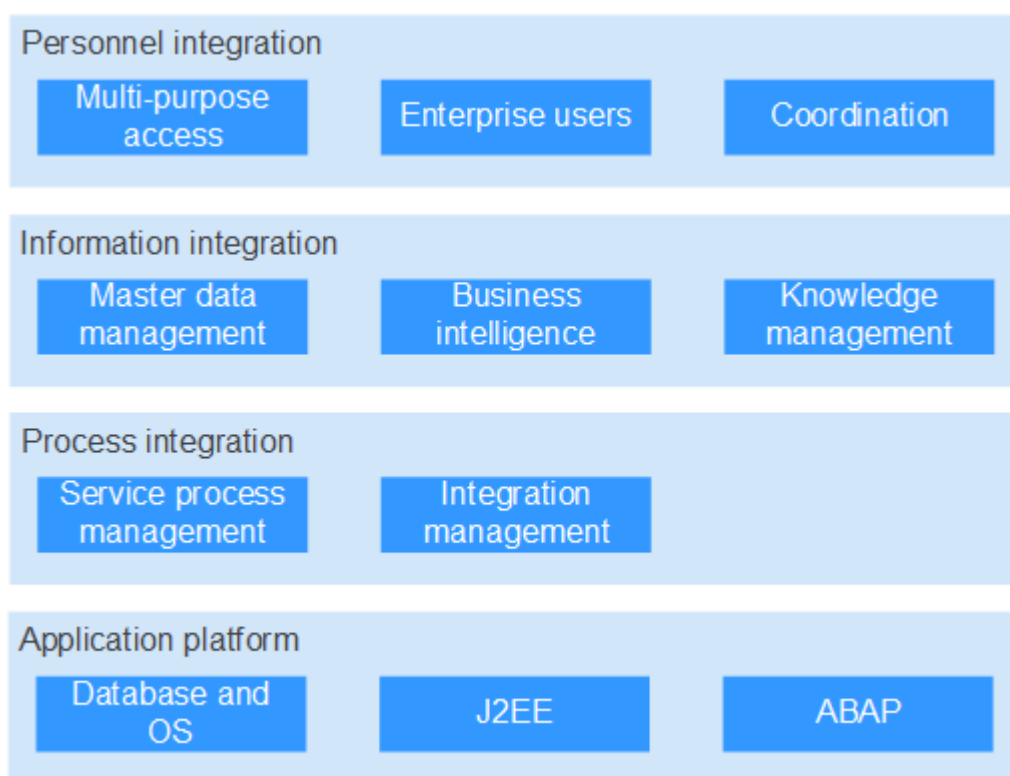
1.2 Introduction to SAP NetWeaver

Overview

SAP NetWeaver is an integrated application platform developed based on professional standards. It remarkably simplifies system integration. As shown in [Figure 1-1](#), components contained in SAP NetWeaver include the portal, application servers, business intelligence (BI) solution, and system and data integration technologies.

SAP NetWeaver can help enterprises integrate personnel, information, and service processes by crossing the boundaries of technologies and organizations. Additionally, SAP NetWeaver fully interacts with IBM Web Sphere (J2EE) and provides customers with flexible infrastructure management, simplifies system complexity, and reduces the total costs.

Figure 1-1 Components contained in SAP NetWeaver



SAP NetWeaver Application Scenarios

SAP NetWeaver applies to the following scenarios:

- Personnel integration
SAP NetWeaver integrates the existing management, office, and document systems into the enterprise information portal to provide a unified portal for the enterprise IT system.

- **Information integration**
SAP NetWeaver integrates the management information stored in databases and unstructured information (including market information and reports) scattered in different departments in an enterprise to build an information warehouse and knowledge management system to support operation decision-making.
- **Process integration**
SAP NetWeaver consolidates service processes in different systems to build an automatic process. Only a set of system is presented to users.
- **Platform integration**
SAP NetWeaver provides underlying architecture that supports open standards, such as xml, and can flexibly connect to other systems.

SAP NetWeaver-Based Products

- SAP ECC (Enterprise Central Component)
- SAP BW (Business Warehouse)
- SAP PI (Process Integration)
- SAP EP (Enterprise Portal)

1.3 SAP NetWeaver and Public Cloud

Advantages of Deploying SAP NetWeaver on the Public Cloud

Deploying the SAP NetWeaver system on the public cloud makes full use of ECS advantages, including:

- **Lowered purchase cost:** You can purchase the SAP NetWeaver system on demand for the specific DEV, TST, and TRN scenario. You will be charged only when the system is being used, which reduces the purchase cost.
- **Improved deployment efficiency:** Purchasing the SAP NetWeaver system on the public cloud shortens the deployment duration from days to hours, saving time and manpower.
- **Flexible expansion:** On the public cloud, a single node can be flexibly expanded to a cluster or a larger scale.
- **Flexible usability:** If an SAP NetWeaver system is used in development, testing, and training scenarios at different time, you can purchase the SAP NetWeaver system in different deployment modes as required.

Relationships Between SAP NetWeaver and Public Cloud Services

- **Elastic Cloud Server (ECS)**
Both SAP NetWeaver and NAT are deployed on ECSs.
- **Elastic Volume Service (EVS)**
All the SAP NetWeaver ECSs have EVS disks attached.
- **Virtual Private Cloud (VPC)**
All SAP NetWeaver 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 NetWeaver ECS, select a proper public image, for example, **SUSE Linux Enterprise Server 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 shared with multiple ECSs.

1.4 Common Concepts

1.4.1 Node and Role

SAP NetWeaver Instance

An SAP NetWeaver system consists of one or more SAP NetWeaver instances. SAP NetWeaver instances are logic units in an SAP NetWeaver system.

SAP GUI

SAP GUI allows users to access SAP NetWeaver application servers from clients. SAP GUI provides the common system information (such as software version), system management capability, and statistics of key system resources.

NAT Server

Provides the capability to switch to the HANA ECS using SSH. It allows you to switch to an SAP NetWeaver node from the NAT server using Secure Shell (SSH).

SFS

The Scalable File Service (SFS) provides the file sharing service and supports two types of file systems: SFS and SFS Turbo. An SFS Turbo file system is needed when the SAP NetWeaver is deployed in distributed mode. You need to create an SFS Turbo and mount it to an SAP NetWeaver instance node. For details about the node specifications, see [2.2.4 Recommended ECS Planning](#).

SAP NetWeaver

SAP NetWeaver has multiple deployment scenarios. When installing SAP NetWeaver, select a proper deployment mode based on the systems, including DEV, QAS, PRD, TST, and POC. For example, use a bound EIP to access the POC and TST systems. For the PRD system, you are advised to access it through a VPN for high security. Additionally, the distributed HA deployment mode of SAP NetWeaver is also available, as shown in section [2.1 Solution Introduction](#).

1.4.2 SAP NetWeaver Instances

The SAP NetWeaver system consists of the following instances in any deployment mode.

- Dialog instance
 Dialog instance is optional and installed on separate hosts to ensure high availability of dialog processes. Dialog instance includes:
 - Dispatcher
 - Work Processes (Dialog, Batch, Spool, and Update)
 - Gateway
 - Internet Communication Manager (ICM)
 - Internet Graphics Service (IGS)

In a cluster scenario, Dialog instance can be added to the cluster. After Dialog instance is added to the cluster, Central instance updates the Dialog instance information. Each cluster requires a load balancing solution, such as SAP Web Dispatcher. [Table 1-1](#) lists the components contained in Dialog instance.

Table 1-1 Components contained in Dialog instance

Instance	Component	Function
Dialog instance	Work Processes (Dialog, Batch, Spool, and Update)	Work processes are used to execute applications and contain the Dialog, Batch, Spool, and Update processes. Work processes are components that are able to execute an application (that is, each dialog step). Each work process is linked to a memory area containing the context of the application being run. The context contains the current data for the application program. This needs to be available in each dialog step.
	Dispatcher	The dispatcher is the link between the work processes and the users logged in to the ABAP application server (that is, the SAP GUIs of these users). Its task is to receive requests for dialog steps from the SAP GUI and direct them to a free work process. In the same way, it directs screen output resulting from the dialog step back to the appropriate user.

Instance	Component	Function
	Gateway	This is the interface for the communication protocols of NetWeaver AS ABAP (RFC, CPI/C). It can communicate with other ABAP application servers of the same NW AS, with other SAP Systems, or with external non-SAP systems.
	Internet Communication Manager (ICM)	The Internet Communication Manager ensures that communication between the SAP system (SAP NetWeaver Application Server) and the outside world via HTTP, HTTPS and SMTP protocols works properly. In its role as a server, the ICM can process requests from the Internet that arrive as URLs with the server/port combination that the ICM can listen to. The ICM then calls the relevant local handler for the URL in question.
	Internet Graphics Service (IGS)	IGS is used to generate Web-based graphics from the SAP Web AS.

- ASCS instance

ASCS instance includes the Enqueue and Message servers. An SAP NetWeaver system contains only one ASCS instance. Therefore, ASCS instance must have no single point of failure (SPOF) in the PRD system. To ensure high availability of ASCS instance, you need to install ERS instance.

- Message Server

A Message server is used for communication among Dialog instances and provides information for Dispatcher for load balancing.

- Enqueue Server

An Enqueue server contains a lock table which contains the database lock and the basic lock information configured by Java Server Process. The Enqueue server can also synchronize data among Java clusters. In an AS ABAP case, an Enqueue server processes the locks of data objects.

- ERS instance

An ERS instance ensures high availability for ASCS instance and protects Message Server and Enqueue Server on ASCS instance.

Table 1-2 lists the components contained in ASCS instance.

Table 1-2 ASCS instance and its components

Instance	Service	Function
ASCS instance	Message server	<p>Message server is an independent process and contained in ASCS instance. One SAP system contains only one Message server. Message Server provides the following functions:</p> <p>It is the core communication channel between the separated application servers.</p> <p>It allocates login users using the login group function of SAP GUI and RFC.</p> <p>It functions as the information center of Web Dispatcher and application servers.</p>
	Enqueue Server	<p>Enqueue Server is a special lock mechanism in the SAP system, which prevents a line of data from being simultaneously changed by two processes and ensures consistency in updating the database.</p>
	Enqueue Replication Server (ERS)	<p>ERS is used to protect Message and Enqueue servers contained in ASCS instance.</p>

- Web Dispatcher
 An SAP Web dispatcher is a link connecting Internet to SAP NetWeaver and locates in the demilitarized zone (DMZ). All HTTP requests pass Web Dispatcher, which ensures connection security. Then Web Dispatcher allocates the requests to multiple SAP NetWeaver application servers.
- Database instance
 The Database instance is mandatory in an SAP NetWeaver system and is used to create an ABAP schema for the SAP system in the database.

Other related software includes SAP Host Agent, SWPM, and SAPCAR.

1.5 Technical Support

If any problem occurs when using Huawei Cloud, contact the after-sales technical support team (24/7) at <https://www.huaweicloud.com/intl/en-us/service/help-tools.html>.

2 Solution

[2.1 Solution Introduction](#)

[2.2 Data Planning](#)

2.1 Solution Introduction

2.1.1 Solution Overview

SAP NetWeaver is generally deployed in the following systems:

- PRD (Production): indicates the production system where SAP applications are formally used.
- Quality Assure (QAS): indicates the quality assurance system where SAP application functions, performance, and reliability are fully verified.
- Development (DEV): indicates the development system where the development engineers commission SAP NetWeaver application software and SAP HANA, and optimize the application software during application software development.
- Training (TRN): indicates the training and demonstration system where you provide a training or demonstration after deploying SAP applications.
- Test (TST): indicates the test system where the development engineers test application software and SAP products to verify the functions of application software after application software development is complete.
- Proof of Concept (POC): indicates the verification system where a prototype demonstration can be made within a shorter period of time used for verifying the software function and applicability and determining whether the SAP product needs to be rolled out.

 **NOTE**

You are advised to use a VPN to access the DEV, QAS, and PRD systems and deploy the PRD system in distributed HA deployment mode.

You have been familiar with all related SAP Notes before planning and using the SAP NetWeaver AS ABAP/Java on the public cloud.

This document describes how to deploy SAP NetWeaver in an AZ.

2.1.2 License

SAP NetWeaver is authorized in Bring Your Own License (BYOL) mode. In this mode, you must log in to the SAP [technical support website](#) and apply for a license.

In addition to applying for a license, you must purchase public-cloud-related resources, such as ECS, EVS, VPC, IMS, SFS, and VBS.

2.1.3 SAP Indicator Collector

Data Provider is an SAP indicator collector on Huawei Cloud. Data Provider is installed on each ECS where SAP NetWeaver is installed. For details about how to install and configure Data Provider, see [Data Provider for SAP User Guide](#).

2.1.4 Standard Deployment

SAP NetWeaver can be deployed in the standard distributed mode and integrated mode, as shown in [Figure 2-1](#) and [Figure 2-2](#).

Figure 2-1 Distributed deployment mode of SAP NetWeaver

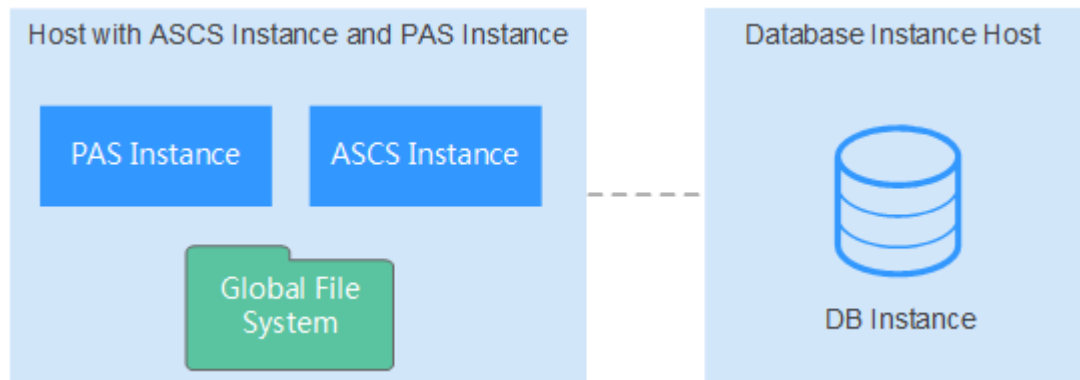
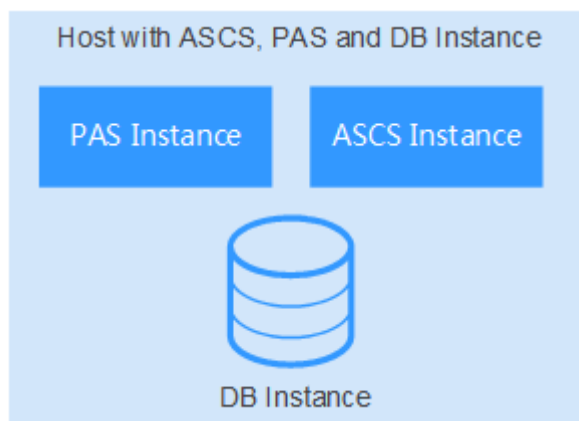


Figure 2-2 Integrated deployment mode of SAP NetWeaver



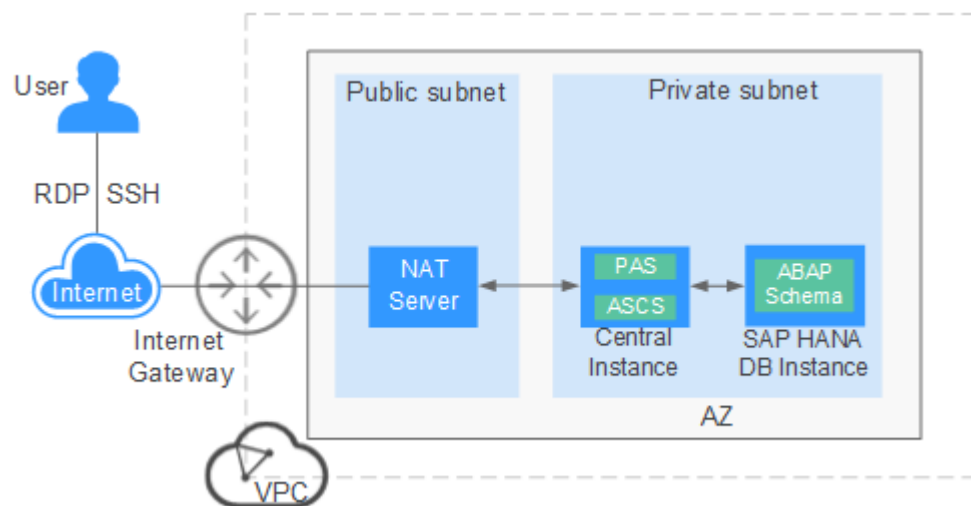
In these deployment modes, all main instances (except for SAP HANA DB instance) run on a separated ECS. The deployment mode is used for all the scenarios, except for PRD. SAP NetWeaver includes the following instances:

- ABAP Central Services instance (ASCS instance)
- SAP HANA database instance (DB instance)
- Primary application server instance (PAS)

Huawei Cloud can be connected to SAP NetWeaver servers through a NAT server (binding an EIP) or using a VPN.

- **Figure 2-3** shows the access to the SAP NetWeaver servers through a NAT server.

Figure 2-3 Accessing to SAP NetWeaver servers through a NAT server

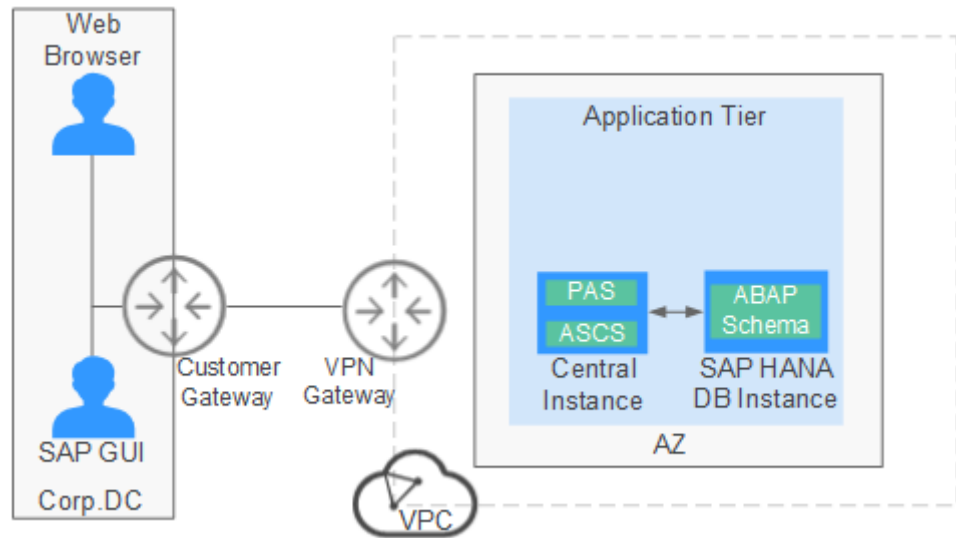


The concepts involved in the preceding figure are as follows:

- VPC: All ECSs in the SAP NetWeaver system are deployed in a VPC to protect network security. SAP NetWeaver ECSs belong to a private subnet, and the NAT ECS belongs to a public subnet.
- Users can log in to the NAT ECS with an EIP bound using RDP or SSH and use SAP GUI on the NAT ECS to access SAP NetWeaver ECSs.
 - Public subnet:
 - NAT server: allows you to access SAP NetWeaver ECSs using Secure Shell (SSH).
 - SAP GUI is installed on the NAT ECS and allows users to access SAP NetWeaver ECSs on the private subnet.
 - Private subnet:
 - Central instance is used to deploy the ASCS instance and PAS instance.
 - SAP HANA database instance is used to deploy the SAP HANA database.

- **Figure 2-4** shows the access to SAP NetWeaver ECSs using a VPN.

Figure 2-4 Accessing to SAP NetWeaver ECSs using a VPN



The concepts involved in the preceding figure are as follows:

- VPC: To ensure network security, all SAP NetWeaver ECSs are in the same VPC.
- The user uses SAP GUI or Web Browser to access SAP NetWeaver ECSs through the VPN.
 - The user or technical engineer is responsible for building the VPN.
 - The user can use the VPC to access SAP application ECSs from the internal network.

Table 2-1 shows the file systems planned for the standard deployment mode.

Table 2-1 File systems planned for the standard deployment mode

Mount Point	File System Type	Description
/usr/sap	ext3	Stored on the local VM (for details, see section 2.2 Data Planning).
/sapmnt	ext3	Stored on the local VM (for details, see section 2.2 Data Planning).

Select a proper deployment mode as required. **Table 2-2** lists the recommended application scenarios.

Table 2-2 Mapping between deployment modes and scenarios

Deployment Scenario	Deployment Mode	Access Mode
TRN POC TST	Standard deployment	EIP (NAT)
DEV QAS	Standard deployment	VPN

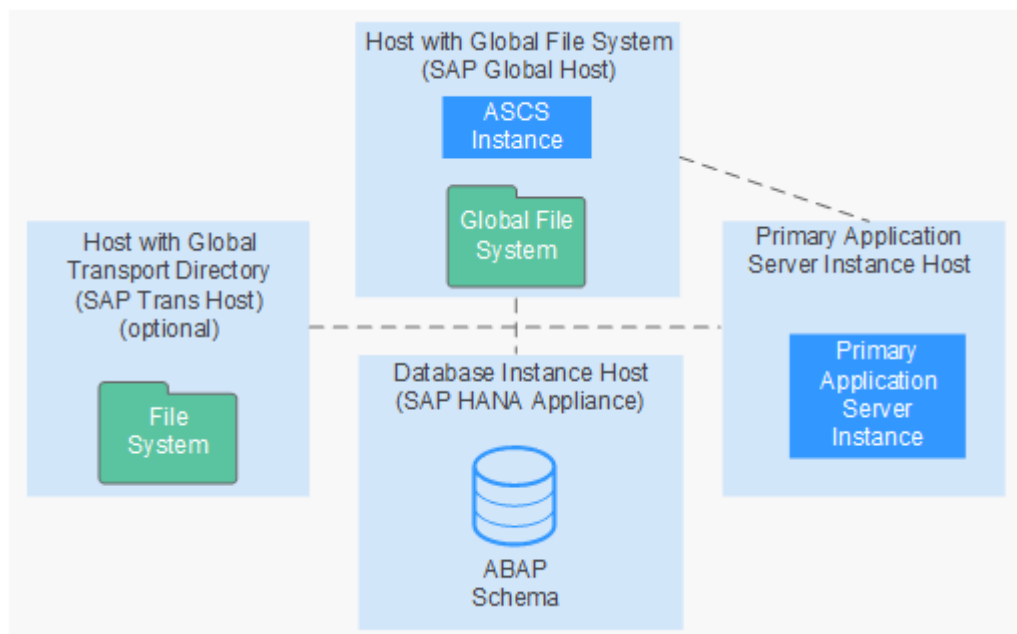
NOTE

The NAT server functions as only jump server.

2.1.5 Distributed Deployment

Figure 2-5 shows the distributed deployment mode of SAP NetWeaver.

Figure 2-5 Distributed deployment mode of SAP NetWeaver

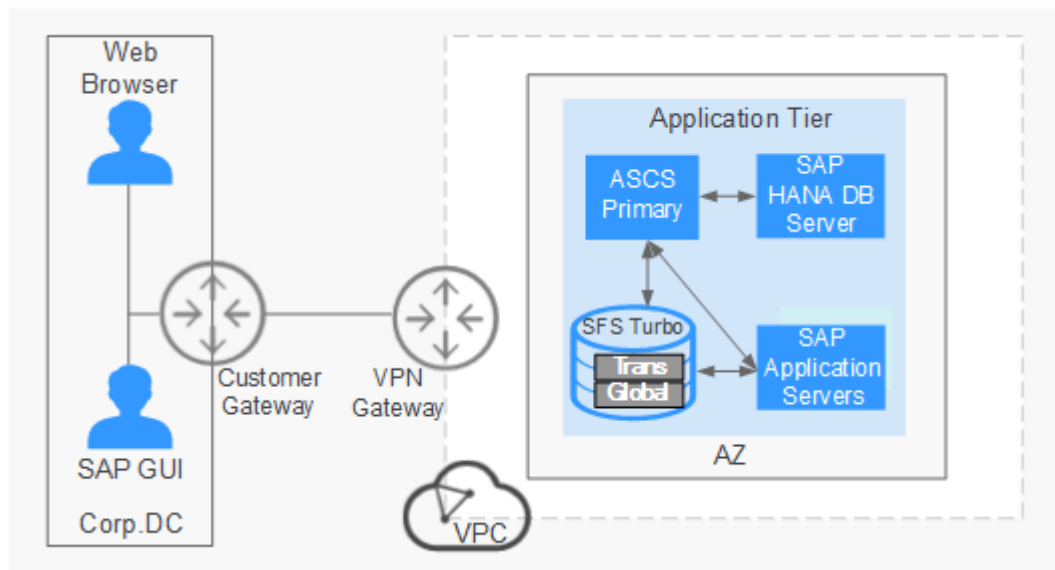


In the distributed deployment mode, the SAP NetWeaver system consists of multiple SAP instances. An SAP instance is a group of processes that are simultaneously started or stopped. In the distributed SAP NetWeaver system, all instances are deployed on separated ECSs. The main instances are as follows:

- ABAP Central Services instance (ASCS instance)
- SAP HANA database instance (DB instance)
- Primary application server instance (PAS instance)

Figure 2-6 shows the recommended distributed deployment mode of SAP NetWeaver on the public cloud.

Figure 2-6 Recommended distributed deployment mode of SAP NetWeaver



The description of each part is the same as that in section [2.1.4 Standard Deployment](#). The difference is that ASCS instance and PAS instance are deployed on different ECSs in the distributed deployment mode. Applying for multiple ECSs as application servers are scheduled by Web Dispatcher. SFS Turbo provides the file sharing service. Global files are shared by all SAP NetWeaver ECSs. Trans files are attached to SAP application servers.

[Table 2-3](#) shows the file systems planned for the distributed deployment mode.

Table 2-3 File systems planned for the distributed deployment mode

Mount Point	File System Type	Description
/usr/sap	ext3	Local disk. For details, see section 2.2 Data Planning .
/sapmnt/<SID>	ext3	SFS Turbo file system, which provides the shared storage. For details, see section 2.2 Data Planning . SFS is attached to all SAP NetWeaver ECSs.
/usr/sap/trans	ext3	SFS Turbo file system, which provides the shared storage. For details, see section 2.2 Data Planning . SFS is attached to all application servers.

Select a proper deployment mode as required. [Table 2-4](#) lists the recommended application scenarios.

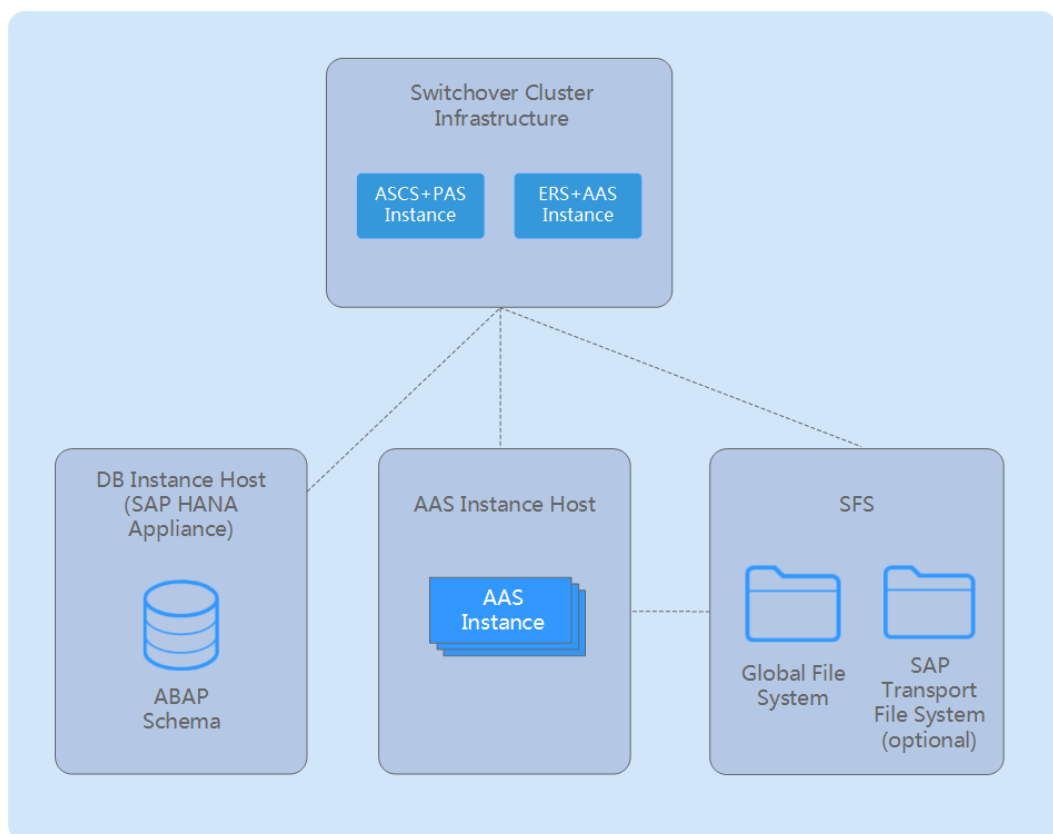
Table 2-4 Mapping between deployment modes and scenarios

Deployment Scenario	Deployment Mode	Access Mode
QAS PRD	Distributed deployment	VPN

2.1.6 Distributed HA Deployment Mode

[Figure 2-7](#) shows the distributed HA deployment mode of SAP NetWeaver.

Figure 2-7 Distributed HA deployment mode of SAP NetWeaver



In this deployment mode, the SAP NetWeaver system consists of multiple SAP instances. An SAP instance is a group of processes that are simultaneously started or stopped. In the distributed HA deployment mode, all instances are deployed on separated ECSs. The main instances are as follows:

- ASCS instance (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 2-5 lists the SAP NetWeaver component features.

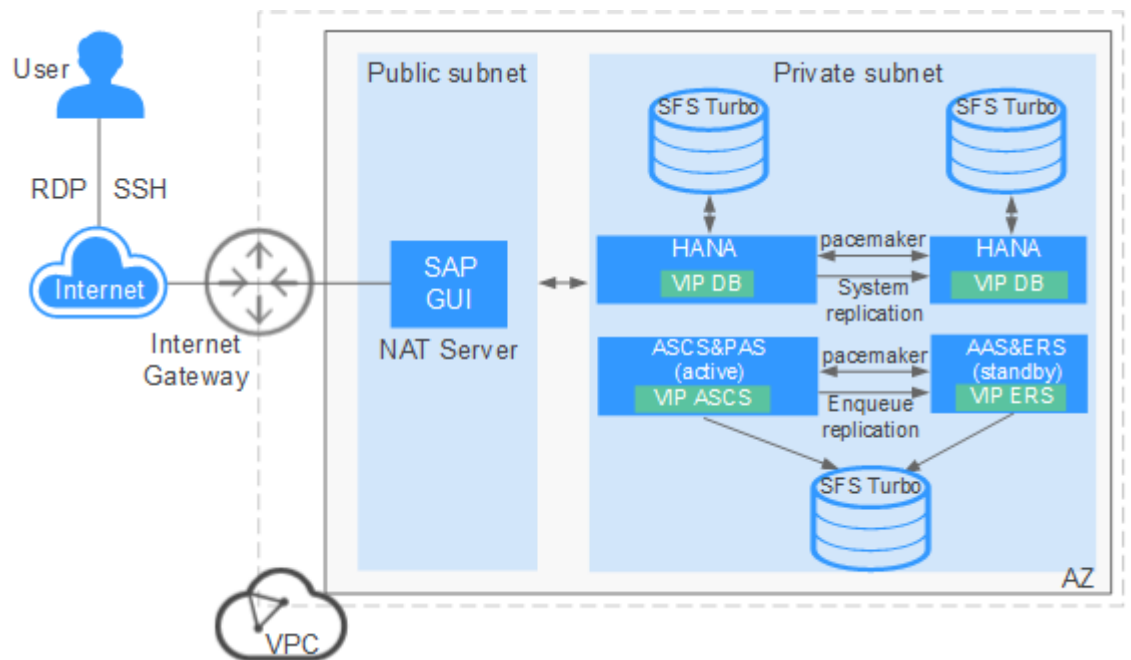
Table 2-5 SAP NetWeaver component features

SAP NetWeaver Component	Reliability Assurance
<ul style="list-style-type: none"> • ASCS instance (including 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 the SAP NetWeaver software, install Dialog instance in distributed mode to ensure HA.

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

Figure 2-8 shows the recommended distributed HA deployment mode of SAP NetWeaver on the public cloud.

Figure 2-8 Recommended distributed HA deployment mode of SAP NetWeaver



The preceding describes an example of the SAP NetWeaver HA deployment mode. You can install SAP NetWeaver as required.

- ASCS instance (including 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 to a shared disk. The ASCS instance is installed on the active ECS, and the ERS instance is installed on the standby ECS. The time synchronization and disk formatting must be performed on the two ECSs.
- SAP HANA databases are deployed in the active/standby mode. The PAS instance is deployed on the active database and the AAS instance is deployed on the standby database. For details about how to install SAP HANA, see the *SAP HANA User Guide*.
- You can create an SFS Turbo file system to provide the file sharing storage. You can also use NFS to share files.
- The security group and elastic NICs are used to protect SAP NetWeaver Central instance, ASCS instance, and DB instance to avoid communication errors and isolate failed resources.
- [Table 2-6](#) and [Table 2-7](#) show the file system planning for the active and standby ASCS nodes.

Table 2-6 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 2.2 Data Planning . NOTE In the cross-AZ or cross-region deployment scenario, the SFS Turbo file system provides the shared storage.
/sapmnt	sfs	SFS Turbo file system, which provides the shared storage. For details, see section 2.2 Data Planning .
/usr/sap/<SID>/SYS	sfs	SFS Turbo file system, which provides the shared storage. For details, see section 2.2 Data Planning .
/sapcd	sfs	SFS Turbo file system, which provides the shared storage. The SAP NetWeaver installation package is uploaded to this directory.

Table 2-7 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 2.2 Data Planning . NOTE In the cross-AZ or cross-region deployment scenario, the SFS Turbo file system provides the shared storage.

Mount Point	File System Type	Description
/sapmnt	sfs	SFS Turbo file system, which provides the shared storage. For details, see section 2.2 Data Planning .
/usr/sap/<SID>/SYS	sfs	SFS Turbo file system, which provides the shared storage. For details, see section 2.2 Data Planning .
/sapcd	sfs	SFS Turbo file system, which provides the shared storage. The SAP NetWeaver installation package is uploaded to this directory.

- Select a proper deployment mode as required. [Table 2-8](#) lists the recommended application scenarios.

Table 2-8 Mapping between deployment modes and scenarios

Deployment Scenario	Deployment Mode	Access Mode
PRD	Distributed HA deployment	NAT

2.2 Data Planning

2.2.1 SAP NetWeaver ECS Hardware Evaluation (SAP Sizing)

Before applying for SAP NetWeaver 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 NetWeaver, see SAP note: [1953429](#) and [SAP Installation Guides](#).

2.2.2 Region and AZ

Select the ECS of the target region and AZ to install the SAP NetWeaver.

2.2.3 IAM Requirements

To ensure the stable running of Data Provider, create the agency for the SAP NetWeaver ECS and bind it to the ECS.

- For details about how to create an agency and install Data Provider, see the [Data Provider for SAP User Guide](#).
- When creating an ECS, specify the agency to the ECS. For details, see section [3.2.1 Creating ECSs for SAP NetWeaver](#) .

2.2.4 Recommended ECS Planning

This section describes the planning of SAP NetWeaver ECSs and NAT server (SAP GUI).

 **NOTE**

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

Table 2-9 Specifications of ECSs for SAP NetWeaver

Type	Flavor	vCPUs	Memory (GB)
High-Performance computing H1 ECS	h1.xlarge.4	4	16
	h1.2xlarge.4	8	32
	h1.4xlarge.4	16	64
	h1.8xlarge.4	32	128
Memory-optimized M3 ECS	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
General Computing-plus ECS	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

Type	Flavor	vCPUs	Memory (GB)
Memory-optimized M6 ECS	m6.large.8	2	16
	m6.xlarge.8	4	32
	m6.2xlarge.8	8	64
	m6.3xlarge.8	12	96
	m6.4xlarge.8	16	128
	m6.6xlarge.8	24	192
	m6.8xlarge.8	32	256
	m6.16xlarge.8	64	512

Plan the data for each ECS by referring to [Table 2-10](#). For details about the hardware configuration, see section [2.2.1 SAP NetWeaver ECS Hardware Evaluation \(SAP Sizing\)](#).

Table 2-10 Recommended ECS planning

Node	Specifications
SAP NetWeaver ECS planning in the standard deployment mode	Recommended configurations: <ul style="list-style-type: none"> ● OS: SUSE Linux Enterprise Server 12 SP1 for SAP or later ● Flavor: h1.2xlarge.4 (8 vCPUs and 32 GB memory) ● Disk: <ul style="list-style-type: none"> - System disk: ultra-high I/O, 100 GB - Data disk: ultra-high I/O, 200 GB
SAP NetWeaver ECS planning in the distributed deployment mode	Recommended configurations: <ul style="list-style-type: none"> ● OS: SUSE Linux Enterprise Server 12 SP1 for SAP or later ● Flavor: h1.2xlarge.4 (8 vCPUs and 32 GB memory) ● System disk: ultra-high I/O, 100 GB

Node	Specifications
SAP NetWeaver ECS planning in the distributed HA deployment mode	<p>Recommended configurations:</p> <ul style="list-style-type: none"> ● OS: SUSE Linux Enterprise Server 12 SP1 for SAP or later ● Flavor: h1.2xlarge.4 (8 vCPUs and 32 GB memory) ● Disk: <ul style="list-style-type: none"> – System disk: ultra-high I/O, 100 GB – Data disk (created on the active ASCS node): ultra-high I/O, SCSI, and three shared disks with a total of 170 GB memory. After a data disk is created, bind it to the standby ASCS node. Only create a system disk for the standby ASCS 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 3.5 Configuring iSCSI (Cross-AZ HA Deployment).</p>
NAT Server	<ul style="list-style-type: none"> ● OS: SUSE Linux Enterprise Server 12 SP1 or later ● Flavor: s1.medium (1 vCPU and 4 GB memory) or higher ● System disk: high I/O, 40 GB

[Table 2-11](#) and [Table 2-12](#) list the file system planning in the distributed HA deployment mode.

Table 2-11 Planning of the shared disk file system

Parti tion	Capac ity (GB)	Mounting Directory	Description
sda	10	N/A	Used as the SBD disk.
sdb	80	/usr/sap/<SID>/ASCS<##>	Partition of the active ASCS node, which is used to install the ASCS instance.
sdc	80	/usr/sap/<SID>/ERS<##>	Partition of the standby ASCS 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 [3.5 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 2-13](#) describes the planning of the SFS Turbo file system in the cross-AZ HA scenario.

Table 2-12 Planning of the SFS Turbo file system

Name	Total Capacity (GB)	Mounting Directory	Description
sapmnt	100	/sapmnt	Shared to all nodes in the SAP NetWeaver system
usrsapsys	10	/usr/sap/<SID>/SYS	Shared to all nodes in the SAP NetWeaver system
sapmedia	100	/sapcd	Shared to all nodes in the SAP NetWeaver system

Table 2-13 Planning of the SFS Turbo file system in the cross-AZ HA scenario.

Name	Total Capacity (GB)	Mounting Directory	Description
sapmnt	100	/sapmnt	Shared to all nodes in the SAP NetWeaver system
usrsapsys	10	/usr/sap/<SID>/SYS	Shared to all nodes in the SAP NetWeaver system
sapmedia	100	/sapcd	Shared to all nodes in the SAP NetWeaver system
ASCS	80	/usr/sap/<SID>/ASCS<##>	Shared to the active ASCS node, which is used to install the ASCS instance.
ERS	80GB	/usr/sap/<SID>/ERS<##>	Shared to the standby ASCS node, which is used to install the ERS instance.

2.2.5 Network Planning

2.2.5.1 Network Plane Planning

The network information needs to be planned based on application scenarios and SAP NetWeaver planning.

The network segments and IP addresses are for reference only. You can configure it based on site requirements.

- Network plane planning in the standard deployment scenario where the SAP NetWeaver system is accessed using the NAT server with an EIP bound

In this scenario, an SAP NetWeaver instance node uses only one NIC for network communication between servers and clients. **Figure 2-9** shows the network planning in the standard deployment mode.

Figure 2-9 Network planning in the standard deployment mode

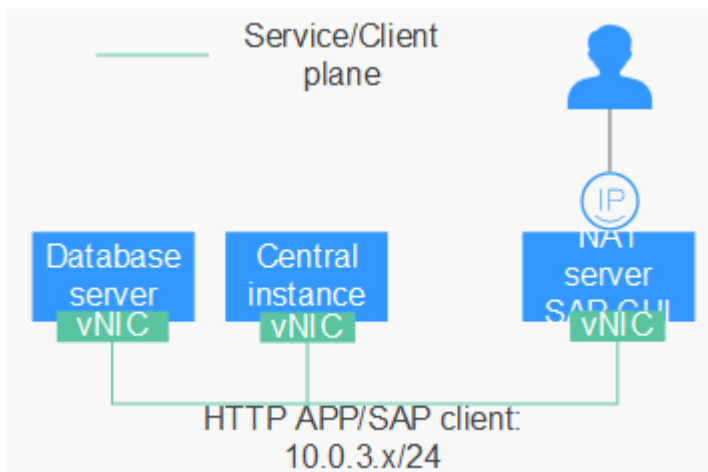


Table 2-14 shows the planned network information.

Table 2-14 Network planning in the single-node scenario where HA is not required and an EIP is used to access the NAT server

Parameter	Description	Example Value
IP address of the server/client plane	Specifies the IP address of the primary NIC plane. The central instance communicates with the SAP HANA database or the SAP GUI client using this IP address.	Central instance: 10.0.3.2 NAT server: 10.0.3.202 Database server: 10.0.3.3
EIP	A public IP address, which allows you to access the NAT server	Automatically allocated by the public cloud

- Network plane planning (using a VPN to access the SAP NetWeaver system in the distributed deployment scenario)
 In this scenario, an SAP NetWeaver instance node uses only one NIC for network communication between servers and clients. **Figure 2-10** shows the network plane planning in distributed deployment mode where SAP NetWeaver is accessed using a VPN.

Figure 2-10 Network planning in distributed deployment mode

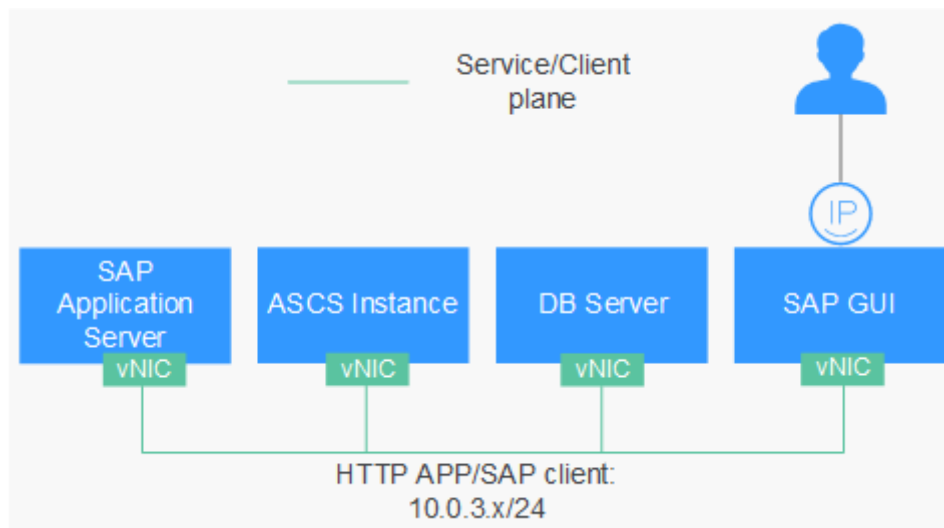


Table 2-15 shows the network information in distributed deployment mode.

Table 2-15 Network information planning (distributed VPN deployment mode)

Parameter	Description	Example Value
IP address of the server/client plane	Specifies the IP address of the primary NIC of the server/client plane. The ASCS instance communicates with the SAP HANA database or the SAP GUI client using this IP address.	ASCS instance: 10.0.3.2 Database server: 10.0.3.3 SAP application server: 10.0.3.4

- Network plane planning
 In this 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 2-11 shows the network planning in distributed HA deployment mode where SAP NetWeaver is accessed using a VPN.

Figure 2-11 Network planning in distributed HA deployment mode

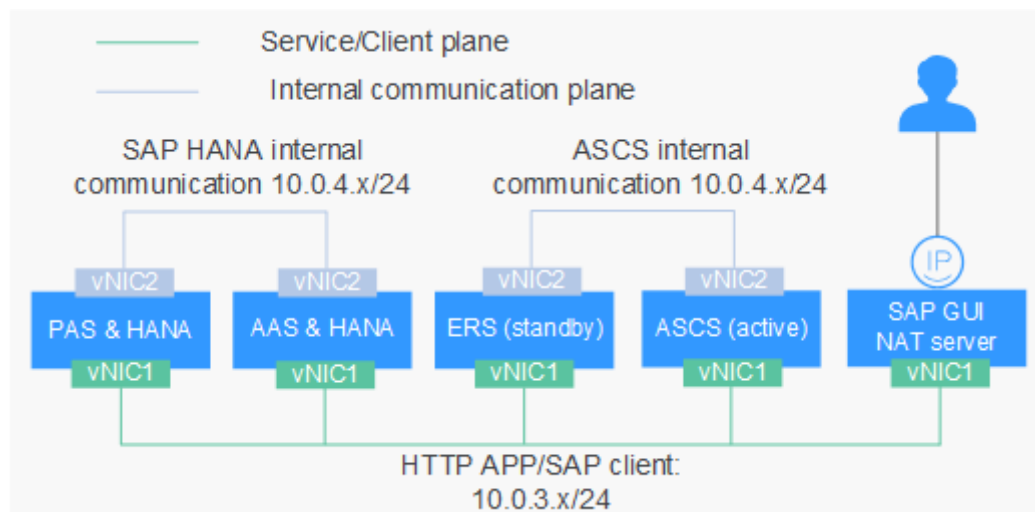


Table 2-16 Network information planning (distributed and HA EIP deployment mode)

Parameter	Description	Example Value
IP address of the server/client plane	Specifies the IP address of the primary NIC plane. The active and standby ASCS nodes communicate with the SAP GUI and SAP HANA databases using this IP address.	ASCS active node: 10.0.3.2 ASCS standby node: 10.0.3.13 SAP GUI: 10.0.3.4 PAS & HANA: 10.0.3.5 AAS & HANA: 10.0.3.6
IP address of the internal heartbeat communication plane	The active and standby ASCS 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.	ASCS active node: 10.0.4.2 ASCS standby node: 10.0.4.3 SAP HANA database server active node: 10.0.4.6 SAP HANA database server standby node: 10.0.4.7

2.2.5.2 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 2-17](#), [Table 2-18](#), and [Table 2-19](#).

 **NOTE**

- The network segments and IP addresses are for reference only. The following security group rules are recommended practices. You can configure your own security group rules as you need.
- In the following table, ## stands for the SAP NetWeaver instance ID. Ensure that this ID is the same as that specified when you installed the SAP NetWeaver software.

Table 2-17 Security group rules (SAP Application Server nodes)

Source/ Destination	Protocol	Port Range	Description
Inbound			
10.0.3.0/24	TCP	32##	Allows SAP GUI to access SAP NetWeaver.
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.
10.0.3.0/24	TCP	22	Allows SAP NetWeaver to be accessed using SSH.
10.0.3.0/24	UDP	123	Allows other servers to synchronize time with SAP NetWeaver.
Determined by the public cloud	All	All	The security group rule is created by the system by default. Allows ECSs in the same security group to communicate with each other.
Outbound			

Source/ Destination	Protocol	Port Range	Description
0.0.0.0/0	All	All	The security group rule is created by the system by default. Allows SAP NetWeaver to access all peers.

Table 2-18 Security group rules (SAP ASCS nodes)

Source/ Destination	Protocol	Port Range	Description
Inbound			
10.0.3.0/24	TCP	36##	Specifies the message server ports.
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.
10.0.3.0/24	TCP	22	Allows SAP NetWeaver to be accessed using SSH.
10.0.3.0/24	UDP	123	Allows other servers to synchronize time with SAP NetWeaver.
Determined by the public cloud	All	All	The security group rule is created by the system by default. Allows ECSs in the same security group to communicate with each other.
Outbound			

Source/ Destination	Protocol	Port Range	Description
0.0.0.0/0	All	All	The security group rule is created by the system by default. Allows SAP NetWeaver to access all peers.

Table 2-19 Security group rules (NAT Server nodes)

Source/ Destination	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	All	All	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	All	All	The security group rule is created by the system by default. Allows the NAT server to access all peers.

3 Deploying SAP NetWeaver

- [3.1 Resource Preparation](#)
- [3.2 Creating ECSs](#)
- [3.3 Configuration Before Installation](#)
- [3.4 Installing SAP NetWeaver](#)
- [3.5 Configuring iSCSI \(Cross-AZ HA Deployment\)](#)

3.1 Resource Preparation

3.1.1 Software and Tools

Table 3-1 lists the required software and tools.

Table 3-1 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

Item	Description	How to Obtain
OBS Browser+	Used for uploading the SAP NetWeaver and SAP HANA installation packages to the public ECS. You can use the wget command to download the uploaded files to the nodes where SAP NetWeaver is to be installed. For details, see section 3.4.3 Installing the SAP NetWeaver Software .	Downloading OBS Browser+
VNC Viewer for Windows	Used for providing the GUI on the local computer for installing SAP NetWeaver	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.	


Item	Description	How to Obtain
SAP NetWeaver installation package NOTE Install the required SAP NetWeaver version based on version mapping.	The SAP NetWeaver 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.

3.1.2 Applying for a VPC

Scenarios

All SAP NetWeaver ECSs must be in the same VPC. Therefore, you must apply a VPC for an SAP NetWeaver system and specify the subnet segment for the VPC.

Procedure

- Step 1** Log in to the public cloud management console.
- Step 2** In the navigation pane on the left, click  and choose **Network > Virtual Private Cloud**.
- Step 3** Click **Create VPC** on the right of the page.
- Step 4** On the **Create VPC** page, configure VPC parameters.

The parameters are as follows:

Basic Information

- **Name:** specifies the VPC name.
- **CIDR Block:** specifies the IP address range for the VPC. The subnet IP address range in the VPC must be within this IP address range. Configure the VPC IP address range, for example, **10.0.0.0/8**, based on the subnet information in sections [2.2.5.1 Network Plane Planning](#) and [2.2.5.2 Security Group Planning](#).
- **Enterprise Project:** If an enterprise project has been created, you can add the VPC to an enabled enterprise project. For example, SAP.

Enterprise project management allows users to manage cloud resources based on enterprise projects. This helps you manage resources and personnel in your projects.

For details about creating and managing enterprise projects, see the [Enterprise Management User Guide](#).

- **Tag:** specifies the VPC tag, which consists of a key and value pair. This parameter is optional.

Default Subnet

- **AZ:** specifies the AZ of the VPC subnet.
- **Name:** specifies the name of the default VPC subnet. You are recommended to set this parameter value to the name of the service or client plane subnet, for example, **10.0.3.x**.
- **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 deployment plan described in sections [2.2.5.1 Network Plane Planning](#) and [2.2.5.2 Security Group Planning](#).
- **Gateway:** specifies the gateway IP address of the subnet.
- **Advanced Settings:** If you set it to **Custom**, you need to configure the following parameters:
 - **Gateway:** specifies the gateway IP address of the subnet.
 - **DNS Server Address:** An external DNS server address is used by default. If you need to change the DNS server address, ensure that the DNS server addresses you configured are available.

Step 5 Click **Create Now**.

----End


3.1.3 Creating a Subnet and Configuring a Security Group

Scenarios

To ensure proper communication between all SAP NetWeaver 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 **Network > Virtual Private Cloud**.
3. Choose **Subnets** on the left of the page.
4. In the upper right corner of the page, click **Create Subnet**.
5. In the **Create Subnet** dialog box, configure parameters as prompted.
 - **VPC:** Select the VPC created in [3.1.2 Applying for a VPC](#).
 - **Name:** Configure the subnet name that is easy to identify, for example, **service_subnet**.

- **CIDR Block:** Configure this parameter according to the deployment plan described in sections [2.2.5.1 Network Plane Planning](#) and [2.2.5.2 Security Group Planning](#).
 - **Gateway:** Use the default setting for this parameter.
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 [2.2.5.1 Network Plane Planning](#) and [2.2.5.2 Security Group Planning](#).

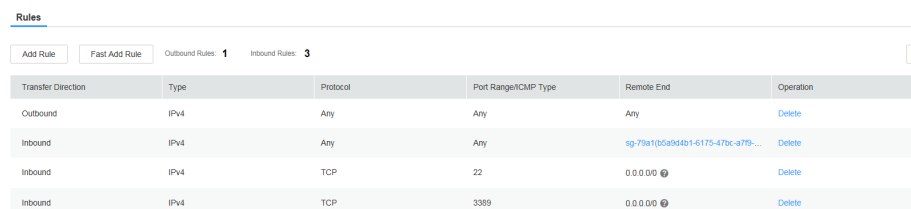
Step 2 Set security groups.

SAP NetWeaver, NFS server, NAT server, and SAP HANA require security groups.

1. Choose **Network > Virtual Private Cloud**. In the navigation pane on the left, choose **Access Control > Security Groups** and then click **Create Security Group** in the upper right corner of the page.
2. Enter a security group name, select the target enterprise project from the drop-down list, and click **OK**. Name the security group that is easy to identify, for example, **studio_security_group**.
3. Click **Access Control > Security Groups** on the left and then click the security group to which the access rule is to be added in the security group list.
4. Click **Add Rule** on the **Inbound Rules** or **Outbound Rules** tab as planned.
5. On the displayed page, add the rule according to the requirements specified in sections [2.2.5.1 Network Plane Planning](#) and [2.2.5.2 Security Group Planning](#).

[Figure 3-1](#) shows some default security group rules.

Figure 3-1 Some default security group rules



Transfer Direction	Type	Protocol	Port Range/CMP Type	Remote End	Operation
Outbound	IPv4	Any	Any	Any	Delete
Inbound	IPv4	Any	Any	sg-75a1f0ca94b16175-47bc-a7f9-...	Delete
Inbound	IPv4	TCP	22	0.0.0.0 @	Delete
Inbound	IPv4	TCP	3389	0.0.0.0 @	Delete

6. Repeat [Step 2.1](#) to [Step 2.5](#) to configure all security groups.

----End

3.1.4 Creating an SFS Turbo File System

Scenarios

In distributed deployment and distributed HA deployment scenarios, create an SFS Turbo file system to provide the file sharing storage. Create an SFS Turbo file system on the public cloud platform based on [Table 3-2](#).

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 3-2](#).

Table 3-2 Parameters

Parameter	Description	Example Value
File System Type	File system type. Select SFS Turbo .	SFS Turbo
Billing Mode	Select a mode based on the site requirements.	Yearly/Monthly
Region	Select the target region.	AP-Hong-Kong
AZ	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 (GB)	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.	5120
VPC	Select the VPC and subnet used by the ECS. For details, see 3.1.2 Applying for a VPC and 3.1.3 Creating a Subnet and Configuring a Security Group .	-
Security Group	Select the security group where the ECSs belong. For details, see 3.1.3 Creating a Subnet and Configuring a Security Group .	-
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

3.2 Creating ECSs

3.2.1 Creating ECSs for SAP NetWeaver

Scenarios

SAP NetWeaver 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 navigation pane on the left, and choose **Computing > Elastic Cloud Server** to switch to the **Elastic Cloud Server** page.
- Step 2** Click **Buy ECS** on the right. A page for creating ECSs is displayed.
- Step 3** Configure the parameters listed in [Table 3-3](#).

Table 3-3 SAP NetWeaver 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. Select an AZ as required.

Parameter	Description
CPU Architecture	<p>The value can be x86 or Kunpeng.</p> <ul style="list-style-type: none">• x86: The X86-based CPU architecture uses Complex Instruction Set Computing (CISC). Each instruction can be used to execute low-level hardware operations, and the length of each instruction is different. Therefore, the number of instructions is large and they are complex. Therefore, executing such an instruction is complex and time-consuming.• Kunpeng: The Kunpeng-based CPU architecture uses Reduced Instruction Set Computing (RISC). RISC is a microprocessor that executes fewer types of computer instructions but at a higher speed than CISC. RISC simplifies the computer architecture and improves the running speed. Compared with the x86-based CPU architecture, the Kunpeng-based CPU architecture has a more balanced performance and power consumption ratio. Kunpeng features high density, low power consumption, high cost-effectiveness.
Specifications	Set the type of SAP NetWeaver ECSs to High-performance computing . Set the ECS specifications based on 2.2.4 Recommended ECS Planning or site requirements.
Image	Select Marketplace image and click Select Image . In the displayed Select Marketplace Image dialog box, enter SAP in the search box and select the target image.
System Disk	<p>Plan the system disk and data disk by referring to section 2.2.4 Recommended ECS Planning.</p> <p>Plan the file systems based on scenarios and recommended file system planning in section 2.1 Solution Introduction.</p>

Step 4 Click Next: Configure Network.

Configure network information for the SAP NetWeaver ECS as prompted.

Table 3-4 SAP NetWeaver ECS network configuration

Parameter	Description
Network	Choose the VPC and subnet in specified in 3.1.3 Creating a Subnet and Configuring a Security Group .
Extension NIC	Create an NIC by referring to section 2.2.5 Network Planning .
Security Group	Use the security group in section 3.1.3 Creating a Subnet and Configuring a Security Group .
EIP	Do not bind an EIP to an ECS. The SAP NetWeaver ECS on the private subnet can be accessed through the NAT server.

Step 5 Click Next: Configure Advanced Settings.

Configure parameters in advanced settings of the SAP NetWeaver ECS as prompted.

Table 3-5 SAP NetWeaver ECS advanced configuration

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>This parameter is available only when the Login Mode is set to Key pair.</p> <p>The SSH key certificate will be used for logging in to an SAP NetWeaver ECS. Ensure that the ECSs where SAP NetWeaver and NAT server are to be deployed use the same key. Otherwise, SAP NetWeaver 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>Specify an SAP NetWeaver 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 NetWeaver 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. • Distributed HA deployment: All SAP NetWeaver 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	This parameter is available only when Advanced Options is set to Configure now . You need to specify the DataproviderAccess agency for the SAP NetWeaver ECS to interconnect with Data Provider. For details about how to create an agency, see the Data Provider for SAP User Guide .

Step 6 Click **Next: Confirm**.

Confirm the configuration information about the SAP NetWeaver ECS.

Table 3-6 SAP NetWeaver ECS configuration 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 7 Click **Next** and complete the payment as prompted.

Step 8 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 9 After the SAP NetWeaver ECS is created, you can view the ECS from the ECS list on the right of the page.

Step 10 Create other SAP NetWeaver ECSs as required.

Step 11 Change the **root** password for logging in to all SAP NetWeaver 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 NetWeaver ECSs.
2. Run the following command to change the password for user **root**:

passwd

Enter the password as prompted for confirmation.

----**End**

3.2.2 Creating an ECS Used as an NAT Server

Scenarios

In the scenario where tenants access SAP NetWeaver using an NAT server (with an EIP bound), create an ECS to be used as an NAT server on the public subnet. Tenants can access SAP NetWeaver applications on the private subnet through SAP GUI installed on the NAT server. Tenants can also use SSH to access SAP NetWeaver nodes through the NAT server to locate and rectify faults.

Procedure


- Step 1** On the public cloud management console, click  in the navigation pane on the left, and choose **Computing > Elastic Cloud Server** to switch to the **Elastic Cloud Server** page.
- Step 2** Click **Buy ECS** on the right. A page for creating ECSs is displayed.
- Step 3** Configure the parameters listed in [Table 3-7](#).

Table 3-7 NAT server 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. Select an AZ as required. All SAP NetWeaver ECSs must be within the same AZ.
CPU Architecture	The value can be x86 or Kunpeng . <ul style="list-style-type: none">● x86: The X86-based CPU architecture uses Complex Instruction Set Computing (CISC). Each instruction can be used to execute low-level hardware operations, and the length of each instruction is different. Therefore, the number of instructions is large and they are complex. Therefore, executing such an instruction is complex and time-consuming.● Kunpeng: The Kunpeng-based CPU architecture uses Reduced Instruction Set Computing (RISC). RISC is a microprocessor that executes fewer types of computer instructions but at a higher speed than CISC. RISC simplifies the computer architecture and improves the running speed. Compared with the x86-based CPU architecture, the Kunpeng-based CPU architecture has a more balanced performance and power consumption ratio. Kunpeng features high density, low power consumption, high cost-effectiveness.
Specifications	Select s1.medium ECS with 1 vCPU and 4 GB or other specifications under General computing .

Parameter	Description
Image	Select Marketplace image and click Select Image . In the displayed Select Marketplace Image dialog box, enter SAP in the search box and select the target image.
System Disk	40 GB system disk For details about disk requirements, see section 2.2.4 Recommended ECS Planning .

Step 4 Click **Next: Configure Network**.

Configure network information for the NAT Server ECS as prompted.

Table 3-8 NAT server network configuration

Parameter	Description
Network	Choose the VPC and subnet in specified in 3.1.2 Applying for a VPC and 3.1.3 Creating a Subnet and Configuring a Security Group .
Extension NIC	Select a proper NIC according to the information provided in section 2.2.5 Network Planning .
Security Group	Use the security group in section 3.1.3 Creating a Subnet and Configuring a Security Group .
EIP	Select Automatically Assign .
EIP Type	This parameter is available only when EIP is set to Auto assign . Set this parameter based on the site requirements. <ul style="list-style-type: none"> • Dynamic BGP provides automatic failover and load balancing capabilities and makes better routing decisions based on optimal paths when a network connection fails. • When changes occur on a network using static BGP, network configurations cannot be promptly adjusted to ensure optimal user experience.

Parameter	Description
Billed By	<p>This parameter is available only when EIP is set to Auto assign. Billed by indicates the bandwidth billing mode of the purchased EIP, which includes the following options:</p> <ul style="list-style-type: none">• Bandwidth: The billing will be based on the duration for which the bandwidth is used.• Traffic: The billing will be based on the total traffic irrespective of the duration for which the bandwidth is used.• Shared bandwidth: The bandwidth can be used by multiple EIPs. <p>NOTE</p> <ul style="list-style-type: none">- A bandwidth can be shared between a limited number of EIPs. If the number of EIPs cannot meet service requirement, switch to a higher shared bandwidth or apply for expanding the EIP quota of the existing bandwidth.- EIPs that are billed yearly/monthly do not support shared bandwidths.- When a shared bandwidth that is billed yearly/monthly expires, the system automatically deletes the bandwidth configuration and creates a dedicated bandwidth billed by traffic for the EIPs sharing the deleted bandwidth configuration.
Bandwidth Size	<p>This parameter is available only when EIP is set to Auto assign. Set this parameter based on the site requirements.</p>

Step 5 Click **Next: Configure Advanced Settings**.

Configure parameters in advanced settings of NAT Server ECS as prompted.

Table 3-9 NAT server advanced configuration

Parameter	Description
ECS Name	<p>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.</p>
Login Mode	Select Key pair .

Parameter	Description
Key Pair	<p>This parameter is available only when the Login Mode is set to Key pair.</p> <p>Key Pair is recommended. A Secure Shell (SSH) key certificate is used for authenticating users who attempt to log in to SAP application ECSs. Ensure that the ECSs where SAP NetWeaver and NAT server are to be deployed use the same key. Otherwise, SAP NetWeaver 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.
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.

Step 6 Click Next: Confirm.

Confirm the NAT Server ECS configuration as prompted.

Table 3-10 NAT server configuration 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 7 Click **Next** and complete the payment as prompted.

Step 8 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.

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

----End

3.3 Configuration Before Installation

3.3.1 Configuring SSH Switching Permissions

Scenarios

To allow SSH switchovers between SAP NetWeaver 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 NFS 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 NetWeaver 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 NetWeaver 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

3.3.2 Modifying OS Configurations

Scenarios

To ensure the proper installation of the SAP NetWeaver 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 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 SAP NetWeaver nodes.
----End

3.3.3 Attaching a Shared Disk and Binding a Floating IP Address (Distributed HA Deployment)

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 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** On the management console, choose **Compute > Elastic Cloud Server**. The page showing the ECS list is displayed.
- Step 2** Click the name of the active ASCS ECS.
- Step 3**
- Step 4** On the displayed page, click **Attachments** and then **Attach**. The **Attach Disk** page is displayed.
- Step 5** On the **Attach Disk** page, select the target standby ASCS ECS, ensure that its **Mount Point** is the same as the **Device Name** in **Step 4**, and click **OK**.

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** Click **Assign Virtual IP Address**, select the assignment mode as required, and click **OK**. Assign two virtual IP addresses for the switchover between the active and standby ASCS ECSs.
- 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 NetWeaver ECSs to the **/etc/hosts** file. The following uses the active and standby ASCS nodes as an example.

10.0.3.52	netweaver-0001
10.0.3.196	netweaver-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 NetWeaver ECSs.

----End

3.4 Installing SAP NetWeaver

3.4.1 Formatting a Disk

Scenarios

The data disks of SAP NetWeaver 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 in the distributed HA deployment within an AZ. The shared disk of the active ASCS node needs to be formatted based on [Table 2-11](#).

 **NOTE**

- On the ECS homepage, choose **Learn more > Getting Started > Initializing an EVS Disk (Linux)** 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 NetWeaver 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 2-11](#), 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.

 NOTE

- For details about file systems in the standard deployment mode, see [Table 2-1](#).
- For details about file systems in the distributed deployment mode, see [Table 2-3](#).

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 NetWeaver, **00** is the **Instance Number** of ASCS, and **10** is the **Instance Number** of ERS.

Step 4 Save the changes and exit.

----End

3.4.2 Attaching an SFS Turbo File System to an ECS

Scenarios

In distributed deployment and distributed HA deployment scenarios, the created SFS Turbo file system need to be attached to the ECS. This section describes how to attach the SFS Turbo file system in the distributed HA deployment scenario. For details, see [Table 2-12](#).

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 -qa|grep 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 2-12](#):

```
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 `sdcc` to the `fstab` file because the two partitions will be automatically attached when the HA function of SAP NetWeaver 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

3.4.3 Installing the SAP NetWeaver Software

Before installing SAP NetWeaver, modify the configuration file on the ECS where SAP NetWeaver is to be deployed. For details, see [5.1 What Should I Do If a SAP Application on an ECS Cannot Be Started?](#)

Install SAP NetWeaver 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/>

3.4.4 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 NetWeaver.

NOTE

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

3.4.5 Interconnecting SAP GUI with SAP NetWeaver

After installing SAP GUI, configure the SAP GUI, interconnect it with SAP NetWeaver, and then log in to the SAP GUI to process routine services. For details, see SAP documents.

3.4.6 Configuring the HA Function for SAP NetWeaver (Distributed HA Deployment)

Scenarios

To prevent the SAP NetWeaver from being affected by a single point of failure and improve the availability of the SAP NetWeaver, configure HA for the active and standby ASCS nodes of SAP NetWeaver. This operation is required only in the distributed HA deployment scenario.

In the cross-AZ HA scenario, three ECSs are required. Each ECS is bound to the same shared SCSI disk and iSCSI configuration is required for SBD. For details, see section [3.5 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 [3.3.2 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 NetWeaver instance.
 - Log in to the active and standby ASCS nodes one by one and modify the **/etc/hosts** file:

vi /etc/hosts

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

```
10.0.3.52 netweaver-0001
10.0.3.196 netweaver-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.
- Ensure that the dependency packages **patterns-ha-ha_sles** and **sap-suse-cluster-connector** have been installed.

Run the following commands to check whether the dependency packages have been installed:

```
rpm -qa | grep patterns-ha-ha_sles
```

```
rpm -qa | grep sap-suse-cluster-connector
```

If no, run the following commands:

```
zypper in -y patterns-ha-ha_sles
```

```
zypper in -y sap-suse-cluster-connector
```

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.

CN-Hong Kong: `wget https://obs-sap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip -P /sapmnt`

AP-Bangkok: `wget https://obs-sap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip -P /sapmnt`

AF-Johannesburg: `wget https://obs-sap-af-south-1.obs.af-south-1.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip -P /sapmnt`

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 3-11](#) describes the parameters in the file.

Table 3-11 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
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

Type	Name	Description
	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. A maximum of 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.

```

cldusternode0:~/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 cldusternode0
Stack: corosync
Current DC: cldusternode0 (version 1.1.13-10.4-6f22ad7) - partition with quorum
2 nodes and 7 resources configured

Online: [ cldusternode0 cldusternode1 ]

Full list of resources:

stonith-sbd (stonith:external/sbd): Started cldusternode0
Resource Group: grp_ASCS
  rsc_ip_ASCS (ocf::heartbeat:IPaddr2): Started cldusternode0
  rsc_fs_ASCS (ocf::heartbeat:Filesystem): Started cldusternode0
  rsc_sap_ASCS (ocf::heartbeat:SAPInstance): Started cldusternode0
Resource Group: grp_ERS
  rsc_ip_ERS (ocf::heartbeat:IPaddr2): Started cldusternode1
  rsc_fs_ERS (ocf::heartbeat:Filesystem): Started cldusternode1
  rsc_sap_ERS (ocf::heartbeat:SAPInstance): Started cldusternode1
    
```

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

----End

3.4.7 Installing Data Provider

Install Data Provider on all cloud servers so that SAP technical support personnel can use this software to collect information of the platform where the cloud servers run, facilitating fault identification and analysis if the SAP system is faulty or the system performance deteriorates.

NOTE

On the server where SAP NetWeaver is deployed, you must specify the **DataproviderAccess** agency for the ECSs created on the server. In addition, install Data Provider on the server.

Procedure

Step 1 Log in to all cloud servers.

Step 2 Run the following command to check whether Data Provider has been installed:

systemctl status hwdataproviderp3

The command output is similar to the following. If the value of **Active** is **active (running)**, Data Provider has been successfully installed. Otherwise, follow the operations described in the [Data Provider for SAP User Guide](#) to install it.

```
SAPTest:~ # systemctl status hwdataproviderp3
● hwdataproviderp3.service - Huawei dataprovider monitor service daemon
   Loaded: loaded (/etc/systemd/system/hwdataproviderp3.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2020-01-09 16:10:00 CST; 1 weeks 4 days ago
     Process: 43653 ExecStop=/bin/kill -HUP (code=exited, status=1/FAILURE)
    Main PID: 43688 (python3)
      Tasks: 3 (limit: 512)
   CGroup: /system.slice/hwdataproviderp3.service
           └─43688 /usr/bin/python3 /opt/huawei/dataprovider/dataprovider_linux.py > /dev/null 2>&1

Jan 09 16:10:00 host-192-168-230-179 systemd[1]: Started Huawei dataprovider monitor service daemon.
```

----End

3.5 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 NetWeaver and SAP HANA can be deployed on the same ECS. [Table 3-12](#) lists the ECS specifications.

If SAP NetWeaver is deployed across three AZs, create an ECS in each AZ. If SAP NetWeaver 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 3-12 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-lio-server targetcli
```

Step 2 Run the following command to install open-iscsi on the client side (SAP NetWeaver 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/lblock 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 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:

```
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 NetWeaver node (client side) and attach the iSCSI disk of a server side ECS to the SAP NetWeaver 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 NetWeaver 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 NetWeaver 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 NetWeaver nodes and repeat **Step 14** to **Step 15** to configure all SAP NetWeaver nodes of the client side.

----End

4 Backup and Restoration

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

- SAP NetWeaver 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 NetWeaver system using VBS in the standby AZ.
To implement DR restoration, you need to install SAP NetWeaver 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*.

5 FAQs

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

5.1 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
2020-01-17	This issue is the eighth official release, which incorporates the following changes: Added C6 ECS specifications.
2019-03-30	This issue is the seventh official release, which incorporates the following changes: Added the description about SFS Turbo required for distributed deployment.
2018-11-16	This issue is the sixth official release, which incorporates the following change: Added memory-optimized M3 ECSs. For details, see Table 2-9 .
2018-09-03	This issue is the fifth official release, which incorporates the following change: Supported automatic deployment of the ASCS HAE using scripts.
2018-08-20	This issue is the fourth official release, which incorporates the following changes: Updated the network planning information.
2018-03-30	This issue is the third official release, which incorporates the following changes: <ul style="list-style-type: none">• Optimized operations on formatting disks.• Optimized the HA function of SAP NetWeaver.• Added the description of configuring shared disks, for example, iSCSI configuration in the cross-AZ HA deployment scenario.• Added the description of cross-AZ and cross-region DR.

Released On	What's New
2018-01-24	This issue is the second official release, which incorporates the following changes: <ul style="list-style-type: none">• Added description about the HAE automatic switchover.• Add description about the SFS file sharing system.• Modified the installation scheme to the distributed HA deployment.
2018-01-08	This issue is the first official release.