

SAP HANA User Guide (Single Node)

SAP HANA User Guide (Single Node)

Issue 01
Date 2022-12-07



Copyright © Huawei 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 Technologies Co., Ltd.

Trademarks and Permissions



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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: <https://www.huawei.com>

Email: support@huawei.com

Contents

1 Introduction.....	1
1.1 About This Document.....	1
1.2 Node and Role.....	1
1.3 Scale-up and Scale-out.....	4
2 Deployment.....	5
2.1 Scheme.....	5
2.1.1 Scheme Introduction.....	5
2.1.2 Single-Node Scenario Where HA Is Not Required.....	7
2.1.3 Single-Node Scenario Where HA Is Required.....	8
2.2 Data Planning.....	10
2.2.1 SAP HANA Nodes.....	10
2.2.2 Other Nodes.....	13
2.2.3 Network Planning.....	14
2.3 Preparing Resources.....	19
2.3.1 Software and Tools.....	19
2.3.2 License.....	20
2.3.3 Creating a VPC.....	20
2.3.4 Creating a Subnet and Configuring a Security Group.....	23
2.4 Creating ECSs.....	25
2.4.1 Creating an SAP HANA ECS.....	25
2.4.2 Creating an SFS File System.....	30
2.4.3 Creating an SAP HANA Studio ECS.....	32
2.4.4 Creating an NAT ECS.....	37
2.4.5 Configuring SSH Switching Permissions.....	41
2.4.6 Configuring the Mapping Between SAP HANA Host Names and IP Addresses.....	42
2.5 Installing SAP HANA (Single-Node Deployment Without HA Required).....	44
2.5.1 Formatting a Disk.....	44
2.5.2 Installing the SAP HANA Software.....	46
2.5.3 Installing the SAP HANA Studio on a Windows ECS.....	50
2.5.4 Installing the SAP HANA Studio on a Linux ECS.....	51
2.5.5 Connecting SAP HANA Nodes to the SAP HANA Studio.....	52
2.5.6 Configuring the Backup Path.....	57
2.5.7 Configuring SAP HANA Storage Parameters.....	59

2.5.8 Installing Data Provider.....	60
2.6 Installing SAP HANA (Single-Node Deployment with HA Required).....	61
2.6.1 Formatting a Disk.....	61
2.6.2 Installing the SAP HANA Software.....	63
2.6.3 Installing the SAP HANA Studio on a Windows ECS.....	67
2.6.4 Installing the SAP HANA Studio on a Linux ECS.....	68
2.6.5 Connecting SAP HANA Nodes to the SAP HANA Studio.....	69
2.6.6 Configuring the Backup Path.....	74
2.6.7 Configuring the System Replication.....	76
2.6.8 Configuring HA on SAP HANA Nodes.....	79
2.6.9 Configuring SAP HANA Storage Parameters.....	82
2.6.10 Installing Data Provider.....	83
2.6.11 Configuring iSCSI (Cross-AZ HA Deployment).....	83
3 Management and Monitoring.....	87
4 Backing Up and Restoring Data.....	88
4.1 Constraint.....	88
4.2 Obtaining the Backup Size.....	88
4.3 Configuring the Backup Path.....	89
4.4 Creating a Backup Task.....	89
4.5 Canceling a Backup Task.....	92
4.6 Checking Backup File Integrity.....	92
4.7 Restoring SAP HANA Data.....	94
5 FAQs.....	97
5.1 How Do I Start and Stop an ECS Instance?.....	97
5.2 How Do I Connect to the SAP HANA Database?.....	98
5.3 How Do I Check the Port of the SAP HANA Database Server?.....	98
5.4 What Should I Do If I Cannot Switch to an ECS or HANA ECS Using SSH?.....	99
6 Appendix.....	100
6.1 Obtaining the Password for Logging In to a Windows ECS.....	100
6.2 Logging In to a Linux ECS Using an SSH Key.....	101
6.3 Querying the NIC IP Address of an ECS.....	102
6.4 Modifying OS Configurations.....	103
6.5 Obtaining the Key File of an ECS.....	104
A Change History.....	105

1 Introduction

[1.1 About This Document](#)

This document provides instructions for you to prepare resources (such as ECSs and network resources) and install SAP HANA.

[1.2 Node and Role](#)

An SAP HANA system consists of one or more SAP HANA nodes.

[1.3 Scale-up and Scale-out](#)

SAP HANA nodes can be expanded in the scale-up or scale-out mode.

1.1 About This Document

This document provides instructions for you to prepare resources (such as ECSs and network resources) and install SAP HANA.

If you have any trouble in installing and using SAP HANA due to its own problems, contact the SAP technical support.

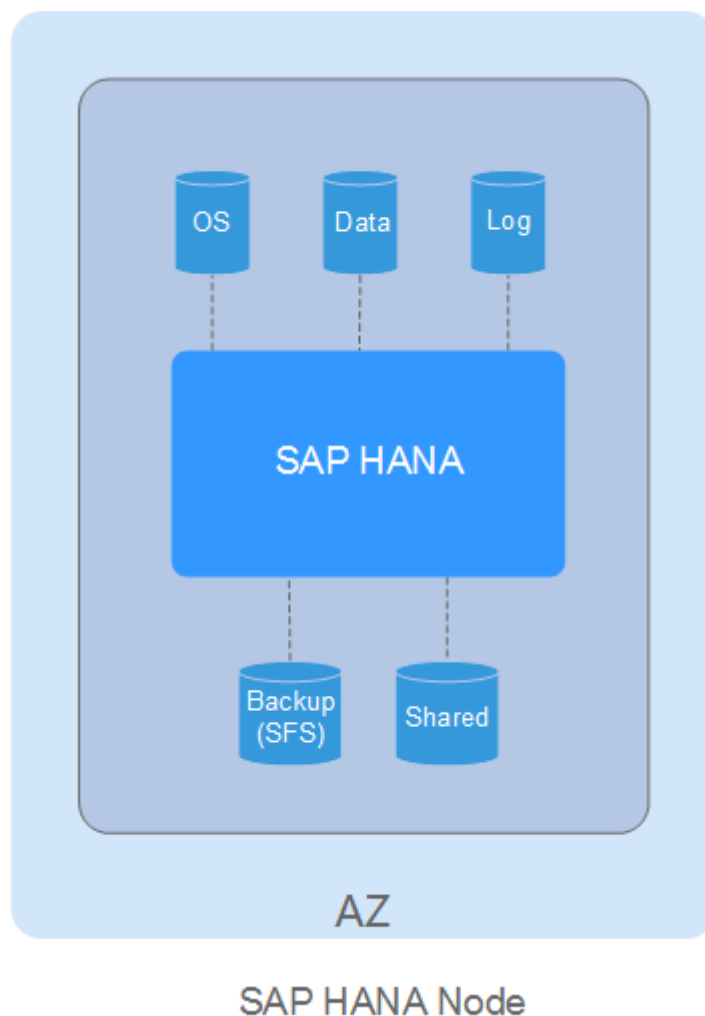
1.2 Node and Role

An SAP HANA system consists of one or more SAP HANA nodes.

SAP HANA Node

SAP HANA nodes are logical units that constitute an SAP HANA system. An SAP HANA node contains the CPU, memory, and storage (such as log, data, shared, and backup volumes) resources with specified specifications, as shown in [Figure 1-1](#).

Figure 1-1 SAP HANA node



SAP HANA Studio

SAP HANA Studio provides management, monitoring, and information modeling of the SAP HANA system. It can also function as a client and provides capabilities to access user data. The information that the SAP HANA Studio provides includes the system information (such as software version), alarm information (generated by Statistics Server), 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 HANA node from the NAT server using Secure Shell (SSH).

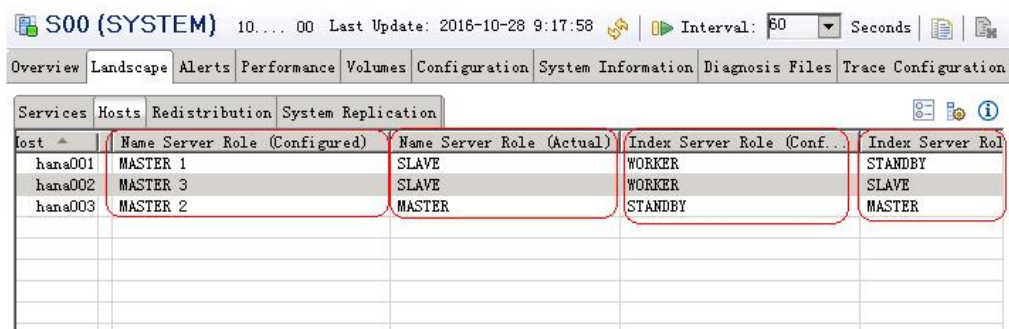
SFS

Scalable File Service (SFS) provides the file sharing service. Create a file system to provide the backup volumes and the shared path to SAP HANA nodes.

SAP HANA Roles

In SAP HANA cluster deployment mode, the roles assigned to SAP HANA nodes are shown in [Figure 1-2](#).

Figure 1-2 Roles assigned to SAP HANA nodes



Host	Name Server Role (Configured)	Name Server Role (Actual)	Index Server Role (Conf.)	Index Server Role
hana001	MASTER 1	SLAVE	WORKER	STANDBY
hana002	MASTER 3	SLAVE	WORKER	SLAVE
hana003	MASTER 2	MASTER	STANDBY	MASTER

Each SAP HANA node has the NameServer and IndexServer processes. [Table 1-1](#) provides the roles of the processes.

Table 1-1 SAP HANA roles

Process	Type	Description
NameServer	Configured Role	Initially configured roles <ul style="list-style-type: none"> • Master: functions as a global transaction coordinator, which coordinates global transactions and stores the global metadata of the information about the computing node cluster. A cluster has three master nodes configured, but only one of them is activated. • Slave: An SAP HANA cluster can have one or more slave nodes configured in a distributed architecture to cache metadata and perform database operations assigned by the master node. A cluster has multiple slave nodes.
	Actual Role	Activated roles due to the election mechanism <ul style="list-style-type: none"> • Master: activated master node elected from the configured master nodes • Slave: nodes except master nodes

Process	Type	Description
IndexServer	Configured Role	Initially configured roles <ul style="list-style-type: none">• Worker: nodes that are running and performing database operations• Standby: takes over services of a faulty node. A cluster can have no or any number of standby nodes, and one standby node by default. In normal cases, software on the node is running, but the node's memory database has no data and cannot process services. The standby node takes over services of a faulty node automatically.
	Actual Role	Activated roles due to the election mechanism <ul style="list-style-type: none">• Master: node elected from worker nodes. It is the same as the master node in Name Server.• Slave: worker nodes except the master nodes• Standby: same as parameter Config Role in Index Server. Any node can be the standby node due to multiple times of service switchovers.

1.3 Scale-up and Scale-out

SAP HANA nodes can be expanded in the scale-up or scale-out mode.

- Scale-up mode

Also called single-node system mode, in which an SAP HANA system contains only one valid node. If high availability (HA) is required, construct such architecture using two single nodes through System Replication. This system architecture supports only scale-up expansion. In this mode, add CPUs, memory capacity, and hard disks to the node.

The system does not support expansion for a node on which SAP HANA is running.
- Scale-out mode

Also called cluster system mode, in which an SAP HANA system contains multiple nodes. In scale-out mode, when the system requires expansion, add more nodes to the system.

2 Deployment

- [2.1 Scheme](#)
- [2.2 Data Planning](#)
- [2.3 Preparing Resources](#)
- [2.4 Creating ECSs](#)
- [2.5 Installing SAP HANA \(Single-Node Deployment Without HA Required\)](#)
- [2.6 Installing SAP HANA \(Single-Node Deployment with HA Required\)](#)

2.1 Scheme

2.1.1 Scheme Introduction

This document describes how to deploy SAP HANA systems within an AZ. For details about cross-AZ and cross-region HA and DR deployment, see the [SAP HA and DR Guide](#).

SAP HANA can be deployed in the following scenarios:

- Single-node deployment: applies in OLTP scenarios. You can choose HA configuration as required. SAP HANA receives and processes data quickly, provides processing results in a short period of time, and rapidly responds to user operations.
- Cluster deployment: applies in OLAP scenarios. As a data warehouse, SAP HANA offers support for decision-makers and senior managers. It can quickly and flexibly process complex queries on a large amount of data based on the analysts' requests. It can also provide decision makers with the query results intuitively and clearly. Using SAP HANA, decision makers can obtain accurate information about the enterprise operating status, learn object demands, and make correct decisions.

Table 2-1 lists recommended deployment modes based on systems.

- Production (PRD): indicates the production system where SAP HANA is formally used.

- **Quality Assure (QAS):** indicates the quality assurance system where SAP HANA functions, performance, and reliability are fully verified.
- **Development (DEV):** indicates the development system where development engineers configure and verify the compatibility between application software and SAP HANA and continuously optimize the application software.
- **Training (TRN):** indicates the training and demonstration system where you provide a training or demonstration after deploying SAP HANA.
- **Test (TST):** indicates the test system where the development engineers test the compatibility between application software and SAP HANA to verify the functions of application software after the application software development is complete.

 **NOTE**

In Suite on HANA (SoH) scenario, SAP HANA works with SAP business suites, such as Enterprise Resource Planning (ERP) or Customer Requirement Management (CRM). In this scenario, SAP HANA provides OLTP functions. The SAP HANA process latency is the key concern.

In Business Warehouse on HANA (BWoH) scenario, SAP HANA works with SAP Business Warehouse. In this scenario, SAP HANA provides OLAP functions and supports rapid computing and analyzing on massive data. The SAP HANA processing performance and the network bandwidths between SAP HANA nodes are the key concern.

Table 2-1 Systems and deployment schemes

System	SoH	BWoH (Single-Node)
PRD	Single-node scenario where HA is required	Single-node scenario where HA is required
QAS	Single-node scenario, regardless of whether HA is required or not	Single-node scenario, regardless of whether HA is required or not
DEV	Single-node scenario where HA is not required	Single-node scenario where HA is not required
TRN	Single-node scenario where HA is not required	Single-node scenario where HA is not required
TST	Single-node scenario where HA is not required	Single-node scenario where HA is not required

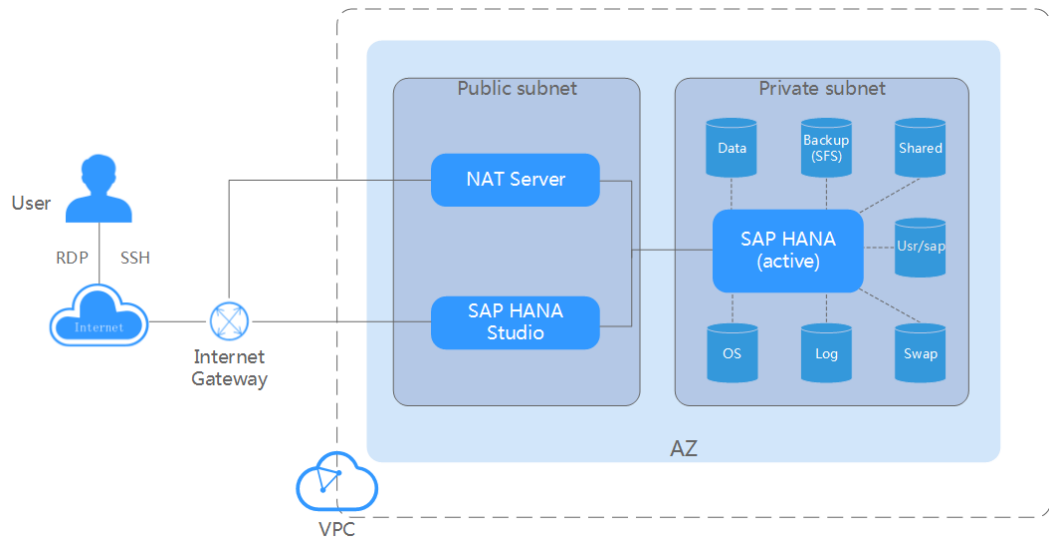
Before installing the SAP HANA, you must plan the following data:

- **Data of SAP HANA nodes:** includes the OSs, specifications, and disk capacities of the SAP HANA nodes used in SoH and BWoH scenarios.
- **Data of other nodes:** includes the OSs, specifications, and disk capacities of the SAP HANA Studio and NAT server.
- **Network data:** includes subnets and security group rules.
- **SAP HANA installation data:** planned based on SAP HANA requirements.

2.1.2 Single-Node Scenario Where HA Is Not Required

Figure 2-1 shows the single-node scenario where HA is not required.

Figure 2-1 Single-node scenario where HA is not required



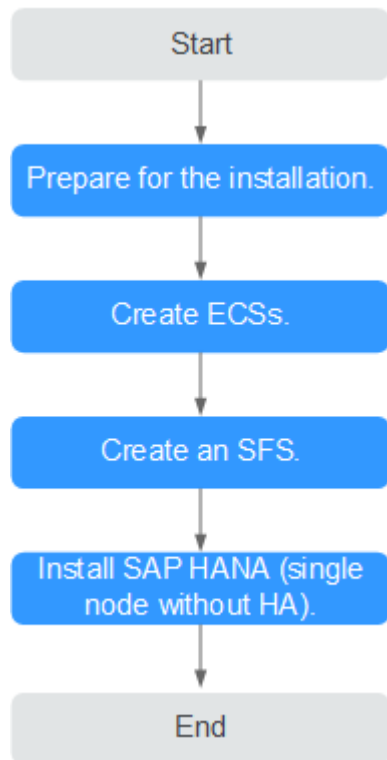
The concepts involved in the preceding figures are as follows:

- VPC network: All SAP HANA nodes are deployed within a VPC network, and all nodes in the HANA system belong to the same AZ to ensure network security.
- Public subnet:
 - Network Address Translation (NAT) instance ECS: allows you to access SAP HANA nodes using SSH.
 - SAP HANA Studio ECS: runs the SAP HANA Studio software. You can use RDP or SSH to access the SAP HANA Studio ECS and manage the SAP HANA system.
- Private subnet:
 - SAP HANA node: used for deploying the SAP HANA software. An SAP HANA server has the following disks attached:
 - OS disk: provides the directory for installing the OS.
 - Data volume: periodically stores the data transmitted from the SAP HANA IMDB (a database running in high-performance memory). The period is 5 minutes by default.
 - Log volume: stores the data triggered by an event. When an event, for example, a record or a batch of records are updated, is triggered for the server IMDB, the system will write the latest IMDB data into the log volume.
 - Shared volume: stores the SAP HANA installation software and SAP HANA database log files.
 - Backup volume: stores SAP HANA database backup files.
 - Usr/sap: used to mount to the **/usr/sap** directory.

- Swap volume: Linux swap space.

Figure 2-2 shows the deployment flowchart.

Figure 2-2 Single-node scenario where HA is not required



2.1.3 Single-Node Scenario Where HA Is Required

Figure 2-3 and Figure 2-4 show the single-node scenario where HA is required.

NOTE

In the single-node scenario where HA is required, active/standby switchovers can be manually performed, or automatically performed using scripts.

Figure 2-3 Single-node HA deployment within an AZ

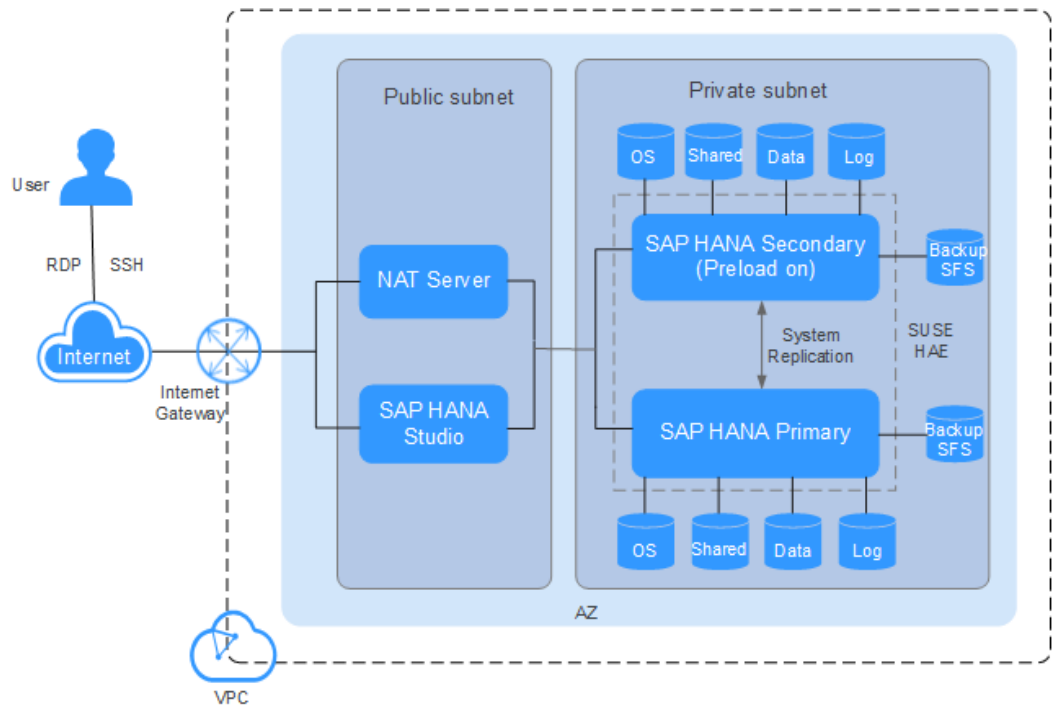
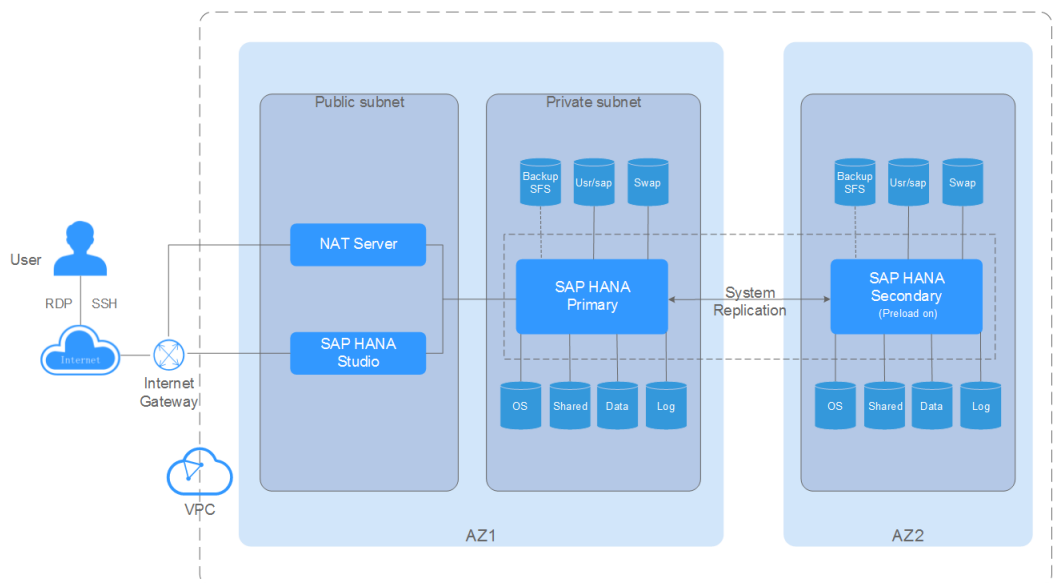


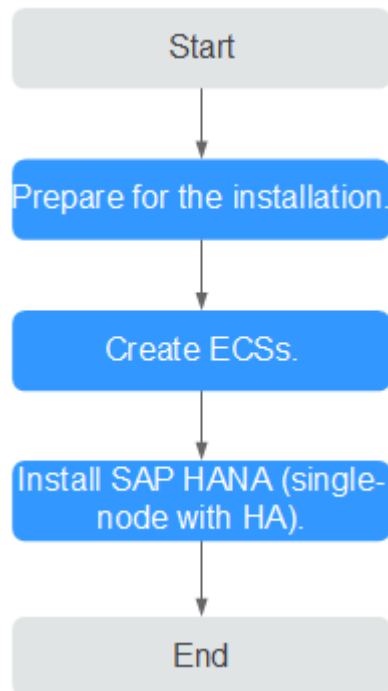
Figure 2-4 Single-node HA deployment across AZs



The concepts involved in this scenario are the same as those involved in [2.1.2 Single-Node Scenario Where HA Is Not Required](#). The differences between the two deployment modes are as follows: Two independent SAP HANA nodes in the same AZ or different AZs are connected to the SAP HANA Studio for management. The two SAP HANA nodes synchronize data and implement HA using System Replication.

Figure 2-5 shows the deployment flowchart in the single-node scenario where HA is required.

Figure 2-5 Deployment flowchart in the single-node scenario where HA is required



Compared with the mode in which HA is not required in the single-node scenario, the mode in which HA is required has the following requirements:

- You must create two servers and synchronize time, format disks, and install the SAP HANA software on them.
- The two HANA ECSs must connect to SAP HANA Studio.
- You must manually configure HA on the two SAP HANA nodes using System Replication.
- You must configure scripts for the two SAP HANA nodes for active/standby switchovers.

This only applies to SAP HANA nodes running the OS SUSE Linux Enterprise Server 12 SP1 for SAP or later.

- In the single-node scenario where SAP HANA nodes are deployed across AZs for HA, three ECSs are required. To support the Split Brain Detection (SBD) function, each ECS is bound to a SCSI disk and iSCSI configuration is required for SBD. For details, see [2.6.11 Configuring iSCSI \(Cross-AZ HA Deployment\)](#).

2.2 Data Planning

2.2.1 SAP HANA Nodes

SAP poses specific requirements on HANA ECSs depending on application scenarios.

 NOTE

The time zone of the server on which SAP NetWeaver is deployed must be the same as that of SAP HANA nodes, excepting the specifications described in this section.

Specifications in SoH Scenario

In SoH scenario, SAP HANA works with SAP business suites, such as ERP or CRM. In this scenario, SAP HANA provides OLTP functions. The SAP HANA process latency is the key concern.

Table 2-2 lists the specifications of HANA ECSs certified by SAP on HUAWEI CLOUD.

Table 2-2 Large-memory E3 ECS specifications

ECS Type	vCPUs	Memory (GB)	Flavor
Large-memory	28	348	e3.7xlarge.12
	56	696	e3.14xlarge.12

Table 2-3 Memory-optimized M6 ECS specifications

ECS Type	vCPUs	Memory (GB)	Flavor
Memory-optimized	32	256	m6.8xlarge.8
	64	512	m6.16xlarge.8

Specifications in BWoH Scenario

In BWoH scenario, SAP HANA works with SAP Business Warehouse. In this scenario, SAP HANA provides OLAP functions and supports rapid computing and analyzing on massive data. The SAP HANA processing performance and the network bandwidths between SAP HANA nodes are the key concern.

Table 2-4 lists the specifications of HANA ECSs certified by SAP on HUAWEI CLOUD.

Table 2-4 Large-memory E3 ECS specifications

ECS Type	vCPUs	Memory (GB)	Flavor
Large-memory	28	348	e3.7xlarge.12
	56	696	e3.14xlarge.12

Requirements on OSs and Disks

 **NOTE**

- SAP HANA ECS volumes include log volumes, data volumes, shared volumes, backup volumes, and /usr/sap volumes.
- A shared disk can be attached to multiple ECSs, while a non-shared disk can only be attached to one ECS.

Table 2-5 Requirements on HANA ECS OS in single-node deployment scenarios

Scenario	Specifications
OS	<ul style="list-style-type: none"> • SUSE Linux Enterprise Server for SAP Applications 12 SP3 • SUSE Linux Enterprise Server for SAP Applications 12 SP4 • SUSE Linux Enterprise Server for SAP Applications 12 SP5 • SUSE Linux Enterprise Server for SAP Applications 15 • SUSE Linux Enterprise Server for SAP Applications 15 SP1

 **NOTE**

In the same AZ HA scenario, to prevent split-brain, you need to create an EVS disk for an SAP HANA node and use it as the SBD volume. After the EVS disk is created, bind it to another SAP HANA node.

In the cross-AZ HA scenario, you do not need to create SBD volumes for SAP HANA nodes. For details, see [2.6.11 Configuring iSCSI \(Cross-AZ HA Deployment\)](#).

Table 2-6 Requirements on E3 ECS disks in single-node deployment scenarios

Disk	Type	Sharing Mode	Size
OS volume	High I/O	Non-shared disk	N/A
Log volume	Ultra-high I/O	Non-shared disk	For details, see Table 2-7 .
Data volume	Ultra-high I/O	Non-shared disk	Create an EVS disk. Use LVM to create soft partitions and logically divide the disk into data volumes. For details, see Table 2-7 .
Shared volume	High I/O	Non-shared disk	The recommended size is at least 1.2 times that of the memory size.
Backup volume	SFS	N/A	The recommended capacity is three times or more of the memory size.

Disk	Type	Sharing Mode	Size
SBD volume	High I/O	Shared disk (SCSI)	10 GB
/usr/sap volume	High I/O	Non-shared disk	100 GB
Swap volume	High I/O	Non-shared disk	10 GB

Table 2-7 Recommended log and data volume specifications for E3 ECSs

Flavor	Log Volume Size (GB)	Data Volume Size
e3.7xlarge.12	200	2 x 250 GB EVS disks
e3.14xlarge.12	512	2 x 450 GB EVS disks

2.2.2 Other Nodes

Other nodes include the NAT server and SAP HANA Studio nodes.

Table 2-8 lists the requirements on these nodes.

Table 2-8 Data planning for other nodes

Node	Specifications
SAP HANA Studio	<ul style="list-style-type: none"> • OS: <ul style="list-style-type: none"> NOTE Based on service requirements, use a Windows or Linux ECS to deploy SAP HANA Studio. – Windows: Windows Server 2012 R2 or Windows Server 2008 R2 – Linux: SUSE Linux Enterprise Server (SLES) 12 SP2 or later • Flavor: s1.xlarge (4 vCPUs and 16 GB memory capacity) • System disk: High I/O and 80 GB
NAT server	<ul style="list-style-type: none"> • OS: SUSE Linux Enterprise Server (SLES) 12 SP2 or later • Flavor: s1.medium (1 vCPU and 4 GB memory capacity) or higher • System disk: High I/O and 40 GB

2.2.3 Network Planning

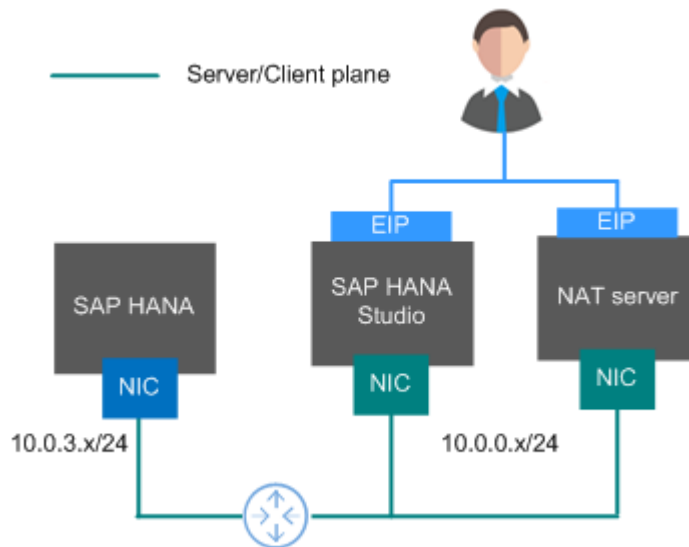
Network Plane in the Single-Node Scenario Where HA Is Not Required

Figure 2-6 shows the network plane planning in the single-node scenario where HA is not required.

NOTE

The network segments and IP addresses are for reference only.

Figure 2-6 Network plane in the single-node scenario where HA is not required



Planning description

- In this scenario, each node uses only one NIC to form the network communication plane.
- **Table 2-9** shows the planned network.

Table 2-9 Network planning in the single-node scenario where HA is not required

Parameter	Description	Example Value
IP address of the server/client plane	Allows an SAP HANA node to communicate with service software (such as SFS and ERP) or SAP HANA Studio client software.	SAP HANA node: 10.0.3.2 SAP HANA Studio: 10.0.0.102 NAT server: 10.0.0.202
Elastic IP address	Allows you to access SAP HANA Studio and NAT server.	Automatically allocated

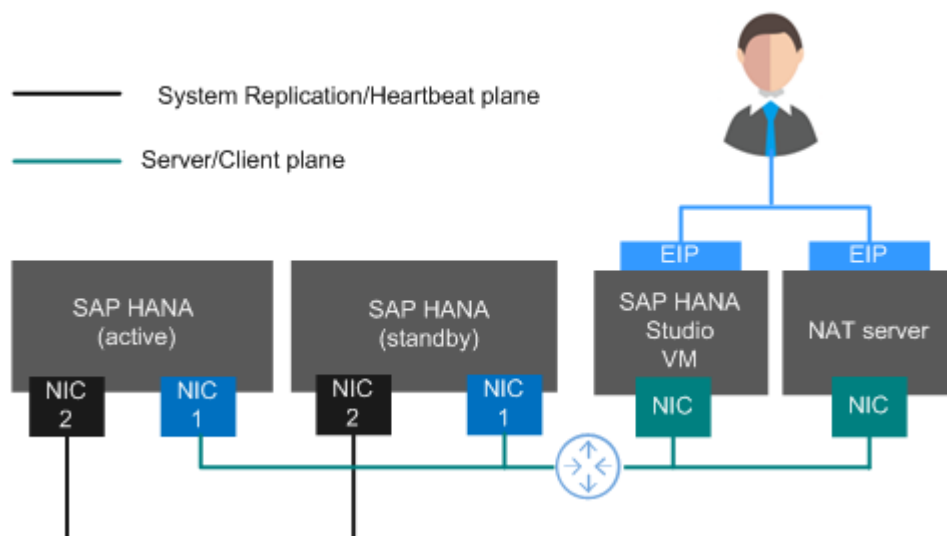
Network Plane in the Single-Node Scenario Where HA Is Required

Figure 2-7 shows the network plane planning in the single-node scenario where HA is required.

NOTE

- The network segments and IP addresses are for reference only.
- **Figure 2-7** applies to performing active/standby switchovers using scripts. If active/standby switchovers are manually performed, no heartbeat plane NIC is required.
- IP addresses of the server plane (server/client plane IP address) and the active/standby internal communication plane (System Replication communication plane IP address and heartbeat plane IP address) must belong to different subnets.

Figure 2-7 Network plane in the single-node scenario where HA is required



Planning description

- The active and standby SAP HANA nodes both have an NIC1 and an NIC2 card. The two NIC1 cards are in the same network segment and belong to the service/client plane. The two NIC2 cards are in another network segment and belong to the system replication/heartbeat plane.
- **Table 2-10** shows the planned network.

Table 2-10 Network planning in the single-node scenario where HA is required

Parameter	Description	Example Value
IP address of the server/client plane	Specifies the IP address of the primary NIC plane. Allows an SAP HANA node to communicate with service software (such as SFS and ERP) or SAP HANA Studio client software.	SAP HANA node: 10.0.3.2 to 10.0.3.3 SAP HANA node floating IP address: 10.0.3.103 SAP HANA Studio: 10.0.0.102 NAT server: 10.0.0.202
IP address of the System Replication communication plane	Specifies the IP address of the plane that SAP HANA nodes use to implement System Replication.	SAP HANA node: 10.0.4.2 to 10.0.4.3
IP address of the heartbeat plane	Specifies the IP address of the plane that SAP HANA nodes use to transmit heartbeat signals to perform automatic active/standby switchovers when a node is faulty.	
Elastic IP address	Allows you to access SAP HANA Studio and NAT server.	Automatically allocated

Security Group Rules

 **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 HANA instance ID, such as 00. Ensure that this ID is the same as the instance ID specified when you install the SAP HANA software.
- For more information about specific ports and security group rules to be accessed by SAP, see [SAP official documents](#).

Table 2-11 Security group rules (SAP HANA)

Source/ Destination	Protocol	Port Range	Description
Inbound			

Source/ Destination	Protocol	Port Range	Description
10.0.0.0/24	TCP	3##13	Allows SAP HANA Studio to access SAP HANA.
10.0.0.0/24	TCP	3##15	Provides ports for the service plane.
10.0.0.0/24	TCP	3##17	Provides ports for the service plane.
10.0.0.0/24	TCP	5##13	Allows SAP HANA Studio to access sapstartsrv.
10.0.0.0/24	TCP	22	Allows SAP HANA to be accessed using SSH.
10.0.0.0/24	TCP	43##	Allows access to XS Engine from the 10.0.0.0/24 subnet using HTTPS.
10.0.0.0/24	TCP	80##	Allows access to XS Engine from the 10.0.0.0/24 subnet using HTTP.
10.0.0.0/24	TCP	8080 (HTTP)	Allows Software Update Manager (SUM) to access SAP HANA using HTTP.
10.0.0.0/24	TCP	8443 (HTTPS)	Allows Software Update Manager (SUM) to access SAP HANA using HTTPS.
10.0.0.0/24	TCP	1128-1129	Allows access to SAP Host Agent using SOAP/HTTP.
Automatically specified by the system	All	All	Security group rule created by the system by default It enables ECSs in the same security group to communicate with each other.
Outbound			
All	All	All	Security group rule created by the system by default Allows all peers to access SAP HANA.

Table 2-12 Security group rules (SAP HANA Studio)

Source/ Destination	Protocol	Port Range	Description
Inbound			
0.0.0.0/0	TCP	3389	Allows users to access SAP HANA Studio using RDP. This rule is required only when SAP HANA Studio is deployed on a Windows ECS.
0.0.0.0/0	TCP	22	Allows users to access SAP HANA Studio using SSH. This rule is required only when SAP HANA Studio is deployed on a Linux ECS.
Automatically specified by the system	All	All	Security group rule created by the system by default It enables ECSs in the same security group to communicate with each other.
Outbound			
All	All	All	Security group rule created by the system by default Allows all peers to access SAP HANA Studio.

Table 2-13 Security group rules (NAT server)

Source/ Destination	Protocol	Port Range	Description
Inbound			
0.0.0.0/0	TCP	22	Allows users to access the NAT server using SSH.
10.0.3.0/24	TCP	80 (HTTP)	Allows users to access the NAT server using HTTP.
10.0.3.0/24	TCP	443 (HTTPS)	Allows users to access the NAT server using HTTPS.

Source/ Destination	Protocol	Port Range	Description
Automatically specified by the system	All	All	Security group rule created by the system by default It enables ECSs in the same security group to communicate with each other.
Outbound			
10.0.3.0/24	TCP	22 (SSH)	Allows the NAT server to access the 10.0.3.0 subnet using SSH.
0.0.0.0/0	TCP	80 (HTTP)	Allows the NAT server to access any network where VPC instances reside using HTTPS.
0.0.0.0/0	TCP	443 (HTTPS)	Allows the NAT server to access any network where VPC instances reside using HTTPS.

2.3 Preparing Resources

2.3.1 Software and Tools

Table 2-14 lists the software and tools to be obtained.

 **NOTE**

Download the **readme.txt** file at <https://obs-sap.obs.cn-east-2.myhuaweicloud.com/readme.txt> on a local computer to obtain the location where the software and configuration file are stored.

Table 2-14 Required software and tools

Item	Description	How to Obtain
Local computer	Runs a Windows OS which is Windows 7 or later.	N/A
WinSCP	Uploads key files to HANA ECSs.	https://winscp.net/eng/index.php

Item	Description	How to Obtain
PuTTY and PuTTYgen	Used for logging in to a HANA ECS and running commands.	https://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
SAP HANA 1.0 or SAP HANA 2.0	SAP HANA installation package. Install the required SAP HANA version based on the version mapping relationship between SAP HANA software version and SUSE OS version on the SAP official website.	https://support.sap.com/swdc
SAP HANA Studio	Install the required SAP HANA Studio version based on version mapping.	
Configuration script	Script file used when configuring the HA function of SAP HANA.	The download addresses vary by region: <ul style="list-style-type: none"> ● CN-Hong Kong: https://obs-sap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip ● AP-Bangkok: https://obs-sap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip

2.3.2 License

SAP HANA 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.

2.3.3 Creating a VPC

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

Procedure



- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and project.
- Step 3** In the navigation pane on the left, click  and choose **Network > Virtual Private Cloud**.
- Step 4** Click **Create VPC** on the right of the page.
- Step 5** On the **Create VPC** page, configure VPC parameters listed in [Table 2-15](#).

Table 2-15 VPC configuration parameters

Item	Parameter	Description	Example Value
Basic Information	Region	A region is a geographical area where you can run your VPC service. Each region comprises one or more AZs and is completely isolated from other regions. Only AZs in the same region can communicate with one another through an internal network. You can use the region selector at the upper left of the main menu bar to change the region.	CN-Hong Kong
	Parameter	Specifies the VPC name.	vpc-sap
	CIDR Block	Specifies the Classless Inter-Domain Routing (CIDR) block for the VPC. The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC), or a subset of the CIDR block for the VPC (for multiple subnets). The following CIDR blocks are supported: 10.0.0.0/8-24 172.16.0.0/12-24 192.168.0.0/16-24 Configure the CIDR block based on the subnet information provided in 2.2.3 Network Planning .	10.0.0.0/8

Item	Parameter	Description	Example Value
	Enterprise Project	<p>When creating a VPC, you can add the VPC to an enabled enterprise project.</p> <p>An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is default.</p> <p>For details about creating and managing enterprise projects, see the Enterprise Management User Guide.</p>	SAP
	Tag	<p>Specifies the VPC tag, which consists of a key and value pair. You can create 10 tags for a VPC. This parameter is optional. Click Advanced Settings to configure it.</p> <p>For details about the tag naming rules, see VPC Tag Naming Rules.</p>	<ul style="list-style-type: none"> • Key: vpc_key1 • Value: vpc-01
Default Subnet	AZ	An AZ is a geographic location with independent power supply and network facilities in a region. AZs are physically isolated, and AZs in the same VPC are interconnected through an internal network.	AZ1
	Name	Specifies the subnet name.	sap_Subnet
	CIDR Block	Specifies the CIDR block for the subnet. This value must be within the VPC CIDR range. Configure the subnet CIDR block based on the information provided in 2.2.3 Network Planning .	10.0.3.0/24
	Advanced Settings	Click Advanced Settings to set parameters such as Gateway and DNS Server Address .	Default
	Gateway	Specifies the address of the subnet gateway.	10.0.0.1

Item	Parameter	Description	Example Value
	DNS Server Address	The external DNS server address is used by default. If you need to change the DNS server address, ensure that the DNS server address you configured is available.	N/A
	DHCP Lease Time	Specifies the period during which a client can use an IP address automatically assigned by the DHCP server. After the lease time expires, a new IP address will be assigned to the client. The unit is day.	365
	Tag	Specifies the subnet tag, which consists of a key and value pair. You can add 10 tags for a subnet. This parameter is optional. For details about the tag naming rules, see VPC Tag Naming Rules .	<ul style="list-style-type: none">• Key: subnet_key1• Value: subnet-01

Step 6 Click **Create Now**.



----End

2.3.4 Creating a Subnet and Configuring a Security Group

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

Procedure

Step 1 Create a subnet.

1. Log in to the management console.
2. Click  in the upper left corner and select a region and project.
3. In the navigation pane on the left, click  and choose **Network > Virtual Private Cloud**.
4. Choose **Subnets** on the left of the page.
5. In the upper right corner of the page, click **Create Subnet**.
6. In the **Create Subnet** dialog box, configure parameters as prompted.
 - **VPC**: Select the VPC created in [2.3.3 Creating a VPC](#).
 - **AZ**: specifies the AZ of the subnet.

- **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 section [2.2.3 Network Planning](#).
 - **Advanced Settings:** Set it to **Default**.
7. Click **OK** to complete the subnet configuration.
 8. Repeat [Step 1.5](#) to [Step 1.7](#) to create all required subnets according to the requirements specified in section [2.2.3 Network Planning](#).

Step 2 Configure a security group.

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

1. Choose **Access Control > Security Groups** on the left and then click **Create Security Group** in the upper right corner. The **Create Security Group** dialog box is displayed.
2. Set the following parameters as prompted:
 - **Template:** The template contains security group rules, which help you quickly create a security group. The following templates are provided:
 - **Custom:** This template allows you to create security groups with custom security group rules.
 - **General-purpose web server:** The security group that will be created using this template is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and allow inbound traffic on ports 22, 80, 443, and 3389.
 - **All ports open:** The security group that will be created using this template includes default rules that allow inbound traffic on any port. Allowing inbound traffic on any port may pose security risks. Exercise caution when using this template.
 - **Name:** specifies the name of the security group. Name the security group that is easy to identify, for example, **studio_security_group**.
 - **Enterprise Project:** You can add the security group to an enabled enterprise project. You can select an enterprise project from the drop-down list.
3. Click **OK**.
4. Repeat [Step 2.1](#) to [Step 2.3](#) to create other security groups.
5. In the navigation pane on the left, choose **Access Control > Security Groups**. In the security group list, click the security group to which you want to add an access rule.
6. Click **Add Rule** on the **Inbound Rules** or **Outbound Rules** tab as planned.
7. On the displayed page, add the rule according to the requirements specified in section [2.2.3 Network Planning](#).
The default security group rules cannot be deleted.
8. Repeat [Step 2.5](#) to [Step 2.7](#) to configure all security groups.

----End

2.4 Creating ECSs

2.4.1 Creating an SAP HANA ECS

SAP HANA software runs on HANA ECSs. Depending on deployment scenarios, you need to create one or more HANA ECSs for deploying the SAP HANA software.

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

Procedure



- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select the desired region and project.
- Step 3** In the navigation plane on the left, click  and choose **Computing > Elastic Cloud Server**.
- Step 4** On the right side of the page, click **Buy ECS**.
- Step 5** Configure basic information about the HANA ECS as prompted.

Table 2-16 HANA 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 ECSs are located. The AZ must support SAP HANA. Choose the AZ as required.
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.

Parameter	Description
Specifications	Click Large-memory . Select a specification based on section 2.2.1 SAP HANA Nodes or as required.
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	In single-node scenarios, regardless of whether HA is required, one system disk and multiple data disks are required. For details about disk requirements, see section 2.2.1 SAP HANA Nodes . If additional disks are required, you can click Add Data Disk to add more disks.

Step 6 Click **Next: Configure Network**.

Step 7 Configure network information for the HANA ECS as prompted.

Table 2-17 HANA ECS network configuration

Parameter	Description
Network	Select the VPC and subnet provided in 2.3.4 Creating a Subnet and Configuring a Security Group .
Extension NIC	Determine the number of NICs according to the deployment plan provided in section 2.2.3 Network Planning . If you need to add a NIC, click Add NIC . NOTE <ul style="list-style-type: none"> In the single-node deployment mode where HA is not required, you do not need to add an extension NIC. In the single-node deployment mode where HA is required, add an extension NIC and deselect Security group disabled.
Security Group	Use the security group in section 2.3.4 Creating a Subnet and Configuring a Security Group .
EIP	Select Not required .

Step 8 Click **Next: Configure Advanced Settings**.

Step 9 Configure advanced settings for the HANA ECS as prompted.

Table 2-18 HANA ECS advanced configuration

Parameter	Description
ECS Name	<p>Specifies the ECS name.</p> <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 hana in ECS Name, the first ECS is hana-0001, and the second ECS is hana-0002.</p> <p>For more details, see SAP Note 611361.</p>
Login Mode	<p>Select Key pair.</p>
Key Pair	<p>This parameter is available only when the Login Mode is set to Key pair.</p> <p>An SSH key certificate is used for authenticating users who attempt to log in to HANA ECSs. To create a key pair, click Create Key Pair. On the displayed Key Pair page, click Create Key Pair.</p> <p>Ensure that the HANA ECSs/ECSs where SAP HANA, SAP HANA Studio, and NAT servers are to be deployed use the same key. Otherwise, SAP HANA installation will fail.</p> <p>NOTE</p> <p>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 HANA ECS or ECS.</p> <p>To create a key, do as follows:</p> <p>Click Create Key Pair. On the displayed Key Pair page, click Create Key Pair, specify the key pair name, and click OK. In the Information dialog box that is displayed, click OK. Then, you can query and save the private key as prompted.</p>

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>You can select one of the following three options for EIP as required:</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>Specifies a HANA ECS group. When you create ECSs, the system will allocate the HANA ECSs in the same server group to different physical servers to ensure the running reliability of these HANA ECSs.</p> <p>Determine the policy of a HANA ECS group based on the scenario:</p> <ul style="list-style-type: none"> • Single-node where HA is not required: You do not need to specify ECS Group. • Single-node scenario where HA is required: The two HANA ECSs must belong to the same ECS Group. <p>NOTE If no ECS group is available, perform the following operations to create one: Click Create ECS Group. On the displayed page, click Create ECS Group, specify the ECS group name, and click OK.</p>
Advanced Options	Select Configure now .

Parameter	Description
Agency	<p>This parameter is available only when Advanced Options is set to Configure now.</p> <p>After the agency is specified, the delegated domain can obtain the credentials from the agency to temporarily access the public cloud.</p> <p>Data Provider is an SAP indicator collector on the public cloud platform to collect key performance data of ECSs and Cloud Eye in the SAP NetWeaver system and then surface the data to SAP applications. Specify the DataproviderAccess agency to ECSs where SAP HANA and SAP NetWeaver are all deployed.</p> <p>Before using the agency, log in to the public cloud management console as the tenant administrator and create the DataproviderAccess agency.</p> <p>For details about how to create an agency, see the Data Provider for SAP User Guide.</p>

Step 10 Click **Next: Confirm**.

Step 11 Confirm the HANA ECS configuration as prompted.

Table 2-19 HANA 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 the site requirements.
Quantity	Set this parameter as required.
Agreement	Select I have read and agree to Huawei Image Disclaimer .

Step 12 Click **Next** and complete the payment as prompted.

Step 13 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 HANA ECS is created, you can view the ECS from the ECS list on the right of the page.

Step 14 Create other HANA ECSs as required.

Step 15 Change the password of user **root** for logging in to all HANA ECSs.

Securely keep the password of user **root**. Ensure that the passwords of user **root** are the same for all HANA ECSs.

1. Use the key to log in to the SAP HANA ECSs.
2. Change the password of user **root**.

passwd

Enter the new password as prompted and confirm it.

----End

2.4.2 Creating an SFS File System

In the SAP HANA system, if the backup volume is provided by SFS, you can create an SFS file system to provide a shared path for SAP HANA ECSs.

Creating an SFS File System

Step 1 (Optional) Purchase an SFS package.

Before creating an SFS file system in SAP HANA, you can purchase an SFS storage package as required.



- Yearly/monthly subscription: You can purchase a yearly or monthly package based on your resource usage and duration plan. When a purchased package is within its validity period, any data used is initially offset by the quota provided. However, when data exceeds this quota, subsequent data is charged on a pay-per-use basis.
 - Pay per use: If you select this mode, perform **Step 2** to create an SFS file system.
1. Log in to the management console.
 2. Click  in the upper left corner and select the desired region and project.
 3. In the navigation pane on the left, click  and choose **Scalable File Service** under **Storage**. The **Scalable File Service** page is displayed.
 4. Click **Buy Storage Package**. The **Buy SFS Package** page is displayed.
 5. Set the parameters as described in **Table 2-20**.

Table 2-20 Parameters

Parameter	Description	Example Value
Region	Storage packages in different regions are isolated. Select the region based on your requirements.	CN-Hong Kong
Storage Package	Select the storage package size based on the site requirements.	5 TB
Usage Duration	Select the effective time of the storage package based on the site requirements.	1 year

6. Click **Next**.

7. Submit the order and pay as prompted.

Step 2 Create an SFS file system.



1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the navigation pane on the left, click  and choose **Scalable File Service** under **Storage**. The **Scalable File Service** page is displayed.
4. Click **Create File System**.
5. Configure the parameters listed in [Table 2-21](#).

Table 2-21 Parameters

Parameter	Description	Example Value
File System Type	Specifies the file system type. Select SFS .	SFS
Region	Select the target region.	CN-Hong Kong
AZ	Specifies the AZ where the file system is located. Select an AZ as required.	AZ1
Protocol Type	Specifies the protocol type. Choose NFS .	NFS
VPC	Select the VPC where SAP HANA ECSs reside.	N/A
Auto Capacity Expansion	This function is enabled by default. When it is enabled, the capacity of the file system is not limited. Therefore, you do not need to adjust the capacity of the file system. You can determine whether to enable the function based on the site requirements. NOTICE If you have purchased an SFS storage package and it is within the validity period, any data used is initially offset by the quota provided. However, when data exceeds this quota, subsequent data is charged on a pay-per-use basis.	N/A
Maximum Capacity	This parameter shows after Automatic Capacity Expansion is disabled. Maximum capacity of a single file system. For details, see 2.2.1 SAP HANA Nodes .	N/A

Parameter	Description	Example Value
Encryption	This parameter is optional. This parameter specifies whether a file system is encrypted. You can create a file system that is encrypted or not, but you cannot change the encryption settings of an existing file system. If you want to encrypt the file system to be created, select Enable static data encryption . For details, see the Getting Started with Scalable File Service .	N/A
Enterprise Project	Select the project according to the site requirements.	SAP
Name	Specifies the file system name.	sfs-share-001
Quantity	Select the quantity according to system requirements.	1

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

2.4.3 Creating an SAP HANA Studio ECS

An SAP HANA system requires an ECS for deploying the SAP HANA Studio software.

Procedure



- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and project.
- Step 3** In the navigation plane on the left, click  and choose **Computing > Elastic Cloud Server**.
- Step 4** On the right side of the page, click **Buy ECS**.
- Step 5** Configure basic settings of the SAP HANA Studio ECS as prompted.

Table 2-22 SAP HANA Studio 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 ECSs are located. Choose an AZ as required.
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	Select All generations and s1.xlarge (4 vCPUs, 16 GB memory).
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	80 GB For details about disk requirements, see section 2.2.2 Other Nodes .

Step 6 Click **Next: Configure Network**.

Step 7 Configure network information for the SAP HANA Studio ECS as prompted.

Table 2-23 SAP HANA Studio ECS network configuration

Parameter	Description
Network	Choose the VPC and subnet created in 2.3.3 Creating a VPC and 2.3.4 Creating a Subnet and Configuring a Security Group .
Extension NIC	Select the target NIC based on 2.2.3 Network Planning .

Parameter	Description
Security Group	Choose the security group created in section 2.3.4 Creating a Subnet and Configuring a Security Group .
EIP	Set the parameter as required.
EIP Type	<p>This parameter is available only when EIP is set to Auto assign. Set this parameter based on the site requirements.</p> <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. • Static BGP gives you more control over the routes but route configuration and update are usually time-consuming and error-prone.
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	This parameter is available only when EIP is set to Auto assign . Set this parameter based on the site requirements.

Step 8 Click **Next: Configure Advanced Settings**.

Step 9 Configure advanced settings for the SAP HANA Studio ECS as prompted.

Table 2-24 SAP HANA Studio ECS advanced configuration

Parameter	Description
ECS Name	Specifies the ECS name. For more details, see SAP Note 611361.

Parameter	Description
Login Mode	Select Key pair .
Key Pair	<p>This parameter is available only when the Login Mode is set to Key pair.</p> <p>An SSH key certificate is used for authenticating users who attempt to log in to the ECSs. To create a key pair, click Create Key Pair. On the displayed Key Pair page, click Create Key Pair.</p> <p>Ensure that the HANA ECSs/ECSs where SAP HANA, SAP HANA Studio, and NAT servers are to be deployed use the same key. Otherwise, SAP HANA installation will fail.</p> <p>NOTE</p> <p>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 HANA ECS or ECS.</p> <p>To create a key, do as follows:</p> <p>Click Create Key Pair. On the displayed Key Pair page, click Create Key Pair, specify the key pair name, and click OK. In the Information dialog box that is displayed, click OK. Then, you can query and save the private key as prompted.</p>

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>You can select one of the following three options for EIP as required:</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 10 Click **Next: Confirm**.

Step 11 Confirm the SAP HANA Studio ECS configuration as prompted.

Table 2-25 SAP HANA Studio ECS configuration information

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

Step 12 Click **Next** and complete the payment as prompted.

Step 13 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


2.4.4 Creating an NAT ECS

In SAP HANA systems, you must create an ECS for deploying the NAT server. You can visit the NAT server and then switch to an SAP HANA node using SSH for fault diagnose and location.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select the desired region and project.

Step 3 In the navigation plane on the left, click  and choose **Computing > Elastic Cloud Server**.

Step 4 On the right side of the page, click **Buy ECS**.

Step 5 Configure the basic settings of the NAT server as required.

Table 2-26 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 ECSs are located. Choose 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	Select All and s1.medium (1 vCPUs, 4 GB memory) or larger specifications.
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>40 GB</p> <p>For details about disk requirements, see section 2.2.2 Other Nodes.</p>

Step 6 Click **Next: Configure Network**.

Step 7 Configure network information for the NAT server as prompted.

Table 2-27 NAT server network configuration

Parameter	Description
Network	Choose the VPC and subnet created in 2.3.3 Creating a VPC and 2.3.4 Creating a Subnet and Configuring a Security Group .
Extension NIC	Select the target NIC based on 2.2.3 Network Planning .
Security Group	Choose the security group created in section 2.3.4 Creating a Subnet and Configuring a Security Group .
EIP	Set the parameter as required.

Parameter	Description
EIP Type	<p>This parameter is available only when EIP is set to Auto assign. Set this parameter based on the site requirements.</p> <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. • Static BGP gives you more control over the routes but route configuration and update are usually time-consuming and error-prone.
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 8 Click **Next: Configure Advanced Settings**.

Step 9 Configure advanced settings for the NAT server as prompted.

Table 2-28 NAT server advanced configuration

Parameter	Description
ECS Name	<p>Specifies the ECS name. For more details, see SAP Note 611361.</p>
Login Mode	<p>Select Key pair.</p>

Parameter	Description
Key Pair	<p>This parameter is available only when the Login Mode is set to Key pair.</p> <p>An SSH key certificate is used for authenticating users who attempt to log in to the NAT server. To create a key pair, click Create Key Pair. On the displayed Key Pair page, click Create Key Pair.</p> <p>Ensure that ECSs where SAP HANA, SAP HANA Studio, and NAT servers are to be deployed use the same key. Otherwise, SAP HANA installation will fail.</p> <p>NOTE</p> <p>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 HANA ECS or ECS.</p> <p>To create a key, do as follows:</p> <p>Click Create Key Pair. On the displayed Key Pair page, click Create Key Pair, specify the key pair name, and click OK. In the Information dialog box that is displayed, click OK. Then, you can query and save the private key as prompted.</p>
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>You can select one of the following three options for EIP as required:</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 10 Click **Next: Confirm**.

Step 11 Confirm the NAT server configuration as prompted.

Table 2-29 NAT server configuration information

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

Step 12 Click **Next** and complete the payment as prompted.

Step 13 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

2.4.5 Configuring SSH Switching Permissions

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

Procedure

Step 1 Upload the key file to the NAT server. The following steps use WinSCP to upload the key file to the NAT server. You are free to use other tools.

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 is used to generate the .ppk file. For details, see section [6.2 Logging In to a Linux ECS Using an SSH Key](#).
2. On the local computer, install the WinSCP software.
3. Upload the certificate private key file (.pem file) to the NAT server.
Use WinSCP to upload the certificate private key file (.pem file) to the **/usr** directory on the NAT server using an elastic IP address. Ensure that user **root** and the key file (.ppk file) are used for authentication.
4. Use PuTTY to log in to the NAT server. Ensure that user **root** and the key file (.ppk file) are used for authentication.

5. Copy the certificate private key file (.pem file) to the `/root/.ssh` directory and rename the file `id_rsa`.

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

```
cp /usr/private.pem /root/.ssh/id_rsa
cd /root/.ssh/
chmod 600 id_rsa
```

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

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 `10.0.3.102`, run the following commands:

```
scp /root/.ssh/id_rsa 10.0.3.102:/root/.ssh/id_rsa
scp /root/.ssh/authorized_keys 10.0.3.102:/root/.ssh/
```

- Step 3** Verify the switching.

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

Switch to an SAP HANA node. Assume that the IP address of the server/client plane of the SAP HANA node is `10.0.3.2`.

```
ssh 10.0.3.2
```

 **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

2.4.6 Configuring the Mapping Between SAP HANA Host Names and IP Addresses

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

Procedure

- Step 1** Use PuTTY to log in to the NAT server with an elastic IP address bound. Ensure that user `root` and the key file (`.ppk` file) are used for authentication. Then, use SSH to switch to the HANA server on which SAP HANA is to be installed.

 **NOTE**

In cluster scenarios, you will switch to the first SAP HANA server. Then, you will perform operations on this HANA server when installing SAP HANA.

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

```
vi /etc/hosts
```

Step 3 Enter `i` to enter editing mode and write the names and IP addresses of all SAP HANA nodes into the `hosts` file.

- In single-node scenarios where HA is not required, **IP-Address** is the IP address of the server or client plane of the SAP HANA ECS. In single-node scenarios where HA is required, **IP-Address** is the IP address of the system replication plane.
- Both **Full-Qualified-Hostname** and **Short-Hostname** are the server name, for example, **hana001**.

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

NOTICE

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

Take the IP addresses 10.0.4.2 to 10.0.4.3 of the system replication plane for two SAP HANA nodes in single-node scenarios where HA is required as an example.

The edited content is as follows:

```
...  
10.0.4.2 hana001 hana001  
10.0.4.3 hana002 hana002
```

Step 4 After you complete editing, press **Esc**, enter `:x`, and press **Enter** to exit the `hosts` file.

Step 5 (Optional) Run the following command to transfer the configured `/etc/hosts` file to other SAP HANA nodes:

The command is in the following format:

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

This operation is performed only in single-node scenarios where HA is required.

Verify the SSH switching between SAP HANA nodes.

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

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

```
ssh hana002
```

```
----End
```

2.5 Installing SAP HANA (Single-Node Deployment Without HA Required)

2.5.1 Formatting a Disk

In single-node deployment scenarios, the data volumes of SAP HANA nodes can be used only after they are formatted and attached to required directories.

Procedure

Step 1 Log in to an SAP HANA node.

Use PuTTY to log in to the NAT server with an elastic IP address bound. Ensure that user **root** and the key file (.ppk file) are used for authentication. Then, use SSH to switch to the SAP HANA nodes.

Step 2 Check the disks that have not been formatted.

Run the following command to query the disks to be formatted:

```
fdisk -l
```

Determine the disks of the `/usr/sap` volumes, data volumes, log volumes, shared volumes, and swap volumes according to the disk capacity.

Step 3 Run the following command to create a disk directory:

```
mkdir -p /hana/log /hana/data /hana/shared /hana/backup /usr/sap
```

Step 4 Create and enable the swap partition. **dev/vdb** is used as an example.

```
mkswap /dev/vdb
```

```
swapon /dev/vdb
```

Step 5 Use LVM to logically create a data volume using two EVS disks. The following uses EVS disks **dev/vdb** and **dev/vdc** as an example.

1. Run the following command to create physical volumes:

```
pvcreate /dev/vdb /dev/vdc
```

2. Run the following command to create volume groups:

```
vgcreate vghana /dev/vdb /dev/vdc
```

3. Run the following command to query the available capacity of the volume group:

```
vgdisplay vghana
```

4. Create logical volumes. The following command uses two EVS disks to create a logical volume.

```
lvcreate -n lvhanadata -i 2 -l 256 -L 348G vghana
```

The parameters are described as follows:

- **-n**: Name of a logical volume

- -i: Number of logical extensions
- -l: Stripe size
- -L: Logical volume size

Step 6 Format disks and logical volumes. **dev/vdd**, **dev/vde**, and **dev/vdf** are used as examples.

```
mkfs.xfs /dev/vdd
```

```
mkfs.xfs /dev/vde
```

```
mkfs.xfs /dev/vdf
```

```
mkfs.xfs /dev/mapper/vghana-lvhanadata
```

Step 7 Write disk attaching relationships into the **/etc/fstab** file.

1. Run the following command to check the UUID of the disk:

```
blkid
```

2. Obtain the shared path in [Step 2.7](#) or `saphana_02_0075.xml#saphana_02_0075/li137231454101` in section [2.4.2 Creating an SFS File System](#). `PublicCloudAddress;/share-d6c6d9e2` is used as an example.

3. Write the attaching relationships between the disk UUID and shared path to the **/etc/fstab** file. UUID is used as an example here.

```
echo "UUID=ba1172ee-39b2-4d28-89b8-282ebabfe8f4 /hana/data xfs
defaults 0 0" >>/etc/fstab
```

```
echo "UUID=d21734c9-44c0-45f7-a37d-02232e97fd3b /hana/log xfs
defaults 0 0" >>/etc/fstab
```

```
echo "UUID=191b5369-9544-432f-9873-1beb2bd01de5 /hana/shared xfs
defaults 0 0" >>/etc/fstab
```

```
echo "UUID=191b5369-9544-432f-9873-1beb2bd01de5 /usr/sap xfs defaults
0 0" >>/etc/fstab
```

```
echo "UUID=1b569544-1225-44c0-4d28-2e97fdeb2bd swap swap defaults 0
0" >> /etc/fstab
```

```
echo "PublicCloudAddress;/share-d6c6d9e2 /hana/backup nfs
noatime,nodiratime,rdirplus,vers=3,wsiz=1048576,rsiz=1048576,noacl,n
octo,proto=tcp,async 0 0" >>/etc/fstab
```

Step 8 Run the following command to attach all disks:

```
mount -a
```

Step 9 Check the disk mounting status. The following is an example:

```
# df -h
Filesystem                Size  Used Avail Use% Mounted on
devtmpfs                  126G   0 126G   0% /dev
tmpfs                      197G   80K 197G   0% /dev/shm
tmpfs                      126G   17M 126G   1% /run
tmpfs                      126G   0 126G   0% /sys/fs/cgroup
/dev/xvda                   50G  4.4G  43G  10% /
/dev/sdd                    254G   93G 162G  37% /hana/shared
/dev/mapper/vghana-lvhanadata 254G   67G 188G  27% /hana/data
/dev/sde                    164G   6.3G 158G   4% /hana/log
/dev/sdf                     50G  267M   50G   1% /usr/sap
/dev/xvdb                   10G    5G   5G  50% /swap
```

```
PublicCloudAddress:/share-d6c6d9e2 384G 0 384G 0% /hana/backup
tmpfs 26G 0 26G 0% /run/user/1002
tmpfs 26G 0 26G 0% /run/user/480
tmpfs 26G 16K 26G 1% /run/user/0
```

----End

2.5.2 Installing the SAP HANA Software

SAP HANA database software must be deployed on ECSs. This section uses the SAP HANA 1.0 installation package as an example. You can download the package from the official website.

Prerequisites

- You have prepared related resources. For details, see section "Preparing Resources".
- You have created ECSs, formatted disks attached to them, and completed required configurations.
- Ensure that the OS firewall of the new node is disabled. For details about how to disable the OS firewall, see [6.4 Modifying OS Configurations](#).

Procedure

Step 1 Log in at <https://support.sap.com/swdc> to download the installation package, and perform the installation.

1. Switch to **SAP Software Download Center**.
 - Choose **Software Downloads**.
 - Choose **INSTALLATIONS & UPGRADES**.
 - Choose **By Alphabetical Index (A-Z)**.
 - Choose **H**.
 - Choose **SAP HANA PLATFORM EDITION**.
 - Choose **DOWNLOADS**.
2. Locate the target package and download it to the local hard disk.
3. Upload the obtained installation package to the **/hana/shared** directory on the ECS where the SAP HANA software is to be installed and decompress it. For example, the installation package is
51052383_part1.exe
cd /hana/shared
unrar x 51052383_part1.exe
4. Run the following command to enter the directory where the installation file is stored, taking **SAP_HANA_DATABASE** as an example:
For example, if the installation file is stored in **/DATA_UNITS/HDB_SERVER_LINUX_X86_64**, run the following commands:
cd 51052383
cd DATA_UNITS/HDB_SERVER_LINUX_X86_64
5. Run the following command to assign execute permissions to the directory:
chmod -R 777 /hana

- Run the following command to perform the installation:

./hdblcm --ignore=check_signature_file

The following information is displayed:

Choose installation

```

Index | System          | Database Properties
-----|-----
1     | Install new system |
      |                   |
2     | Extract components |
3     | Exit (do nothing)  |
    
```

Enter selected system index [2]:

- Enter **1** and press **Enter**.

The following information is displayed:

Select additional components for installation:

```

Index | Components | Description
-----|-----
1     | server     | No additional components
2     | all        | All components
    
```

Enter comma-separated list of the selected indices [1]:

- Enter **1** and press **Enter**.
- Configure parameters as prompted on the page one by one.

 **NOTE**

- During the configuration, press **Enter** if you want to retain the default setting.
- If a parameter is incorrectly set and you have pressed **Enter**, you can press **Ctrl+C** to exit the configuration and run the **./hdblcm --ignore=check_signature_file** command to enter the installation page again.

Table 2-30 lists the parameter configuration requirements.

Table 2-30 Requirements for configuring SAP HANA installation parameters

Parameter	Description
Installation Path	Specifies the installation path, which defaults to /hana/shared/\$SID . The default value is recommended.
Local Host Name	Specifies the local host name.
Do you want to add additional hosts to the system	Enter the value n .
SAP HANA System ID	Specifies the SAP HANA system ID, for example, S00 .

Parameter	Description
Instance Number	Specifies the SAP HANA instance number, for example, 00 . The instance ID is used in Security Group Rules , which must be the same as the planned one.
Database Mode	Specifies the database deployment mode. Retain the default value single_container . You do not need to set this parameter when installing HANA2.0 and the default value is multiple container .
System Usage	Specifies the SAP HANA system type. Set this parameter as required. This parameter is stored in the global.ini file.
Location of Data Volumes Specifies	Specifies the system data volume directory, which is /hana/data/\$SID .
Location of Log Volumes	Specifies the system log volume directory, which is /hana/log/\$SID .
Restrict maximum memory allocation?	Specifies whether maximum memory allocation is restricted, which defaults to n .
Certificate Host Name	Specifies the ECS name that is used to generate a self-signed SSL certificate for the SAP Host Agent.
SAP Host Agent User (sapadm) Password	Enter the SAP Host Agent user password.
System Administrator (s00adm) Password	Enter the system administrator password.
System Administrator Home Directory	Use the default value.
System Administrator Login Shell	Use the default value.
System Administrator User ID	Use the default value.
ID of User Group	Use the default value.
Database User (SYSTEM) Password	Enter the database user password.

10. After you complete the configuration, the system displays the message "Restart system after machine reboot?"
 - In single-node scenarios where HA is not required, enter **y**.

- In single-node scenarios where HA is required, if automatic active/standby switchover is not required, enter **y**; if automatic active/standby switchover (HAE) is required, enter **n**.

Then, press **Enter**. The system displays the installation summary.

11. After confirming the installation information is correct, in the **Do you want to continue?** dialog box, enter **y** and press **Enter** to start to installation.

After the installation is complete, the prompt **Installation done** is displayed.

Step 2 Verify the installation.

1. Run the following command to switch to the **/hana/shared/\$SID/HDB00/** directory:

The following command is used as an example:

```
cd /hana/shared/S00/HDB00
```

2. Switch to the database system administrator.

Account **s00adm** is displayed on the page during the installation. Run the following command:

```
su - s00adm
```

3. Run the following command to query the database version:

If the version can be queried, the database software is installed.

HDB -version

After the database is installed, the system returns the version. [Figure 2-8](#) shows an example.

Figure 2-8 SAP HANA version information

```
HDB version info:
version:          1.00.112.05.1469552341
branch:          fa/newdb100_rel
git hash:        a9abfc92240a2d6e0d96f15c037739b49fd21cd8
git merge time:  2016-07-26 18:59:01
weekstone:      0000.00.0
compile date:   2016-07-26 19:12:32
compile host:   ld7272
compile type:   rel
```

Step 3 Check whether the database process is running properly.

1. Run the following command to check the process, taking the SAP HANA instance with ID 00 as an example:

```
sapcontrol -nr 00 -function GetProcessList
```

In the terminal display, if the **dispstatus** value is **GREEN**, the process is running properly.

```
13.04.2017 16:04:15
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
hdbdaemon, HDB Daemon, GREEN, Running, 2017 04 13 11:18:33, 4:45:42, 3013
hdbcompileserver, HDB Compileserver, GREEN, Running, 2017 04 13 11:18:42, 4:45:33, 3154
hdbindexserver, HDB Indexserver, GREEN, Running, 2017 04 13 11:18:47, 4:45:28, 3180
hdbnameserver, HDB Nameserver, GREEN, Running, 2017 04 13 11:18:34, 4:45:41, 3027
```

```
hdbpreprocessor, HDB Preprocessor, GREEN, Running, 2017 04 13 11:18:42, 4:45:33, 3156  
hdbwebdispatcher, HDB Web Dispatcher, GREEN, Running, 2017 04 13 11:19:09, 4:45:06,  
3513  
hdbxsengine, HDB XSEngine, GREEN, Running, 2017 04 13 11:18:47, 4:45:28, 3182
```

2. Run the following command to return to user **root**:
exit

Step 4 Check the database startup and shutdown.

1. Run the following command to switch to the **/hana/shared/\$SID/HDB00/** directory:

The following command is used as an example:

```
cd /hana/shared/S00/HDB00
```

2. Switch to the database system administrator.

Account **s00adm** is displayed on the page during the installation. Run the following command:

```
su - s00adm
```

3. Run the following command to start the SAP HANA database:

```
HDB start
```

4. Run the following command to stop the SAP HANA database:

```
HDB stop
```

5. Run the following command to restart the SAP HANA database:

```
./HDB restart
```

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

```
exit
```

----End

2.5.3 Installing the SAP HANA Studio on a Windows ECS

SAP HANA Studio manages SAP HANA. After SAP HANA nodes are deployed, you need to install the SAP HANA Studio and use it to manage the SAP HANA nodes.

This section describes how to install the SAP HANA Studio on a Windows ECS.

Prerequisites

- You have prepared related resources. For details, see section "Preparing Resources".
- You have created ECSs, formatted disks attached to them, and installed the SAP HANA.
- The firewall on the target ECS has been disabled.
- Remote login to the target ECS has been enabled.

Procedure

- Step 1** Use the Remote Desktop Protocol (RDP) and elastic IP address to log in to the SAP HANA Studio ECS.

Use the username **Administrator** and the password obtained in section [6.1 Obtaining the Password for Logging In to a Windows ECS](#) to log in to the SAP HANA Studio ECS.

- Step 2** Upload the installation package obtained from the SAP official website to the SAP HANA Studio ECS.
- Step 3** Decompress the installation package and navigate to the directory where SAP HANA Studio is stored.
- Step 4** On the Windows page, switch to the directory where the SAP HANA Studio installation package is stored and double-click **hdbsetup.exe** to open the installation wizard page.
- Step 5** Select the installation path and click **Next**.
- Step 6** On the **Select Features** page, select the features to be installed and click **Next**.
You are advised to select all features.
- Step 7** Confirm all information on the **Review & Confirm** page and click **Install**.
- Step 8** An installation page is displayed. Continue the installation. When the installation is complete, the system displays the message "You have successfully installed the SAP HANA Studio."
- Step 9** Click **Finish**.

----End

2.5.4 Installing the SAP HANA Studio on a Linux ECS

SAP HANA Studio manages SAP HANA. After SAP HANA nodes are deployed, you need to install the SAP HANA Studio and use it to manage the SAP HANA nodes.

This section describes how to install the SAP HANA Studio on a Linux ECS.

Prerequisites

- You have prepared related resources. For details, see section "Preparing Resources".
- You have created ECSs, formatted disks attached to them, and installed the SAP HANA.
- The firewall on the target ECS has been disabled.

Procedure

- Step 1** Log in to the SAP HANA Studio ECS with an elastic IP address bound as user **root** using the key file.
- Step 2** Upload the obtained installation package to the **/hana/shared** directory on the ECS where the SAP HANA Studio is to be installed and decompress it.

Enter the directory where the installation file is stored. For example, if the installation file is stored in **/DATA_UNITS/HDB_STUDIO_LINUX_X86_64**, run the following command:

```
cd /DATA_UNITS/HDB_STUDIO_LINUX_X86_64
```

Step 3 Assign operation permissions to the directory where the installation packages are stored.

For example, if the directory is **HDB_STUDIO_LINUX_X86_64**, run the following command:

```
chmod 777 -R HDB_STUDIO_LINUX_X86_64
```

Step 4 Switch to the directory and perform the installation. The SAP HANA Studio installation page is displayed.

```
./hdbsetup
```

Step 5 Select the installation path and click **Next**.

Step 6 On the **Select Features** page, select the features to be installed and click **Next**.

You are advised to select all features.

Step 7 Confirm all information on the **Review & Confirm** page and click **Install**.

Step 8 An installation page is displayed. Continue the installation. When the installation is complete, the system displays the message "You have successfully installed the SAP HANA Studio."

Step 9 Click **Finish**.

Step 10 Go to [Step 5](#) to select the installation path, edit the **hdbstudio.ini** file, and add parameters to configure the GTK version.

```
vi hdbstudio.ini
```

Add the following parameters:

```
--launcher.GTK_version
```

```
2
```

An example is provided as follows:

```
-startup
plugins/org.eclipse.equinox.launcher_1.3.201.v20161025-1711.jar
--launcher.library
plugins/org.eclipse.equinox.launcher.gtk.linux.x86_64_1.1.401.v20161122-1740
--launcher.GTK_version
2
--launcher.XXMaxPermSize
512m
```

Step 11 (Optional) If the version is not configured in [Step 10](#), run the following commands before starting **hdbstudio** on the Linux OS:

```
export SWT_GTK3=0
```

```
./hdbstudio
```

```
----End
```

2.5.5 Connecting SAP HANA Nodes to the SAP HANA Studio

SAP HANA nodes can be managed only after they are connected to the SAP HANA Studio.

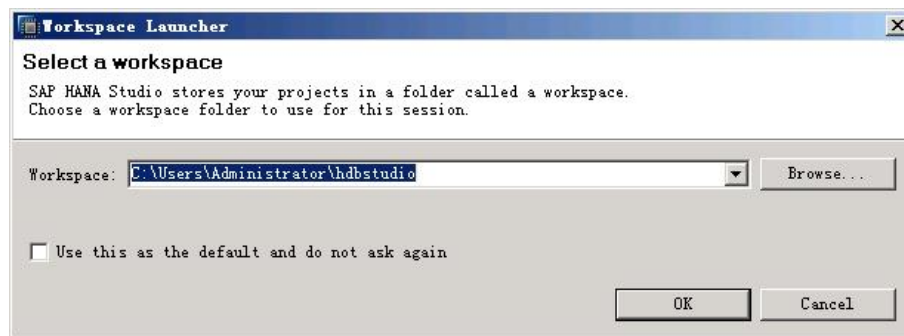
This section uses a Windows ECS where the SAP HANA Studio is deployed as an example.

Procedure

Step 1 Start the SAP HANA Studio.

On the ECS where the SAP HANA Studio is deployed, choose **Start > SAP HANA > SAP HANA Studio**. Then, the system displays the SAP HANA Studio management page and the **Workspace Launcher** dialog box.

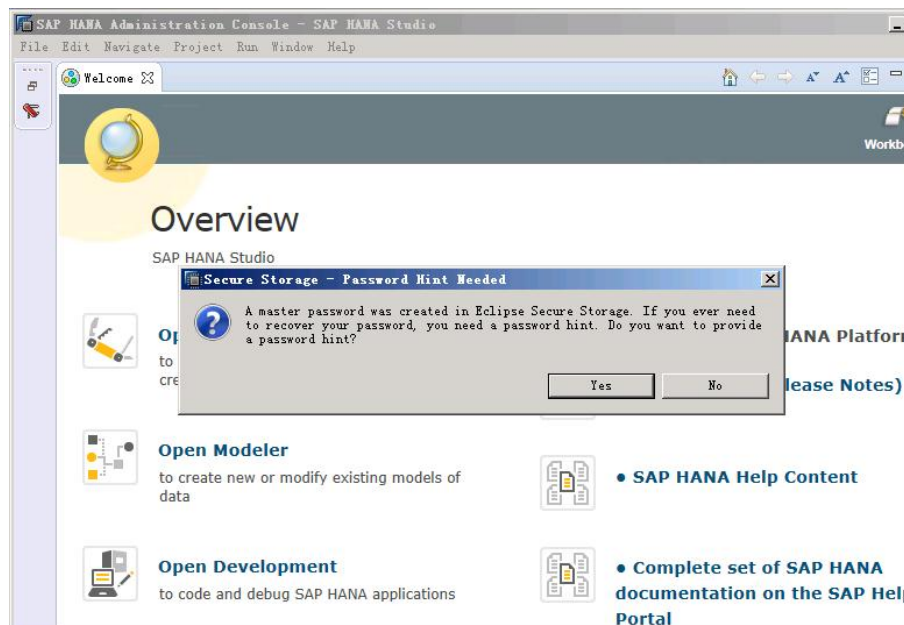
Figure 2-9 Workspace Launcher



Step 2 Specify the **Workspace** directory, select **Use this as the default and do not ask me again**, and click **OK**.

Step 3 The **Security Storage** dialog box is displayed, as shown in [Figure 2-10](#). Click **No**.

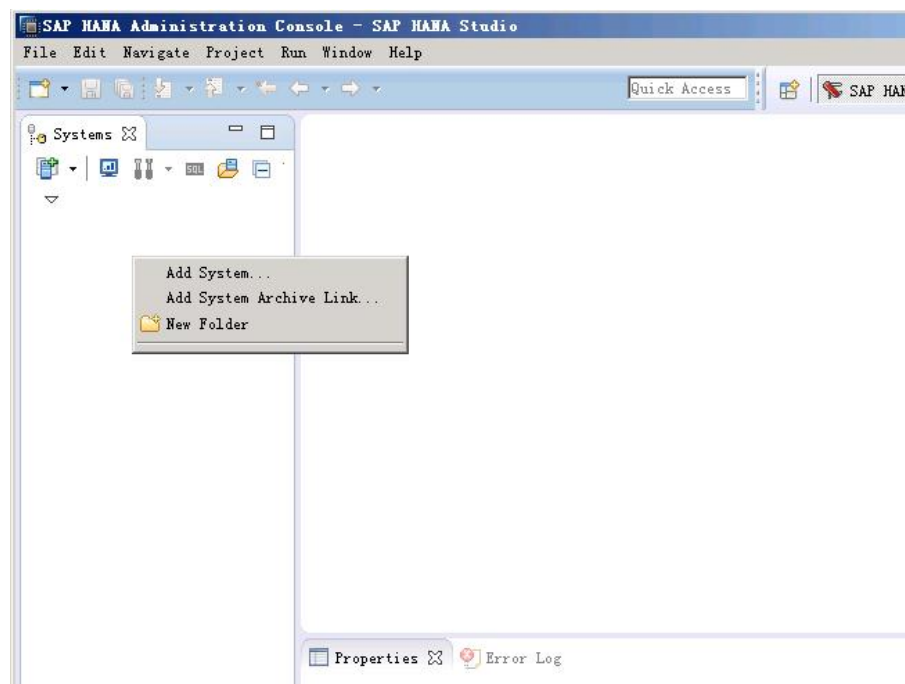
Figure 2-10 Security Storage dialog box



Step 4 On the **Overview** page, click **Open Administration Console** to enter the **SAP HANA Administration Console** page.

Step 5 Right-click the blank area under **System**, as shown in [Figure 2-11](#).

Figure 2-11 SAP HANA Administration Console page



Step 6 Choose **Add System**. The **Specify System** page is displayed, as shown in [Figure 2-12](#). Configure parameters.

Key parameters are as follows:

- **Host Name:** Enter the service or client plane IP address of the SAP HANA ECS.
- **Instance Number:** Enter the number of the instance on the SAP HANA node.
- **Mode:** Select a mode based on actual requirements. When SAP HANA 2.0 is installed, only **Multiple containers** can be selected. In addition, the backup path can be set only when the SAP HANA Studio is interconnected with both the system database and tenant database and runs on the system database.

Figure 2-12 Specify System page

The screenshot shows a 'Specify System' dialog box. The title bar reads 'System'. The main heading is 'Specify System'. Below this, it says 'Specify the host name and instance number of the system.' The form includes the following fields and options:

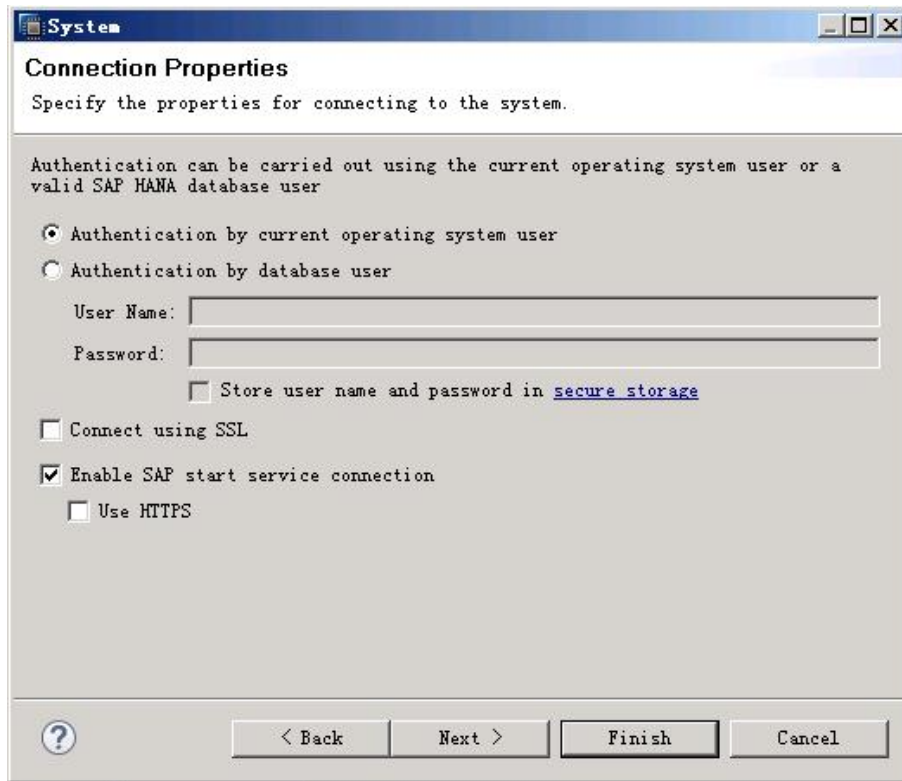
- Host Name: [Text input field]
- Instance Number: [Text input field]
- Mode: Single container, Multiple containers, Tenant database, System database
- Under Tenant database: Name: [Text input field]
- Description: [Text input field]
- Locale: [Dropdown menu showing 'English (United States)']
- Folder: [Text input field containing '/'] [Browse... button]

At the bottom, there is a help icon (?), and navigation buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Step 7 Click **Next** to go to the **System** page, as shown in [Figure 2-13](#). Choose **Authentication by database user** and enter the username and password.

The username and password are those configured during SAP HANA software installation. The username is consistently set to **SYSTEM**.

Figure 2-13 System page



Step 8 Click **Next** and then **Finish**. Then, the SAP HANA Studio automatically connects to the database.

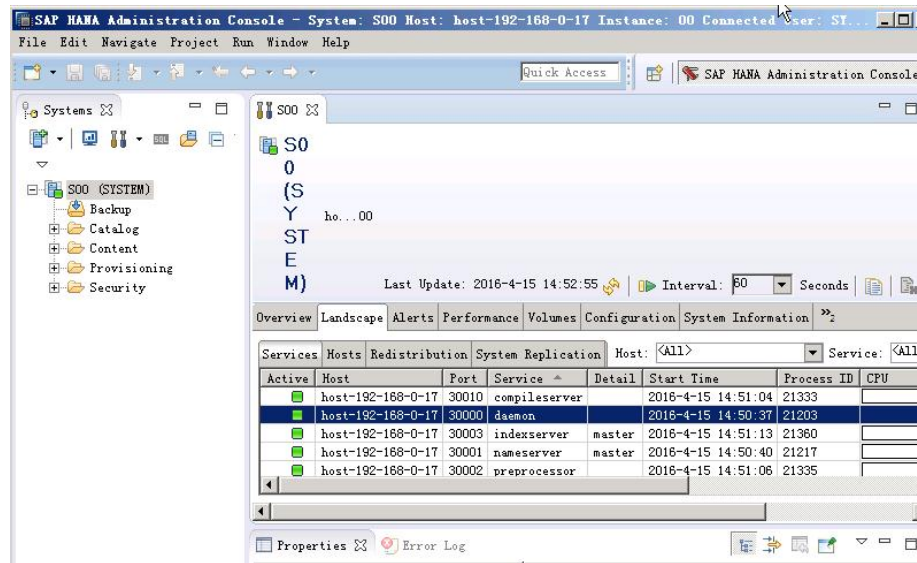
If the connection fails, check whether the database instance on the SAP HANA node is running.

Step 9 Under **System** of the **SAP HANA Administration Console** page, double-click the node to be checked.

Step 10 Click the **Landscape** tab on the right of the page and check the status of each process on the SAP HANA node.

Green indicates that the process is running properly.

Figure 2-14 Landscape page



----End

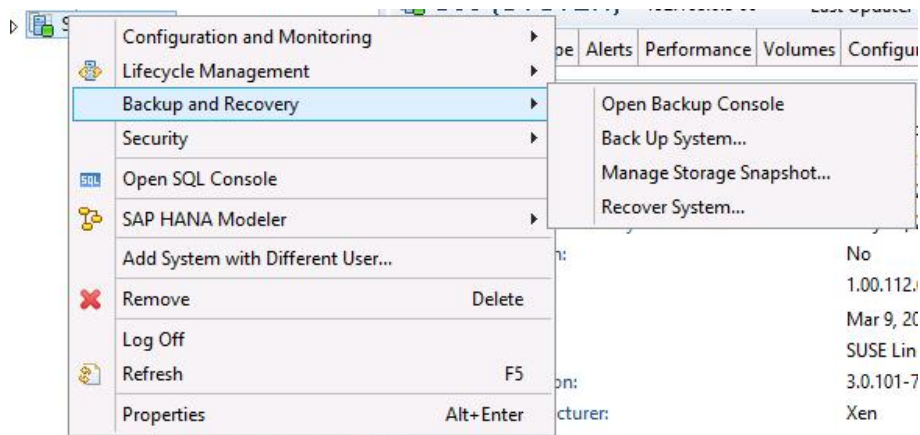
2.5.6 Configuring the Backup Path

A path is required for backing up SAP HANA data. This section uses a Windows ECS where SAP HANA Studio is deployed as an example when SAP HANA 1.0 is used.

Procedure

- Step 1** On the HANA Studio ECS, choose **Start > SAP HANA > SAP HANA Studio** to start the SAP HANA Studio software.
- Step 2** In the **System** area on the left, right-click the database node and choose **Backup and Recovery > Open Backup Console**, as shown in [Figure 2-15](#).

Figure 2-15 Open Backup Console menu



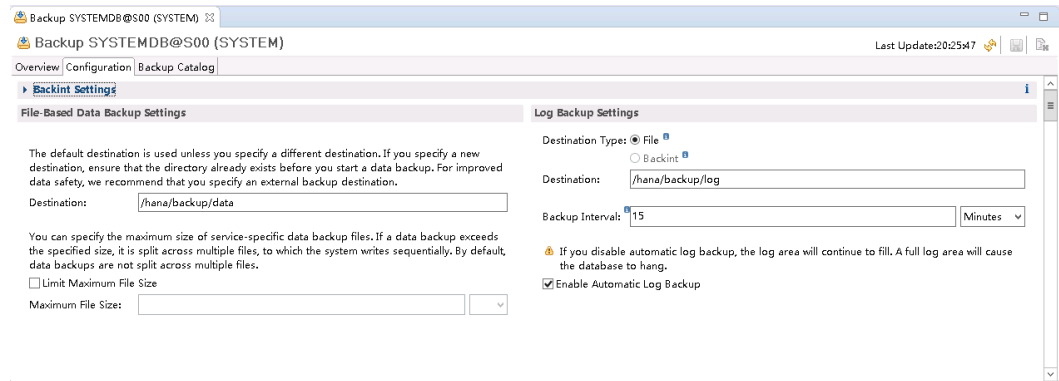
- Step 3** Click the **Configuration** tab on the right and configure the backup path, as shown in [Figure 2-16](#).

 **NOTE**

The backup paths are `/hana/backup/data` and `/hana/backup/log`.

Click the save icon in the upper right corner to save the configuration.


Figure 2-16 Configuring the backup path



Step 4 In the **System** area on the left, right-click the database node and choose **Backup and Recovery > Back Up System...** The **Specify Backup Settings** page is displayed.

Figure 2-17 Specify Backup Settings page

Specify Backup Settings

 There might be not enough disk space for the backup files. Estimated backup size: 1.61 GB.


Backup Type: Complete Data Backup


Destination Type: File

Backup Destination
The default destination is used unless you specify a different destination. If you specify a new destination, ensure that the directory already exists. For improved data safety, we recommend that you specify an external backup destination.

Backup Destination: /hana/backup

Backup Prefix: COMPLETE_DATA_BACKUP

 Note that customer-specific changes to the SAP HANA database configuration are not saved as part of the data backup.
More Information: SAP HANA Administration Guide

 < Back Next > Finish Cancel

Step 5 Use default settings and click **Next**. The **Review Backup Settings** page is displayed. Confirm configurations and click **Finish**. The system starts the backup task.

 **NOTE**

According to SAP requirements, data must be backed up immediately after the SAP HANA system is installed.

When SAP HANA 1.0 is used, you need to back up both the active and standby databases. When SAP HANA 2.0 is used, you need to back up both the system database and the tenant database.

Step 6 Click **Close** after the backup task is complete.

----End

2.5.7 Configuring SAP HANA Storage Parameters

Configure SAP HANA storage parameters based on SAP's requirements.

Only SAP HANA 1.0 needs to be configured because the default configurations of SAP HANA 2.0 meet the specified requirements.

For more information, see as follows:

- SAP Note 2186744 - FAQ: SAP HANA Parameters
- SAP Note 2267798 - Configuration of the SAP HANA Database during Installation Using hdbparam
- [SAP_HANA_Administration_Guide](#)
- SAP Note 2156526 - Parameter constraint validation on section indices does not work correctly with hdbparam
- SAP Note 2399079 - Elimination of hdbparam in HANA 2

Procedure

Step 1 Log in to an SAP HANA node.

Step 2 Run the following command to switch to the SAP HANA administrator:

```
su - s00adm
```

Step 3 Configure SAP HANA storage parameters.

```
hdbparam --paramset fileio.async_read_submit=on
```

```
hdbparam --paramset fileio.async_write_submit_active=on
```

```
hdbparam --paramset fileio.async_write_submit_blocks=all
```

Step 4 (Optional) Configure storage parameters on other SAP HANA nodes according to the preceding steps.

If multiple SAP HANA nodes exist, perform the same configuration for these parameters on other SAP HANA nodes.

----End

2.5.8 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 hwdatapviderp3
● hwdatapviderp3.service - Huawei dataprovider monitor service daemon
   Loaded: loaded (/etc/systemd/system/hwdatapviderp3.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/hwdatapviderp3.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

2.6 Installing SAP HANA (Single-Node Deployment with HA Required)

2.6.1 Formatting a Disk

In single-node deployment scenarios, the data volumes of SAP HANA nodes can be used only after they are formatted and attached to required directories. The SBD volume does not need to be formatted.

Procedure

Step 1 Log in to an SAP HANA node.

Use PuTTY to log in to the NAT server with an elastic IP address bound. Ensure that user **root** and the key file (.ppk file) are used for authentication. Then, use SSH to switch to the SAP HANA nodes.

Step 2 Check the disks that have not been formatted.

Run the following command to query the disks to be formatted:

```
fdisk -l
```

Determine the disks of the /usr/sap volumes, data volumes, log volumes, shared volumes, and swap volumes according to the disk capacity.

Step 3 Run the following command to create a disk directory:

```
mkdir -p /hana/log /hana/data /hana/shared /hana/backup /usr/sap
```

Step 4 Create and enable the swap partition. **dev/vdb** is used as an example.

```
mkswap /dev/vdb
```

```
swapon /dev/vdb
```

Step 5 Use LVM to logically create a data volume using two EVS disks. The following uses EVS disks **dev/vdb** and **dev/vdc** as an example.

1. Run the following command to create physical volumes:

```
pvcreate /dev/vdb /dev/vdc
```

2. Run the following command to create volume groups:

```
vgcreate vghana /dev/vdb /dev/vdc
```

3. Run the following command to query the available capacity of the volume group:

```
vgdisplay vghana
```

4. Create logical volumes. The following command uses two EVS disks to create a logical volume.

```
lvcreate -n lvhanadata -i 2 -l 256 -L 348G vghana
```

The parameters are described as follows:

- **-n**: Name of a logical volume
- **-i**: Number of logical extensions
- **-l**: Stripe size
- **-L**: Logical volume size

Step 6 Format disks and logical volumes. **dev/vdd**, **dev/vde**, and **dev/vdf** are used as examples.

```
mkfs.xfs /dev/vdd
```

```
mkfs.xfs /dev/vde
```

```
mkfs.xfs /dev/vdf
```

```
mkfs.xfs /dev/mapper/vghana-lvhanadata
```

Step 7 Write disk attaching relationships into the **/etc/fstab** file.

1. Run the following command to check the UUID of the disk:

```
blkid
```

2. Obtain the shared path in [Step 2.7](#) or `saphana_02_0075.xml#saphana_02_0075/li137231454101` in section [2.4.2 Creating an SFS File System](#). `PublicCloudAddress:/share-d6c6d9e2` is used as an example.

3. Write the attaching relationships between the disk UUID and shared path to the **/etc/fstab** file. UUID is used as an example here.

```
echo "UUID=ba1172ee-39b2-4d28-89b8-282ebabfe8f4 /hana/data xfs defaults 0 0" >>/etc/fstab
```

```
echo "UUID=d21734c9-44c0-45f7-a37d-02232e97fd3b /hana/log xfs defaults 0 0" >>/etc/fstab
```

```
echo "UUID=191b5369-9544-432f-9873-1beb2bd01de5 /hana/shared xfs defaults 0 0" >>/etc/fstab
```

```
echo "UUID=191b5369-9544-432f-9873-1beb2bd01de5 /usr/sap xfs defaults 0 0" >>/etc/fstab
```

```
echo "UUID=1b569544-1225-44c0-4d28-2e97fdeb2bd swap swap defaults 0 0" >> /etc/fstab
```

```
echo "PublicCloudAddress:/share-d6c6d9e2 /hana/backup nfs noatime,nodiratime,rdirplus,vers=3,wsz=1048576,rsize=1048576,noacl,nocto,proto=tcp,async 0 0" >>/etc/fstab
```

Step 8 Run the following command to attach all disks:

```
mount -a
```

Step 9 Check the disk mounting status. The following is an example:

```
# df -h
Filesystem                Size      Used Avail Use% Mounted on
devtmpfs                  126G       0 126G   0% /dev
tmpfs                      197G    80K 197G   0% /dev/shm
tmpfs                      126G    17M 126G   1% /run
tmpfs                      126G       0 126G   0% /sys/fs/cgroup
/dev/xvda                   50G    4.4G  43G  10% /
/dev/sdd                    254G    93G 162G  37% /hana/shared
/dev/mapper/vghana-lvhanadata 254G    67G 188G  27% /hana/data
/dev/sde                    164G    6.3G 158G   4% /hana/log
/dev/sdf                     50G   267M   50G   1% /usr/sap
/dev/xvdb                    10G     5G   5G  50% /swap
PublicCloudAddress:/share-d6c6d9e2 384G     0 384G   0% /hana/backup
tmpfs                       26G       0  26G   0% /run/user/1002
tmpfs                       26G       0  26G   0% /run/user/480
tmpfs                       26G    16K  26G   1% /run/user/0
```

Step 10 Format disks of the other ECS.

Switch to the other SAP HANA node using SSH and format disks of the node by repeating [Step 2](#) to [Step 8](#).

----End

2.6.2 Installing the SAP HANA Software

SAP HANA database software must be deployed on ECSs. This section uses the SAP HANA 1.0 installation package as an example. You can download the package from the official website.

Prerequisites

- You have prepared related resources. For details, see section "Preparing Resources".
- You have created ECSs, formatted disks attached to them, and completed required configurations.
- Ensure that the OS firewall of the new node is disabled. For details about how to disable the OS firewall, see [6.4 Modifying OS Configurations](#).

Procedure

Step 1 Log in at <https://support.sap.com/swdc> to download the installation package, and perform the installation.

1. Switch to **SAP Software Download Center**.
 - Choose **Software Downloads**.
 - Choose **INSTALLATIONS & UPGRADES**.
 - Choose **By Alphabetical Index (A-Z)**.
 - Choose **H**.
 - Choose **SAP HANA PLATFORM EDITION**.
 - Choose **DOWNLOADS**.
2. Locate the target package and download it to the local hard disk.
3. Upload the obtained installation package to the **/hana/shared** directory on the ECS where the SAP HANA software is to be installed and decompress it. For example, the installation package is

51052383_part1.exe

cd /hana/shared

unrar x 51052383_part1.exe

4. Run the following command to enter the directory where the installation file is stored, taking **SAP_HANA_DATABASE** as an example:

For example, if the installation file is stored in **/DATA_UNITS/HDB_SERVER_LINUX_X86_64**, run the following commands:

cd 51052383

cd DATA_UNITS/HDB_SERVER_LINUX_X86_64

5. Run the following command to assign execute permissions to the directory:

chmod -R 777 /hana

6. Run the following command to perform the installation:

./hdblcm --ignore=check_signature_file

The following information is displayed:

Choose installation

Index	System	Database Properties
1	Install new system	
2	Extract components	
3	Exit (do nothing)	

Enter selected system index [2]:

7. Enter **1** and press **Enter**.

The following information is displayed:

Select additional components for installation:

Index	Components	Description
1	server	No additional components
2	all	All components

Enter comma-separated list of the selected indices [1]:

8. Enter **1** and press **Enter**.
9. Configure parameters as prompted on the page one by one.

 **NOTE**

- During the configuration, press **Enter** if you want to retain the default setting.
- If a parameter is incorrectly set and you have pressed **Enter**, you can press **Ctrl+C** to exit the configuration and run the **./hdblcm --ignore=check_signature_file** command to enter the installation page again.

Table 2-31 lists the parameter configuration requirements.

Table 2-31 Requirements for configuring SAP HANA installation parameters

Parameter	Description
Installation Path	Specifies the installation path, which defaults to /hana/shared/\$SID . The default value is recommended.
Local Host Name	Specifies the local host name.
Do you want to add additional hosts to the system	Enter the value n .
SAP HANA System ID	Specifies the SAP HANA system ID, for example, S00 .
Instance Number	Specifies the SAP HANA instance number, for example, 00 . The instance ID is used in Security Group Rules , which must be the same as the planned one.
Database Mode	Specifies the database deployment mode. Retain the default value single_container . You do not need to set this parameter when installing HANA2.0 and the default value is multiple container .
System Usage	Specifies the SAP HANA system type. Set this parameter as required. This parameter is stored in the global.ini file.
Location of Data Volumes Specifies	Specifies the system data volume directory, which is /hana/data/\$SID .
Location of Log Volumes	Specifies the system log volume directory, which is /hana/log/\$SID .
Restrict maximum memory allocation?	Specifies whether maximum memory allocation is restricted, which defaults to n .
Certificate Host Name	Specifies the ECS name that is used to generate a self-signed SSL certificate for the SAP Host Agent.
SAP Host Agent User (sapadm) Password	Enter the SAP Host Agent user password.
System Administrator (s00adm) Password	Enter the system administrator password.
System Administrator Home Directory	Use the default value.
System Administrator Login Shell	Use the default value.

Parameter	Description
System Administrator User ID	Use the default value.
ID of User Group	Use the default value.
Database User (SYSTEM) Password	Enter the database user password.

10. After you complete the configuration, the system displays the message "Restart system after machine reboot?"
 - In single-node scenarios where HA is not required, enter **y**.
 - In single-node scenarios where HA is required, if automatic active/standby switchover is not required, enter **y**; if automatic active/standby switchover (HAE) is required, enter **n**.

Then, press **Enter**. The system displays the installation summary.

11. After confirming the installation information is correct, in the **Do you want to continue?** dialog box, enter **y** and press **Enter** to start to installation. After the installation is complete, the prompt **Installation done** is displayed.

Step 2 Verify the installation.

1. Run the following command to switch to the **/hana/shared/\$SID/HDB00/** directory:

The following command is used as an example:

cd /hana/shared/S00/HDB00

2. Switch to the database system administrator.

Account **s00adm** is displayed on the page during the installation. Run the following command:

su - s00adm

3. Run the following command to query the database version:

If the version can be queried, the database software is installed.

HDB -version

After the database is installed, the system returns the version. **Figure 2-18** shows an example.

Figure 2-18 SAP HANA version information

```
HDB version info:
version:          1.00.112.05.1469552341
branch:          fa/newdb100_rel
git hash:        a9abfc92240a2d6e0d96f15c037739b49fd21cd8
git merge time:  2016-07-26 18:59:01
weekstone:       0000.00.0
compile date:    2016-07-26 19:12:32
compile host:    ld7272
compile type:    rel
```

Step 3 Check whether the database process is running properly.

1. Run the following command to check the process, taking the SAP HANA instance with ID 00 as an example:

```
sapcontrol -nr 00 -function GetProcessList
```

In the terminal display, if the **dispstatus** value is **GREEN**, the process is running properly.

```
13.04.2017 16:04:15
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
hdbdaemon, HDB Daemon, GREEN, Running, 2017 04 13 11:18:33, 4:45:42, 3013
hdbcompilesrv, HDB Compilesrv, GREEN, Running, 2017 04 13 11:18:42, 4:45:33,
3154
hdbindexsrv, HDB Indexsrv, GREEN, Running, 2017 04 13 11:18:47, 4:45:28, 3180
hdbnamesrv, HDB Namesrv, GREEN, Running, 2017 04 13 11:18:34, 4:45:41, 3027
hdbpreprocessor, HDB Preprocessor, GREEN, Running, 2017 04 13 11:18:42, 4:45:33, 3156
hdbwebdispatcher, HDB Web Dispatcher, GREEN, Running, 2017 04 13 11:19:09, 4:45:06,
3513
hdbxsengine, HDB XSEngine, GREEN, Running, 2017 04 13 11:18:47, 4:45:28, 3182
```

2. Run the following command to return to user **root**:
exit

Step 4 Switch to the other SAP HANA node using SSH and install the SAP HANA software on it by repeating [Step 1](#) to [Step 3](#).

During the software installation, ensure that the installation information of this HANA ECS is the same as that of the previous HANA ECS, excepting the host name.

----End

2.6.3 Installing the SAP HANA Studio on a Windows ECS

SAP HANA Studio manages SAP HANA. After SAP HANA nodes are deployed, you need to install the SAP HANA Studio and use it to manage the SAP HANA nodes.

This section describes how to install the SAP HANA Studio on a Windows ECS.

Prerequisites

- You have prepared related resources. For details, see section "Preparing Resources".
- You have created ECSs, formatted disks attached to them, and installed the SAP HANA.
- The firewall on the target ECS has been disabled.
- Remote login to the target ECS has been enabled.

Procedure

Step 1 Use the Remote Desktop Protocol (RDP) and elastic IP address to log in to the SAP HANA Studio ECS.

Use the username **Administrator** and the password obtained in section [6.1 Obtaining the Password for Logging In to a Windows ECS](#) to log in to the SAP HANA Studio ECS.

- Step 2** Upload the installation package obtained from the SAP official website to the SAP HANA Studio ECS.
- Step 3** Decompress the installation package and navigate to the directory where SAP HANA Studio is stored.
- Step 4** On the Windows page, switch to the directory where the SAP HANA Studio installation package is stored and double-click **hdbsetup.exe** to open the installation wizard page.
- Step 5** Select the installation path and click **Next**.
- Step 6** On the **Select Features** page, select the features to be installed and click **Next**.
You are advised to select all features.
- Step 7** Confirm all information on the **Review & Confirm** page and click **Install**.
- Step 8** An installation page is displayed. Continue the installation. When the installation is complete, the system displays the message "You have successfully installed the SAP HANA Studio."
- Step 9** Click **Finish**.
----End

2.6.4 Installing the SAP HANA Studio on a Linux ECS

SAP HANA Studio manages SAP HANA. After SAP HANA nodes are deployed, you need to install the SAP HANA Studio and use it to manage the SAP HANA nodes.

This section describes how to install the SAP HANA Studio on a Linux ECS.

Prerequisites

- You have prepared related resources. For details, see section "Preparing Resources".
- You have created ECSs, formatted disks attached to them, and installed the SAP HANA.
- The firewall on the target ECS has been disabled.

Procedure

- Step 1** Log in to the SAP HANA Studio ECS with an elastic IP address bound as user **root** using the key file.
- Step 2** Upload the obtained installation package to the **/hana/shared** directory on the ECS where the SAP HANA Studio is to be installed and decompress it.

Enter the directory where the installation file is stored. For example, if the installation file is stored in **/DATA_UNITS/HDB_STUDIO_LINUX_X86_64**, run the following command:

cd /DATA_UNITS/HDB_STUDIO_LINUX_X86_64
- Step 3** Assign operation permissions to the directory where the installation packages are stored.

For example, if the directory is **HDB_STUDIO_LINUX_X86_64**, run the following command:

```
chmod 777 -R HDB_STUDIO_LINUX_X86_64
```

Step 4 Switch to the directory and perform the installation. The SAP HANA Studio installation page is displayed.

```
./hdbsetup
```

Step 5 Select the installation path and click **Next**.

Step 6 On the **Select Features** page, select the features to be installed and click **Next**.

You are advised to select all features.

Step 7 Confirm all information on the **Review & Confirm** page and click **Install**.

Step 8 An installation page is displayed. Continue the installation. When the installation is complete, the system displays the message "You have successfully installed the SAP HANA Studio."

Step 9 Click **Finish**.

Step 10 Go to [Step 5](#) to select the installation path, edit the **hdbstudio.ini** file, and add parameters to configure the GTK version.

```
vi hdbstudio.ini
```

Add the following parameters:

```
--launcher.GTK_version
```

```
2
```

An example is provided as follows:

```
-startup  
plugins/org.eclipse.equinox.launcher_1.3.201.v20161025-1711.jar  
--launcher.library  
plugins/org.eclipse.equinox.launcher.gtk.linux.x86_64_1.1.401.v20161122-1740  
--launcher.GTK_version  
2  
--launcher.XXMaxPermSize  
512m
```

Step 11 (Optional) If the version is not configured in [Step 10](#), run the following commands before starting **hdbstudio** on the Linux OS:

```
export SWT_GTK3=0
```

```
./hdbstudio
```

```
----End
```

2.6.5 Connecting SAP HANA Nodes to the SAP HANA Studio

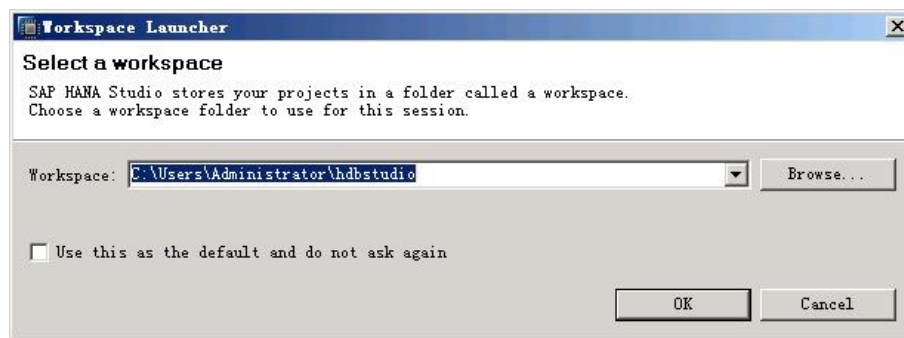
SAP HANA nodes can be managed only after they are connected to the SAP HANA Studio. This section uses a Windows ECS where the SAP HANA Studio is deployed as an example.

Procedure

Step 1 Start the SAP HANA Studio.

On the ECS where the SAP HANA Studio is deployed, choose **Start > SAP HANA > SAP HANA Studio**. Then, the system displays the SAP HANA Studio management page and the **Workspace Launcher** dialog box.

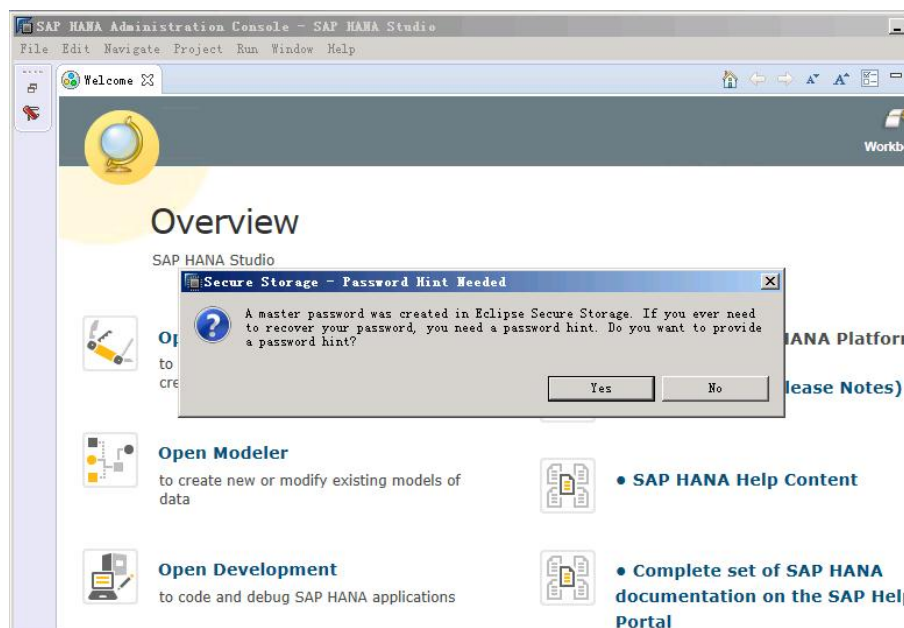
Figure 2-19 Workspace Launcher page



Step 2 Specify the **Workspace** directory, select **Use this as the default and do not ask me again**, and click **OK**.

Step 3 The **Security Storage** dialog box is displayed, as shown in [Figure 2-20](#). Click **No**.

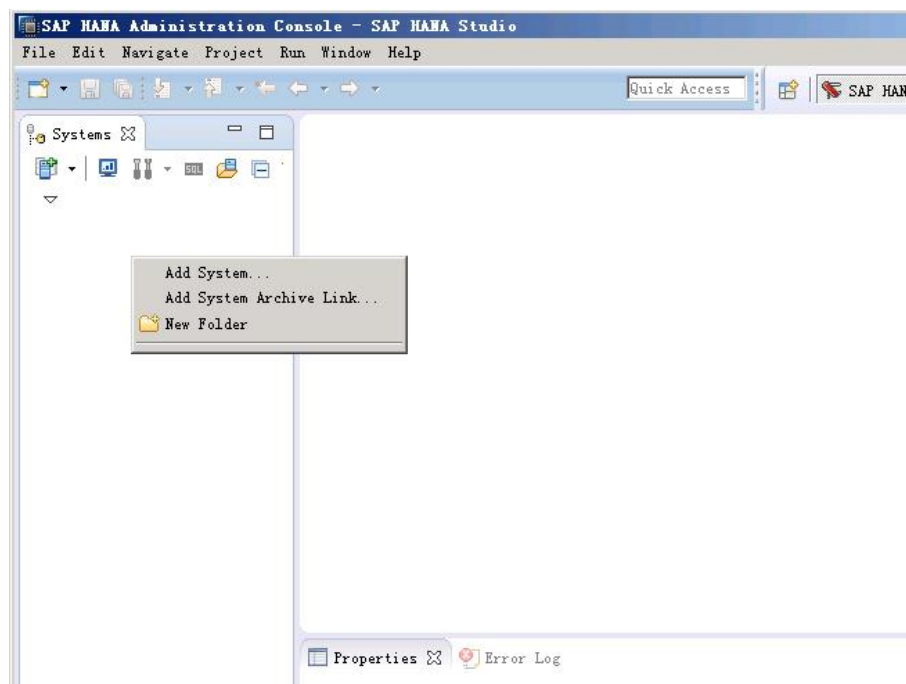
Figure 2-20 Security Storage dialog box



Step 4 On the **Overview** page, click **Open Administration Console** to enter the **SAP HANA Administration Console** page.

Step 5 Right-click the blank area under **System**, as shown in [Figure 2-21](#).

Figure 2-21 SAP HANA management console page

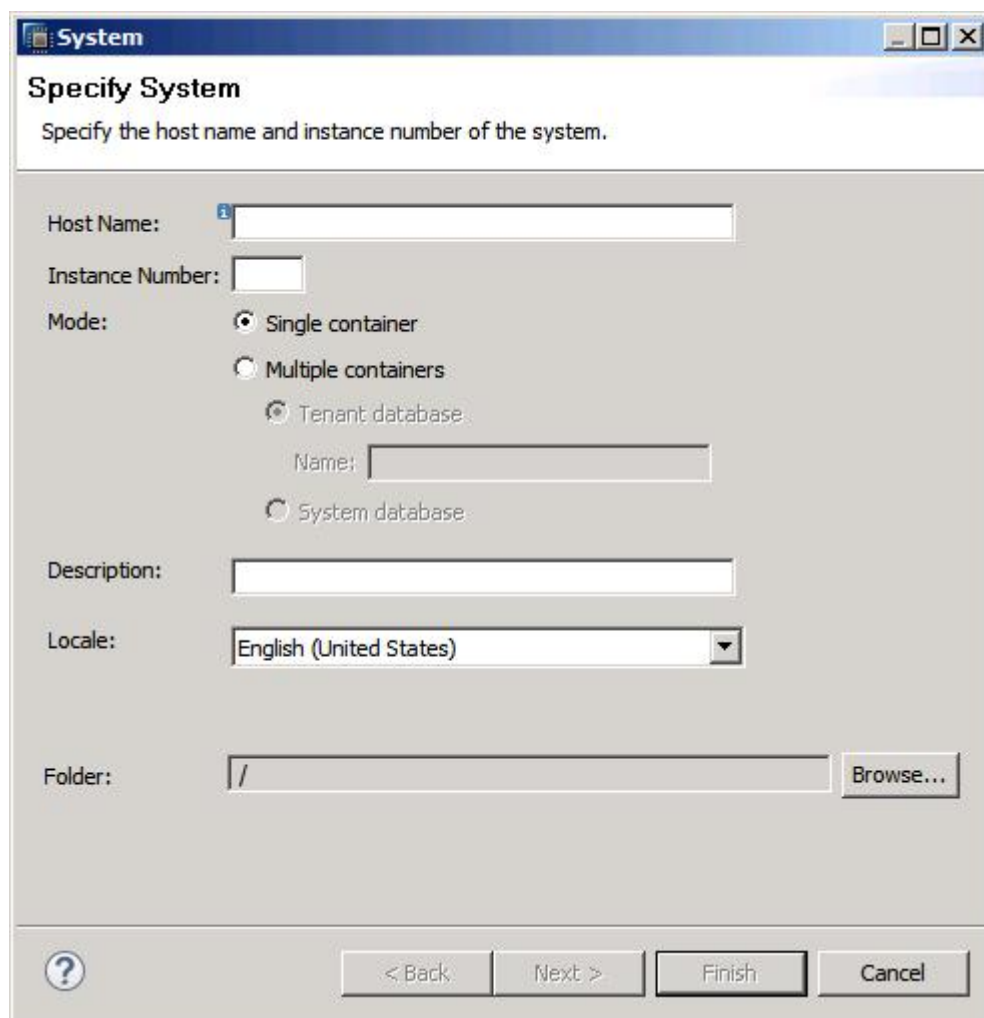


Step 6 Choose **Add System**. The **Specify System** page is displayed, as shown in [Figure 2-22](#). Configure parameters.

Key parameters are as follows:

- **Host Name:** Enter the service or client plane IP address of the SAP HANA ECS.
- **Instance Number:** Enter the number of the instance on the SAP HANA node.
- **Mode:** Select a mode based on actual requirements. If SAP HANA 2.0 is installed, select **Multiple containers** and **Tenant database** or **System database** based on the actual requirements.

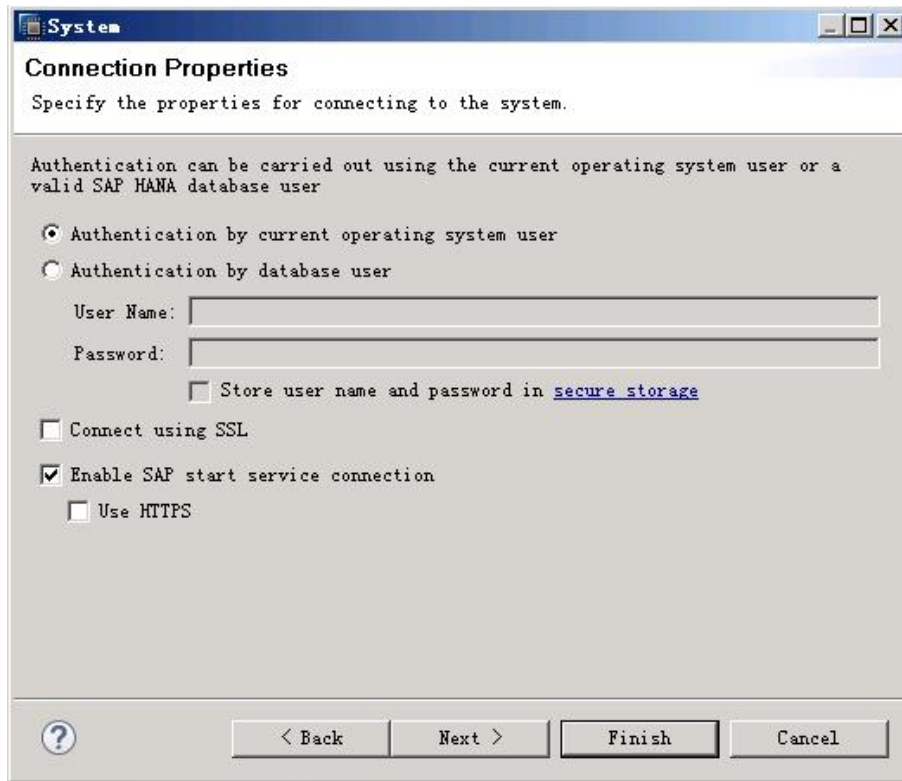
Figure 2-22 Specify System page



Step 7 Click **Next** to go to the **System** page, as shown in [Figure 2-23](#). Choose **Authentication by database user** and enter the username and password.

The username and password are those configured during SAP HANA software installation. The username is consistently set to **SYSTEM**.

Figure 2-23 System page



Step 8 Click **Next** and then **Finish**. Then, the SAP HANA Studio automatically connects to the database.

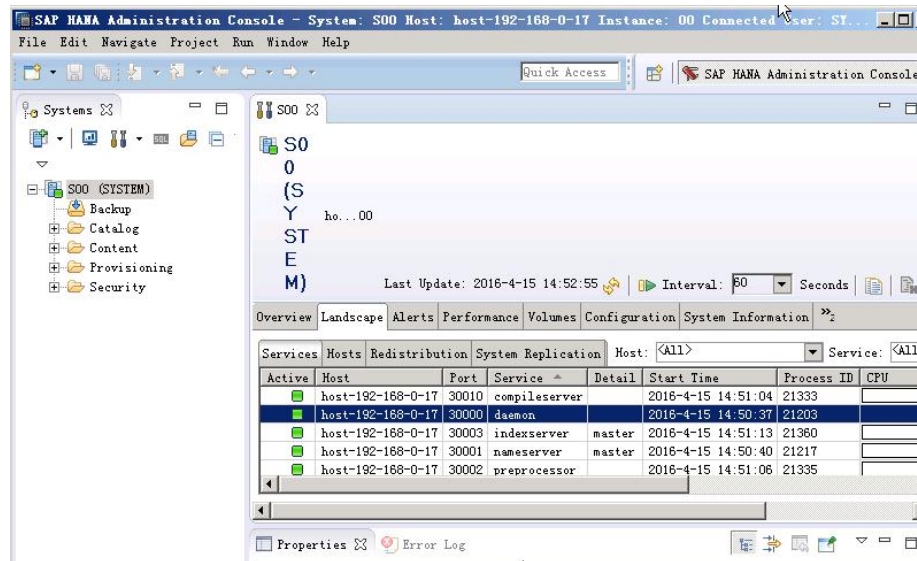
If the connection fails, check whether the database instance on the SAP HANA node is running.

Step 9 Under **System** of the **SAP HANA Administration Console** page, double-click the node to be checked.

Step 10 Click the **Landscape** tab on the right of the page and check the status of each process on the SAP HANA node.

Green indicates that the process is running properly.

Figure 2-24 Landscape page



Step 11 Connect the other SAP HANA node to the SAP HANA Studio.

Repeat **Step 5** to **Step 10** to connect the other SAP HANA node to the SAP HANA Studio.

----End

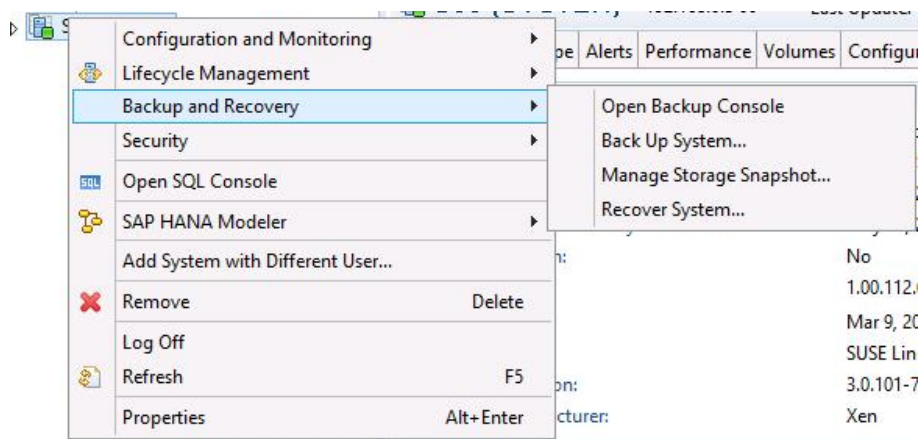
2.6.6 Configuring the Backup Path

A path is required for backing up SAP HANA data. This section uses a Windows ECS where SAP HANA Studio is deployed as an example when SAP HANA 1.0 is used.

Procedure

- Step 1** On the HANA Studio ECS, choose **Start > SAP HANA > SAP HANA Studio** to start the SAP HANA Studio software.
- Step 2** In the **System** area on the left, right-click the database node and choose **Backup and Recovery > Open Backup Console**, as shown in **Figure 2-25**.

Figure 2-25 Open Backup Console menu



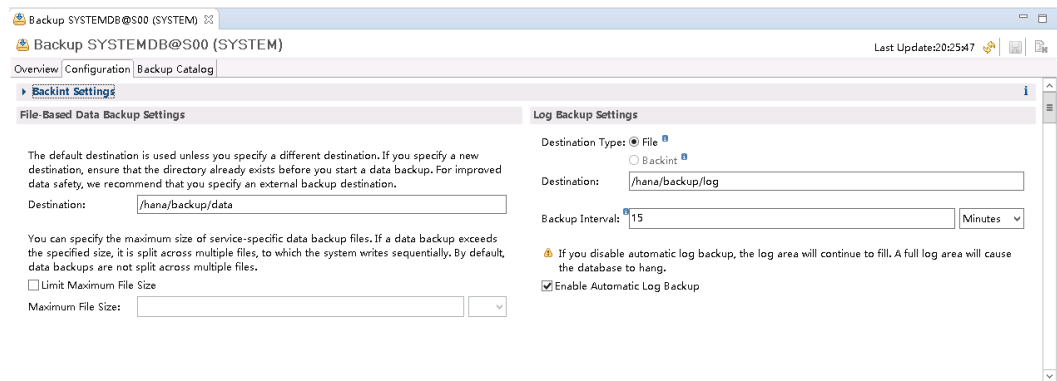
Step 3 Click the **Configuration** tab on the right and configure the backup path, as shown in **Figure 2-26**.

 **NOTE**

The backup paths are **/hana/backup/data** and **/hana/backup/log**.

Click the save icon in the upper right corner to save the configuration.

Figure 2-26 Configuring the backup path



Step 4 In the **System** area on the left, right-click the database node and choose **Backup and Recovery > Back Up System....** The **Specify Backup Settings** page is displayed.

Figure 2-27 Specify Backup Settings page

Specify Backup Settings

⚠ There might be not enough disk space for the backup files. Estimated backup size: 1.61 GB.

Backup Type: Complete Data Backup

Destination Type: File

Backup Destination

The default destination is used unless you specify a different destination. If you specify a new destination, ensure that the directory already exists. For improved data safety, we recommend that you specify an external backup destination.

Backup Destination: /hana/backup

Backup Prefix: COMPLETE_DATA_BACKUP

i Note that customer-specific changes to the SAP HANA database configuration are not saved as part of the data backup.
More Information: SAP HANA Administration Guide

? < Back Next > Finish Cancel

Step 5 Use default settings and click **Next**. The **Review Backup Settings** page is displayed. Confirm configurations and click **Finish**. The system starts the backup task.

NOTE

According to SAP requirements, data must be backed up immediately after the SAP HANA system is installed.

When SAP HANA 1.0 is used, you need to back up both the active and standby databases. When SAP HANA 2.0 is used, you need to back up both the system database and the tenant database.

Step 6 Click **Close** after the backup task is complete.

----End

2.6.7 Configuring the System Replication

After installing two single SAP HANA nodes for HA, configure the System Replication function on them.

 NOTE

In the cross-AZ or cross-region DR scenario, configure the Multitier System Replication function after the System Replication function between the nodes for HA has been configured successfully.

Configuration scheme: Set the standby HA node as the active node and the DR node as the standby node. The DR node synchronizes data with the standby HA node. Configure the mode of Multitier System Replication to **async**.

Prerequisites

- Before configuring HA, make sure that you have enabled data backup and backed up the database on the two SAP HANA nodes. For details, see section [2.6.6 Configuring the Backup Path](#).
- Before configuring HA, make sure that you have written the mapping between the IP addresses of the two SAP HANA nodes and the node names (see section [2.4.6 Configuring the Mapping Between SAP HANA Host Names and IP Addresses](#)) into the `/etc/hosts` files of the two nodes.

Procedure

Step 1 Configure the active node.

1. Use PuTTY to log in to the NAT server with an elastic IP address bound. Ensure that user **root** and the key file (.ppk file) are used for authentication. Then, use SSH to switch to the ECS that will work as the active node.
2. Switch to the administrator mode:

```
su - $S/Dadm
```

For example, run the following command to switch to the administrator mode:

```
su - s00adm
```

Information similar to the following is displayed:

```
hana001:/hana/shared/S00/HDB00>
```

3. Run the following command to configure the SAP HANA node as the active one:

```
hdbnsutil -sr_enable --name=siteA
```

In the preceding command, **siteA** is the name of the active HANA node, which can be customized.

For example, if the name of the active HANA node is **hana001**, run the following command:

```
hdbnsutil -sr_enable --name=hana001
```

Step 2 Configure the standby HANA node.

1. Switch to the other SAP HANA node using SSH.
2. Enter the administrator mode:

```
su - $S/Dadm
```

For example, run the following command to enter the administrator mode:

```
su - s00adm
```

Information similar to the following is displayed:

```
hana002:/hana/shared/S00/HDB00>
```

3. Run the following command to stop the SAP HANA database:

HDB stop

4. Run the following command to enable System Replication:

```
hdbnsutil -sr_register --remoteHost=remoteHostName --  
remoteInstance=remoteInstanceNumber --replicationMode=sync --  
name=siteB
```

In the preceding command, **remoteHostName** is the name of the active node, **remoteInstanceNumber** is the instance ID of the active node, and **SiteB** is the name of the standby node, which can be customized.

For example, if **remoteHostName** is **hana001**, **remoteInstanceNumber** is **00**, and **SiteB** is **hana002**, run the following command:

```
hdbnsutil -sr_register --remoteHost=hana001 --remoteInstance=00 --  
replicationMode=sync --name=hana002
```

NOTE

- If the **SSFS_S00.DAT** and **SSFS_S00.KEY** files on the active and standby nodes are different when the SAP HANA 2.0 installation package is used, see the official SAP document [SAP Note 2369981](#) to resolve the problem.
 - In the cross-AZ DR scenario, set the mode of Multitier System Replication to **async**, that is, **replicationMode=async**.
5. Run the following command to start the SAP HANA database:

HDB start

Step 3 Query the System Replication status in the SAP HANA system.

1. Run the following command in the administrator mode on the active node CLI:

hdbnsutil -sr_state

Information similar to the following is displayed:

```
checking for active or inactive nameserver ...  
System Replication State  
~~~~~  
mode: primary  
site id: 1  
site name: hana001  
Host Mappings:  
~~~~~  
hana001 -> [hana001] hana001  
hana001 -> [hana002] hana002  
done.
```

2. Query the active node status on SAP HANA Studio.

NOTE

In actual application scenarios, the service software has connected to the SAP HANA node. If you manually switch the SAP HANA node, you must change the IP address of the SAP HANA node on the service software and restart the service software.

----End

2.6.8 Configuring HA on SAP HANA Nodes

Use scripts (HAE) to configure HA on SAP HANA nodes, improving SAP HANA node reliability.

This only applies to SAP HANA nodes running the OS SUSE Linux Enterprise Server 12 SP1 for SAP or later for automatic active/standby switchovers.

In the cross-AZ HA scenario, three ECSs are required. Each ECS is bound to a SCSI disk and iSCSI configuration is required for SBD. For details, see section [2.6.11 Configuring iSCSI \(Cross-AZ HA Deployment\)](#).

Prerequisites

SSH switching between SAP HANA nodes has been allowed.

Procedure

Step 1 Attach the SBD volume to the other SAP HANA node.

The reason is as follows: When one SAP HANA node is created, the SBD volume is attached to it. This SBD volume must be attached to the other SAP HANA node.

1. On the management console, click **Service List** and choose **Computing > Elastic Cloud Server**. On the left side of the page, choose **Elastic Cloud Server**. The system displays all ECSs on the right side of the page.
2. Locate the HANA ECS attached with the SBD volume by ECS name and click its name.
3. On the page providing details about the ECS, click the **EVS** tab and locate the disk of the SBD volume. Then, click the target data disk.
4. On the page providing details about the data disk, view and record its mount point. Then, click the data disk **ID**.
5. On the page that is displayed, click **Mount Point** and then **Attach** to switch to **Attach Disk** page.
6. On the **Attach Disk** page, select the target ECS to which the disk is to be attached, ensure that the device name of the ECS is the same as that of the ECS involved in [Step 1.4](#), and attach the disk to the ECS.

Step 2 Create a floating IP address.

1. On the management console, click **Service List** and choose **Computing > Elastic Cloud Server**. On the left side of the page, choose **Elastic Cloud Server** to switch to the **Elastic Cloud Server** page.
2. Locate an SAP HANA node and click the HANA ECS name. Then, the page for the HANA ECS details is displayed.
3. Click the **NICs** tab and then **Manage Virtual IP Address** in the row of the cloud management or backup plane NIC. Then, the system displays the **Virtual IP Addresses** page.
4. Click **Assign Virtual IP Address** to assign a floating IP address. Locate the row that contains the target IP address, click **Bind to Server** to bind the IP address to the target ECS, and repeat this operation to bind the IP address to other ECSs.

Step 3 Use PuTTY to log in to the NAT server with an elastic IP address bound. Ensure that user **root** and the key file (.ppk file) are used for authentication. Then, use SSH to switch to the SAP HANA node that works as the active node.

Step 4 Run the following commands to check whether the dependency packages **patterns-ha-ha_sles** and **sap-suse-cluster-connector** have been installed:

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

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

- If yes, go to [Step 5](#).
- If no, run the following commands:

```
zypper in -y patterns-ha-ha_sles  
zypper in -y sap-suse-cluster-connector
```

Step 5 Download scripts and configure the file.

1. Download scripts and configure the file.

Access the URL for your region. For detailed URLs, see section [2.3.1 Software and Tools](#). The following command uses the URL for **CN-Hong-Kong** as an example:

```
wget https://obs-sap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip -P /hana/shared
```

2. Run the following commands to decompress the file:

```
cd /hana/shared  
unzip ha_auto_script.zip
```

Step 6 Modify the configuration file.

```
vi /hana/shared/ha_auto_script/hana_ha.cfg
```

Set the parameters in the configuration file based on the actual requirements. The following is an example:

```
[masterNode]
# Host name of the active node
masterName=hana001
# Heartbeat IP address of the active node
masterHeartbeatIP1=10.0.4.2
masterHeartbeatIP2=

[slaveNode]
# Host name of the standby node
slaveName=hana002
# Heartbeat IP address of the standby node
slaveHeartbeatIP1=10.0.4.3
slaveHeartbeatIP2=

[trunkInfo]
# Floating IP address of SAP HANA
hanaBusinessIP=10.0.3.103

[hanaInfo]
# SBD volume path
SBDDDevice=/dev/sdc,/dev/sdd,/dev/sde
# SAP HANA administrator account
hanaUser=s00adm
# SAP HANA instance number
InstanceNumber=00
```

 NOTE

This script supports the configuration of the two heartbeat network planes. During the configuration, you need to add the IP addresses of the server or client plane after **masterHeartbeatIP2** and **slaveHeartbeatIP2** parameters respectively in the script.

In the cross-AZ scenario, configure **SBDDevice** to the drive letters of SBD volumes on the three ECSs. For example, **SBDDevice=/dev/sbd1,/dev/sbd2,/dev/sbd3**.

Step 7 Run the following commands to grant the execute permission to the script:

```
cd ha_auto_script
chmod +x hana_auto_ha.sh
```

Step 8 Execute the script.

```
sh hana_auto_ha.sh
```

 NOTE

- If the script execution fails, you have to run the command **sh hana_auto_ha.sh unconf** to roll back manually before executing the script again. In addition, configure the **ha_auto.cfg** file based on the latest drive letter of the SBD volume.
- After the switchover between active and standby nodes is complete, configure the new standby node to make HA take effect. Perform the operations described as follows:

1. Run the following command on the standby node to switch to the administrator mode:

```
su - <SID>adm
```

2. Stop the database of the standby node.

```
HDB stop
```

3. Register the standby node with the active node.

Set **secondary** to the host name of the new active node. Set **site_name** to the original active node name defined when configuring System Replication.

```
hdbnsutil -sr_register --remoteHost=<secondary> --
remotelInstance=<instance_number> --replicationMode=sync --name=<site_name>
```

4. Start the database on the standby node and exit the administrator mode.

```
HDB start
```

```
exit
```

5. Run the following command on both the active and standby nodes to start the HAE service:

```
systemctl start pacemaker
```

6. Clear resources on the original active node (current standby node).

rsc_SAPHana_SLE_HDB00 is an example resource name, which can be obtained by running the **crm_mon - r1** command. Set **primary** to the name of the host on which the standby node is deployed.

```
crm resource cleanup <rsc_SAPHana_SLE_HDB00> <primary>
```

The following information is displayed if the command is successfully executed:

```
Online: [ hana001 hana002 ]
Full list of resources:
Clone Set: cln_SAPHanaTopology_SLE_HDB00 [rsc_SAPHanaTopology_SLE_HDB00]
  Started: [ hana001 hana002 ]
rsc_ip_SLE_HDB00?(ocf::heartbeat:IPaddr2):?Started hana001
stonith-sbd?(stonith:external/sbd):?Started hana001
Master/Slave Set: msl_SAPHana_SLE_HDB00 [rsc_SAPHana_SLE_HDB00]
```

```
Masters: [ hana001 ]
Slaves: [ hana002 ]
All Complete!
```

Step 9 Connect SAP HANA nodes to the SAP HANA Studio again.

Step 10 On the SAP HANA Studio, delete the two connected SAP HANA nodes. Then, use the floating IP address of the SAP HANA nodes to connect them to the SAP HANA Studio again and configure the backup path.

 **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

2.6.9 Configuring SAP HANA Storage Parameters

Configure SAP HANA storage parameters based on SAP's requirements.

Only SAP HANA 1.0 needs to be configured because the default configurations of SAP HANA 2.0 meet the specified requirements.

For more information, see as follows:

- SAP Note 2186744 - FAQ: SAP HANA Parameters
- SAP Note 2267798 - Configuration of the SAP HANA Database during Installation Using hdbparam
- [SAP_HANA_Administration_Guide](#)
- SAP Note 2156526 - Parameter constraint validation on section indices does not work correctly with hdbparam
- SAP Note 2399079 - Elimination of hdbparam in HANA 2

Procedure

Step 1 Log in to an SAP HANA node.

Step 2 Run the following command to switch to the SAP HANA administrator:

```
su - s00adm
```

Step 3 Configure SAP HANA storage parameters.

```
hdbparam --paramset fileio.async_read_submit=on
```

```
hdbparam --paramset fileio.async_write_submit_active=on
```

```
hdbparam --paramset fileio.async_write_submit_blocks=all
```

Step 4 (Optional) Configure storage parameters on other SAP HANA nodes according to the preceding steps.

If multiple SAP HANA nodes exist, perform the same configuration for these parameters on other SAP HANA nodes.

----End

2.6.10 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

2.6.11 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. [Table 2-32](#) lists the ECS specifications.

If an SAP NetWeaver system is deployed across three AZs, create an ECS in each AZ. If an SAP NetWeaver system 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 2-32 ECS specifications

OS	SUSE Linux Enterprise Server 12 SP1
Flavor	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. Run the following command to update the software source:

```
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 HANA node):

```
zypper in open-iscsi
```

```
----End
```

Server side configuration

Step 1 Log in to a server side ECS.

Step 2 Run the following commands to configure automatic service startup:

```
systemctl enable targetcli
```

```
systemctl enable target
```

Step 3 Run the following command to use the `/dev/sda` disk to create an lblock device named `stonith_bd`:

```
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 4 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 5 Create a target using the queried IQN.

targetcli /iscsi create *Queried IQN*

Information similar to the following is displayed:

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

Step 6 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 lblock device created in [Step 3](#).

Step 7 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** in [Step 5](#).

Step 8 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***

Step 9 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**

Step 10 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 11 Log in to the other two ECSs of the server side one by one and repeat [Step 2](#) to [Step 10](#) to configure the server side.

----End

Client side configuration

Step 1 Log in to an SAP HANA node (client side) and attach the iSCSI disk of a server side ECS to the SAP HANA node.

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

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

 **NOTE**

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

Step 2 Run the following command to attach iSCSI disks automatically once the SAP HANA node starts:

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

 **NOTE**

- `iqn.2003-01.org.linux-iscsi.scsi-0003.x8664:sn.38370da481a5` is the ID of `iqn` in [Step 5](#).
- `10.0.3.250` is the IP address of a server side ECS.

Step 3 Log in to other SAP HANA nodes and repeat [Step 1](#) to [Step 2](#) to configure all SAP HANA nodes of the client side.

----End

3 Management and Monitoring

Managing the Public Cloud Resources Used by SAP HANA

You can use Cloud Eye on the public cloud platform to monitor and manage public cloud resources, such as Elastic Cloud Server (ECS) and Elastic Volume Service (EVS) resources, used by SAP HANA.

For example, Cloud Eye monitors the CPU usage and disk read/write rate of the ECS where SAP HANA is deployed and generates alarms when the metrics exceed alarm thresholds.

For more information, see Cloud Eye introduction and *Cloud Eye User Guide*.

Managing SAP HANA

SAP provides customers with various tools and instructions to manage SAP HANA.

- To manage SAP HANA, SAP supports:
 - Landscape-, system-, and database-level monitoring and management.
 - Security-related monitoring and configuration.
 - High reliability and scalability management

For details, see [SAP HANA Administration Guide](#) released by SAP.

- To back up and restore data, SAP supports:
 - Complete backup.
 - Incremental backup.
 - Backup using a third-party tool.
 - Backup lifecycle management.

For details, see [SAP HANA Database Backup and Recovery](#) released by SAP.

4 Backing Up and Restoring Data

- [4.1 Constraint](#)
- [4.2 Obtaining the Backup Size](#)
- [4.3 Configuring the Backup Path](#)
- [4.4 Creating a Backup Task](#)
- [4.5 Canceling a Backup Task](#)
- [4.6 Checking Backup File Integrity](#)
- [4.7 Restoring SAP HANA Data](#)

4.1 Constraint

To ensure data reliability, back up SAP HANA data.

You can use SAP HANA Studio, SQL command, or SAP DBA Cockpit to start SAP HANA database backup. Log files are automatically backed up unless automatic backup is manually disabled.

This section describes how to use SAP HANA Studio to back up SAP HANA (SAP HANA 1.0) data into **/hana/backup** and use the data to restore SAP HANA so that you can learn typical backup and restoration operations.

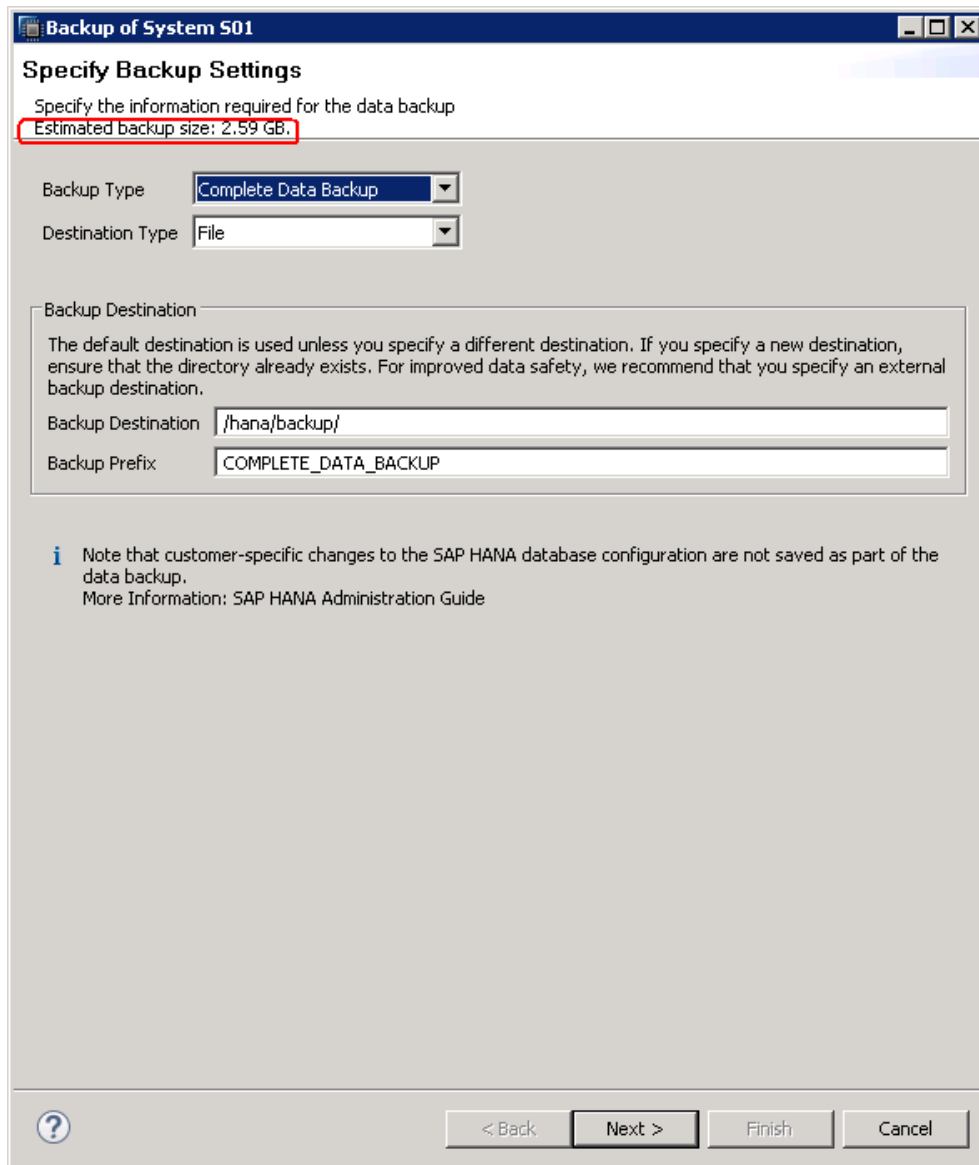
For details about requirements and operation guide, see related documents released by SAP at their official website.

4.2 Obtaining the Backup Size

Before installing SAP HANA, make sure that the available space in **/hana/backup** on SAP HANA nodes is at least three times the SAP HANA memory capacity.

Obtain the backup size before backing up data. The size is displayed on the wizard page for creating a backup task, as shown in [Figure 4-1](#). Ensure that the available space in **/hana/backup** meets the backup size requirement.

Figure 4-1 Obtaining the backup size



4.3 Configuring the Backup Path

Before backing up data, configure the default backup path.

For details, see section "Configuring the Backup Path" in [2.5 Installing SAP HANA \(Single-Node Deployment Without HA Required\)](#) and [2.6 Installing SAP HANA \(Single-Node Deployment with HA Required\)](#).

4.4 Creating a Backup Task

Scenarios

Create a data backup so that it can be used to restore SAP HANA if an error occurs, thereby ensuring SAP HANA reliability.

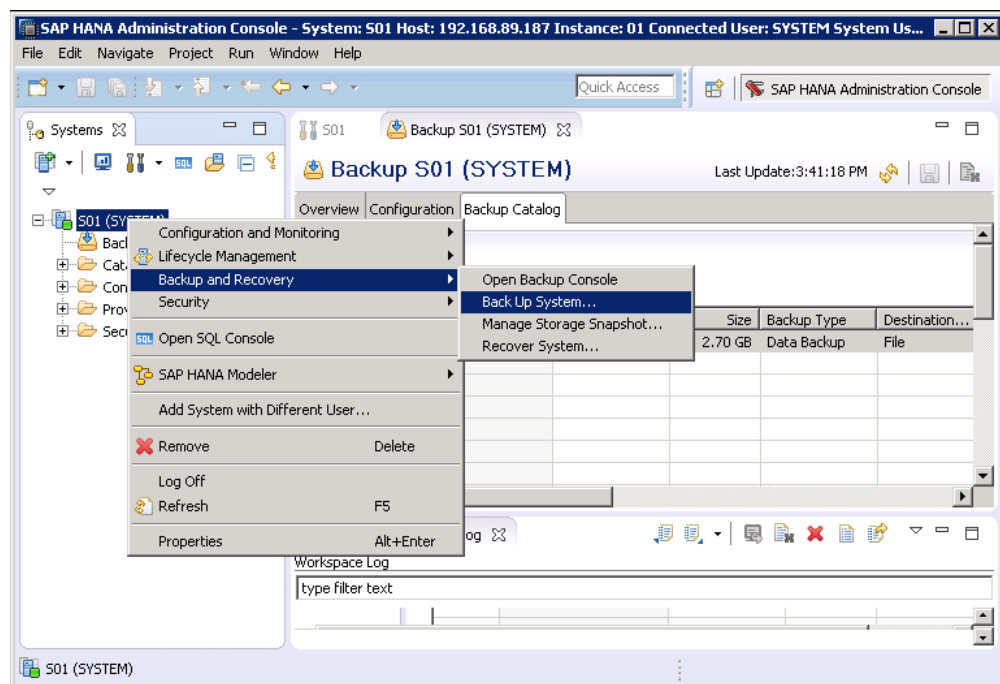
This section uses an SAP HANA system with SAP HANA Studio installed on a Windows ECS as an example to describe how to completely back up SAP HANA data.

For details about operation requirements and notes, see [SAP HANA Database Backup and Recovery](#) released by SAP.

Procedure

- Step 1** On the SAP HANA Studio web page, right-click the SAP HANA system to be backed up and choose **Backup and Recovery > Back Up System** from the shortcut menu.

Figure 4-2 Backup entry

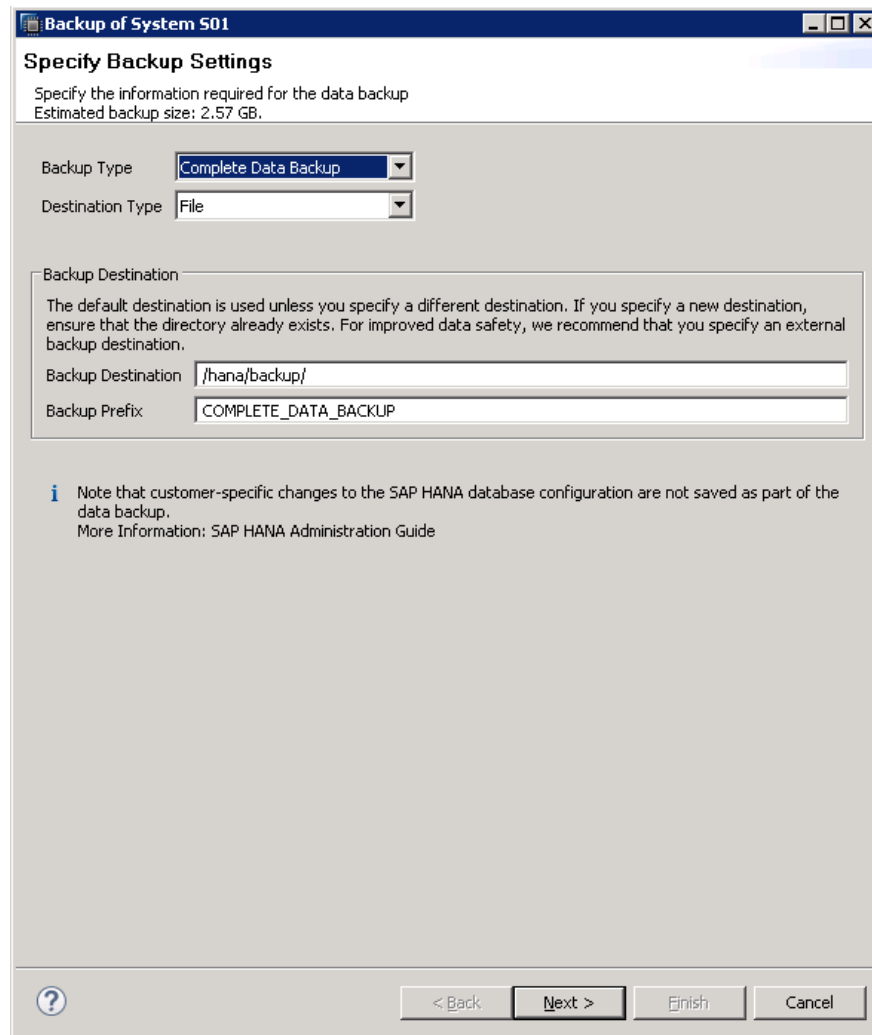


- Step 2** On the **Specify Backup Settings** page, configure backup parameters.

The parameters are as follows:

- **Backup Type:** specifies the type of the backup. In this section, select **Complete Data Backup**, indicating that the backup contains all data required for restoring SAP HANA.
- **Destination Type:** specifies the target backup type. In this section, select **File**, indicating that the backup data is stored in a file.
- **Backup Destination:** specifies the target backup path. The default backup path, **/hana/backup**, is the path you have specified.
For file backup, ensure that the target backup path has sufficient space to store the backup file. You can change the target backup path as needed.
- **Backup Prefix:** specifies the backup file prefix. Time or date is recommended, for example, **COMPLETE_DATA_BACKUP_20170622**.

Figure 4-3 Specify Backup Settings page



Step 3 Click **Next**.

Brief information about the backup configuration is displayed.

Step 4 Confirm the information and click **Finish**.

The system starts the backup.

Step 5 After the backup is complete, click **Close**.

Step 6 Log in to the SAP HANA node as user **root**, switch to **/hana/backup**, and run the following command:

```
ls -l | grep COM
```

In the preceding command, *COM* indicates that the files with prefix **COM** are to be displayed.

Displayed backup files are as follows:

```
-rw-r----- 1 s01adm sapsys 163840 Jun 23 16:22  
COMPLETE_DATA_BACKUP_20170622_databackup_0_1  
-rw-r----- 1 s01adm sapsys 83894272 Jun 23 16:22  
COMPLETE_DATA_BACKUP_20170622_databackup_1_1
```

```
-rw-r----- 1 s01adm sapsys 83894272 Jun 23 16:22  
COMPLETE_DATA_BACKUP_20170622_databackup_2_1  
-rw-r----- 1 s01adm sapsys 2181046272 Jun 23 16:22  
COMPLETE_DATA_BACKUP_20170622_databackup_3_1  
-rw-r----- 1 s01adm sapsys 285220864 Jun 23 16:22  
COMPLETE_DATA_BACKUP_20170622_databackup_4_1  
-rw-r----- 1 s01adm sapsys 285220864 Jun 23 16:22  
COMPLETE_DATA_BACKUP_20170622_databackup_5_1
```

----End

4.5 Canceling a Backup Task

Scenarios

Cancel a backup task during the backup process if the backup task is not required.

For details about operation requirements and notes, see [SAP HANA Database Backup and Recovery](#) released by SAP.

Procedure

- Step 1** On the SAP HANA Studio web page, right-click the SAP HANA system that is being backed up and choose **Backup and Recovery > Open Backup Console** from the shortcut menu.

The backup task that is in process is displayed on the **Overview** page.

- Step 2** Click **Cancel Backup** to cancel the backup task.

----End

4.6 Checking Backup File Integrity

Scenarios

Before restoring data, check backup file integrity, preventing errors during the restoration process.

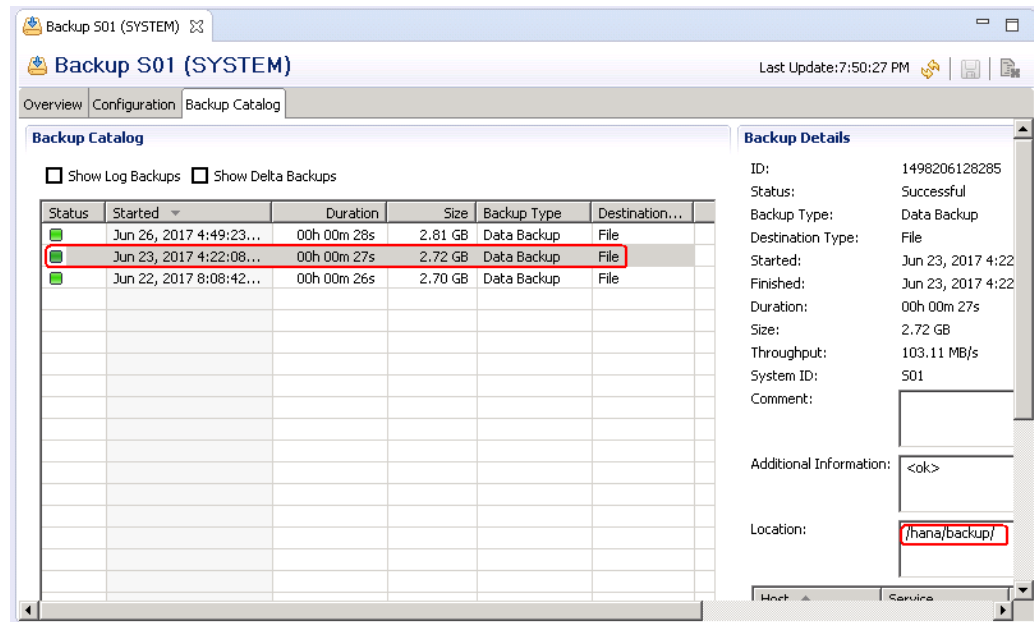
For details about operation requirements and notes, see [SAP HANA Database Backup and Recovery](#) released by SAP.

Procedure

- Step 1** On the SAP HANA Studio web page, right-click the target SAP HANA system and choose **Backup and Recovery > Open Backup Console** from the shortcut menu.

- Step 2** On the page that is displayed, click **Backup Catalog**, select the backup file to be checked, and obtain the path in which the file is stored.

Figure 4-4 Obtaining the path in which the backup file is stored



Step 3 Log in to the ECS where the backup file is stored as user **root** and switch to the administrator account for logging in to the SAP HANA system.

For example, if the SAP HANA **SID** is **s01**, the administrator username for logging in to the SAP HANA system is **s01adm**.

```
su - s01adm
```

Step 4 Run the following command to switch to the directory in which the backup file is stored:

```
cd /hana/backup
```

Step 5 Run the following command to view the name of the backup file:

```
ls -l | grep COM
```

In the preceding command, *COM* indicates that the files with prefix **COM** are to be displayed.

Displayed backup files are as follows:

```
-rw-r----- 1 s01adm sapsys 163840 Jun 23 16:22
COMPLETE_DATA_BACKUP_20170622_databackup_0_1
-rw-r----- 1 s01adm sapsys 83894272 Jun 23 16:22
COMPLETE_DATA_BACKUP_20170622_databackup_1_1
-rw-r----- 1 s01adm sapsys 83894272 Jun 23 16:22
COMPLETE_DATA_BACKUP_20170622_databackup_2_1
-rw-r----- 1 s01adm sapsys 2181046272 Jun 23 16:22
COMPLETE_DATA_BACKUP_20170622_databackup_3_1
-rw-r----- 1 s01adm sapsys 285220864 Jun 23 16:22
COMPLETE_DATA_BACKUP_20170622_databackup_4_1
-rw-r----- 1 s01adm sapsys 285220864 Jun 23 16:22
COMPLETE_DATA_BACKUP_20170622_databackup_5_1
```

Step 6 Run the following command to check the integrity of the backup file:

```
hdbbackupcheck COMPLETE_DATA_BACKUP_20170622_databackup_0_1
```

The following information is displayed if the check result is normal:

```
Backup '/hana/backup/COMPLETE_DATA_BACKUP_20170622_databackup_0_1' successfully checked.
```

Step 7 Repeat **Step 6** to check the integrity of other backup files.

----End

4.7 Restoring SAP HANA Data

Scenarios

SAP HANA must be restored if the data volume or log volume of the SAP HANA system is unavailable, or other exceptions occur in the SAP HANA system.

This section uses an SAP HANA system with SAP HANA Studio installed on a Windows ECS as an example to describe how to use the backup data to restore SAP HANA.

For details about operation requirements and notes, see [SAP HANA Database Backup and Recovery](#) released by SAP.

Procedure

Step 1 On the SAP HANA Studio web page, right-click the SAP HANA system to be stopped and choose **Configuration and Monitoring > Stop System** from the shortcut menu.

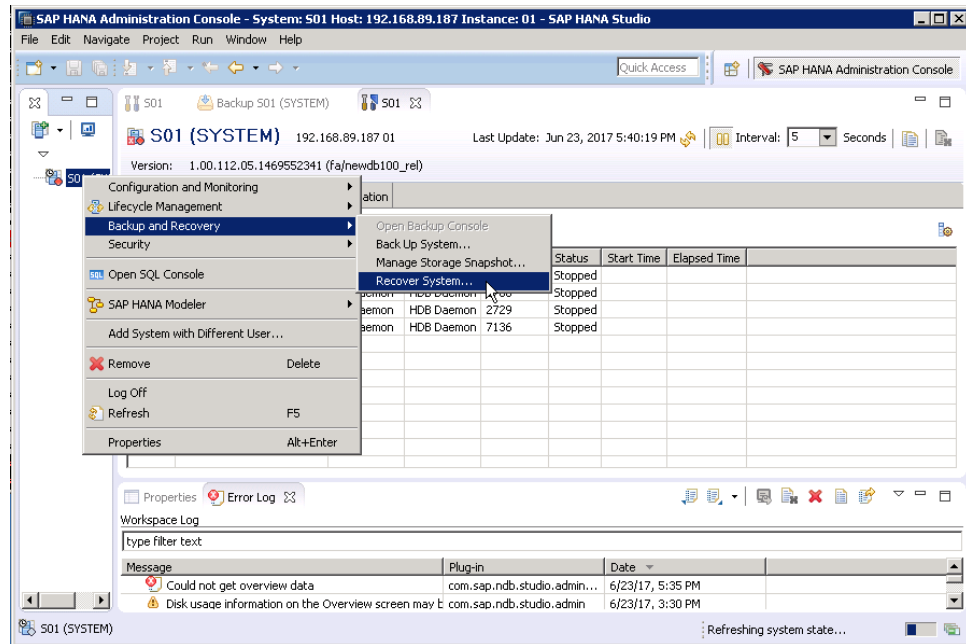
Step 2 On the page that is displayed, set **Shutdown Type** to **Soft** and click **OK**.

Step 3 Enter the administrator account for logging in to the SAP HANA system as prompted.

For example, if the SAP HANA **SID** is **s01**, the administrator username for logging in to the SAP HANA system is **s01adm**.

Step 4 Right-click the SAP HANA system to be restored and choose **Backup and Recovery > Recover System** from the shortcut menu.

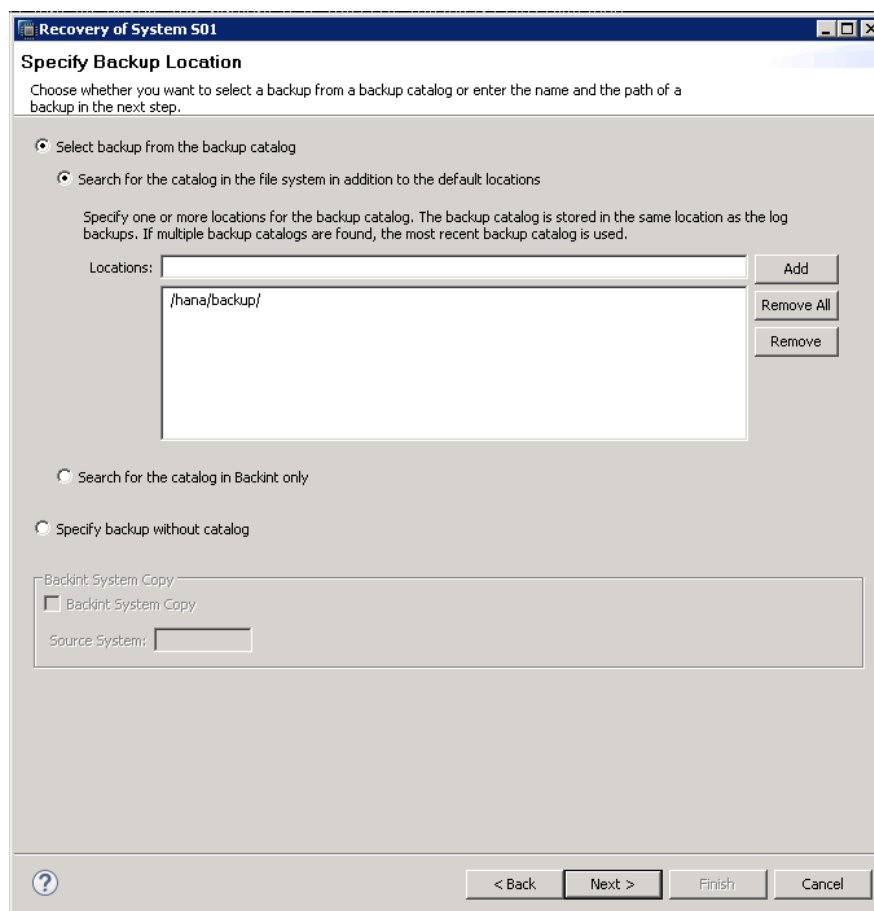
Figure 4-5 Restoration entry



Step 5 On the **Specify Recovery Type** page, select **Recovery the database to a specific data backup or storage snapshot** and click **Next**.

Step 6 On the **Specify Backup Location** page, retain default settings and click **Next**.

Figure 4-6 Specifying the path in which the backup file is to be stored



Step 7 On the **Select a Backup** page, select a backup record for recovery and click **Next**.

Step 8 On the **Other Settings** page, retain the default settings and click **Next**.

Step 9 On the page showing the brief information, click **Finish** to start the restoration.

Step 10 After the restoration is complete, click **Close**.

On the SAP HANA Studio web page, you can find that SAP HANA has started and is running properly.


----End

5 FAQs

- [5.1 How Do I Start and Stop an ECS Instance?](#)
- [5.2 How Do I Connect to the SAP HANA Database?](#)
- [5.3 How Do I Check the Port of the SAP HANA Database Server?](#)
- [5.4 What Should I Do If I Cannot Switch to an ECS or HANA ECS Using SSH?](#)

5.1 How Do I Start and Stop an ECS Instance?

Starting an ECS Instance


- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and project.
- Step 3** Click **Service List** and choose **Computing > Elastic Cloud Server** to switch to the **Elastic Cloud Server** page.
- Step 4** In the ECS instance list, select the ECS instance to be started.
- Step 5** Click **Start** in the upper left corner to start the ECS instance.

 **NOTE**

You can start the ECS only when the ECS is shut down.

----End

Stopping an ECS Instance

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region and project.
- Step 3** Click **Service List** and choose **Computing > Elastic Cloud Server** to switch to the **Elastic Cloud Server** page.
- Step 4** In the ECS instance list, select the ECS instance to be stopped.

Step 5 Click **Stop** in the upper left corner to stop the ECS instance.

 **NOTE**

You can stop the ECS only when the ECS is started.

----End

5.2 How Do I Connect to the SAP HANA Database?

HUAWEI CLOUD provides multiple connections between the local system of a user and the SAP system running on HUAWEI CLOUD. You can select a connection type as required.

- **Direct Internet Connection**
You can configure a public EIP address on the cloud server to connect it to the public network through the EIP service.
- **Direct Connect**
Direct Connect helps you establish a dedicated network that connects your local data center to the public cloud. Direct Connect sets up dedicated connections between the Direct Connect gateway and a VPC on the public cloud. With Direct Connect, you can establish network circuits between the cloud and your data center, office, or collocation environment. Direct Connect can effectively reduce network latency and improve network experience.
- **VPN**
VPN establishes a secure, encrypted communication tunnel between the VPN gateway of the VPC on HUAWEI CLOUD and the VPN gateway of your local data center, allowing you to directly use resources in the VPC through the VPN.
By default, cloud servers in a VPC cannot communicate with your data center or private network. To enable communication between them, you can create a VPN.

5.3 How Do I Check the Port of the SAP HANA Database Server?

Step 1 Log in to the management console.

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

Step 3 Click **Service List** and choose **Computing > Elastic Cloud Server** to switch to the **Elastic Cloud Server** page.

Step 4 Click the name of the created HANA ECS to go to the details page.

Step 5 Click the **Security Groups** tab to view the security group.

Step 6 Click the security group name and view the port number of the SAP HANA database server in the **Port Range/ICMP Type** column.

----End

5.4 What Should I Do If I Cannot Switch to an ECS or HANA ECS Using SSH?

Symptom

When I switched from a Linux ECS/HANA ECS to another Linux ECS/HANA ECS using SSH, the system displayed a message indicating the switching failed.

The message is as follows:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@
@  WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!  @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
2c:d0:17:8a:82:4c:23:d6:14:be:d0:1d:88:8b:8b:03 [MD5].
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /root/.ssh/known_hosts:1
You can use following command to remove all keys for this IP:
ssh-keygen -R fanhana-0002 -f /root/.ssh/known_hosts
RSA host key for fanhana-0002 has changed and you have requested strict checking.
Host key verification failed.
```

Possible Causes

- OpenSSH has been reinstalled on the target ECS/HANA ECS.
- The node IP address or name has been changed.
- Other issues have occurred.

Handling Method

Delete the **known_hosts** file on the local end to resolve this issue. To do so, perform the following operations:

1. On the local ECS/HANA ECS, switch to the CLI as user **root**.
2. Run the following command to delete the **known_hosts** file:

```
rm /root/.ssh/known_hosts
```

NOTE

After the file deletion, when you attempt to switch to the target ECS/HANA ECS using SSH, 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.

6 Appendix

[6.1 Obtaining the Password for Logging In to a Windows ECS](#)

[6.2 Logging In to a Linux ECS Using an SSH Key](#)

[6.3 Querying the NIC IP Address of an ECS](#)

[6.4 Modifying OS Configurations](#)

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

[6.5 Obtaining the Key File of an ECS](#)

6.1 Obtaining the Password for Logging In to a Windows ECS

Scenarios

Password authentication mode is required to log in to a Windows ECS. Therefore, you must use the key file used when you created the ECS to obtain the administrator password generated when the ECS was initially installed. The administrator user is **Administrator** or the user configured using Cloudbase-Init. This password is randomly generated, offering high security.

You can obtain the initial password for logging in to a Windows ECS using either the management console or API. For details, see this section.

Obtaining the Password Using the Management Console

1. Obtain the private key file (.pem file) used when you created the ECS.
2. Log in to the management console.
3. Under **Computing**, click **Elastic Cloud Server**.
4. In the ECS list, select the ECS whose password you want to get.
5. In the **Operation** column, click **More** and choose **Get Password**.
6. Use either of the following methods to obtain the password through the key file:

- Click **Select File** and upload the key file from a local directory.
 - Copy the key file content to the text field.
7. Click **Get Password** to obtain a random password.

Obtaining the Password Using APIs

1. Obtain the private key file (.pem file) used when you created the ECS.
2. Set up the API calling environment.
3. For details, see section "API Calling" in the *Elastic Cloud Server API Reference*.
4. Obtain the ciphertext password.

Call the password obtaining APIs to obtain the ciphertext password of the public key encrypted using RSA. The API URI is in the format "GET /v2/{tenant_id}/servers/{server_id}/os-server-password".

NOTE

For instructions about how to call an API, see section "Retrieving the Password for Logging In to a Windows ECS (Native OpenStack API)" in *Elastic Cloud Server API Reference*.

5. Decrypt the ciphertext password.
Use the private key file used when you created the ECS to decrypt the ciphertext password obtained in step 4.
 - a. Run the following command to convert the ciphertext password format to ".key -nocrypt" using OpenSSL:
openssl pkcs8 -topk8 -inform PEM -outform DER -in rsa_pem.key -out pkcs8_der.key -nocrypt
 - b. Invoke the Java class library **org.bouncycastle.jce.provider.BouncyCastleProvider** and use the private key file to edit the code decryption ciphertext.

6.2 Logging In to a Linux ECS Using an SSH Key

Prerequisites

- You have obtained the key file of the ECS. For details about how to obtain the key file, see [6.5 Obtaining the Key File of an ECS](#).
- An elastic IP address has been bound to the ECS.
- You have configured the inbound rules of the security group.

Logging In to the Linux ECS from a Windows Computer

This section describes how to log in to the Linux ECS from a Windows computer.

The following operations use PuTTY as an example to log in to the ECS. Before the login, you must convert the private key format.

1. Visit the following website and download PuTTY and PuTTYgen:
<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

 **NOTE**

PuTTYgen is a private key generator, which is used to create an SSH key pair that consists of a public key and a private key for PuTTY.

2. Run PuTTYgen.
3. In the **Actions** area, click **Load** and import the private key file stored during HANA ECS creation.

The file to be imported must be in the format of "All files (*.*)".

4. Click **Save private key**.
5. Save the converted private key to the local computer. For example, **kp-123.ppk**.
6. Run PuTTY.
7. Choose **Connection > data** and enter **:root** in **Auto-login username**.
8. Choose **Connection > SSH > Auth**. In the last configuration item **Private key file for authentication**, click **Browse** and select the private key converted in step 5.
9. Click **Session** and enter the elastic IP address of the ECS under **Host Name (or IP address)**.
10. Click **Open**.

The ECS is logged in.

Logging In to the Linux ECS from a Linux Computer

This section describes how to log in to the Linux ECS from a Linux computer. The following operations use private key file **kp-123.pem** as an example to log in to the ECS.

1. On the Linux CLI, run the following command to change the permission:

```
chmod 600 /path/kp-123
```

 **NOTE**

In the preceding command, **path** specifies where the private key file is saved.

2. Run the following command to log in to the ECS:

```
ssh -i /path/kp-123 root@Elastic IP address
```

 **NOTE**

- In the preceding command, **path** specifies where the private key file is saved.
- *Elastic IP address* is the elastic IP address bound to the ECS.

6.3 Querying the NIC IP Address of an ECS

Scenarios

The IP address of an ECS is required.

Procedure

- Step 1** On the management console, choose **Computing > Elastic Cloud Server**. On the left side of the page, choose **Elastic Cloud Server**. Then, the system displays all ECSs on the right side of the page.
- Step 2** Click the name of the HANA ECS to be queried. Then, the page for the HANA ECS details is displayed.
- Step 3** Click the **NIC** tab. On the page providing detailed information, click target NIC. In the expanded area, check the IP address information.

NOTE

- **EIP**: specifies the EIP bound to the ECS.
- **Private IP Address**: specifies the private IP address of the ECS NIC.

----End

6.4 Modifying OS Configurations

To ensure the proper installation of the SAP HANA 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 SAP HANA nodes.
- Step 2** Run the following commands on the SAP HANA node to disable automatic firewall enabling and disable the firewall:

- If the OS is SUSE Linux Enterprise Server 12, run the following commands:

SuSEfirewall2 off

SuSEfirewall2 stop

systemctl disable SuSEfirewall2_init.service

systemctl disable SuSEfirewall2.service

systemctl stop SuSEfirewall2_init.service

systemctl stop SuSEfirewall2.service

Run the following command to check the firewall status:

systemctl status SuSEfirewall2.service

If information similar to the following is displayed, automatic firewall start and stop are disabled:

```
Active: inactive (dead)
b1-wang:~ # systemctl status SuSEfirewall2.service
● SuSEfirewall2.service - SuSEfirewall2 phase 2
  Loaded: loaded (/usr/lib/systemd/system/SuSEfirewall2.service; disabled; vendor preset: disabled)
  Active: inactive (dead)
b1-wang:~ #
```

- If the OS is SUSE Linux Enterprise Server 15, run the following commands:

systemctl stop firewalld

systemctl disable firewalld

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

----End


6.5 Obtaining the Key File of an ECS

After a key pair is created for an ECS, the browser prompts you to download or automatically downloads the private key file. Keep the private key file secure. When logging in to the ECS using SSH, you need to provide the private key.

Procedure

Step 1 Log in to the management console.

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

Step 3 In the navigation plane on the left, click  and choose **Computing > Elastic Cloud Server**.

Step 4 In the navigation pane on the left, choose **Key Pair**.

Step 5 On the right side of the page, click **Create Key Pair**.

Step 6 Enter the key name and click **OK**.

An automatically allocated key name consists of **KeyPair-** and a 4-digit random number. Change it to an easy-to-remember one, for example, **KeyPair-xxxx_ecs**.

Download the private key file. Alternatively, the system will automatically download it for you. The file name is the specified key pair name with a suffix **.pem**. Securely store the private key file. In the displayed dialog box, click **OK**.

NOTICE

This is the only opportunity for you to save the private key file. Keep it secure. When creating an ECS, provide the name of your desired key pair. Each time you log in to the ECS using SSH, provide the private key.

Step 7 (Optional) To keep your private key file secure, you can enable [Data Encryption Workshop \(DEW\)](#). Then, you can manage key pairs, including binding, viewing, resetting, replacing, unbinding, and deleting key pairs. For details, see [Managing Key Pairs](#).

Example:

- If a private key file is lost, you can reset the key pair of the ECS.
- If a private key file is leaked, you can use a new key pair to replace the original one of the ECS.

----End

A Change History

What's New	Released On
This issue is the second official release. This release incorporates the following change: Added descriptions of purchasing an SFS storage package.	2019-03-30
This issue is the first official release.	2018-11-30