SAP Best Practices

SAP Best Practices

Issue 01

Date 2024-03-12

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Contents

1 SAP Best Practices

This document summarizes operation practices in common SAP application scenarios. Each practice provides detailed solution description and operation guide, helping you easily use SAP services.

Table 1-1 SAP best practices

Best Practice	Description
HUAWEI CLOUD SAP on DB2 Installation Best Practice	This section provides guidance for preparing resources (such as cloud servers and network resources) on the HUAWEI CLOUD platform and installing SAP on DB2.
HUAWEI CLOUD SAP on SQL Server Installation Best Practice	This section provides guidance for preparing resources (such as cloud servers and network resources) on the public cloud platform and installing SAP on SQL Server.
SAP S/4HANA (1809) HA Deployment Best Practice	This section provides instructions to prepare resources (such as ECSs and network resources) on the public cloud platform, and install SAP S/4HANA (1809) in high availability (HA) mode.
HUAWEI CLOUD SAP Business One on HANA Installation Best Practice	This section provides guidance for preparing resources (such as cloud servers and network resources) on the public cloud platform and installing SAP Business One on HANA.
SAP Monitoring Best Practices	This section describes how to deploy the SAP large-screen monitoring on the public cloud platform to monitor the SAP system and learn about the resource usage, alarms, and SAP system running status in real time.
Best Practices of SAP Migration to HUAWEI CLOUD	This section describes how to migrate the SAP system to HUAWEI CLOUD. HUAWEI CLOUD provides an improved solution to help you migrate with higher efficiency and lower costs.

Best Practice	Description
Best Practice of Using Block-Level Migration of SMS to Migrate SAP Applications and Databases Running on Linux Servers	This section describes how to use block-level migration of SMS to migrate SAP applications and databases running on Linux servers, helping you improve efficiency and reduce costs.
Best Practice of SAP Migration from Xen to KVM	This section describes how to migrate the SAP system from the Xen platform of HUAWEI CLOUD to the KVM platform to meet service development and capacity expansion requirements.
Best Practice of SAP Disaster Recovery with SDRS	This section describes how to use SDRS to implement the SAP disaster recovery on the public cloud platform.
Best Practice of Rsync-based SAP Disaster Recovery	This section describes how to Rsync to implement SAP disaster recovery on the public cloud platform.
SAP Backint Installation Guide	This section describes how to install Backint Agent to back up the data in the SAP HANA database to the OBS bucket, restore the data using backups, and delete backups.
Best Practices for Uploading SAP Backups to the OBS Bucket	This section describes how to use scripts to call obsutil to back up local files to the OBS bucket and store copies locally within a certain period of time.
Best Practices of the SAP ASE Solution	This section describes the HUAWEI CLOUD SAP on ASE solution, including information about resource selection, system backup, high availability (HA), disaster recovery (DR), and offline system migration. HUAWEI CLOUD provides various cloud services to ensure stable and secure running of the SAP Adaptive Server Enterprise (ASE) system.
Best Practices of SAP System Capacity Expansion	This section describes how to expand ECSs and EVS disk capacity in the SAP systems.

2 Huawei Cloud SAP on DB2 Installation Best Practice

2.1 About This Document

This document provides guidance for preparing resources (such as cloud servers and network resources) on the HUAWEI CLOUD platform and installing SAP on DB2. SAP is authorized in Bring Your Own License (BYOL) mode. You need to log in at **SAP Support Portal** to purchase licenses.

This document cannot replace the standard SAP document. If you have any trouble in installing and using SAP due to its own problems, contact the SAP technical support.

This document is written based on the OS SUSE Linux Enterprise Server and applies to the standalone installation and deployment of SAP on DB2. The deployment modes mentioned in the document are only for reference. Install it by referring to the standard SAP installation manual or based on site requirements.

For details about the official SAP installation guide and related notes, see the following documents:

- **SAP Installation Guides**
- **SAP Notes**
- **SAP Library**

2.2 Preparations

Logging in to Huawei Cloud

Before deploying the SAP system on Huawei Cloud, register a HUAWEI ID and enable Huawei Cloud services. Through this account, you can use Huawei Cloud services and pay only for the services you use.

For details, see **Registering a HUAWEI ID and Enabling Huawei Cloud Services**.

You can log in to Huawei Cloud using any of the methods described in **Logging In to Huawei Cloud**.

SAP License

SAP is authorized in Bring Your Own License (BYOL) mode. In this mode, you need to log in to the SAP Support Portal and apply for a license.

NAT Server

Prepare a Network Address Translation (NAT) server on which SAP GUI for accessing SAPinst installation page and SAP application is installed.

2.3 Resource Planning

2.3.1 Network Planning

The network information needs to be planned based on application scenarios and SAP planning. The following table lists the network segments and IP addresses required for installing standard standalone SAP on DB2. You can configure it based on site requirements.

Parameter	Description	Example
IP address of the server/client plane	Specifies the IP address of the primary NIC plane. The ABAP SAP Central Services (ASCS) nodes communicate with the SAP GUI and SAP databases using this IP address.	ASCS/Primary Application Server (PAS) node: 10.10.1.93 DB2 node: 10.10.1.93

2.3.2 Security Group Planning

SAP Security Group Planning

The security group planning needs to meet the requirements for communication between SAP nodes over the management plane and internal communication

plane. You need to configure the security group together with the network department. For details about SAP's requirements for security group rules, see **TCP/IP ports used by SAP applications**.

You can configure the security group by referring to **Table 1 SAP node security group rules**.

NOTE

- Plan the network segments and IP addresses based on the site requirements. The following security group rules are for reference only. You can configure your own security group rules as needed.
- In the following table, *##* stands for the SAP instance number, which must be consistent with the instance number specified when the SAP software is installed. If there are multiple instance numbers, enter them in sequence.

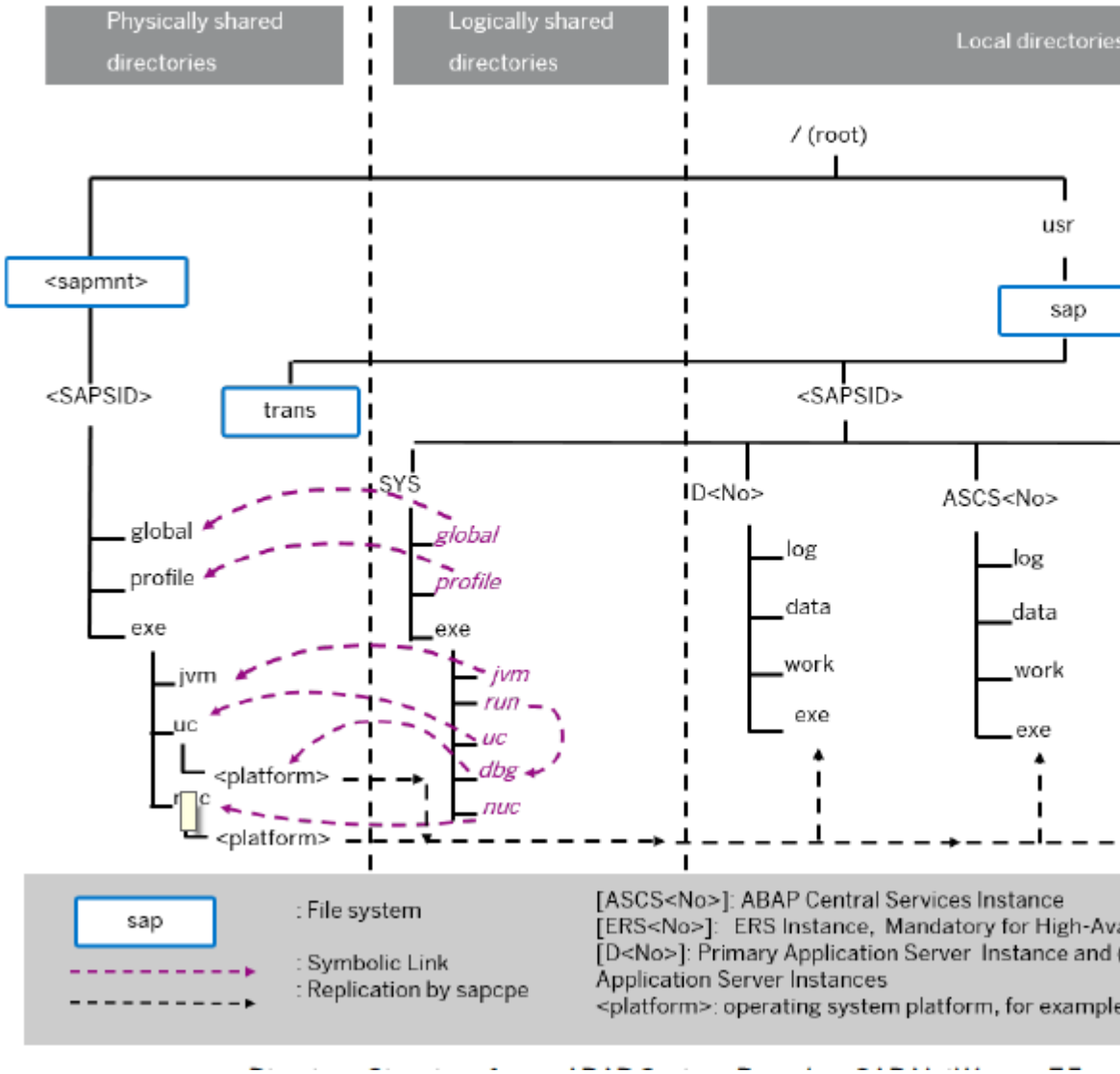
Table 2-1 SAP node security group rules

Source/ Destination	Protocol	Port Range	Description
Inbound			
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.
10.10.1.0/24	TCP	32##	Allows SAP GUI to access SAP.
10.10.1.0/24	TCP	36##	Message port with profile parameter rdisp/msserv
10.10.1.0/24	TCP	5##13 ~ 5##14	Allows ASCS to access SAP application server.
10.10.1.0/24	TCP	33##, 38##, 48##	Port used by CPIC and RFC
10.10.1.0/24	TCP	22	Allows SAP to be accessed using SSH.
10.10.1.0/24	TCP	123	Allows other servers to synchronize time with SAP.
Outbound			
All	All	All	Security group rule created by the system by default Allows SAP to access all peers.

2.3.3 File System Planning

SAP File System Planning

The following figure shows the SAP file system planning. Ensure that the capacity of the **/sapmnt** and **/usr/sap** file systems is greater than 2.5 GB and 25 GB, respectively. For details, see SAP official document.



DB2 File System Planning

Before the installation, set required file system nodes for the DB2 database. **Table 1** shows the file system planning. The total capacity of the **/DB2** file must be greater than 100 GB.

For details about the file system size, see section "3.1 Setting Up File Systems for Shared Disk Scenario" in related SAP official document.

Table 2-2

File System	Description
/db2/db2<dbsid>	Contains the home directory of db2<sapsid>
/db2/<DBSID>/log_dir	Contains at least the online database log files
/db2/<DBSID>/db2dump	Contains DB2 diagnostic log files, DB2 dump files, and further service engineer information
/db2/<DBSID>/db2<dbsid>	Contains the local database directory
/db2/<DBSID>/db2<dbsid>	Contains the temporary tablespace(s)
/db2/<DBSID>/sapdata1	SAP data for container type database managed space (DMS) FILE or for use of DB2's automatic storage management

The following table shows an example of the SAP file system.

Mount Point	File System Capacity	File System Type	Shared	Description
/	100 GB	-	No	OS volume
/usr/sap	100 GB	xfs	No	/usr/sap volume
/sapmnt	40 GB	xfs	No	Shared to all nodes in the SAP system
/db2sfs	Auto capacity expansion	SFS	No	Stores the SAP installation package, which is shared to all nodes in the SAP system.
/db2	300 GB	xfs	No	Used to store DB2 file system nodes.
-	20 GB	swap	No	Swap volume

2.3.4 Software and Hardware Planning

Hardware Planning

The following table lists the requirements for the disk space of SAP hardware. For details, see **SAP official document**.

Table 2-3

Requirement	Parameter
Hardware	Supports 64 bits.
CPU	> 2 cores
CD/ROM or DVD drive	Compatible with ISO9600
Available disk	Archive space for kernel: 2 GB ABAP central services instance (ASCS): 2G ERS instance: 2 GB Database Instance: SAP ERP: Minimum 75 GB SAP CRM: Minimum 50 GB SAP SRM: Minimum 55 GB SAP SCM: Minimum 50 GB SAP NetWeaver: Minimum 40 GB Primary application server instance: Minimum 2 GB (SAP NetWeaver BW server: Minimum 30 GB) Additional application server instance: Minimum 2 GB (SAP NetWeaver BW server: Minimum 30 GB) SAP Host Agent: Minimum 0.5 GB
Memory	ABAP central services instance (ASCS instance): Minimum 1 GB Database Instance: Minimum 2 GB Primary application server instance: Minimum 3 GB (BW server: Minimum 2 GB) Additional application server instance: Minimum 3 GB SAP Host Agent: Minimum 1 GB
Linux: Swap space	SWAP required

Software Planning

The following table lists the requirements of the SAP application and database for OS. For details, see **SAP official document**.

Table 2-4

Requirement	Parameter
Database	View supported database platforms at http://support.sap.com/pam.
Linux OSs	Install DB212 on SLES12.
SAP kernel release version	To use regular Software Provisioning Manager (SWPM10 <version> SAR) with SAP kernel 7.49 or later on RHEL 6, SLES 11, or DB2 Linux 6, you must install the libstdc ++ RPM software package.
Linux kernel parameters	Obtain the Linux kernel version certified by SAP DB2 Linux: SAP Note 1565179 SLES 15: SAP Note 2578899 SLES 12: SAP Note 1984787 SLES 11: SAP Note 1310037 RHEL8: SAP Note 2772999 RHEL7: SAP Note 2002167 RHEL6: SAP Note 1496410
Language environment.	de_DE, en_US

2.3.5 ECS Planning

- SAP ECS specifications

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

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

  SAP-certified ECSs must be used for installing the SAP application. For details, see **SAP Notes**.

- OS

  The following table lists the OS supported by SAP ECSs.

Table 2-5 SAP ECS OS

Name	Specification
OS	SUSE Linux Enterprise Server for SAP Applications 12 SP1

- SAP node planning

ECS Name	Server/ Client IP Address	Specification	Type	Instance Number	SID	Image
sapondb2	10.10.1.93	c6.3xlarge.2	ASCS Instance	01	S01	SUSE Enterprise 12 SP1 for SAP
			PAS Instance	02		
			DB Instance	None		

2.4 Preparing for SAP Installation

Before installing the SAP system, you need to purchase and mount an SFS disk to the ECS, initialize the disk, and set the SWAP partition.

2.4.1 Creating a VPC

A VPC is logically isolated, configurable, and manageable virtual network for cloud servers, cloud containers, and cloud databases. It improves resource security and simplifies network deployment on the cloud. With a VPC, you can configure and manage the networks in the VPC, and make changes to these networks as needed, quickly and securely. For more information about VPC, see **VPC Overview**.

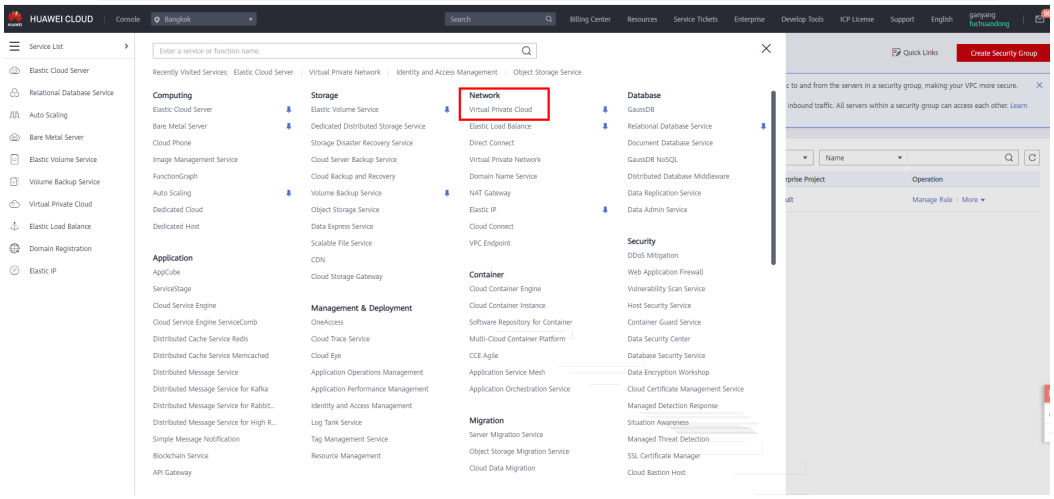
When creating a VPC, create the subnet 10.10.1.0, which is used as the server/client plane IP address and system replication/heartbeat plane IP address of SAP and DB2.

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 pane on the left, click and choose **Network** > **Virtual Private Cloud**.



Step 4 Click **Create VPC** on the right of the page.

Step 5 Configure required parameters as prompted based on **Table 2-6**.

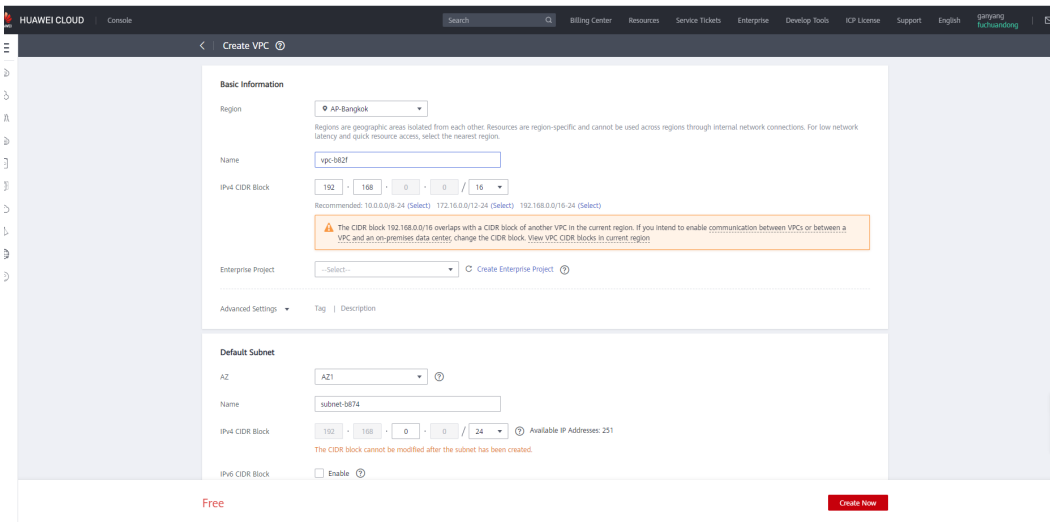


Table 2-6 VPC configuration parameters

Item	Parameter	Description
Basic information	Region	A region is a geographical area where you can run your VPC service. Each region comprises one or more availability zones (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 on the upper left of the page to change the region.
	Name	VPC name

Item	Parameter	Description
	Network segment	CIDR block of 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 in the VPC). 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 **Network Planning**.
	Enterprise project	The enterprise project to which the VPC belongs. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**. For details about creating and managing enterprise projects, see the **Enterprise Management User Guide**.
	Tag	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. For details about the tag naming rules, see **VPC Tag Naming Rules**.
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 private networks.
	Name	Subnet name
	CIDR Block (of the subnet)	The CIDR block for the subnet. This value must be within the VPC CIDR block. Configure the subnet CIDR block based on the information provided in **Network Planning**.
	Advanced settings	Click **Advanced Settings** to set parameters such as **Gateway** and **DNS Server Address**.

Item	Parameter	Description
	Gateway	Gateway address of the subnet
	DNS server address	External DNS server addresses are used by default. If you need to change the DNS server address, ensure that the DNS server addresses you configured are available.
	DHCP lease time	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.
	Tag	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**.
Add a subnet	You can click **Add Subnet** to add a subnet.	

Step 6 Click **Create Now**.

----End

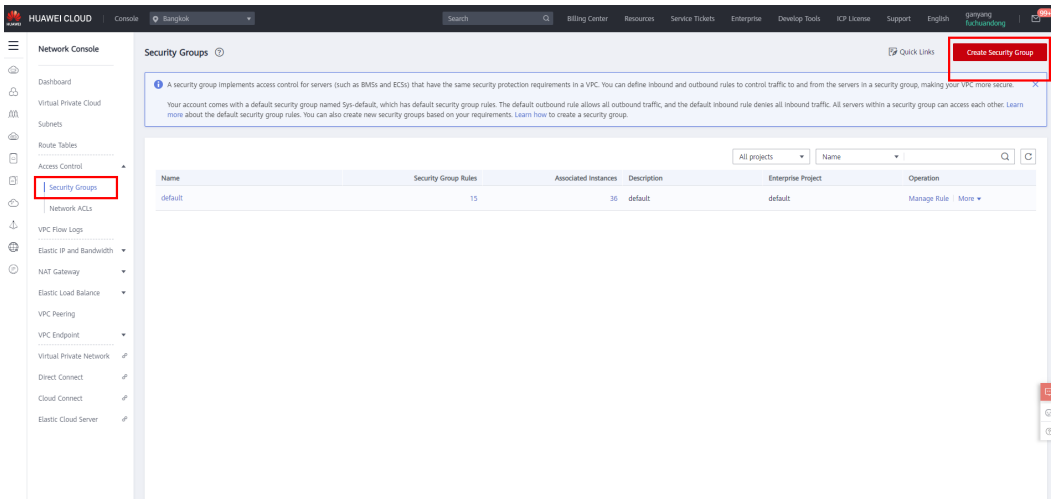
2.4.2 Creating a Security Group

A security group is a collection of access control rules for ECSs that have the same security protection requirements and are mutually trusted. After a security group is created, you can create various access rules for the security group, and these rules will apply to all ECSs added to this security group. For more information about security groups, see **Security Group Overview**.

Procedure

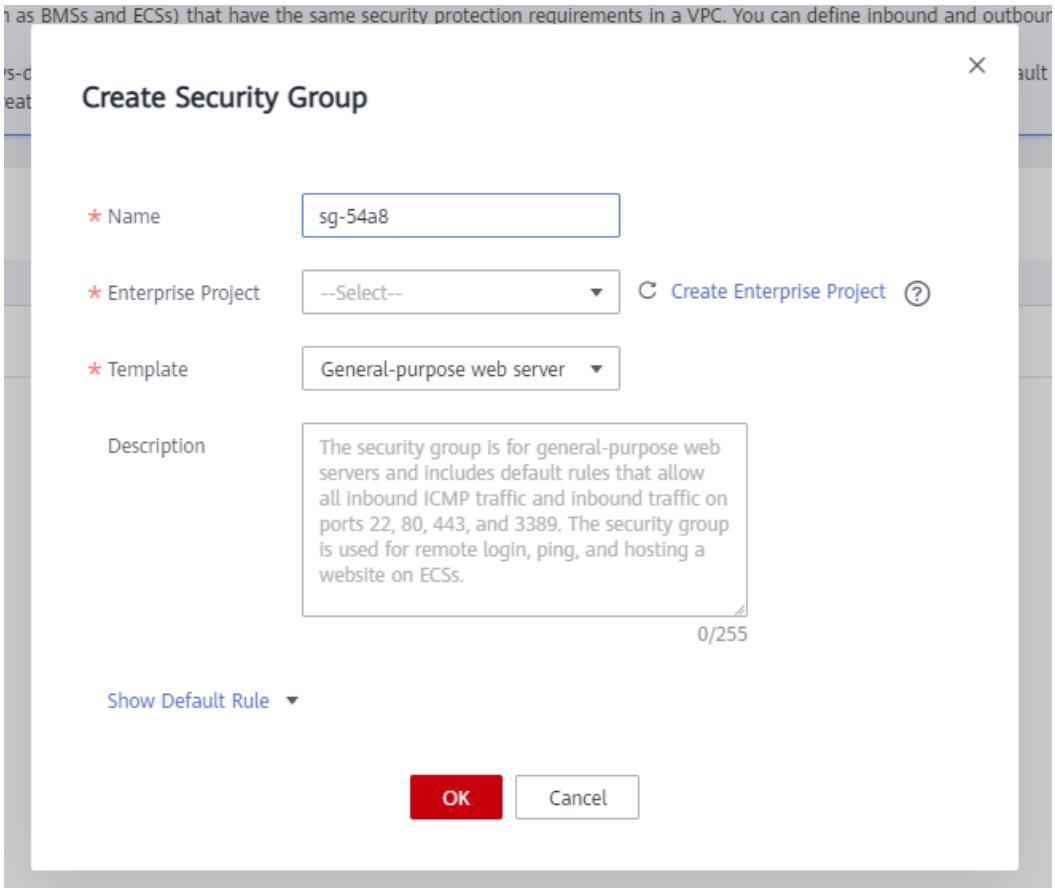
Step 1 Create a SAP security group.

Choose **Access Control** > **Security Groups** in the navigation pane on the left of the VPC console. On the **Security Groups** page, click **Create Security Group**.



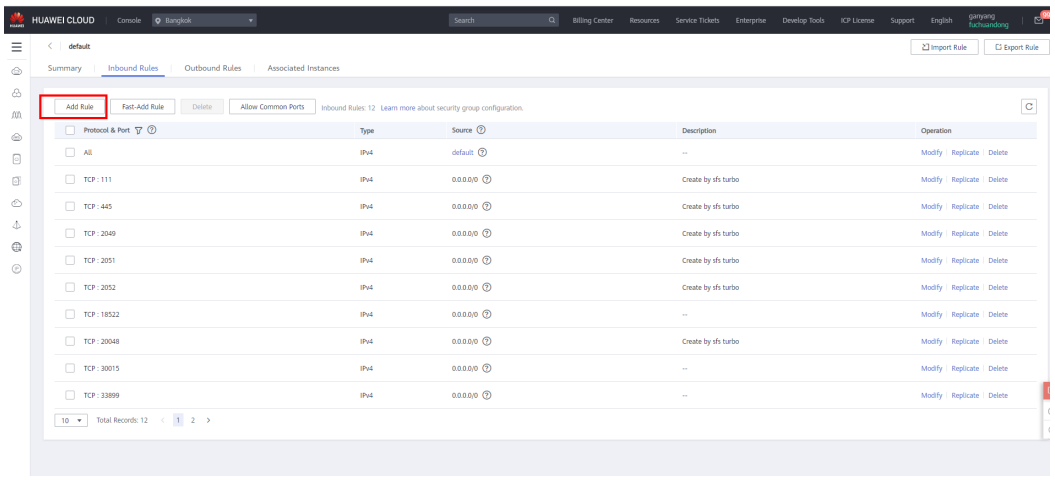
Step 2 Set required parameters to create a security group.

- **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, **sg_sap_**.
- **Enterprise project**: You can add the security group to an enabled enterprise project. You can select an enterprise project from the drop-down list, for example, **SAP**.



Step 3 Click **OK**.

Locate the row that contains the newly created security group, and click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, add the desired ports listed in **Security Group Planning**.



----End

2.4.3 Purchasing ECSs

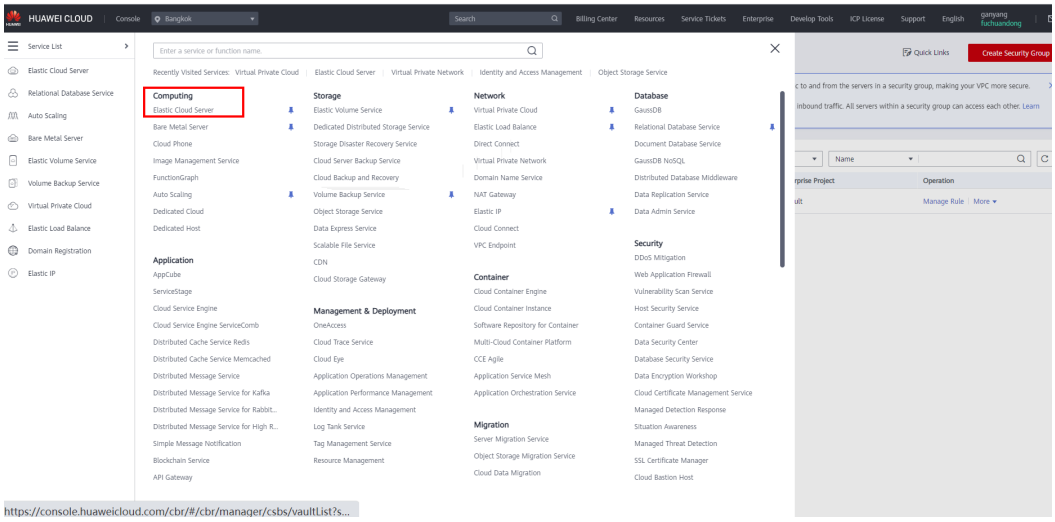
You need to create two ECSs. One is used to install SAP applications and DB2 using Linux, and the other is used to install SAP GUI and functions as a jump server. **Table 1** lists the details of the two ECSs for reference. Purchase them based on the site requirements.

Table 2-7 ECS details

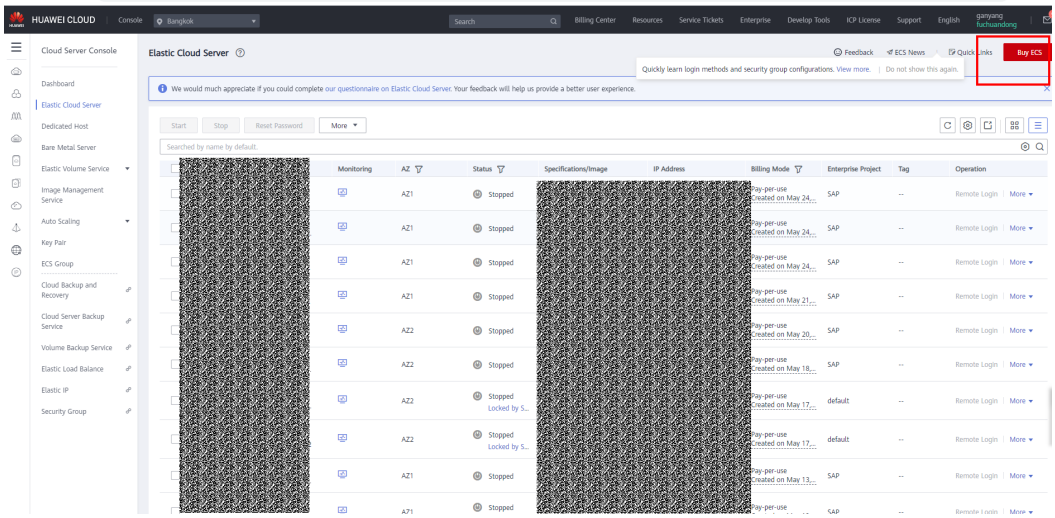
ECS Name	Specification	Model	Image	Remarks
sapondb2	c6.3xlarge.2	12vCPUs | 24GB	SUSE Enterprise 12 SP1 for SAP	Installing SAP and DB2
ecswindows	c6.4xlarge.2	16vCPUs | 32GB	Windows Server 2012 R2 Standard 64-bit Chinese	Installing SAP GUI and functioning as a jump server

ECS Specifications	Model	File System Size	Disk Size (GB)		Storage Category	OS
c6.3xlarge.2	12 vCPUs, 24 GB	570	System disk	100	High I/O	Suse 12.1 for SAP
			/usr/sap	100	High I/O	
			/sapmnt	40	High I/O	
			SWAP	30	High I/O	
			/DB2	300	High I/O	
			/orasfs	N/A	SFS	
c6.4xlarge.2	16vCPUs | 32GB	700	System disk	200	High I/O	Windows Server 2012 R2 Standard 64-bit Chinese
			D	500	High I/O	

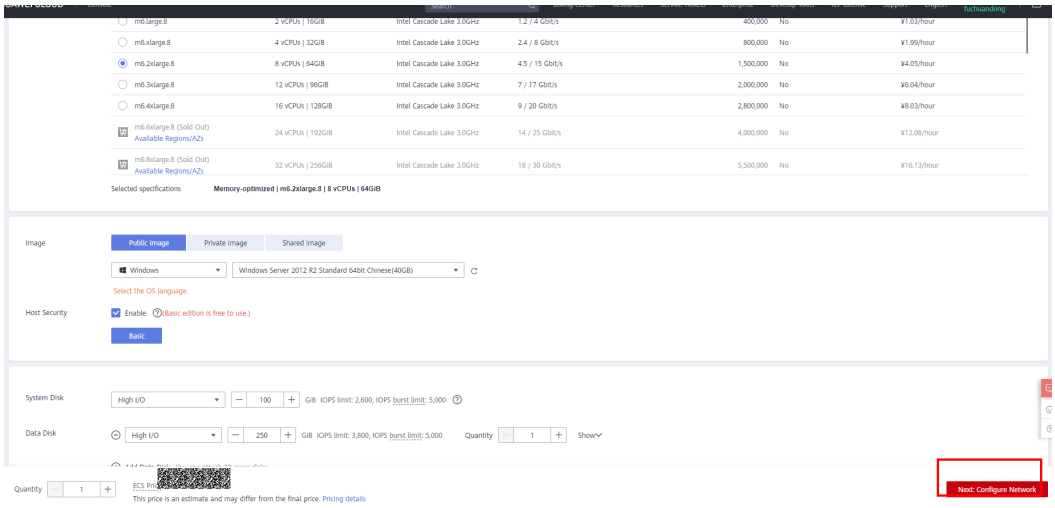
Step 1 Log in to the HUAWEI CLOUD management console, click the service list icon, and choose **Computing** > **Elastic Cloud Server**.



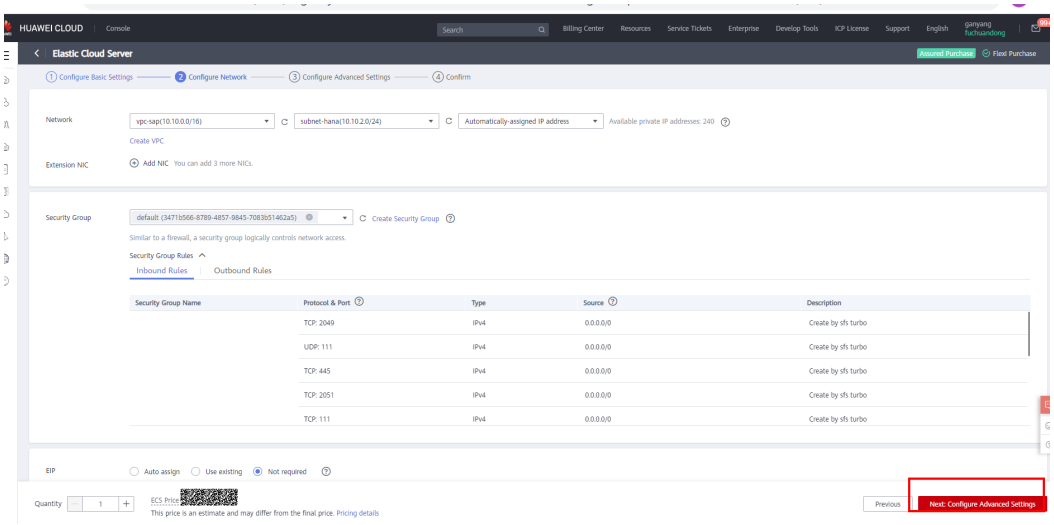
Step 2 Click **Buy ECS**.



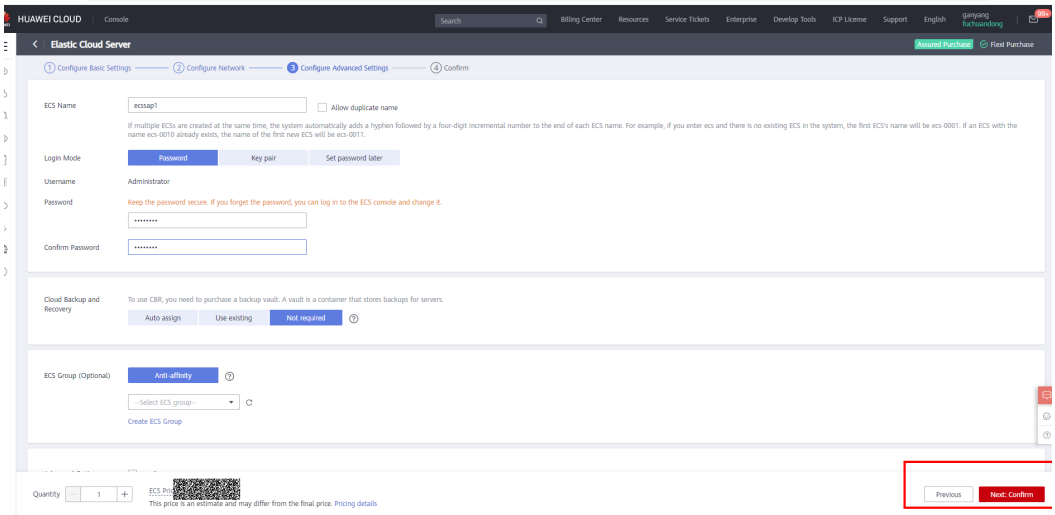
Step 3 Select the ECS flavor, image, and disk size based on **Table 2-7**.



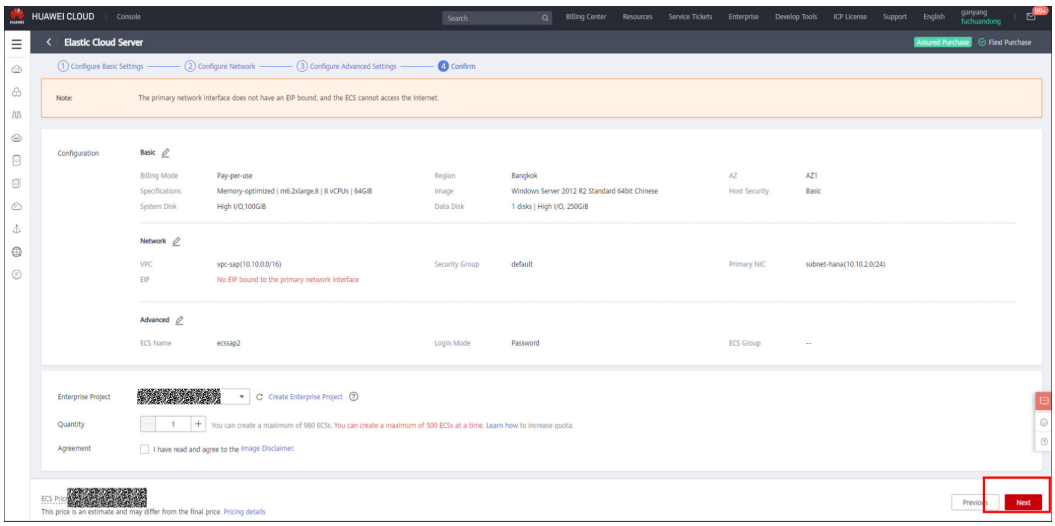
Step 4 Click **Next: Configure Network**. Select the created VPC and security group, confirm the configuration, and click **Next: Configure Advanced Settings**.



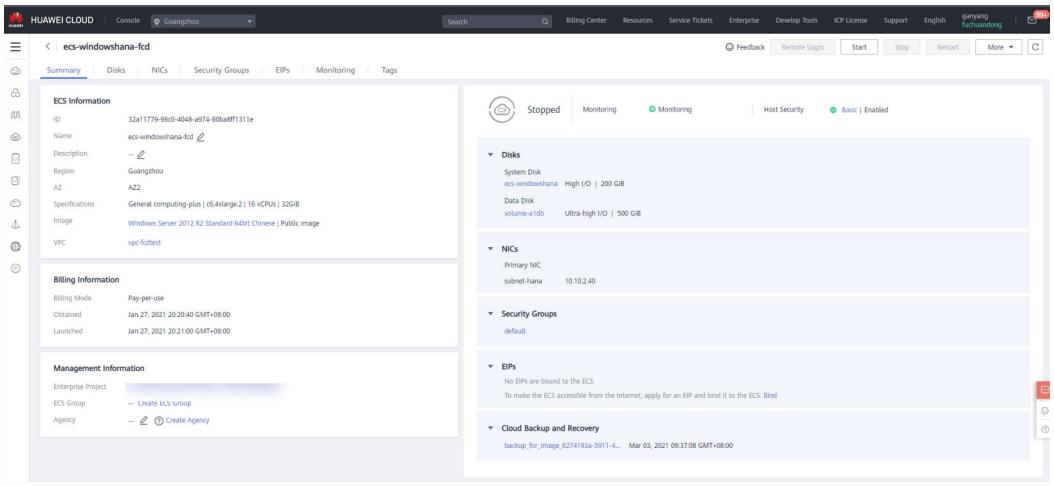
Step 5 Enter the ECS name and password of the **root** user, and click **Next: Confirm**.



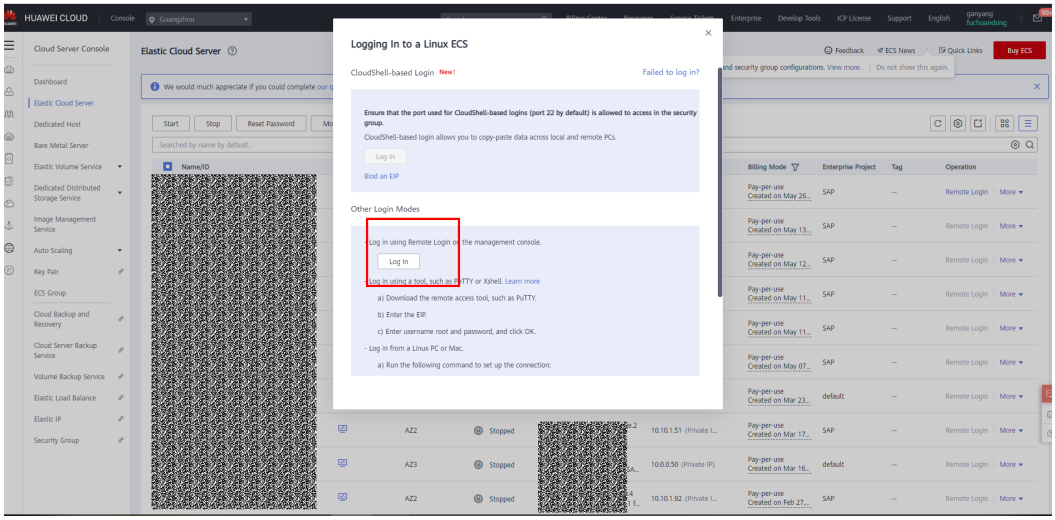
Step 6 Select an enterprise project and click **Next**.



Step 7 Create and purchase a Windows jump server.



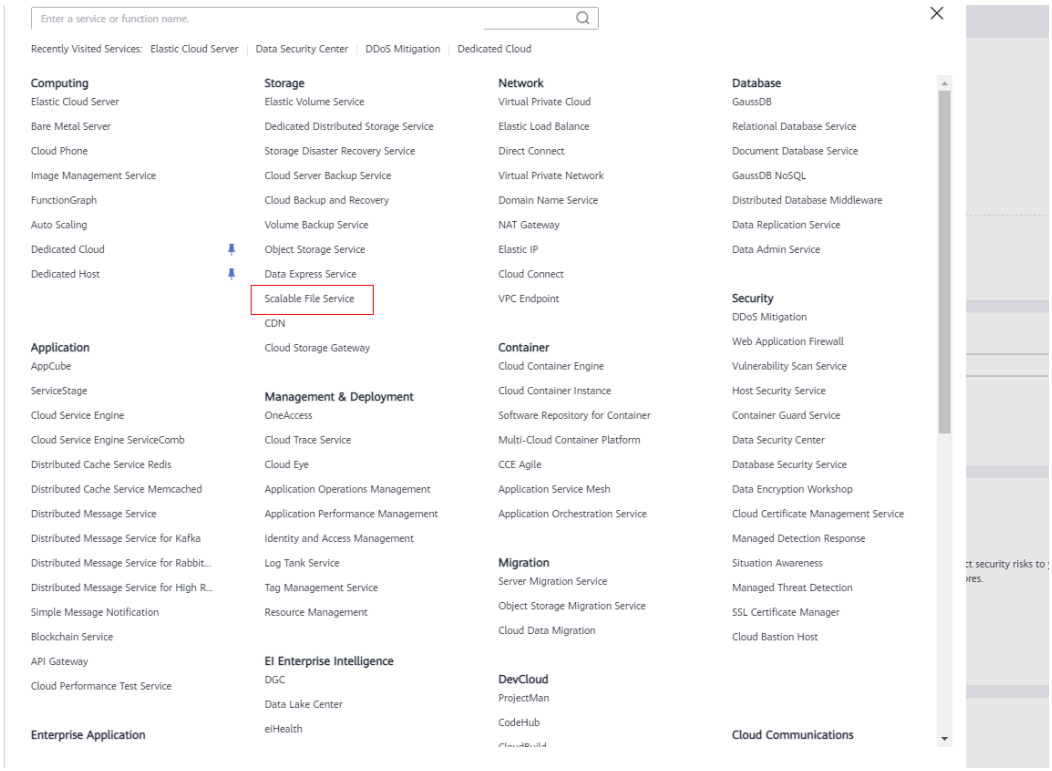
Step 8 After ECSs are created, locate the created ECSs in the ECS list and click **Remote Login** in the **Operation** column. Log in to the ECSs as user **root** using VNC.



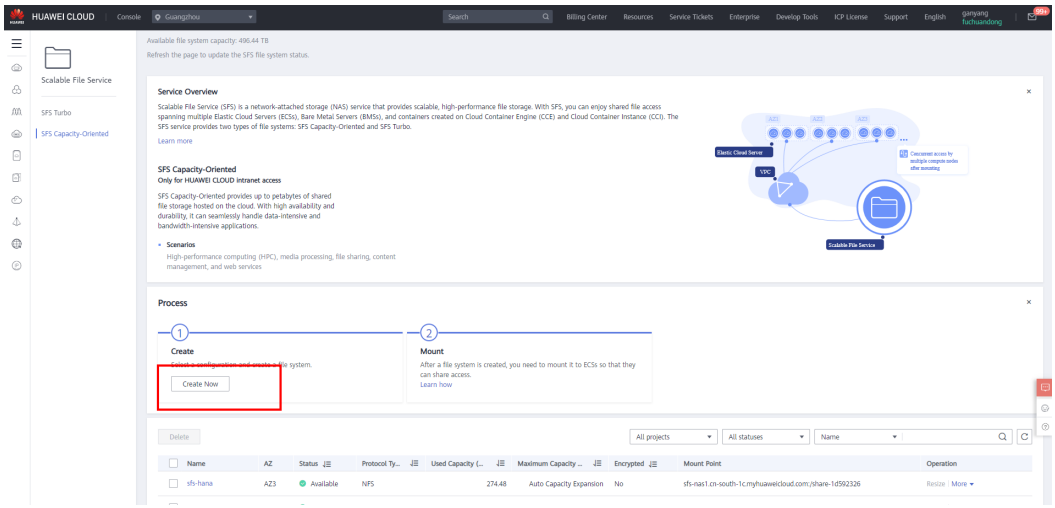
----End

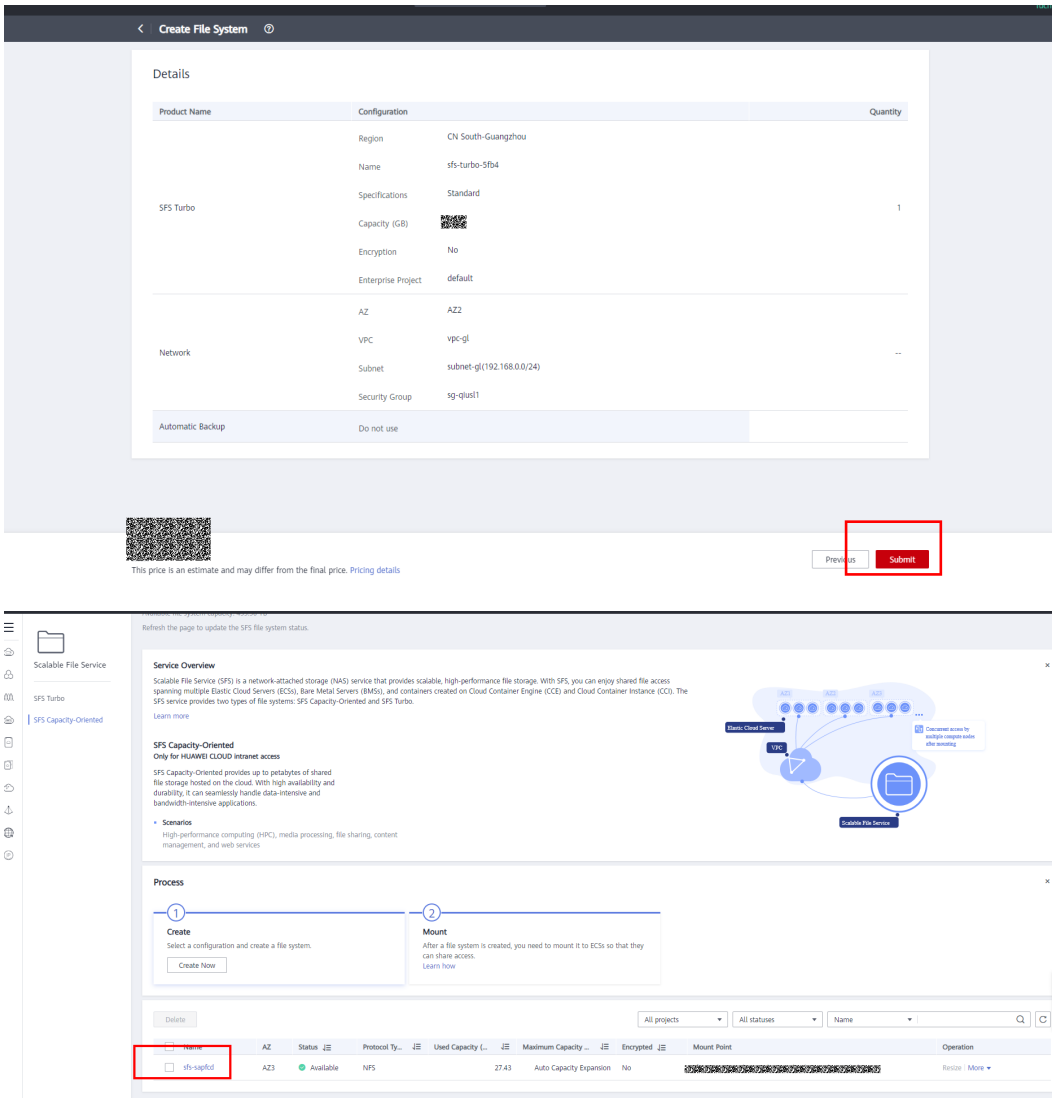
2.4.4 Purchasing and Mounting an SFS Disk

Step 1 Log in to the HUAWEI CLOUD management console, click the service list icon, and choose **Storage** > **Scalable File Service**.



Step 2 Create a file system and record the mount address.





Step 3 Log in to the ECS server and create the **mkdir /db2sfs** folder.

```
sapondb2:~ #
sapondb2:~ # mkdir /db2sfs
sapondb2:~ #
sapondb2:~ #
```

Step 4 Mount the **/db2sfs** directory to SFS.

echo "sfs-nas1.*:/share-cd3dc3c2 /db2sfs nfs vers=3,timeo=600,nolock 1 2" >>/etc/fstab**

Run the **mount -a** command to mount the directory.

```
sapondb2:~ #
sapondb2:~ # echo "[redacted]loud.com:/share-cd3dc3c2 /db2sfs n
sapondb2:~ #
sapondb2:~ # mount -a
```

Step 5 Run the **df -h** command to view the mounting result.


```
sapondb2:~ # df -h
Filesystem                                                Size  Used Avail Use% Mou
/dev/vda1                                                 99G  4.3G   90G   5% /
devtmpfs                                                  48G  8.0K   48G   1% /dev
tmpfs                                                     71G   84K   71G   1% /dev
tmpfs                                                     48G  9.8M   48G   1% /run
tmpfs                                                     48G     0   48G   0% /sys
[redacted]icloud.com:/share-cd3dc3c2                      10P     0   10P   0% /db2
```

----End

2.4.5 Creating a File System

Step 1 Run the **fdisk -l** command to check the unformatted disks.

```
sapondb2:~ # fdisk -l

Disk /dev/vda: 100 GiB, 107374182400 bytes, 209715200 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x000434aa

Device     Boot Start       End   Sectors  Size Id Type
/dev/vda1        2048 209715166 209713119  100G 83 Linux

Disk /dev/vdb: 100 GiB, 107374182400 bytes, 209715200 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/vdc: 40 GiB, 42949672960 bytes, 83886080 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/vdd: 30 GiB, 32212254720 bytes, 62914560 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/vde: 300 GiB, 322122547200 bytes, 629145600 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

Format disks and logical volumes.

mkfs.xfs /dev/vdb

mkfs.xfs /dev/vdc

mkfs.xfs /dev/vde

```
sapondb2:~ # mkfs.xfs /dev/vdb
meta-data=/dev/vdb               isize=256    agcount=4, agsize=6
         =                       sectsz=512   attr=2, projid32bit
         =                       crc=0        finobt=0
data     =                       bsize=4096   blocks=26214400, im
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
log      =internal log           bsize=4096   blocks=12800, versi
         =                       sectsz=512   sunit=0 blks, lazy-
realtime =none                   extsz=4096   blocks=0, rtextents
sapondb2:~ # mkfs.xfs /dev/vdc
meta-data=/dev/vdc               isize=256    agcount=4, agsize=2
         =                       sectsz=512   attr=2, projid32bit
         =                       crc=0        finobt=0
data     =                       bsize=4096   blocks=10485760, im
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
log      =internal log           bsize=4096   blocks=5120, versio
         =                       sectsz=512   sunit=0 blks, lazy-
realtime =none                   extsz=4096   blocks=0, rtextents
sapondb2:~ # mkfs.xfs /dev/vdd
meta-data=/dev/vdd               isize=256    agcount=4, agsize=1
         =                       sectsz=512   attr=2, projid32bit
         =                       crc=0        finobt=0
data     =                       bsize=4096   blocks=7864320, ima
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
log      =internal log           bsize=4096   blocks=3840, versio
         =                       sectsz=512   sunit=0 blks, lazy-
realtime =none                   extsz=4096   blocks=0, rtextents
sapondb2:~ # mkfs.xfs /dev/vde
meta-data=/dev/vde               isize=256    agcount=4, agsize=1
         =                       sectsz=512   attr=2, projid32bit
         =                       crc=0        finobt=0
data     =                       bsize=4096   blocks=78643200, im
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
log      =internal log           bsize=4096   blocks=38400, versi
         =                       sectsz=512   sunit=0 blks, lazy-
realtime =none                   extsz=4096   blocks=0, rtextents
sapondb2:~ #
```

Create a file system directory.

mkdir -p /usr/sap /sapmnt /db2

```
sapondb2:~ # mkdir -p /usr/sap /sapmnt /db2
sapondb2:~ #
sapondb2:~ #
```

Run the **blkid** command to obtain the UUID of the disk.

```
sapondb2:~ # blkid
/dev/vda1: UUID="27a5e4ec-1915-4161-b94c-675c7393b494" TYPE="ext
/dev/vdb: UUID="3813b122-7ba0-4333-a791-d8881dbf9783" TYPE="xfs"
/dev/vdc: UUID="4c1a7079-9aee-4e80-9a04-fac2bf19734f" TYPE="xfs"
/dev/vdd: UUID="5c33db87-94b0-4e04-b417-5e6d8df4a6d4" TYPE="xfs"
/dev/vde: UUID="5e1e498e-e704-4e46-840b-4dbea0205166" TYPE="xfs"
```

Create mount points in **/etc/fstab**.

echo "UUID=3813b122-7ba0-4333-a791-d8881dbf9783 /usr/sap xfs defaults 0 0" >>/etc/fstab

echo "UUID=4c1a7079-9aee-4e80-9a04-fac2bf19734f /sapmnt xfs defaults 0 0" >>/etc/fstab

echo "UUID=5e1e498e-e704-4e46-840b-4dbea0205166 /db2 xfs defaults 0 0" >>/etc/fstab

```
sapondb2:~ #
sapondb2:~ # echo "UUID=3813b122-7ba0-4333-a791-d8881dbf9783 /usr
sapondb2:~ # echo "UUID=4c1a7079-9aee-4e80-9a04-fac2bf19734f /sap
sapondb2:~ # echo "UUID=5e1e498e-e704-4e46-840b-4dbea0205166 /db2
sapondb2:~ #
```

Run the **mount -a** command to mount all disks and run the **df -h** command to check the disk mounting results.

```
sapondb2:~ # mount -a
```

```
sapondb2:~ # df -h
Filesystem                                                Size  Used
/dev/vda1                                                  99G  4.3G
devtmpfs                                                   48G  8.0K
tmpfs                                                      71G   84K
tmpfs                                                      48G  9.8M
tmpfs                                                      48G     0
sfs-nas1.cn-south-1c.myhuaweicloud.com:/share-cd3dc3c2     10P     0
/dev/vdb                                                  100G   33M
/dev/vdc                                                   40G   33M
/dev/vde                                                  300G   33M
```

----End

2.4.6 Configuring the Swap Partition

Step 1 Use partitions/disks as the swap partition.

Run the following command to configure the swap partition.

mkswap /dev/vdd

```
sapondb2:~ # mkswap /dev/vdd
mkswap: /dev/vdd: warning: wiping old xfs signature.
Setting up swapspace version 1, size = 31457276 KiB
no label, UUID=43a73cdb-4359-4141-a255-b86156d1f433
sapondb2:~ #
```

Step 2 Run the following command to enable the swap partition.

swapon /dev/vdd

```
sapondb2:~ # swapon /dev/vdd
sapondb2:~ #
sapondb2:~ #
```

Step 3 Write the following information to **/etc/fstab**.

echo "UUID=43a73cdb-4359-4141-a255-b86156d1f433 swap swap defaults 0 0" >> /etc/fstab

```
sapondb2:~ # echo "UUID=43a73cdb-4359-4141-a255-b86156d1f433 swap
sapondb2:~ #
```

Step 4 Run the following command to check the size of the current memory and swap space. The default unit is KB, and the unit of **-m** is MB

free -m

```
sapondb2:~ # free -m
              total        used        free      shared     buffers
Mem:          96879        1182       95696           9          36
-/+ buffers/cache:         765       96113
Swap:         30719           0       30719
```

Step 5 Run the following command to check swap information, including detailed information about files and partitions.

swapon -s

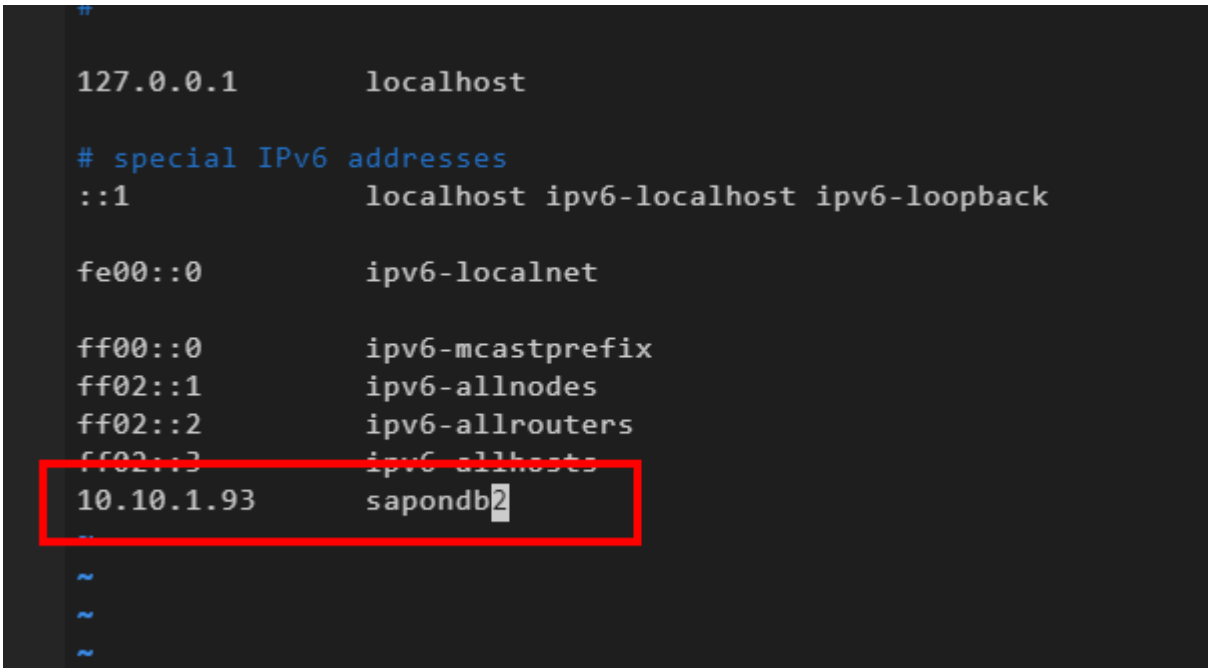
```
sapondb2:~ # swapon -s
Filename                                Type            Size
/dev/vdd                                partition       31457276
sapondb2:~ #
```


----End

2.4.7 Configuring the hosts File

Configure the **hosts** file. During SAP software installation, the SAP software automatically maps host names to IP addresses.

Step 1 Run the **vi /etc/hosts** command to add the IP addresses mapped to the host names.



----End

2.4.8 Downloading and Decompressing the SAP Software Package

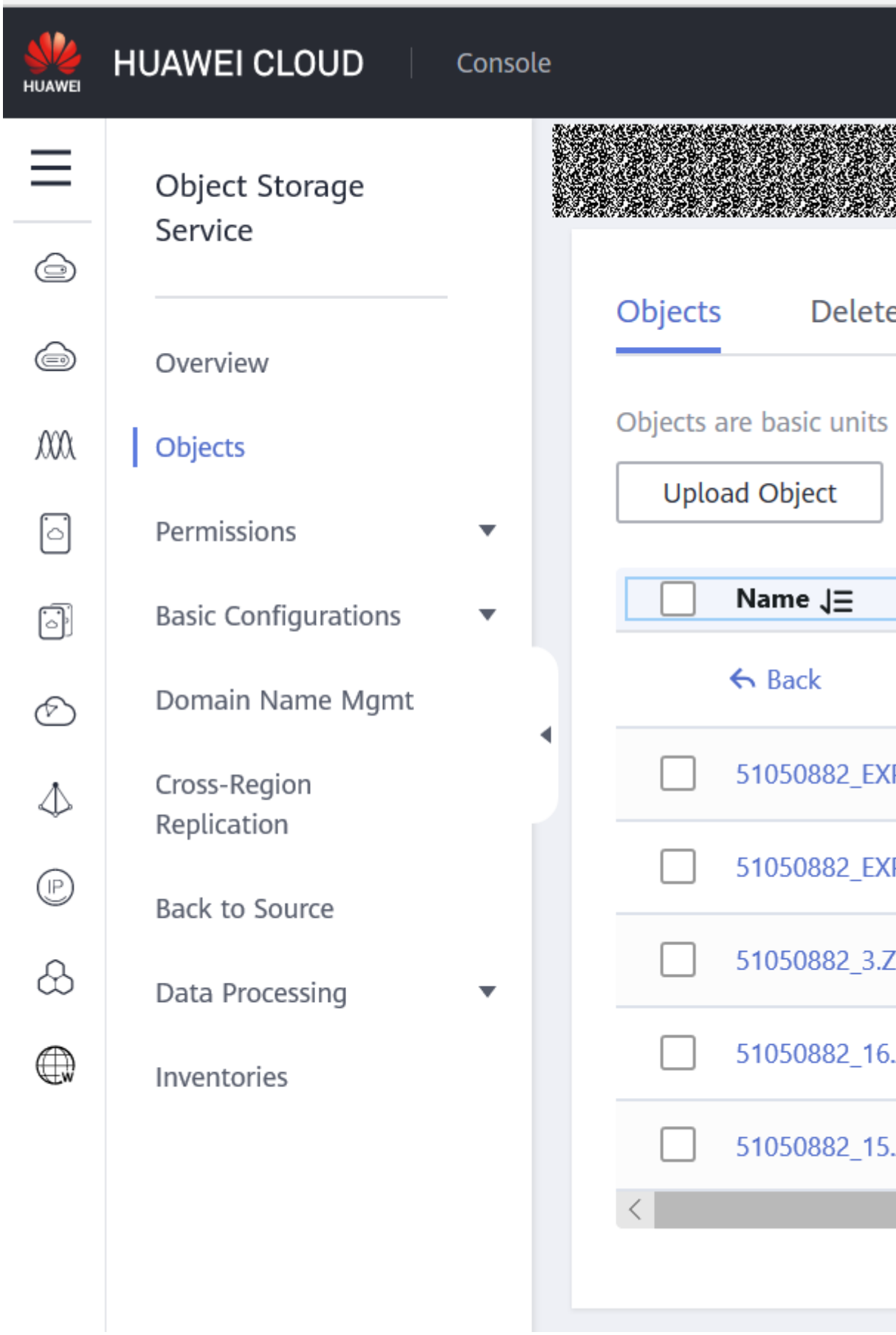
Download the SAP application and DB2 installation files from the official website, upload them to the OBS bucket, copy them to the ECSs, decompress them, and start the software installation.

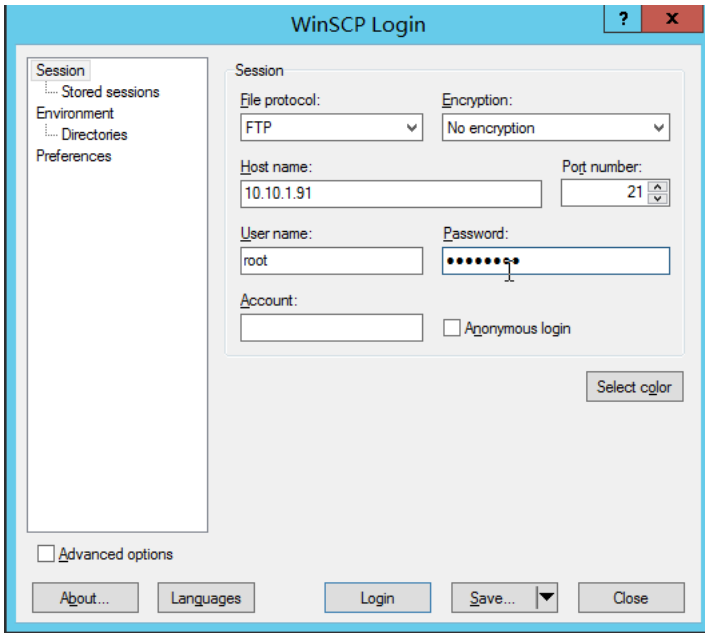
Download the software from **https://support.sap.com/swdc** by referring to official SAP installation guide.

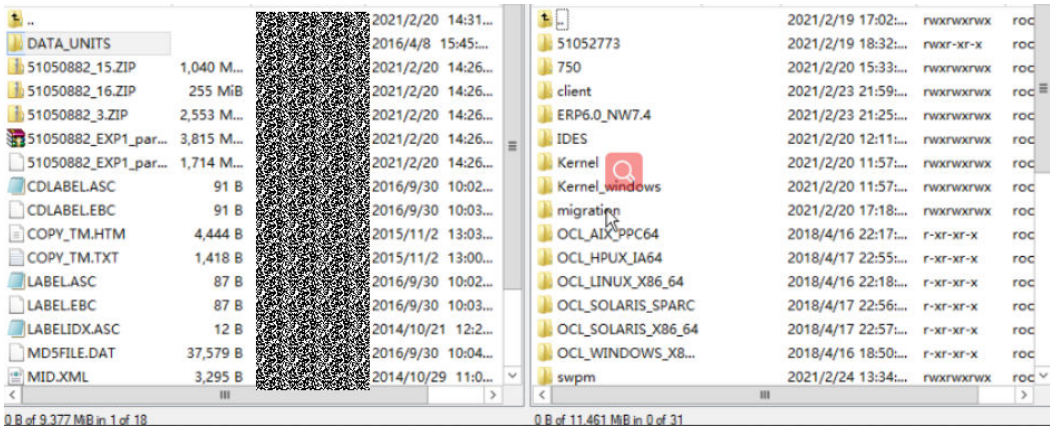
Decompressing the Software Packages

After the SAP software is downloaded and copied to the ECS, decompress the software package.

Step 1 Decompress the ERP6.0 EHP7 software package compressed using exe in Windows and copy it to the SAP DB2 virtual machine (VM) using SCP. An example is as follows:







Step 2 Go to the directory where the downloaded software package is stored on the ECS and run the **unzip** command to decompress it. An example is provided as follows:

Step 3 Go to the **DATA_UNITS** folder and modify the **LABELIDX.ASC** file. This step will be verified during SAP software installation.

vi LABELIDX.ASC

Step 4 Decompress the SWPM. An example is as follows:

Go to the **SWPM** directory and run the following command:

chmod 777 SAPCAR.EXE

./SAPCAR.EXE -xvf SWPM**.SAR

```
db2test:/db2sfs/db2/sap_on_db2/swpm # chmod 777 SAPCAR_721-20010450.EXE
db2test:/db2sfs/db2/sap_on_db2/swpm # ./SAPCAR_721-20010450.EXE -xvf SWPM1
2-20009701.SAR
SAPCAR: processing archive SWPM10SP25_2-20009701.SAR (version 2.01)
x BPP07
x BPP07/HDB
x BPP07/HDB/CP
x BPP07/HDB/CP/jexclude.xml
x BPP07/HDB/CP/packages.xml
x BPP07/HDB/CP/pfl_ASCS_ind_ind_ind.pfl
x BPP07/HDB/CP/pfl_CI_ind_ind_ind.pfl
x BPP07/HDB/CP/pfl_default_ind_ind_ind.pfl
x BPP07/HDB/CP/pfl_DI_ind_ind_ind.pfl
x BPP07/HDB/CP/pfl_ERS_ind_ind_ind.pfl
```

----End

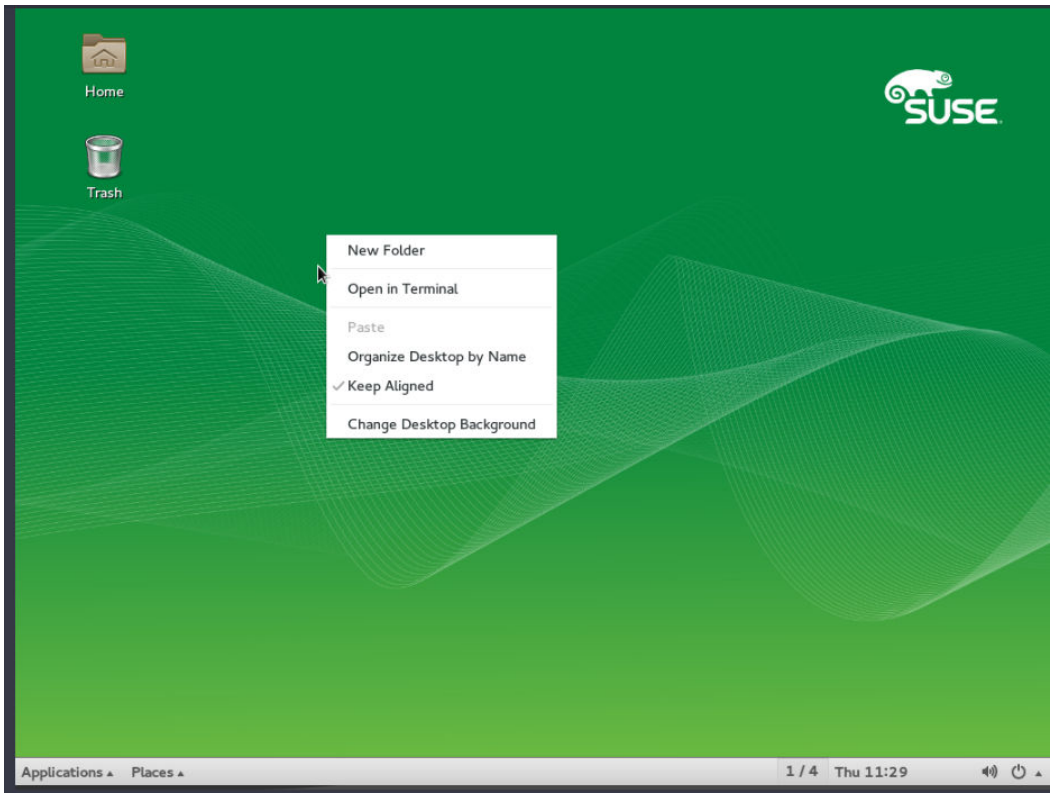
2.5 Installing SAP Software and DB2

Download the SAP application installation packages from the official website, upload them to the ECSs, decompress the packages, and start the software installation.

2.5.1 Installing the SAP Application

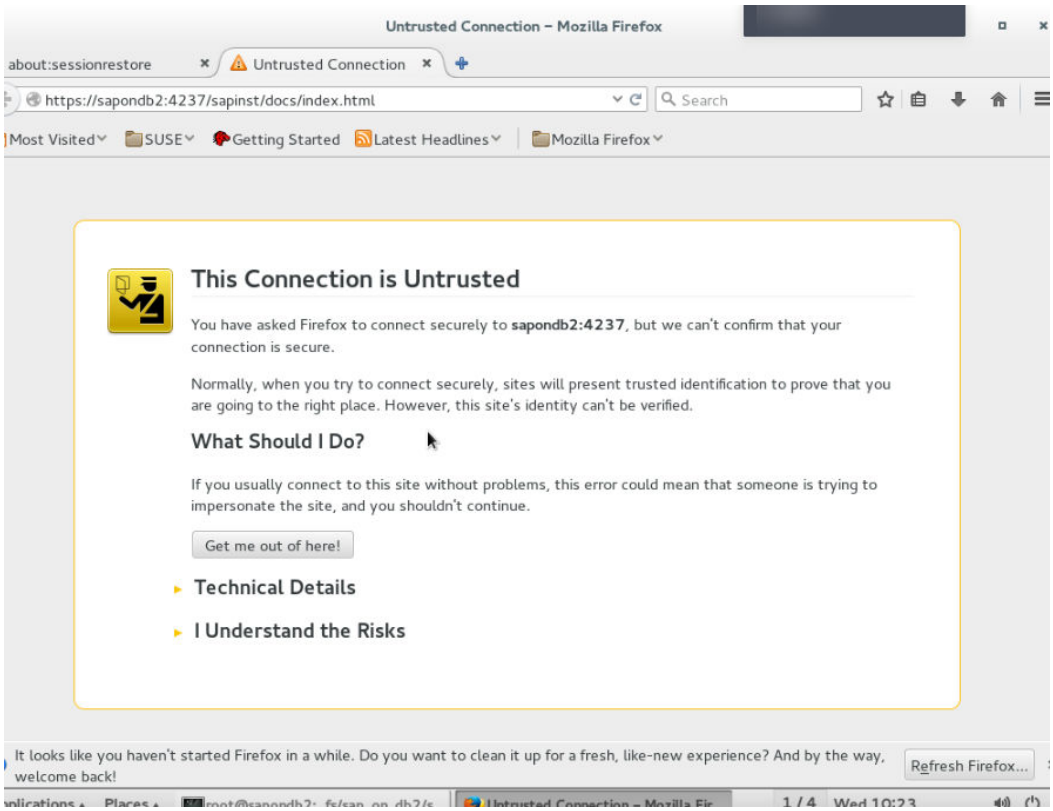
Before installing SAP on DB2, you need to install SAP using the sapint (during the installation, DB2 is automatically installed).

Step 1 On the HUAWEI CLOUD console, log in to the ECS as the **root** user using VNC, right-click, and choose **Open in Terminal**.

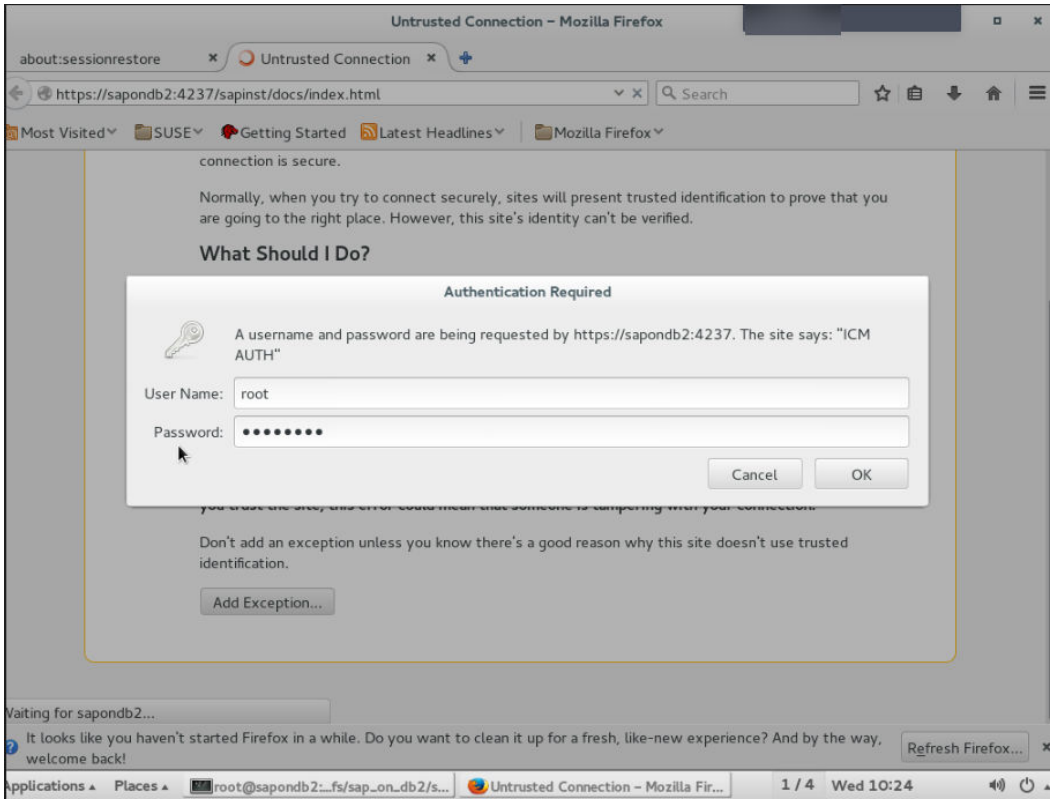


Step 2 Go to the **swpm** directory and run the **./sapinst** command.

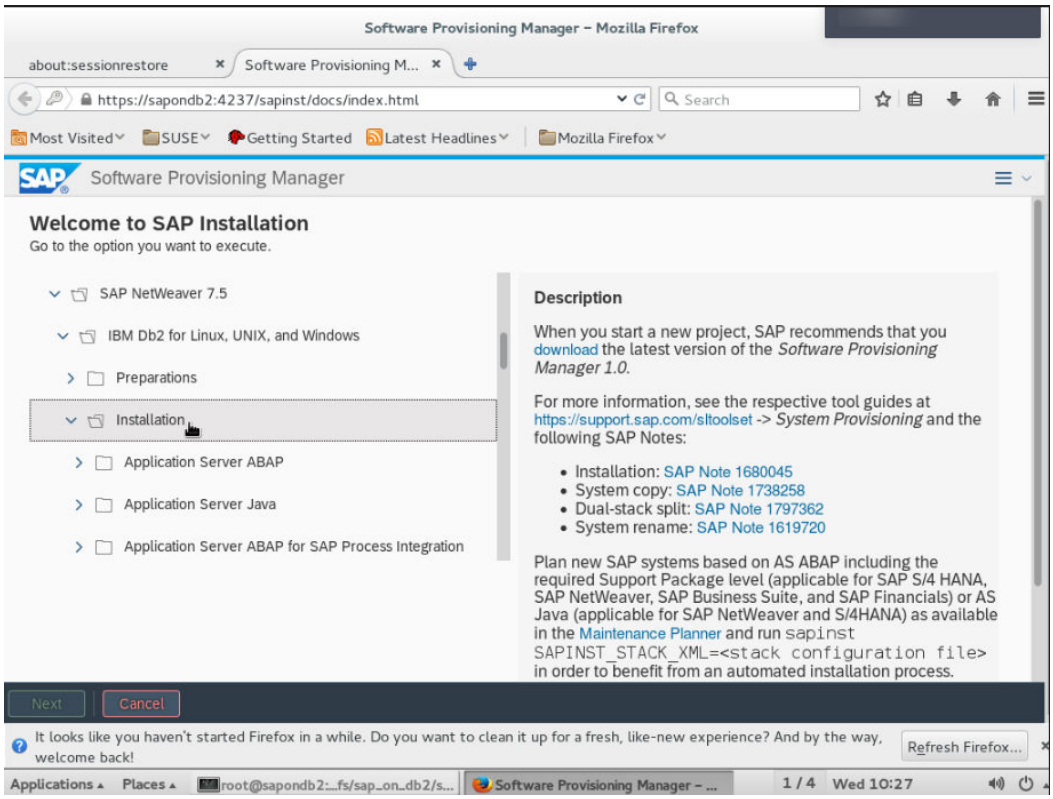
Step 3 Open a browser, enter **https://***host name***:4237/sapinst/docs/index.html** in the address box, and press **Enter**.

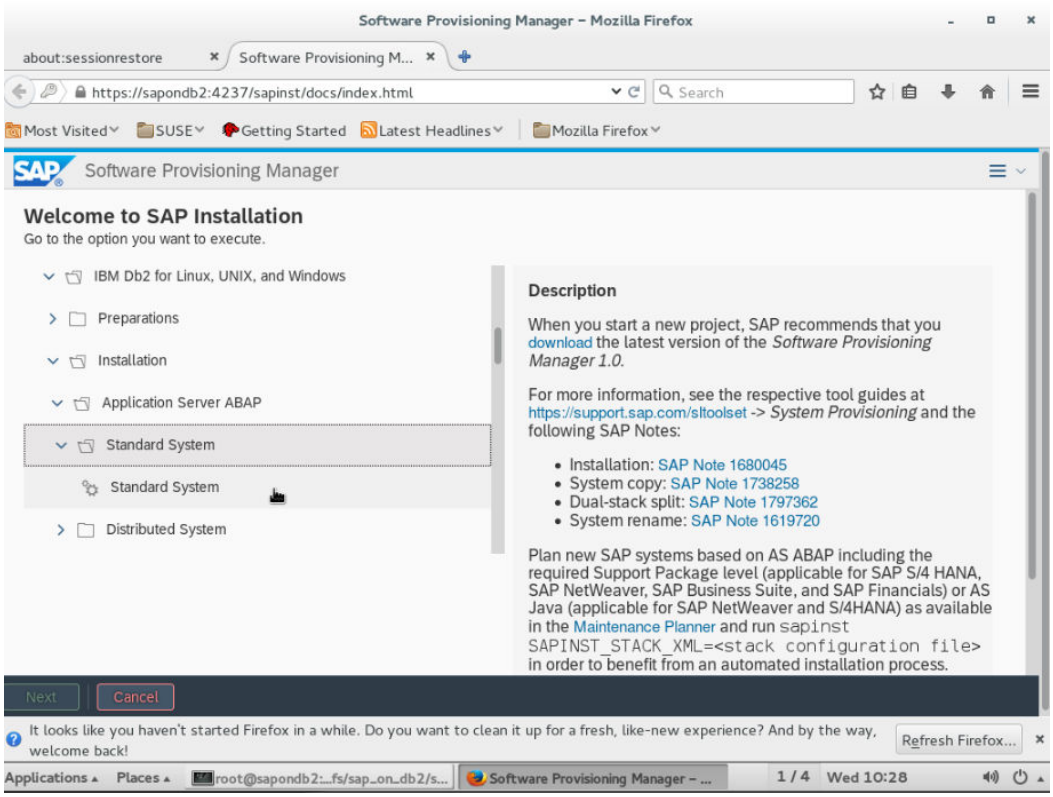


Step 4 Enter the **root** username and password.

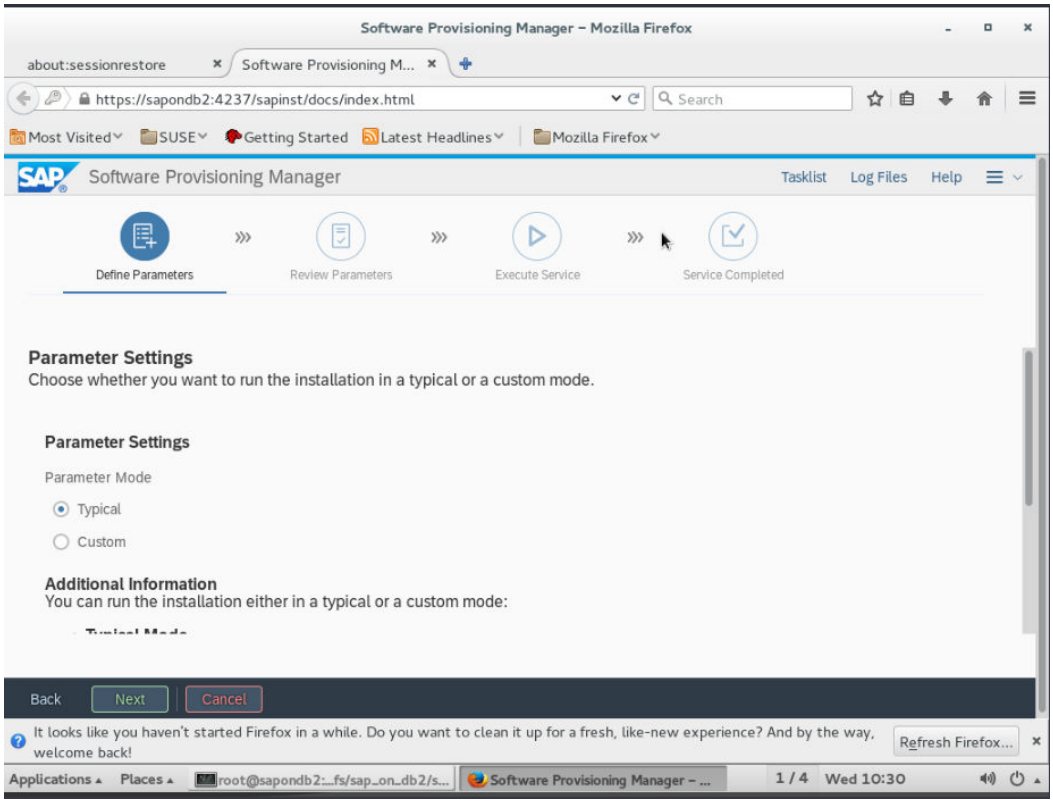


Step 5 Choose **SAP NetWeaver 7.5** > **IBM DB2 for Linux, UNIX, and Windows** > **Installation** > **Application Server ABAP** > **Standard System** > **Standard System**, and click **Next**.

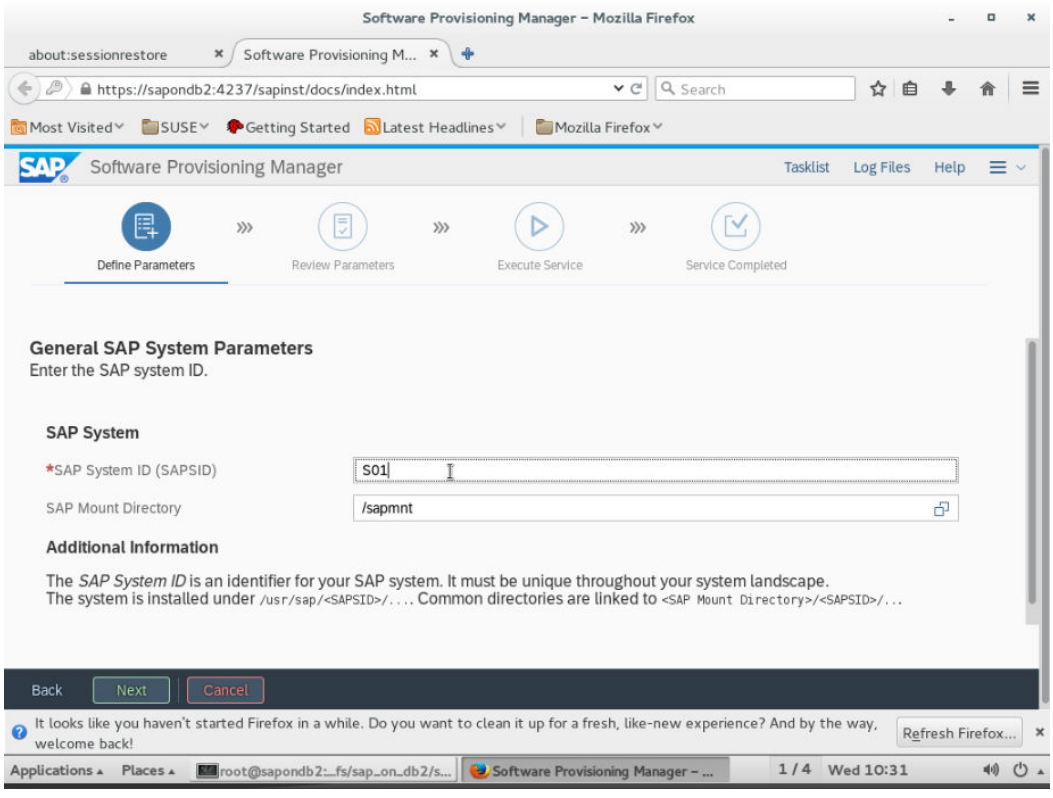




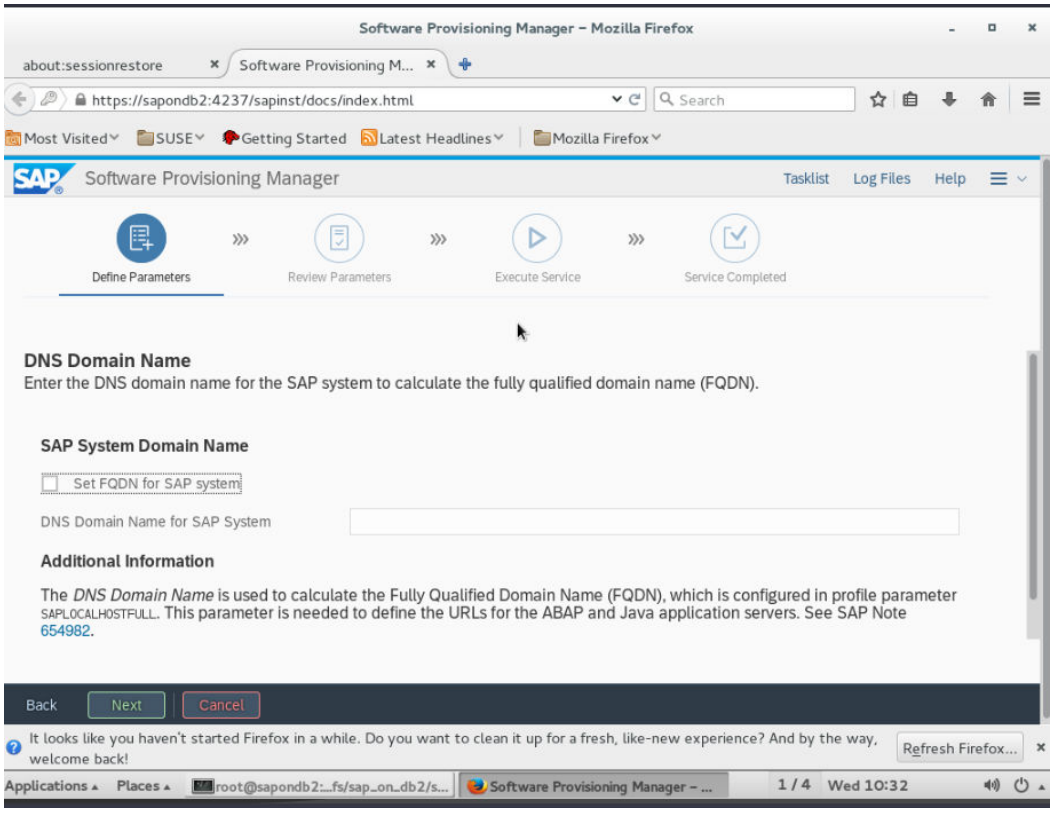
Step 6 Use the default settings, and click **Next**.



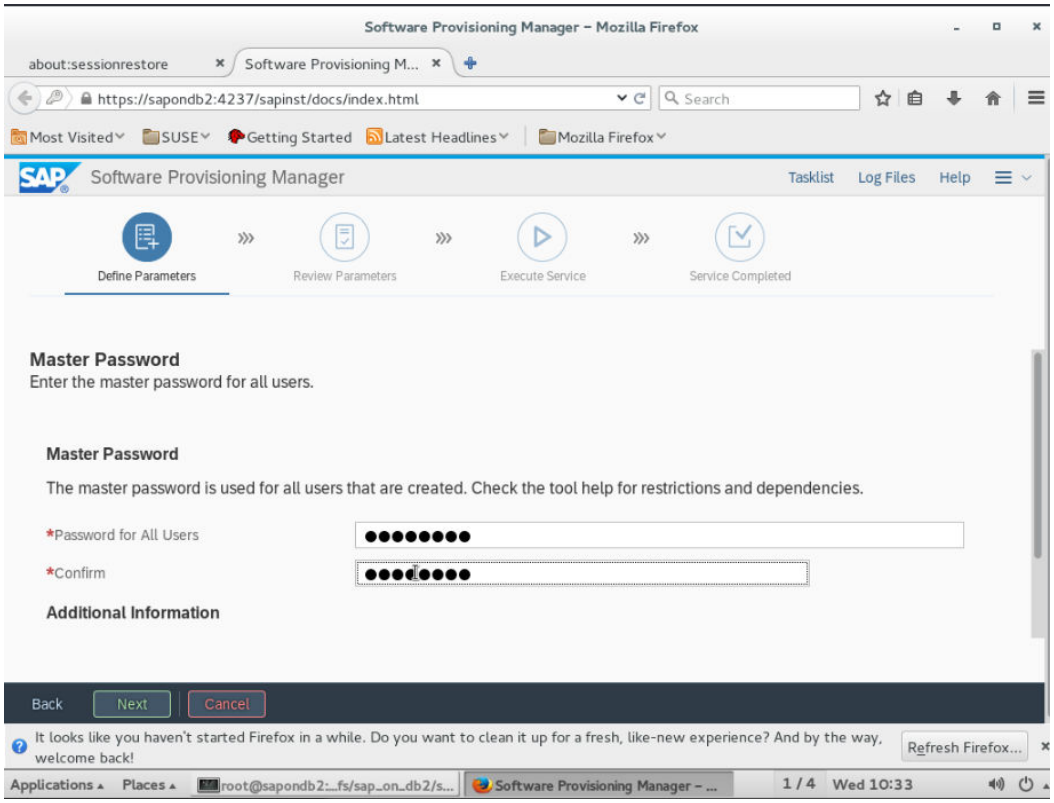
Step 7 Enter the SID to be created and click **Next**.



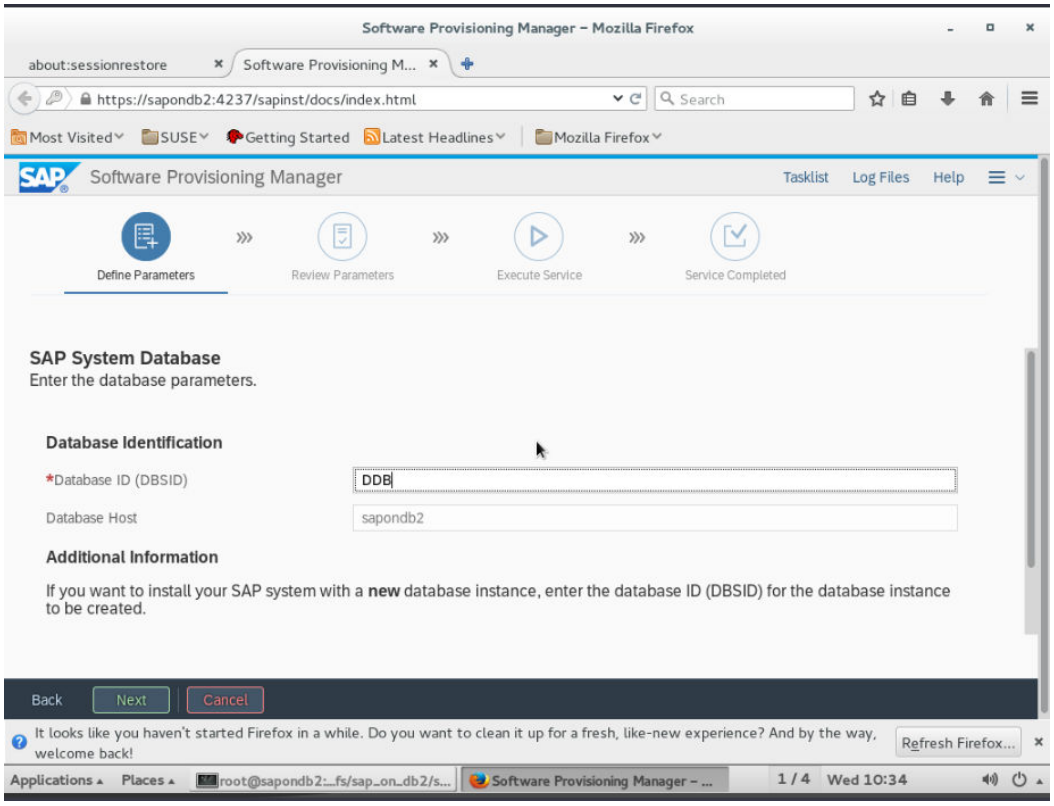
Step 8 Deselect **Set FQDN for SAP system** and click **Next**.



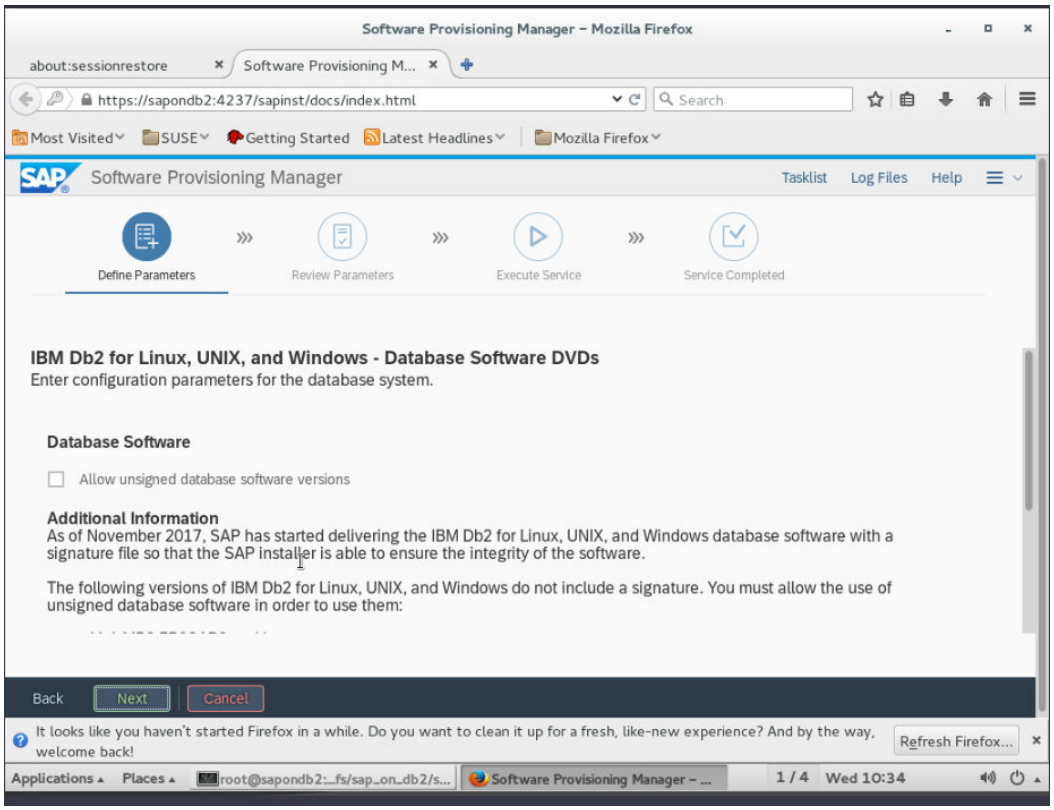
Step 9 Enter the passwords of all users to be created and click **Next**.



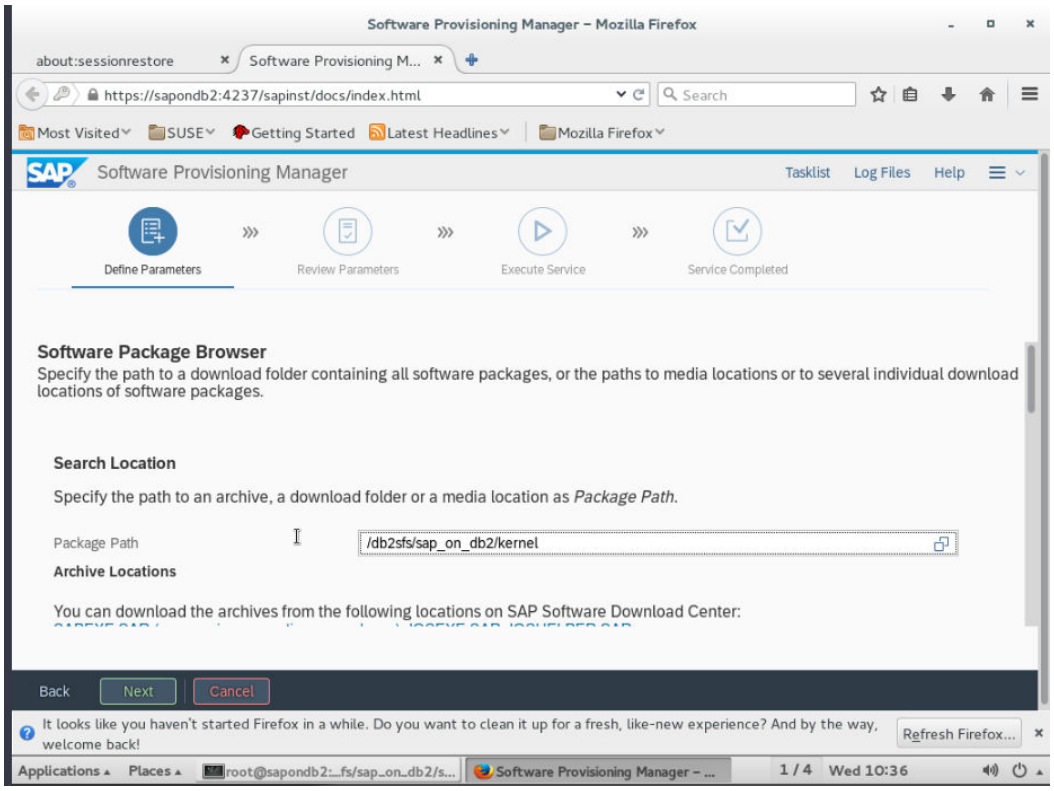
Step 10 Enter the SID of the database to be created, select a file system, and click **Next**.



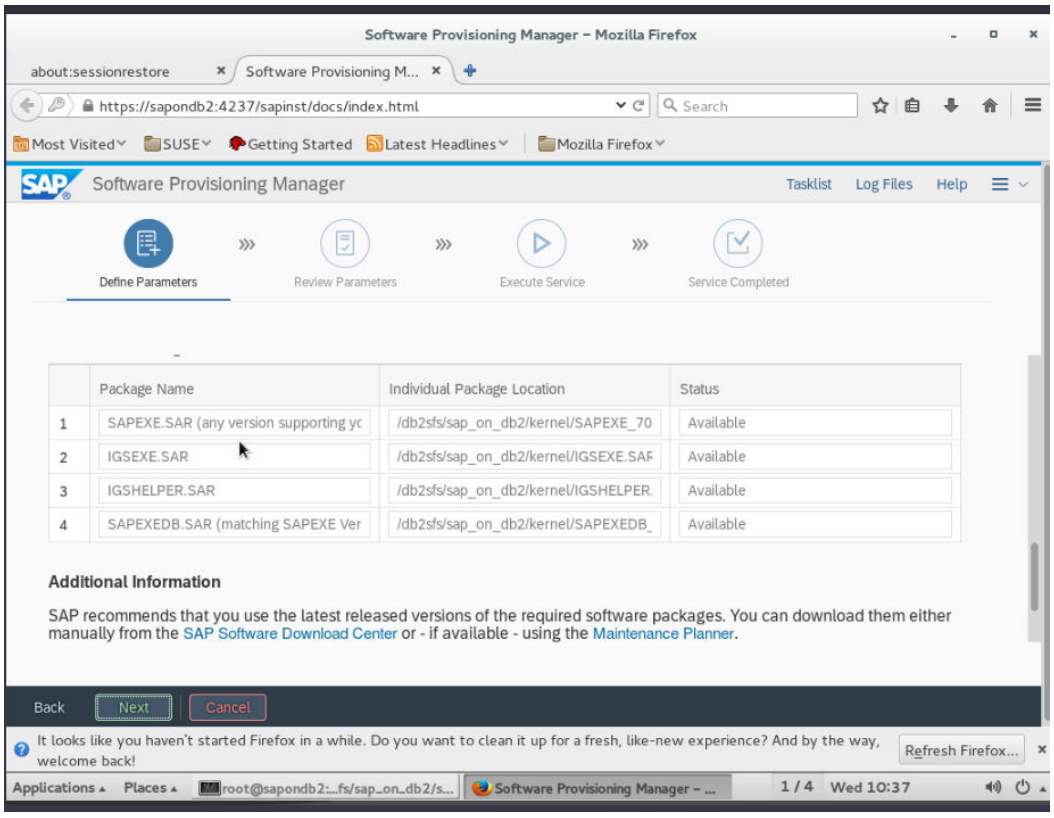
Step 11 Use the default settings and click **Next**.



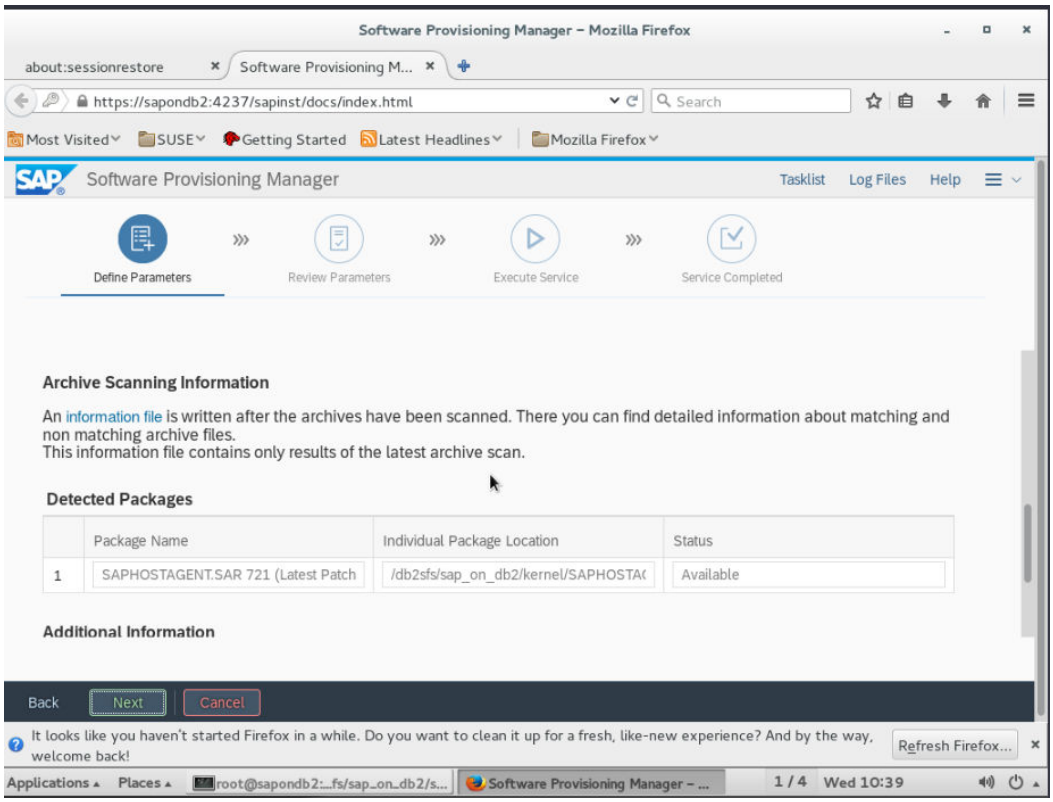
Step 12 Select the path where the kernel software package is stored and click **Next**.



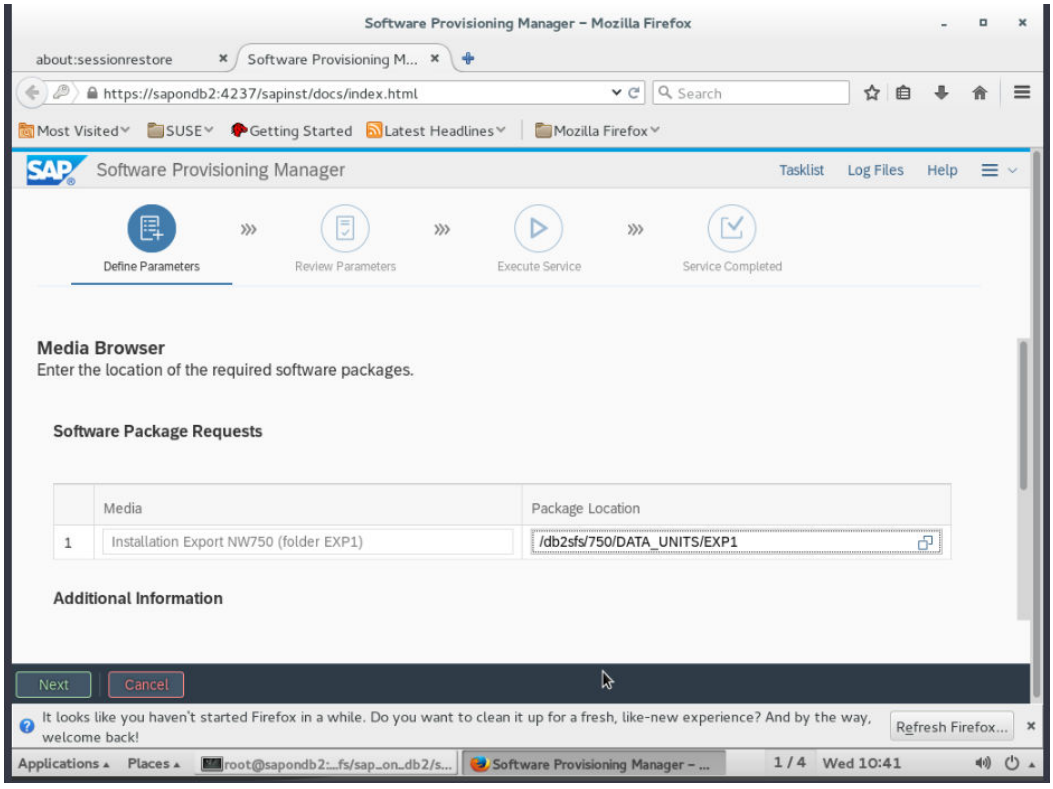
Step 13 After the software package status changes to **Available**, click **Next**.



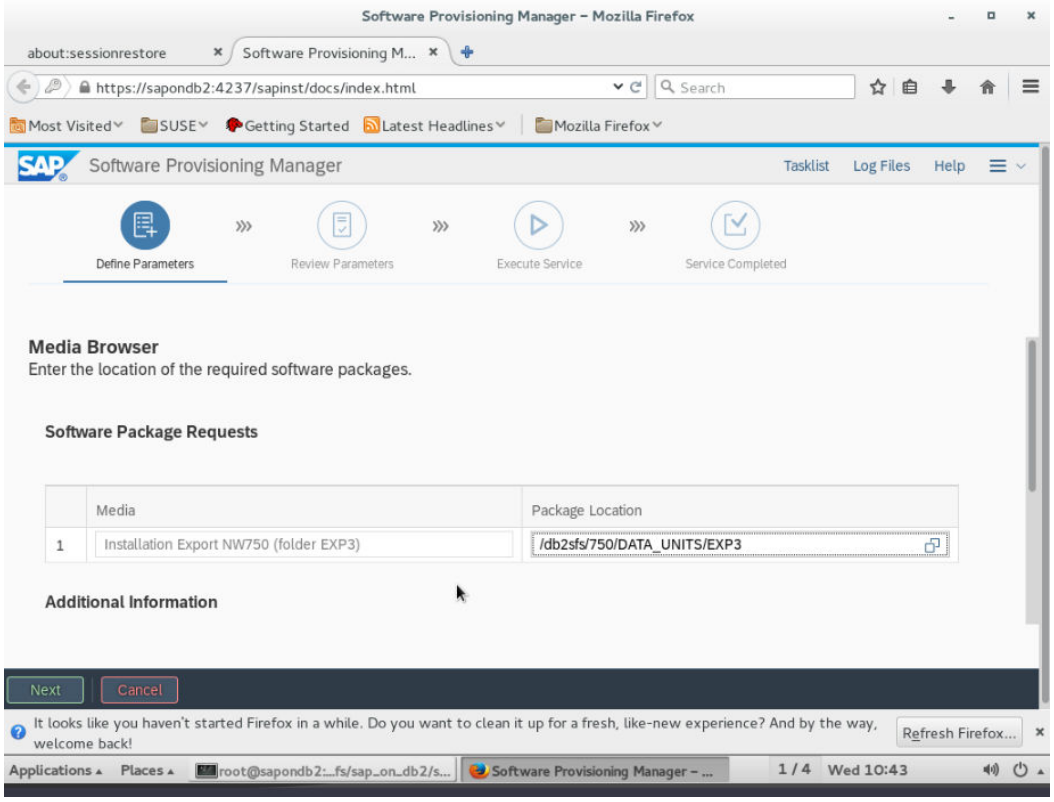
Step 14 Click **Next**.



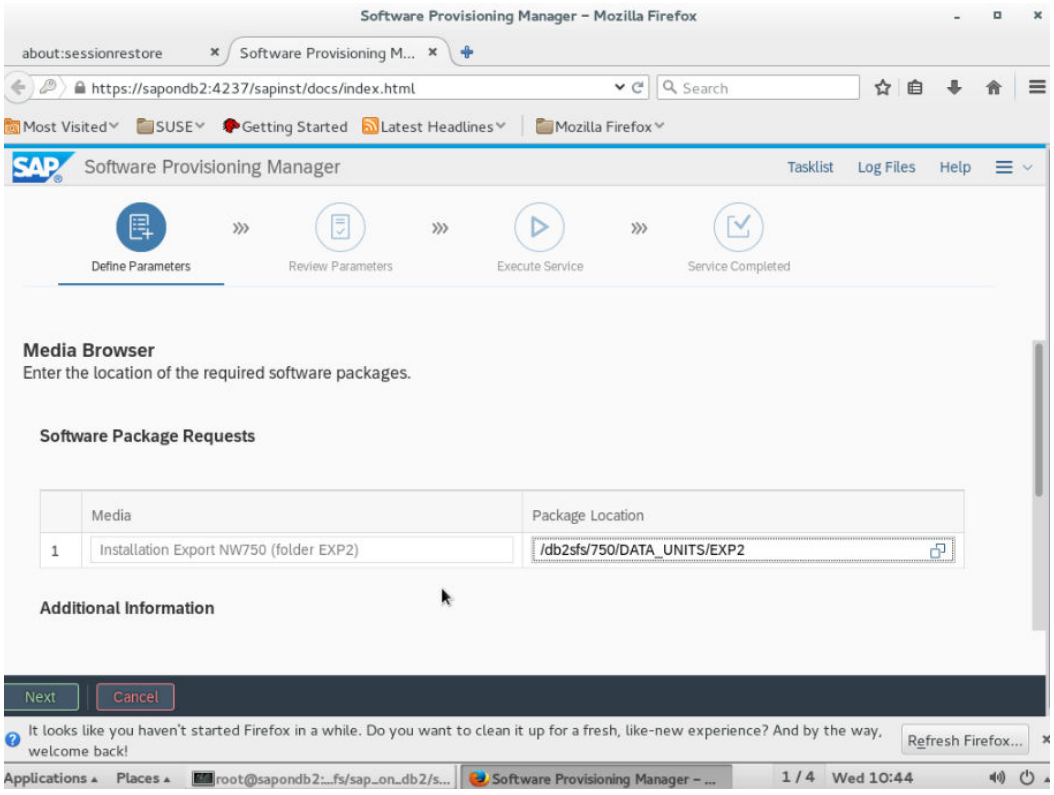
Step 15 Select the path where EXPORT_1 is located and click **Next**.



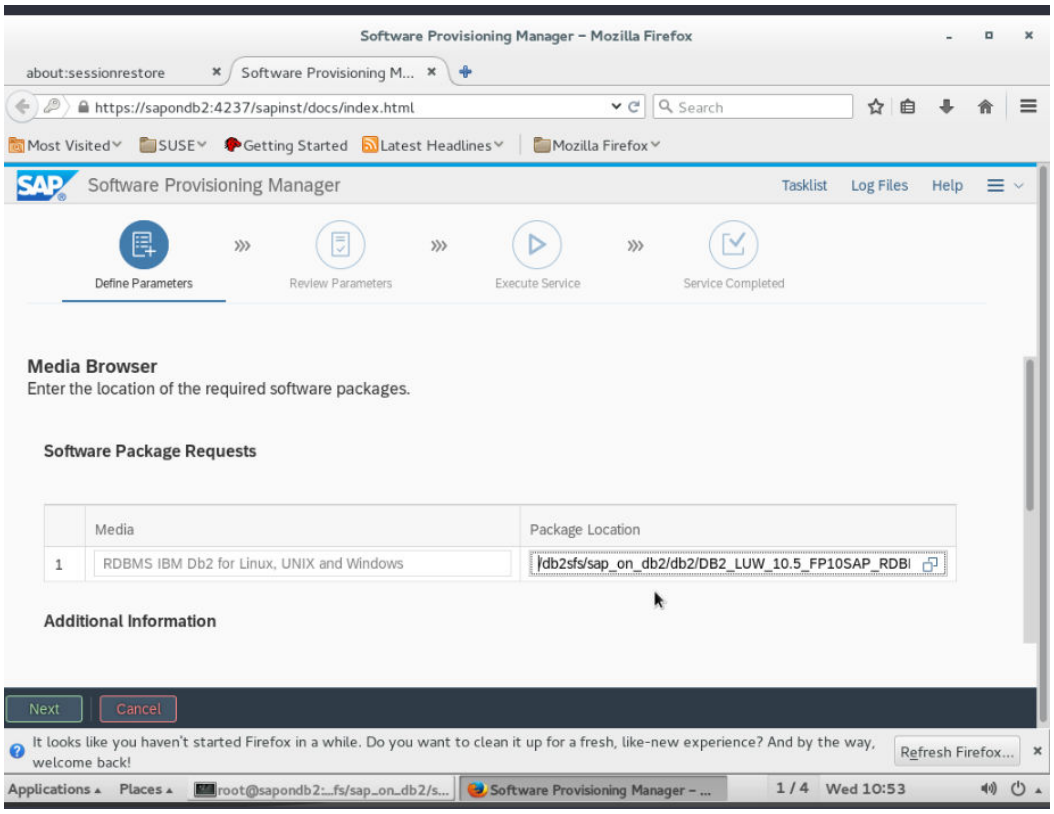
Step 16 Select the path where EXPORT3 is located and click **Next**.



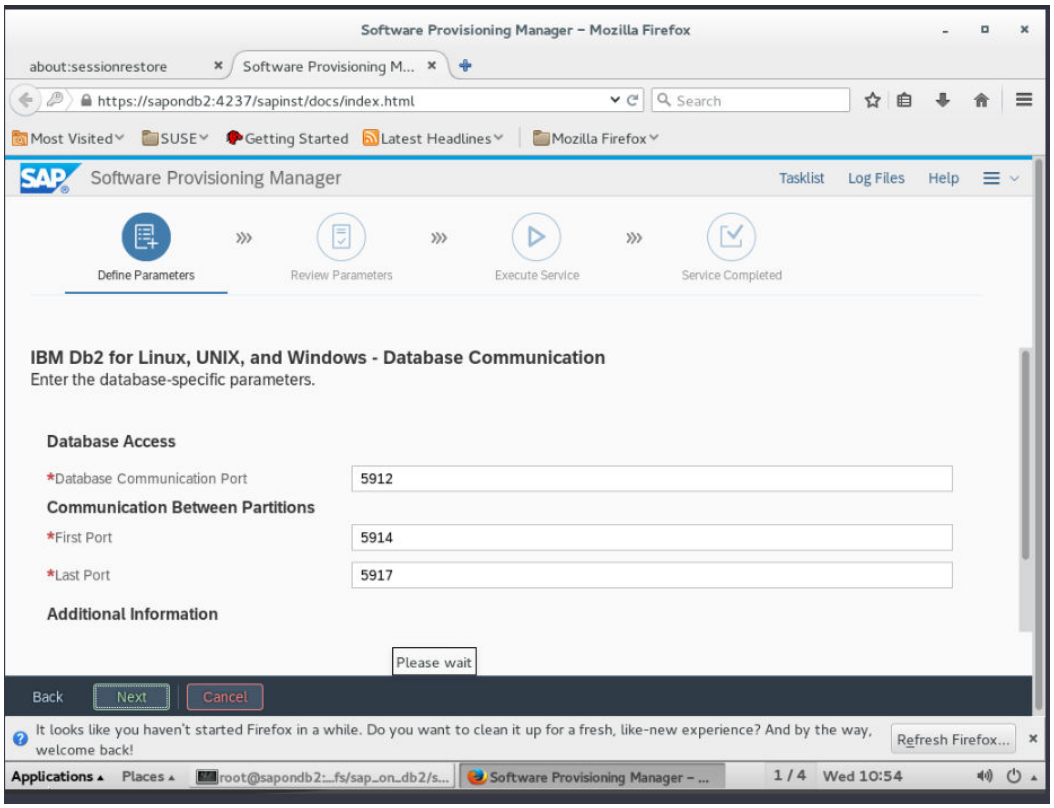
Step 17 Select the path where EXPORT2 is located and click **Next**.



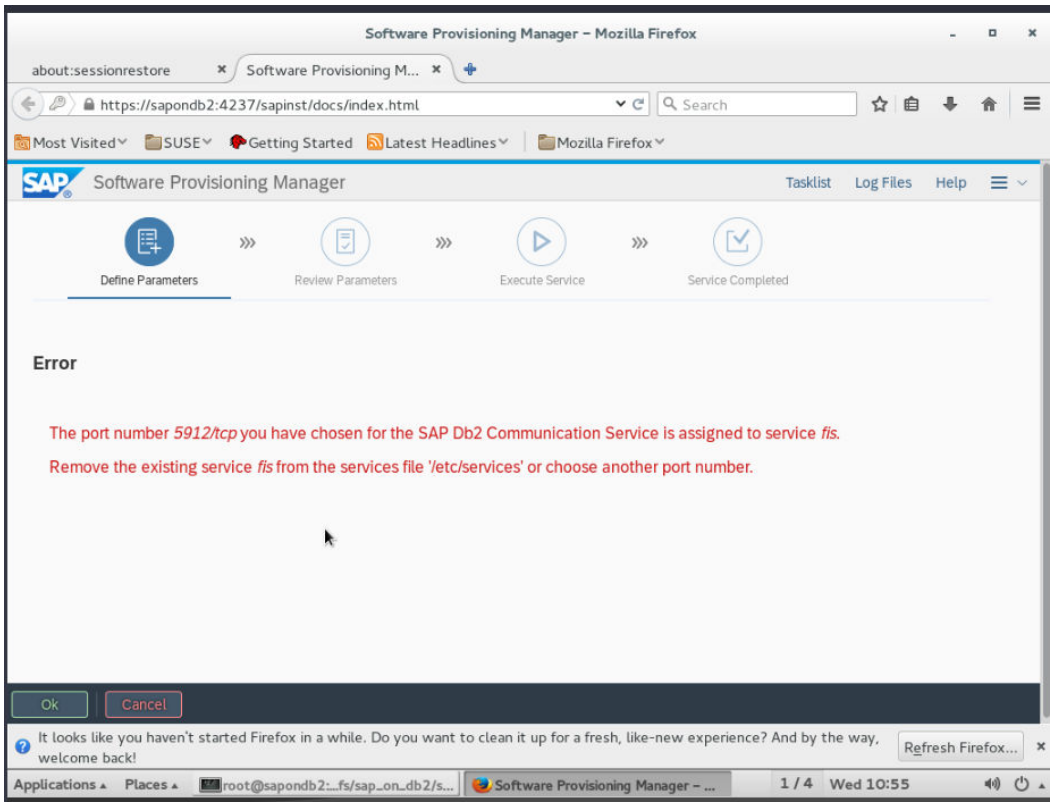
Step 18 Select the path where RDBMS is located and click **Next**.



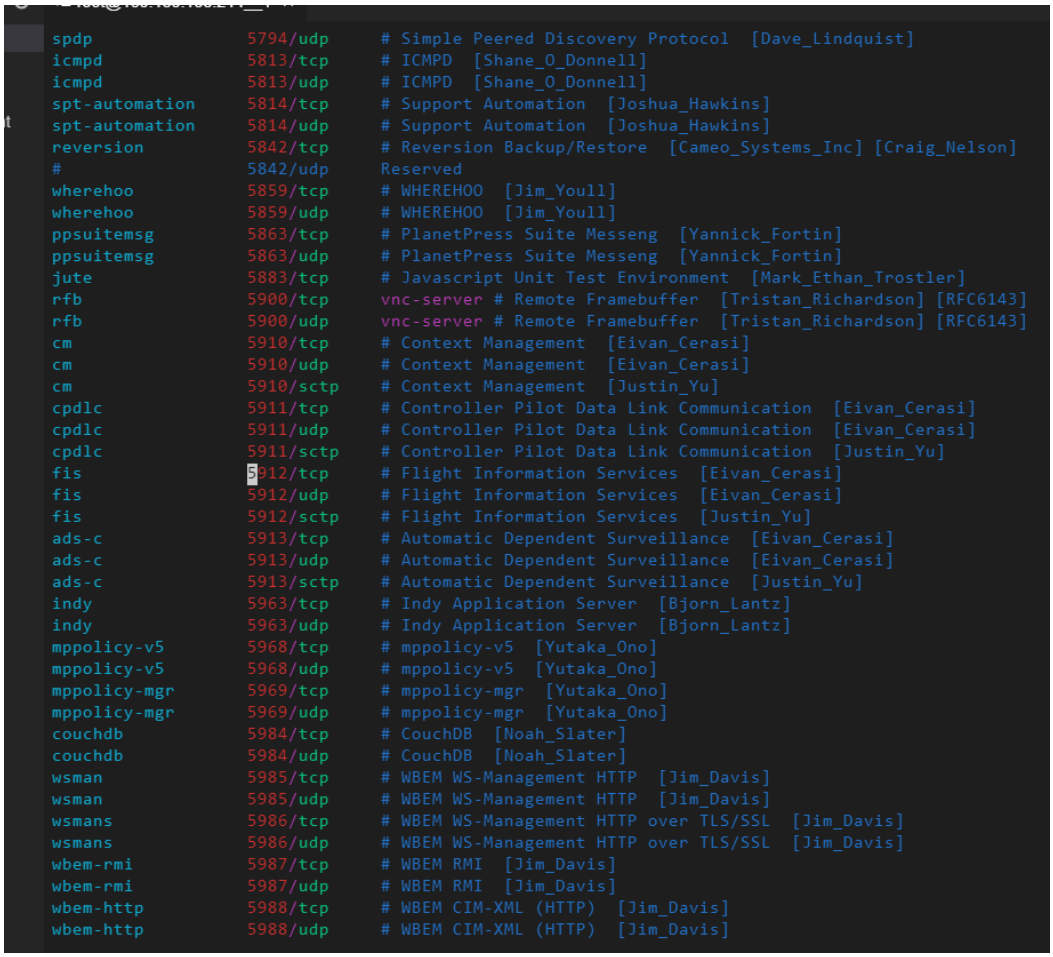
Step 19 Use the default port, and click **Next**.



Step 20 A message indicating that the port is occupied is displayed. Go to **/etc/services** to view the idle ports.

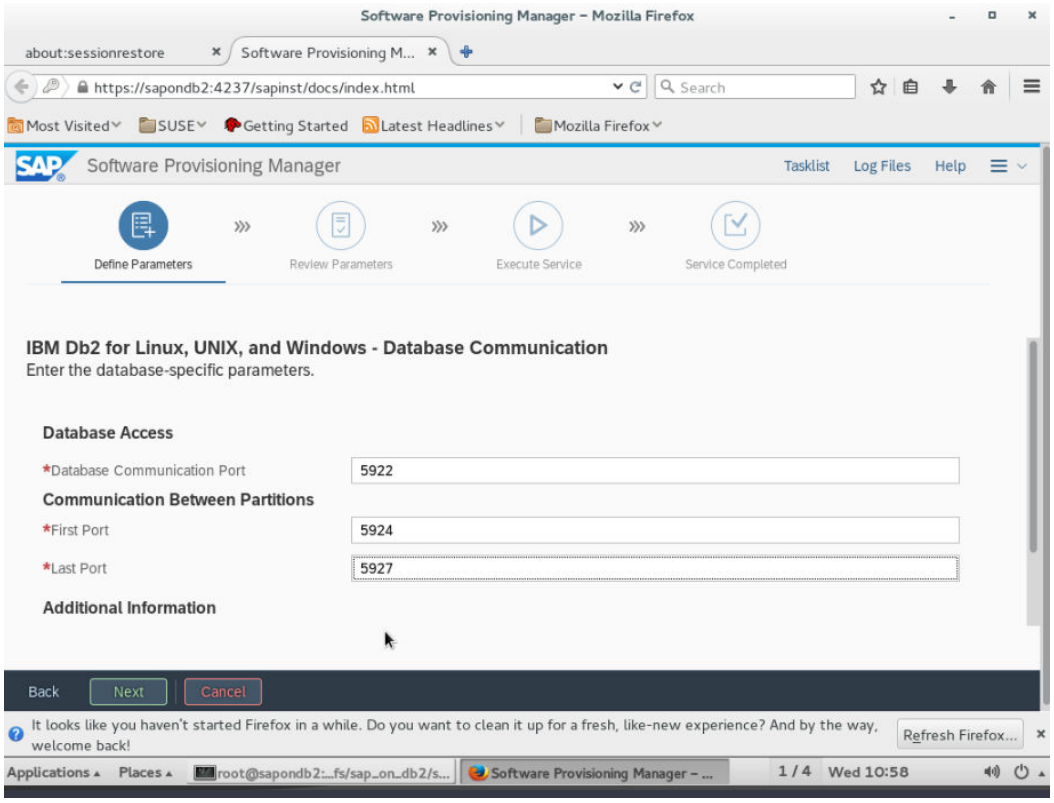


vi /etc/services

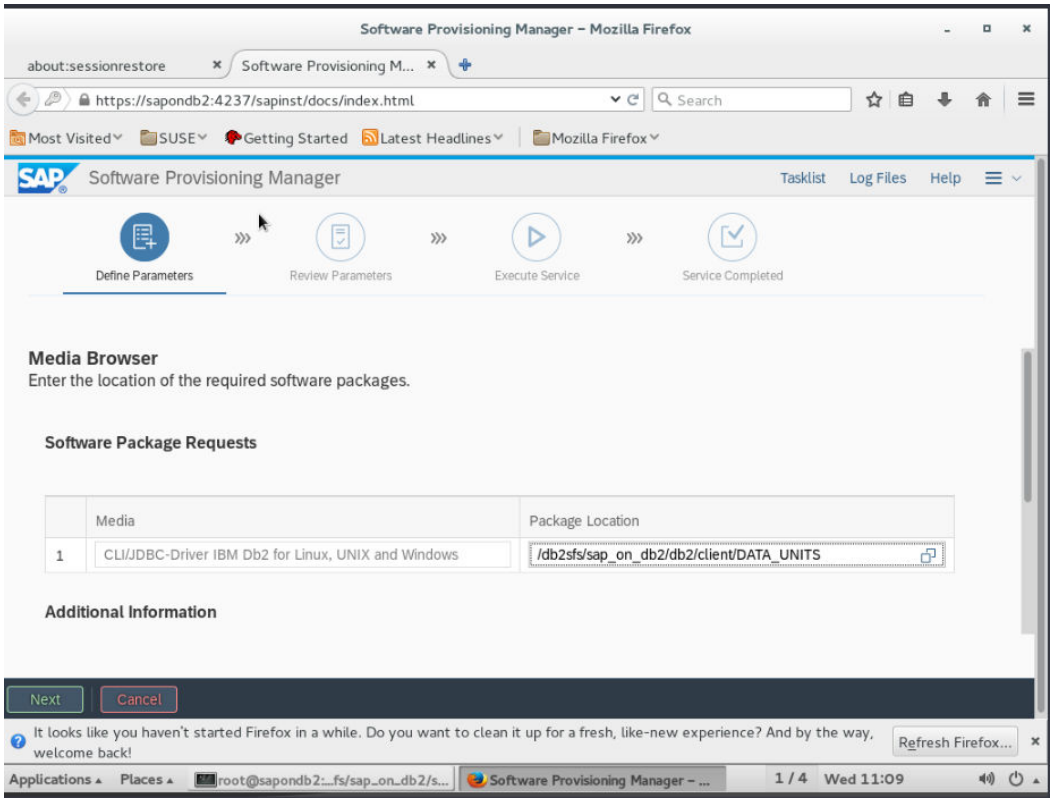


```
spdp                5794/udp     # Simple Peered Discovery Protocol  [Dave_Lindquist]
icmpd               5813/tcp     # ICMPD  [Shane_O_Donnell]
icmpd               5813/udp     # ICMPD  [Shane_O_Donnell]
spt-automation      5814/tcp     # Support Automation  [Joshua_Hawkins]
spt-automation      5814/udp     # Support Automation  [Joshua_Hawkins]
reversion           5842/tcp     # Reversion Backup/Restore  [Cameo_Systems_Inc] [Craig_Nelson]
#                   5842/udp     Reserved
wherehoo            5859/tcp     # WHEREHOO  [Jim_Youll]
wherehoo            5859/udp     # WHEREHOO  [Jim_Youll]
ppsuitemsg          5863/tcp     # PlanetPress Suite Messeng  [Yannick_Fortin]
ppsuitemsg          5863/udp     # PlanetPress Suite Messeng  [Yannick_Fortin]
jute                5883/tcp     # Javascript Unit Test Environment  [Mark_Ethan_Trostler]
rfb                 5900/tcp     vnc-server # Remote Framebuffer  [Tristan_Richardson] [RFC6143]
rfb                 5900/udp     vnc-server # Remote Framebuffer  [Tristan_Richardson] [RFC6143]
cm                  5910/tcp     # Context Management  [Eivan_Cerasi]
cm                  5910/udp     # Context Management  [Eivan_Cerasi]
cm                  5910/sctp    # Context Management  [Justin_Yu]
cpdlc               5911/tcp     # Controller Pilot Data Link Communication  [Eivan_Cerasi]
cpdlc               5911/udp     # Controller Pilot Data Link Communication  [Eivan_Cerasi]
cpdlc               5911/sctp    # Controller Pilot Data Link Communication  [Justin_Yu]
fis                 5912/tcp     # Flight Information Services  [Eivan_Cerasi]
fis                 5912/udp     # Flight Information Services  [Eivan_Cerasi]
fis                 5912/sctp    # Flight Information Services  [Justin_Yu]
ads-c               5913/tcp     # Automatic Dependent Surveillance  [Eivan_Cerasi]
ads-c               5913/udp     # Automatic Dependent Surveillance  [Eivan_Cerasi]
ads-c               5913/sctp    # Automatic Dependent Surveillance  [Justin_Yu]
indy                5963/tcp     # Indy Application Server  [Bjorn_Lantz]
indy                5963/udp     # Indy Application Server  [Bjorn_Lantz]
mppolicy-v5         5968/tcp     # mppolicy-v5  [Yutaka_Ono]
mppolicy-v5         5968/udp     # mppolicy-v5  [Yutaka_Ono]
mppolicy-mgr        5969/tcp     # mppolicy-mgr  [Yutaka_Ono]
mppolicy-mgr        5969/udp     # mppolicy-mgr  [Yutaka_Ono]
couchdb             5984/tcp     # CouchDB  [Noah_Slater]
couchdb             5984/udp     # CouchDB  [Noah_Slater]
wsman               5985/tcp     # WBEM WS-Management HTTP  [Jim_Davis]
wsman               5985/udp     # WBEM WS-Management HTTP  [Jim_Davis]
wsmans              5986/tcp     # WBEM WS-Management HTTP over TLS/SSL  [Jim_Davis]
wsmans              5986/udp     # WBEM WS-Management HTTP over TLS/SSL  [Jim_Davis]
wbem-rmi            5987/tcp     # WBEM RMI  [Jim_Davis]
wbem-rmi            5987/udp     # WBEM RMI  [Jim_Davis]
wbem-http           5988/tcp     # WBEM CIM-XML (HTTP)  [Jim_Davis]
wbem-http           5988/udp     # WBEM CIM-XML (HTTP)  [Jim_Davis]
```

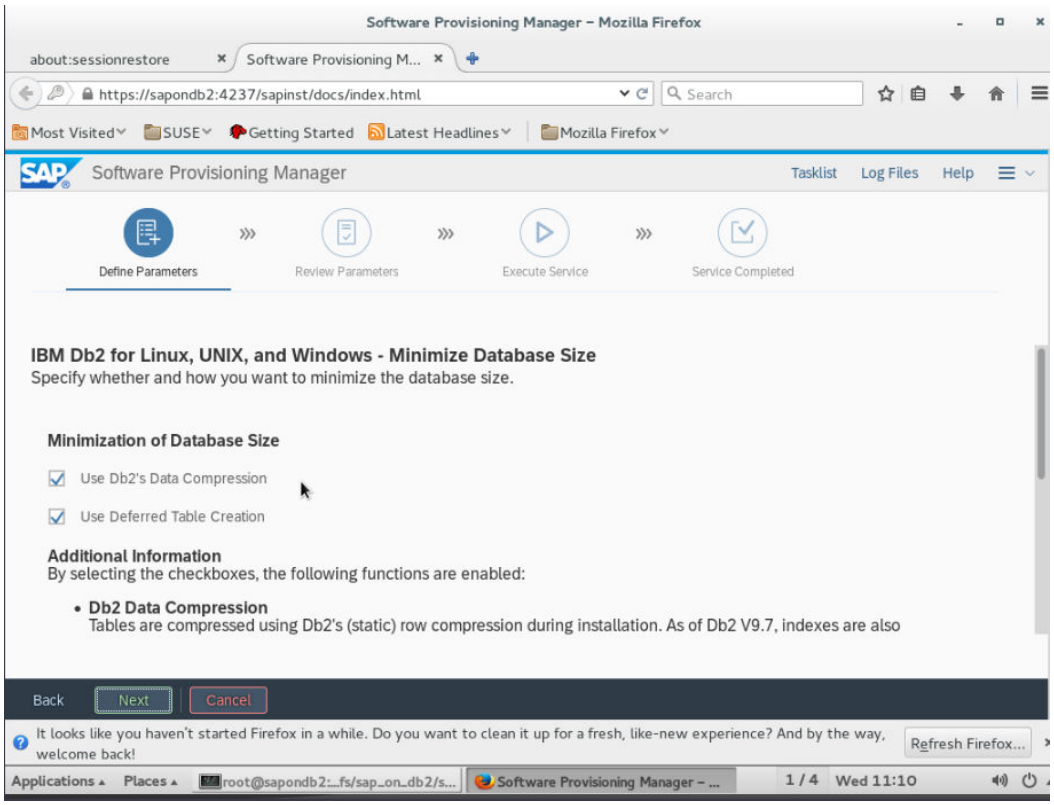
Step 21 Change the default port to an idle one in the service and the security group, and click **Next**.



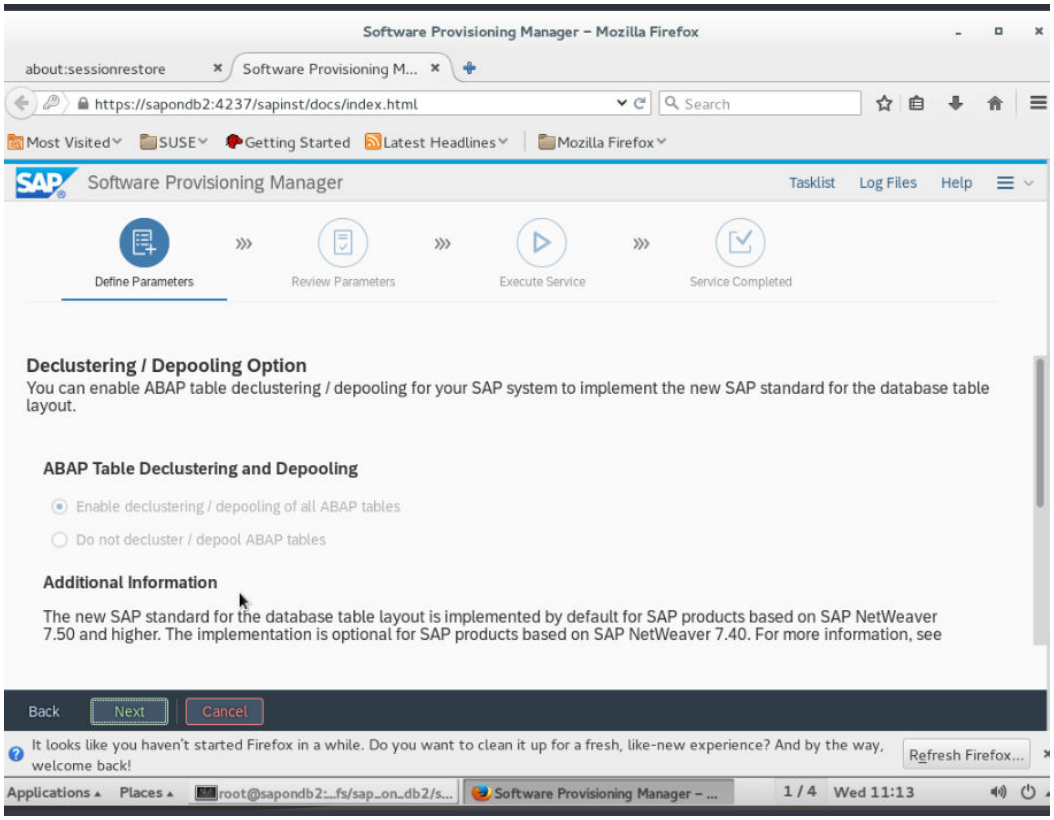
Step 22 Select the path of the **Client** database for the first installation and click **Next**.



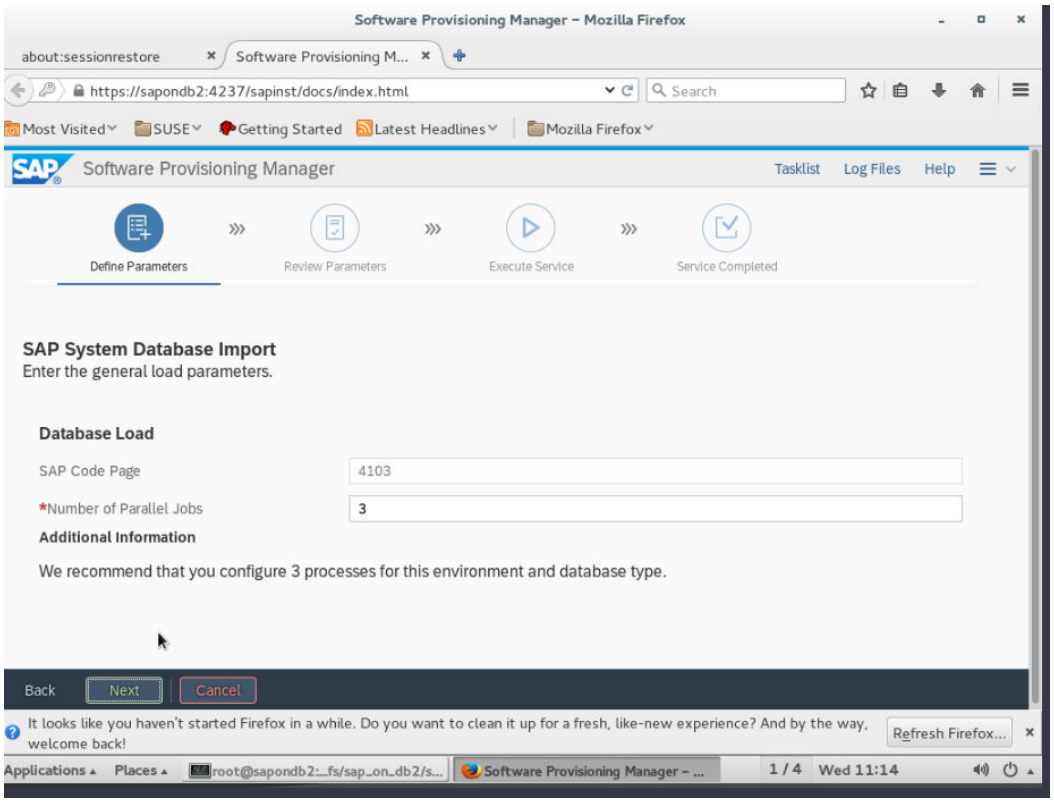
Step 23 Use the default settings and click **Next**.



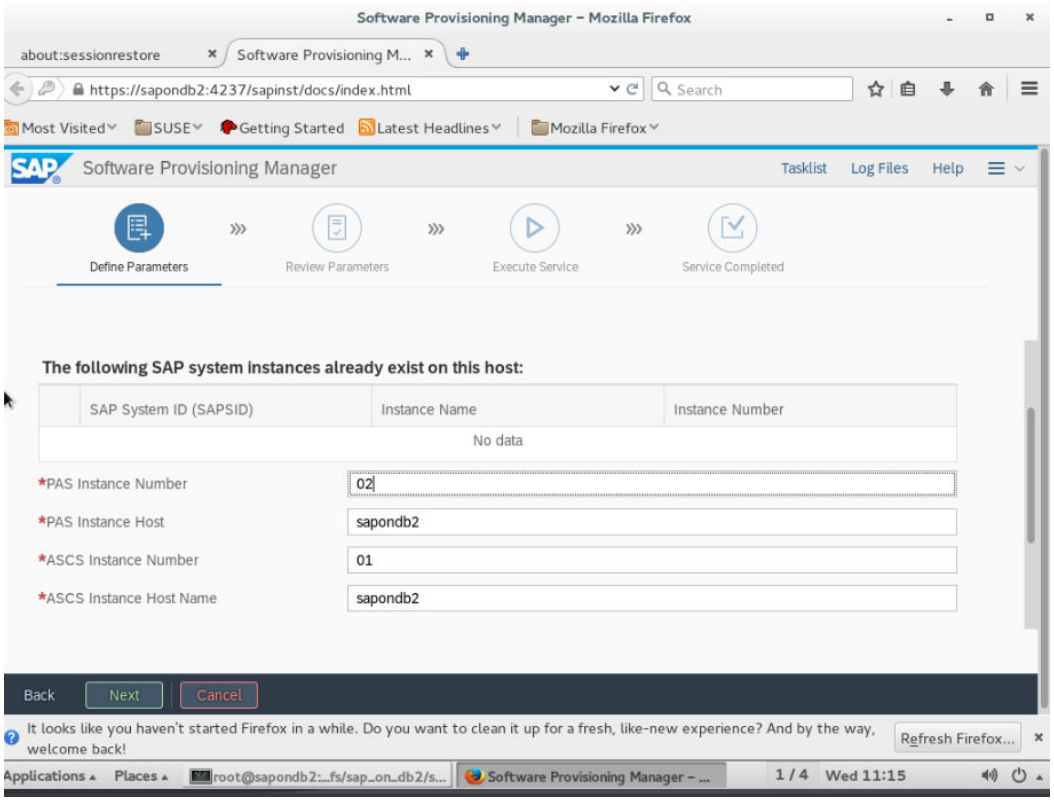
Step 24 Use the default settings and click **Next**.



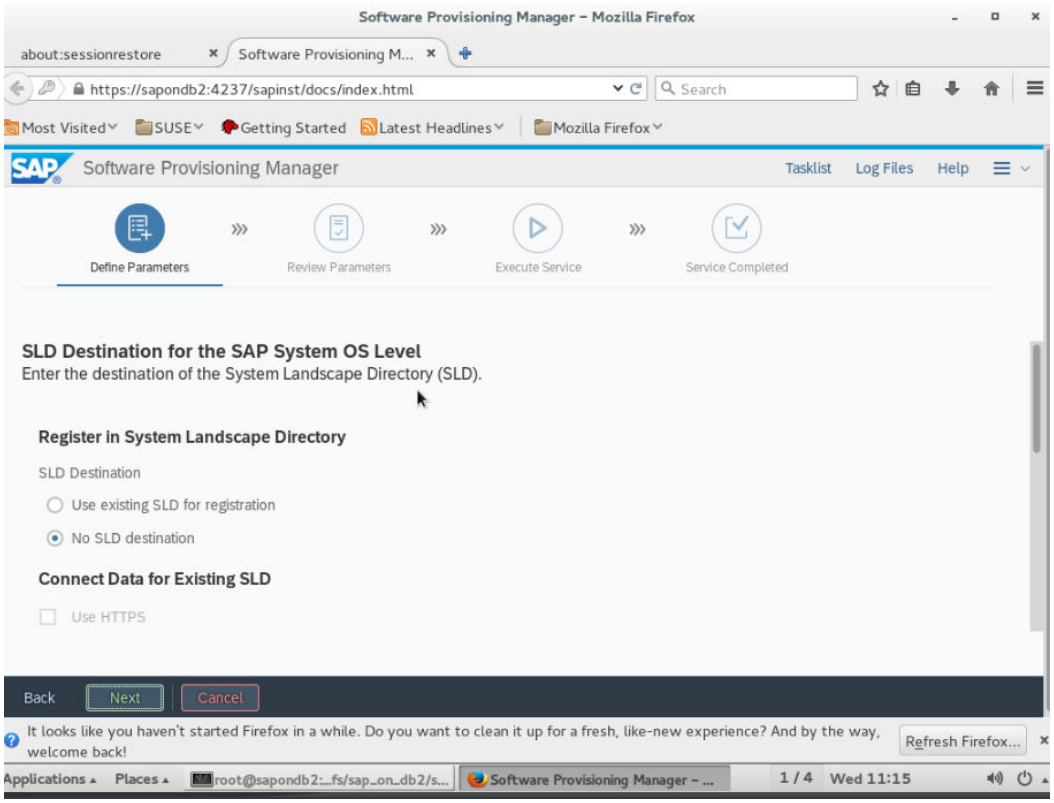
Step 25 Use the default settings and click **Next**.



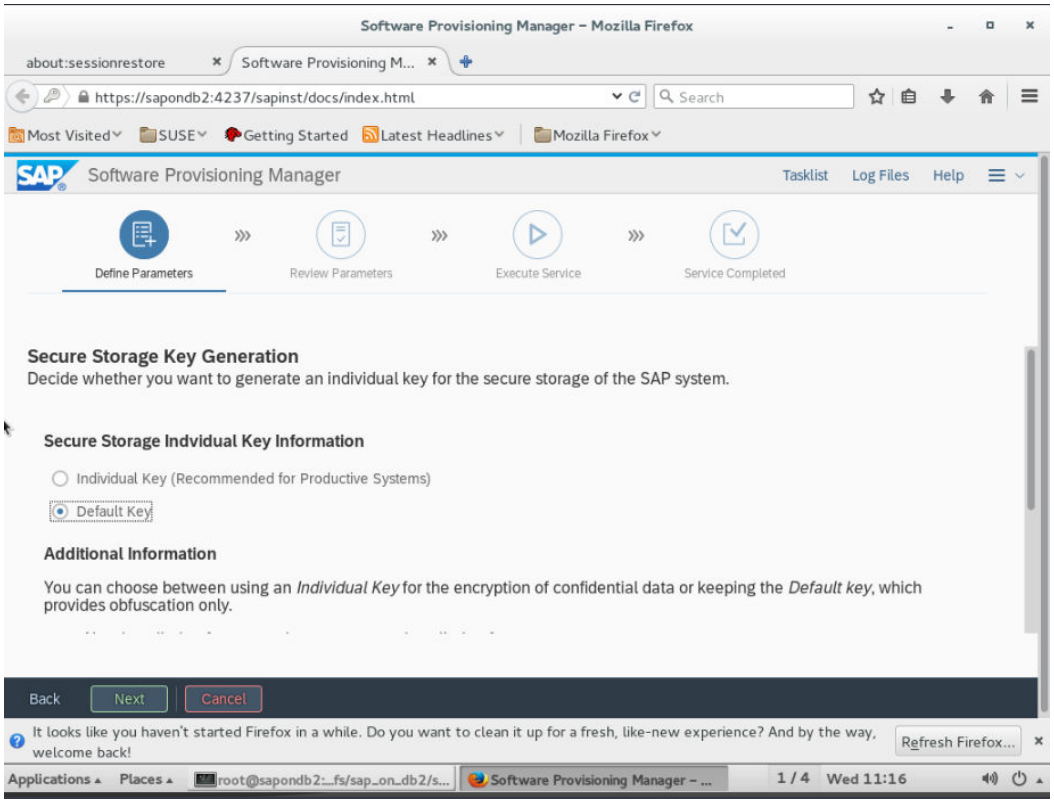
Step 26 Enter the ASCS and PAS instance numbers and click **Next**.



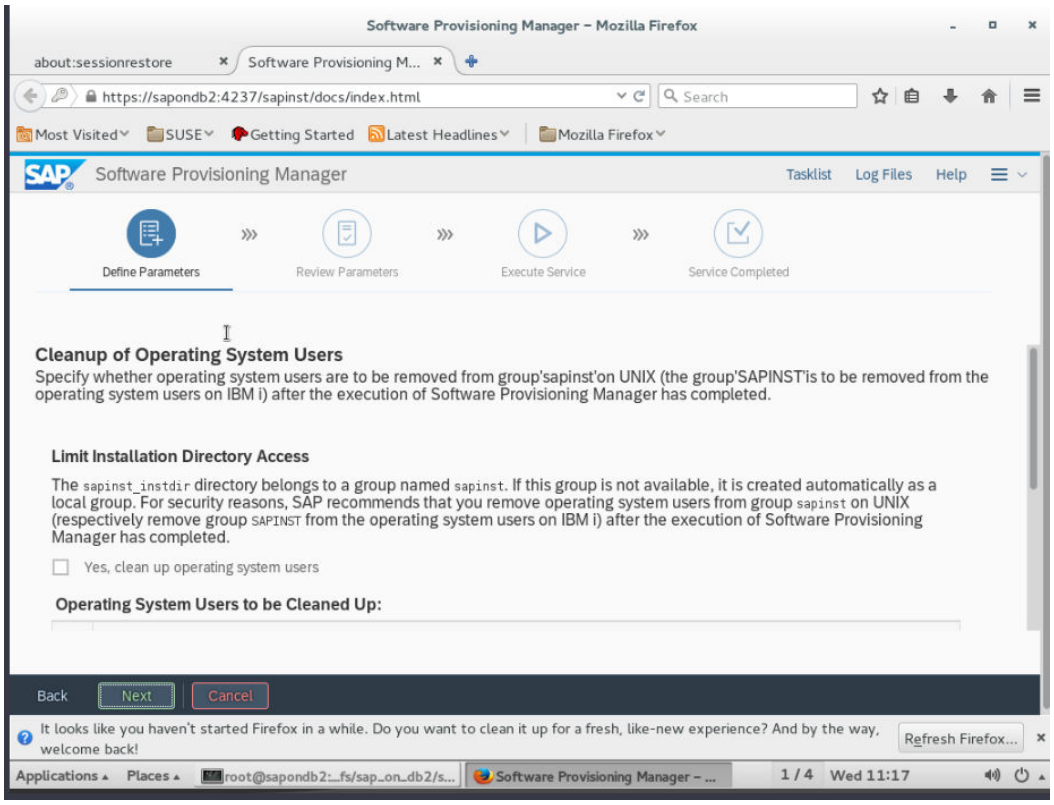
Step 27 Use the default settings and click **Next**.



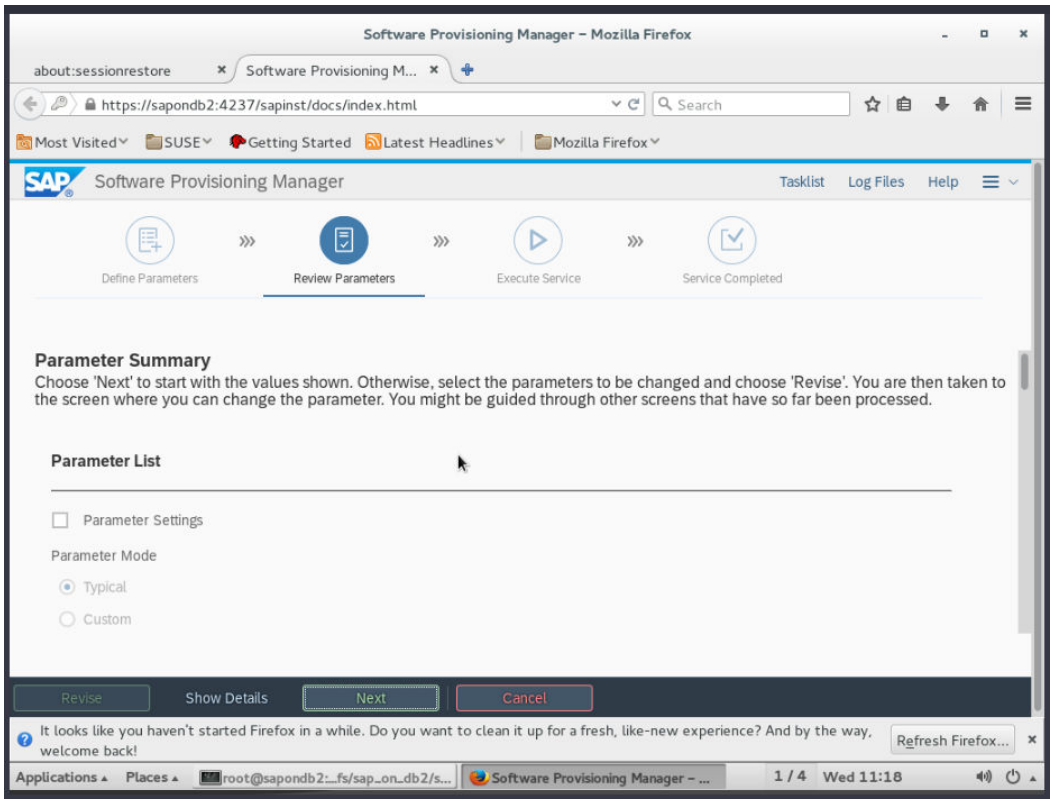
Step 28 Select **Default Key** and click **Next**.



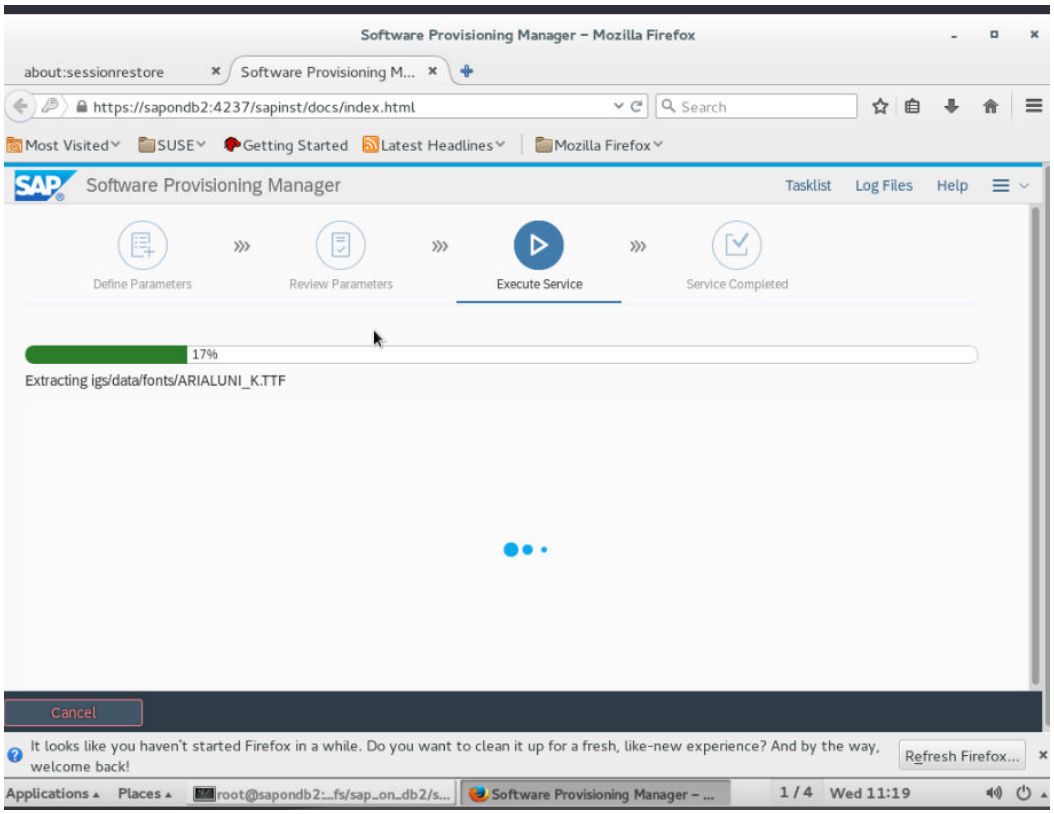
Step 29 Use the default settings and click **Next**.



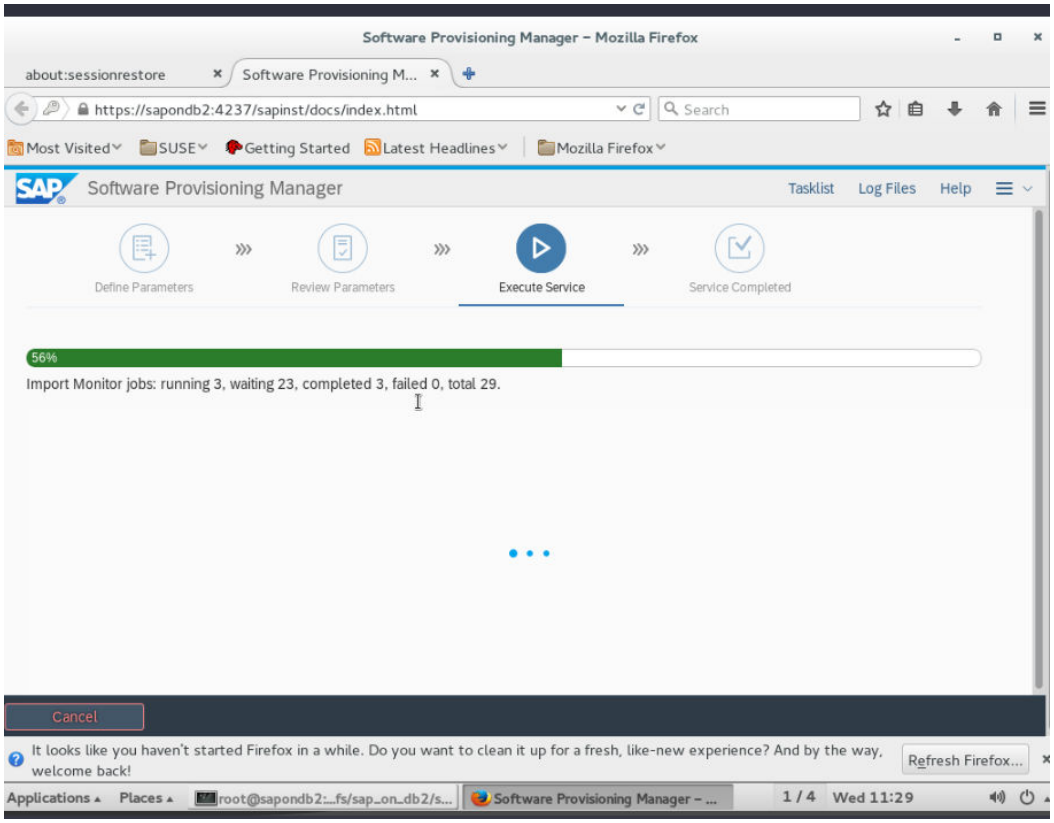
Step 30 Confirm the parameters and click **Next**.



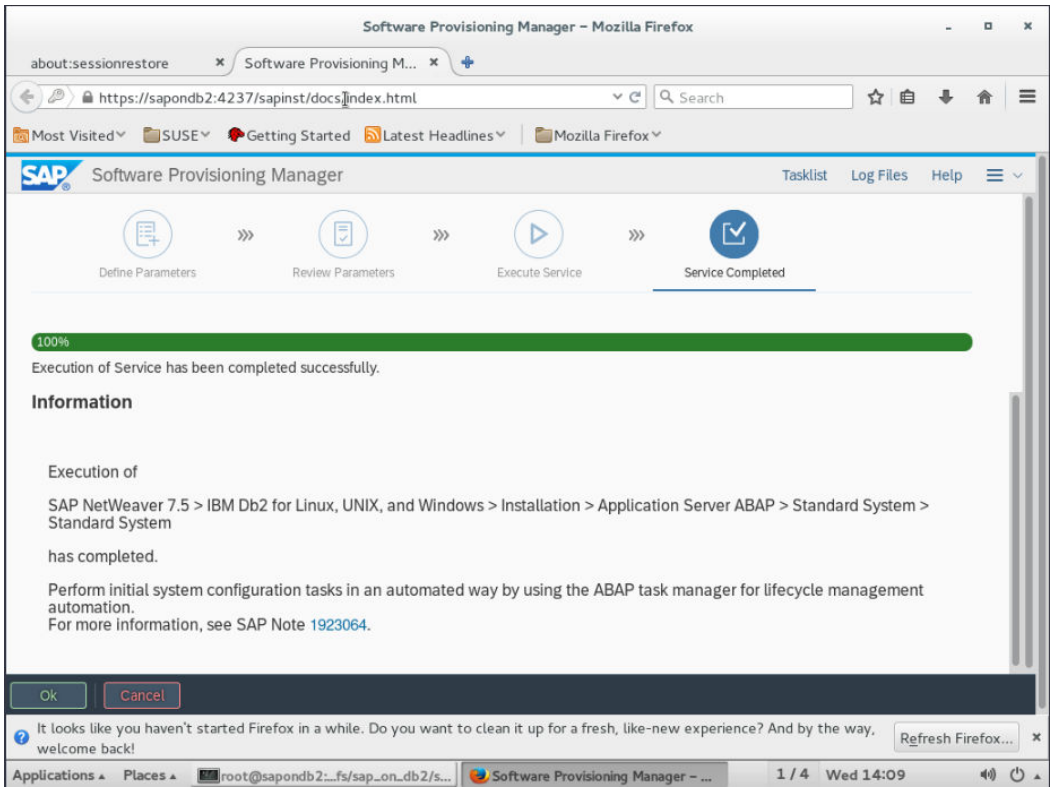
Step 31 Install SAP.

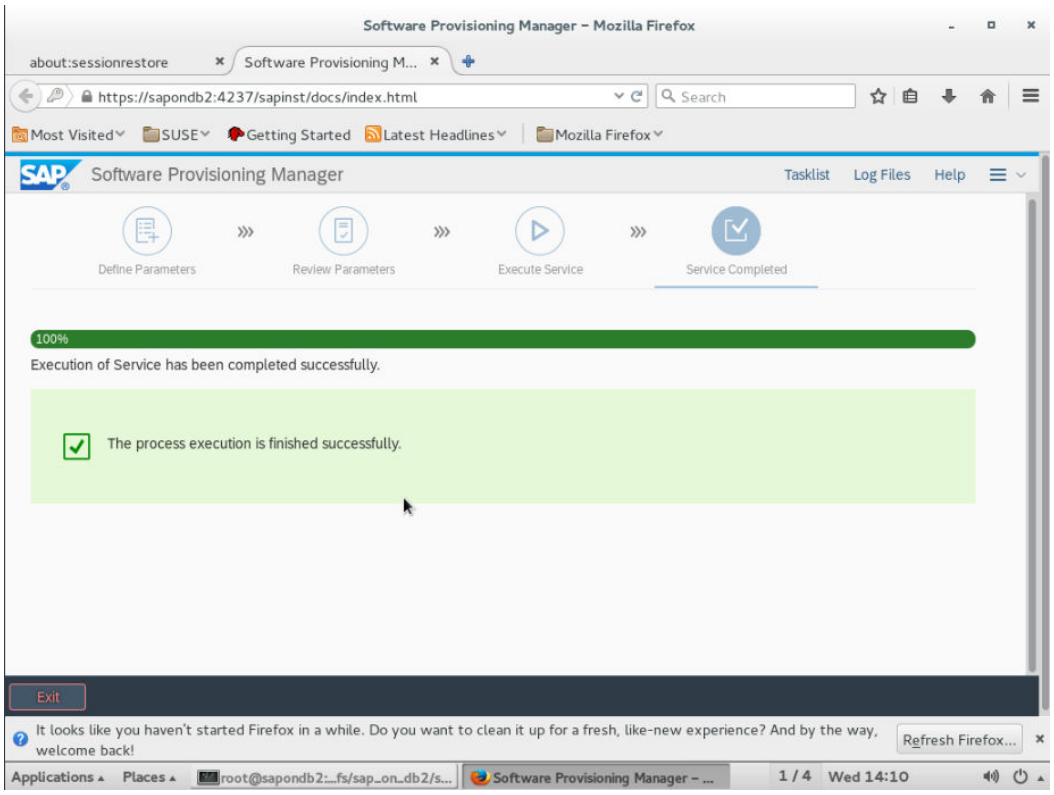


Step 32 Wait patiently. The installation takes about one hour.



Step 33 Click **OK** after installation.



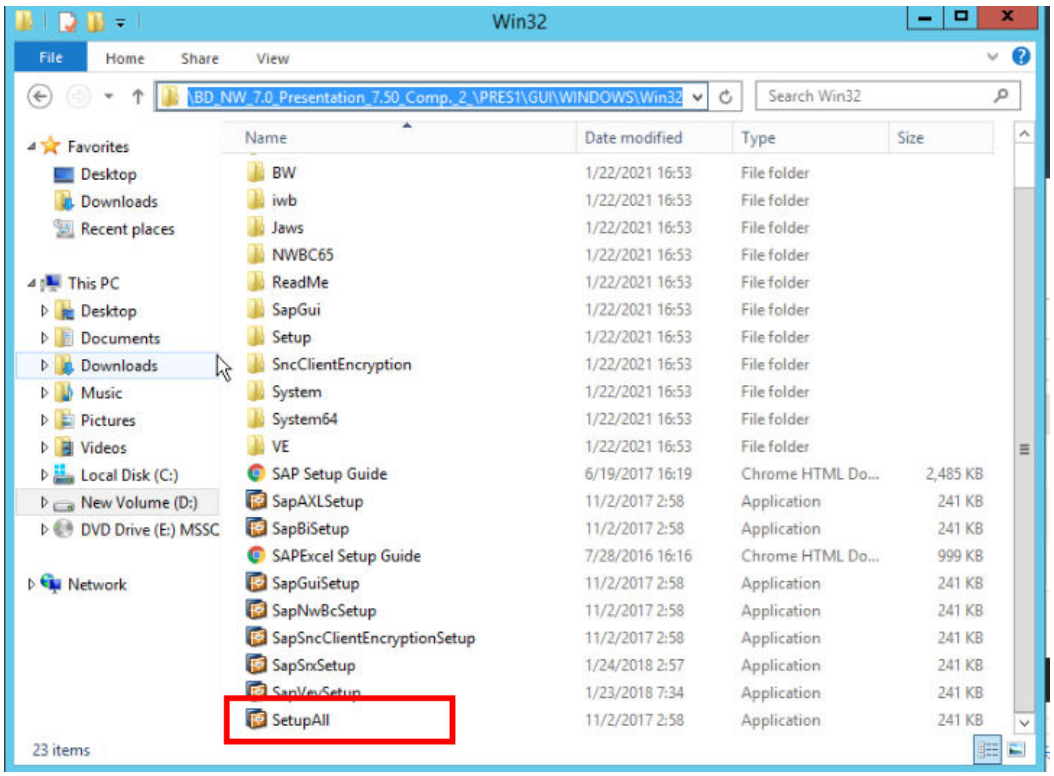


----End

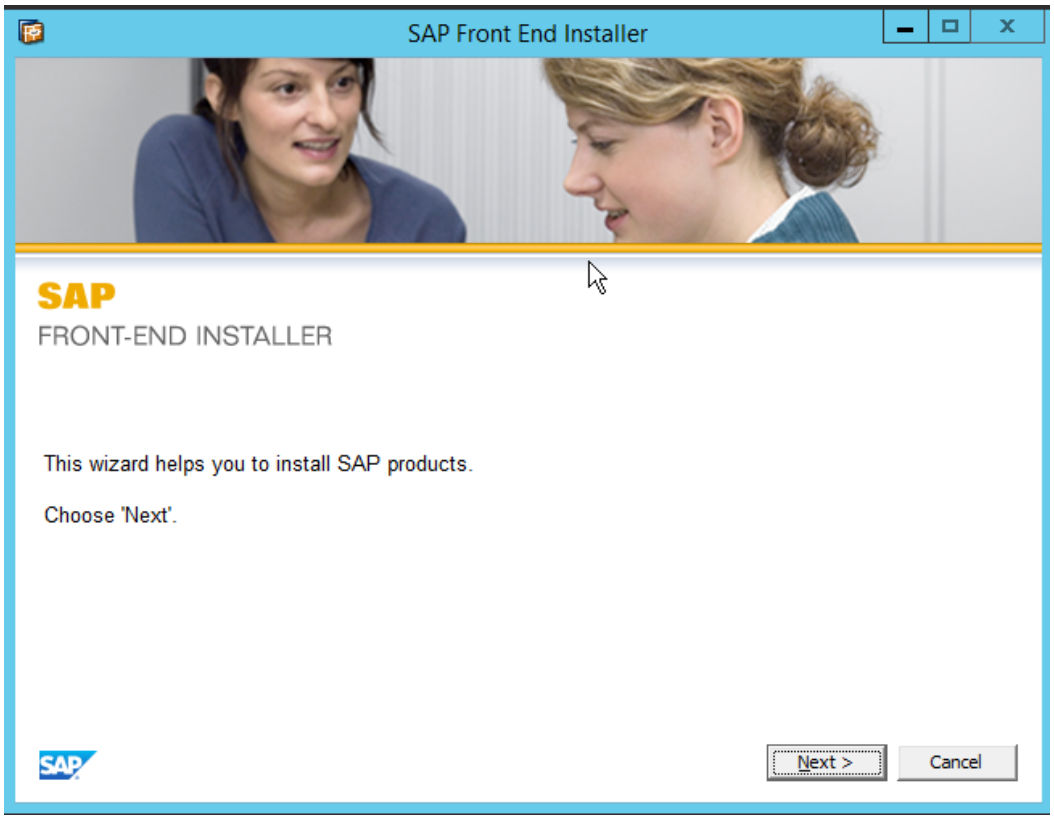
2.5.2 Installing SAP GUI

Install SAP GUI on the ECS running Windows.

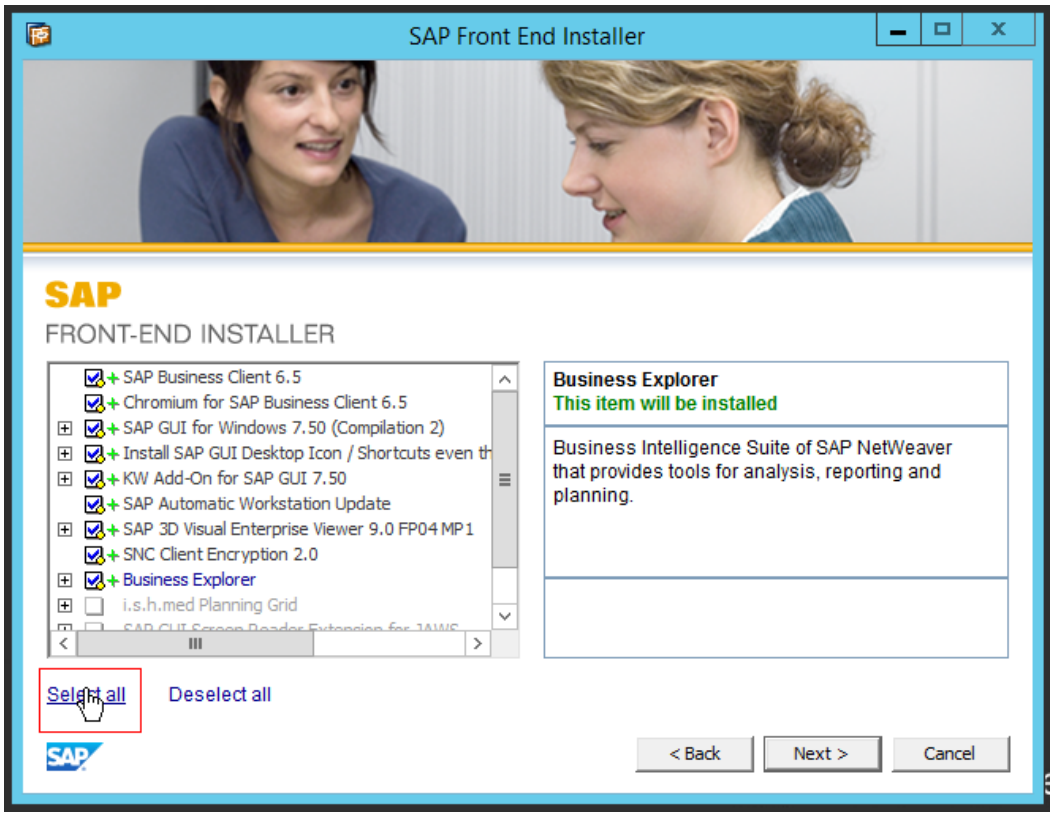
Step 1 Go to the SAP GUI installation directory. Run the installation program.



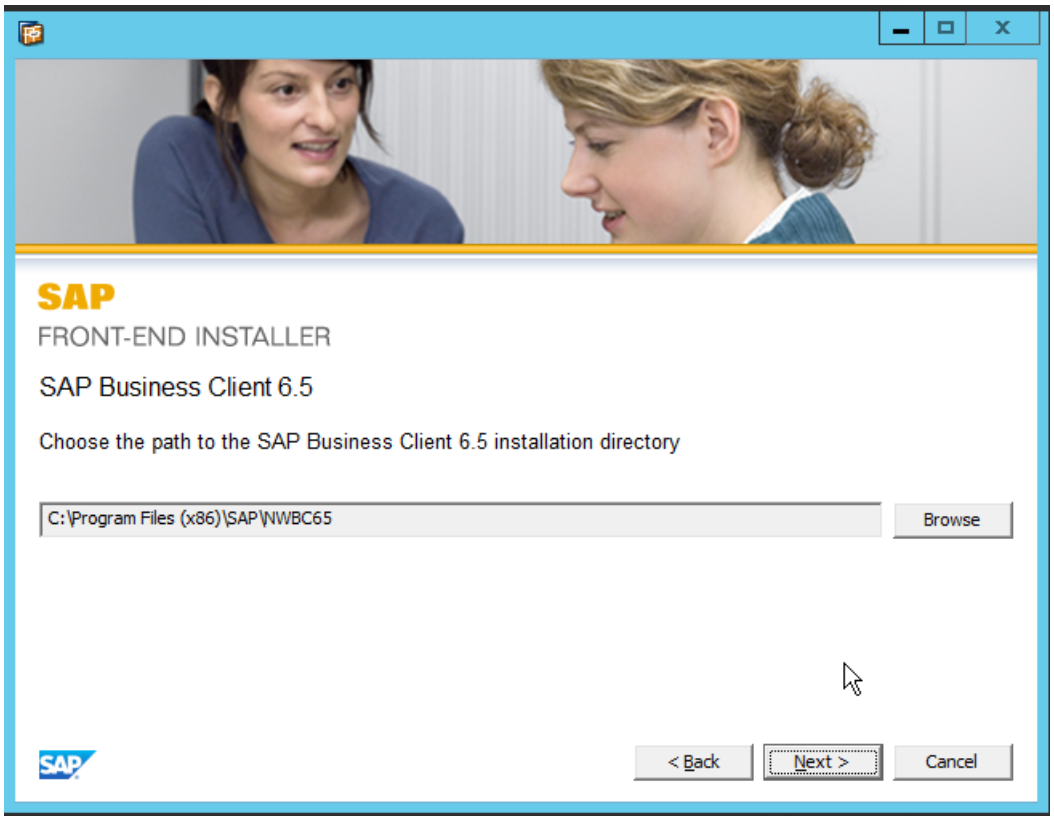
Step 2 Click **Next**.



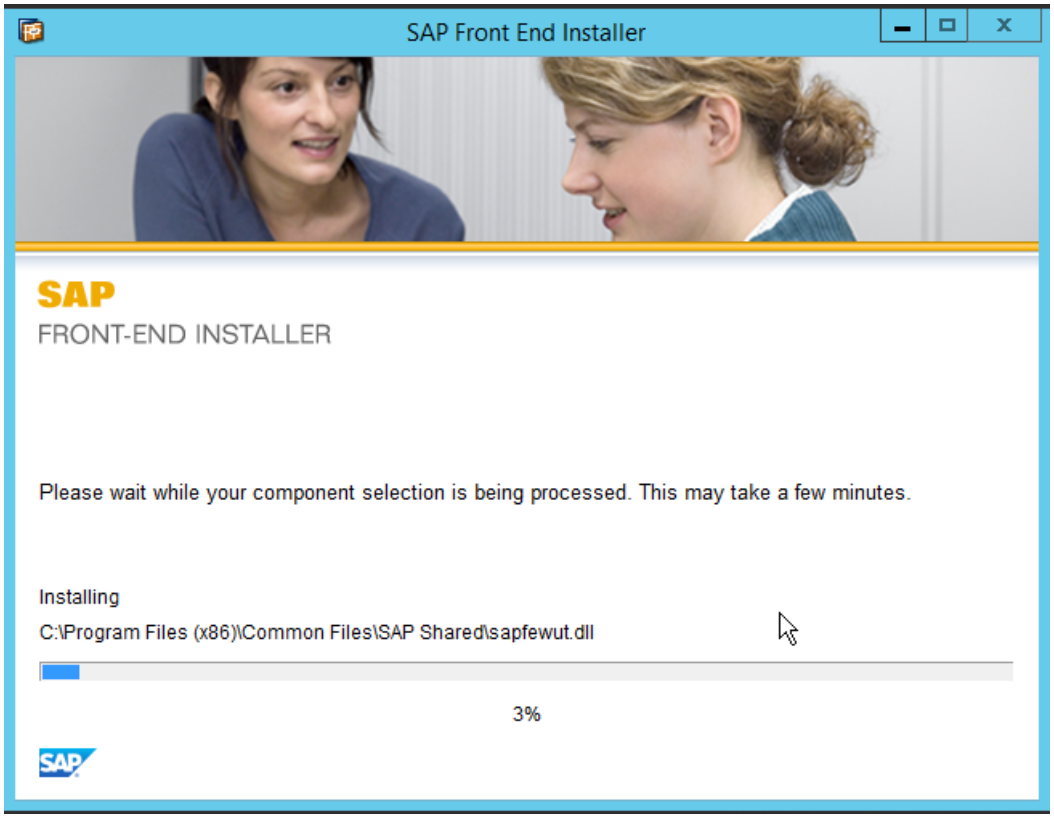
Step 3 Select the components to be installed. Here, click **Select all** and then **Next**.



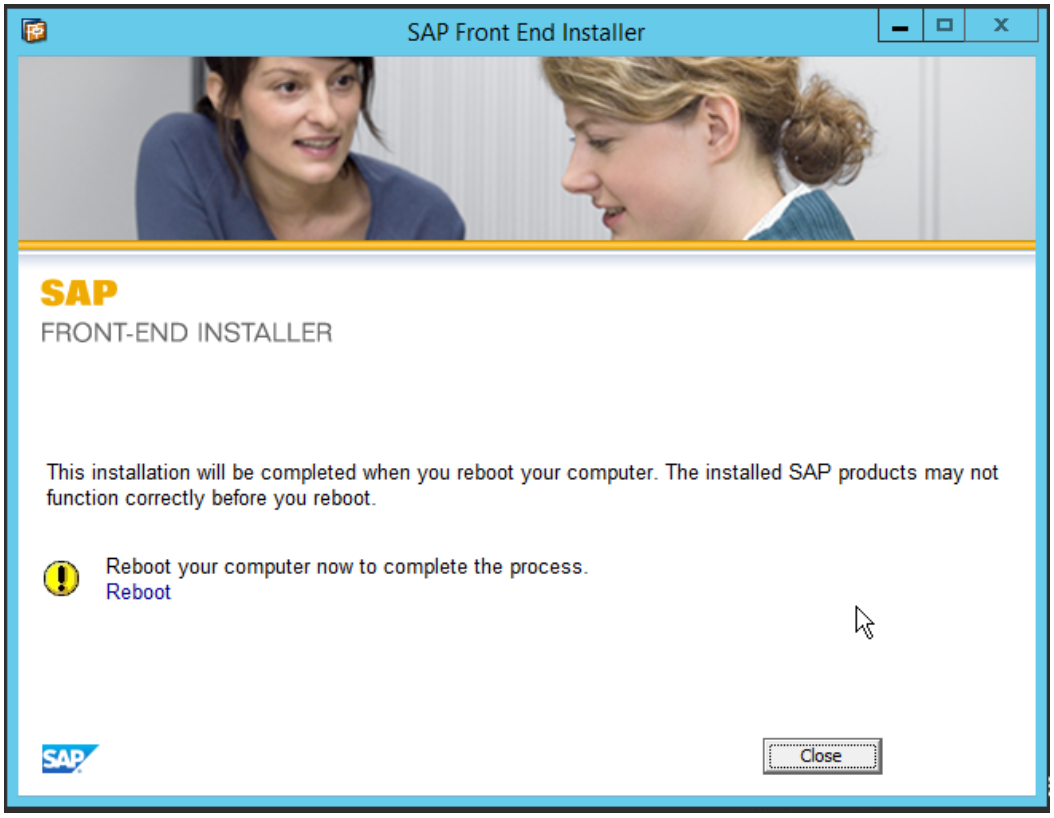
Step 4 Select the installation location for each component. Retain the default settings and click **Next** until the installation location is set for all components.



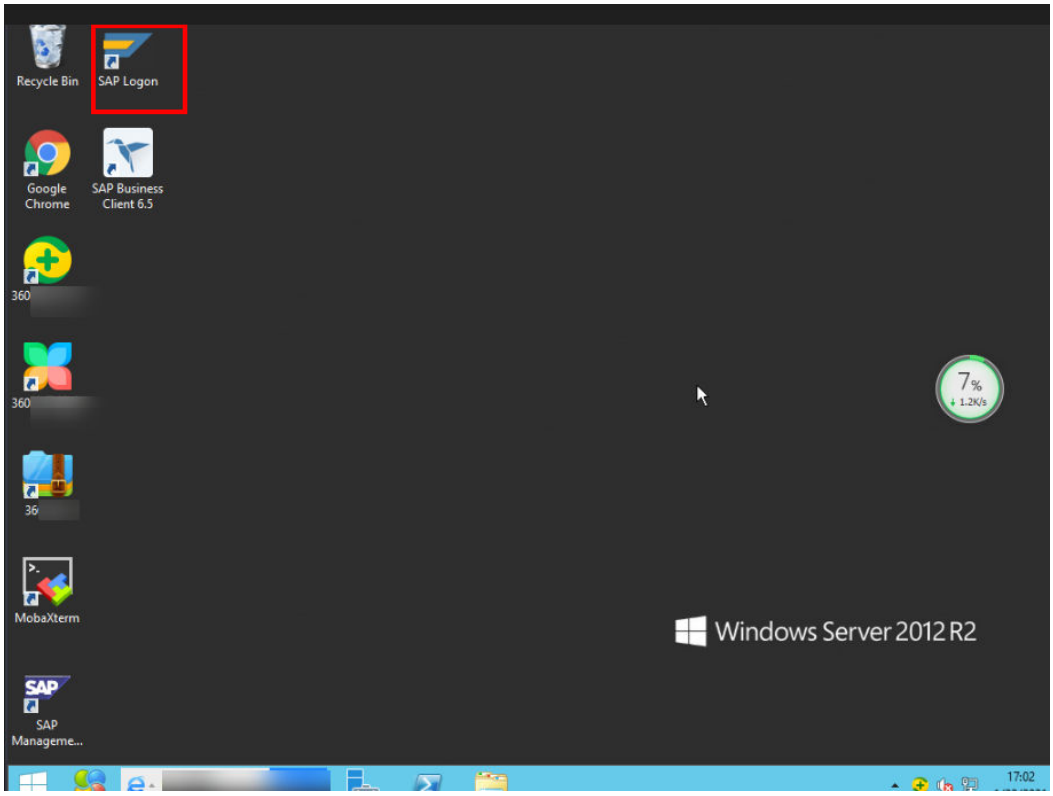
Step 5 Start the installation.



Step 6 After the installation is complete, restart the computer as required. You can restart it during off-peak hour.



Step 7 Restart the computer.



----End

2.6 Verifying the Installation

2.6.1 Checking Instance Status

Procedure

Step 1 Log in to the ECS as the **root** user and switch to the **sidadm** user.

su - s01adm

```
sapondb2:/db2sfs/sap_on_db2/swpm # vi /etc/passwd
sapondb2:/db2sfs/sap_on_db2/swpm # su - s01adm
```

Step 2 Run the following commands to check the instance status:

sapcontrol -nr 01 -function GetProcessList

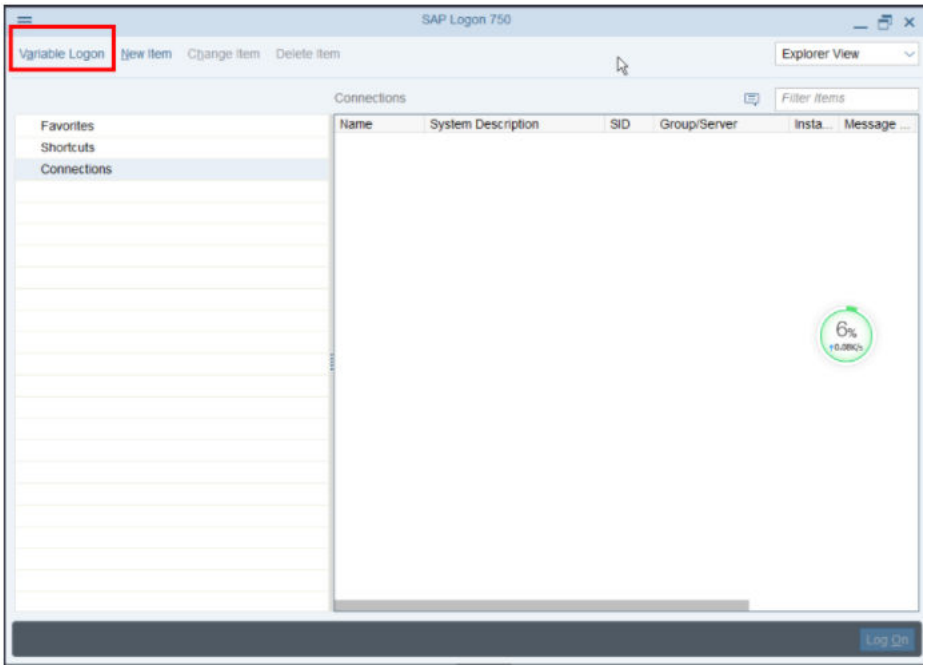
sapcontrol -nr 02 -function GetProcessList


```
sapondb2:s01adm 2> sapcontrol -nr 01 -function GetProcessList
uncti
03.03.2021 14:12:34
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
msg_server, MessageServer, GREEN, Running, 2021 03 03 12:02:44, 2:09:50, 5
enserver, EnqueueServer, GREEN, Running, 2021 03 03 12:02:44, 2:09:50, 570
sapondb2:s01adm 3> sapcontrol -nr 02 -function GetProcessList

03.03.2021 14:12:37
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
disp+work, Dispatcher, GREEN, Running, 2021 03 03 12:14:20, 1:58:17, 1441
igswd_mt, IGS Watchdog, GREEN, Running, 2021 03 03 12:14:20, 1:58:17, 144
gwrd, Gateway, GREEN, Running, 2021 03 03 12:14:23, 1:58:14, 14435
icman, ICM, GREEN, Running, 2021 03 03 12:14:23, 1:58:14, 14436
sapondb2:s01adm 4>
sapondb2:s01adm 4>
```

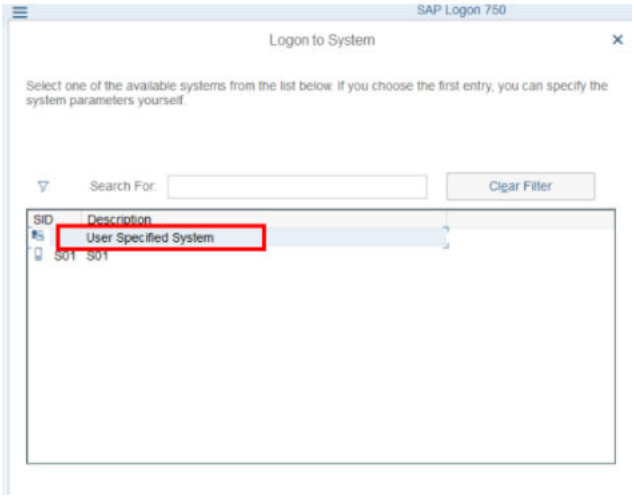
----End

2.6.2 Using SAP GUI to Connect to the SAP Application

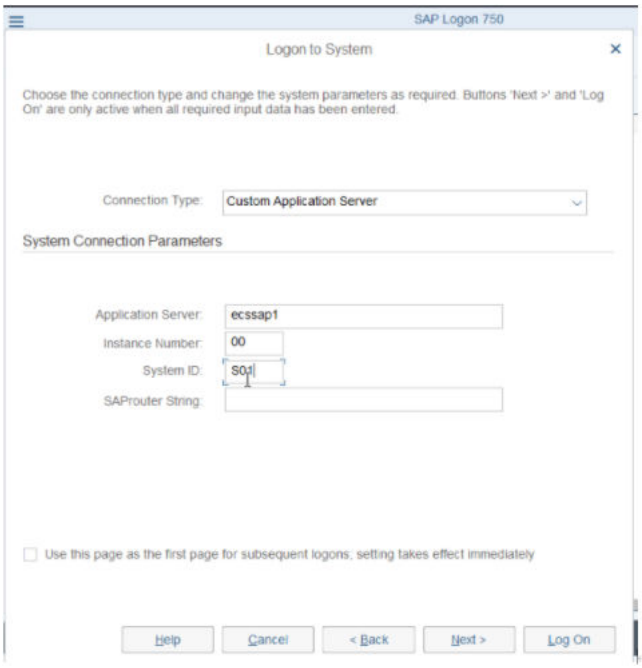
Step 1 Log in to the ECS running Windows, open the SAP GUI, and click **Variable Login**.



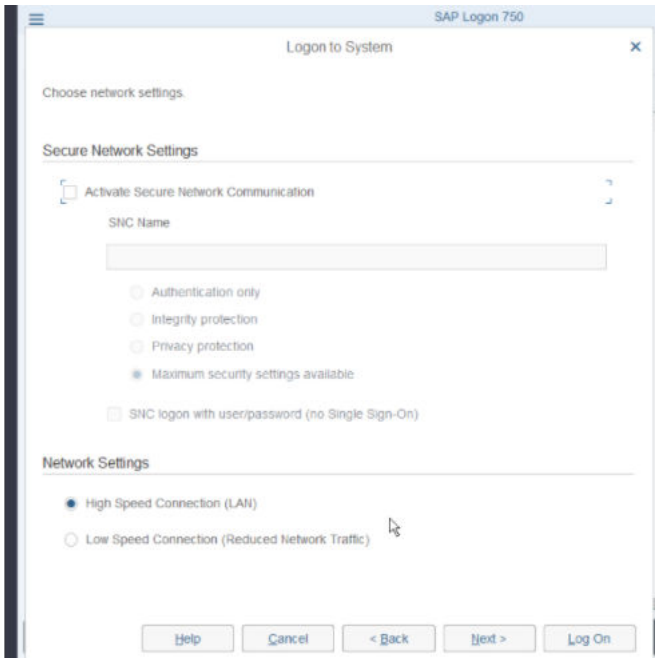
Step 2 Double-click the **User Specified System**.



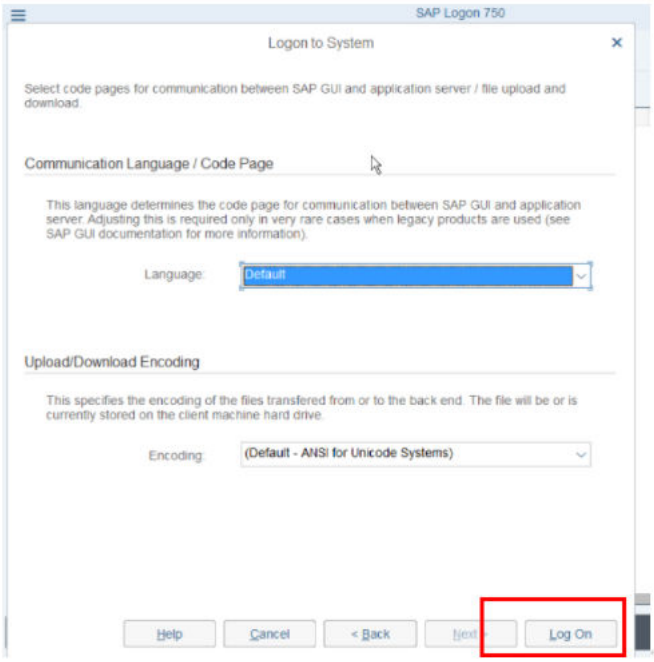
Step 3 Enter the IP address of SAP on DB2, instance ID of PAS, and SID, and click **Next**.



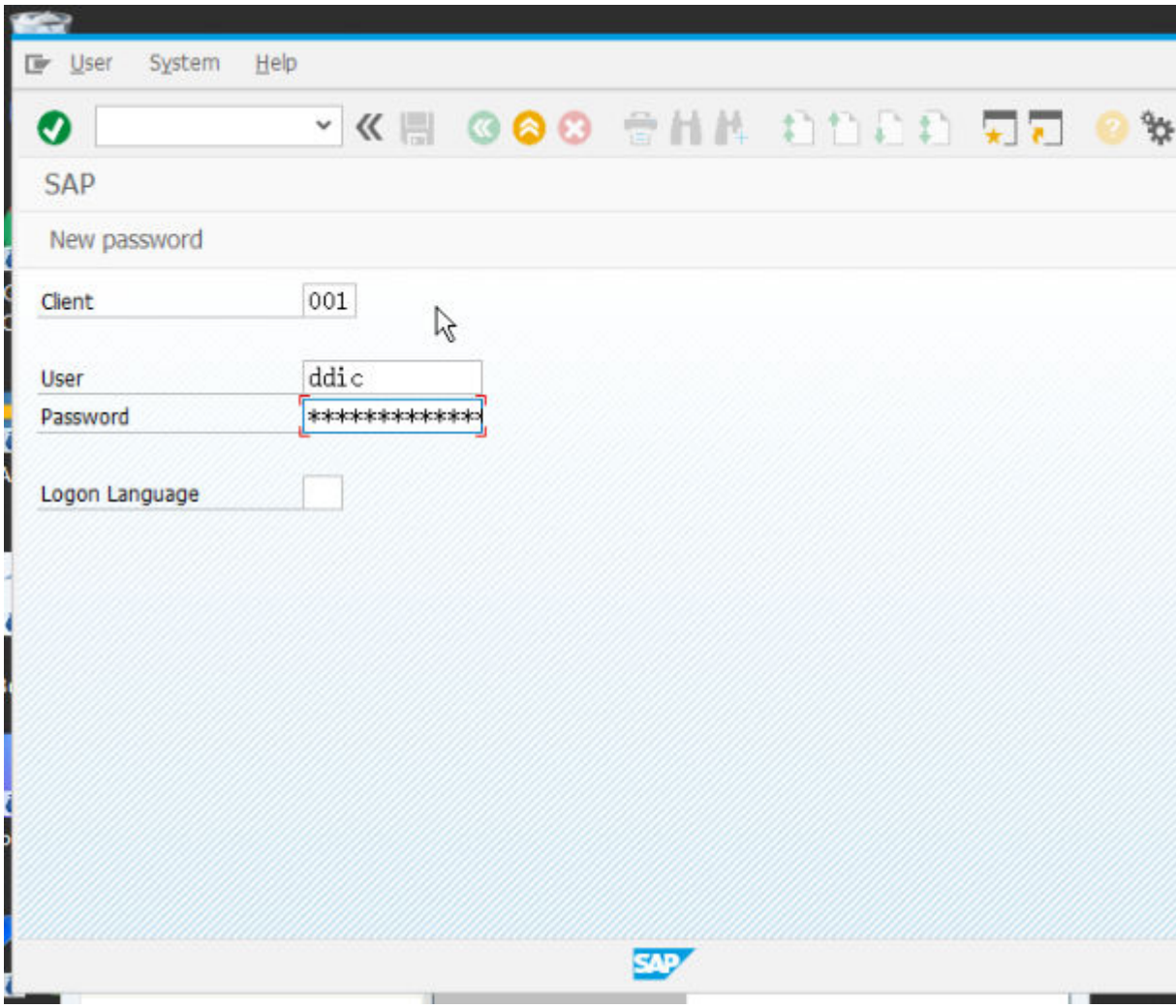
Step 4 Retain the default settings and click **Next**.



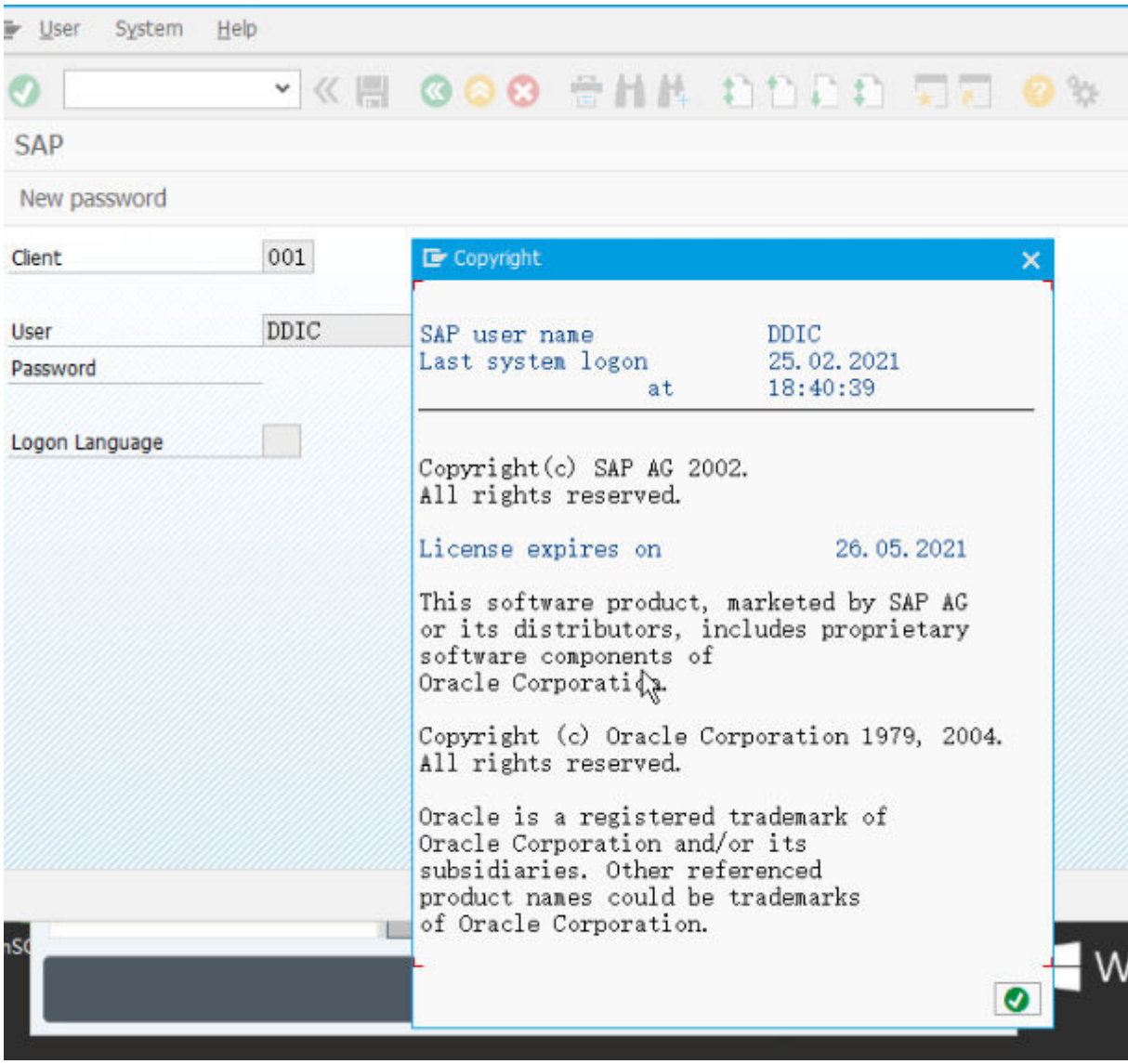
Step 5 Click **Log On**.



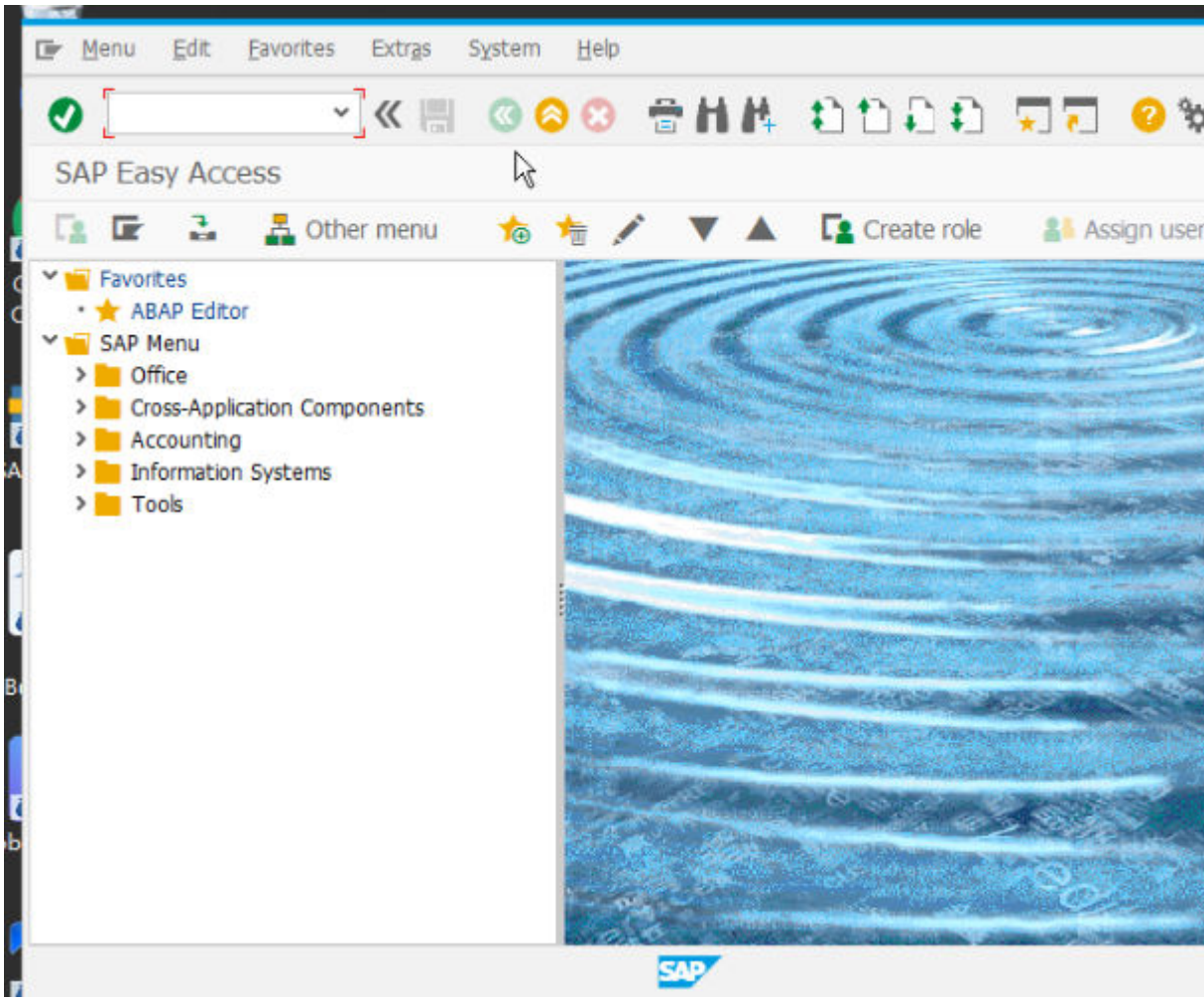
Step 6 Enter the username **ddic** and password, and press **Enter**.

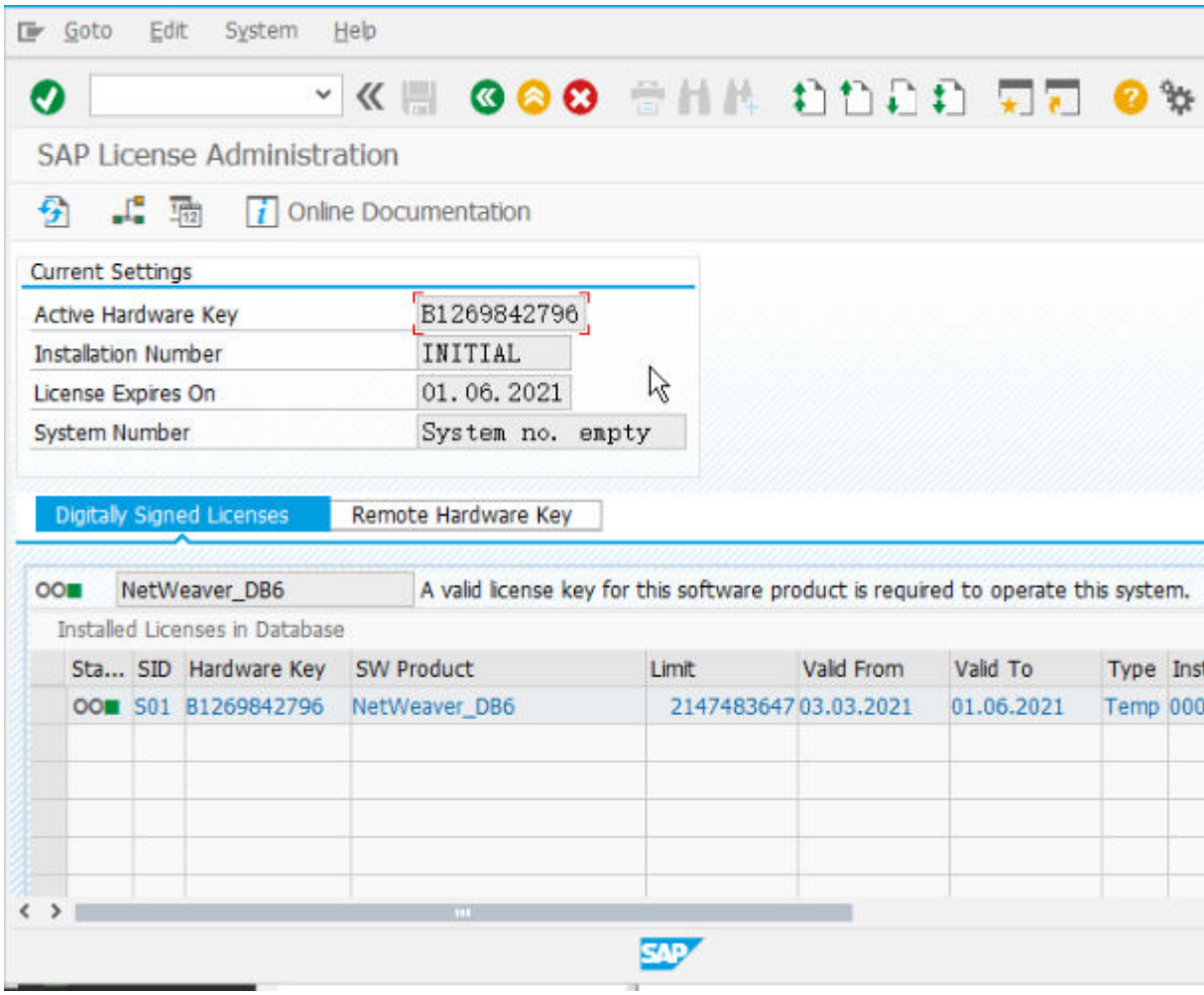


Step 7 Click **Yes**.



Step 8 Enter **slicense** in the search box and press **Enter** to view the hardware key.





----End

2.7 Change History

Table 2-8

Change History	Date	Prepared By
Initial version	2021-05-20	Fu Chuandong/00469497

3 Huawei Cloud SAP on SQL Server Installation Best Practice

3.1 About This Document

This document provides guidance for preparing resources (such as cloud servers and network resources) on the public cloud platform and installing SAP on SQL Server. SAP is authorized in Bring Your Own License (BYOL) mode. You need to log in at **SAP Support Portal** to purchase licenses.

This document cannot replace the standard SAP document. If you have any trouble in installing and using SAP due to its own problems, contact the SAP technical support.

This document is written based on the Windows OS. The deployment methods mentioned in the document are only for reference. Install SAP on SQL Server by referring to the standard SAP installation manual or based on site requirements.

For details about the official SAP installation guide and related notes, see the following documents:

- **SAP Installation Guides**
- **SAP Notes**
- **SAP Library**

3.2 Pre-installation Preparations

Logging in to Huawei Cloud

Before deploying the SAP system on Huawei Cloud, register a HUAWEI ID and enable Huawei Cloud services. Through this account, you can use Huawei Cloud services and pay only for the services you use.

For details, see **Registering a HUAWEI ID and Enabling Huawei Cloud Services**.

You can log in to Huawei Cloud using any of the methods described in **Logging In to Huawei Cloud**.

SAP License

SAP is authorized in Bring Your Own License (BYOL) mode. In this mode, you need to log in to the SAP Support Portal and apply for a license.

3.3 Resource Planning

3.3.1 Network Planning

The network information needs to be planned based on application scenarios and SAP planning. The following table lists the network segments and IP addresses required for installing standard SAP on SQL Server. You can configure it based on site requirements.

Parameter	Description	Example
IP address of the server/client plane	Specifies the IP address of the primary NIC plane. The ABAP SAP Central Services (ASCS) nodes communicate with the SAP GUI and SAP databases using this IP address.	ASCS/Primary Application Server (PAS) node: 10.10.0.2 SQL node: 10.10.0.2 Additional Application Server (AAS) node: 10.10.0.3

3.3.2 Security Group Planning

SAP Security Group Planning

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

You can configure the security group by referring to **Table 3-1**.

NOTE

- Plan the network segments and IP addresses based on the site requirements. The following security group rules are for reference only. You can configure your own security group rules as needed.
- In the following table, *##* stands for the SAP instance number, which must be consistent with the instance number specified when the SAP software is installed.

Table 3-1 SAP node security group rules

Source/ Destination	Protocol	Port Range	Description
Inbound			
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.
10.10.0.0/24	TCP	32##	Allows SAP GUI to access SAP.
10.10.0.0/24	TCP	36##	Message port with profile parameter rdisp/msserv
10.10.0.0/24	TCP	5##13 ~ 5##14	Allows ASCS to access SAP application server.
10.10.0.0/24	TCP	33##, 38##, 48##	Port used by CPIC and RFC
10.10.0.0/24	TCP	22	Allows SAP to be accessed using SSH.
10.10.0.0/24	TCP	123	Allows other servers to synchronize time with SAP.
Outbound			
All	All	All	Security group rule created by the system by default Allows SAP to access all peers.

3.3.3 File System Planning

When the SAP system is installed, a home directory is automatically created. The following describes the directory planning for the SAP system.

Table 3-2

Directory Type	Directory Structure	Description
SAP System	\usr\sap \usr\sap\trans	SAP kernel and related files SAP transport directory
Database Management System (DBMS)	\Program Files\Microsoft SQL Server	SQL Server program files including the master, msdb and model database files.
SAP Database	\<SAPSID>DATA0 \<SAPSID>DATA1 \<SAPSID>DATA2 \<SAPSID>DATA3 ... \<SAPSID>DATA<N>	Database data files <0-N>
SAP Database Transaction Log	\<SAPSID>log<N>	Database transaction log files
Tempdb	\Tempdb	Tempdb data files

3.3.4 Software and Hardware Planning

Hardware Planning

The following table lists the requirements for the SAP hardware disk space. For details, see **SAP official document**.

Table 3-3

Item	Requirement
Minimum Disk Space	• Database software:4 GB • ABAP central services instance (ASCS) (not including paging file): 5 GB (x64) 8 GB (IA64) • Database instance (not including paging file):18 GB • Primary application server instance (not including paging file): 5 GB (x64) 8 GB (IA64) • Additional application server instance (not including paging file): 2.5 GB (x64) 5 GB (IA64) • SAP Host Agent:256 MB • Temporary disk space for every required installation medium that you have to copy to a local hard disk:Up to 6 GB
Minimum Memory	• All instances, except SAP Host Agent:4 GB • SAP Host Agent:0.5 GB
CPU	> 2 cores

Software Planning

The following table lists the requirements of the SAP application and database for OS. For details, see **SAP official document**.

Table 3-4

Item	Requirement
Windows OS	64Bit It must be later than Windows Server 2008 (R2).

Item	Requirement
Database	ABAP central services instance (ASCS), primary application server instance, or additional application server instance: SQL 2014 and higher ODBC Driver for SQL Server. SQL Server 2012 or SQL Server 2008 (R2) Native Access Client (SNAC) software Database instance:○ SQL 2008 (R2) and higher: Enterprise Edition: Server Software○ Latest service pack and hotfix, if available. SQL_Latin1_General_CP850_BIN2
SAP Kernel Version	SAP kernel 7.40 and higher: IP Multicast Configu-ration Make sure that you have applied the operating system patches required for IP Multicast Config-uration.
Region	English (United States) must be set by default. For more information about localized Windows versions, see SAP Note 362379. You can install additional languages but the default setting for new users must always be English (United States).
Browser	Use the latest version of the following browsers: ●Microsoft Internet Explorer 11 or higher ●Microsoft Edge ●Mozilla Firefox ●Google Chrome

3.3.5 ECS Planning

- SAP ECS specifications

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

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

SAP-certified ECSs must be used for installing the SAP application. For details, see *SAP Note 2582296 - SAP Applications on Huawei Cloud Supported Products and ECS VM types*.

- Operating system

  The following table lists the OS supported by SAP ECSs.

ECS Name	Flavor	Disk	Image	Remarks
ecssap1	m6.2xlarge.8	System disk: 100 GB, ultra-high I/O Data disk: 250 GB, ultra-high I/O	Windows Server 2012 R2 Standard 64-bit English (40 GB)	Used for installing SAP ERP and SQL Server
ecssap2	m6.xlarge.8			Used for installing AAS and SAP GUI

- SAP node planning

Host Name	Server/Client IP Address	Type	Instance Number	SID
ecssap1	10.10.0.2	ASCS Instance	01	S01
		PAS Instance	02	
		DB Instance	None	
ecssap2	10.10.0.3	AAS Instance	03	

3.4 Preparing for SAP Installation

3.4.1 Creating a VPC

A VPC is logically isolated, configurable, and manageable virtual network for cloud servers, cloud containers, and cloud databases. It improves resource security and simplifies network deployment on the cloud. With a VPC, you can configure and manage the networks in the VPC, and make changes to these networks as needed, quickly and securely. For more information about VPC, see **VPC Overview**.

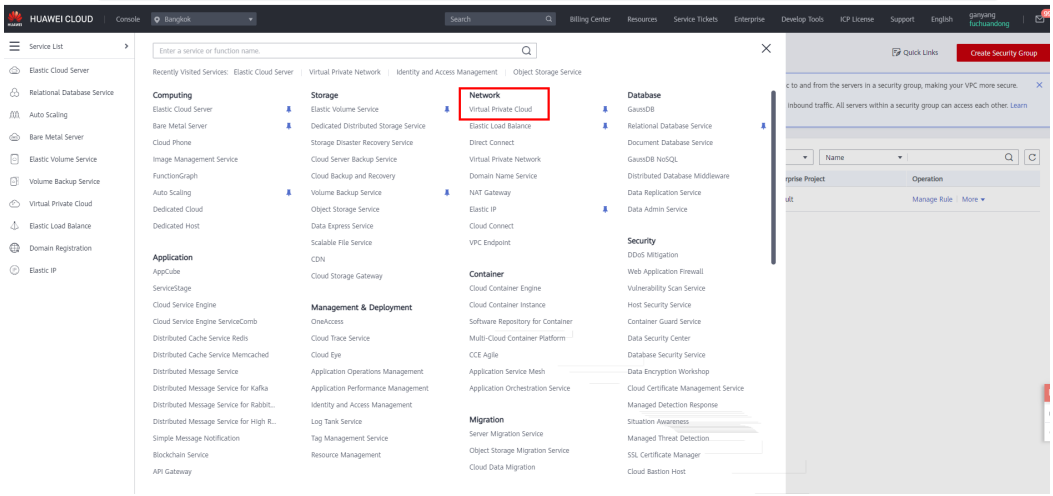
When creating a VPC, create the subnet 10.10.1.0, which is used as the server/client plane IP address and system replication/heartbeat plane IP address of SAP and DB2.

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 pane on the left, click and choose **Network** > **Virtual Private Cloud**.



Step 4 Click **Create VPC** on the right of the page.

Step 5 Configure required parameters as prompted based on **Table 3-5**.

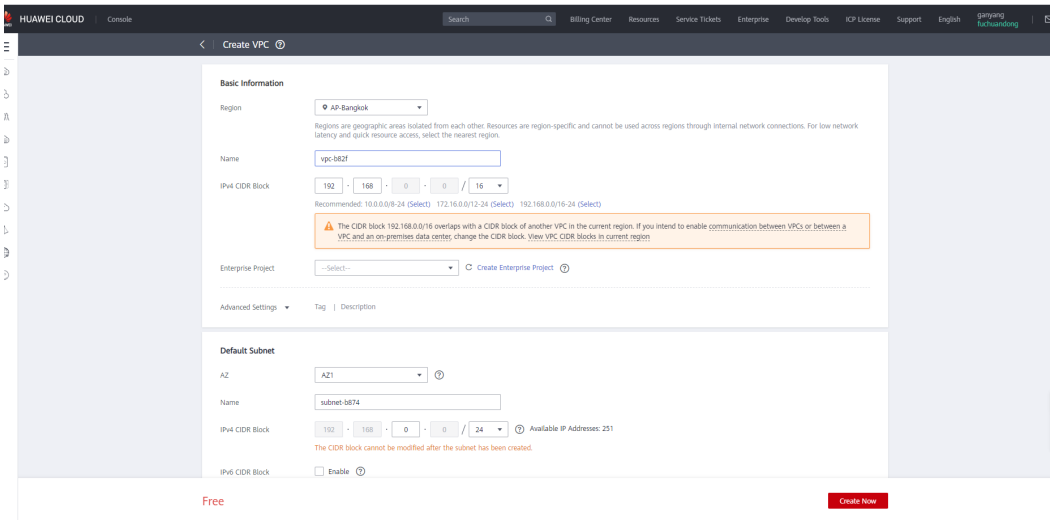


Table 3-5 Parameters required for creating a VPC

Item	Parameter	Description
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 on the upper left of the page to change the region.
	Name	VPC name
	CIDR Block	The CIDR block of 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 in the VPC). 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 **Network Planning**.
	Enterprise Project	The enterprise project to which the VPC belongs. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**. For details about creating and managing enterprise projects, see the **Enterprise Management User Guide**.
	Tag	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. For details about the tag naming rules, see **VPC Tag Naming Rules**.

Item	Parameter	Description
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 private networks.
	Name	Subnet name
	CIDR Block (of the subnet)	The CIDR block for the subnet. This value must be within the VPC CIDR block. Configure the subnet CIDR block based on the information provided in **Network Planning**.
	Advanced Settings	Click **Advanced Settings** to set parameters such as **Gateway** and **DNS Server Address**.
	Gateway	The gateway address of the subnet.
	DNS Server Address	External DNS server addresses are used by default. If you need to change the DNS server address, ensure that the DNS server addresses you configured are available.
	DHCP Lease Time	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.
	Tag	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**.
Add Subnet	You can click **Add Subnet** to add a subnet.	

Step 6 Click **Create Now**.

----End

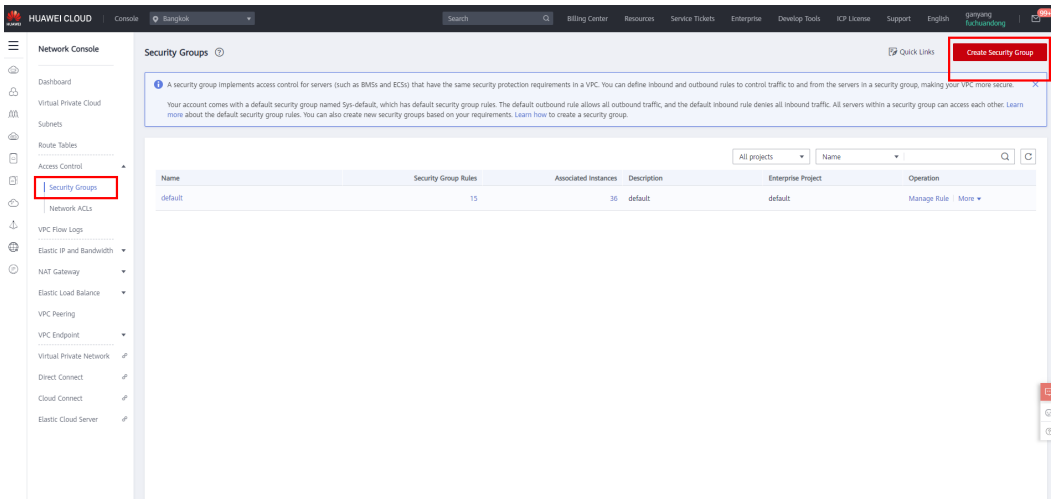
3.4.2 Creating a Security Group

A security group is a collection of access control rules for ECSs that have the same security protection requirements and are mutually trusted. After a security group is created, you can create various access rules for the security group, and these rules will apply to all ECSs added to this security group. For more information about security groups, see **Security Group Overview**.

Procedure

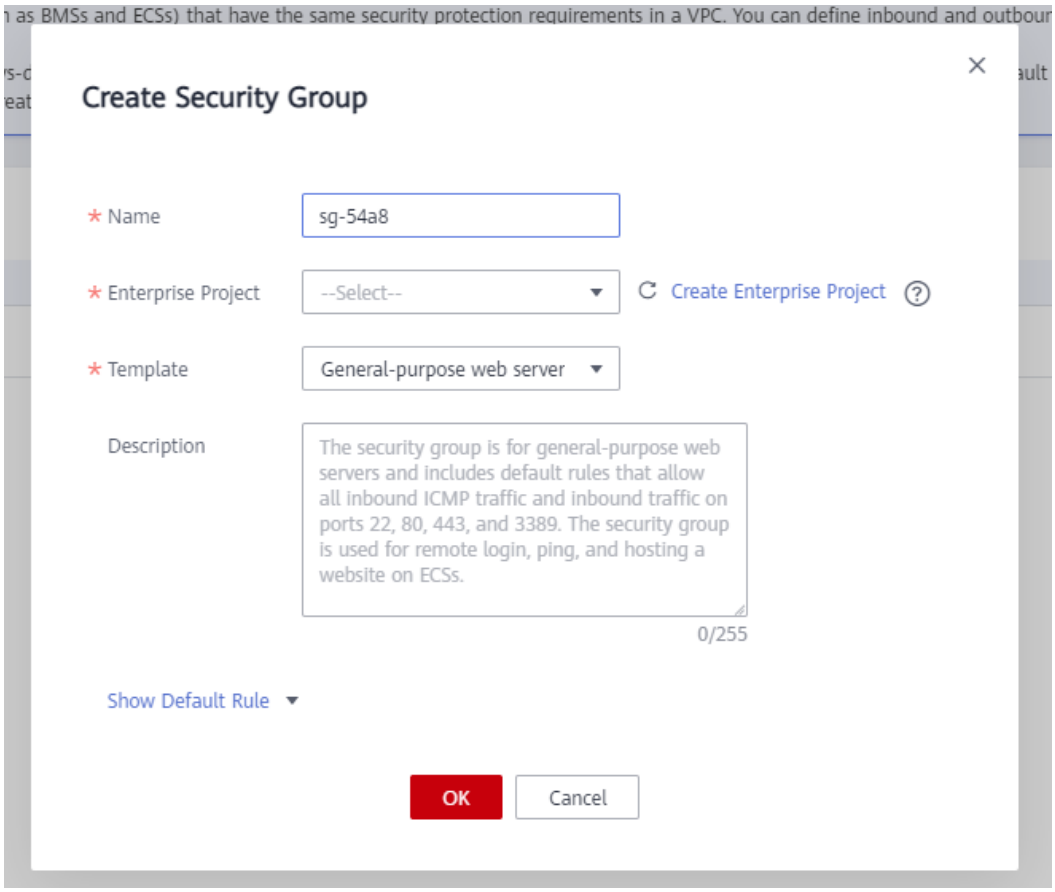
Step 1 Create a SAP security group.

Choose **Access Control** > **Security Groups** in the navigation pane on the left of the VPC console. On the **Security Groups** page, click **Create Security Group**.

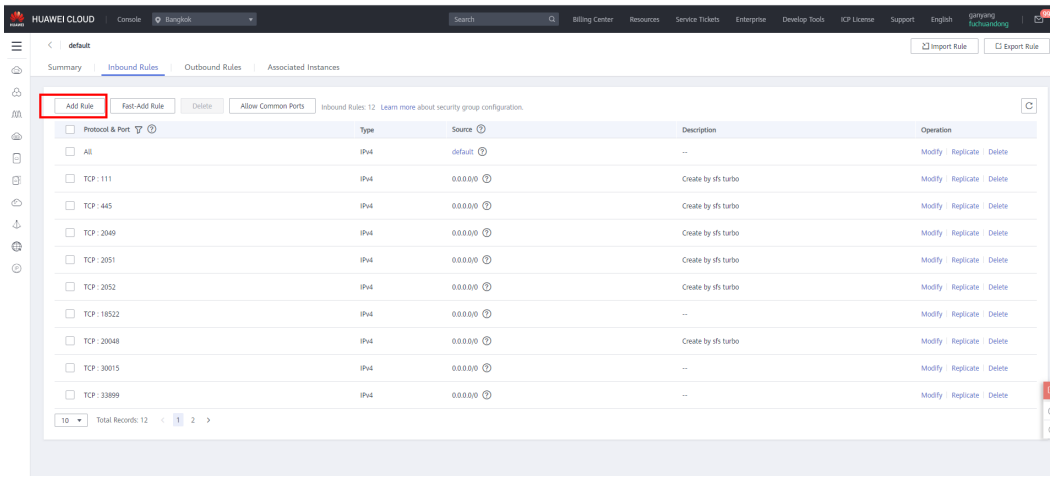


Step 2 Set required parameters to create a security group.

- **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 you create 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 you create using this template includes default rules that allow inbound traffic on any port. Note that allowing inbound traffic on any port poses security risks.
- **Name**: specifies the name of the security group. Name the security group that is easy to identify, for example, **sg_sap_**.
- **Enterprise Project**: You can add the security group to an enabled enterprise project. You can select an enterprise project from the drop-down list, for example, **SAP**.



Step 3 Click **OK**. Locate the row that contains the newly created security group, and click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, add the desired ports listed in **Security Group Planning**.



----End

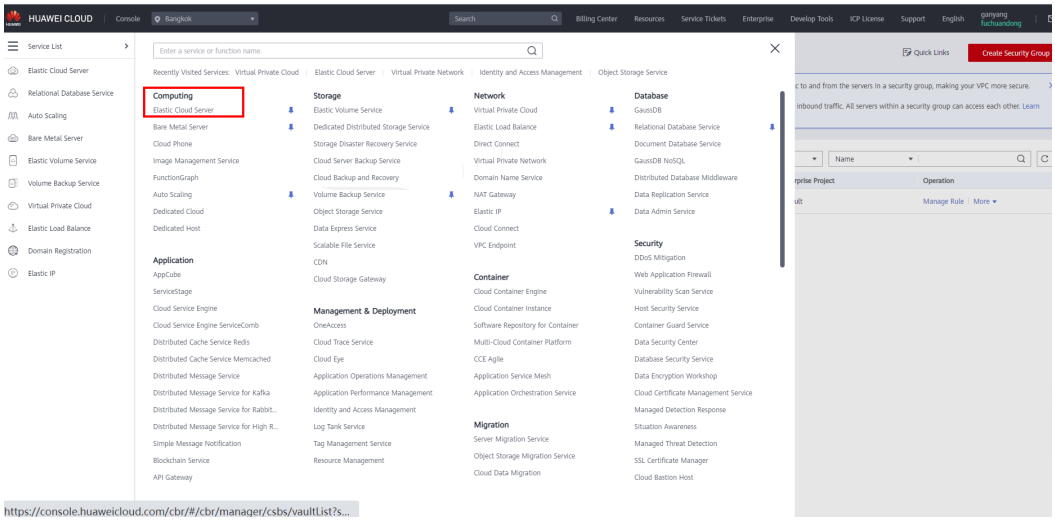
3.4.3 Creating ECSs

You need to create two ECSs. One is used to install the SAP application and SQL Server, and the other is used to install AAS.

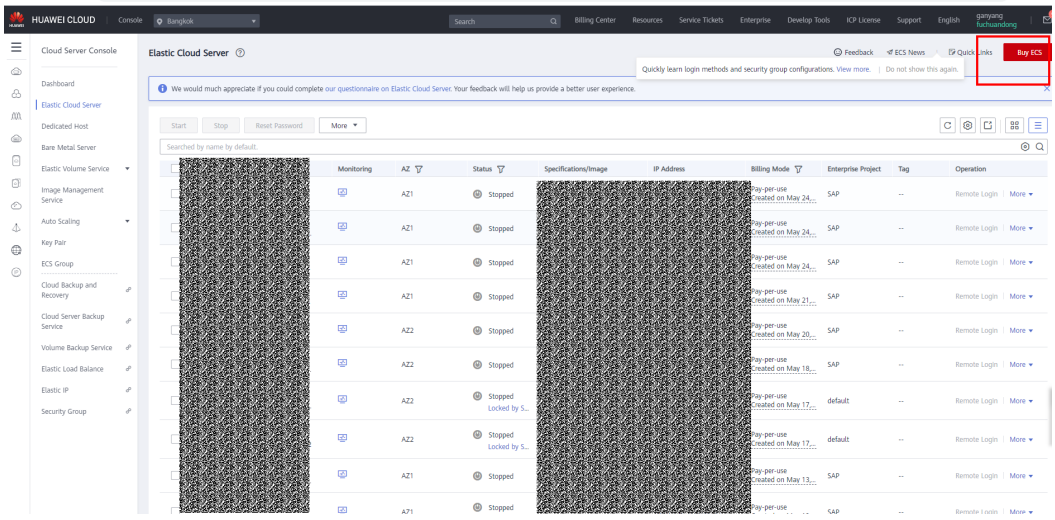
Table 3-6 ECS details

Name	Flavor	Disk	Image	Remarks
ecssap1	m6.2xlarge.8	System disk: 100 GB, ultra-high I/O Data disk: 250 GB, ultra-high I/O	Windows Server 2012 R2 Standard 64-bit English (40 GB)	Used for installing SAP ERP and SQL Server
ecssap2	m6.xlarge.8			Used for installing AAS and SAP GUI

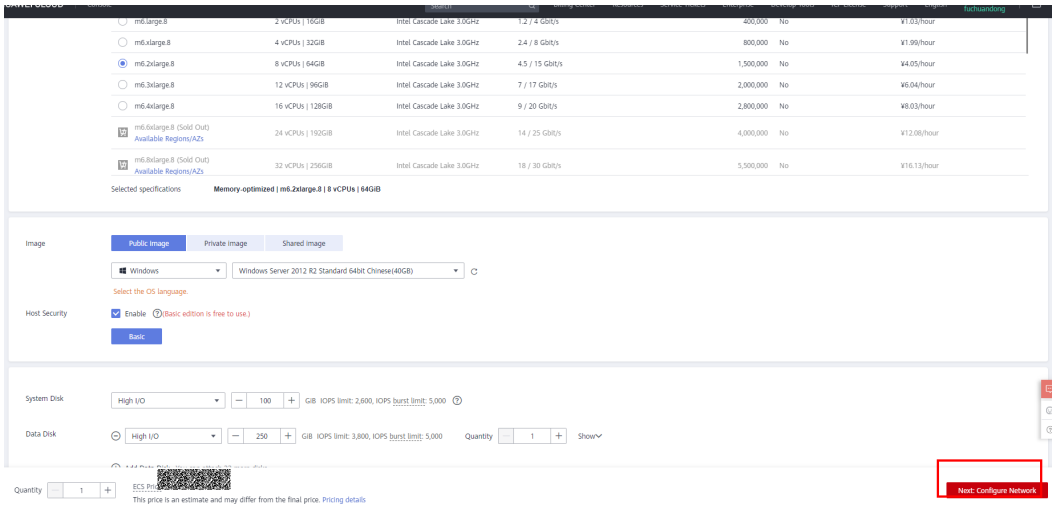
Step 1 Log in to the HUAWEI CLOUD management console, click the service list icon, and choose **Computing** > **Elastic Cloud Server**.



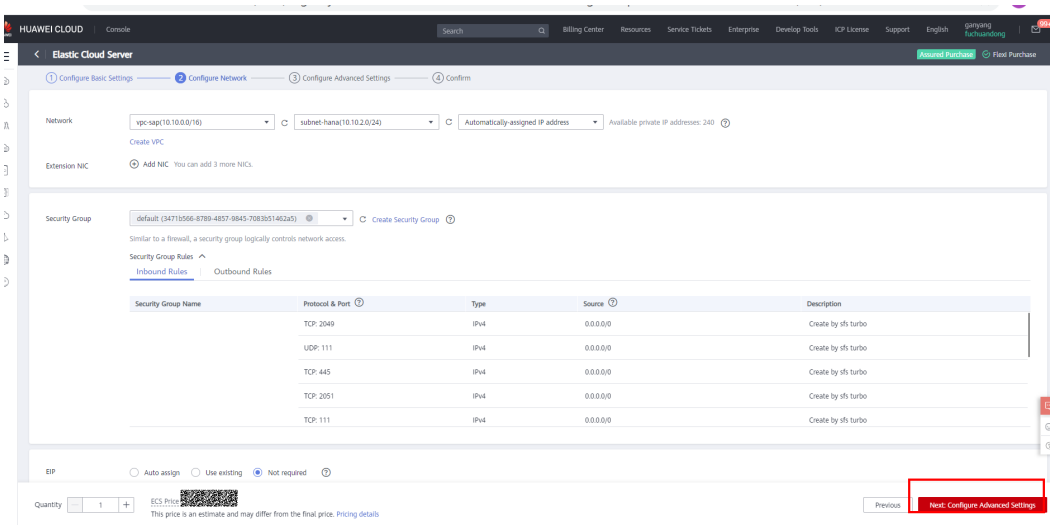
Step 2 Click **Buy ECS**.



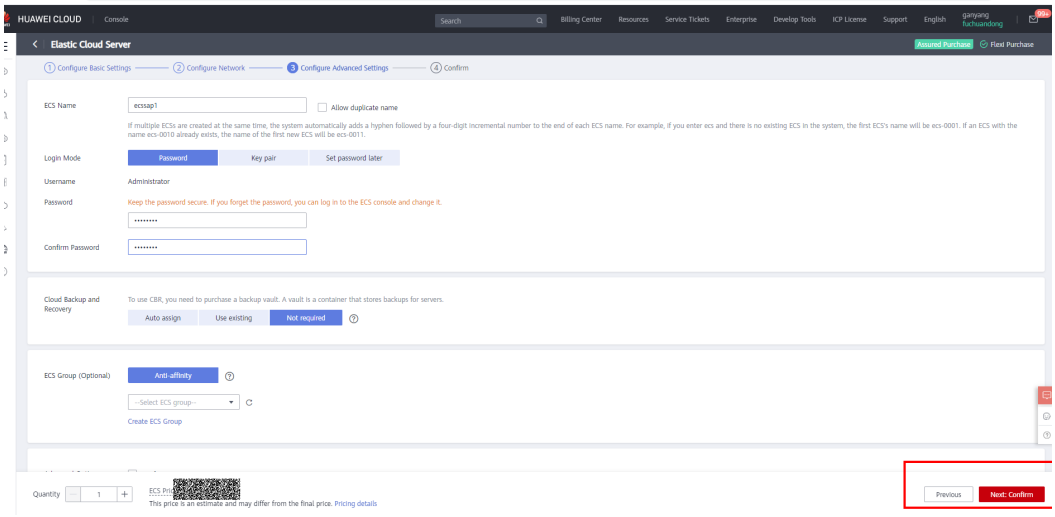
Step 3 Select the ECS flavor, image, and disk size based on **Table 3-6**.



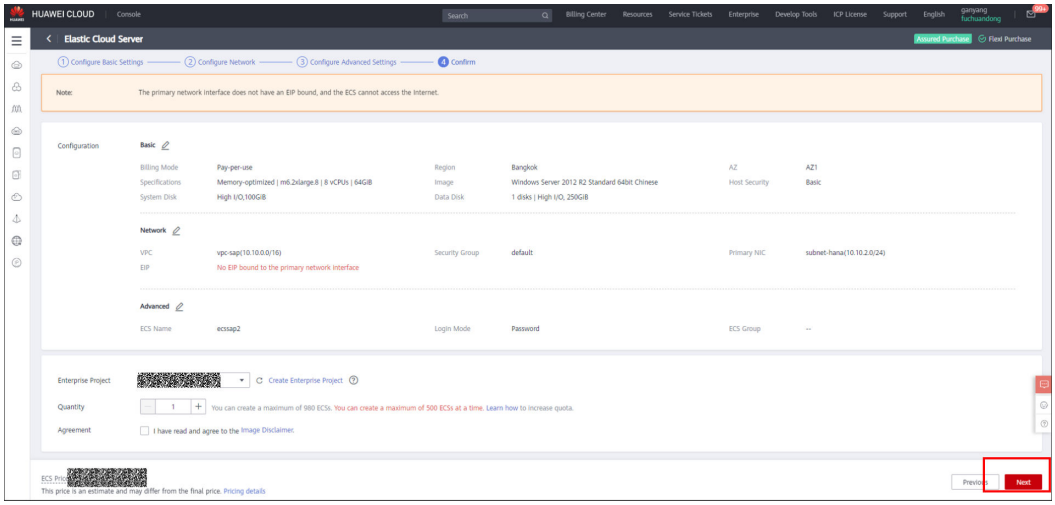
Step 4 Click **Next: Configure Network**. Select the created VPC and security group, confirm the configuration, and click **Next: Configure Advanced Settings**.



Step 5 Enter the ECS name and password of the **root** user, and click **Next: Confirm**.

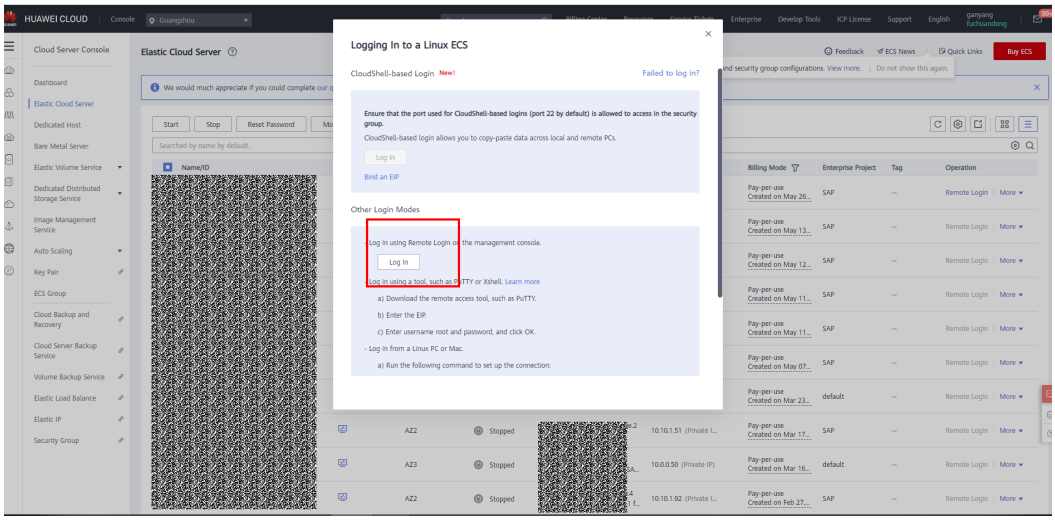


Step 6 Select an enterprise project and click **Next**.



Step 7 Repeat the preceding steps to create another ECS (ecssap2).

Step 8 After ECSs are created, locate the created ECSs in the ECS list and click **Remote Login** in the **Operation** column. Log in to the ECSs as user **root** using VNC.

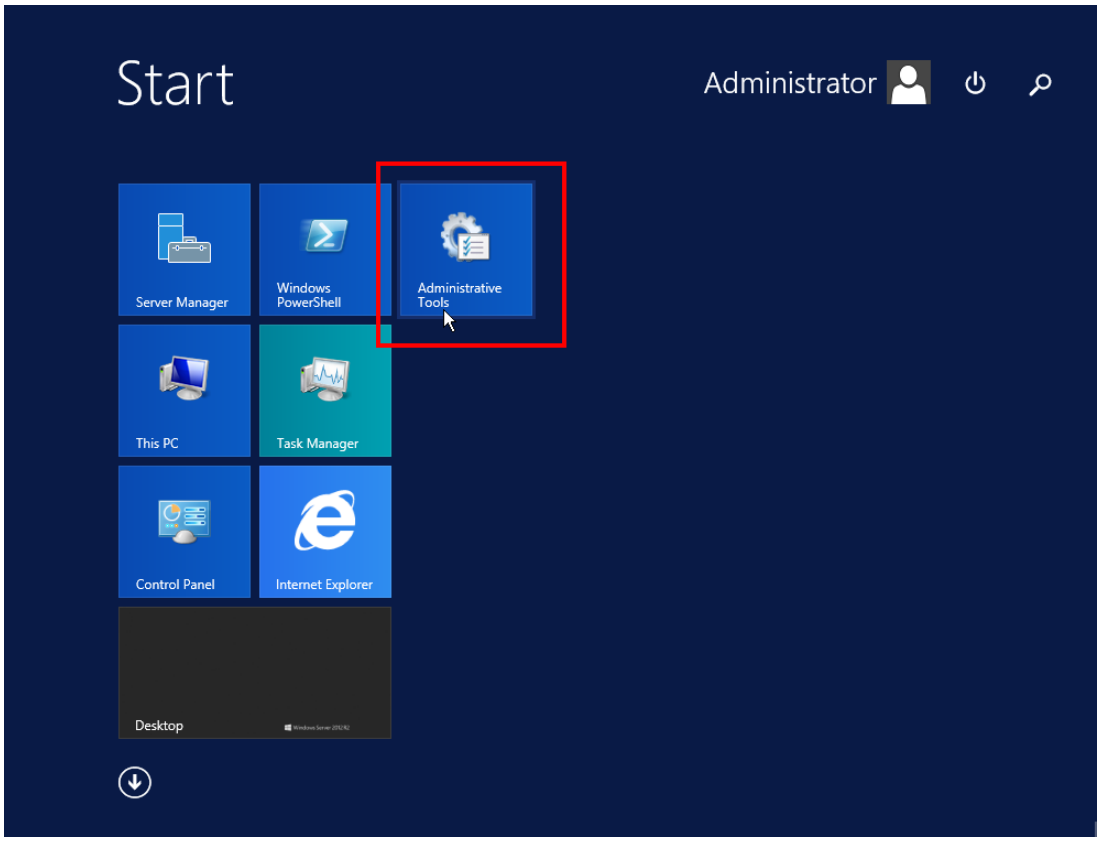


----End

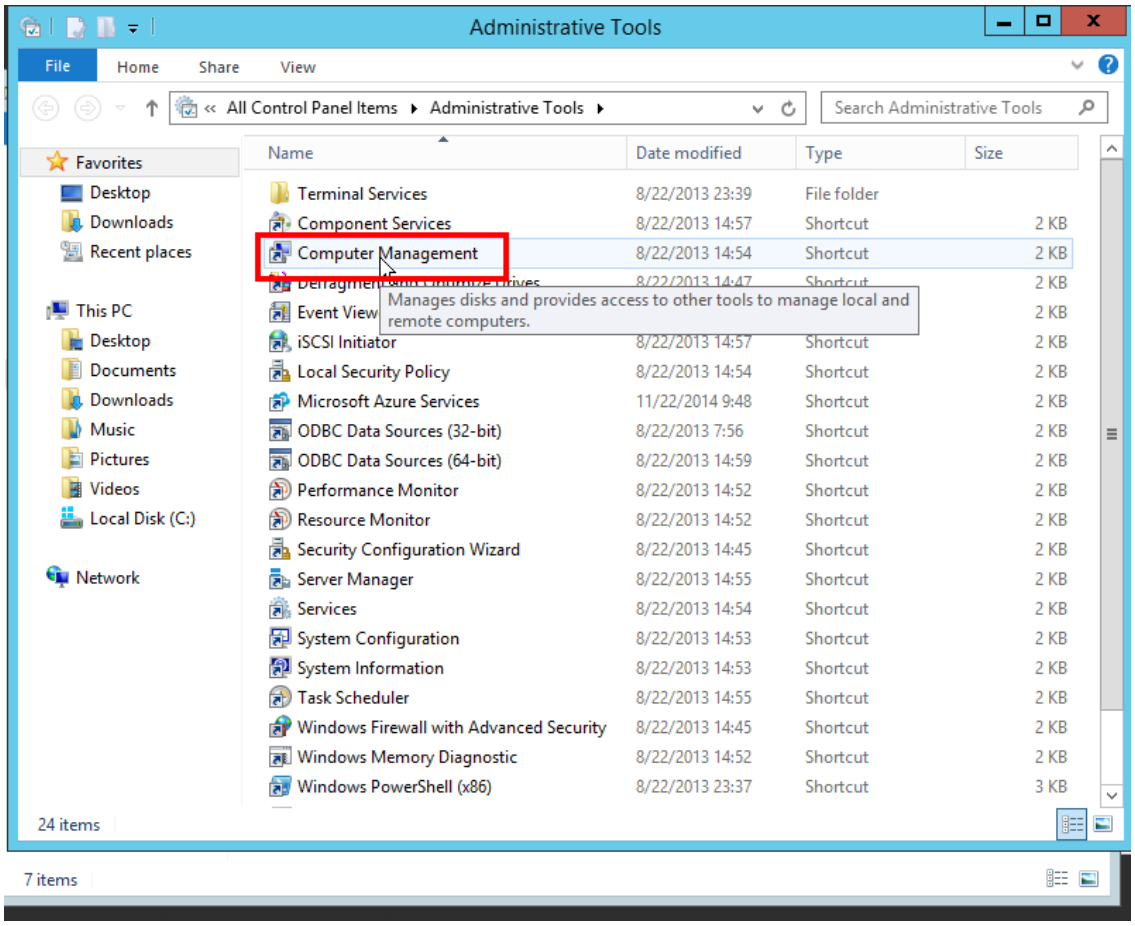
3.4.4 Creating Data Disk and Specifying the Size

Perform the following operations on the two ECSs.

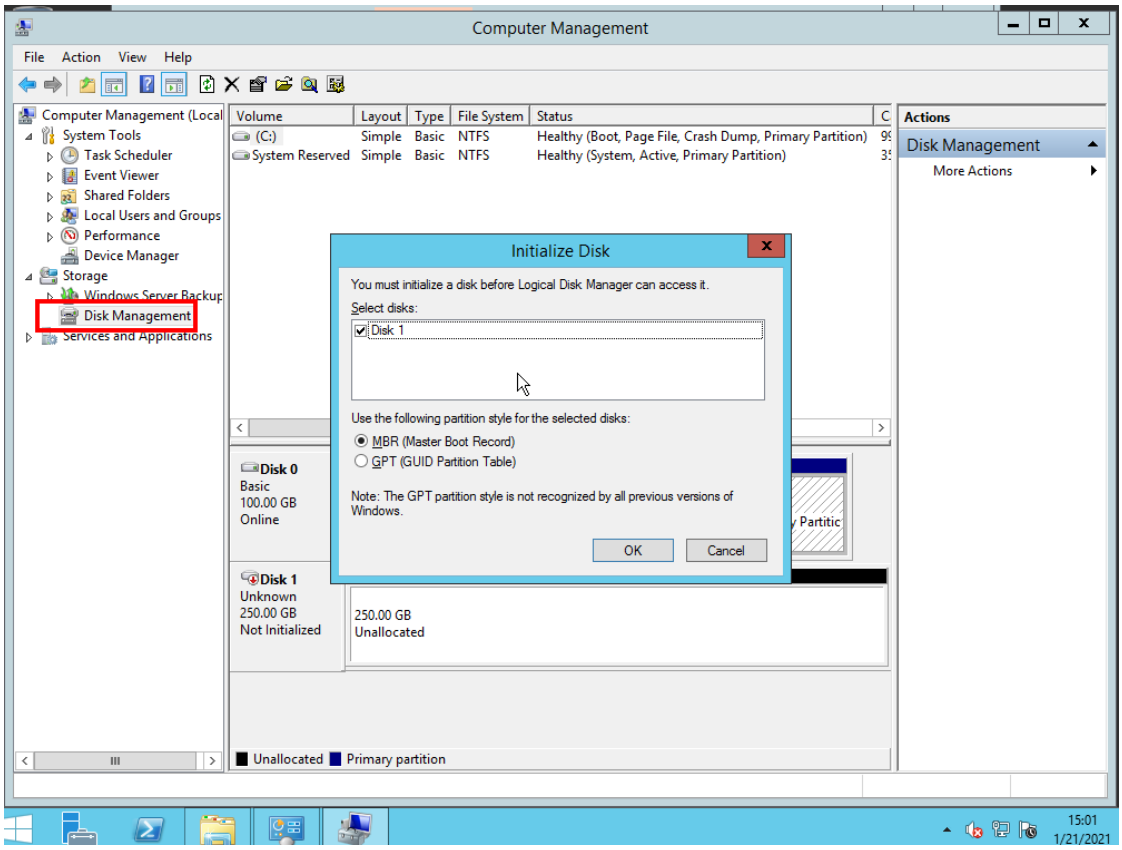
Step 1 In the window similar to the following figure, click **Administrative Tools**.



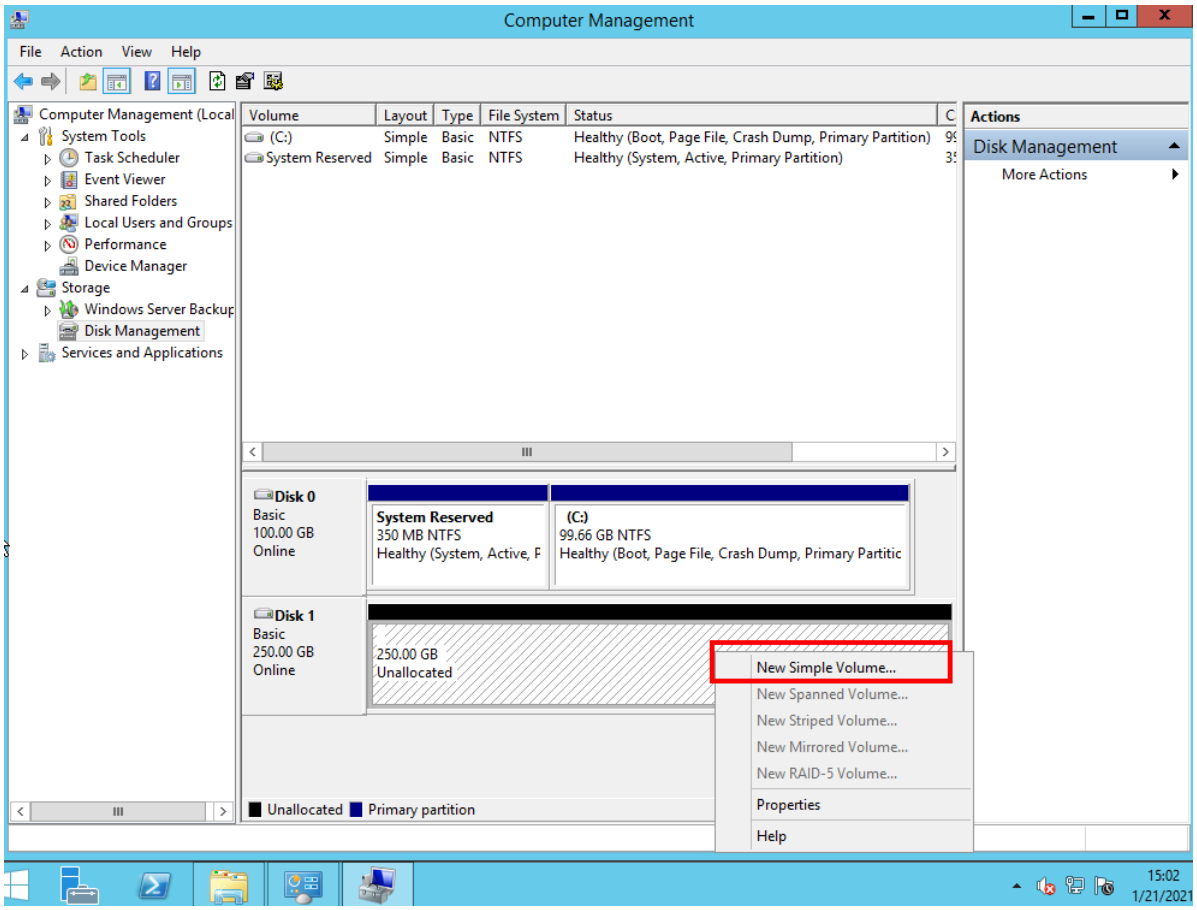
Step 2 Click **Computer Management**.



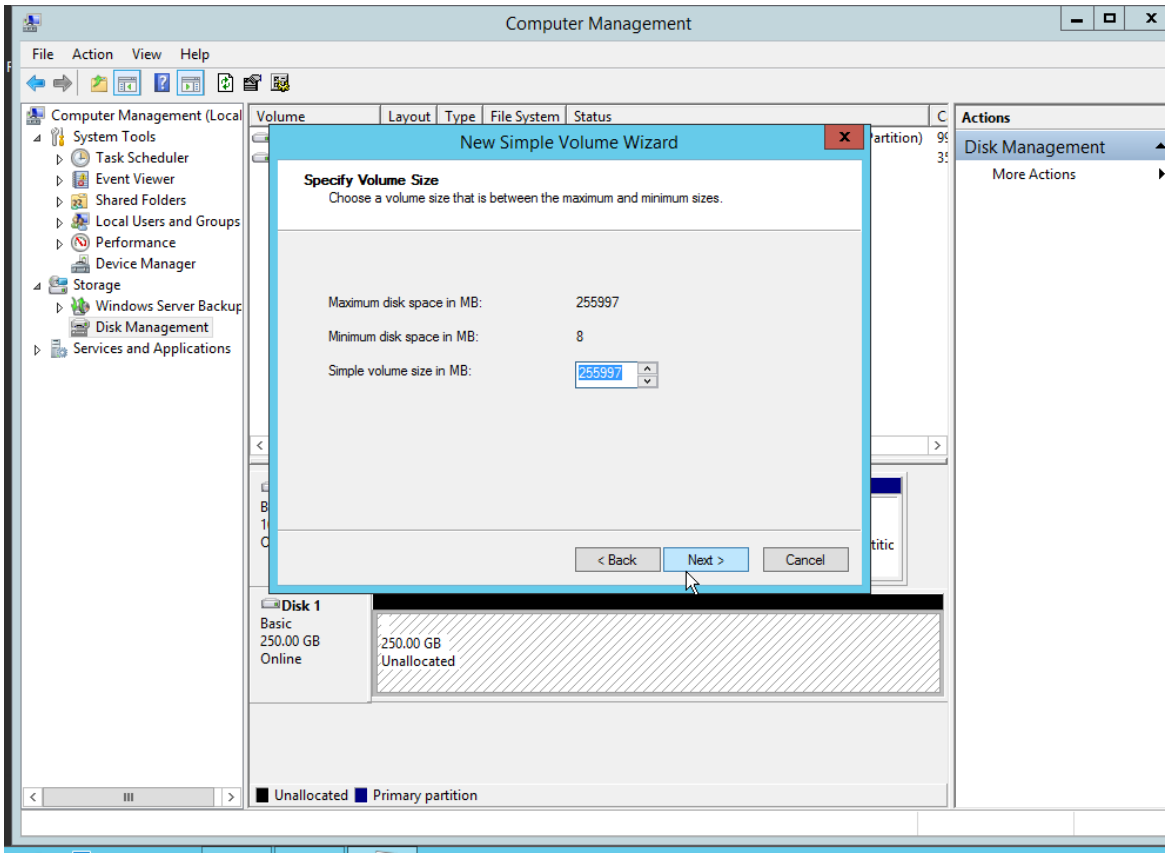
Step 3 Choose **Disk Management**.



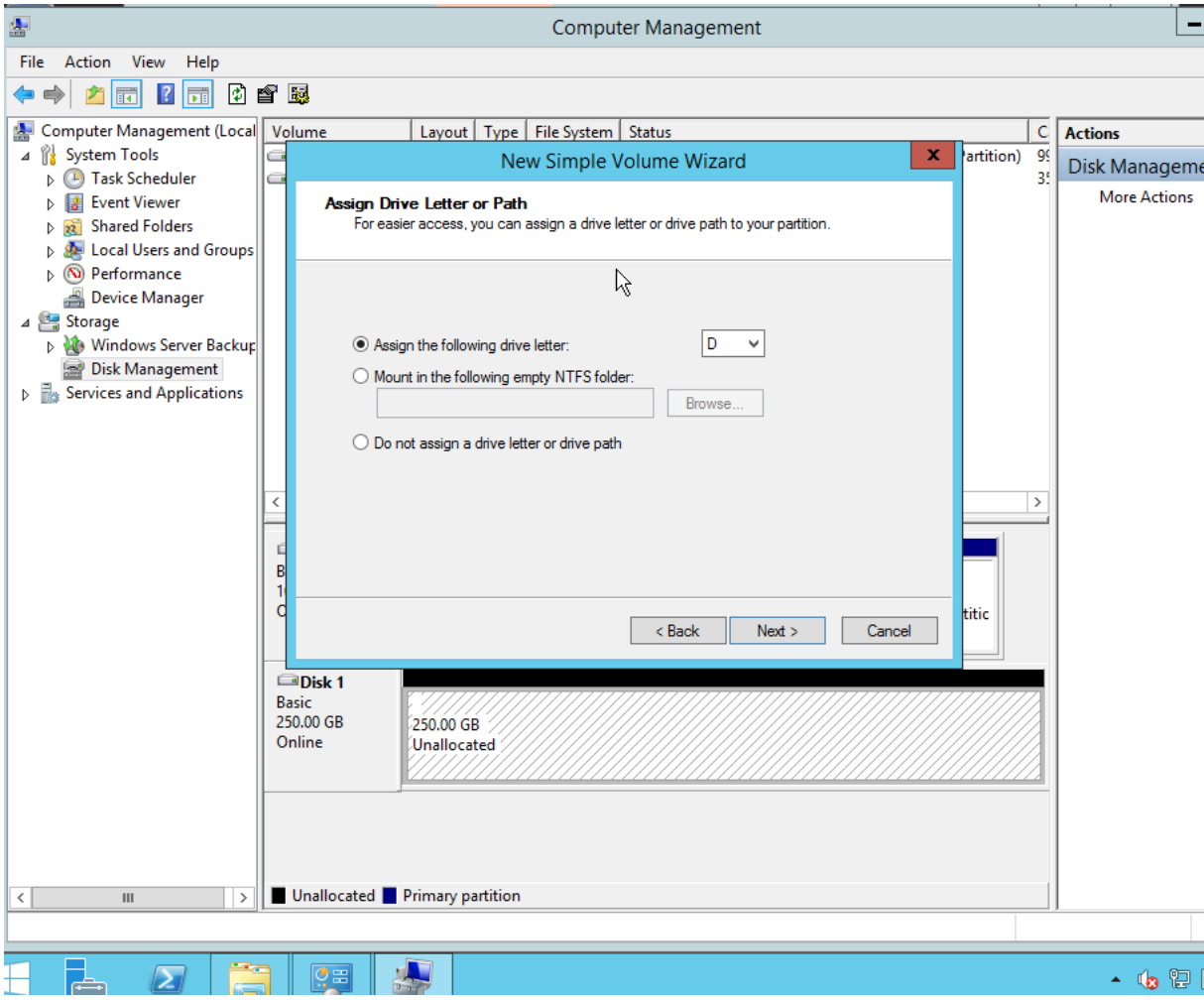
Step 4 Right-click the disk and choose **New Simple Volume**.



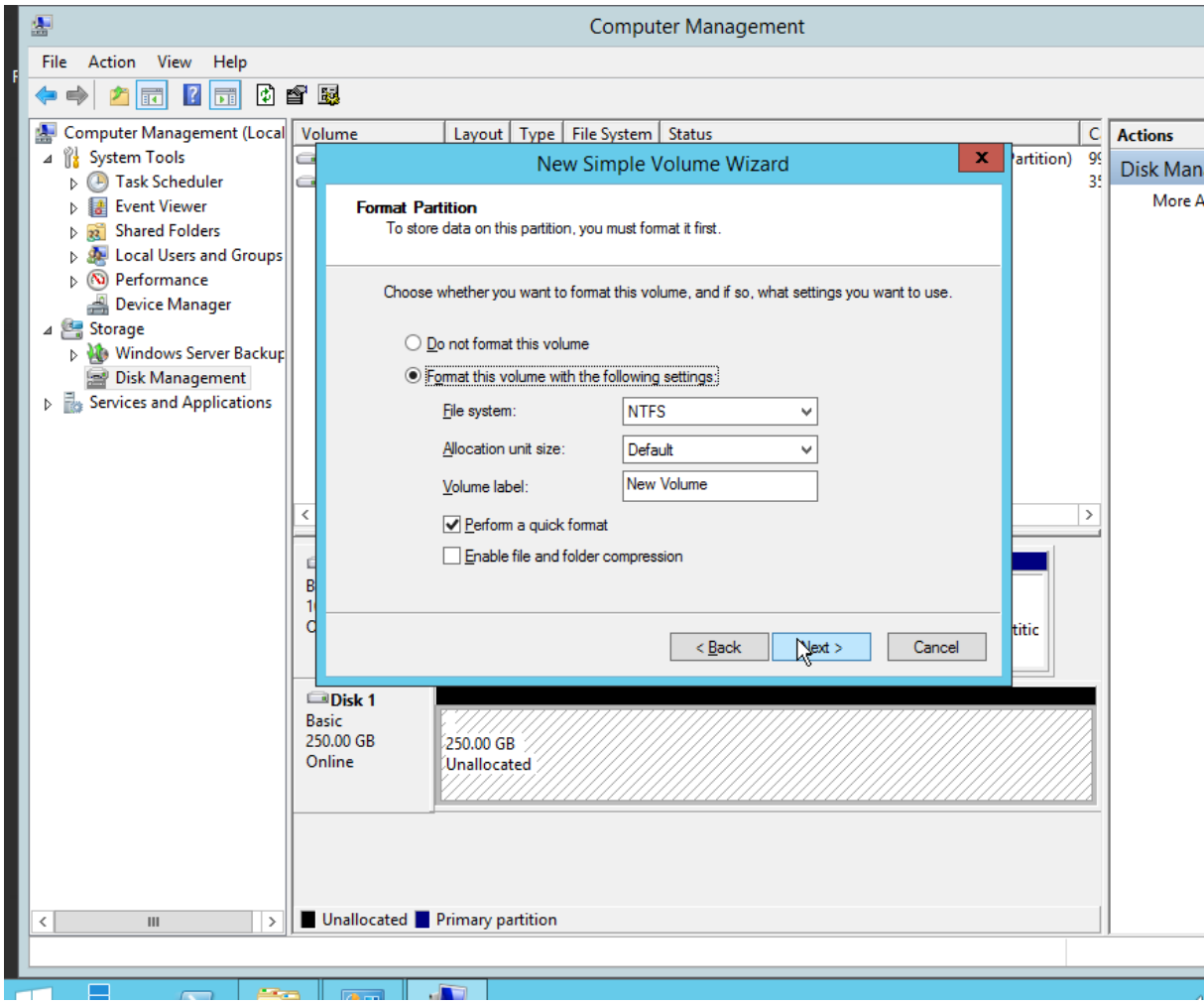
Step 5 Enter the disk size to be allocated.



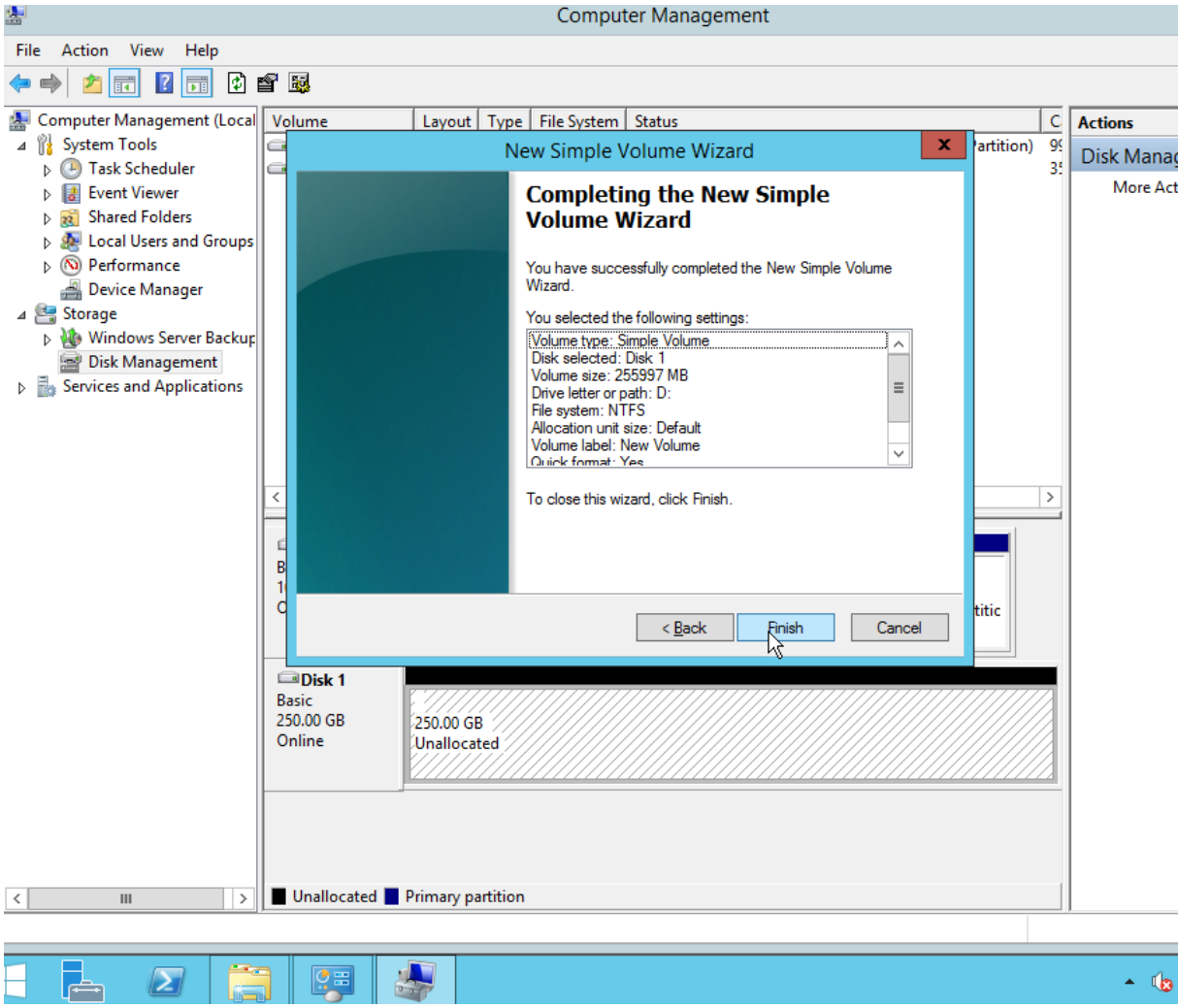
Step 6 Assign drive letter or path.



Step 7 Use the default settings, and click **Next**.



Step 8 Click **Finish**.

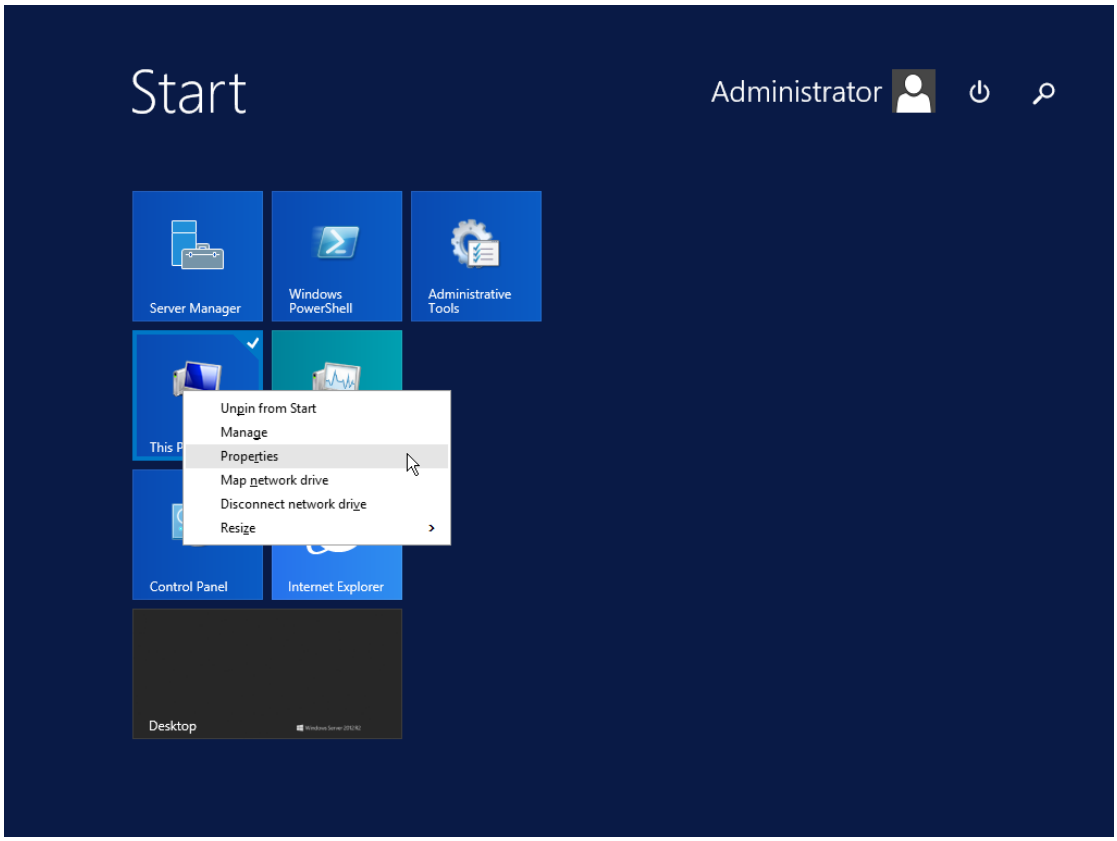


----End

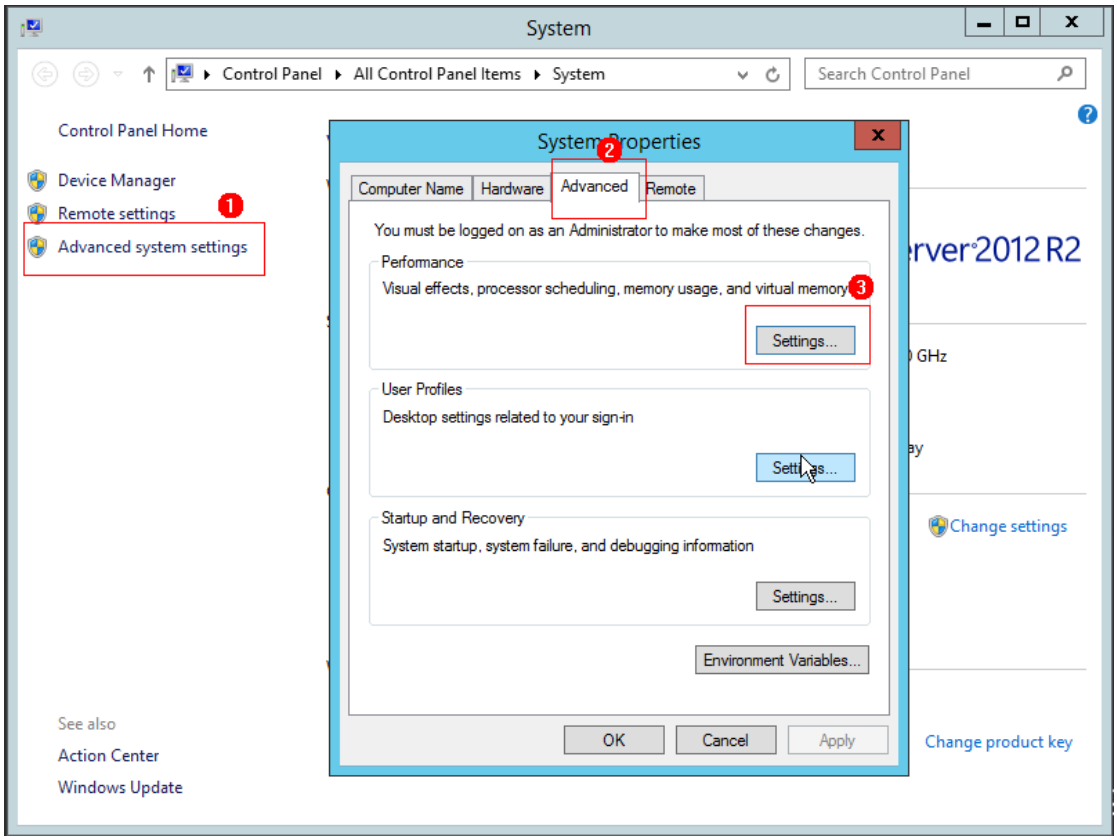
3.4.5 Customizing the Virtual Memory

Perform the following operations on the two ECSs to set the virtual memory to 64 GB, that is, 65,536 MB.

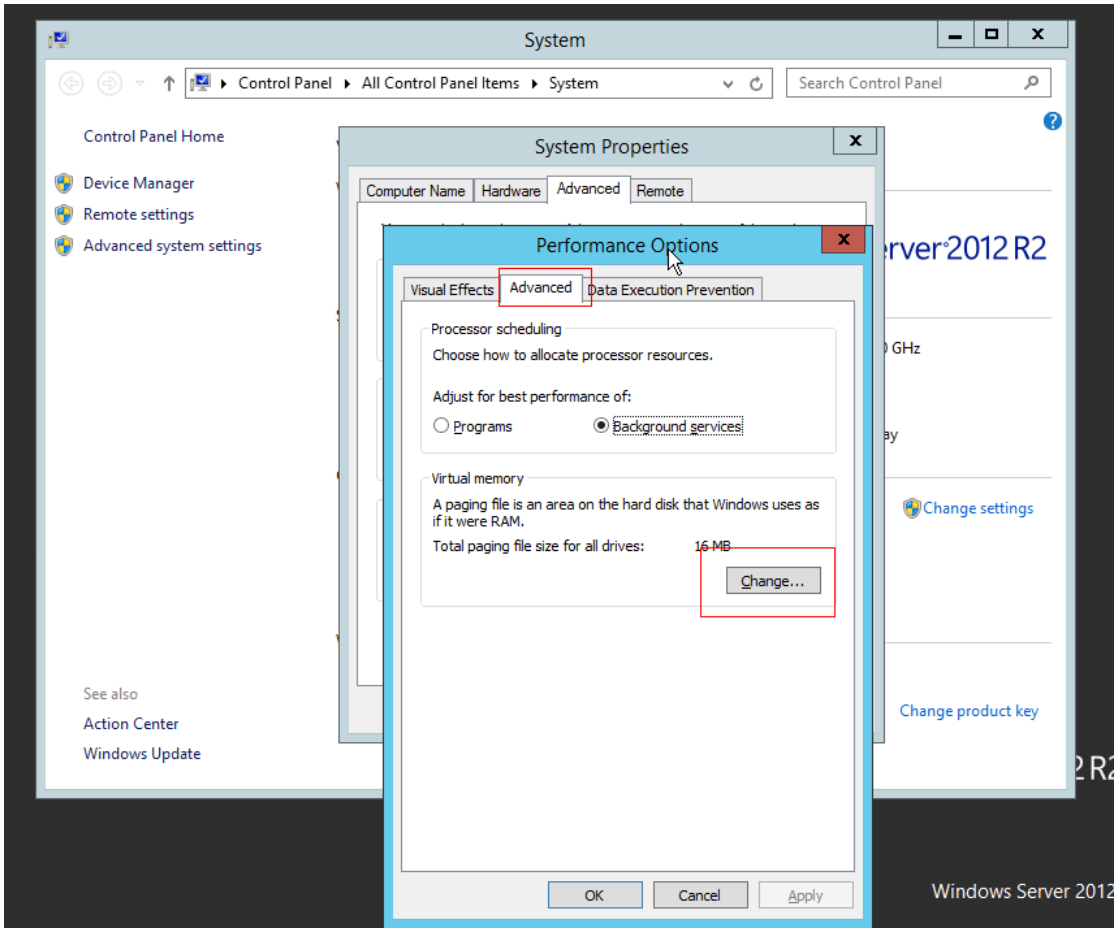
1. Click the start icon in the lower left corner of the PC, right-click **This PC**, and choose **Properties** from the shortcut menu.



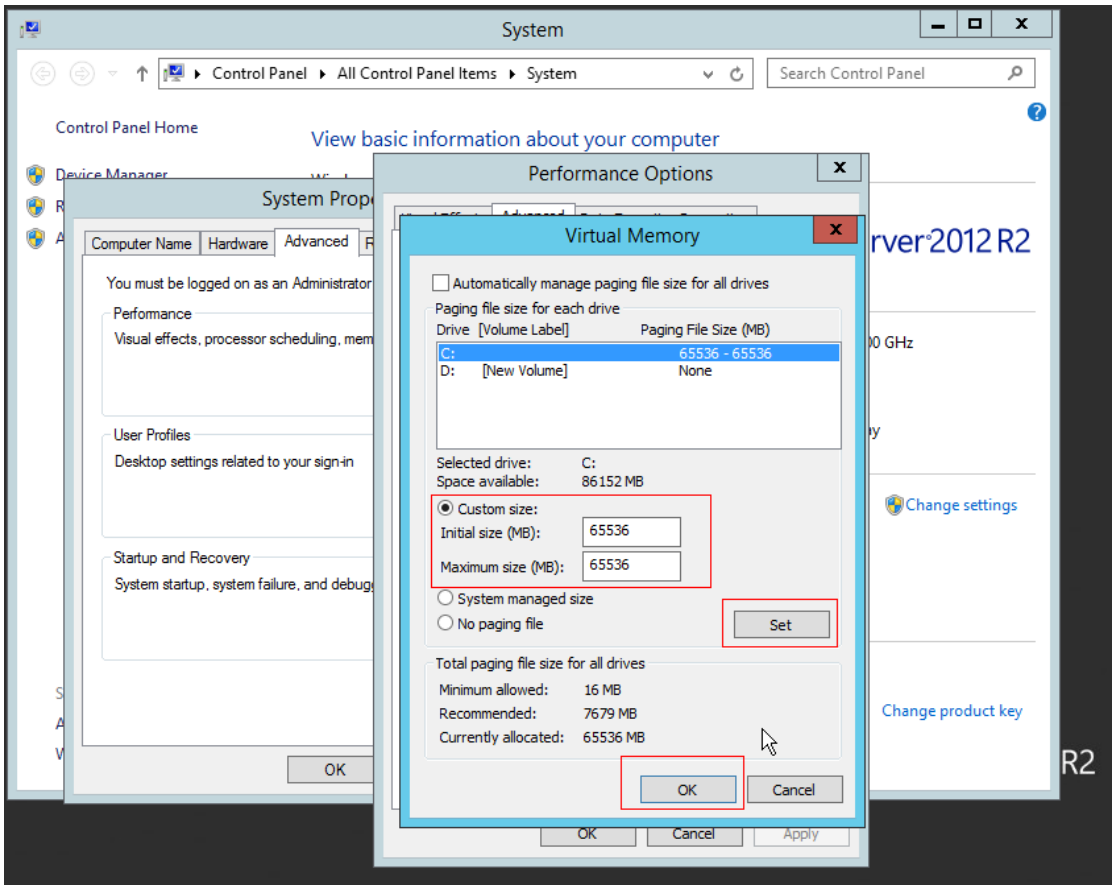
2. Choose **Advanced system settings**, select **Advanced**, and click **Settings** in the **Performance** area.



3. In the displayed dialog box, choose **Advanced** > **Virtual memory** > **Change**.



4. In the **Custom size** area of the displayed dialog box, set **Initial size (MB)** and **Maximum size (MB)** to **65536**. Then, click **Set** and **OK**.



3.4.6 Modifying the Registry

The following operations must be performed on the two ECSs. For details, see **http://support.microsoft.com/kb/2820470**.

Resolution

Important This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:

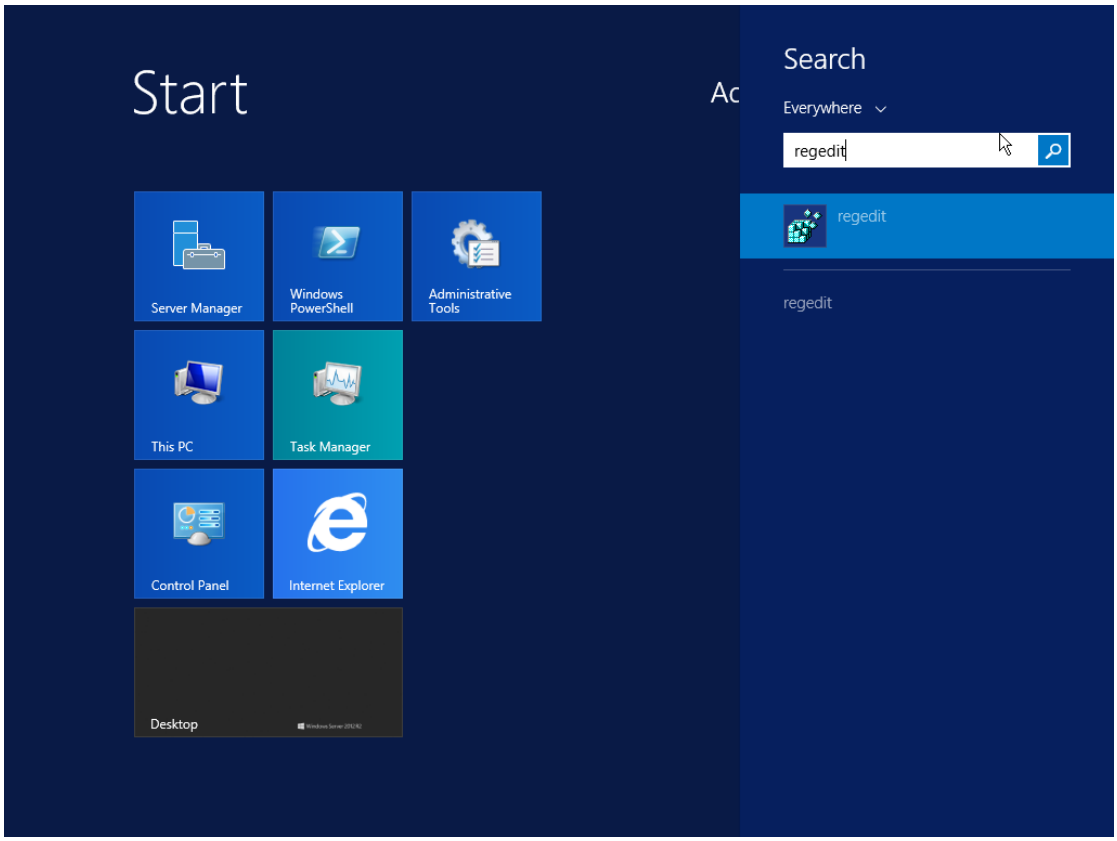
322756 How to back up and restore the registry in Windows To resolve this issue in Windows 8 or Windows Server 2012, install the hotfix that is described in this article on the SMB client computer. This hotfix is also available at Microsoft Update Catalog.

To resolve this issue on a Windows 8.1-based, Windows 10-based, Windows Server 2012 R2-based, Windows Server 2016-based, or Windows Server 2019-based SMB client computer, create a new registry key named DisableCARetryOnInitialConnect and set the value of the registry key to 1 by following these steps:

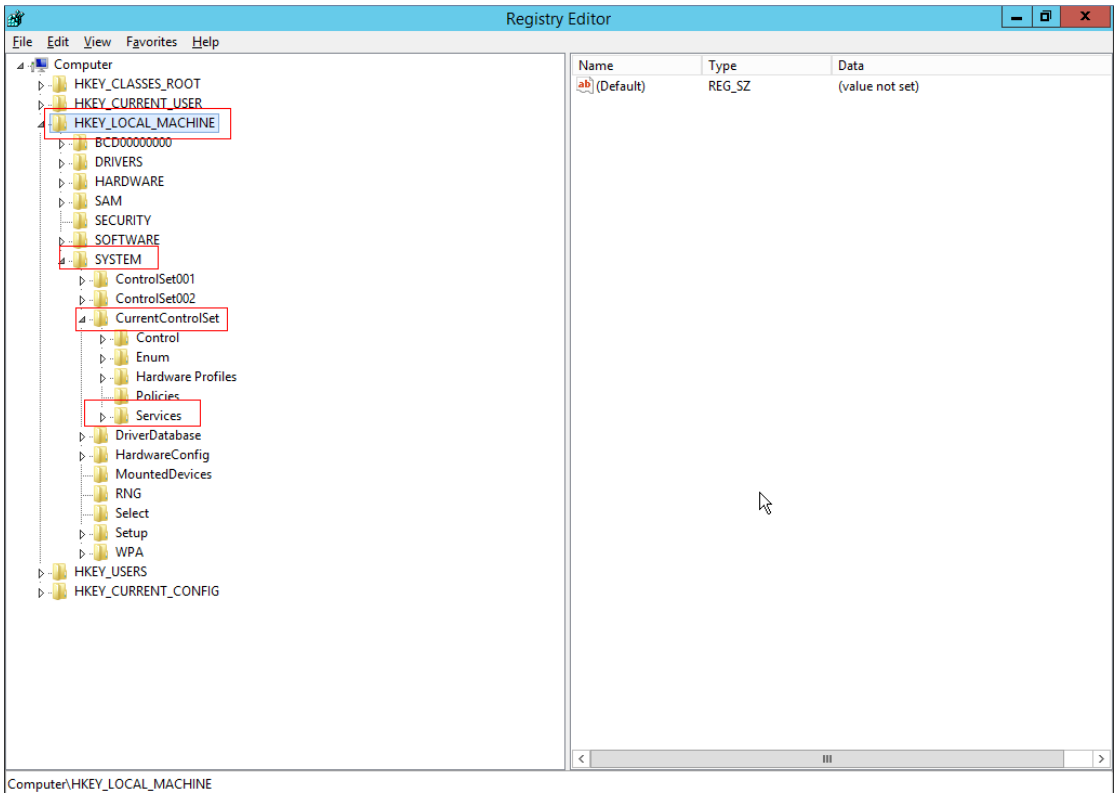
1. Swipe in from the right edge of the screen, and then tap **Search**. Or, if you are using a mouse, point to the lower-right corner of the screen, and then click **Search**.
2. In the search box, type regedit, and then tap or click **regedit**.
   If you are prompted to enter an administrator password, type the password. If you are prompted to provide confirmation, provide confirmation.
3. Locate and then tap or click the following registry subkey:
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkStation\Parameters
4. On the **Edit** menu, point to **New**, and then tap or click **DWORD Value**.
5. Type DisableCARetryOnInitialConnect.
6. Press and hold or right-click DisableCARetryOnInitialConnect, and then tap or click **Modify**.
7. In the **Value data** box, type 1, and then tap or click **OK**.
8. Exit Registry Editor.

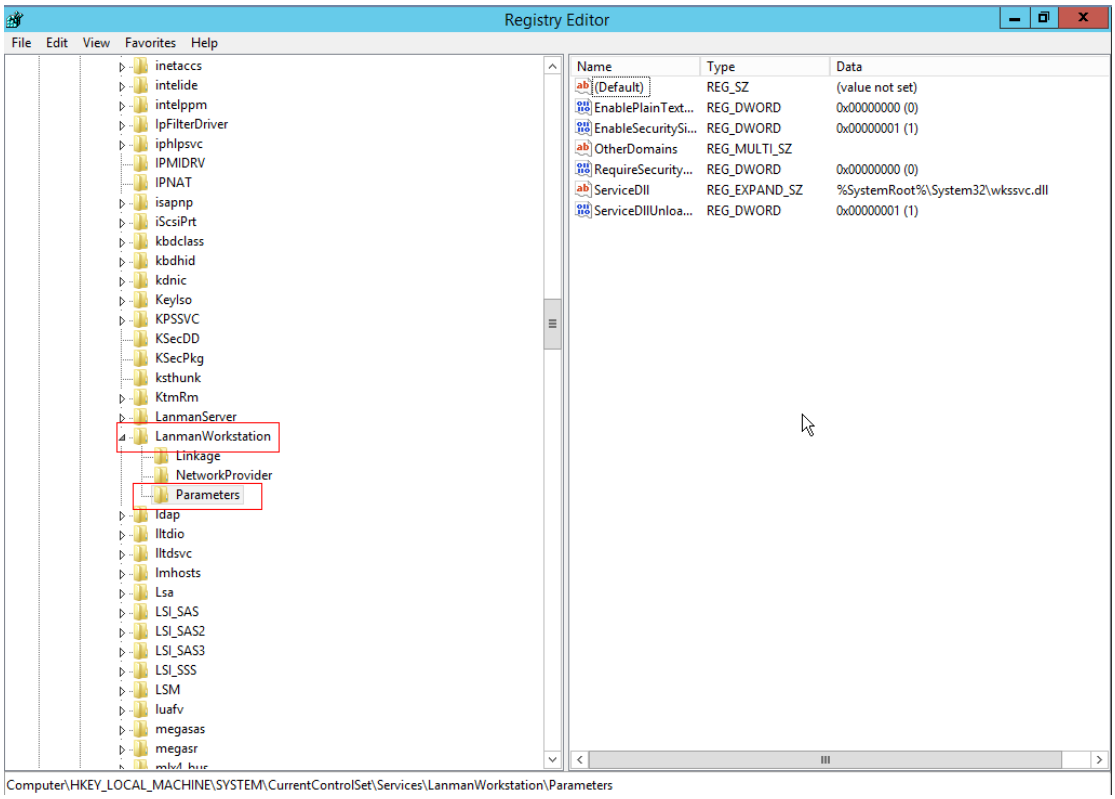
After you configure the DisableCARetryOnInitialConnect registry key, the Continuous Availability feature is disabled for the initial Server Message Block (SMB) tree connect command that is run against a share. If you want to enable the Continuous Availability feature, set the value of the registry key to 0.

1. Search for regedit.

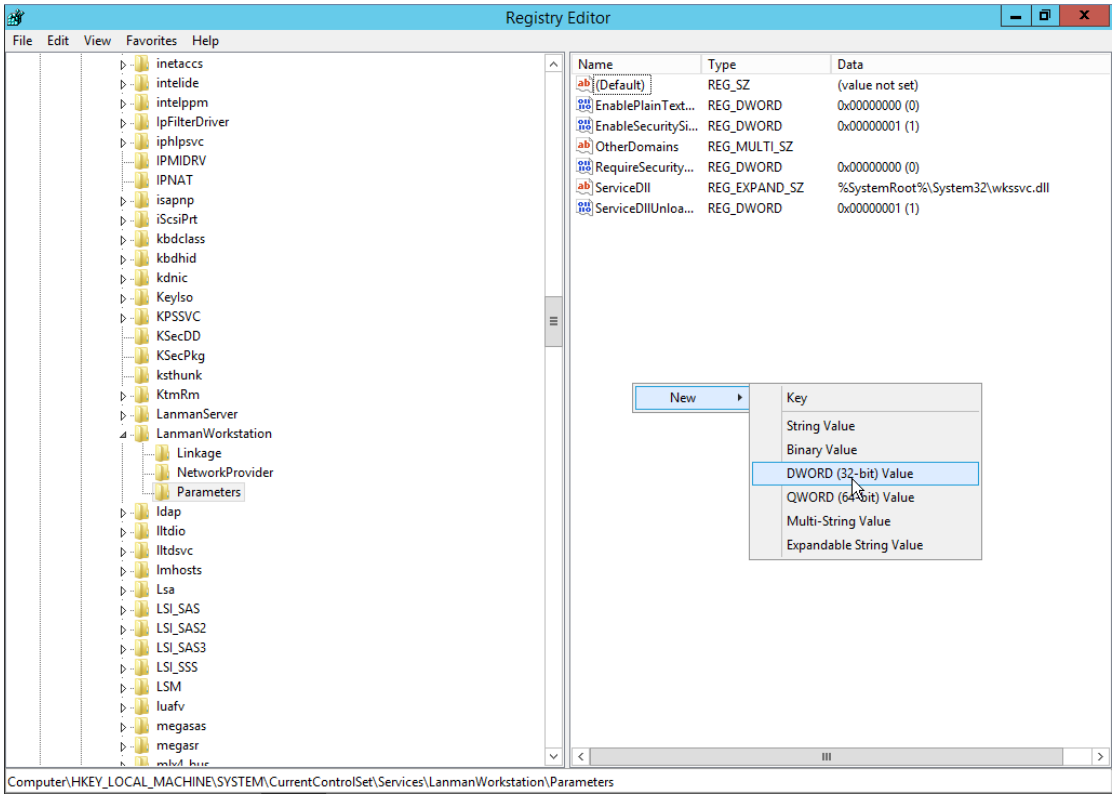


2. Locate and then tap or click the following registry subkey: **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkStation\Parameters**

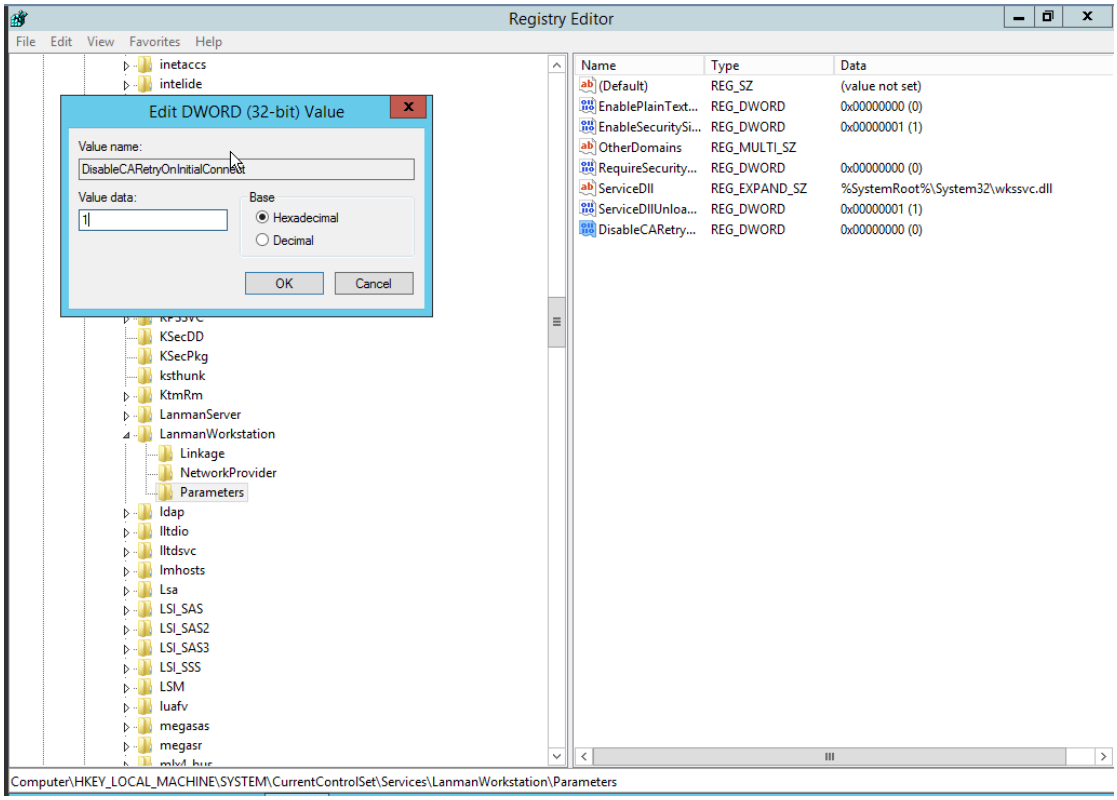


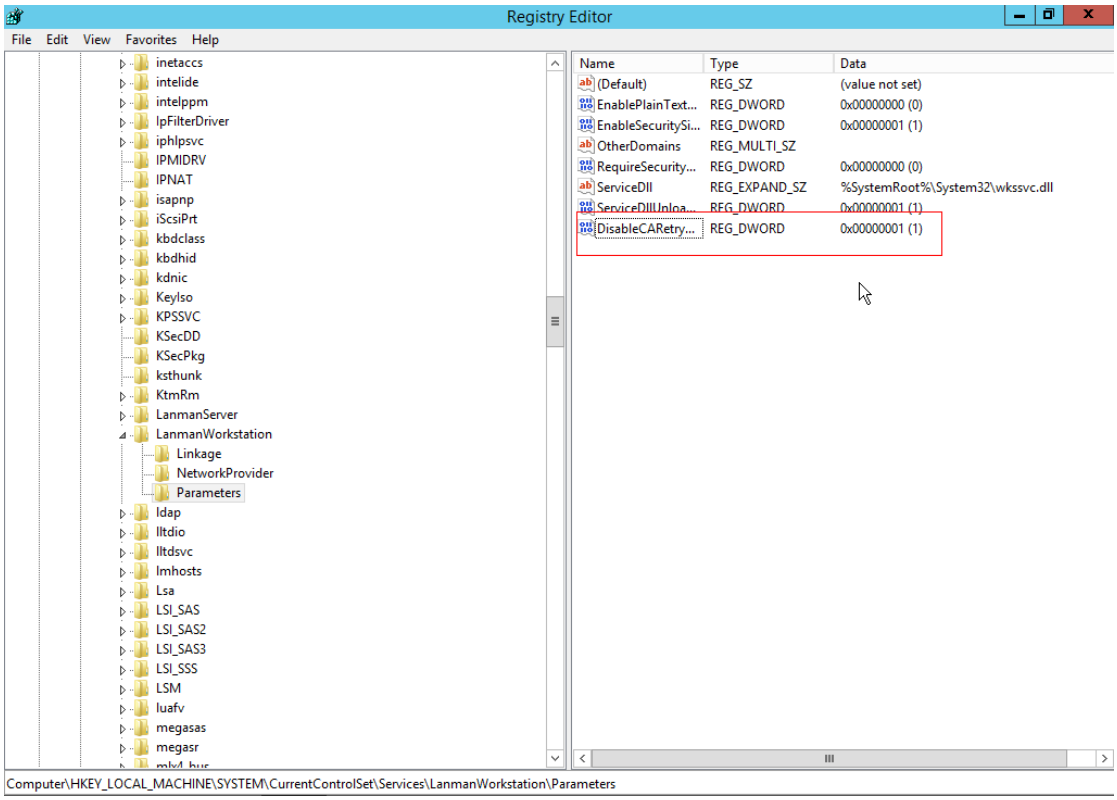


3. On the **Edit** menu, point to **New**, and then click **DWORD Value**.



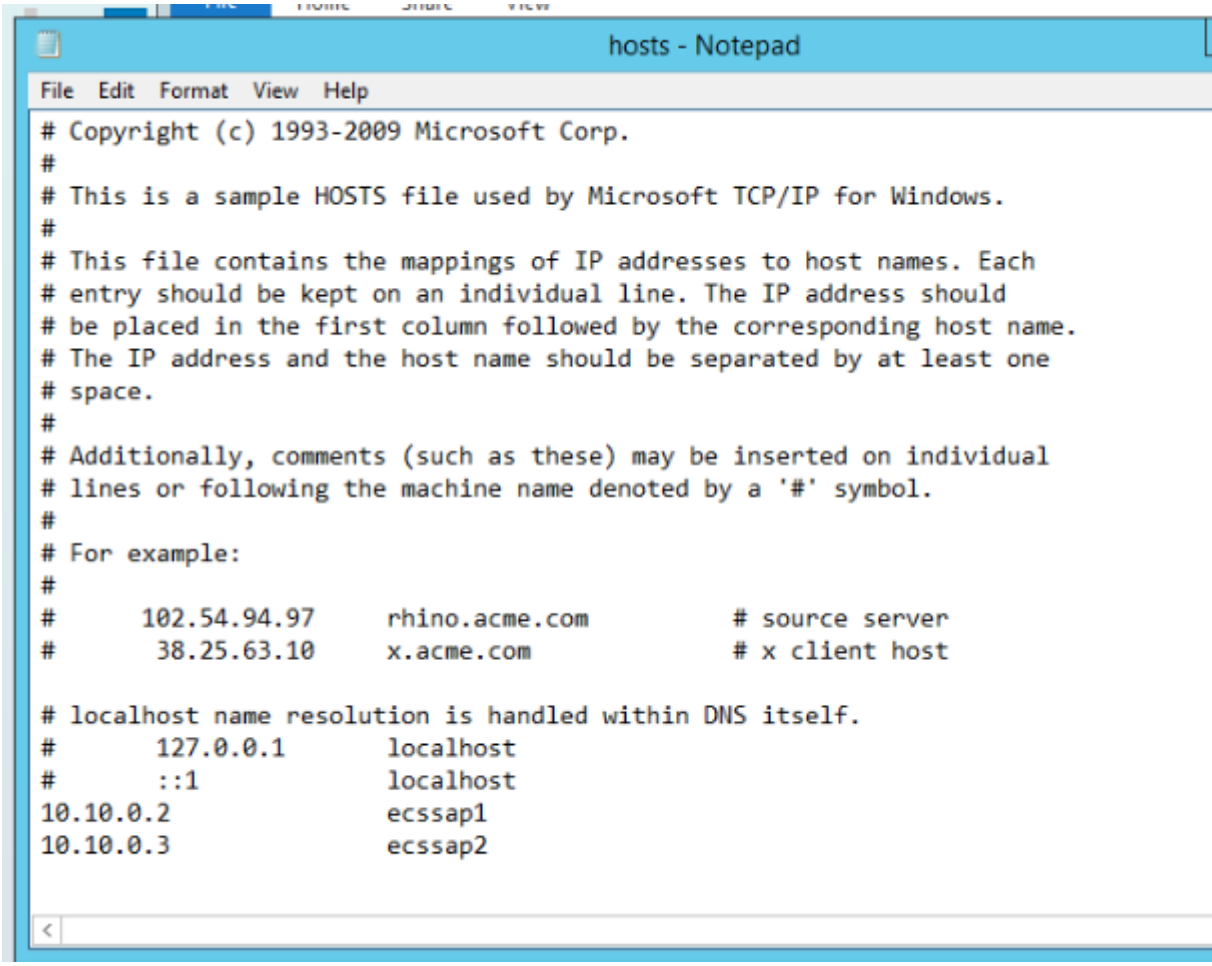
4. Type **DisableCARetryOnInitialConnect**. Right-click **DisableCARetryOnInitialConnect**, and then click **Modify**. In the **Value data** box, type **1**, and then click **OK**.





3.4.7 Configuring the Hosts Configuration File

Write the private IP addresses and host names of the two ECSs into their hosts files, respectively. C:\Windows\System32\drivers\etc\hosts



After the IP addresses and host names are added to the ECSs, restart them.

3.4.8 Downloading and Decompressing the SAP Software Package

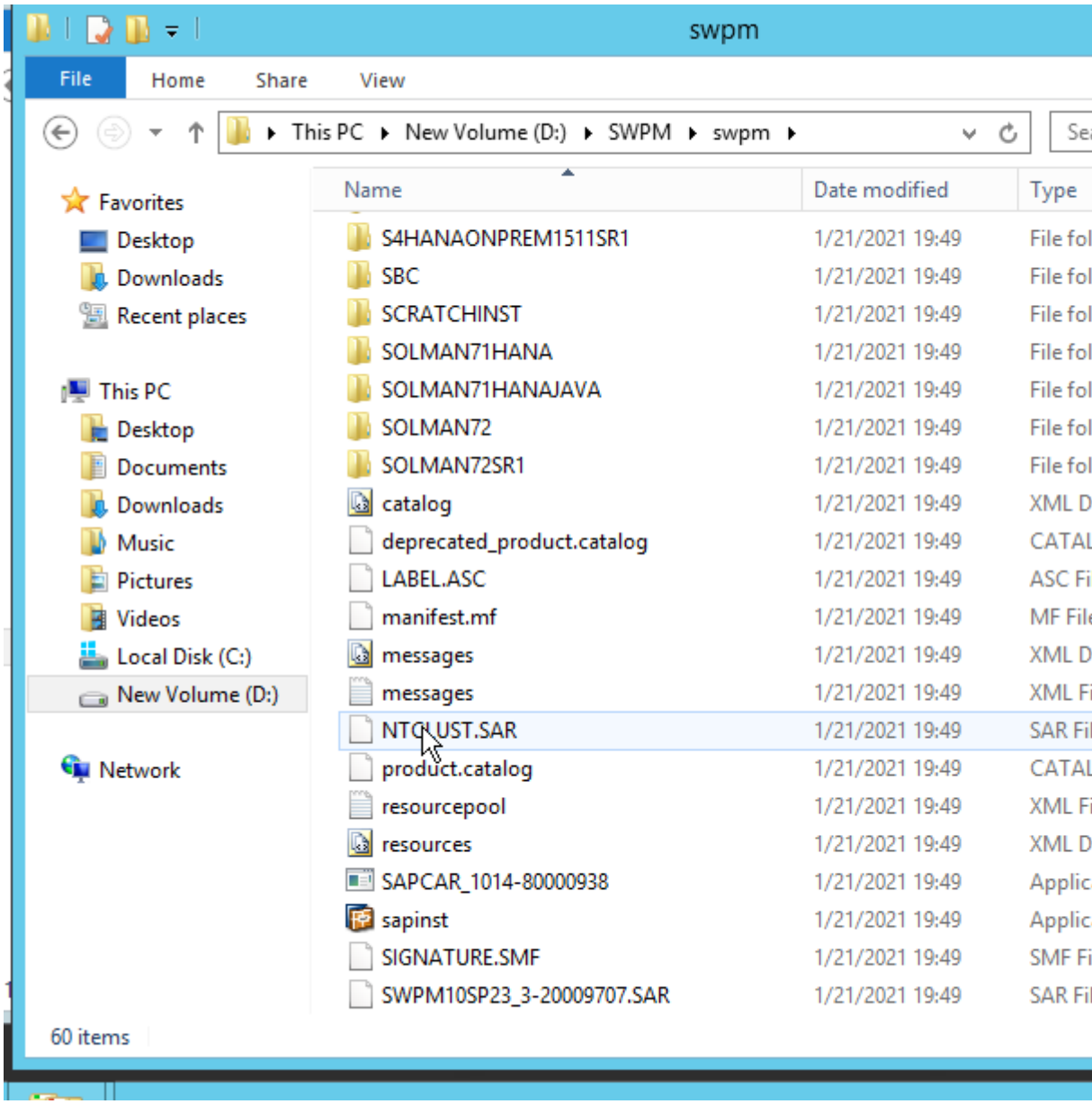
Download the SAP application and SQL Server installation files from the official website, upload them to the OBS bucket, copy them to the ECSs, decompress them, and start the software installation.

For details about how to download the software, see section "4.7 Preparing the Installation Media" in the SAP installation guide.

Download the required software from **https://support.sap.com/swdc**.

Decompressing the Software Packages

Step 1 Decompress the swpm package.



Step 2 (Optional) If the downloaded package is in the SAR format, run the **SAPCAR -xvf SWPM20SP04*.SAR** command in CMD to decompress it to the current file.

----End

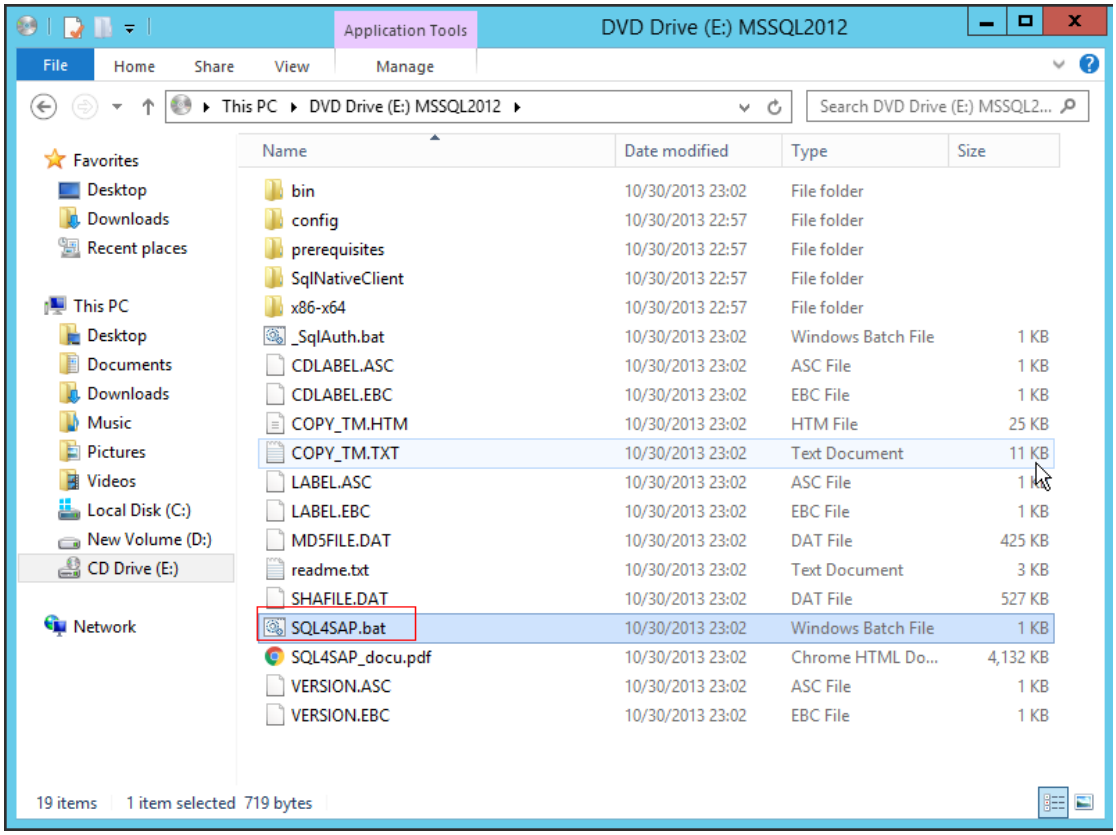
3.5 SAP Software Installation

Download the SAP application and SQL Server installation packages from the official website, upload them to the ECSs, decompress the packages, and start the software installation.

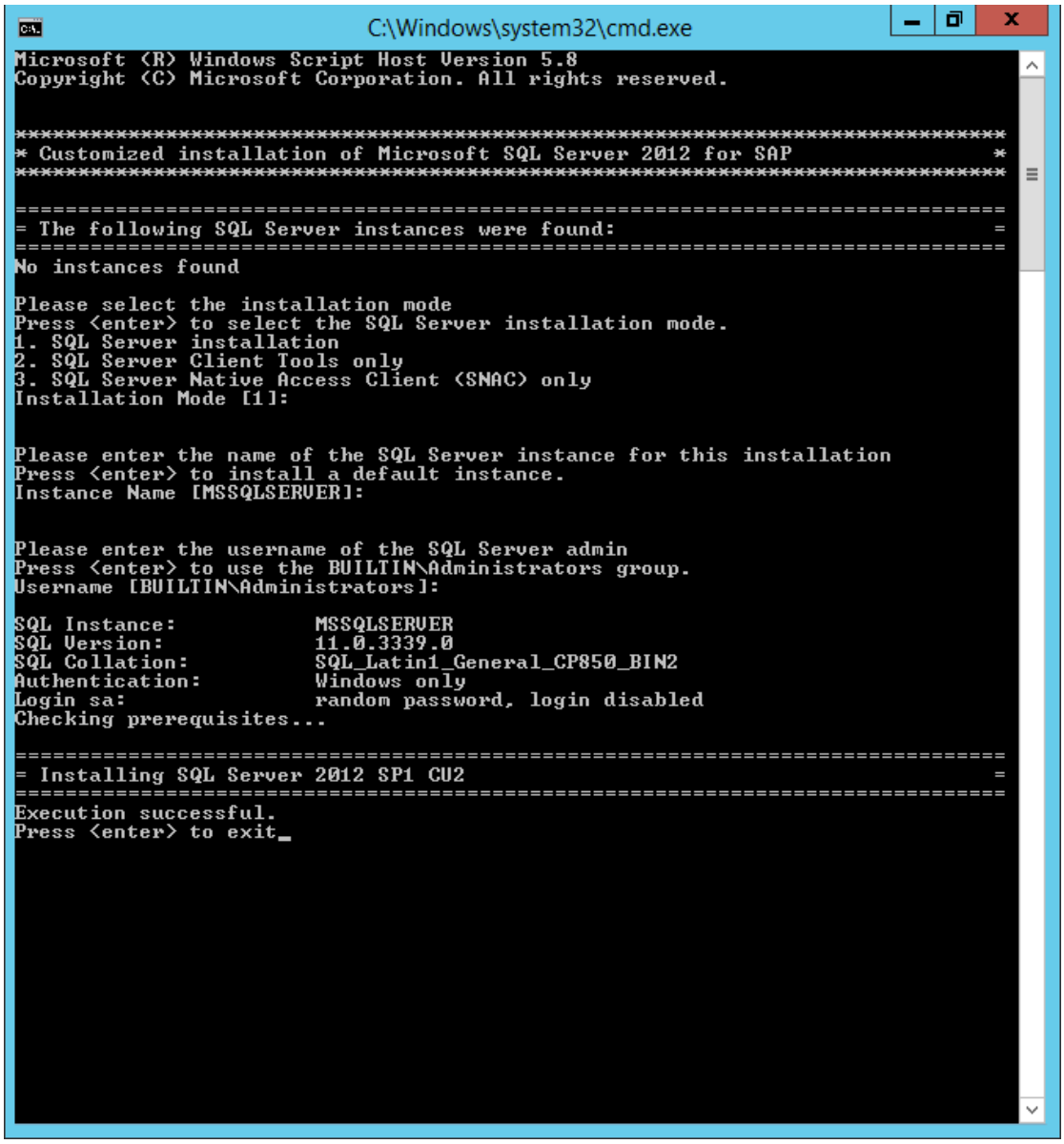
3.5.1 Installing SQL Server Database

Log in to the ECS **ecssap1** where the SAP application and SQL Server are to be deployed. Install the SQL Server and then the SAP application.

Step 1 Click and run the installation program.



Step 2 Retain the default settings, press **Enter**, and wait until the installation is complete.

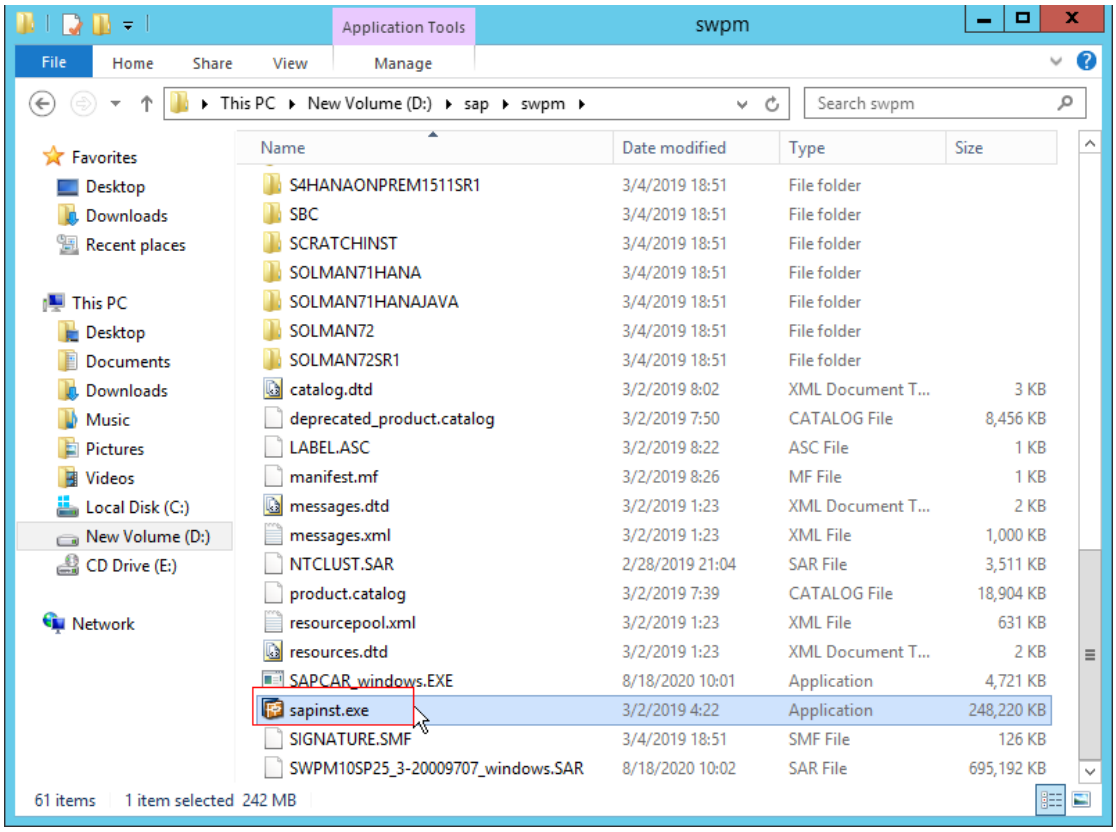


----End

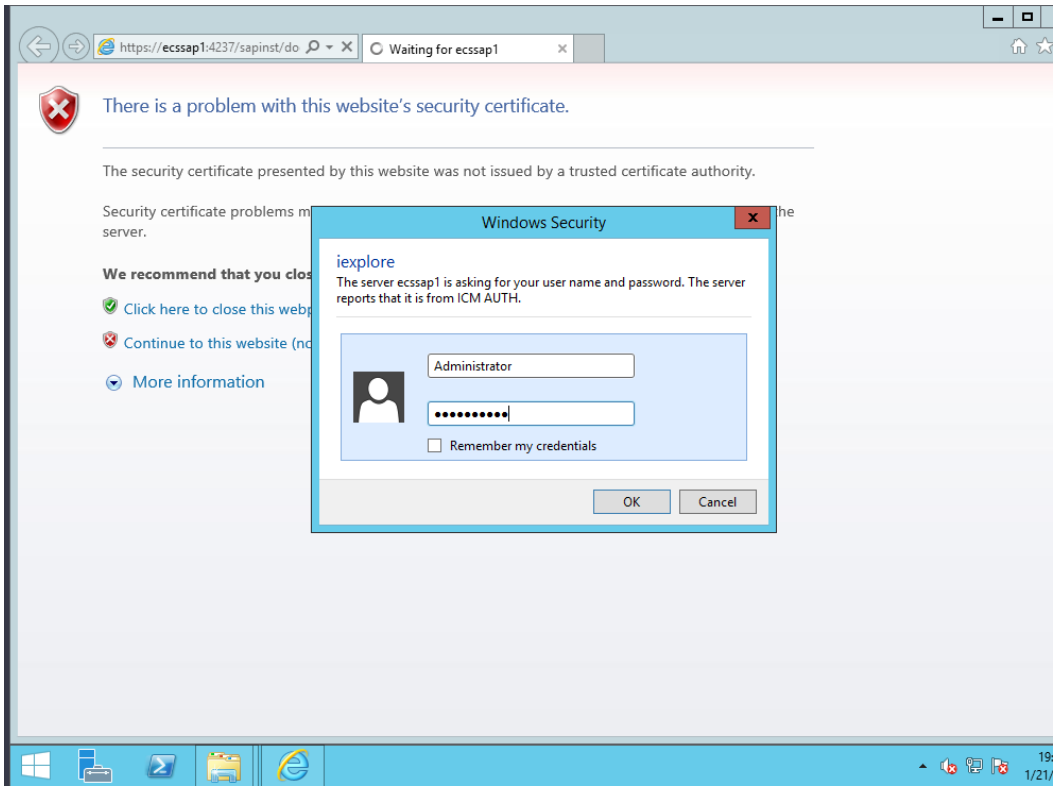
3.5.2 Installing the SAP Application

You need to use a browser to install the SAP application. In this example, Google Chrome is used. Log in to **ecssap1** where the SQL Server is installed and install the SAP application.

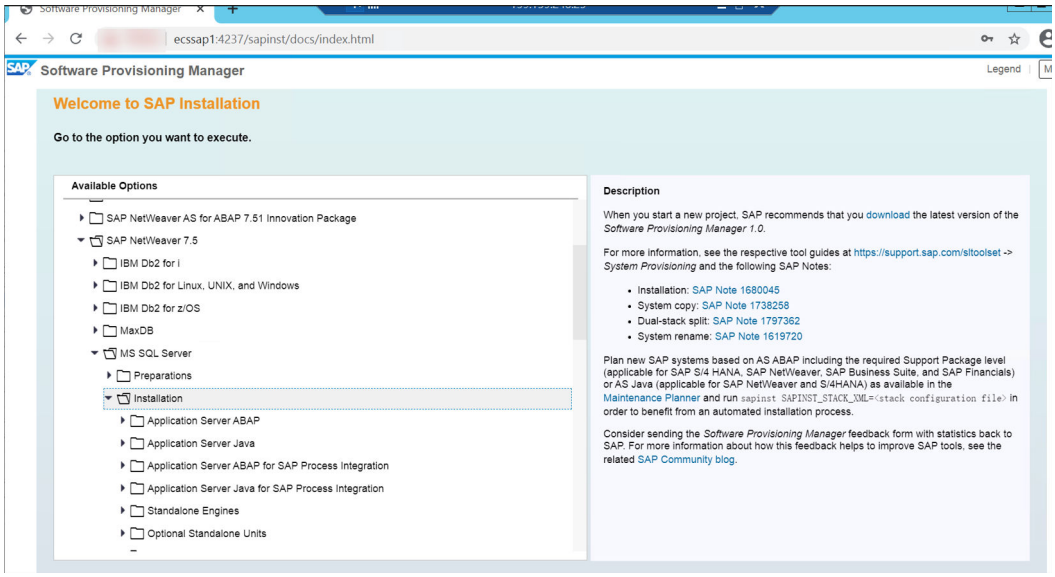
Step 1 Go to the decompressed SAP application installation package, go to the installation directory, and run the installation program.

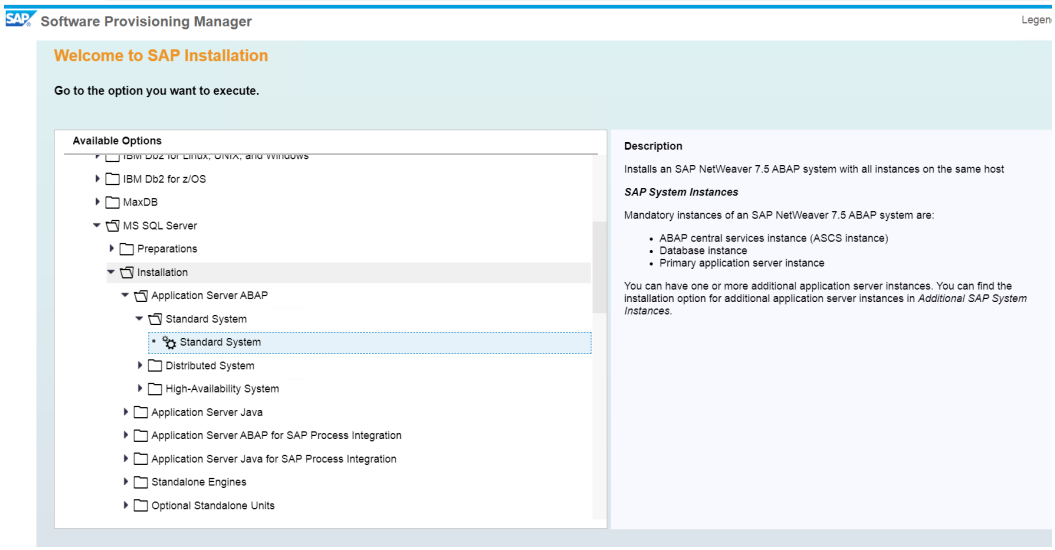


Step 2 Enter your username and password.

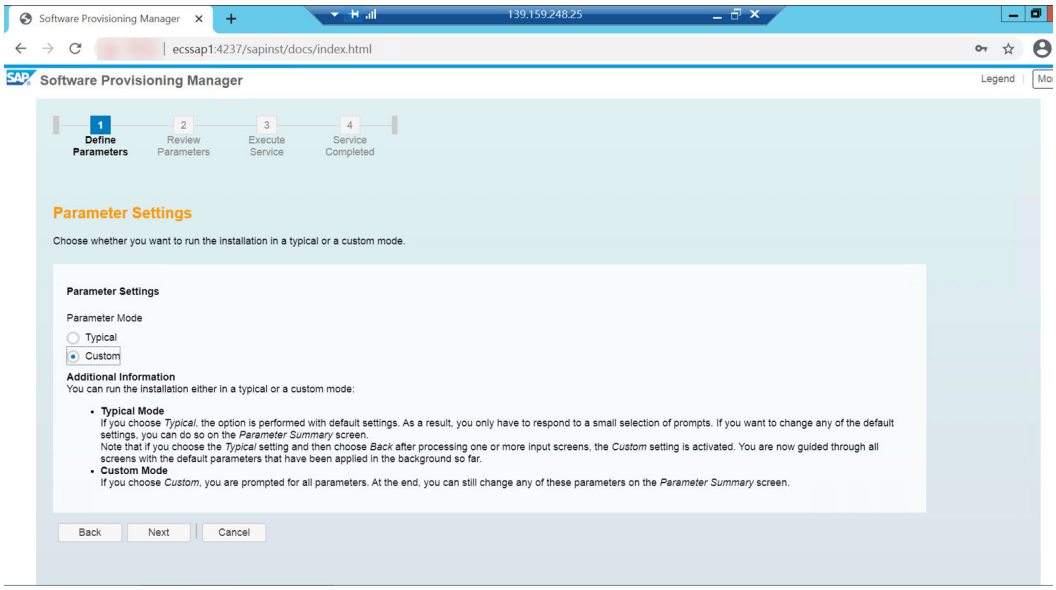


Step 3 Select **SAP NetWeaver 7.5/MS SQL Server/Installation/Application Server ABAP/Standard System**, click **Next**, and then **Next**.

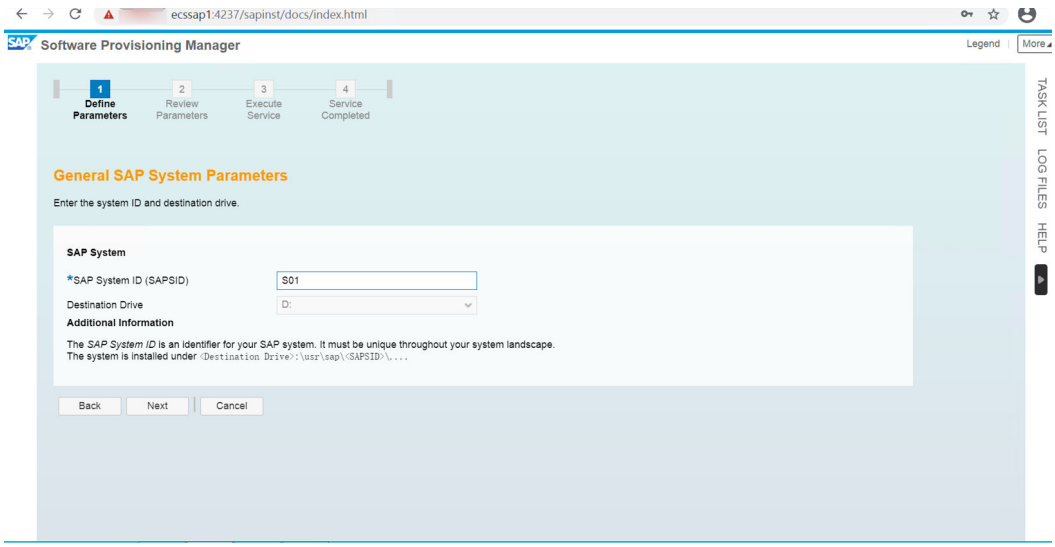




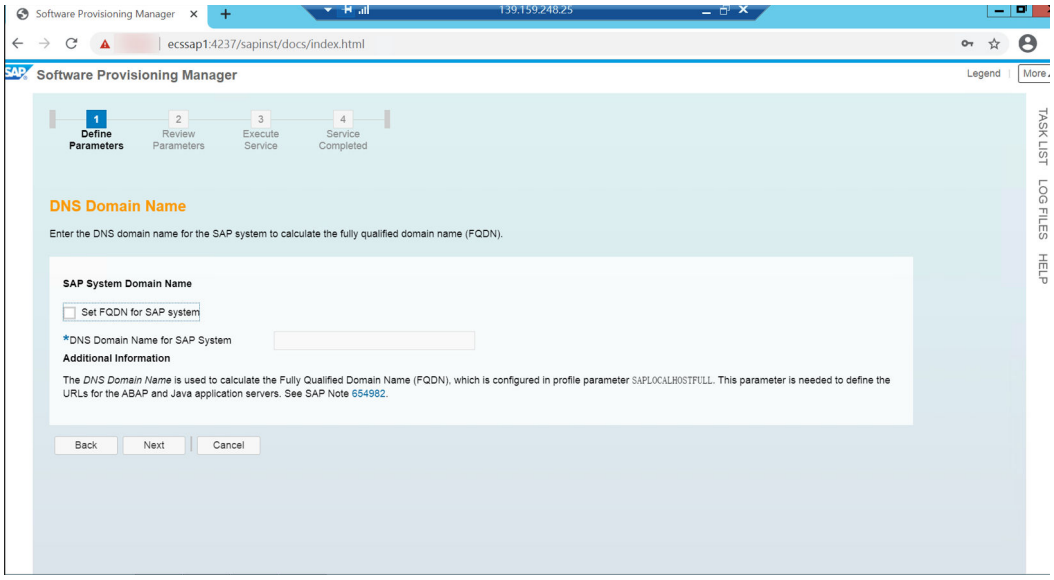
Step 4 Select **Custom** and click **Next**.



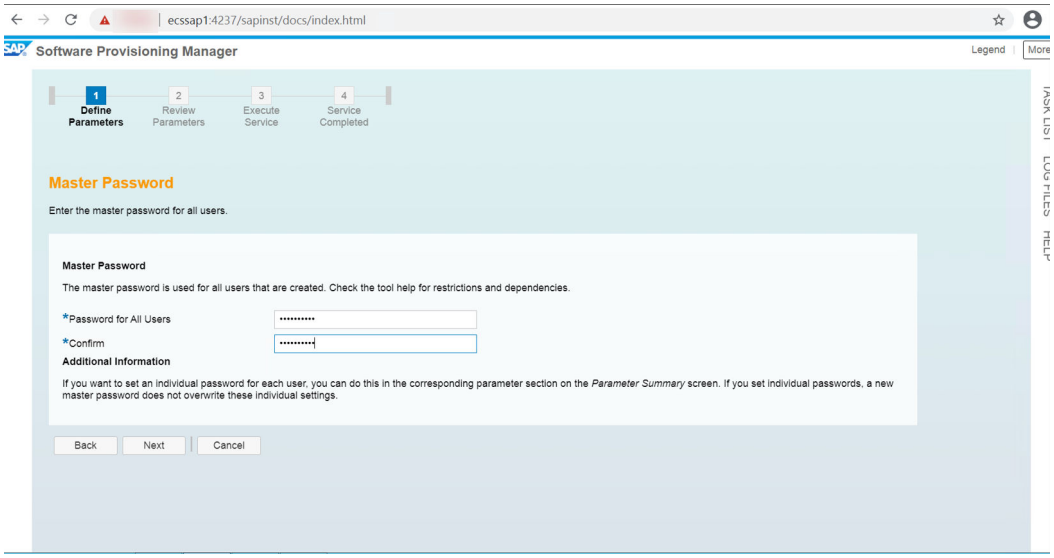
Step 5 Enter the SAP system ID and click **Next**.



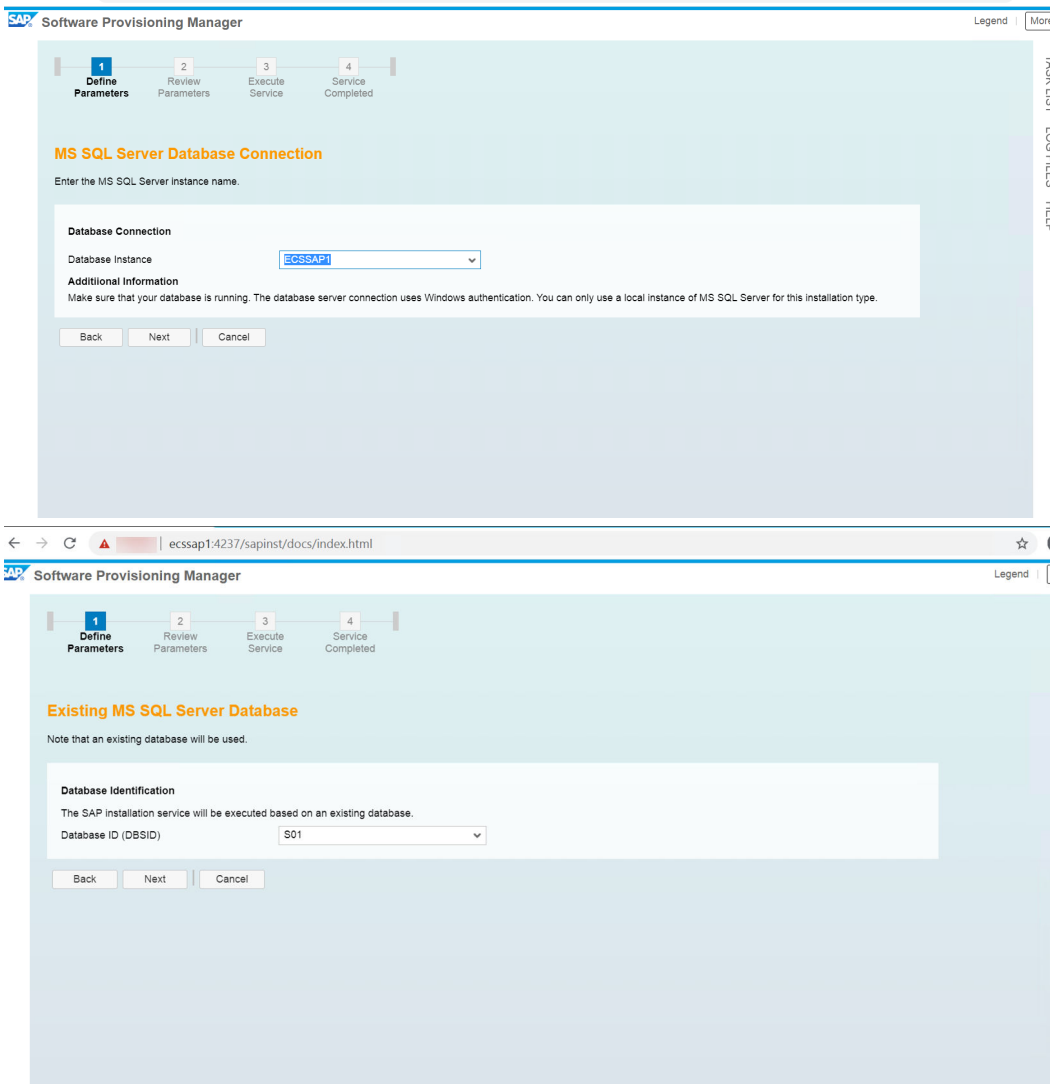
Step 6 Deselect **Set FQDN for SAP System** and click **Next**.



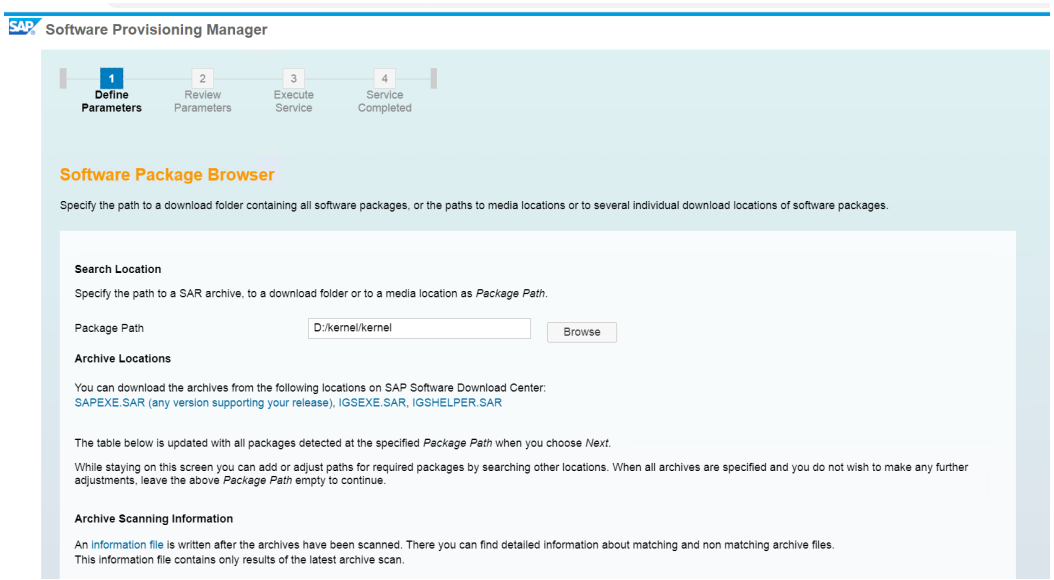
Step 7 Set the password and click **Next**.



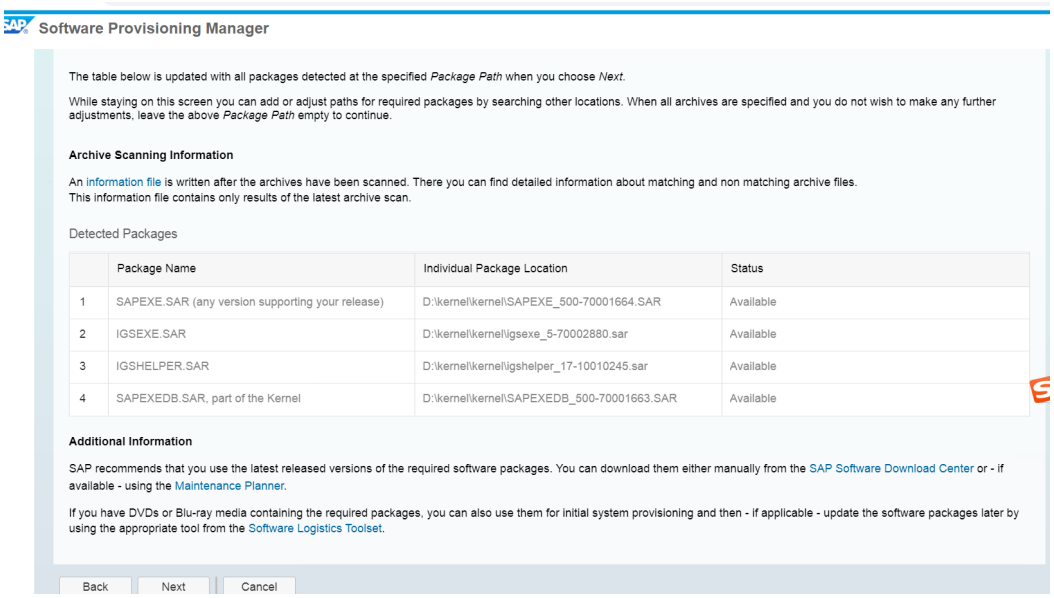
Step 8 Retain the default settings and click **Next**.



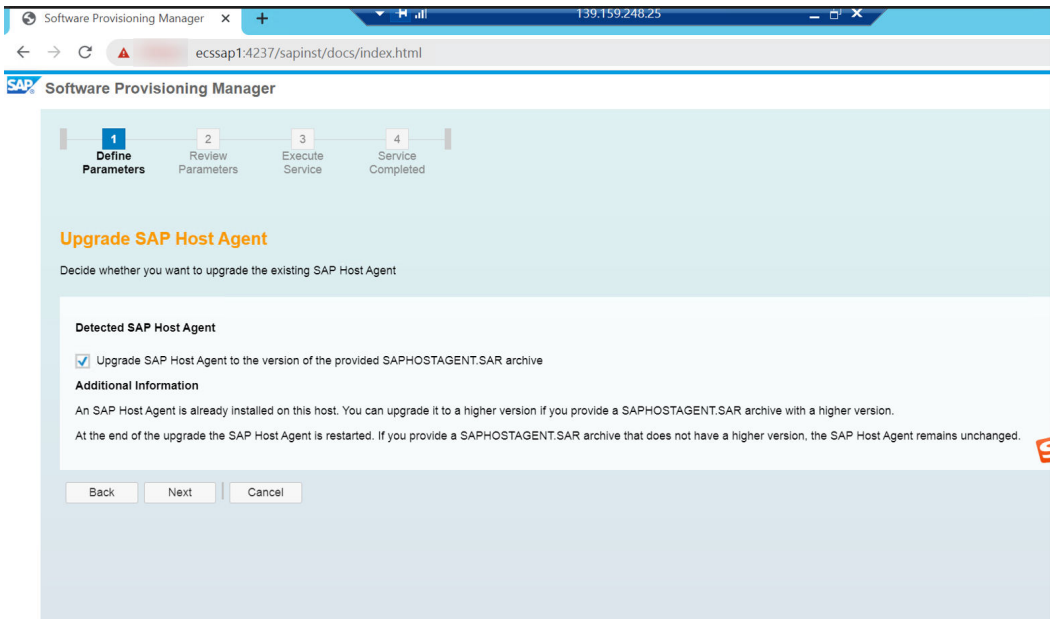
Step 9 Specify the package path and click **Next**.



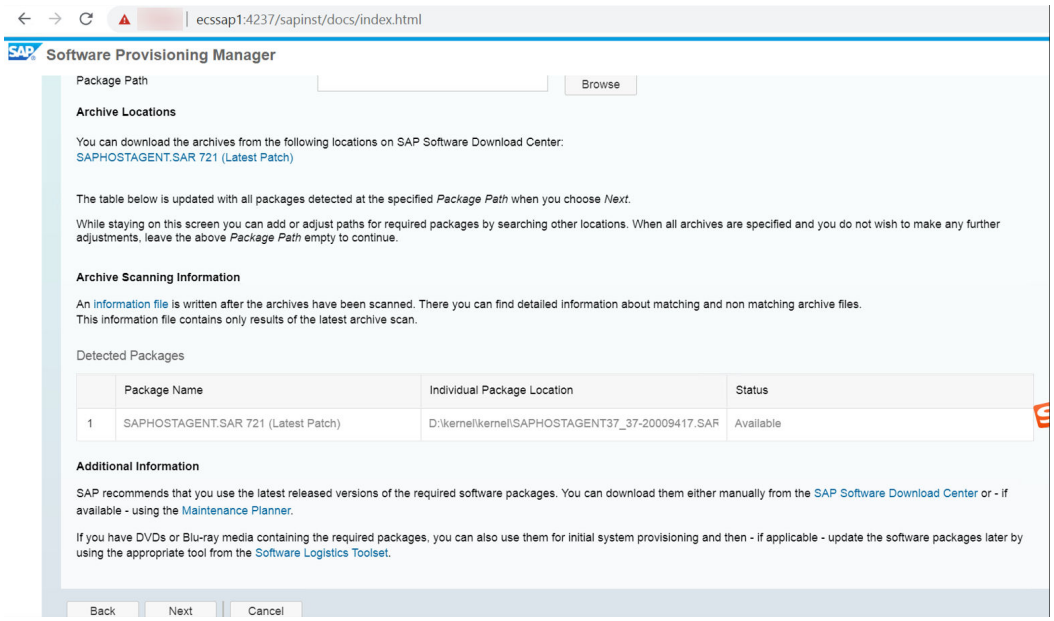
Step 10 The required packages are located, and click **Next**.



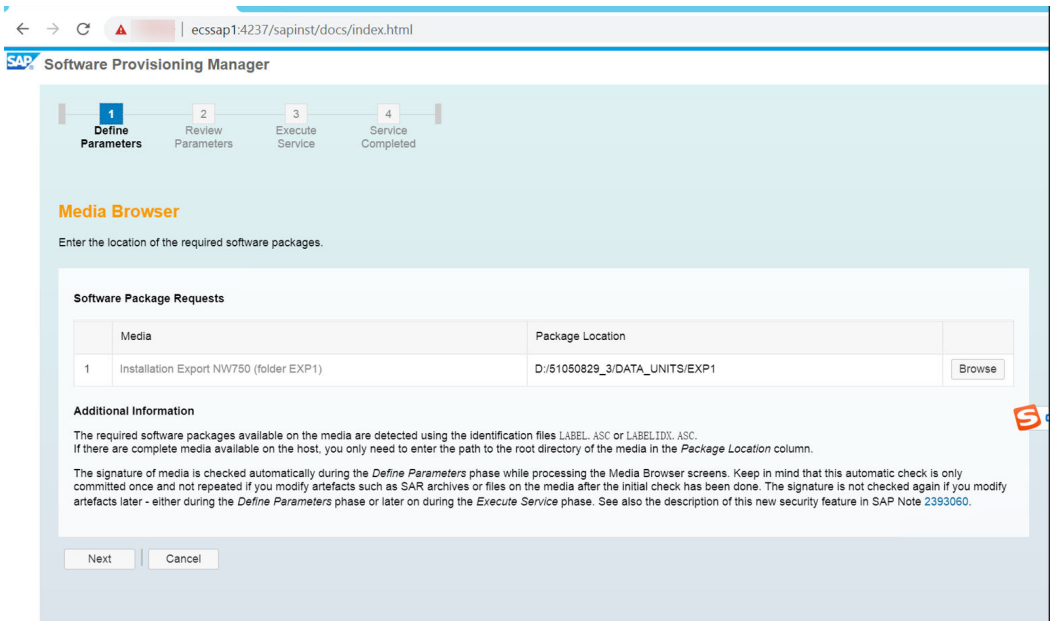
Step 11 Retain the default settings and click **Next**.



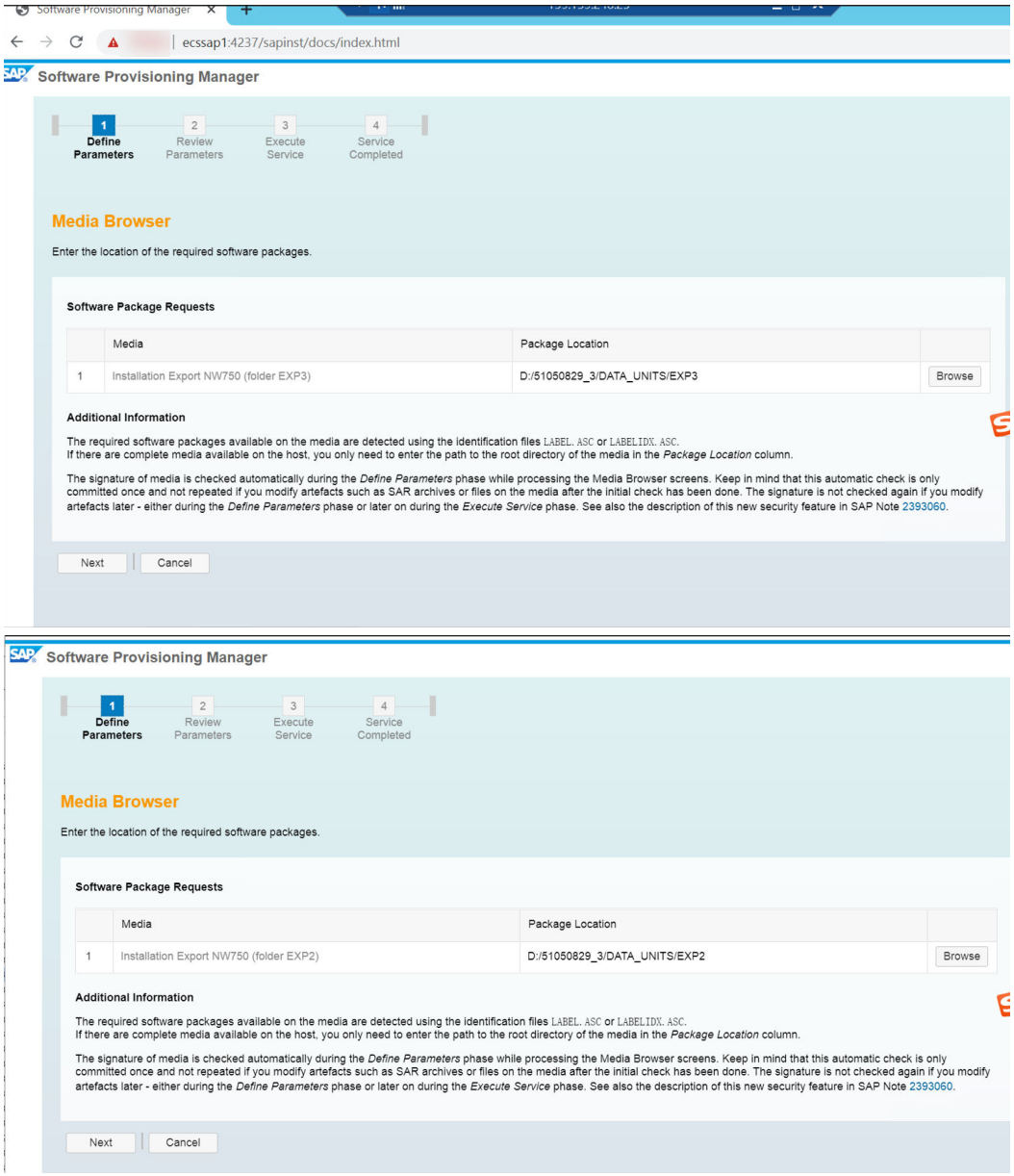
Step 12 Click **Next**.



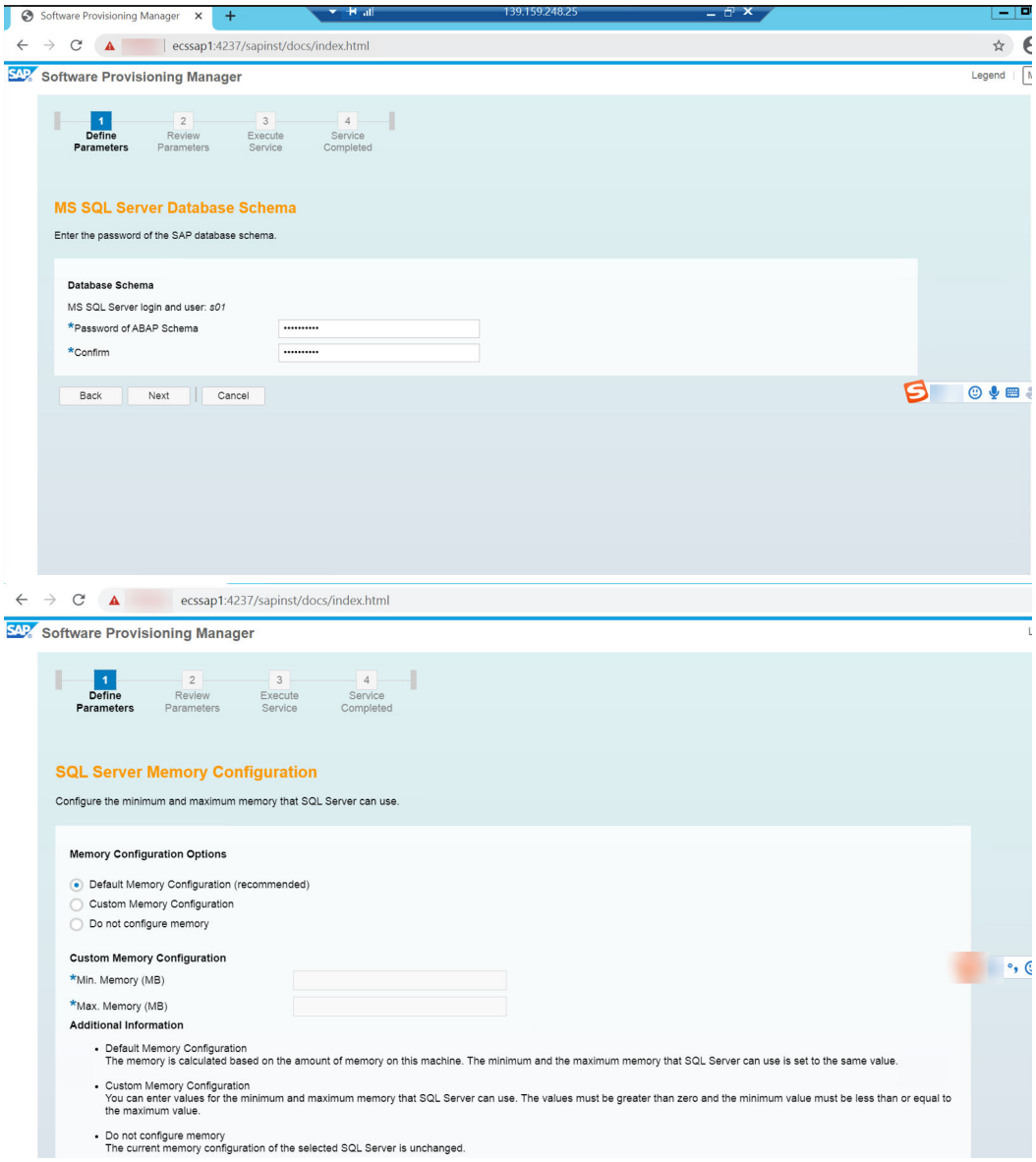
Step 13 Specify the package path, and then click **Next**.



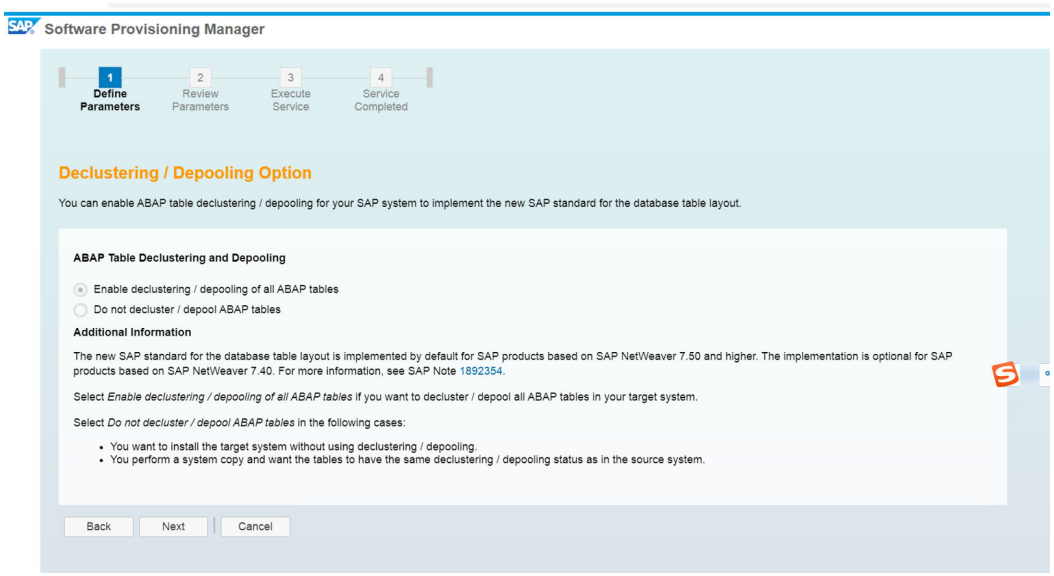
Step 14 Specify the package path, and then click **Next**.



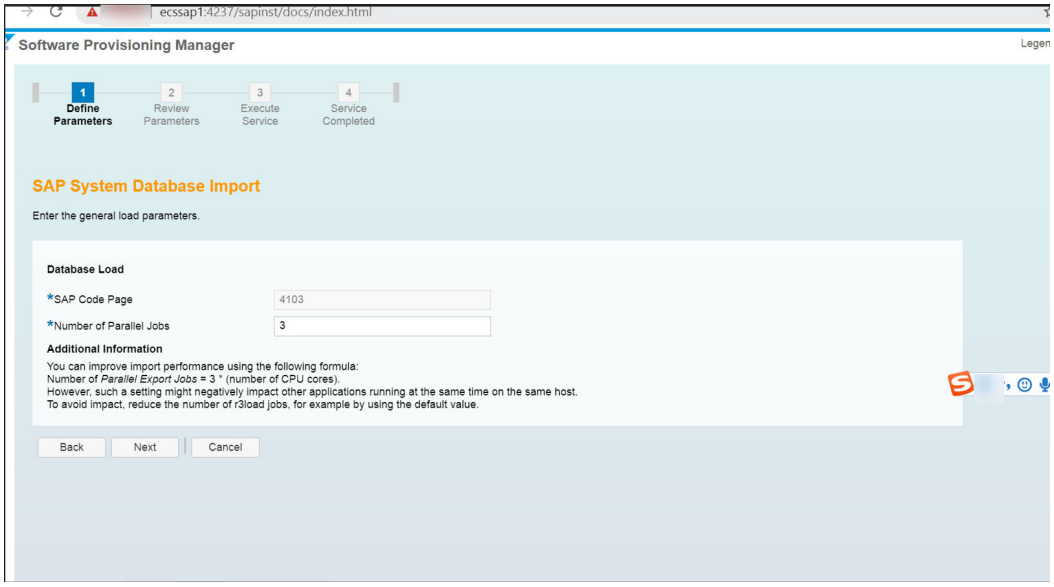
Step 15 Retain the default settings and click **Next**.



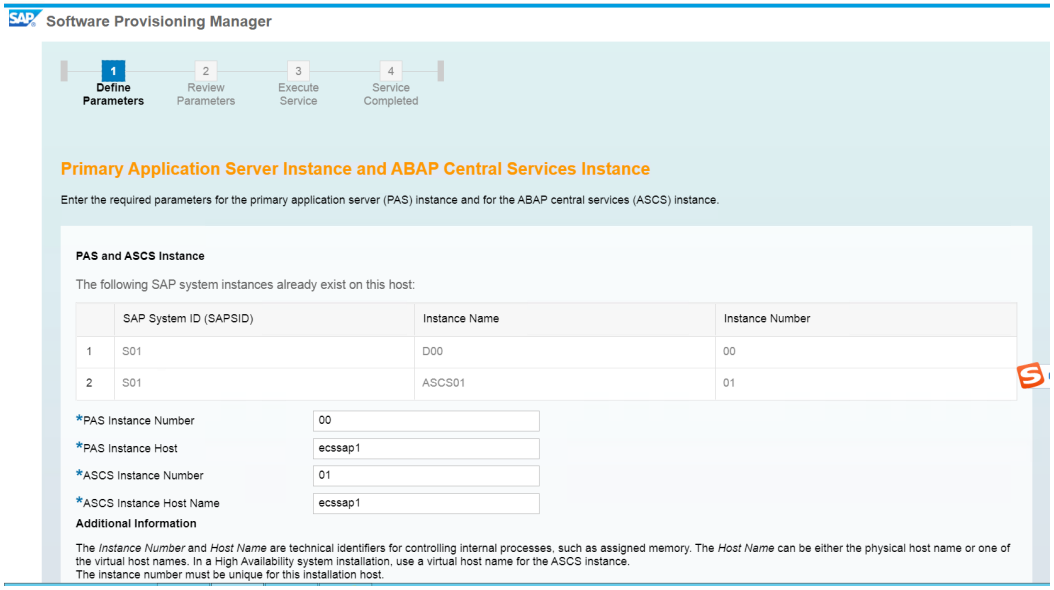
Step 16 Retain the default settings and click **Next**.

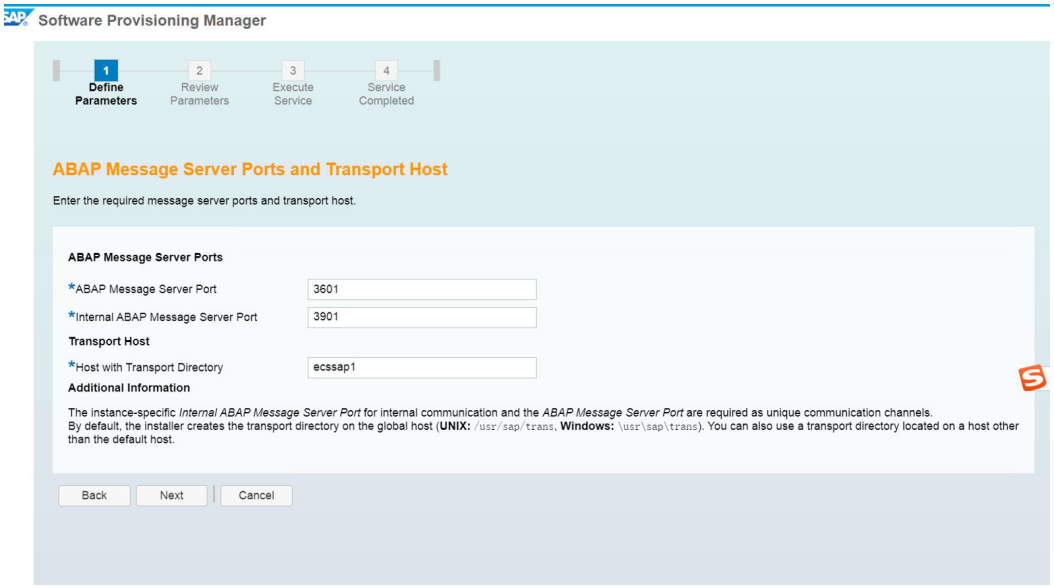


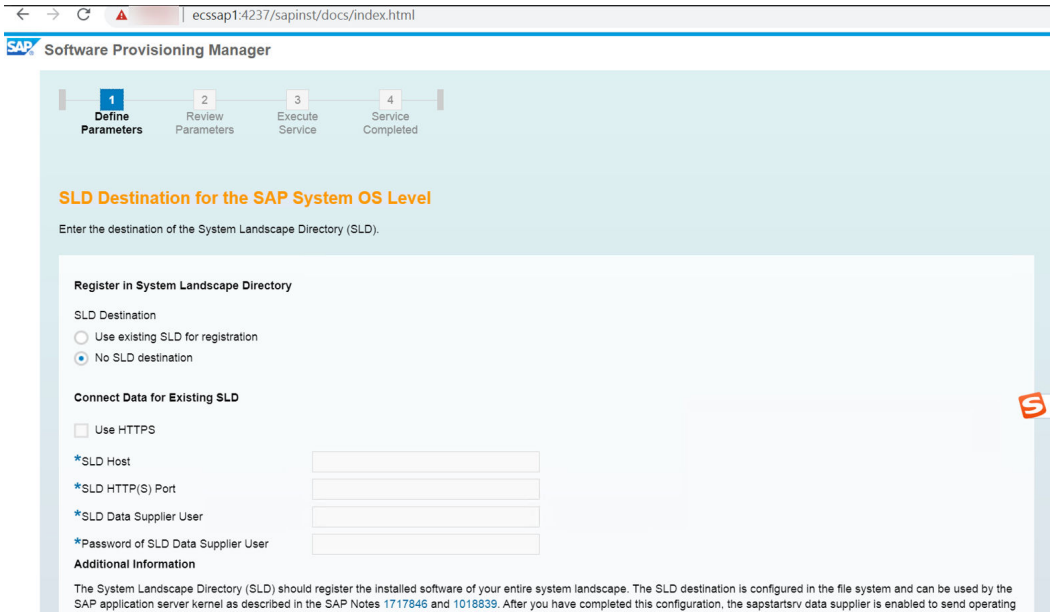
Step 17 Retain the default settings and click **Next**.

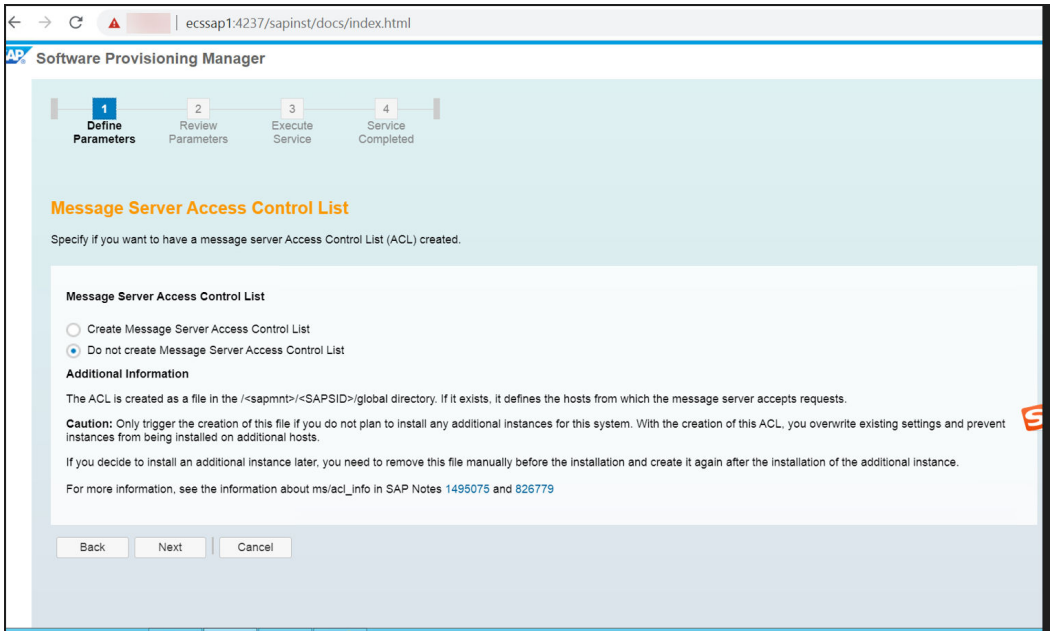


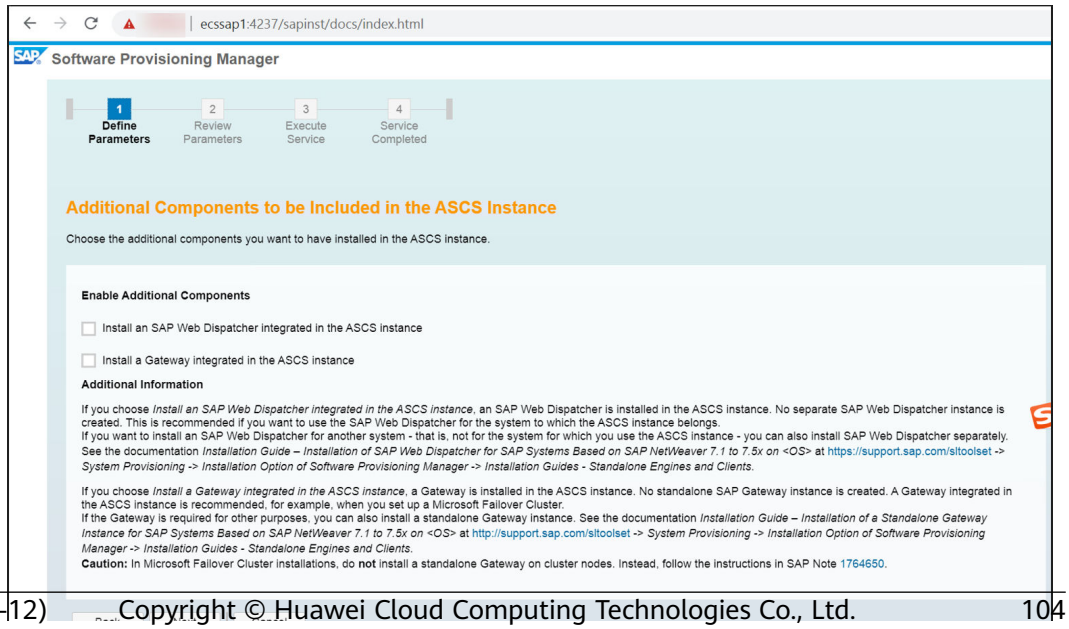
Step 18 Configure the PAS and ASCS instance numbers and host names and click **Next**.



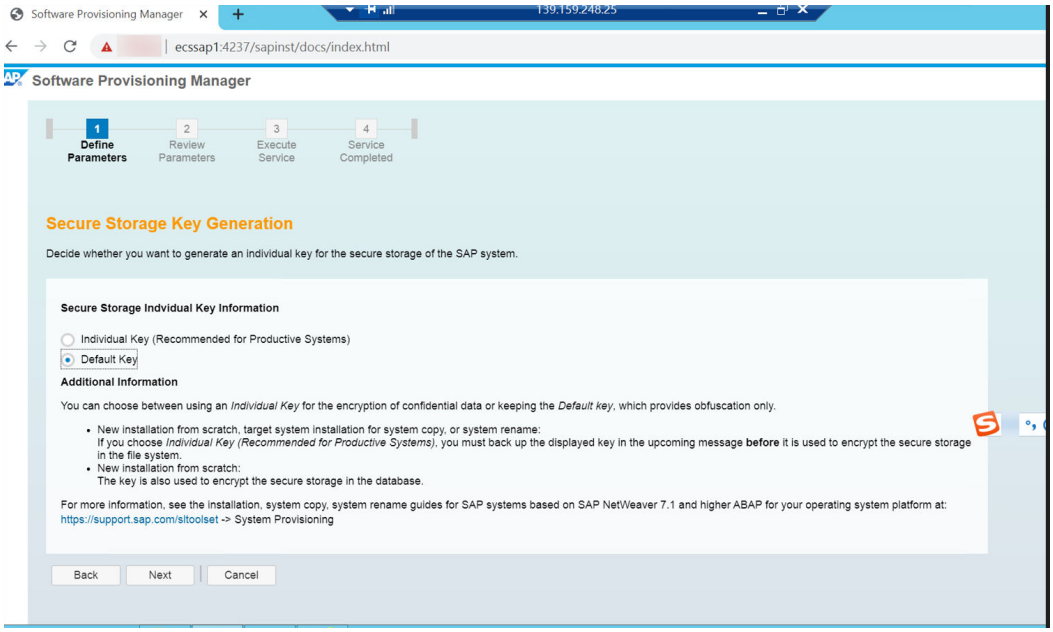




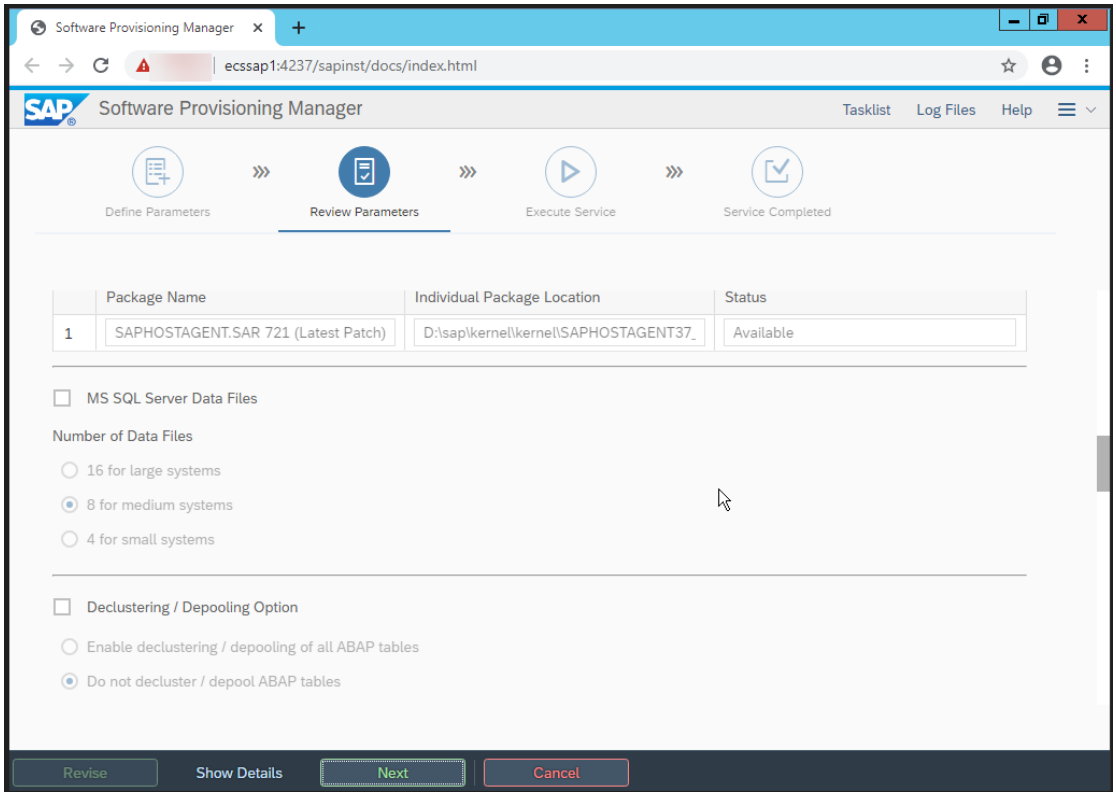




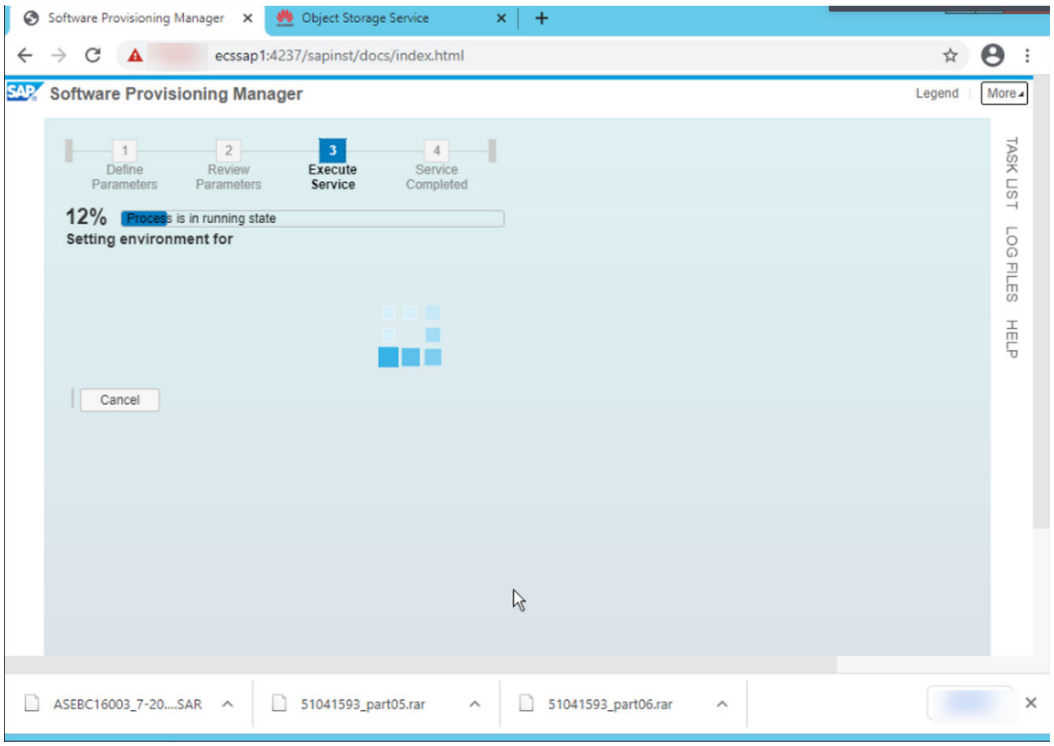
Step 19 Select **Default Key** and click **Next**.

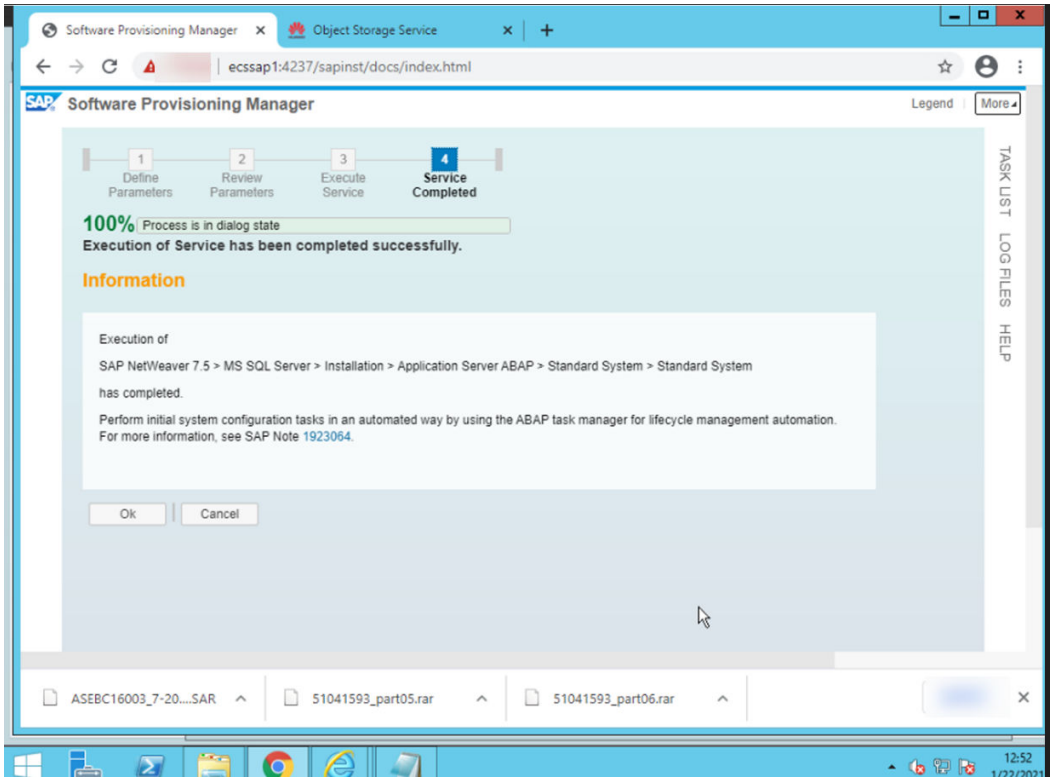


Step 20 Confirm the parameters and click **Next**.



Step 21 Wait until the installation is complete.



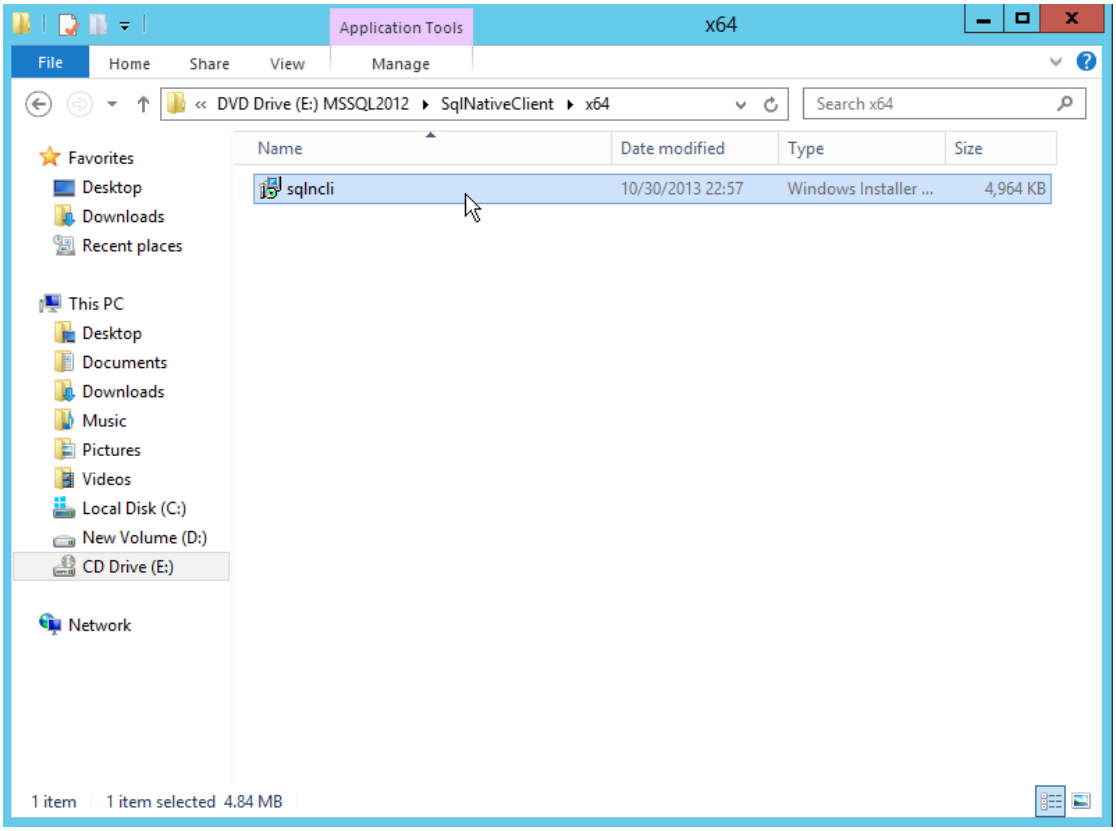


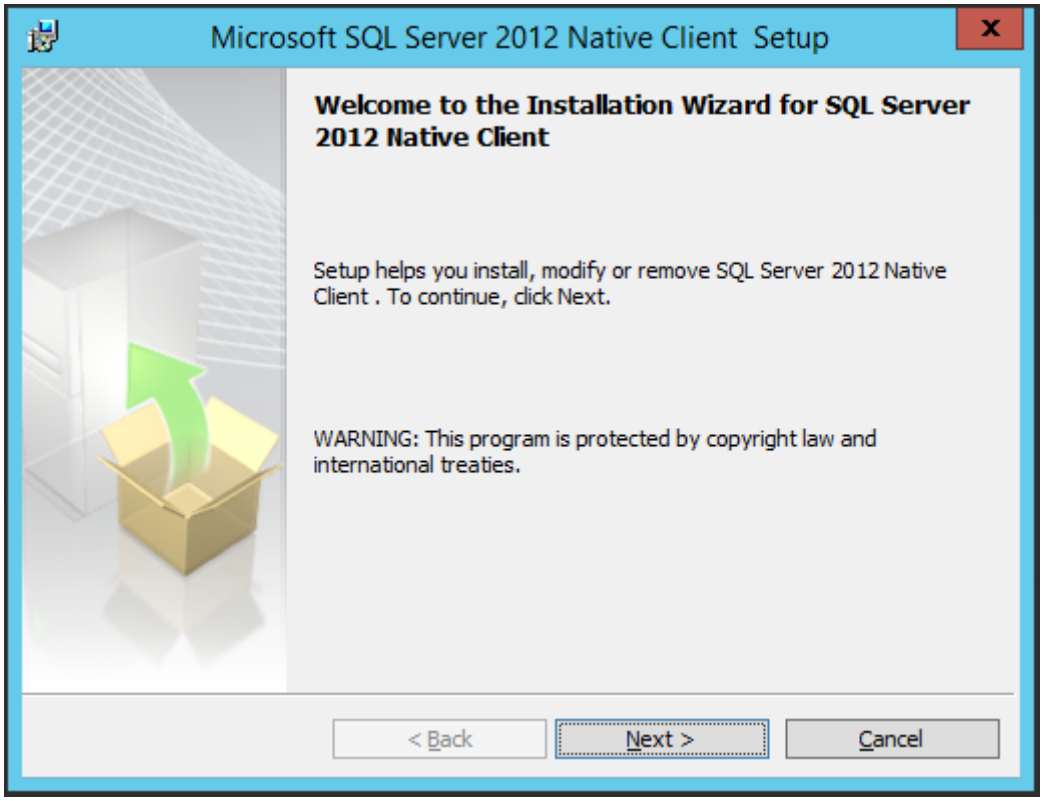
----End

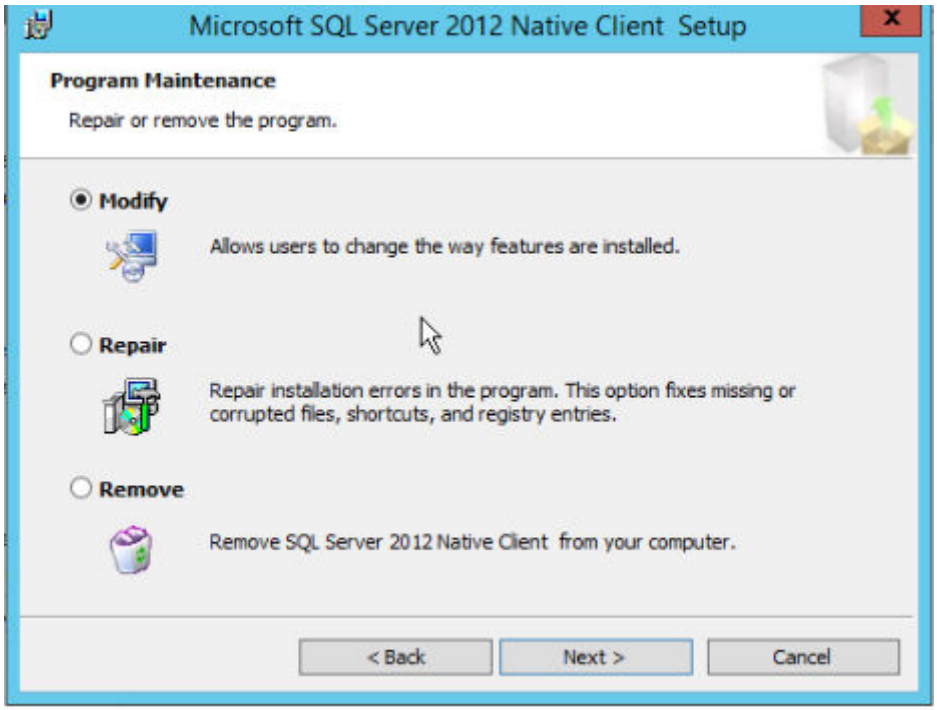
3.5.3 Installing the SQL Server Client

Log in to the ECS **ecssap2** where the AAS is to be installed. Install the SQL Server Client and then AAS.

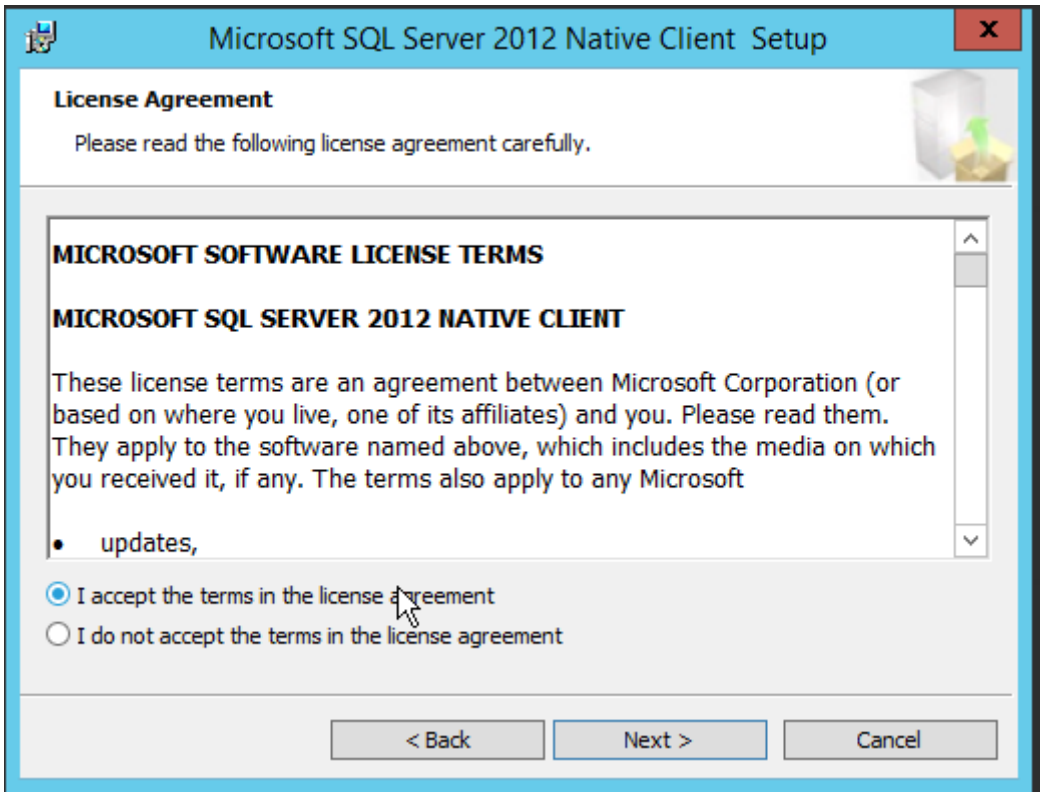
1. Go to the SQL Server Client installation directory and run the installation program.



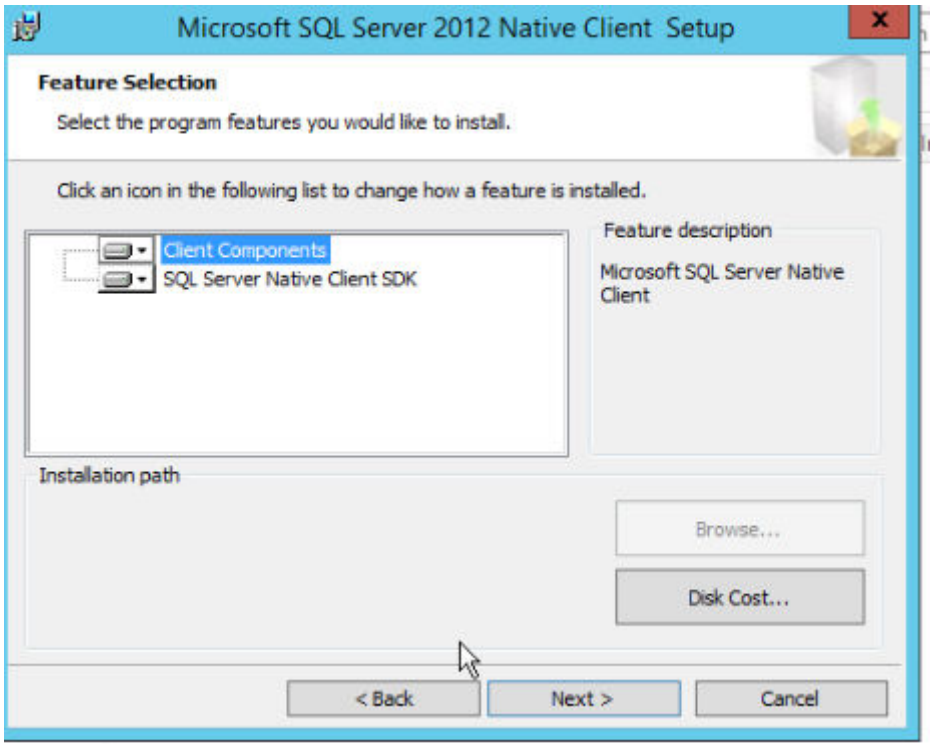




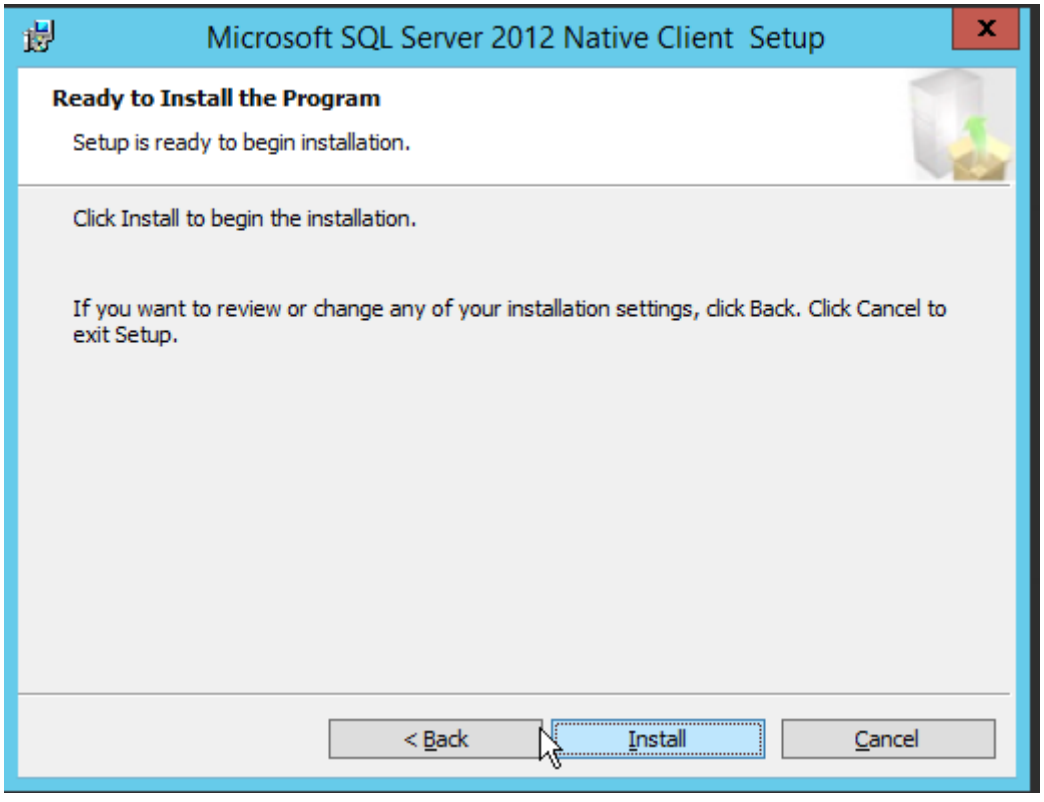
2. Select **I accept the terms in the license agreement**, and click **Next**.



3. Retain the default settings and click **Next**.



4. Click **Install**.

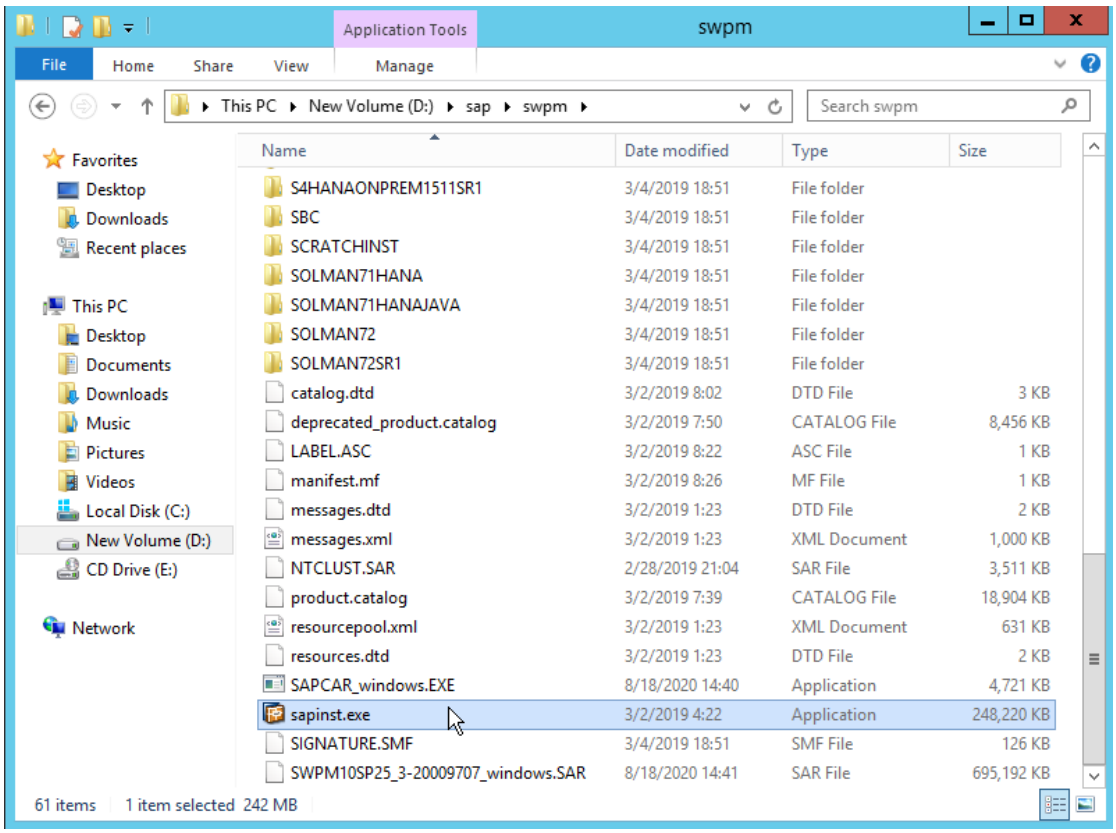


3.5.4 Installing AAS

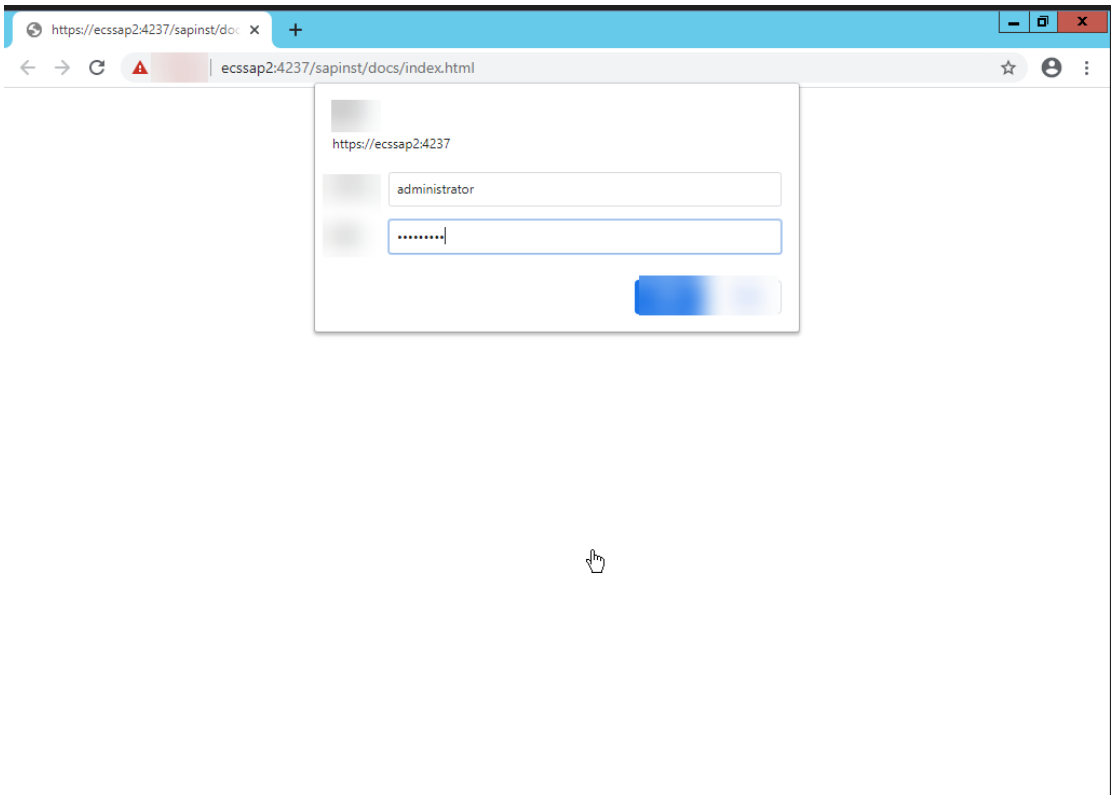
Log in to the ECS **ecssap2** where the SQL Server Client has been installed and install AAS.

Go to the SAP AAS installation directory and run the installation program.

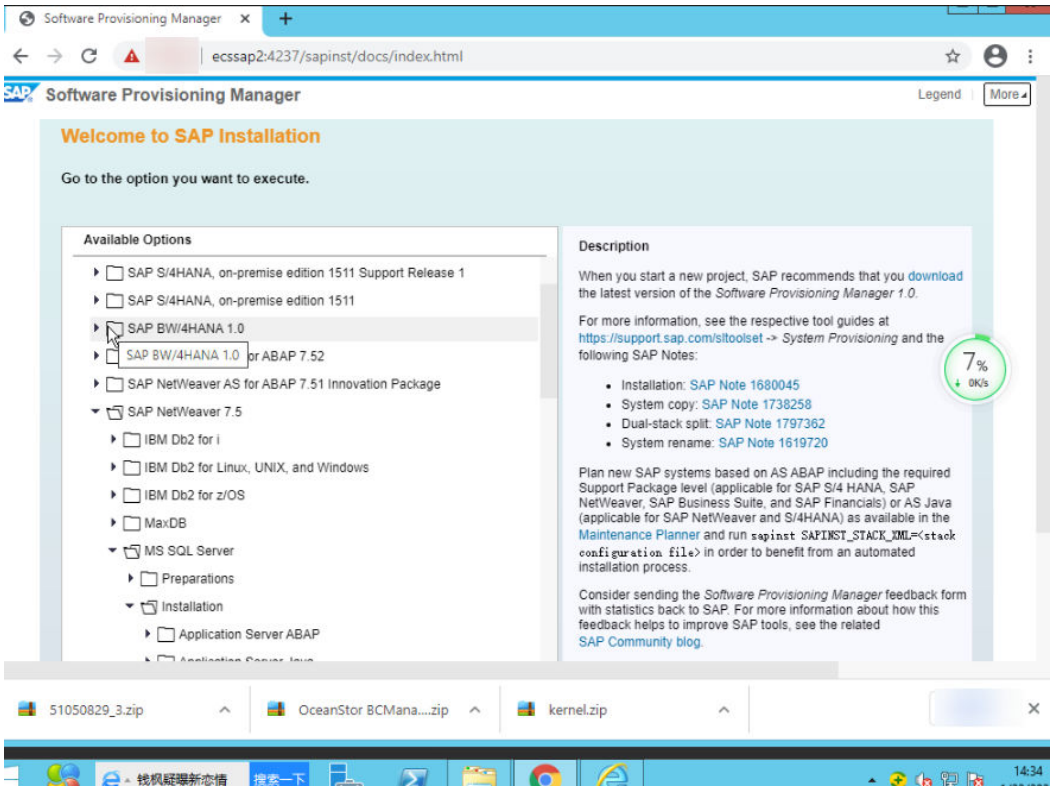
Step 1 Run the installation program.

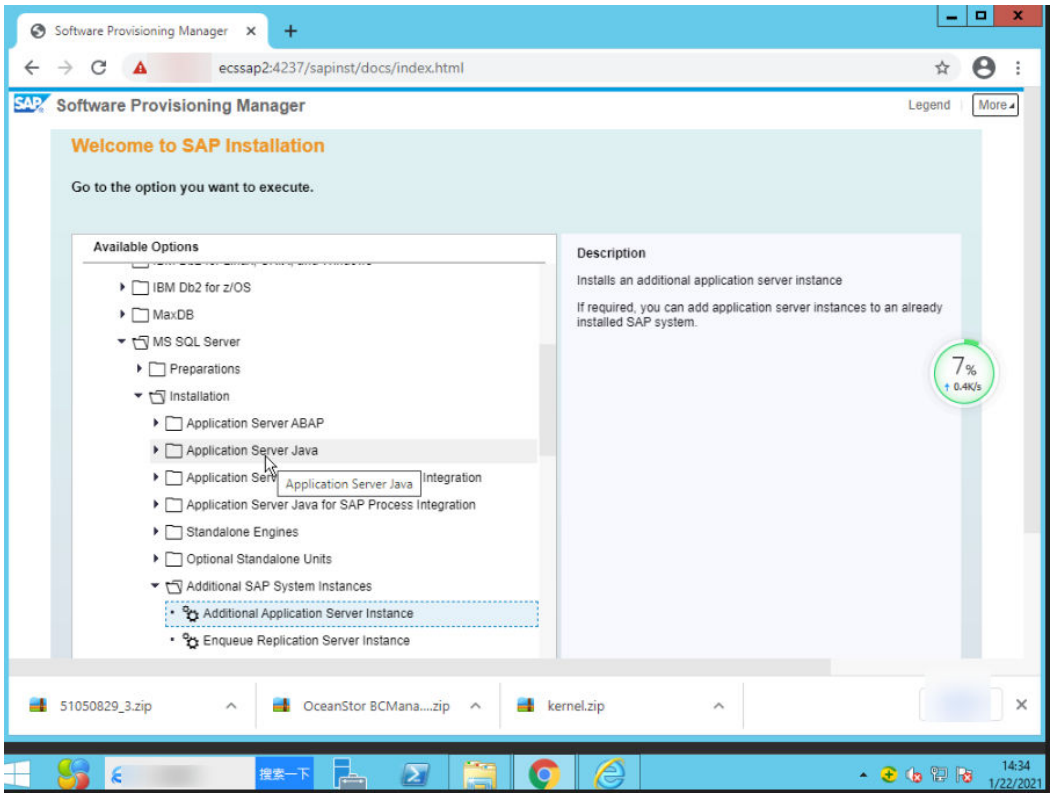


Step 2 Enter the username and password to log in.

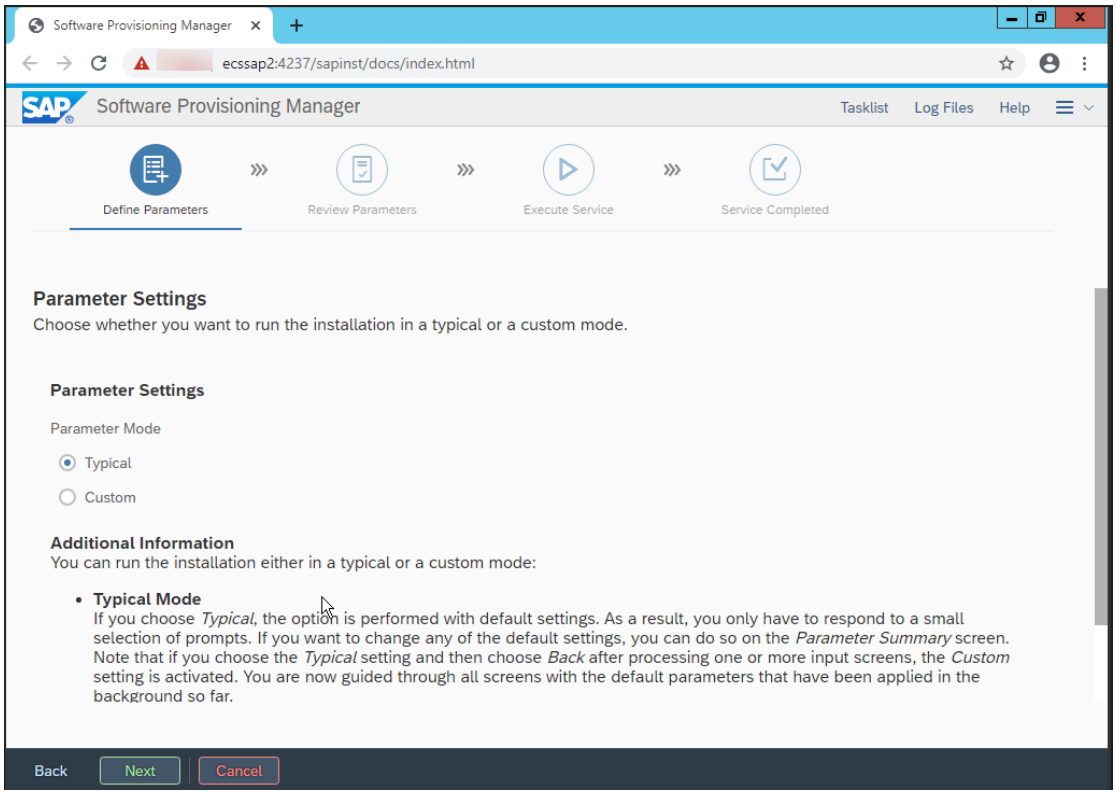


Step 3 Select **SAP NetWeaver 7.5/MS SQL Server/Installation/Additional SAP System Instance/Additional Application Server Instance** and click **Next**.

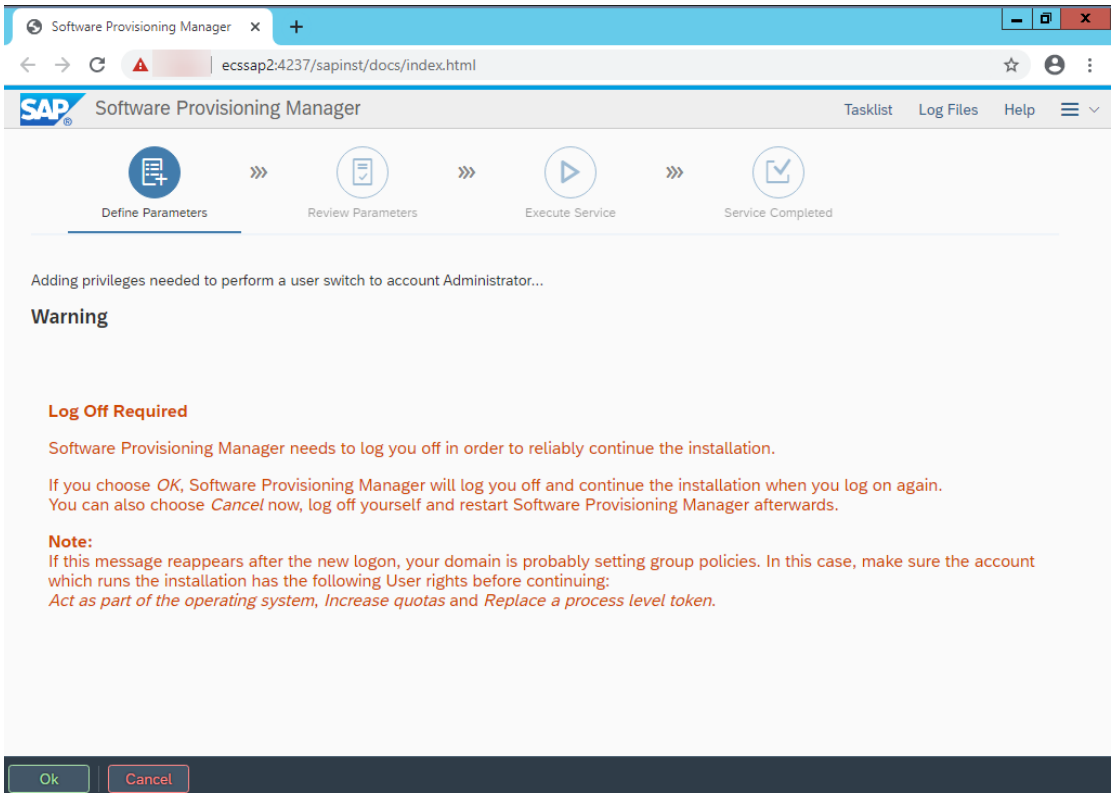




Step 4 Select **Custom** and click **Next**.



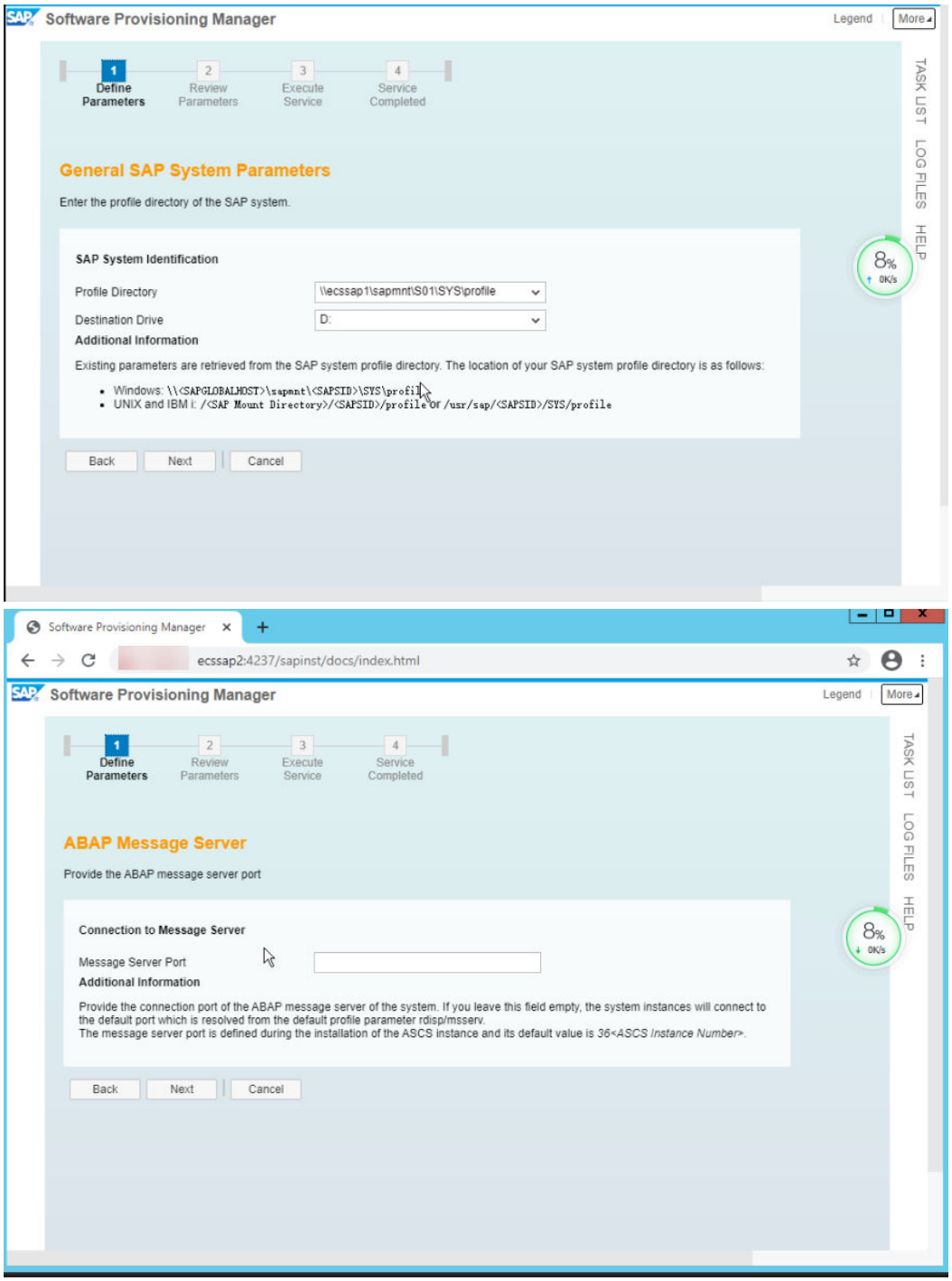
Step 5 You will log out of the ECS after clicking **OK**. You need to log in to the ECS again. After the login, the SAP installation program automatically runs and continues to install the SAP application.



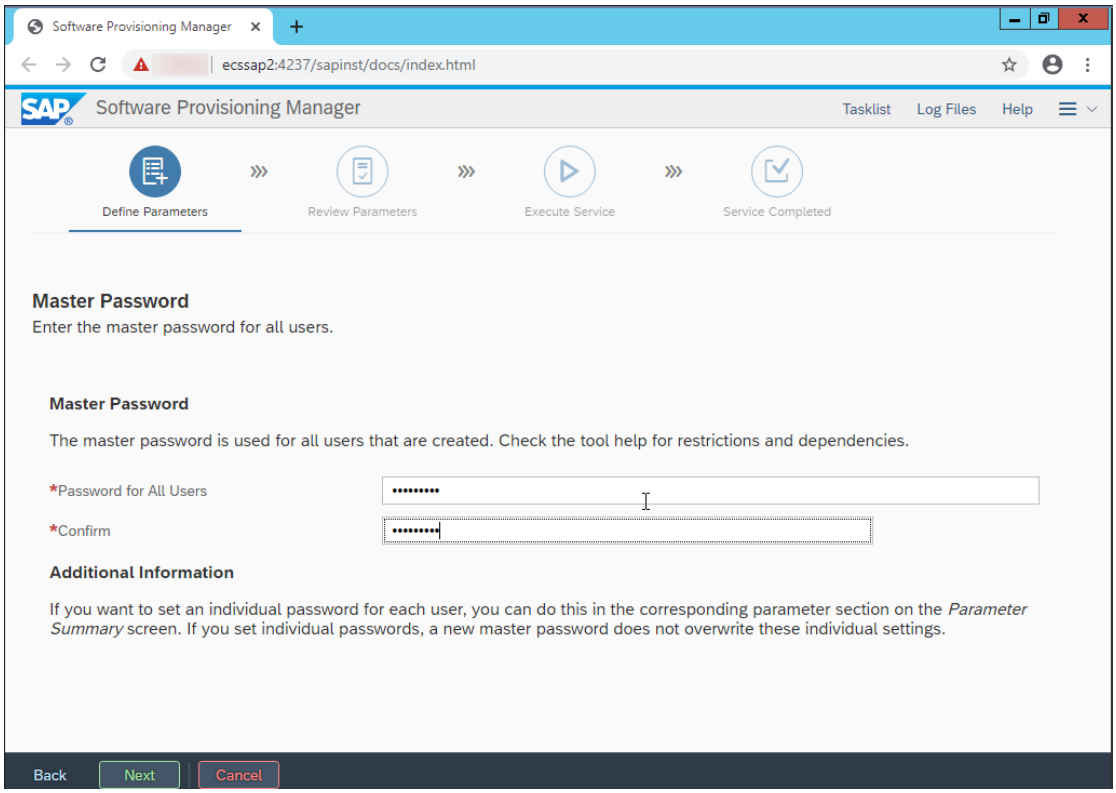
Step 6 Enter the username and password to log in and continue the installation.

Step 7 Find the location of the profile file on **ecssap1**. The profile file location is automatically shared in Windows OS. Write the profile file directory in the following format and click **Next**.

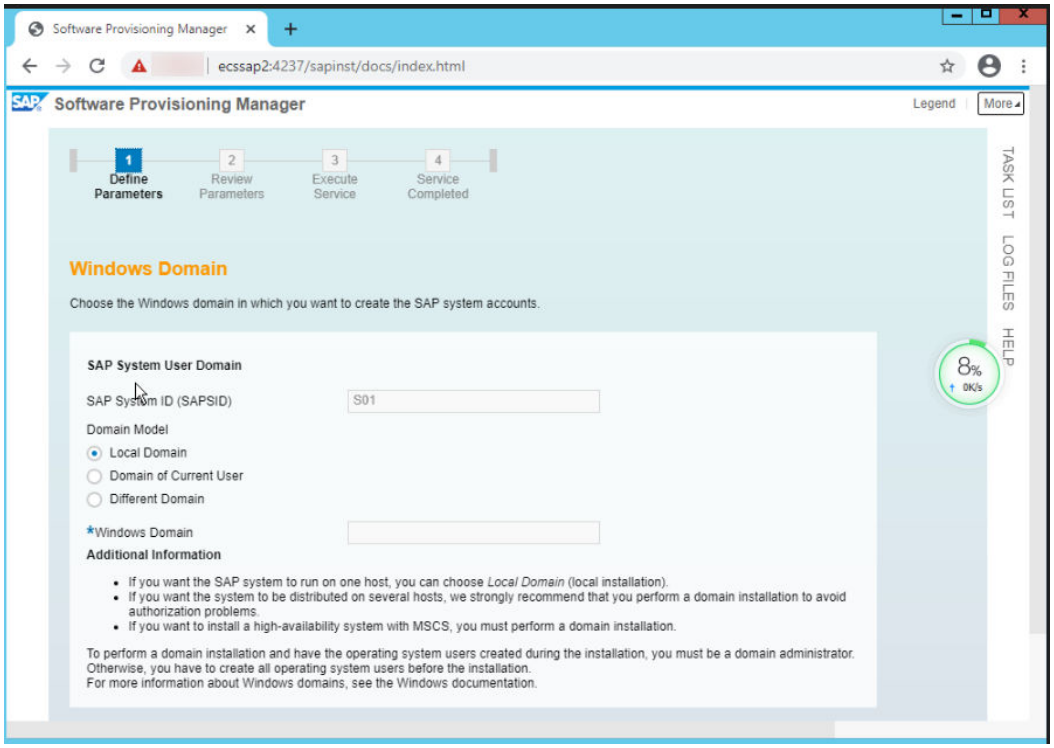
\\ecssap1\sapmnt\S01\SYS\profile



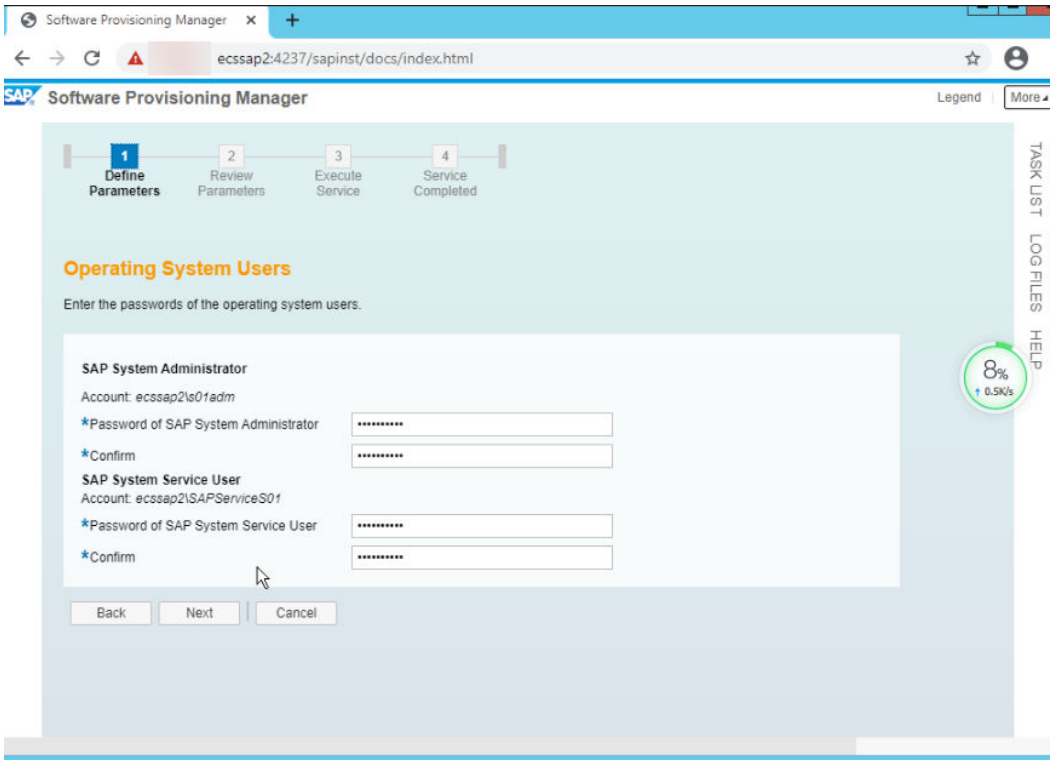
Step 8 Set the password and click **Next**.



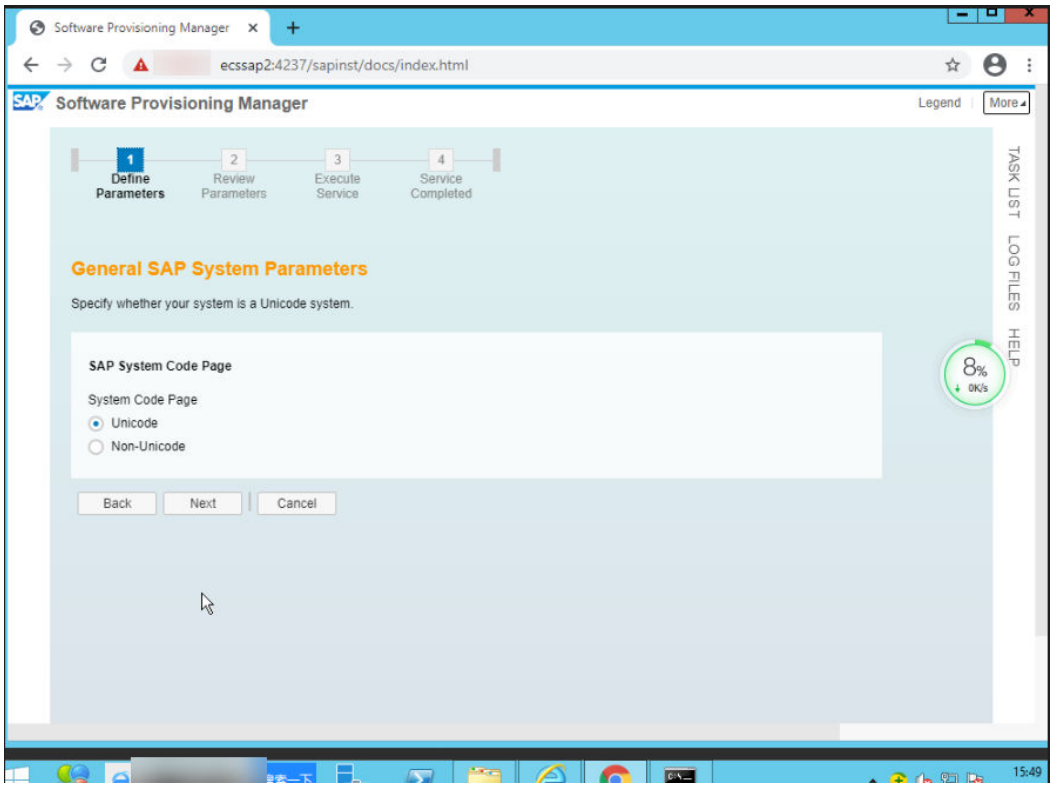
Step 9 Retain the default settings and click **Next**.

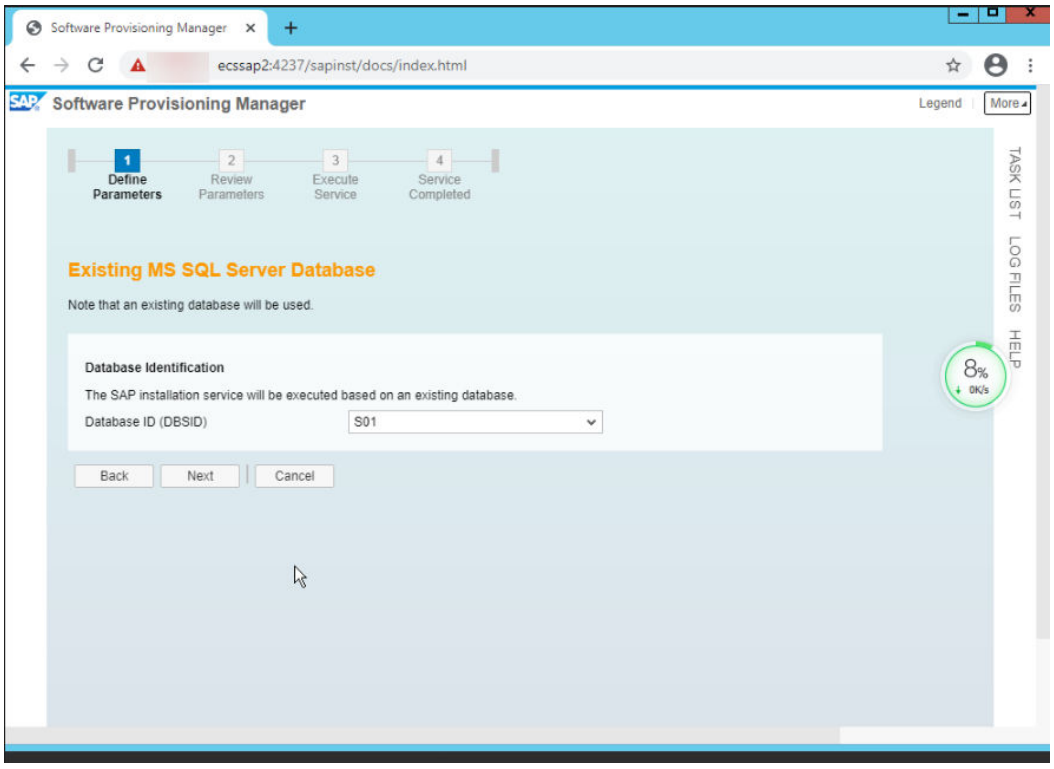


Step 10 Retain the default settings and click **Next**.

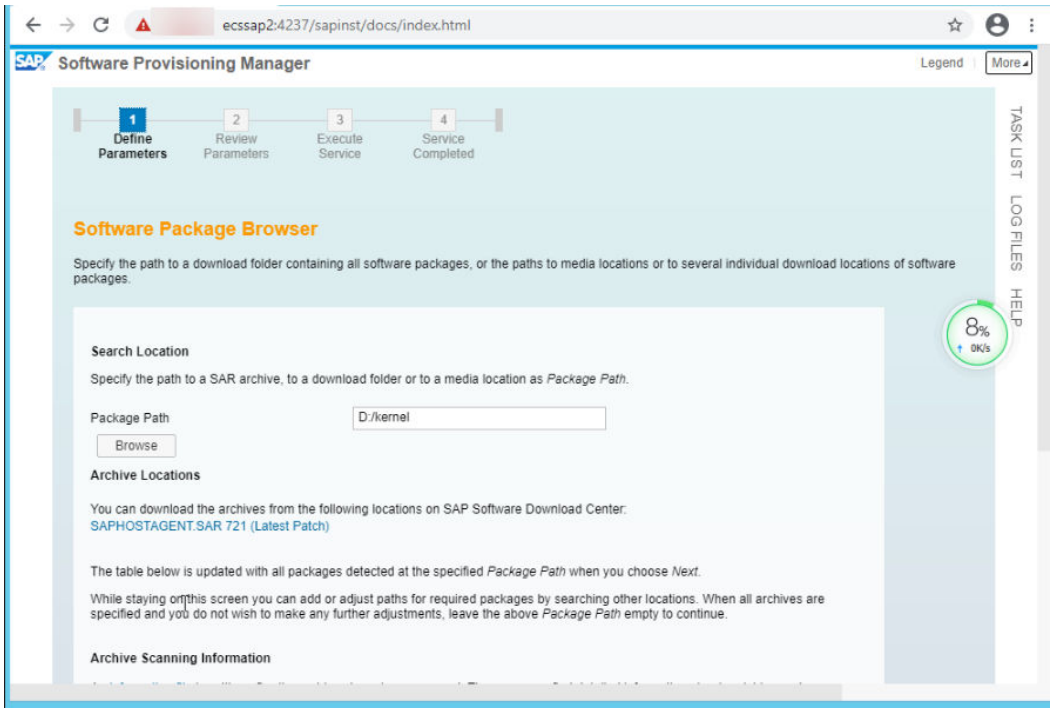


Step 11 Retain the default settings and click **Next**.

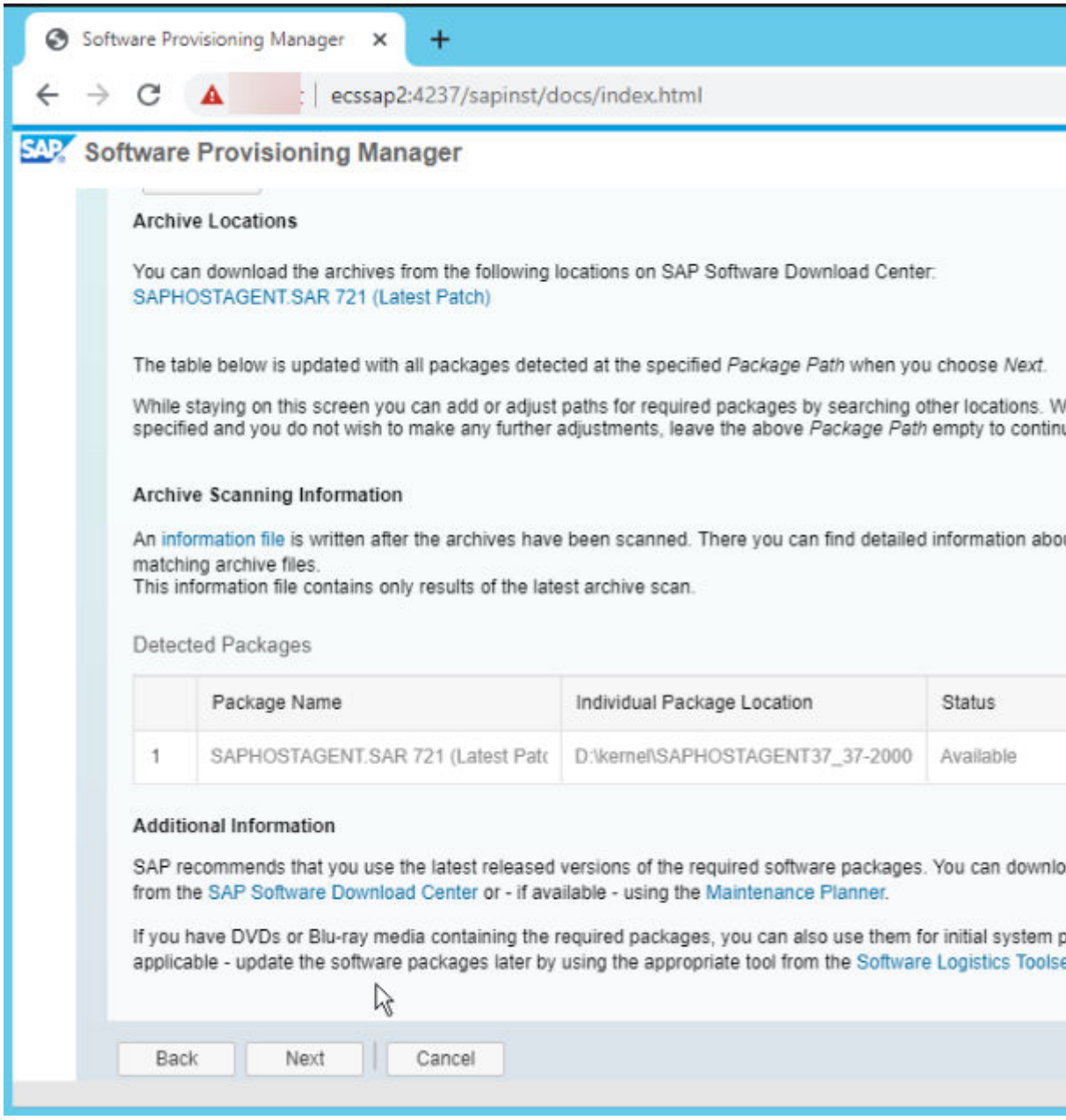


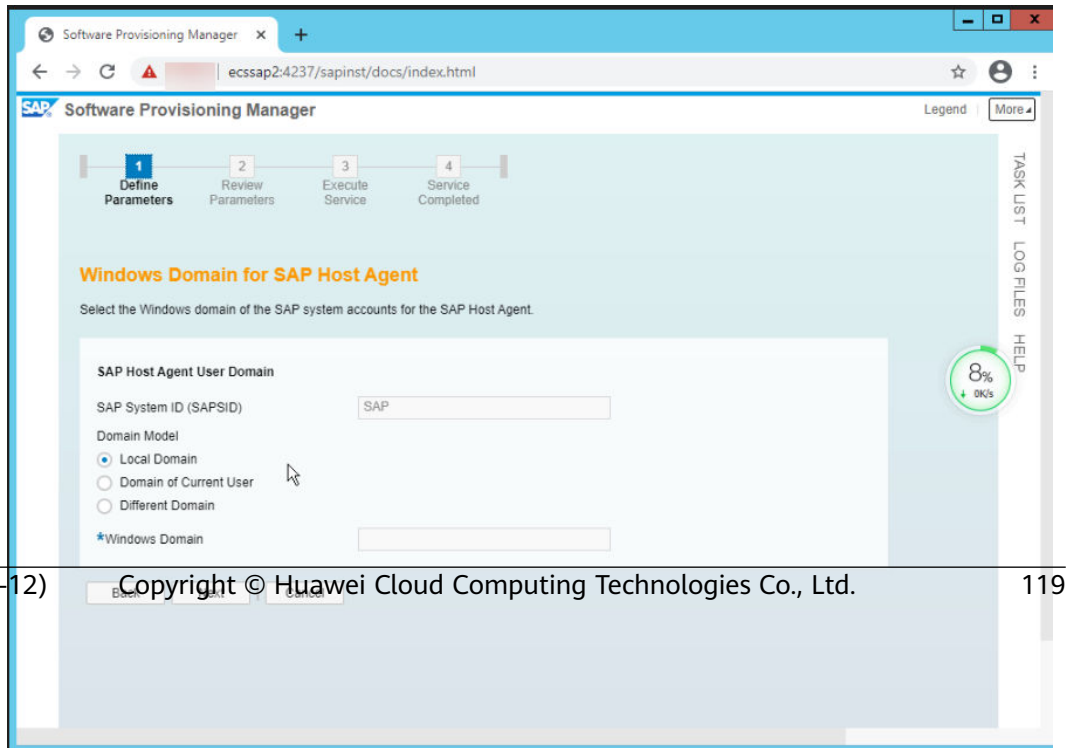


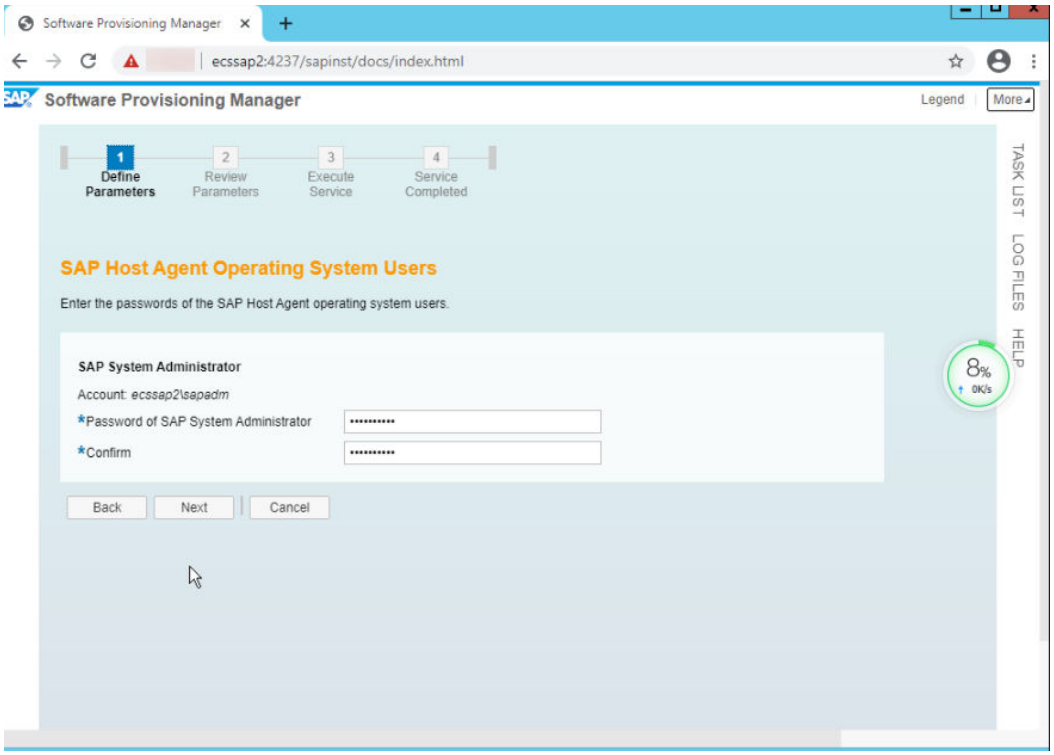
Step 12 Specify the package path and click **Next**.



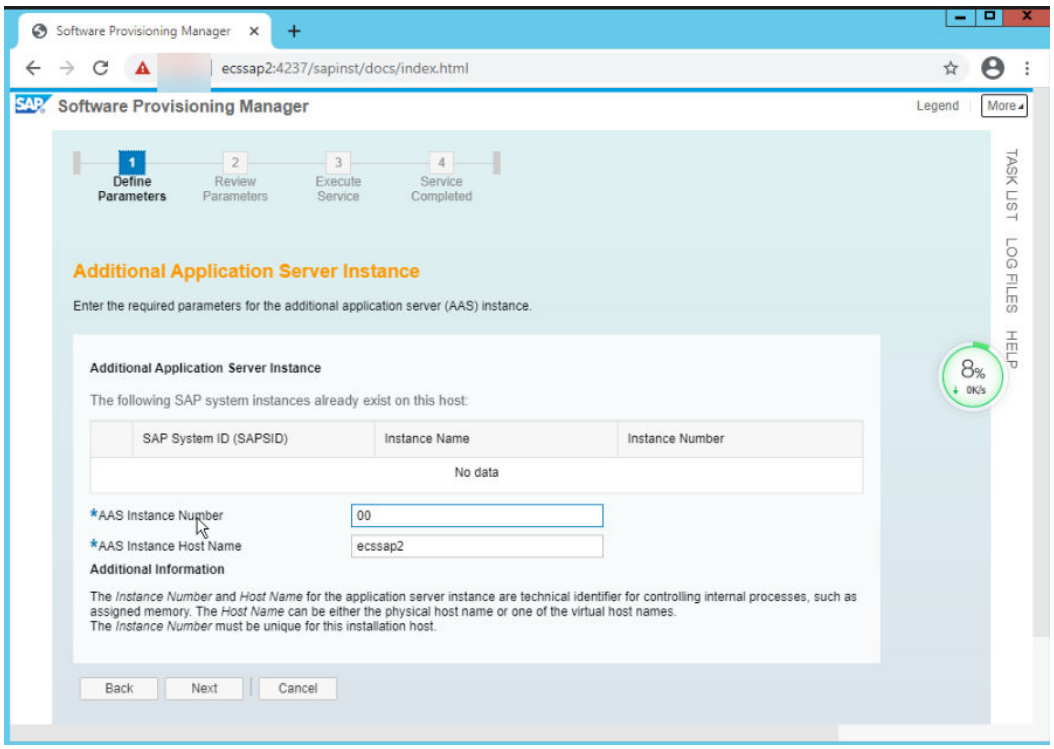
Step 13 Click **Next**.



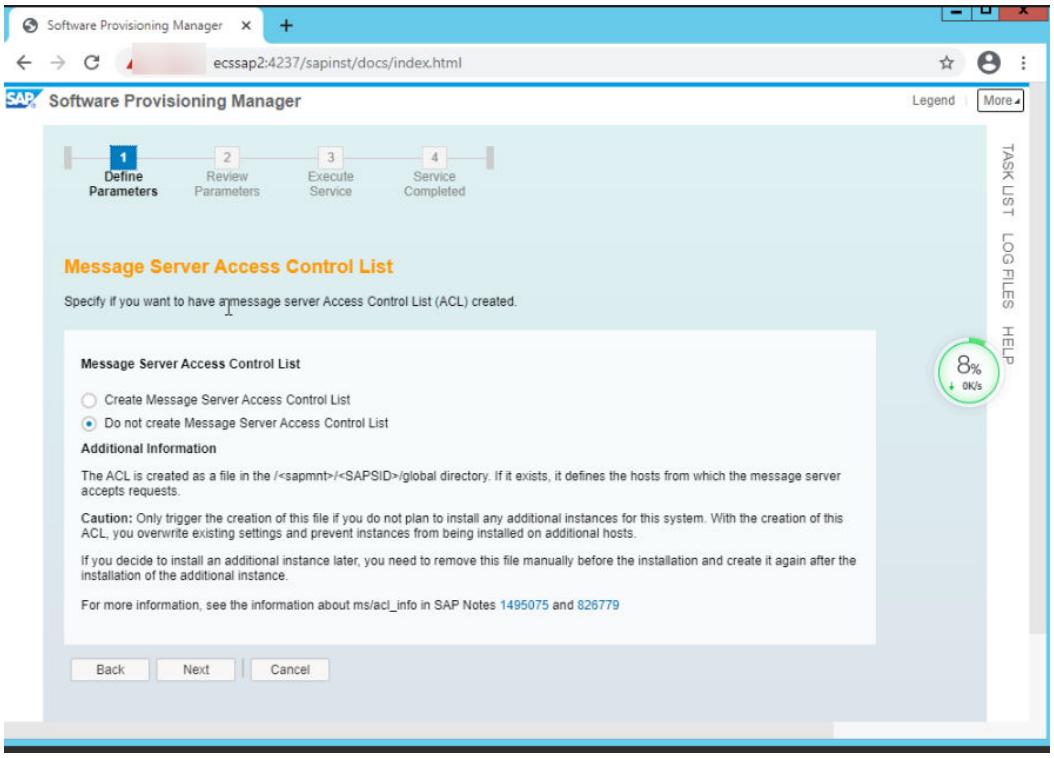




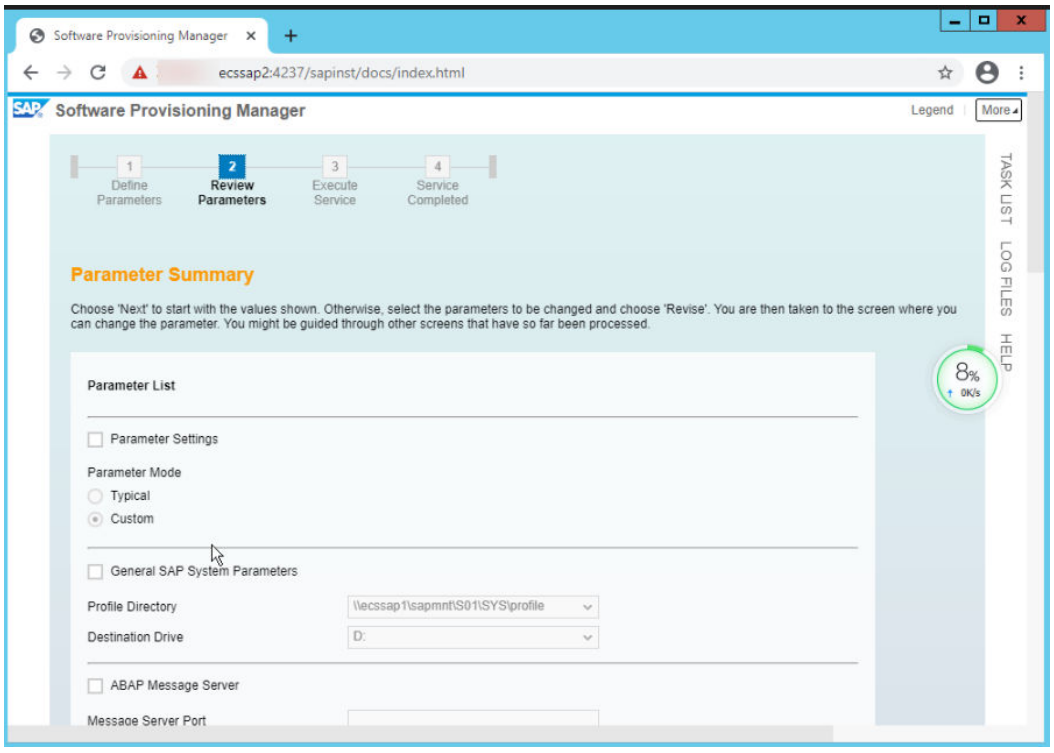
Step 14 Configure the AAS instance number and click **Next**.



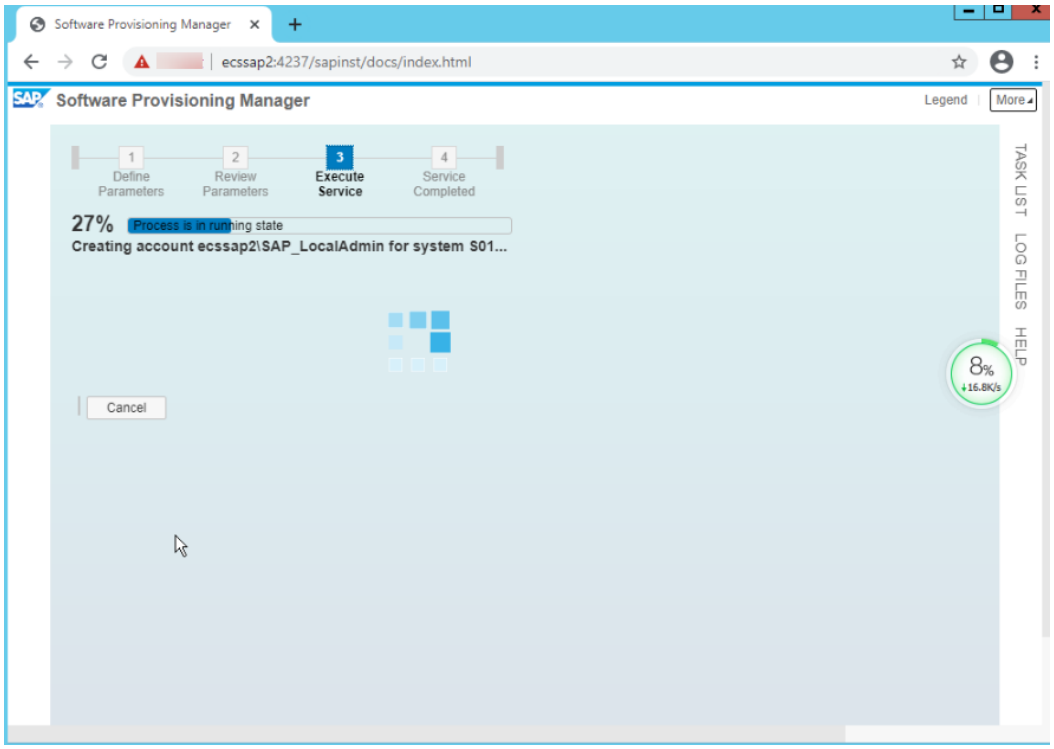
Step 15 Retain the default settings and click **Next**.

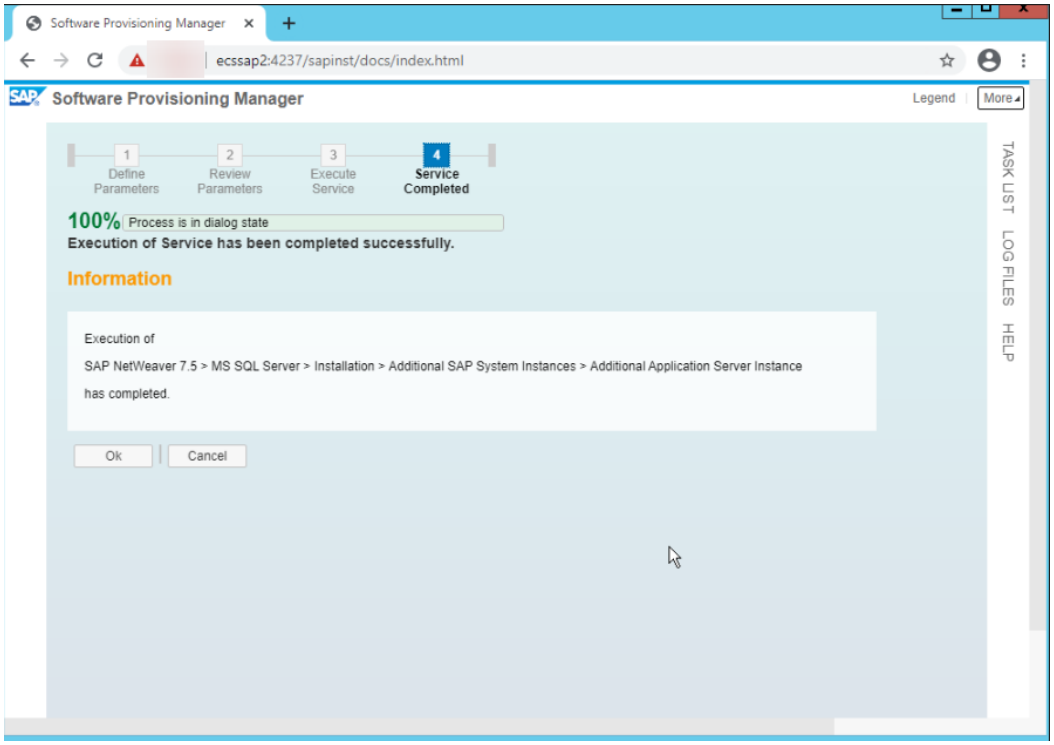


Step 16 Confirm the parameters and click **Next**.



Step 17 The installation starts.



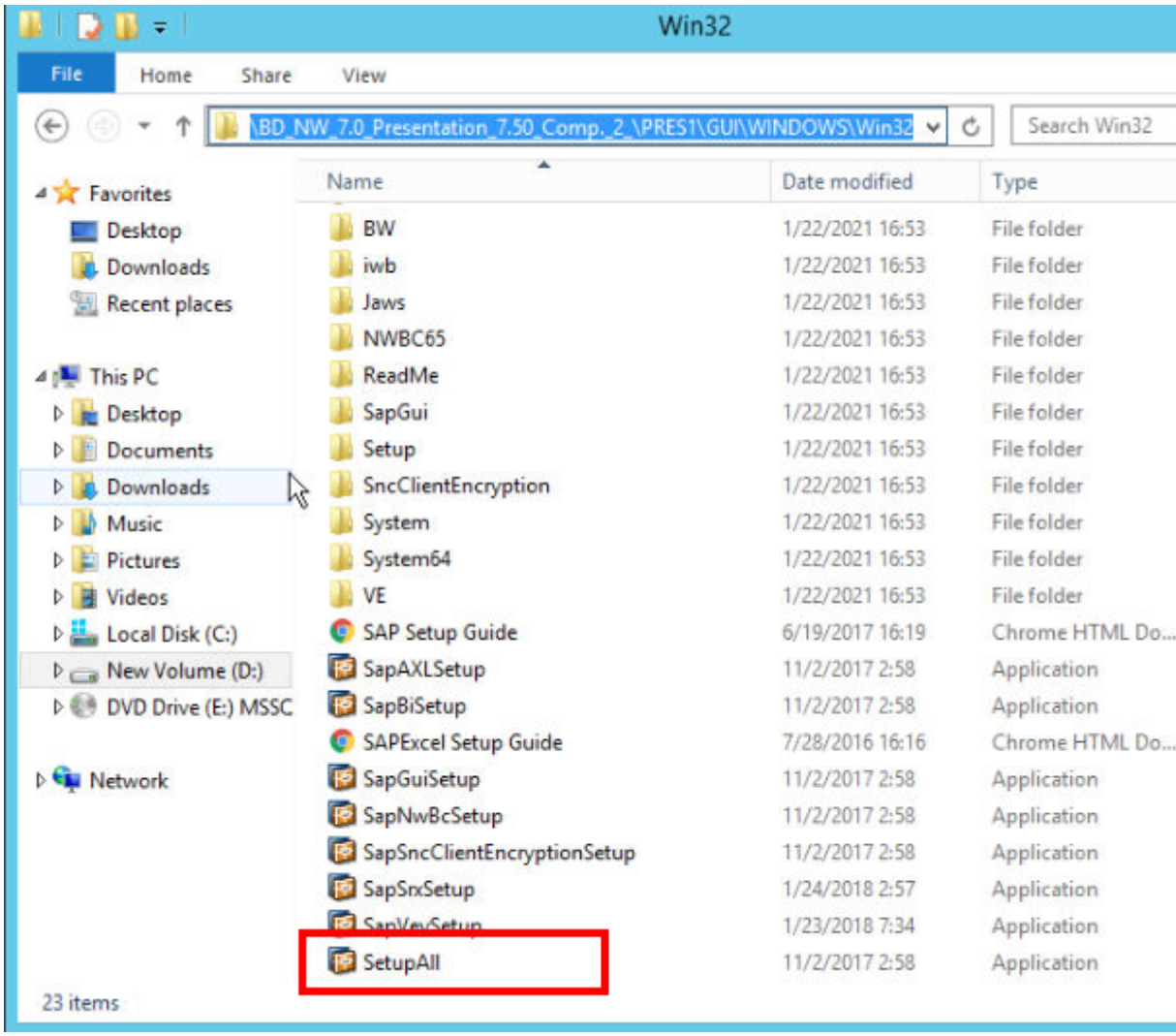


----End

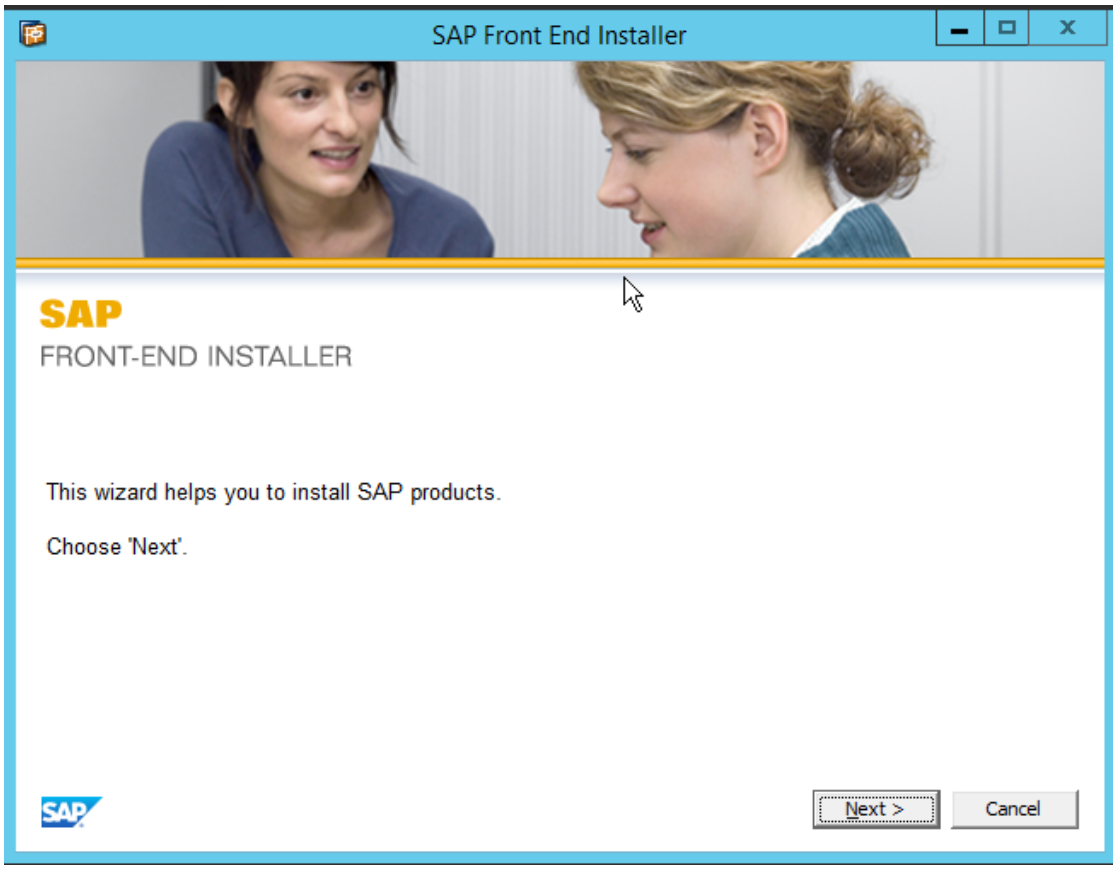
3.5.5 Installing SAP GUI

Install the SAP GUI on the ECS **ecssap2** where AAS is installed.

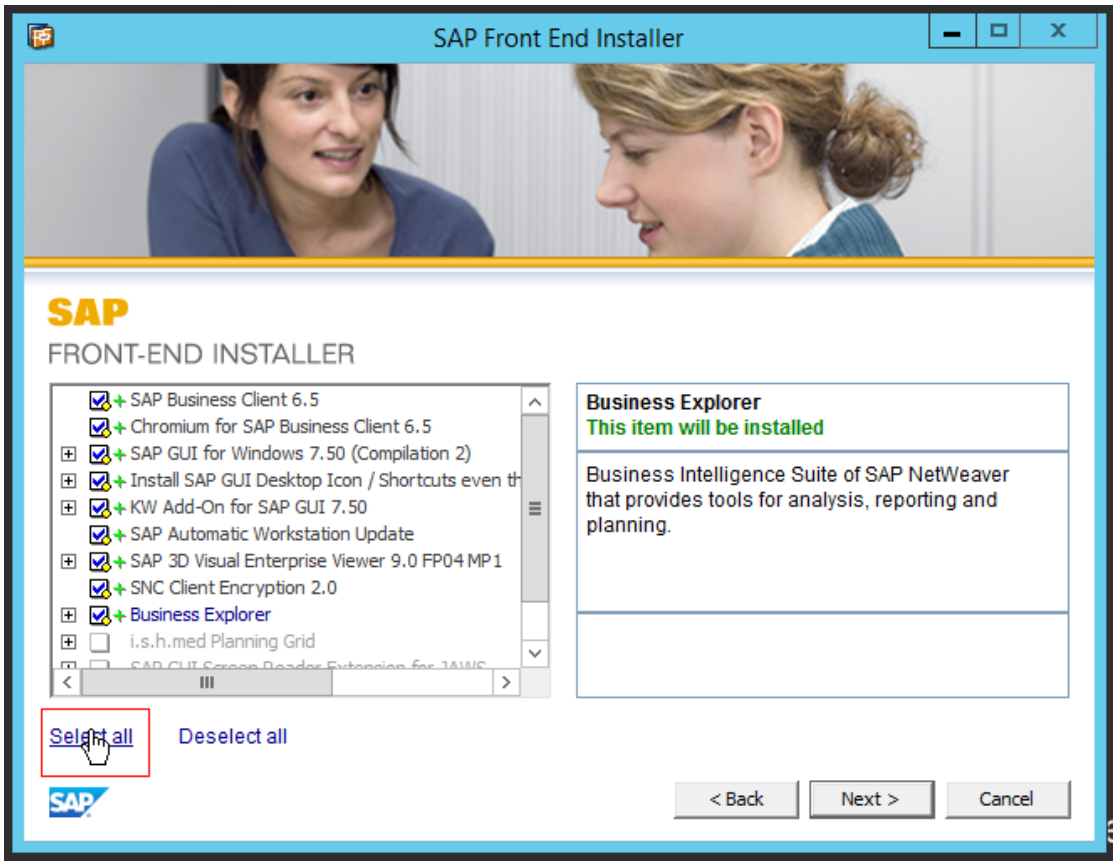
Step 1 Go to the SAP GUI installation directory. Run the installation program.



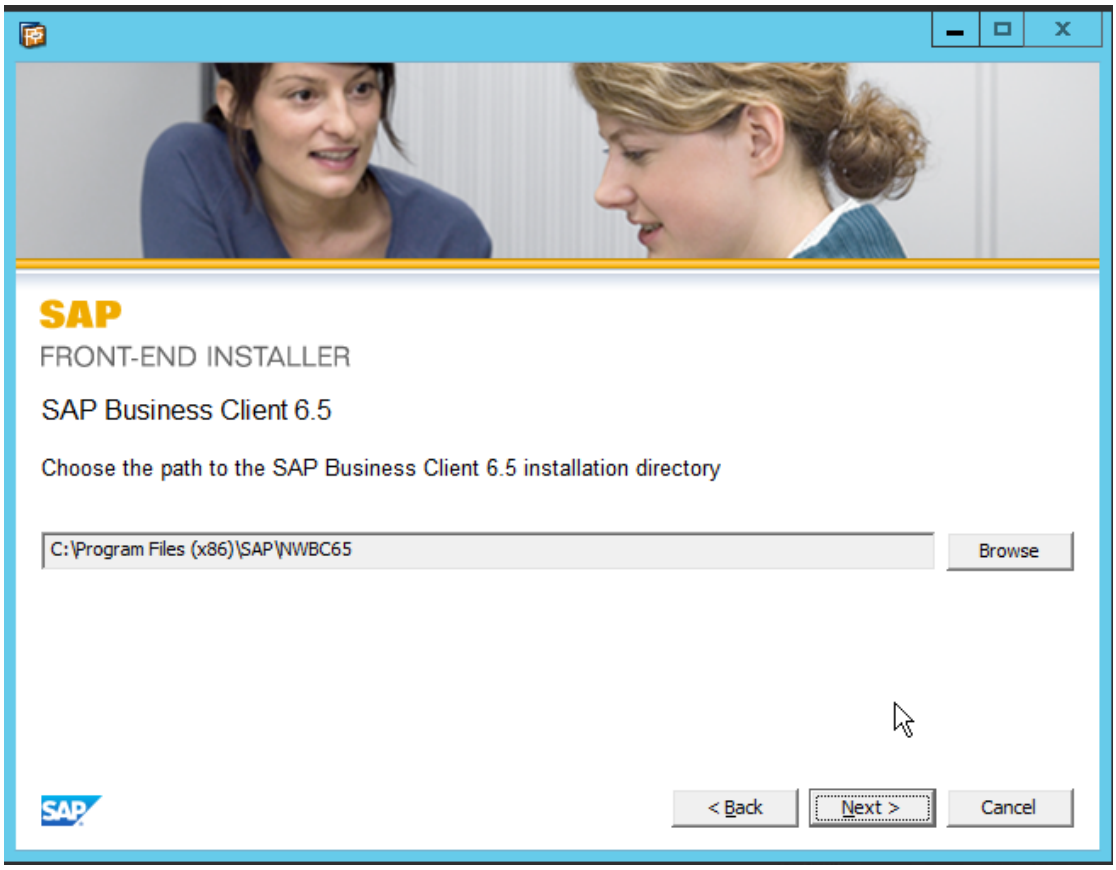
Step 2 Click **Next**.



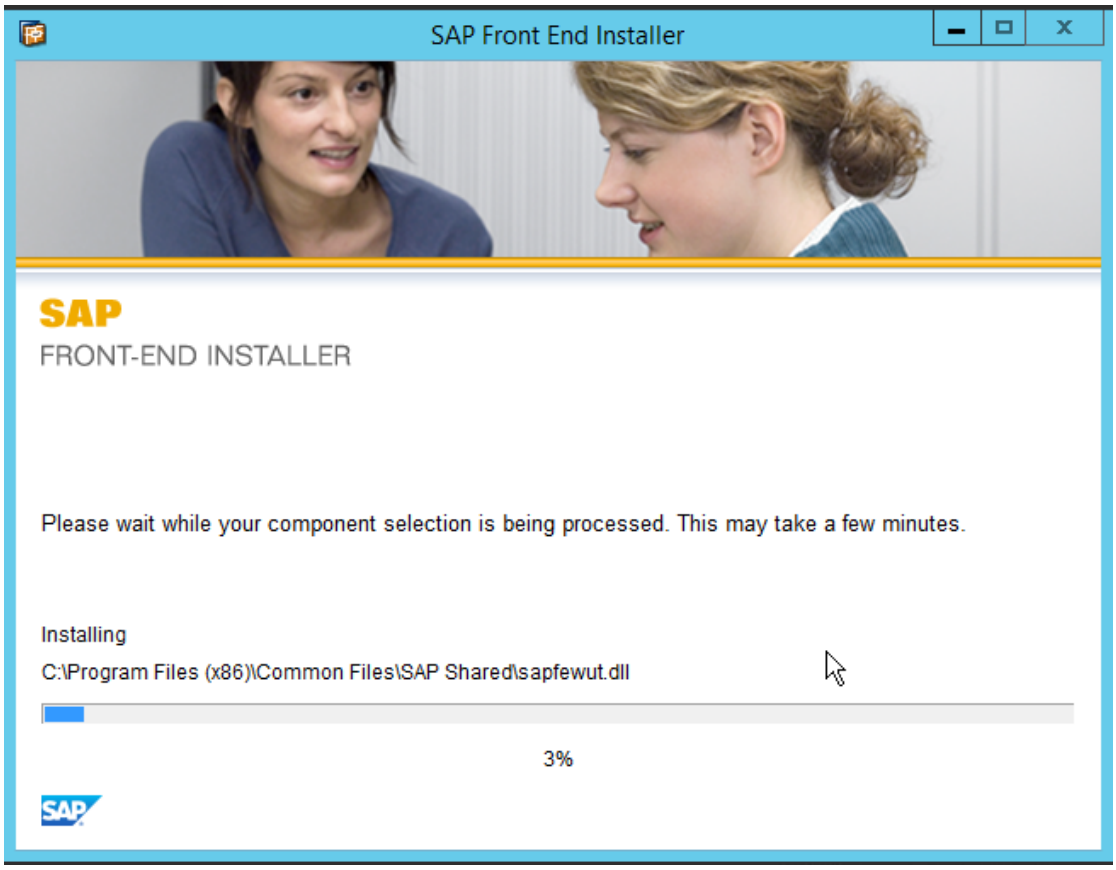
Step 3 Select the components to be installed. Here, click **Select all** and then **Next**.



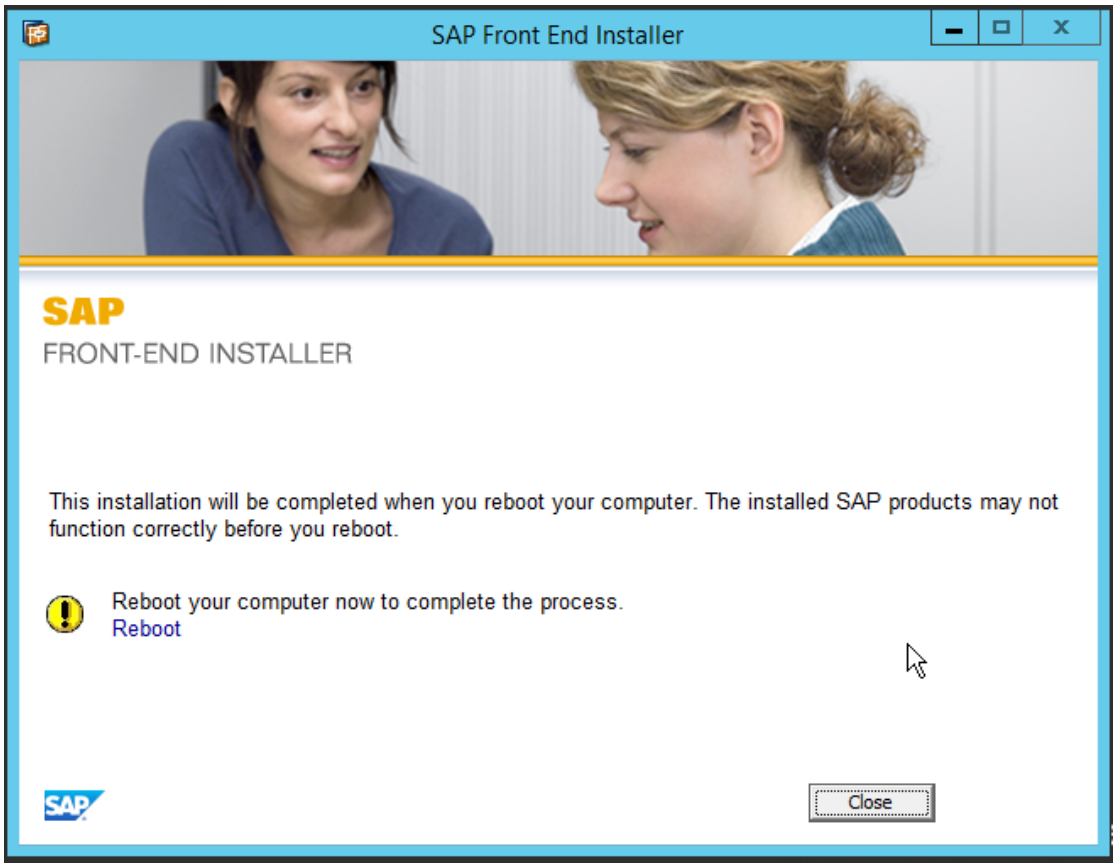
Step 4 Select the installation location for each component. Retain the default settings and click **Next** until the installation location is set for all components.



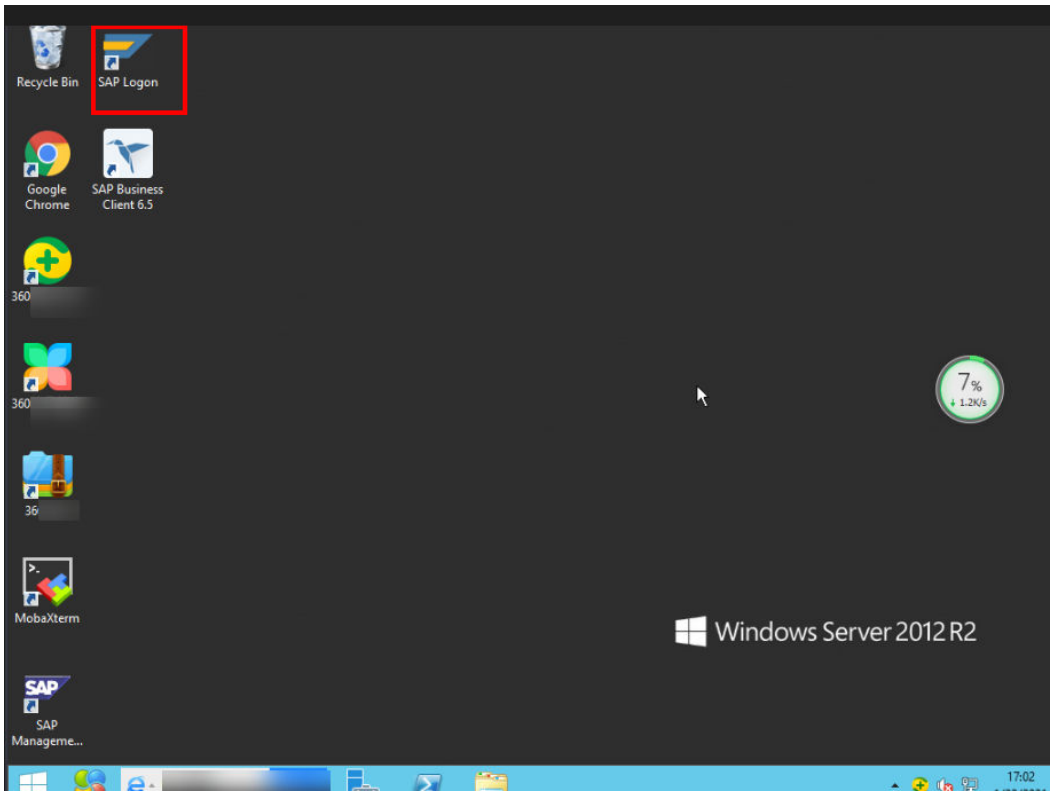
Step 5 The installation starts.



Step 6 After the installation is complete, restart the computer as required. You can restart it during off-peak hour.



Step 7 Restart the computer.



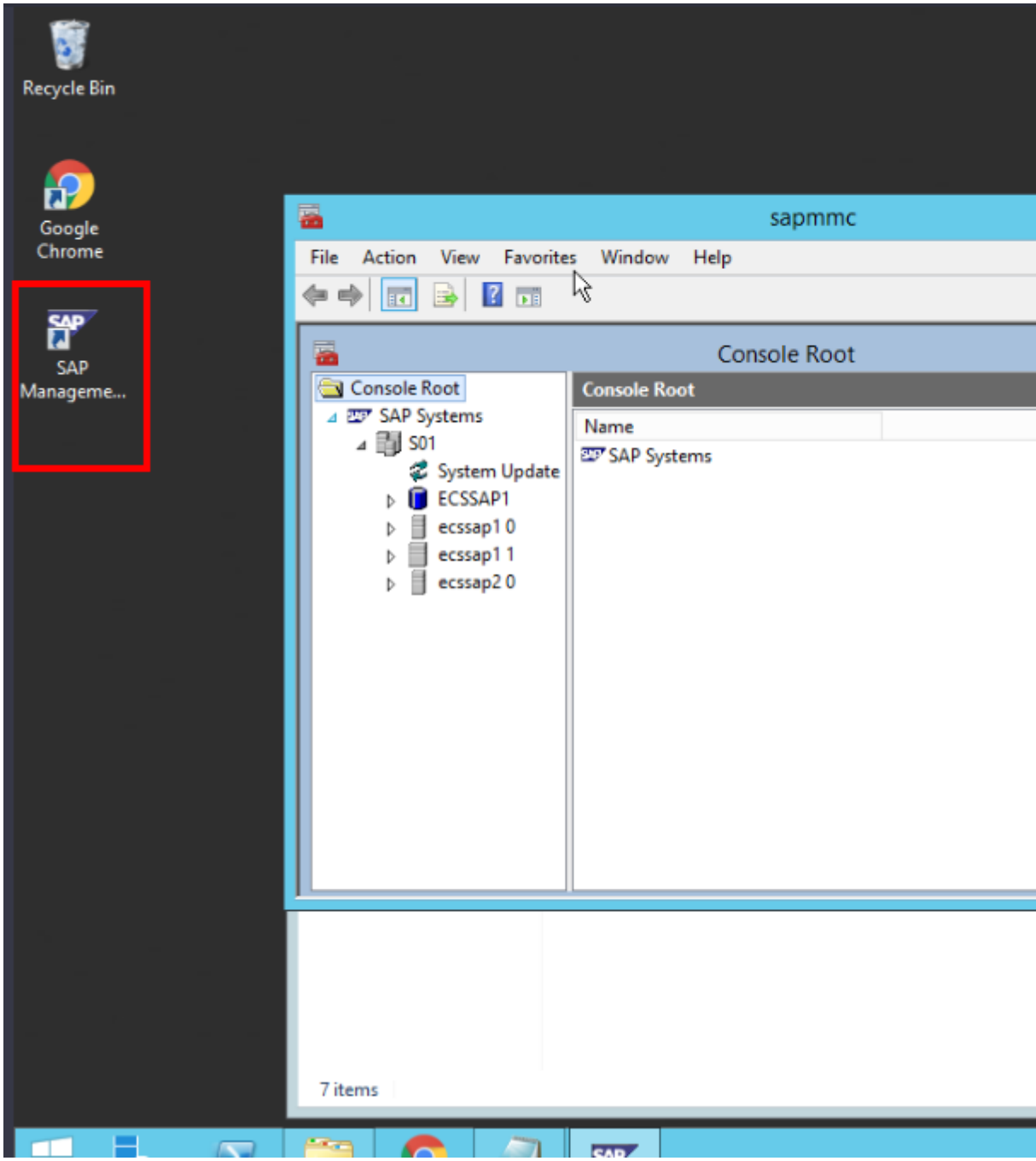
----End

3.6 Installation Verification

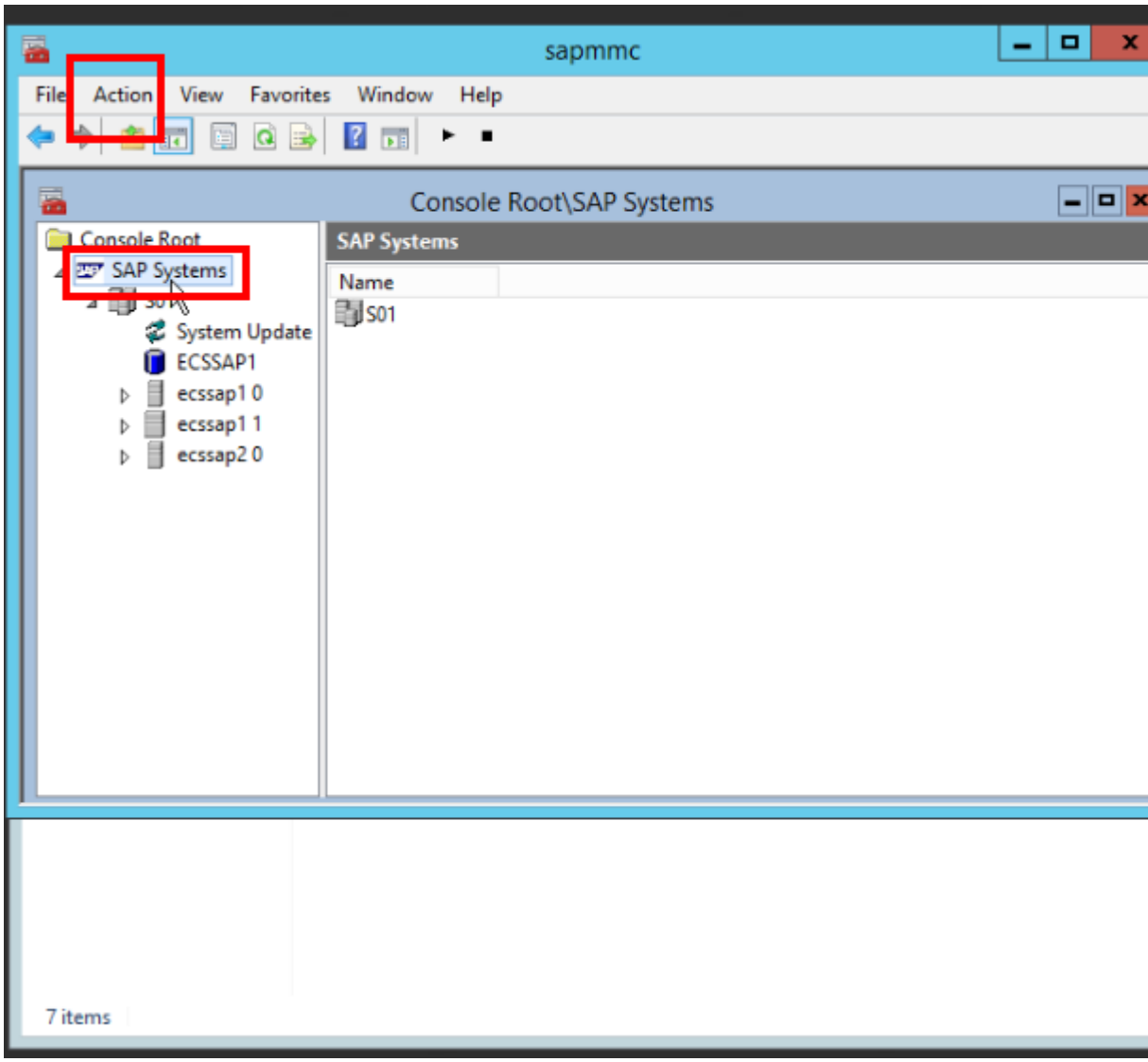
3.6.1 Checking Instance Status

The following demonstrates how to start SAP.

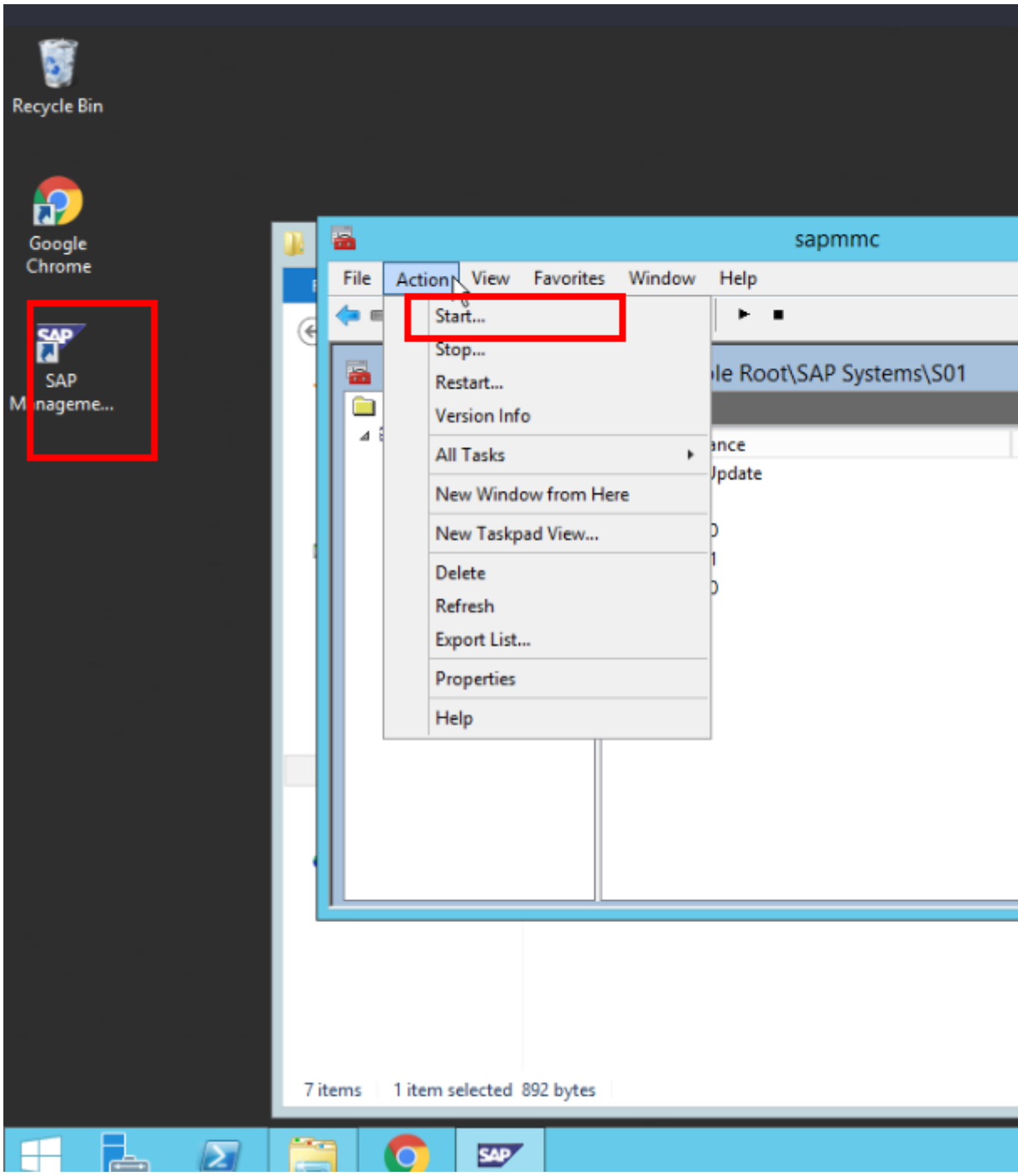
Step 1 Start the SAP Management Console client on **ecssap1**.



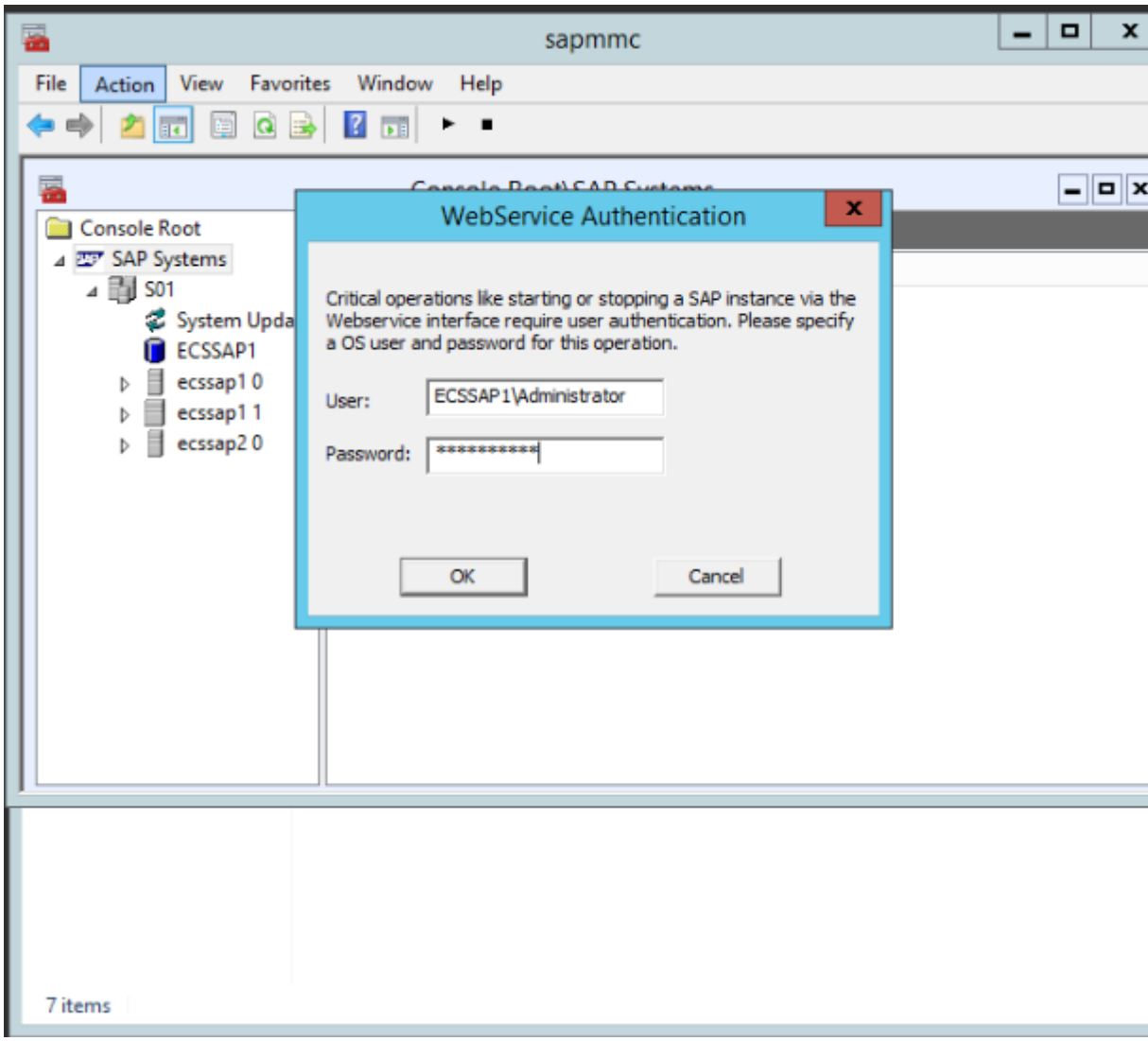
Step 2 Select **Sap System**, choose **Action** > **Start**, enter the password, and click **OK**.



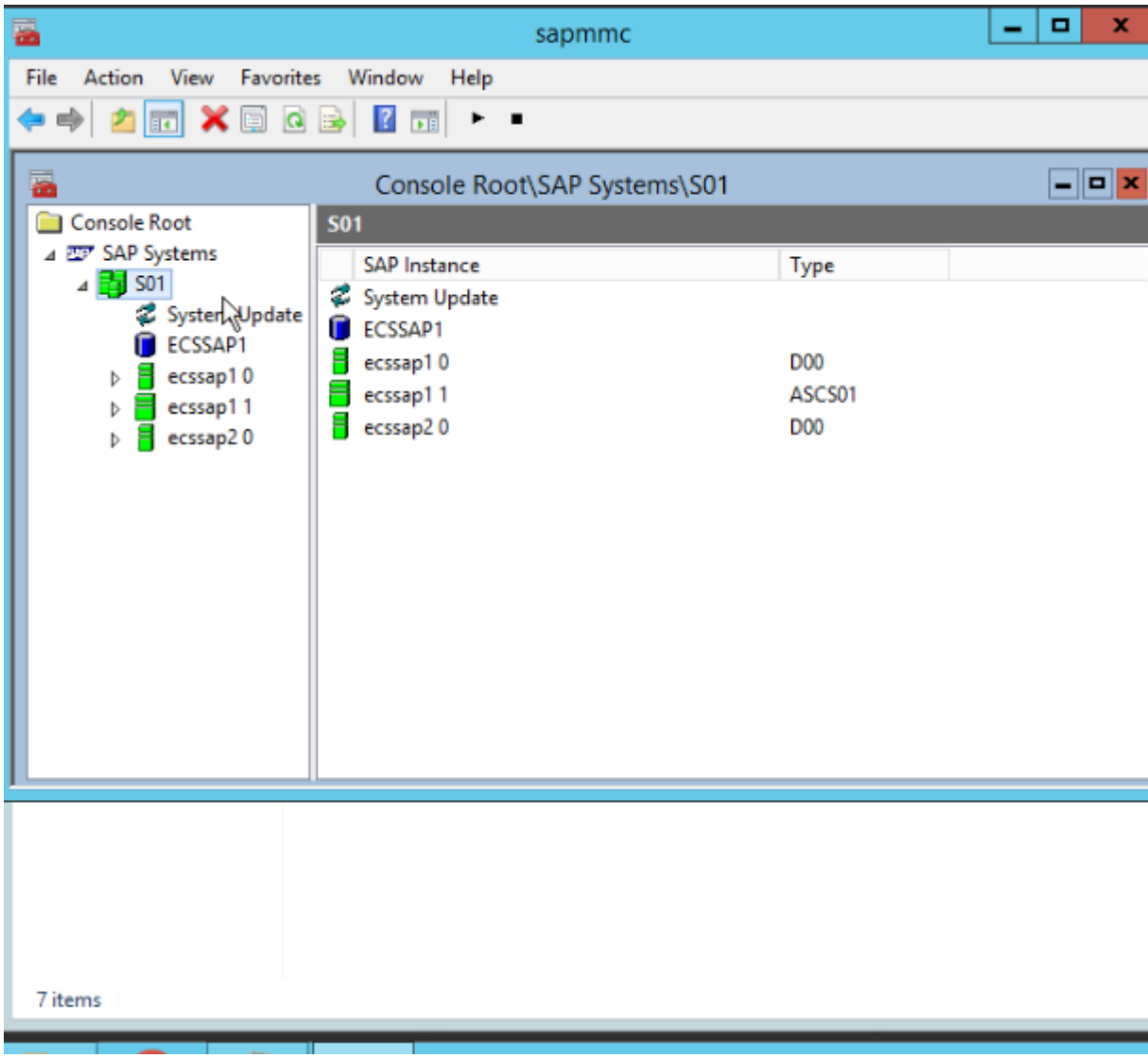
Step 3 Click **Start**.



Step 4 Enter the username and password of the administrator, and then click **OK**.



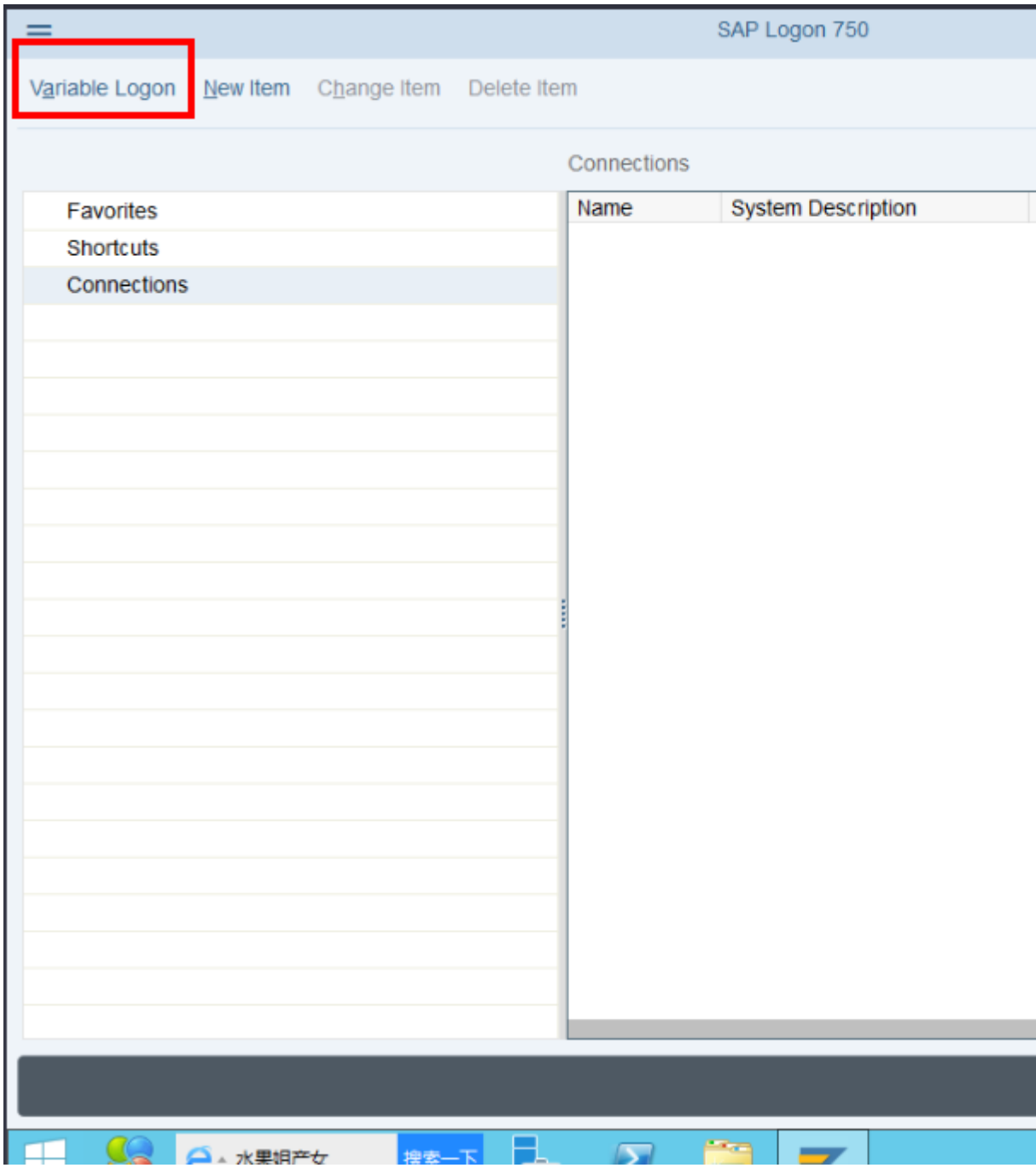
Step 5 Wait for a while. When all the icons before the instance name become green, the SAP instances are running normally.



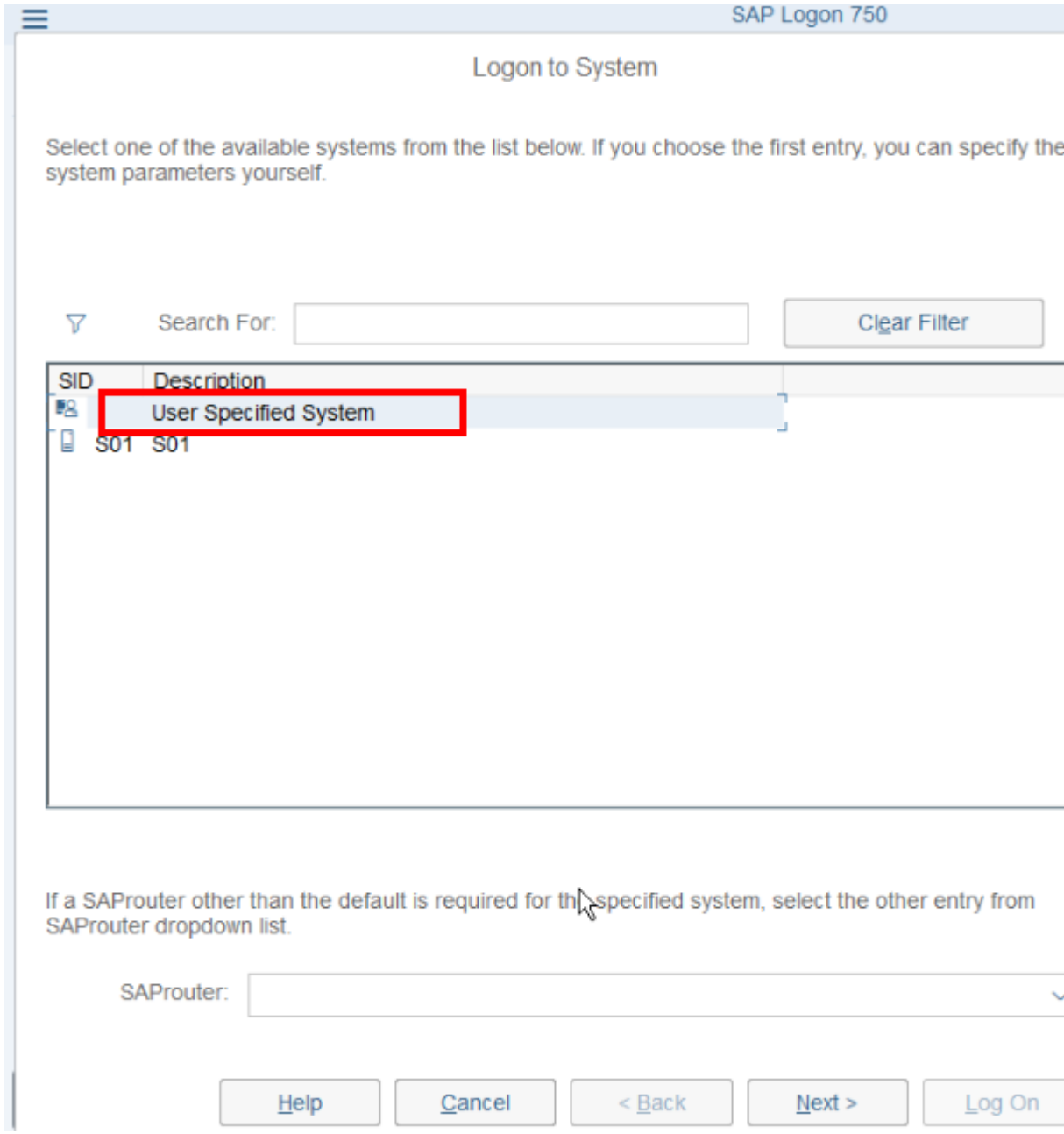
----End

3.6.2 Using SAP GUI to Connect to the SAP Application

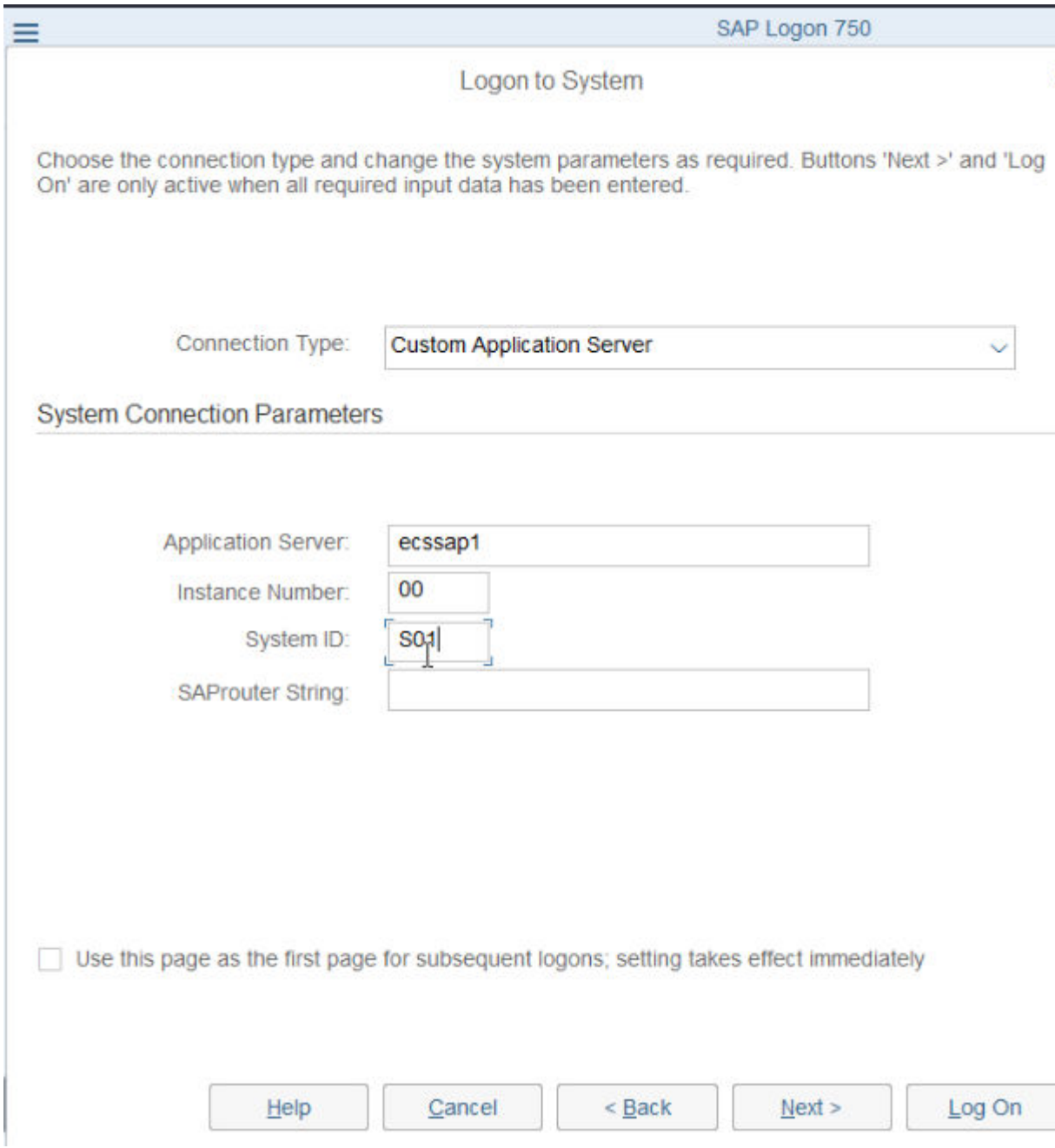
Step 1 Log in to **ecssap2** at the production site, run SAP Logon, and click **Variable Logon**.

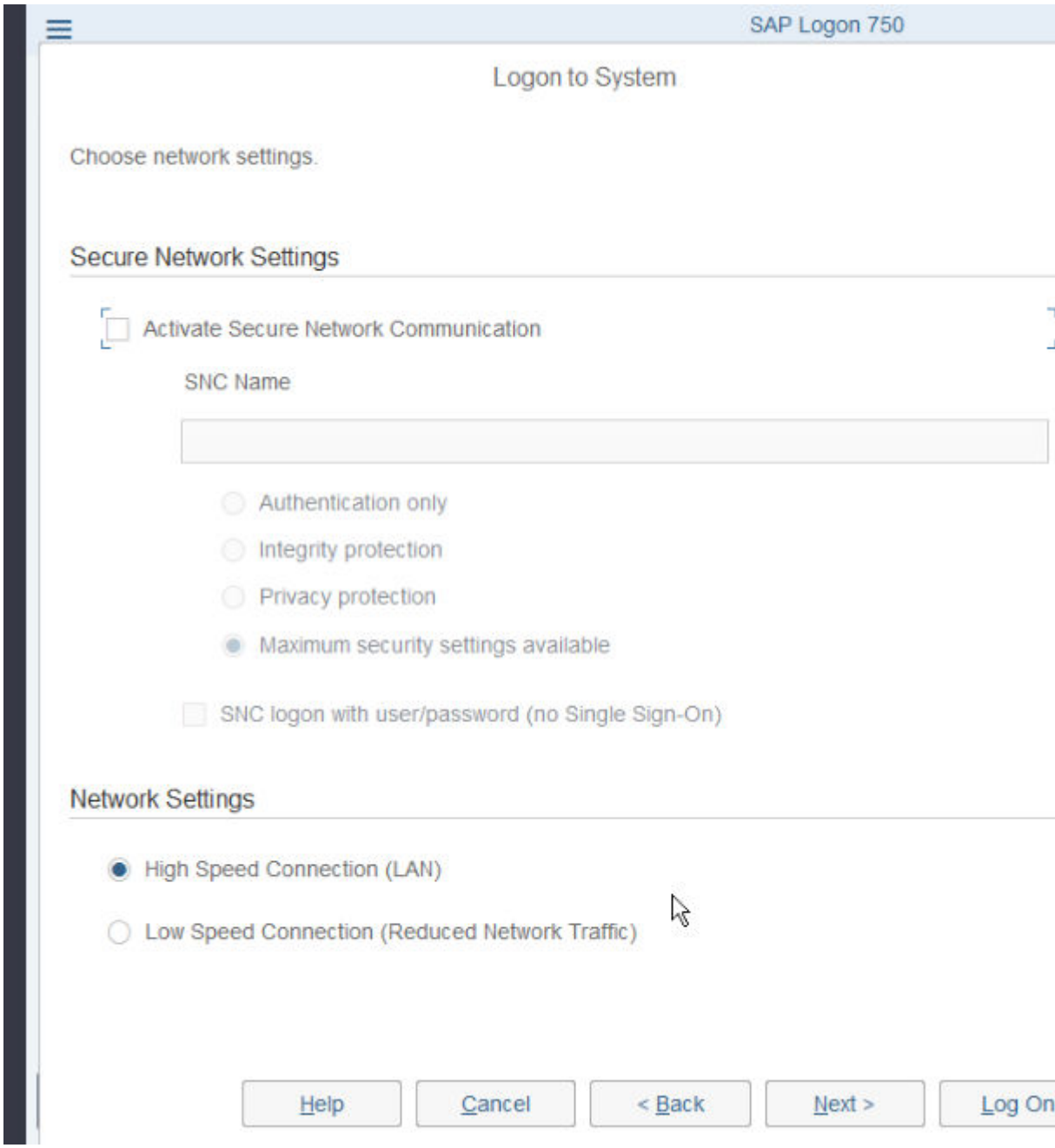


Step 2 Double-click **User Specified System**.

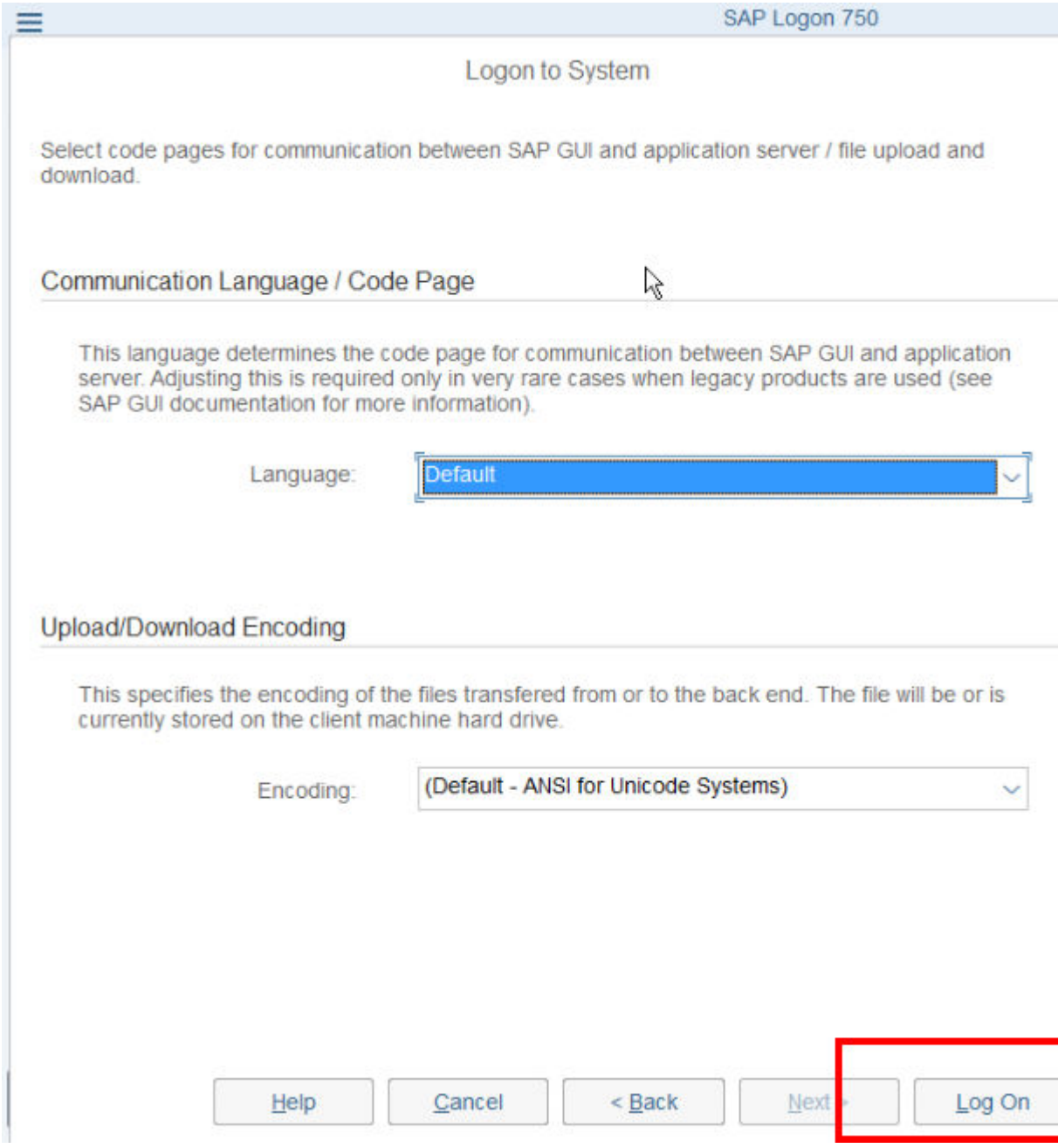


Step 3 Configure required parameters based on the site requirements and click **Next**.

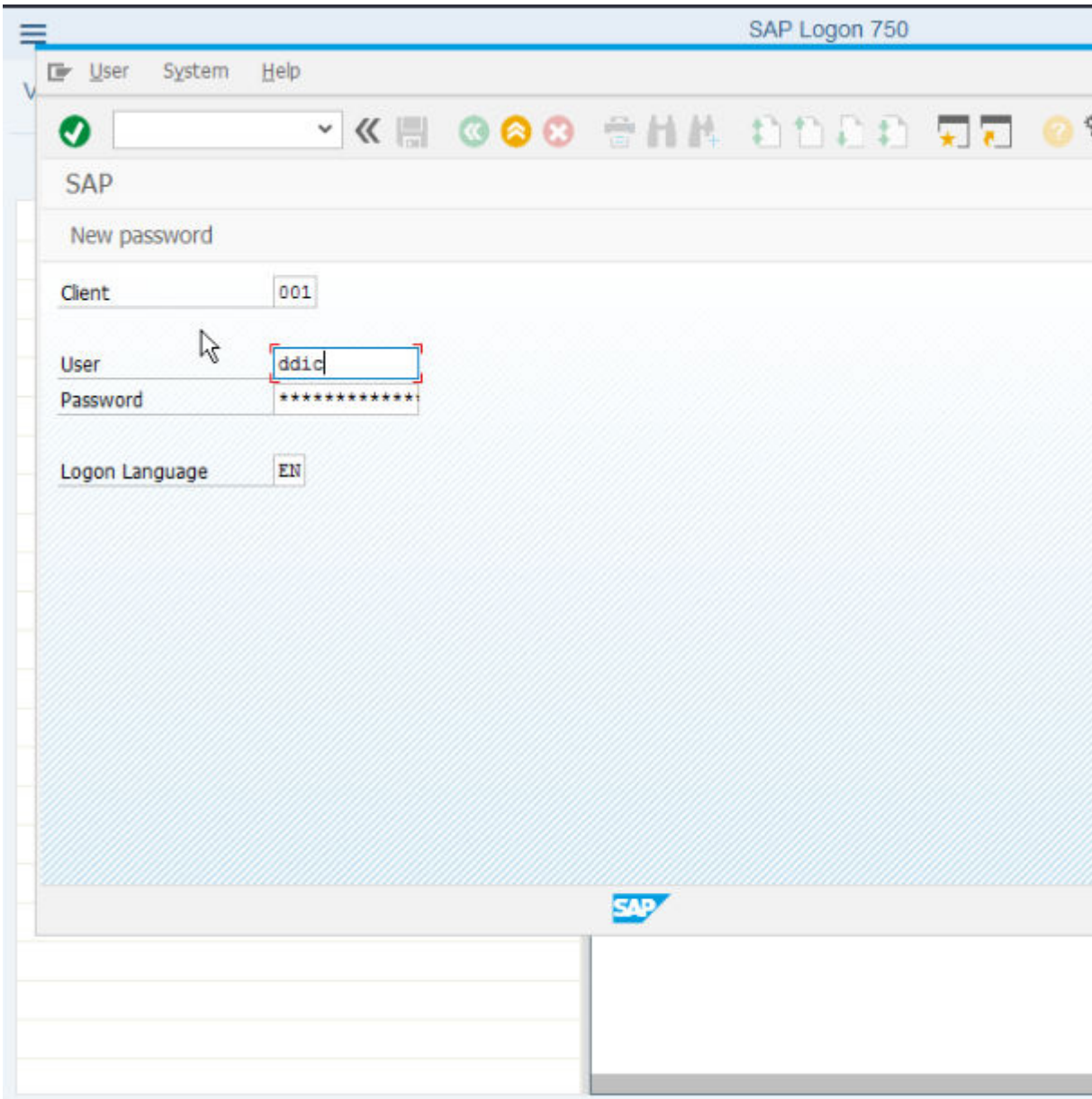


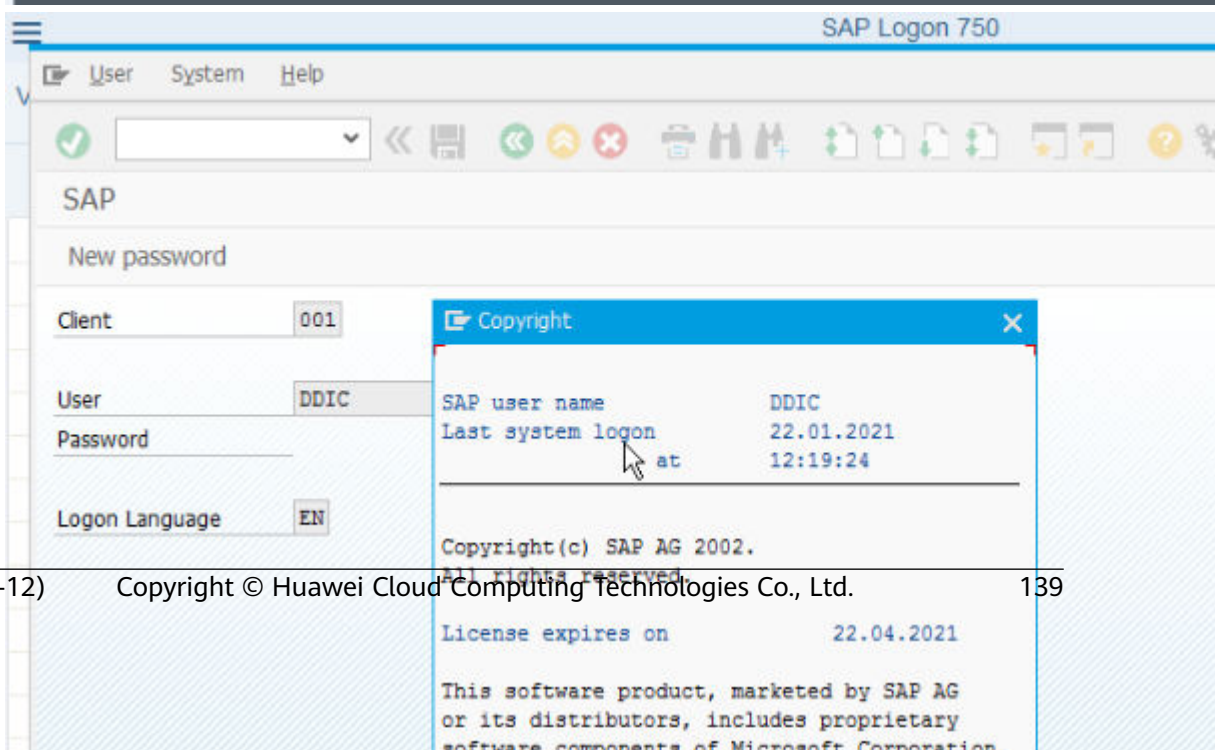


Step 4 Click **Log On**.

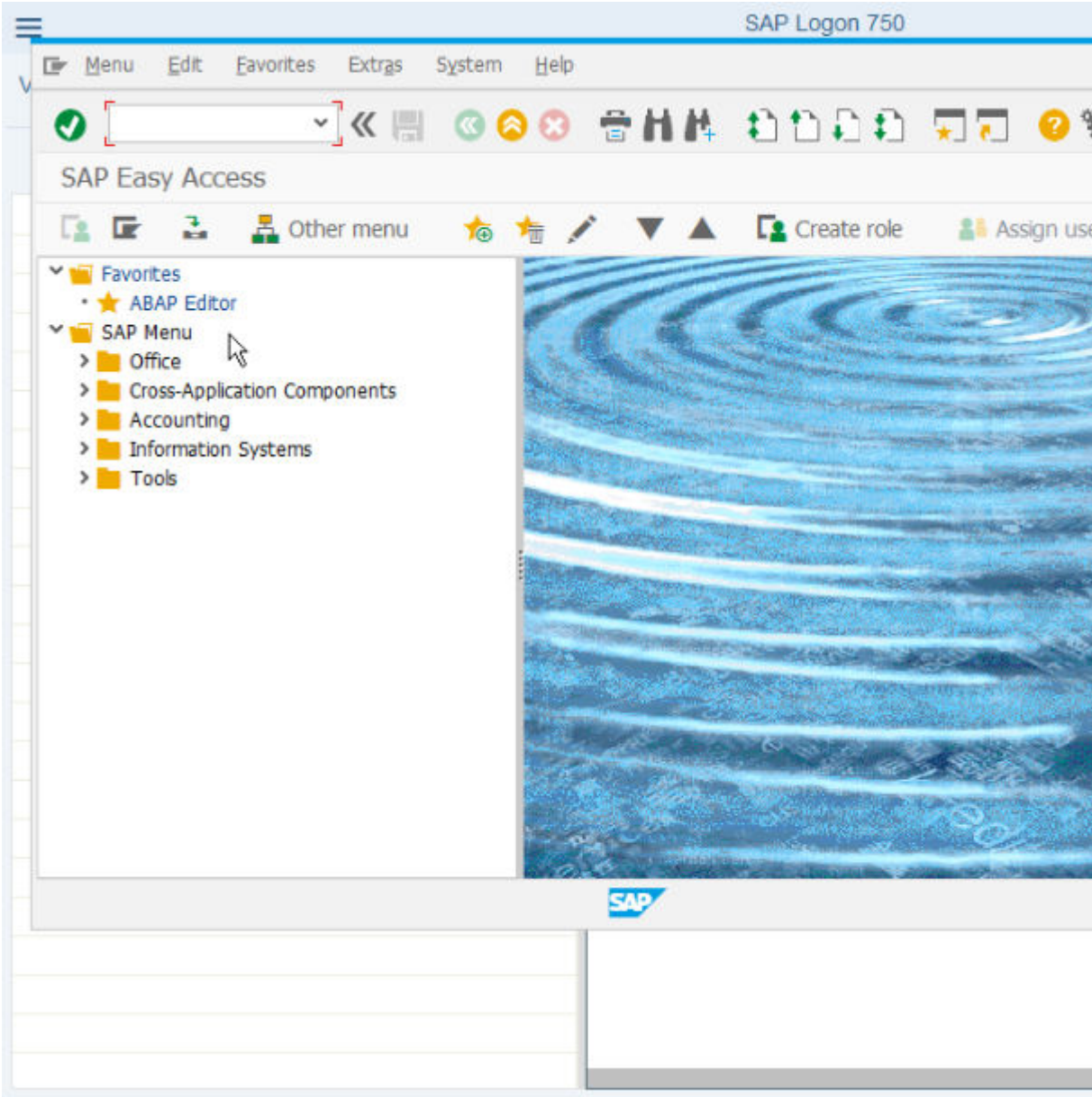


Step 5 Type the username **ddic** and the password, and then press **Enter**.

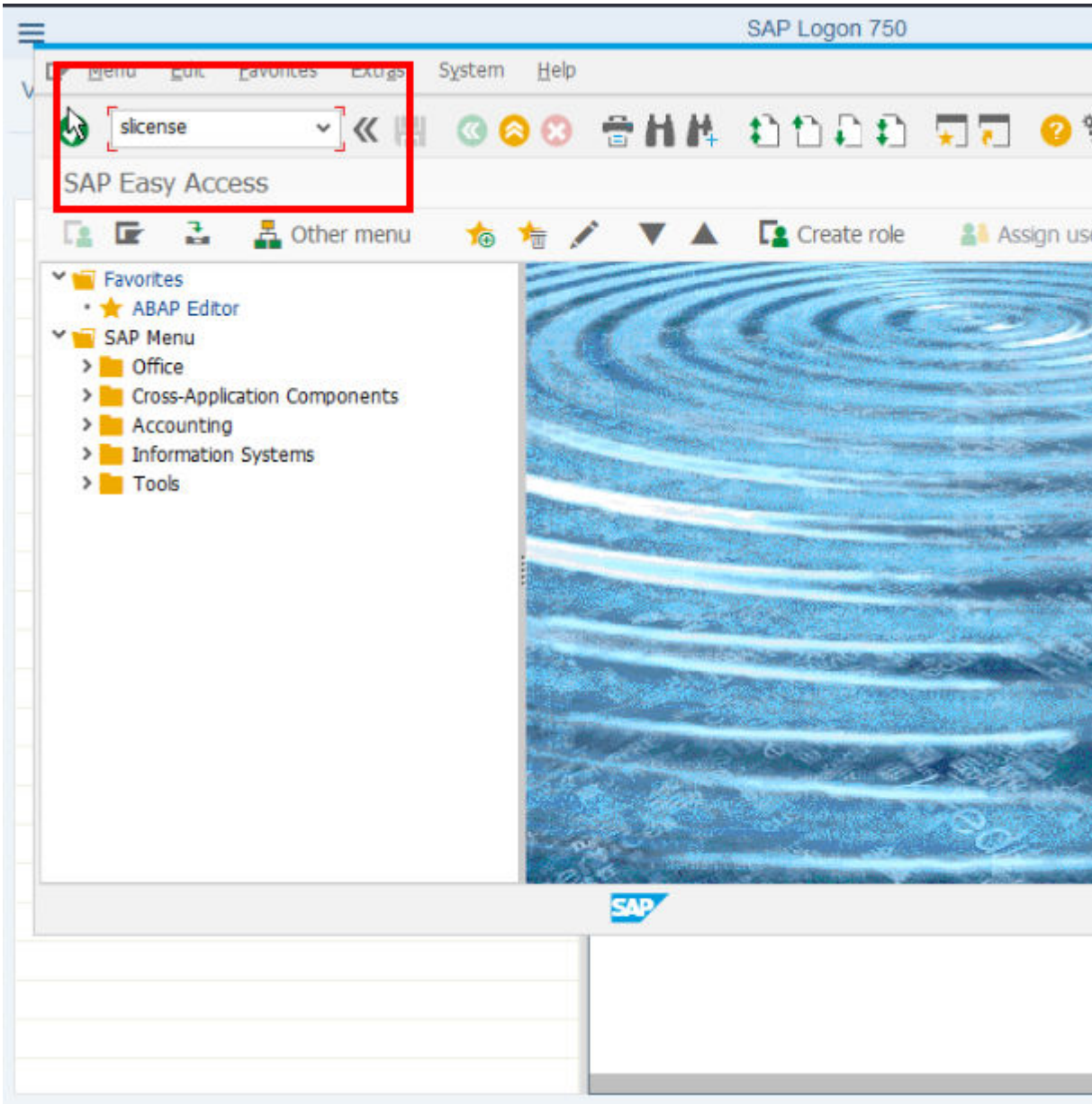


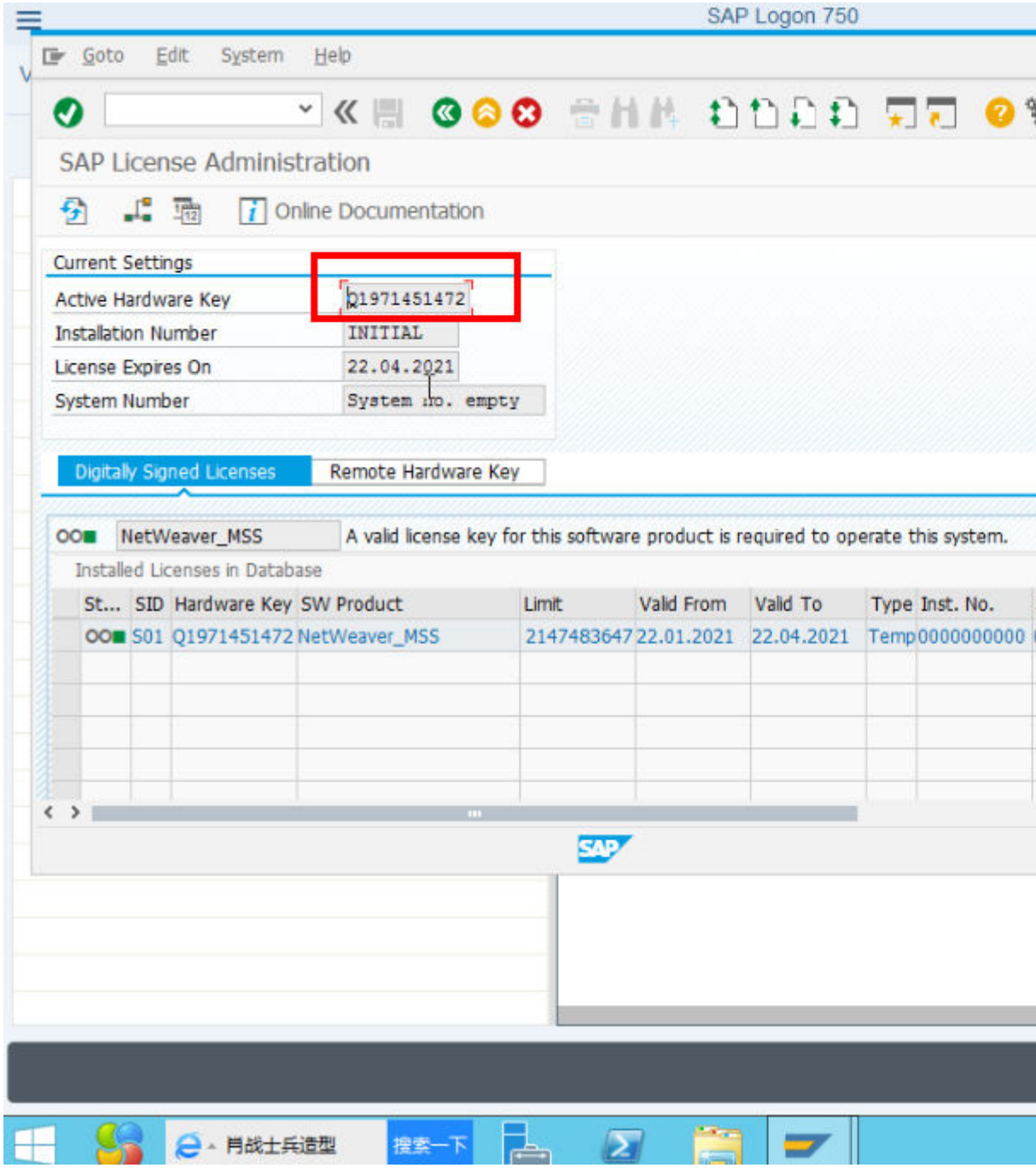


Step 6 The login to SAP GUI is successful.



Step 7 Enter **slicense** in the search box and press **Enter** to view the hardware key.





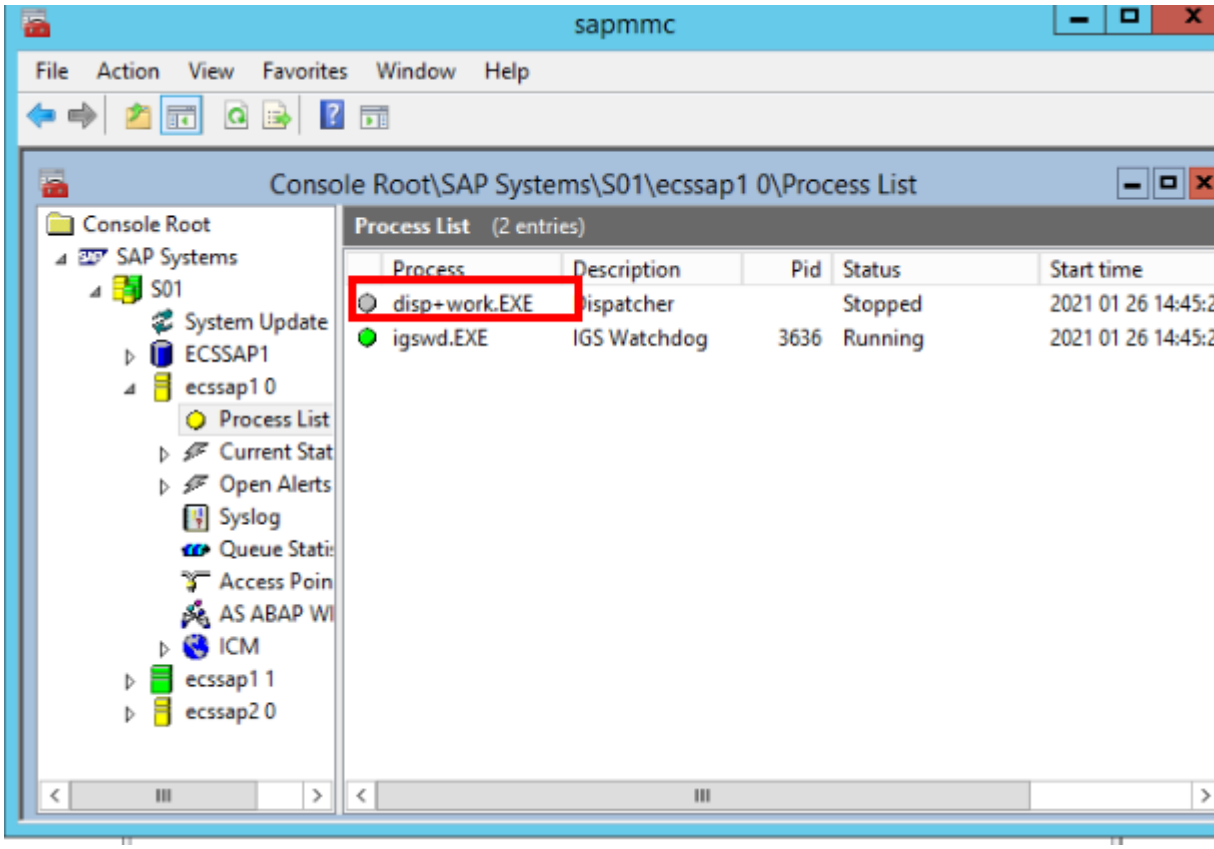
----End

3.7 FAQ

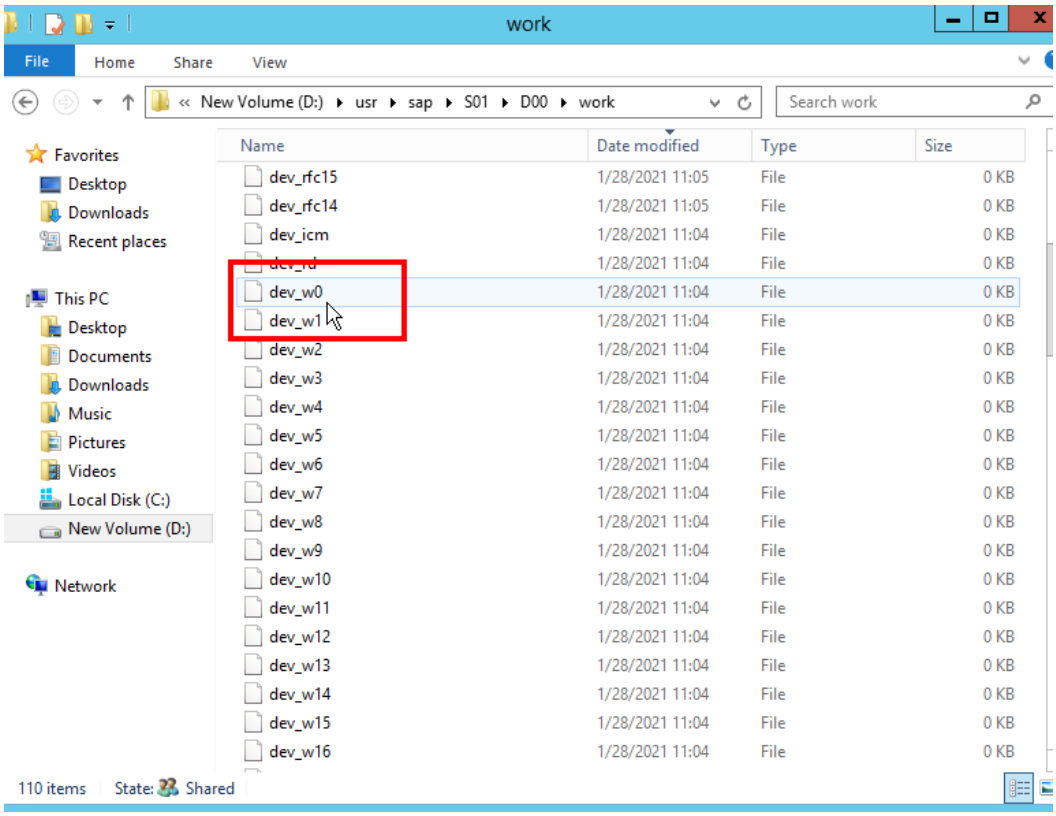
3.7.1 What Should I Do If SAP Failed to Be Started?

Symptom

1. SAP failed to be started because the disp+work instance is not started.

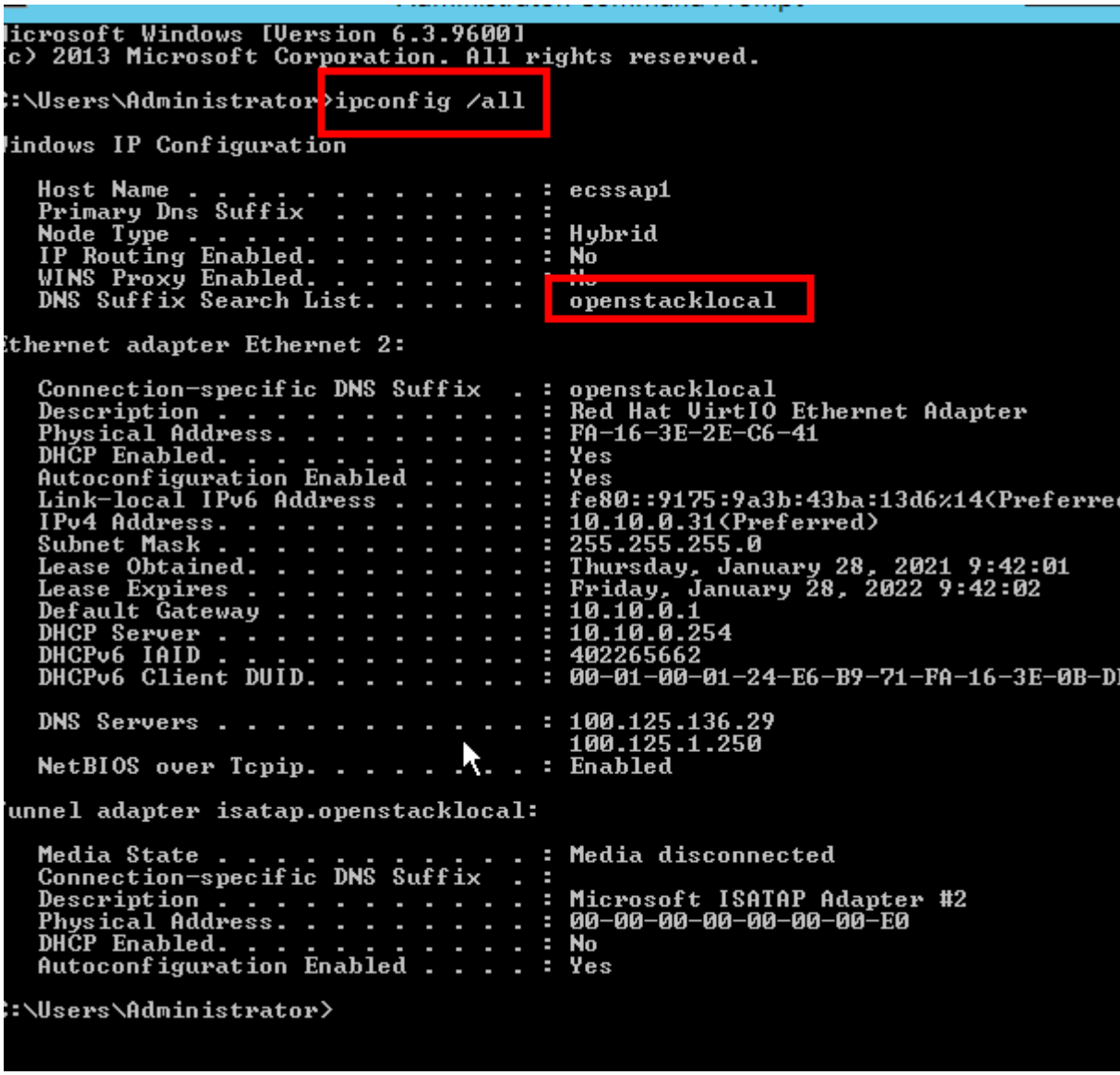


2. View logs.



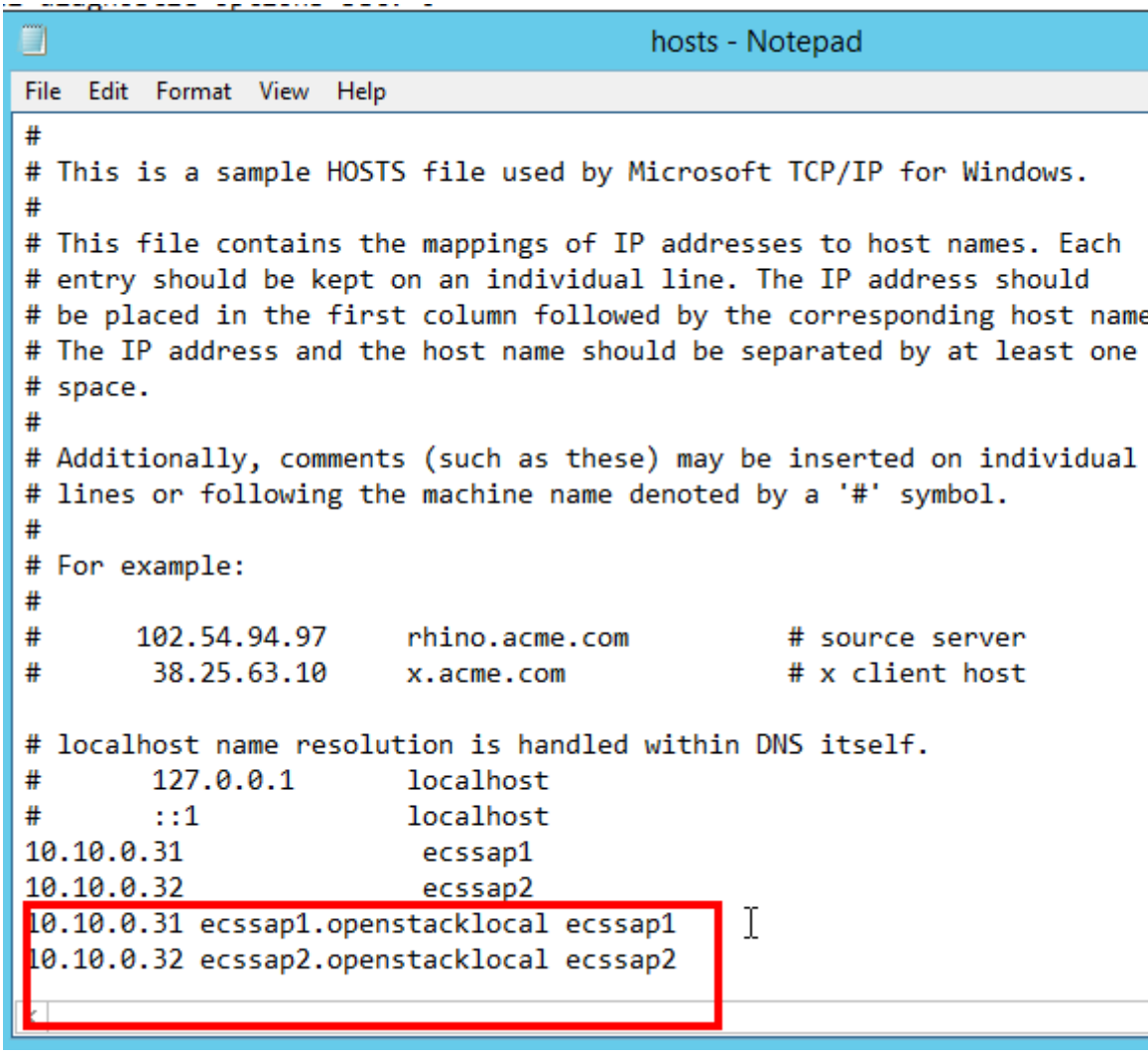

```
Thu Jan 28 09:47:25:342 2021
 ThStart: taskhandler started
 ThInit: initializing DIA work process W0
 *** ERROR => ThSetGwParam : NiHostToAddr ecssap1.openstacklocal failed [thParam.c    3426]
 in_ThErrHandle: 1
 *** ERROR => ThInit: ThProfileRead (step TH_INIT, thRc ERROR-CORE-INIT_FAILED, action STOP_WP, level 1) [thxxhead.c   2559]

 Info for wp 0
```

The root cause is that the domain name has not been added to the hosts file.

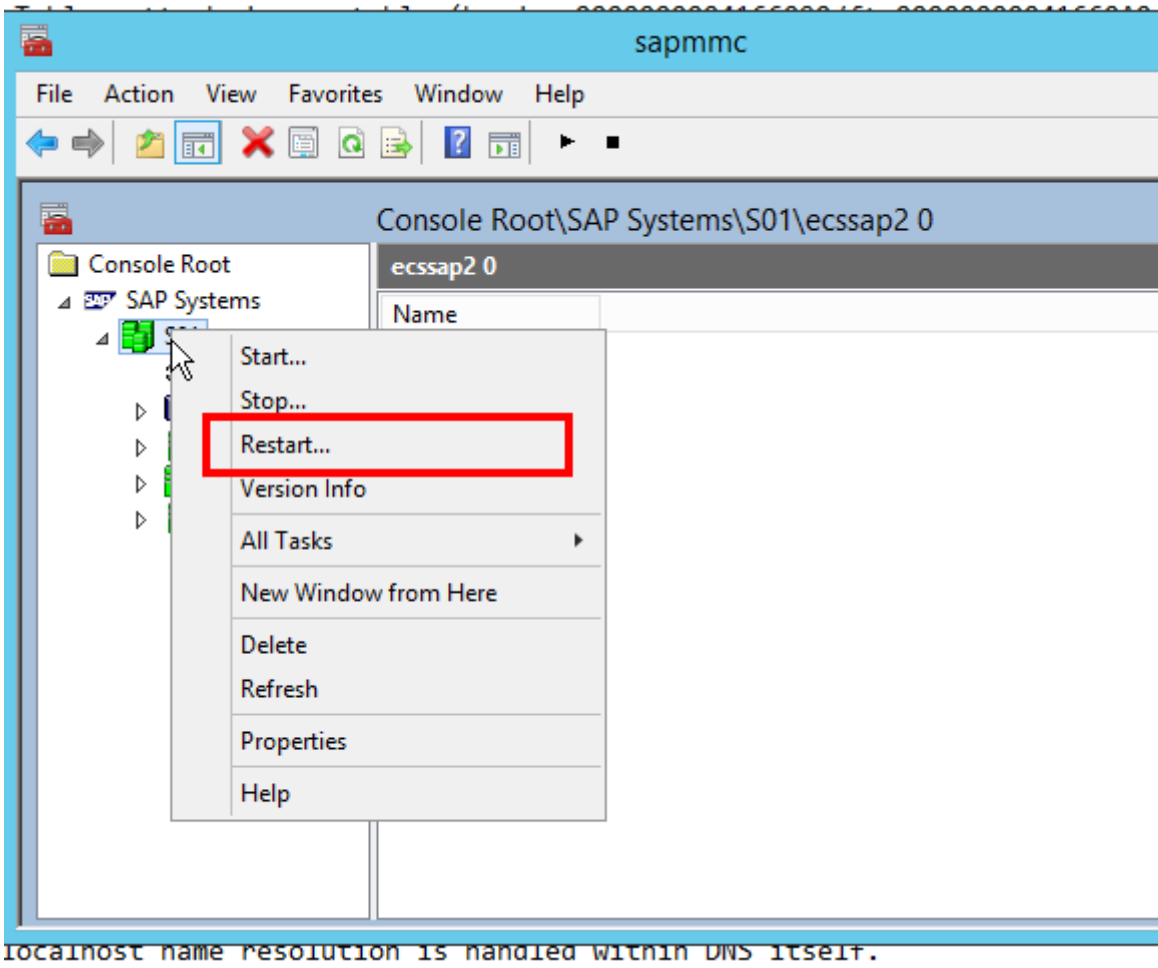


Solution

1. Add the domain name to the hosts file.



2. Restart the SAP. The SAP is successfully started.



3.8 Change History

Table 3-7

Description	Date	Prepared By
Initial version	2020-08-21	Xiong Peng/00508152
Optimized operations.	2021-05-20	Fu Chuandong/00469497

4 SAP S/4HANA (1809) HA Deployment Best Practice

4.1 Overview

This document provides instructions to prepare resources (such as ECSs and network resources) on the public cloud platform, and install SAP S/4HANA (1809) in high availability (HA) mode. SAP S/4HANA is authorized in Bring Your Own License (BYOL) mode. In this mode, you must log in at **SAP Support Portal Home** and apply for a license.

This document cannot replace the standard SAP document. If you have any trouble in installing and using SAP S/4HANA due to its own problems, contact the SAP technical support.

This document is written based on the OS SUSE Linux Enterprise Server. The deployment modes mentioned in the document are only for reference. Install SAP S/4HANA by referring to the standard SAP installation manual or based on sizing results and site requirements.

For details about the official SAP installation guide and related notes, see the following documents:

- **SAP Installation Guides**
- **SAP Notes**
- **SAP Library**

4.2 Preparations

Logging in to Huawei Cloud

Before deploying the SAP system on Huawei Cloud, register a Huawei ID and enable Huawei Cloud services. Through this account, you can use Huawei Cloud services and pay only for the services you use.

For details, see **Registering a HUAWEI ID and Enabling Huawei Cloud Services**

You can log in to Huawei Cloud using any of the methods described in **Logging In to Huawei Cloud**.

SAP License

BYOL is used for authorizing SAP HANA and SAP S/4HANA. You need to log in at **SAP Support Portal Home** and apply for the licenses.

NAT Server

Prepare a Network Address Translation (NAT) server on which SAP Studio for accessing SAP HANA and SAP GUI for accessing SAP applications are installed.

4.3 Resource Planning

4.3.1 Network Planning

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

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

NOTE

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

Figure 4-1 shows the network planning in HA scenario.

Figure 4-1 Network planning in HA scenario

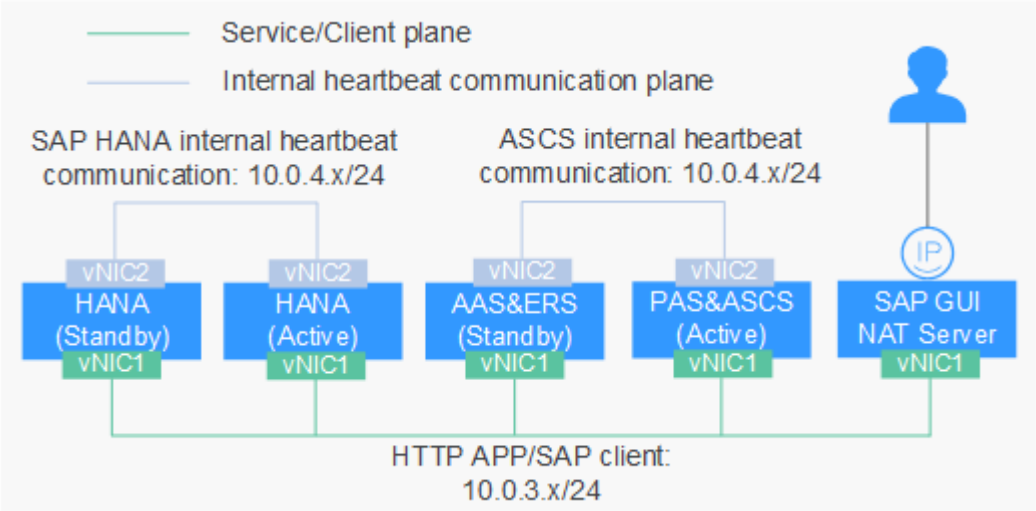


Table 4-1 describes the network planning parameters.

Table 4-1 Network planning parameters

Parameter	Description	Example Value
IP address of the server/client plane	Specifies the IP address of the primary NIC plane. The active and standby ASCS nodes communicate with the SAP GUI and SAP HANA databases using this IP address.	Active ASCS node: 10.0.3.10 ERS node: 10.0.3.20 Active HANA node: 10.0.3.30 Standby HANA node: 10.0.3.40
IP address of the internal heartbeat communication plane	The active and standby ASCS nodes use this network plane to communicate with each other. The active and standby SAP HANA databases use this network plane to communicate with each other.	Active ASCS node: 10.0.4.110 ERS node: 10.0.4.120 Active HANA node: 10.0.4.130 Standby HANA node: 10.0.4.140

4.3.2 Security Group Rules

SAP HANA Security Group Planning

Table 4-2 describes the SAP HANA 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 needed.
- In the following table, ## stands for the SAP HANA instance ID, such as **00**. The instance ID must be the same as that specified during SAP HANA software installation. For details about SAP HANA instance ID planning, see **SAP HANA ECS Planning**.
- For more information about the specific ports to be accessed by SAP software and security group rules, see **SAP official documents**.

Table 4-2 SAP HANA security group rules

Source/ Destination	Protocol	Port Range	Description
Inbound			
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.
0.0.0.0	TCP	22	Allows users to access the SAP HANA Studio using Secure Shell (SSH) protocol. This rule is required only when SAP HANA Studio is deployed on a Linux ECS.
0.0.0.0	TCP	3389	Allows users to access the SAP HANA Studio using Remote Desktop Protocol (RDP). This rule is required only when the SAP HANA Studio is deployed on a Windows ECS.
10.0.0.0/24	TCP	80 (HTTP)	Allows users to access the NAT server using Hypertext Transfer Protocol (HTTP).
10.0.0.0/24	TCP	443 (HTTPS)	Allows users to access the NAT server using Hypertext Transfer Protocol Secure (HTTPS).
10.0.0.0/24	TCP	1128-1129	Allows access to SAP Host Agent using SOAP/HTTP.

Source/ Destination	Protocol	Port Range	Description
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	Allows Software Update Manager (SUM) to access SAP HANA using HTTP.
10.0.0.0/24	TCP	8443	Allows Software Update Manager (SUM) to access SAP HANA using HTTPS.
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.
Outbound			
All	All	All	Security group rule created by the system by default Allows SAP HANA to access all peers.

SAP S/4HANA Security Group Planning

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

You can configure the security group by referring to **Table 4-3**.

NOTE

- Plan the network segments and IP addresses based on the site requirements. The following security group rules are recommended practices. You can configure your own security group rules as needed.
- In the following table, ## stands for the SAP S/4HANA instance ID, which must be consistent with the instance ID specified when the SAP S/4HANA software is installed.

Table 4-3 SAP S/4HANA security group rules

Source/ Destination	Protocol	Port Range	Description
Inbound			
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.
10.0.3.0/24	TCP	32##	Allows SAP GUI to access SAP S/4HANA.
10.0.3.0/24	TCP	36##	Message Port with profile parameter rdisp/msserv
10.0.3.0/24	TCP	5##13 ~ 5##14	Allows ASCS to access SAP application server.
10.0.3.0/24	TCP	33##, 38##, 48##	Port used by CPIC and RFC
10.0.3.0/24	TCP	22	Allows SAP S/4HANA to be accessed using SSH.
10.0.3.0/24	TCP	123	Allows other servers to synchronize time with SAP S/4HANA.
Outbound			
All	All	All	Security group rule created by the system by default Allows SAP 4/HANA to access all peers.

4.3.3 File System Planning

SAP HANA File System Planning

Table 4-4 describes the specifications of the file system planned for SAP HANA.

Table 4-4 File system planned for SAP HANA

Mount Point	File System Capacity (GB)	File System Type	Shared	Remarks
/	40 GB or larger	N/A	No	OS volume
/hana/data	400	xfs	No	Data volume: ultra-high I/O; it is recommended that the capacity of the data volume be at least one time the size of the memory; use two physical disks to make a data volume in using Logical Volume Manager (LVM).
/hana/log	200	xfs	No	Log volume: ultra-high I/O; when the memory is less than or equal to 512 GB, the log volume capacity is half of the memory and rounded up for decimal places. When the memory is greater than 512 GB, the log volume capacity is 512 GB.
/hana/shared	400	xfs	No	Shared volume. If the memory size is smaller than 1 TB, the recommended volume size is at least one time that of the memory size. If the memory size is larger than or equal to 1 TB, the recommended volume size is up to 1 TB.
/hana/backup	Auto expansion	(Optional) SFS/SFS Turbo	No	Create an SFS or SFS Turbo file system as the backup volume.

Mount Point	File System Capacity (GB)	File System Type	Shared	Remarks
/usr/sap	50	xfs	No	/usr/sap volume
N/A	10	swap	No	Swap volume
N/A	10	N/A	Yes (SCSI)	SBD volume. You need to create this volume on the active HANA node and mount this volume to the standby HANA node. The SBD volume does not need to be formatted.

NOTE

You only need to create an SBD volume on the active ECS and mount it to the standby ECS.

SAP S/4HANA File System Planning

Table 4-5 describes the specifications of the file system planned for SAP S/4HANA.

Table 4-5 File system planned for SAP S/4HANA

Mount Point	File System Capacity (GB)	File System Type	Shared	Description
/	40 GB or larger	N/A	No	OS volume
/usr/sap	50	xfs	No	/usr/sap volume
/sapmnt	40	SFS	Yes	Shared to all nodes in the SAP S/4HANA system
/sapcd	Auto expansion	SFS	Yes	Stores the SAP installation package, which is shared to all nodes in the SAP S/4HANA system.
/usr/sap/trans	60	SFS	Yes	Shared to all nodes in the SAP S/4HANA system

Mount Point	File System Capacity (GB)	File System Type	Shared	Description
/usr/sap/<SID>/ASCS##	80	xfs	Yes	Shared to the active ASCS node, which is used to install the ASCS instance.
/usr/sap/<SID>/ERS##	80	xfs	Yes	Shared to the standby ASCS node, which is used to install the ERS instance.
N/A	10	N/A	Yes	SBD volume, which is shared to the active and standby nodes.
N/A	30G	swap	No	Swap volume

NOTE

SID is the SID parameter specified when SAP S/4HANA is installed., and *##* indicates the instance number when ASCS and ERS are installed. For details, see **SAP S/4HANA ECS Planning**.

4.3.4 ECS Planning

SAP HANA ECS Planning

- ECS specifications

SAP HANA ECSs must be certified by SAP. For details about the SAP-certified ECSs, visit **https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/#/solutions?filters=iaas;ve:5**.

- OS

  Table 4-6 lists the OS supported by SAP HANA ECSs.

  Table 4-6 SAP HANA ECS OS

Name	Specifications
OS	SUSE Linux Enterprise Server for SAP Applications 15 SP1

- SAP HANA node planning

  You need to create two ECSs, hana001 and hana002, for installing SAP HANA. ECS hana001 is the active SAP HANA node, and ECS hana002 is the standby SAP HANA node. **Table 4-7** describes SAP HANA node information.

Table 4-7 SAP HANA node information

ECS Name	Role	Server/ Client IP Address	System Replication/ Heartbeat IP Address	Floating IP Address	SID	Instance Number
hana001	Active HANA node	10.0.3.30	10.0.4.130	10.0.3.100	S00	00
hana002	Standby HANA node	10.0.3.40	10.0.4.140			

SAP S/4HANA ECS Planning

- ECS specifications

  Before applying for SAP S/4HANA ECSs, evaluate the SAP Application Performance Standard (SAPS) value based on the standard SAP Sizing method. Then apply for the ECSs based on the evaluation results. For details, see **SAP Quick Sizer**.

  For details about the minimum hard disk space, RAM, and minimum software requirements of each component in SAP S/4HANA, see SAP note **1953429** and **SAP Installation Guides**.

  SAP-certified ECSs must be used for installing SAP S/4HANA. For details, see *SAP Note 2582296 - SAP Applications on Huawei Cloud Supported Products and ECS VM types*.

- OS

  Table 4-8 lists the OS supported by SAP S/4HANA ECSs.

  Table 4-8 SAP S/4HANA ECS OS

Name	Specifications
OS	SUSE Linux Enterprise Server for SAP Applications 15 SP1

- SAP S/4HANA node planning

  Two ECSs, s4001 and s4002, need to be created for installing SAP S/4HANA. s4001 is the active node and s4002 is the standby node.

Table 4-9 SAP S/4HANA node information

ECS Name	Server/ Client IP Address	Active Heartbeat IP Address	Type	Instance Number	SID	Virtual IP Address
S4001	10.0.3.10	10.0.4.110	ASCS Instance	01	S01	10.0.3.110 10.0.3.120
			PAS Instance	02		
			DB Instance	None		
S4002	10.0.3.20	10.0.4.120	ERS Instance	10		
			AAS Instance	03		

4.4 Resource Creation

4.4.1 Creating a VPC

The Virtual Private Cloud (VPC) service enables you to provision logically isolated, configurable, and manageable virtual networks for cloud servers, cloud containers, and cloud databases, improving cloud service security and simplifying network deployment. With a VPC, you can configure and manage the networks in the VPC, and make changes to these networks as needed, quickly and securely. For more information about VPC, see **VPC Overview**.

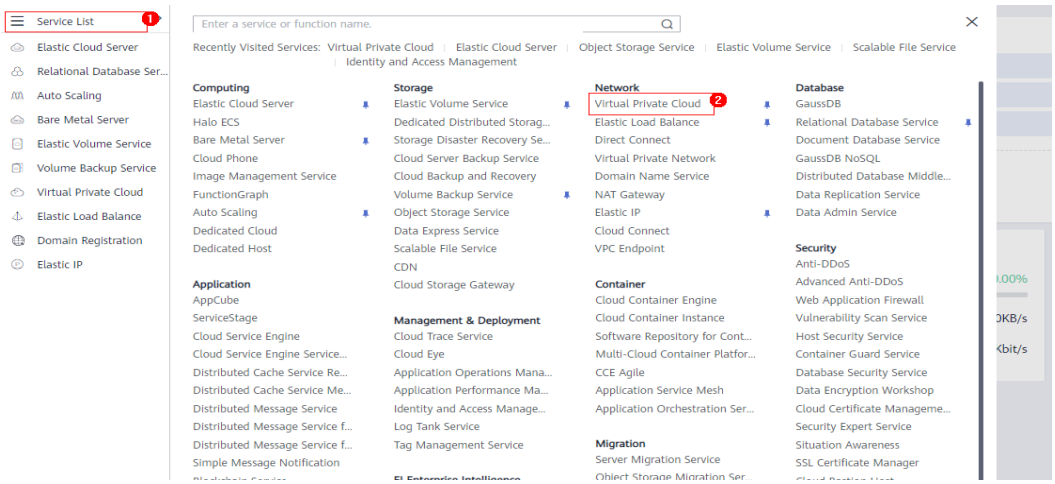
When creating a VPC, create two subnets 10.0.3.0 and 10.0.4.0, which are used as the server/client plane IP address and system replication/heartbeat plane IP address of SAP HANA and SAP S/4HANA.

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 Click in the navigation pane on the left, and choose **Network > Virtual Private Cloud**.



Step 4 Click **Create VPC** on the right of the page.

Step 5 Configure required parameters as prompted based on **Table 4-10**.

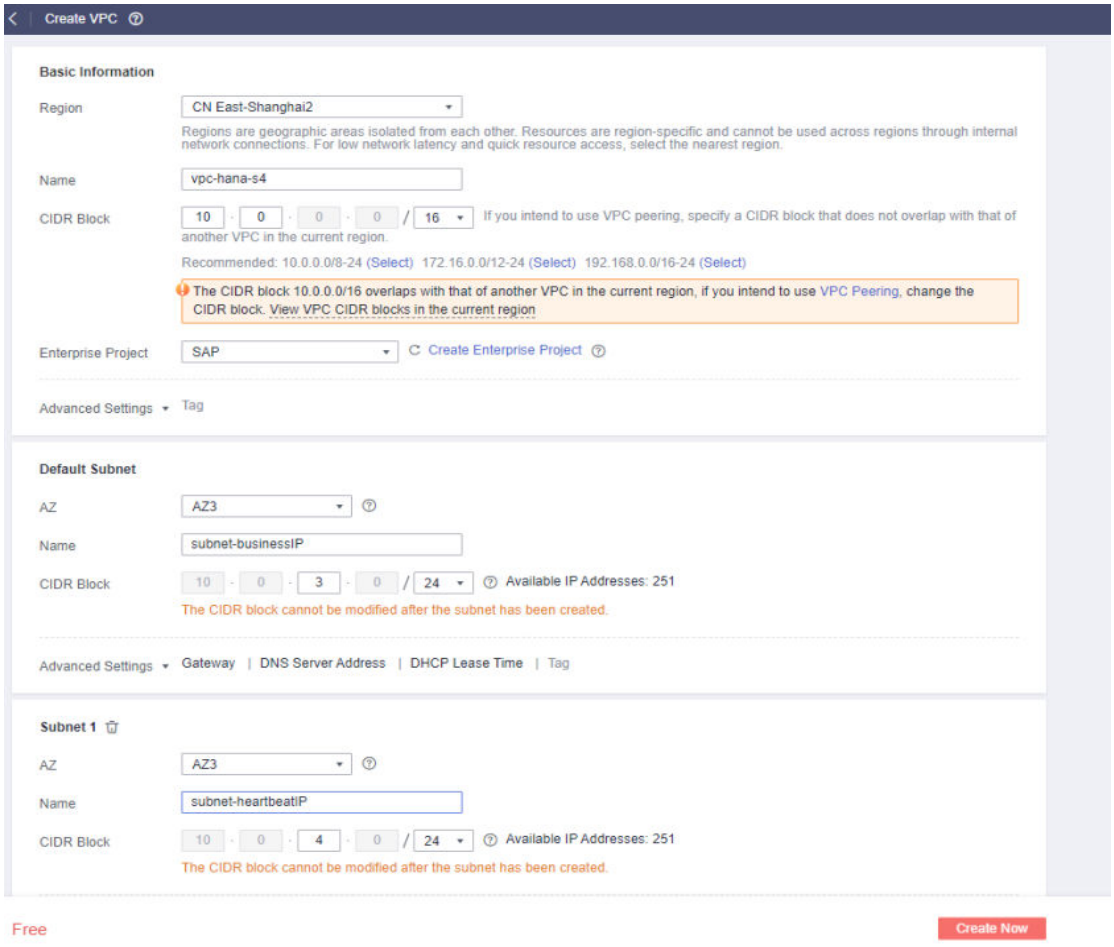


Table 4-10 Parameters required for creating a VPC

Category	Parameter	Description
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 on the upper left of the page to change the region.
	Name	VPC name
	CIDR Block	CIDR block of 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 in the VPC). 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 **Network Planning**.
	Enterprise Project	When creating a VPC, you can add the VPC to an enabled enterprise project. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**. For details about creating and managing enterprise projects, see the **Enterprise Management User Guide**.
	Tag	VPC tag that 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. For details about naming rules of tags, see **Tag Naming Rules**.

Category	Parameter	Description
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 private networks.
	Name	Subnet name
	CIDR Block	CIDR block for the subnet. This value must be within the VPC CIDR block. Configure the subnet CIDR block based on the information provided in **Network Planning**.
	Advanced Settings	Click **Advanced Settings** to set parameters such as **Gateway** and **DNS Server Address**.
	Gateway	Gateway address of the subnet
	DNS Server Address	External DNS server addresses are used by default. If you need to change the DNS server address, ensure that the DNS server addresses you configured are available.
	DHCP Lease Time	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.
	Tag	Subnet tag that 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**.
Add Subnet	You can click **Add Subnet** to add a subnet.	

Step 6 Click **Create Now**.

----End

4.4.2 Creating a Security Group

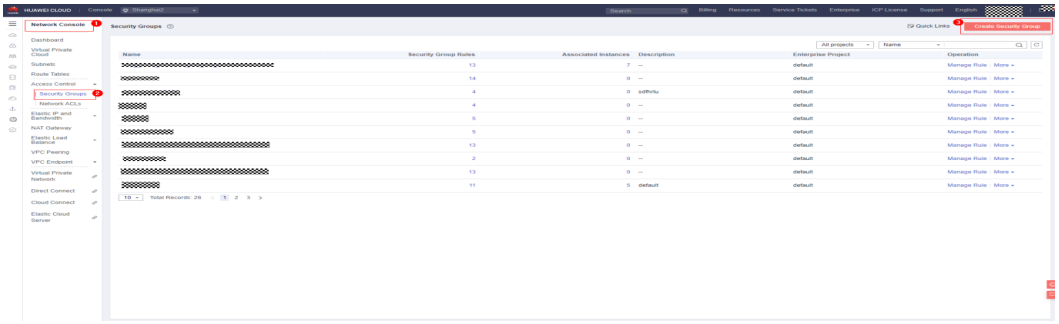
A security group is a collection of access control rules for ECSs that have the same security protection requirements and are mutually trusted. After a security group is created, you can create various access rules for the security group, and these rules will apply to all ECSs added to this security group. For more information about security groups, see **Security Group Overview**.

You need to create two security groups, one for the active and standby SAP HANA ECSs, and the other for the active and standby SAP S/4HANA ECSs.

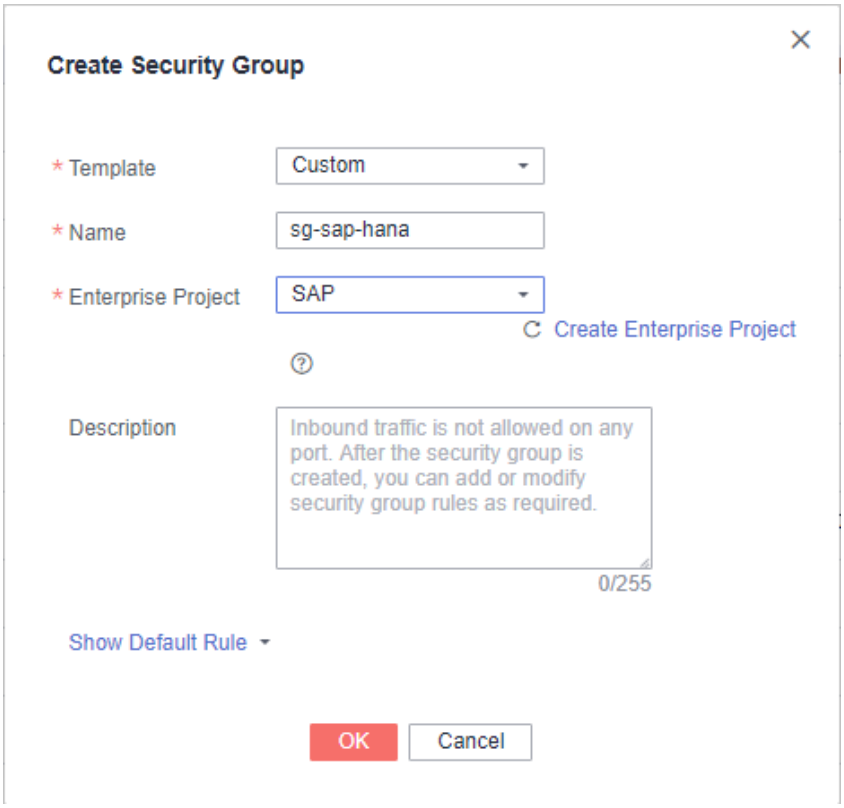
Procedure

Step 1 Create a security group for SAP HANA ECSs.

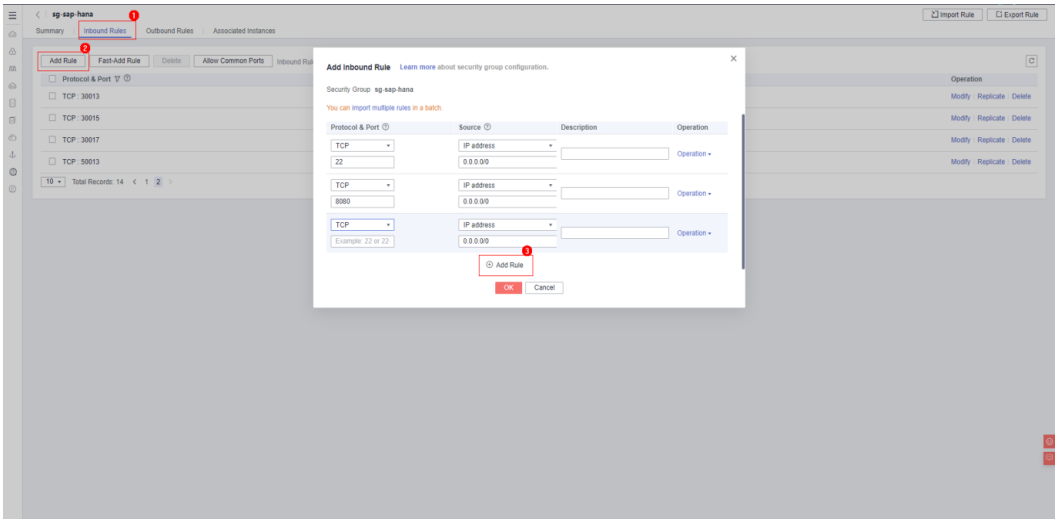
1. Choose **Access Control** > **Security Groups** in the navigation pane on the left of the VPC console. On the **Security Groups** page, click **Create Security Group**.



2. On the **Security Group** page, click **Create Security Group**.
   - **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, **sg_sap_hana**.
   - **Enterprise Project**: You can add the security group to an enabled enterprise project. You can select an enterprise project from the drop-down list, for example, **SAP**.

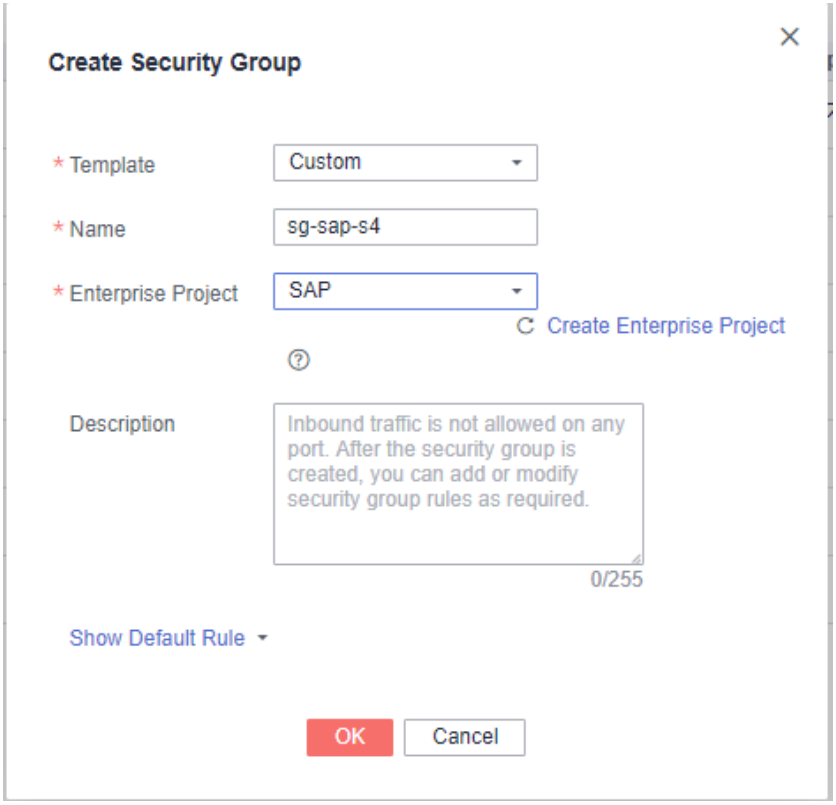


3. Click **OK**.
4. Locate the row that contains the newly created security group **sg-sap-hana**, click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, add the desired ports based on **Table 4-2**.

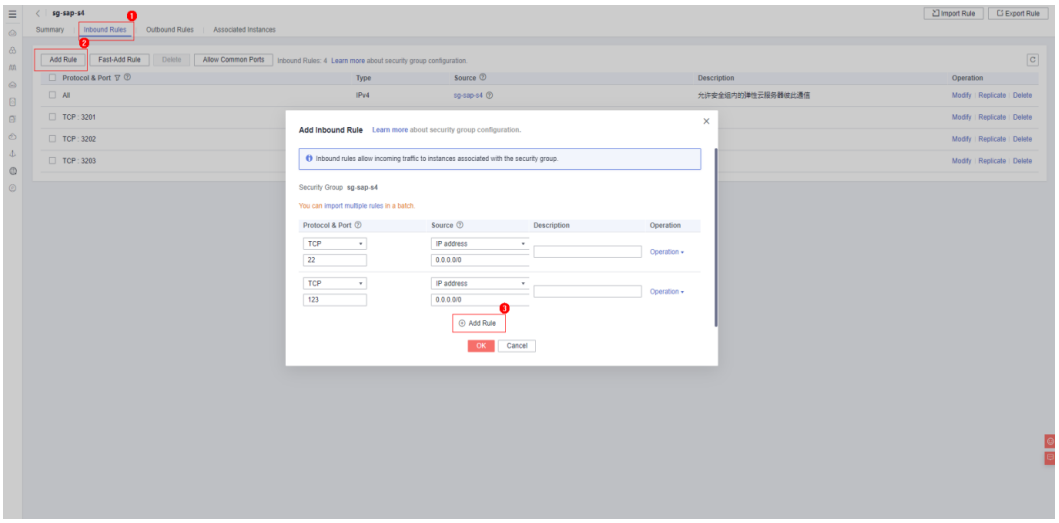


Step 2 Create a security group for SAP S/4HANA ECSs.

1. Choose **Access Control** > **Security Groups** in the navigation pane on the left of the VPC console. On the **Security Groups** page, click **Create Security Group**.
2. Set parameters required for creating a security group (sg-sap-s4) for SAP S/4HANA ECSs as prompted.



3. Locate the row that contains the newly created security group **sg-sap-s4**, click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, add the desired ports based on **Table 4-3**.



----End

4.4.3 Creating an SFS or SFS Turbo File System

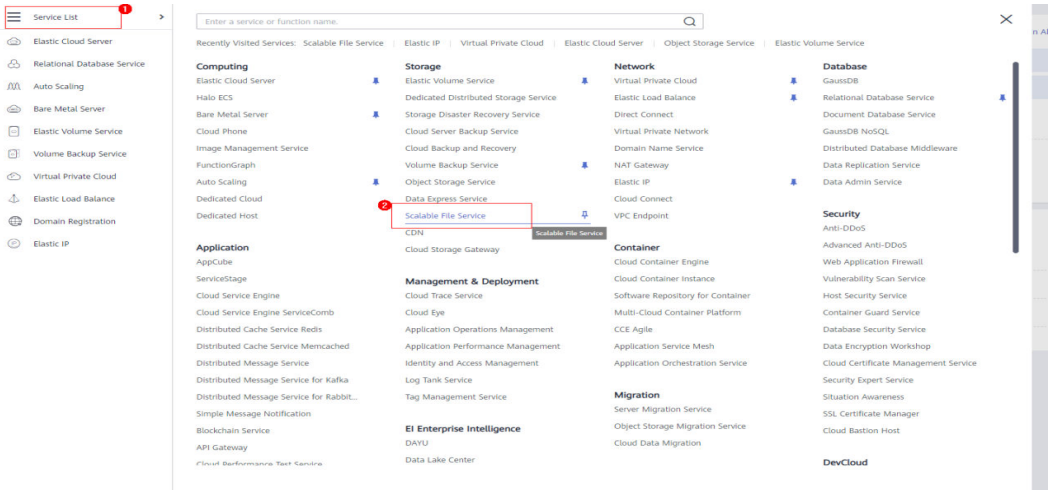
Scalable File Service (SFS) is a network attached storage (NAS) service that provides scalable, high-performance file storage. With the service, shared file access can be achieved among multiple Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), and containers created on Cloud Container Engine (CCE). For more information about SFS, see **SFS Overview**.

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.

Two SFS file systems are created and attached to the active and standby SAP HANA nodes, respectively. You need to create one SFS file system and mount it to **/sapcd** on the active and standby SAP S/4HANA nodes, and create two SFS Turbo file systems and respectively mount them to **/sapmnt** and **/usr/sap/trans** on the active and standby SAP S/4HANA nodes. For the details about the parameter configurations for creating SFS and SFS Turbo file systems, see **Getting Started with SFS**.

Procedure

Step 1 Click ☰ in the navigation pane on the left, and choose **Scalable File Service** under **Storage**.



Step 2 Click **Create File System**. Set required parameters on the displayed page based on **Table 4-11**.

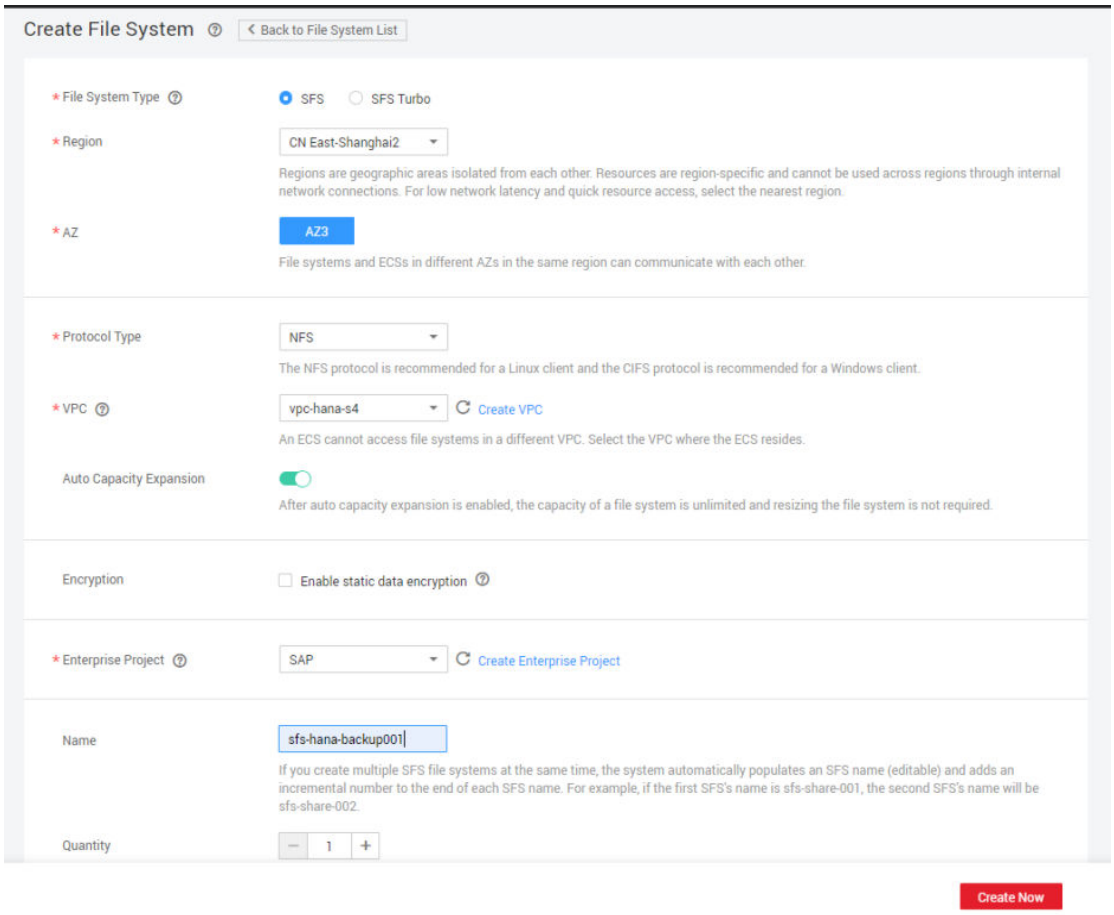


Table 4-11 Parameter description

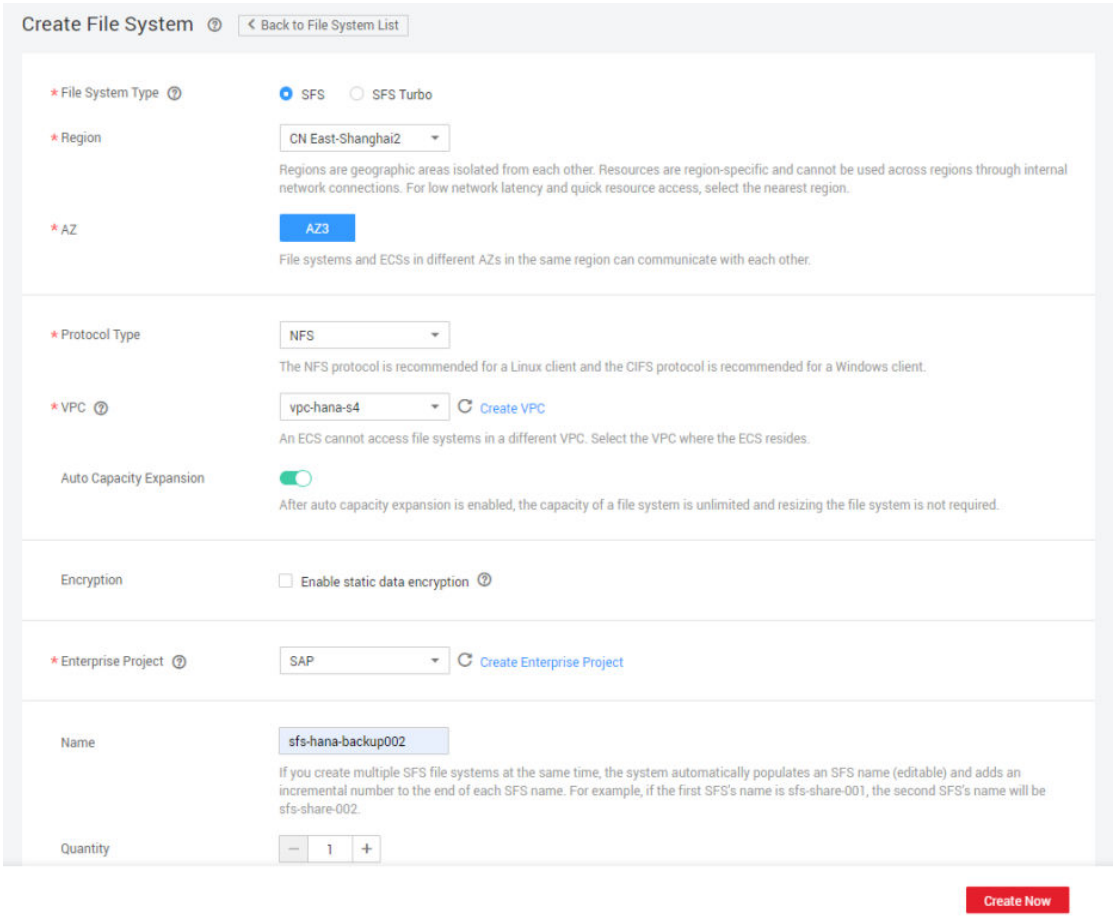
Parameter	Description
File System Type	Select the type of the file system to be created.
Region	Select the target region.
AZ	Specifies the AZ where the file system is located. Select your desired AZ.
Protocol Type	Specifies the protocol type. Select **NFS**.
VPC	Select **vpc-hana-s4** for SAP HANA.
Auto Capacity Expansion	This function is enabled by default. When it is enabled, you do not need to manually adjust the capacity of the file system. You can determine whether to enable the function based on the site requirements.

Parameter	Description
Maximum Capacity	This parameter shows after **Automatic Capacity Expansion** is disabled. Specifies the maximum capacity of a single file system.
Encryption	Optional. 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 select Enable static data encryption, follow the instructions described in **Getting Started with SFS**.
Enterprise Project	Select the target project.
Name	Specifies the file system name.
Quantity	Select the quantity based on the site requirements.

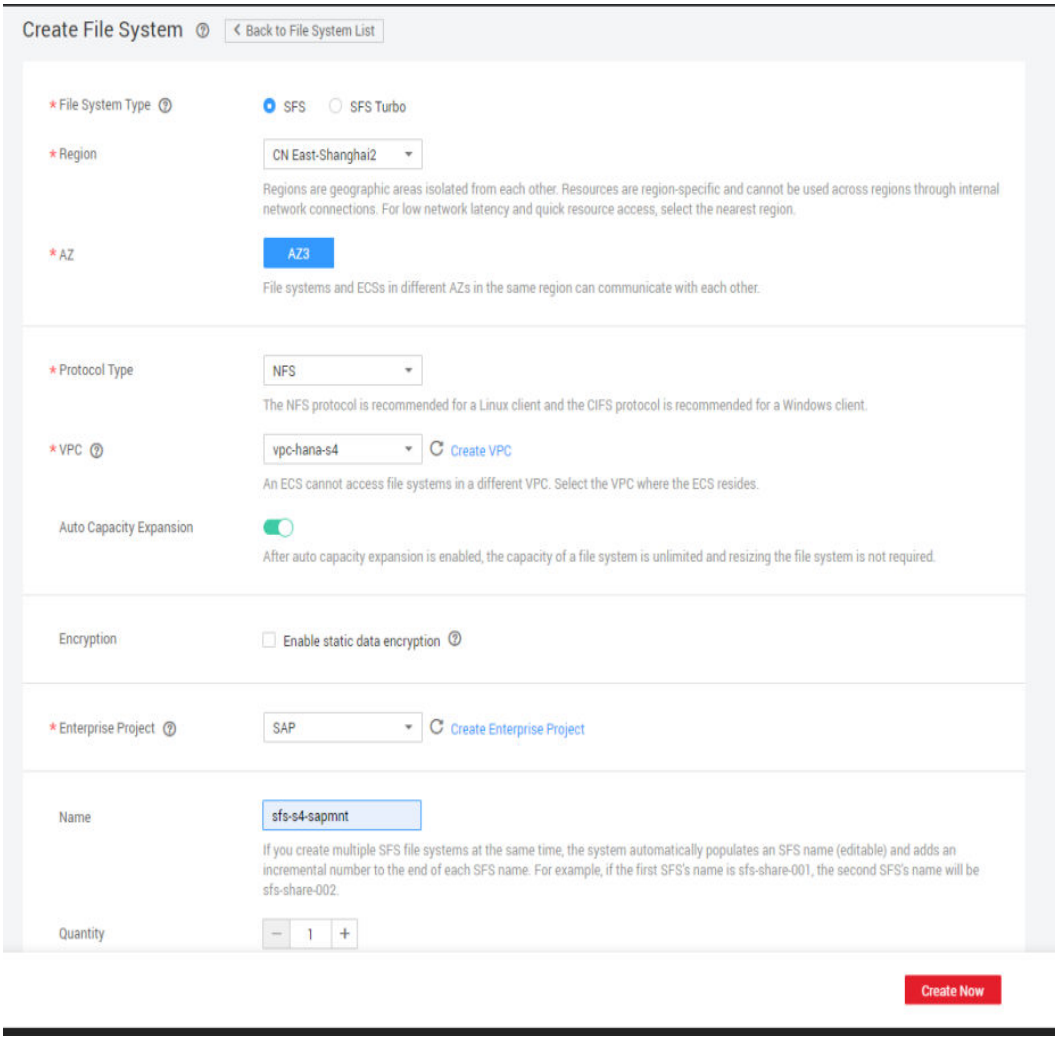
Step 3 Click **Create Now**. Confirm the file system information and click **Submit** on the displayed page. You can locate the created file system using its name in the file system list. In the **Shared Path** column, query the shared path.

Step 4 Repeat **Step 2** and **Step 3** to create other SFS file systems.

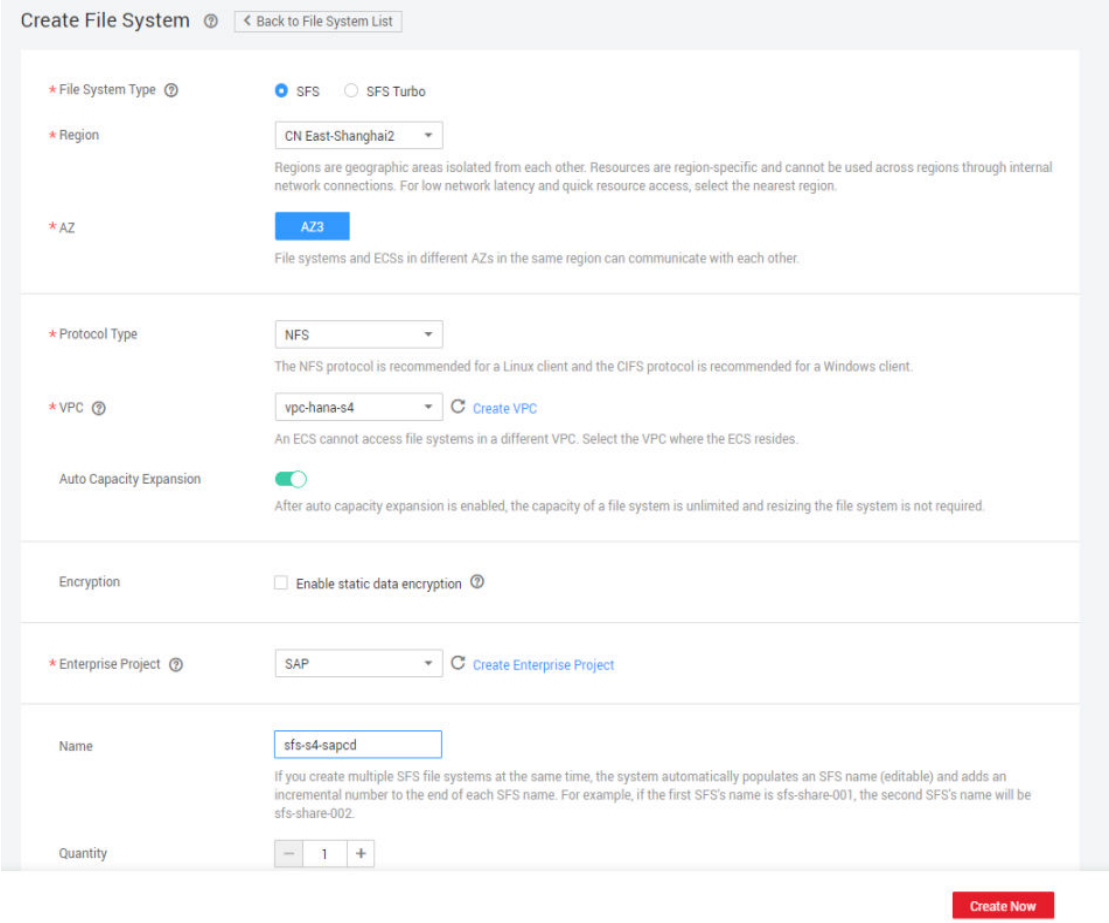
1. Create an SFS file system sfs-hana-backup002 and mount it to the **/hana/backup** directory on the standby SAP HANA node.



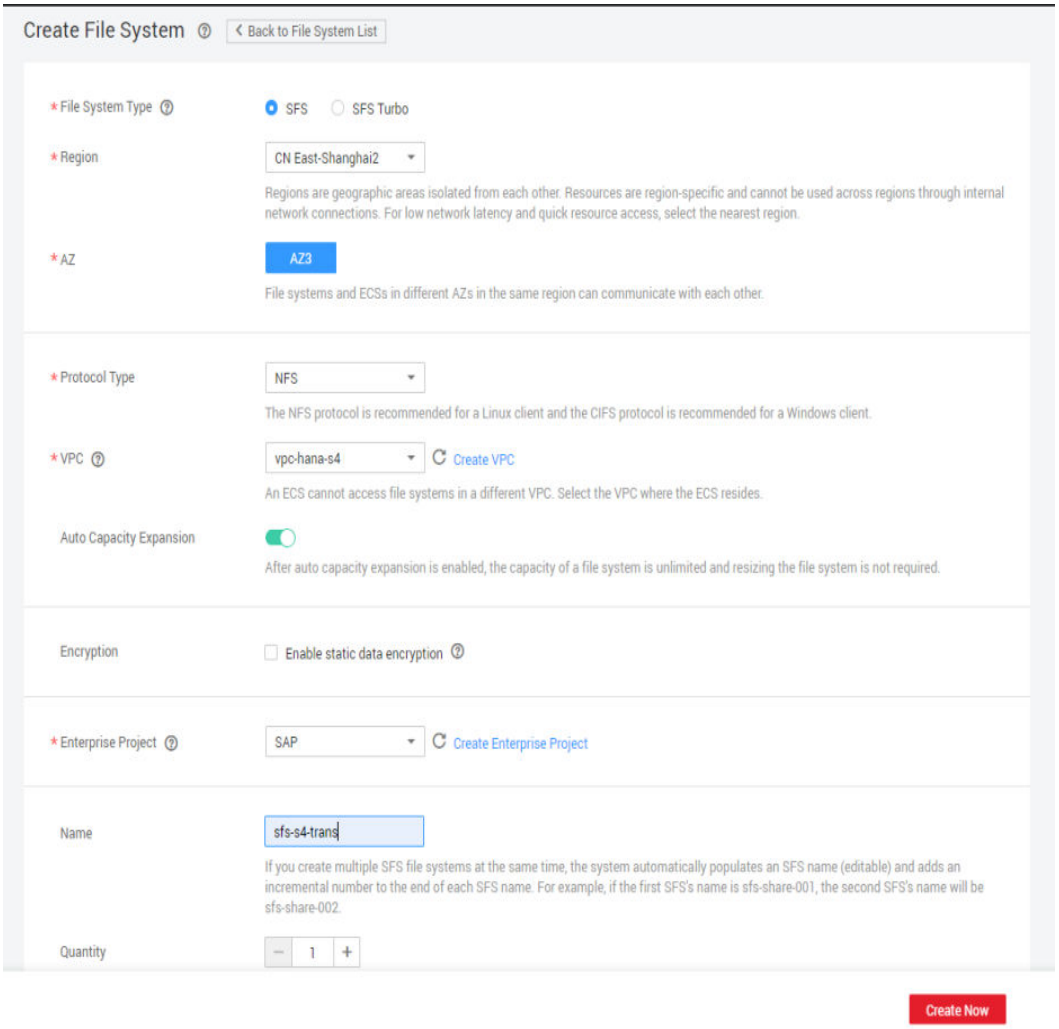
2. Create a 40 GB SFS Turbo file system sfs-turbo-s4-sapmnt and mount it to the **/sapmnt** directory on the active and standby SAP S/4HANA nodes.



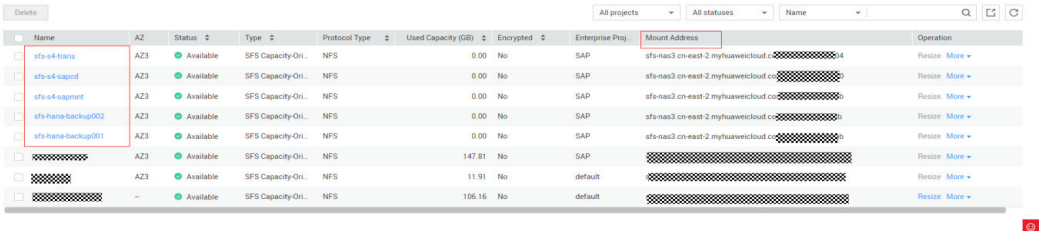
3. Create an SFS file system sfs-s4-sapcd and mount it to the **/sapcd** directory on the active and standby SAP S/4HANA nodes.



4. Create a 60 GB SFS Turbo file system sfs-turbo-s4-trans and mount it to the **/usr/sap/trans** directory on the active and standby SAP S/4HANA nodes.



Step 5 The following figure shows the details about the created SFS file systems.



----End

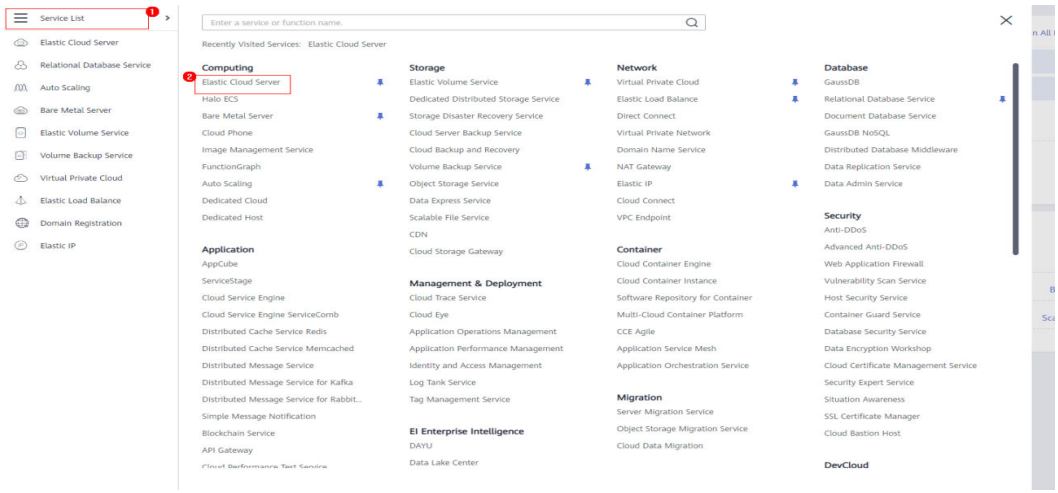
4.4.4 Creating ECSs

4.4.4.1 Creating SAP HANA ECSs

Two ECSs need to be created for installing the SAP HANA software.

Procedure

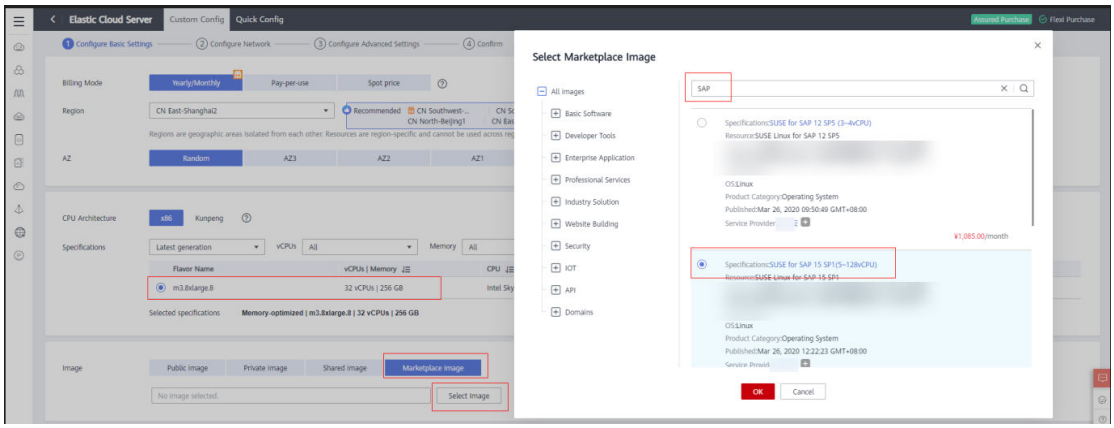
Step 1 Click ☰ in the navigation plane on the left, and choose **Computing** > **Elastic Cloud Server**.

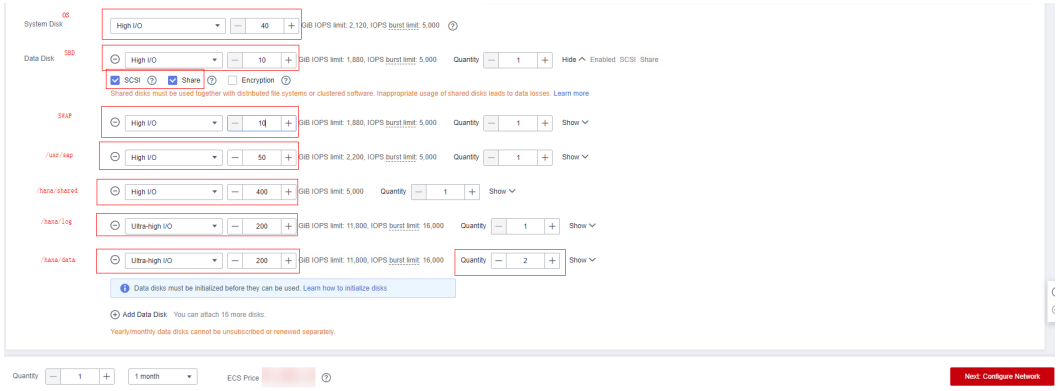


Step 2 Click **Buy ECS**. On the displayed page, configure basic settings of the ECS to be created for the active SAP HANA node. **Table 4-12** describes the parameters.

Table 4-12 Basic settings of the active SAP HANA ECS

Parameter	Description
Billing Mode	Select **Yearly/Monthly**.
Region	Select the target region. For example, **CN East-Shanghai2**.
AZ	Specifies the AZ where ECSs are located. Choose an AZ as required.
CPU Architecture	Select **x86**.
Specifications	For details about SAP HANA ECS specifications, see **SAP HANA ECS Planning**. For example, select **m3.8xlarge.8**.
Image	Select **Marketplace image**. Click **Select Image**, enter **SAP** in the search box, and select **SUSE for SAP 15 SP1**. **NOTE** To use marketplace images, such as **SUSE for SAP 15 SP1**, ensure that your ECS is billed on a yearly/monthly basis.
System Disk	Set this parameter as required. If you need multiple data disks, click **Add Data Disk** to add more data disks.

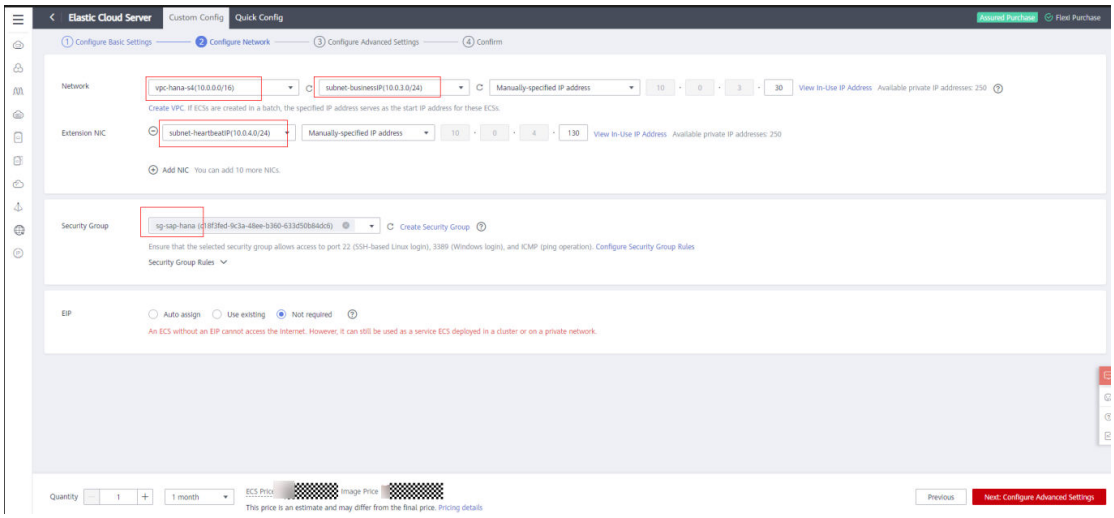




Step 3 Click **Next: Configure Network** and configure network information based on **Table 4-13**.

Table 4-13 Network configuration for the active SAP HANA ECS

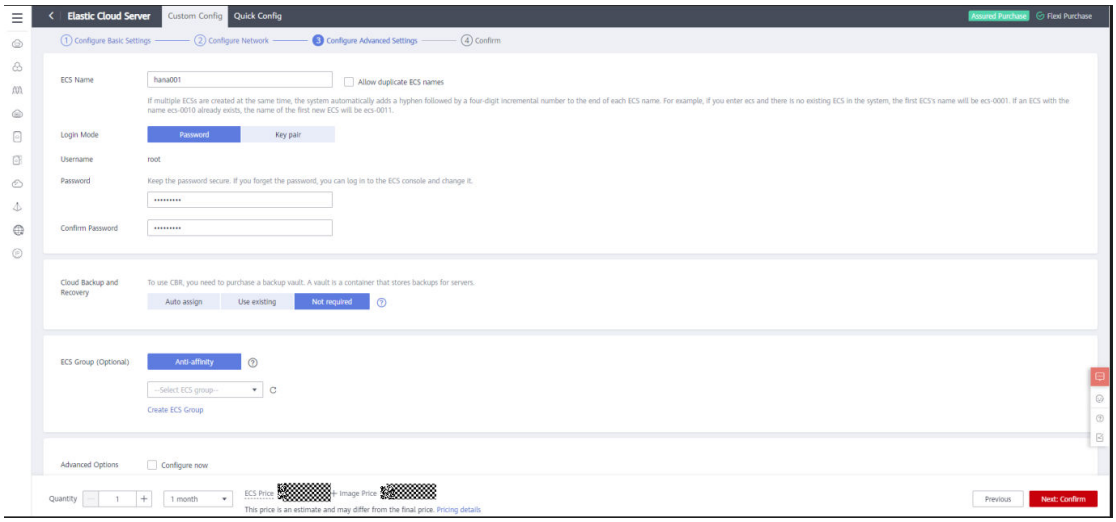
Parameter	Description
Network	Select the VPC and subnet created in **Creating a VPC**.
Extension NIC	If you need more NICs, click **Add NIC**.
Security Group	Select the security group created in **Step 1**.
EIP	Select **Not required**.



Step 4 Click **Next: Configure Advanced Settings**. On the displayed page, configure the advanced settings for the active SAP HANA ECS based on **Table 4-14**.

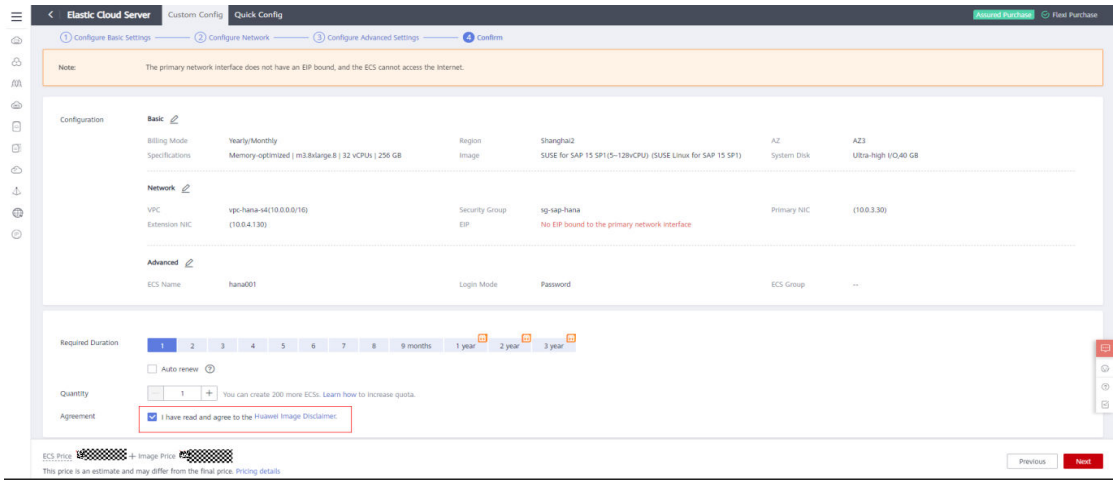
Table 4-14 Advanced settings for the active SAP HANA ECS

Parameter	Description
ECS Name	Enter **hana001**.
Login Mode	Select **Password**.
Cloud Backup and Recovery	Set it based on the site requirements, for example, **Not required**.
ECS Group (Optional)	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. **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**.
Advanced Options	Do not set this parameter.



Step 5 Click **Next: Confirm**.

Check the ECS configurations and select **I have read and agree to the Huawei Image Disclaimer**. Click **Next**.



Step 6 Repeat **Step 2** to **Step 5** to create the ECS hana002 for the standby SAP HANA node.

The procedure for creating the active and standby SAP HANA ECSs is similar. You do not need to create SBD shared volume when creating the standby SAP HANA ECS because you can mount the SBD shared volume created for the active SAP HANA ECS to the standby ECS.

----End

4.4.4.2 Creating SAP S/4HANA ECSs

Two ECSs need to be created for installing the SAP S/4HANA software.

Procedure

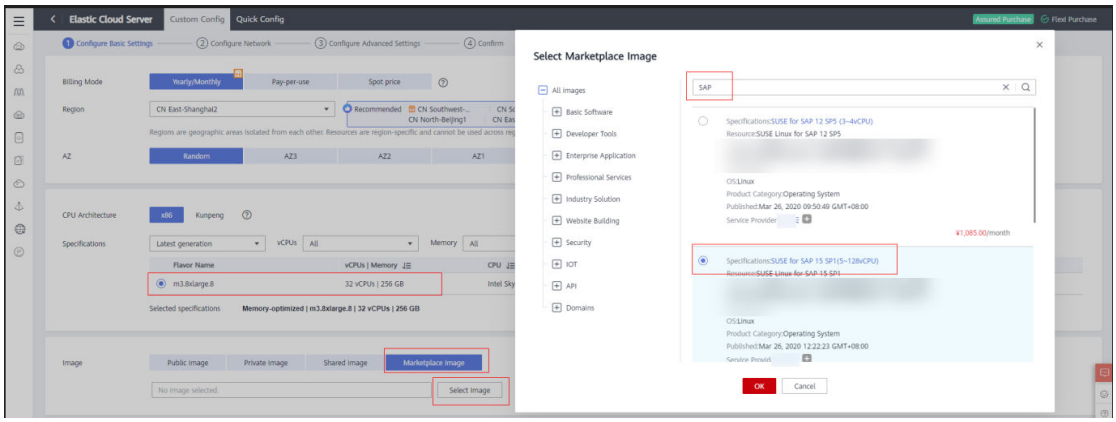
Step 1 On the public cloud management console, click ☰ in the upper left corner and choose **Computing** > **Elastic Cloud Server**.

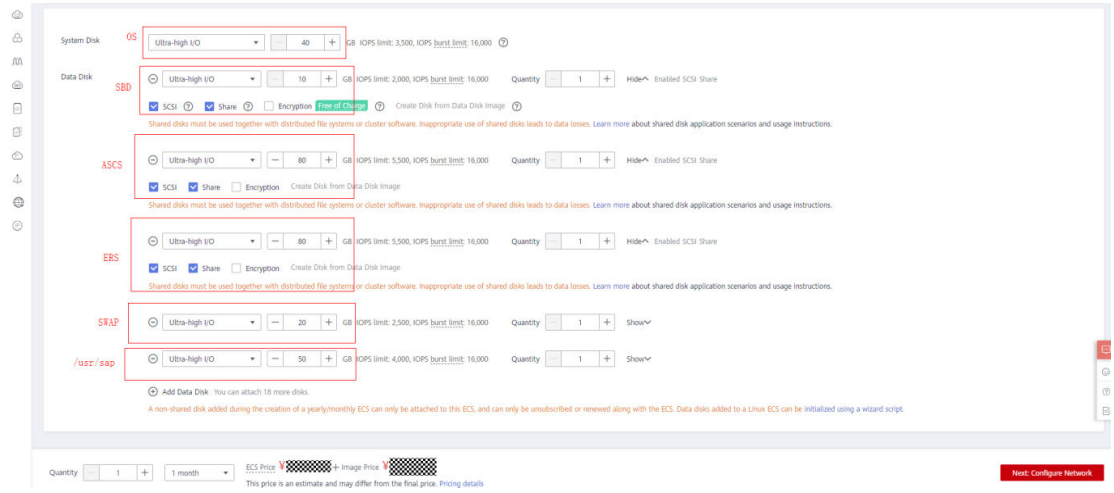
Step 2 Click **Buy ECS** in the upper right corner. A page for creating ECSs is displayed.

Step 3 Ser parameters required for creating the ECS s4001 for the active SAP S/4HANA node based on **Table 4-15**.

Table 4-15 Basic settings of the active SAP S/4HANA ECS

Parameter	Description
Billing Mode	Select **Yearly/Monthly**.
Region	Select the target region. For example, **CN East-Shanghai2**.
AZ	Specifies the AZ where ECSs are located. Choose an AZ as required.
CPU Architecture	Select **x86**.
Specifications	For details about the SAP S/4HANA ECS specifications, see **SAP S/4HANA ECS Planning**. For example, select **c6.4xlarge.4**.
Image	Select **Marketplace image**. Click **Select Image**, enter **SAP** in the search box, and select **SUSE for SAP 15 SP1**. **NOTE** To use marketplace images, such as **SUSE for SAP 15 SP1**, ensure that your ECS is billed on a yearly/monthly basis.
System Disk	Set this parameter as required. If you need multiple data disks, click **Add Data Disk** to add more data disks.

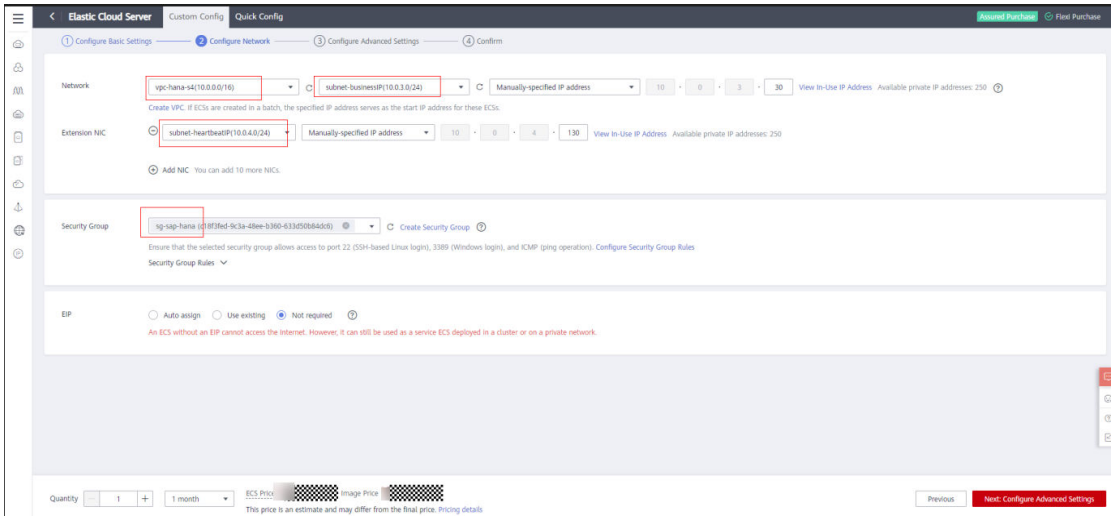




Step 4 Click **Next: Configure Network** and configure network information based on **Table 4-16**.

Table 4-16 Network configurations for the active SAP S/4HANA ECS

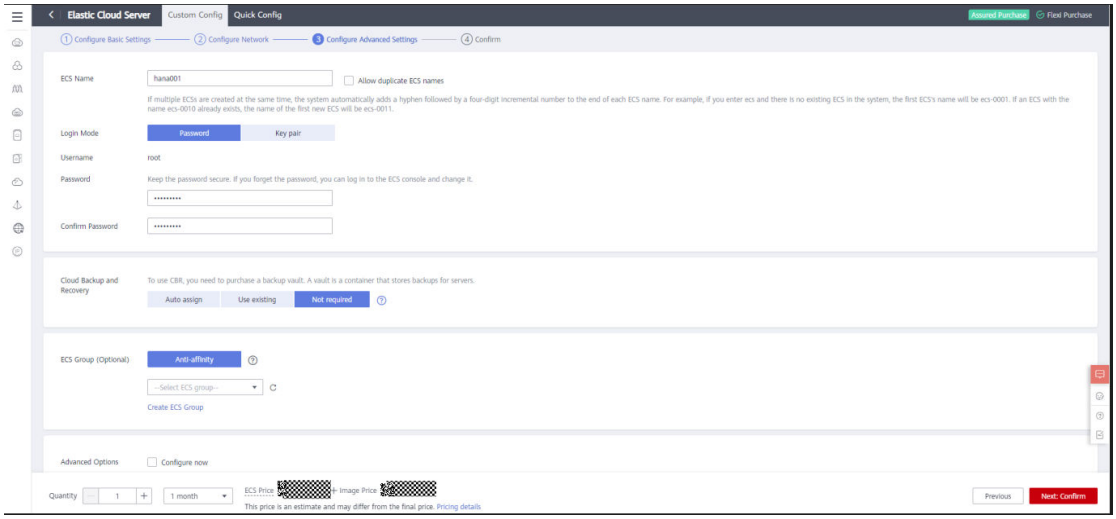
Parameter	Description
Network	Select the VPC and subnet created in **Creating a VPC**.
Extension NIC	If you need more NICs, click **Add NIC**.
Security Group	Select the security group created in **Step 2**.
EIP	Select **Not required**.



Step 5 Click **Next: Configure Advanced Settings**. On the displayed page, configure the advanced settings for the active SAP S/4HANA ECS based on **Table 4-17**.

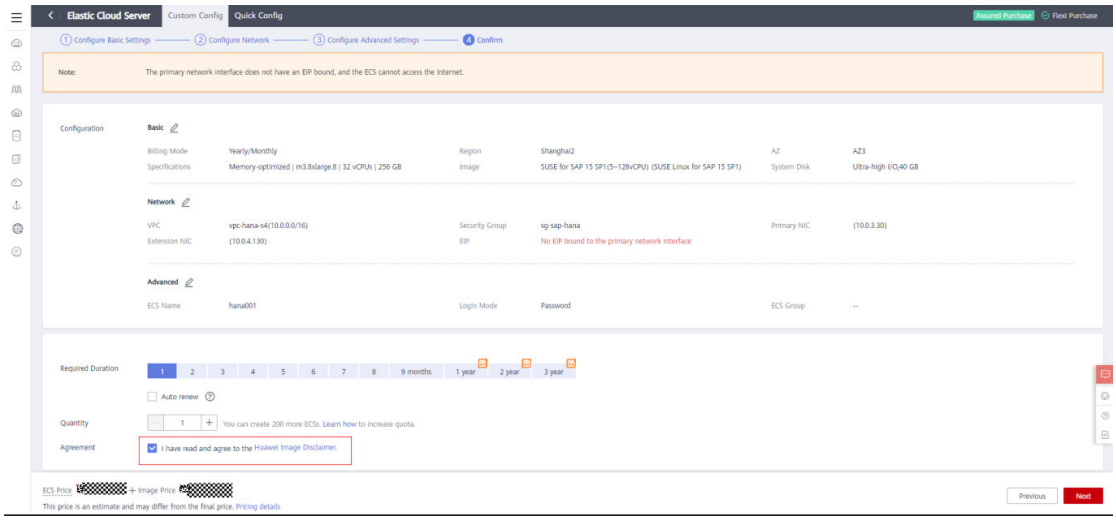
Table 4-17 Advanced settings of the active SAP S/4HANA ECS

Parameter	Description
ECS Name	Enter **s4001**.
Login Mode	Select **Password**.
Cloud Backup and Recovery	Select **Not required**.
ECS Group (Optional)	Specifies a SAP S/4HANA ECS group. When you create ECSs, the system will allocate the ECSs in the same server group to different physical servers to ensure the running reliability of these SAP S/4HANA ECSs. **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**.
Advanced Options	Do not set this parameter.



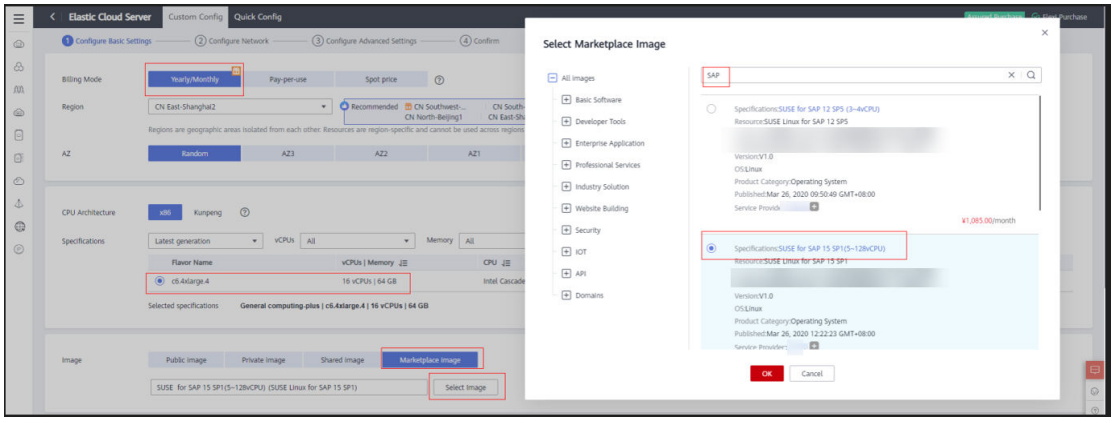
Step 6 Click **Next: Confirm**.

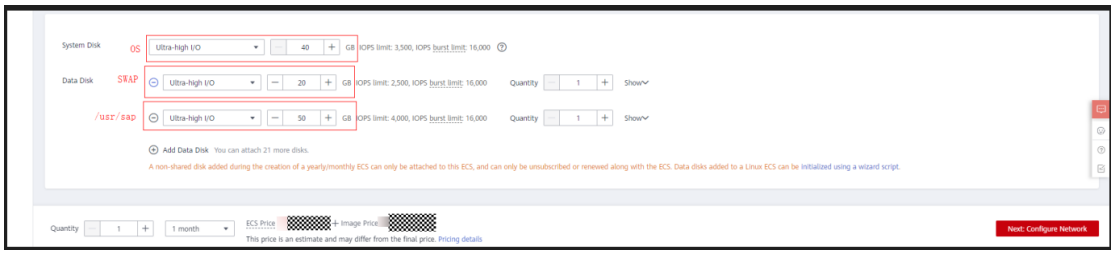
Check the ECS configurations and select **I have read and agree to the Huawei Image Disclaimer**. Click **Next**.



Step 7 Repeat **Step 2** to **Step 6** to create an ECS for the standby SAP S/4HANA node.

When creating the standby SAP S/4HANA ECS, you do not need to create a shared disk.





----End

4.4.5 Assigning a Virtual IP Address

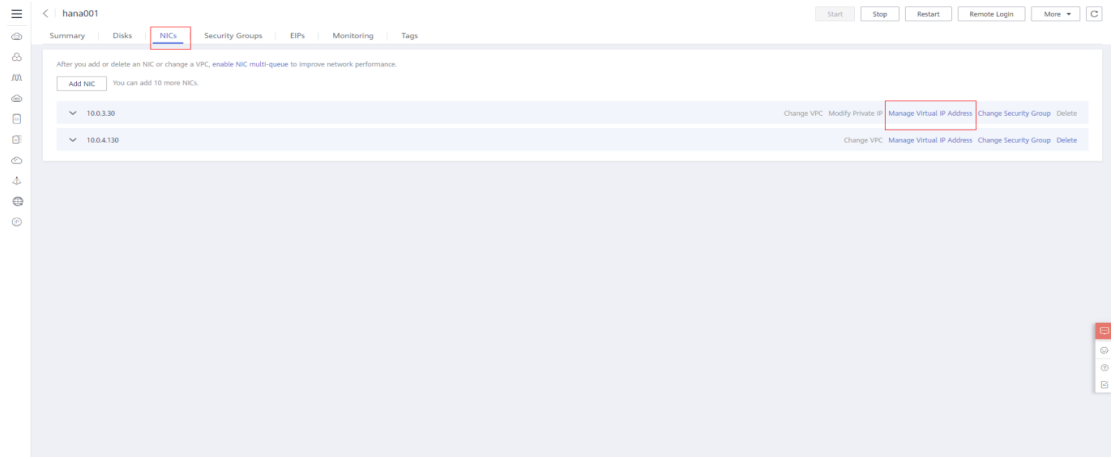
Virtual IP addresses are used for active and standby switchover of ECSs to achieve high availability. If the active ECS becomes faulty and cannot provide services, the virtual IP address is dynamically re-assigned to the standby ECS so services can continue uninterrupted. For more information about virtual IP addresses, see **Virtual IP Address Overview**.

Procedure

Step 1 Click ☰ in the navigation plane on the left, and choose **Computing** > **Elastic Cloud Server**.

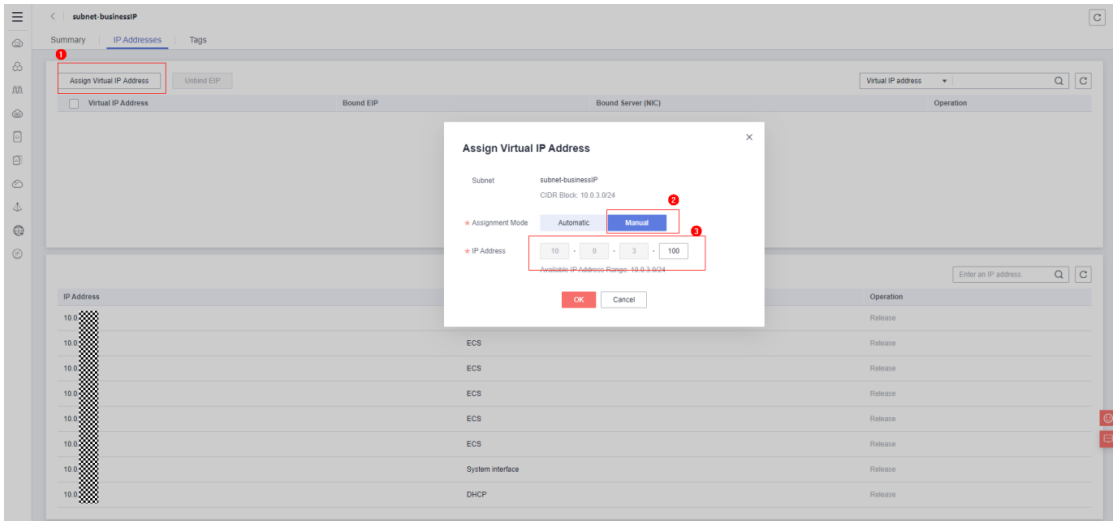
Step 2 In the Elastic Cloud Server list, locate the created active SAP HANA ECS and click the ECS name to view its details.

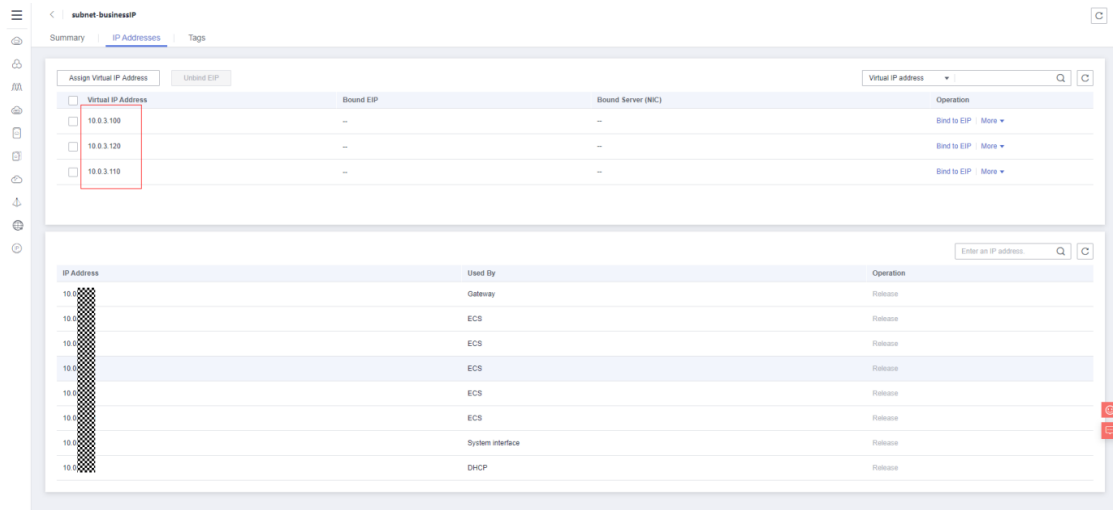
Step 3 Click the **NICs** tab and then **Manage Virtual IP Address** in the row of the ECS service/management plane NIC.



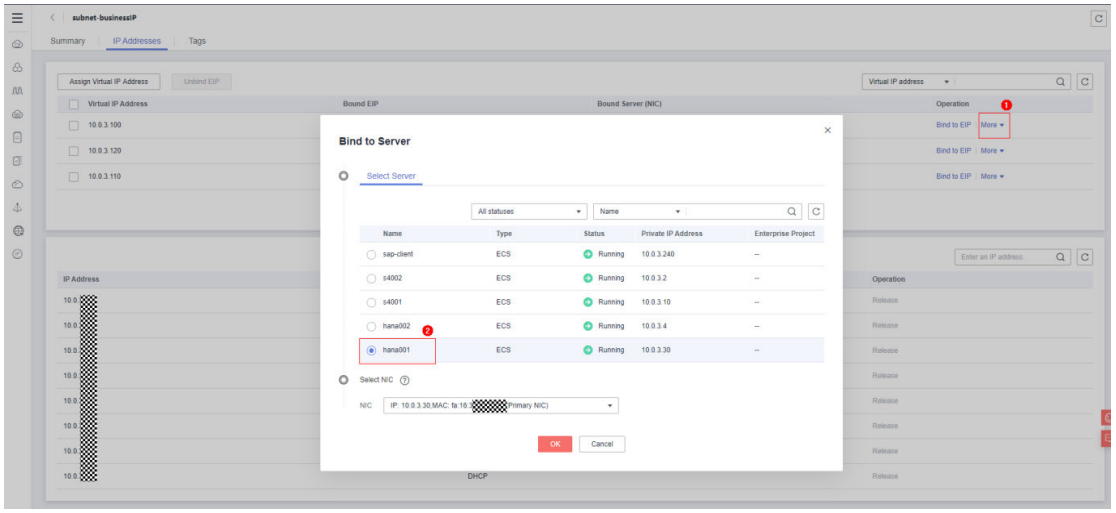
Step 4 Click **Assign Virtual IP Address**. In the dialog box that is displayed, select **Manual** for **Assignment Mode**, and configure the IP address based on **ECS Planning**.

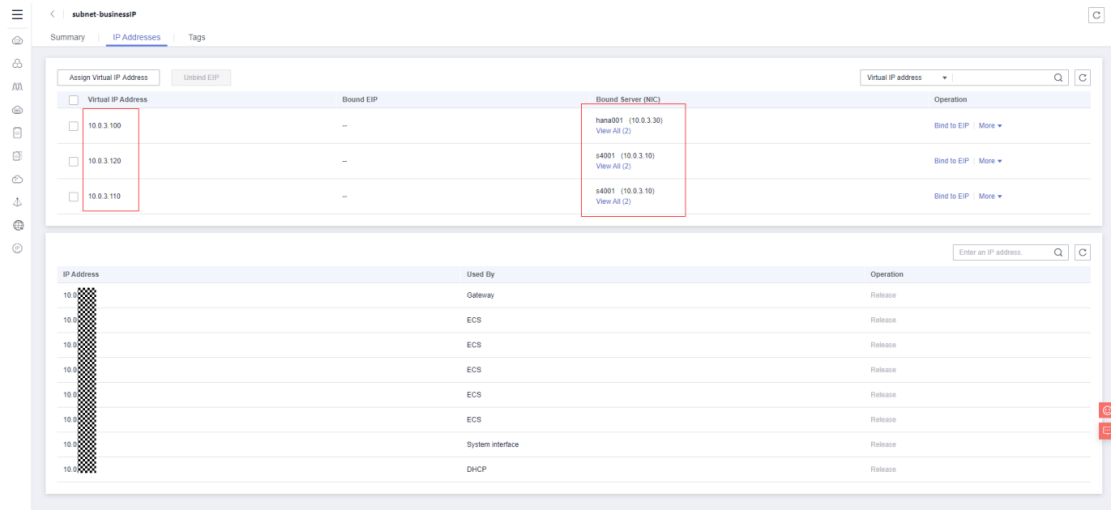
You need to assign three virtual IP addresses: 10.0.3.100, 10.0.3.110, and 10.0.3.120.





Step 5 Select a created virtual IP address and click **More** > **Bind to Server** in the **Operation** column. Bind 10.0.3.100 to the active and standby SAP HANA ECSs, and respectively bind 10.0.3.110 and 10.0.3.120 to the active and standby SAP S/4HANA ECSs.





----End

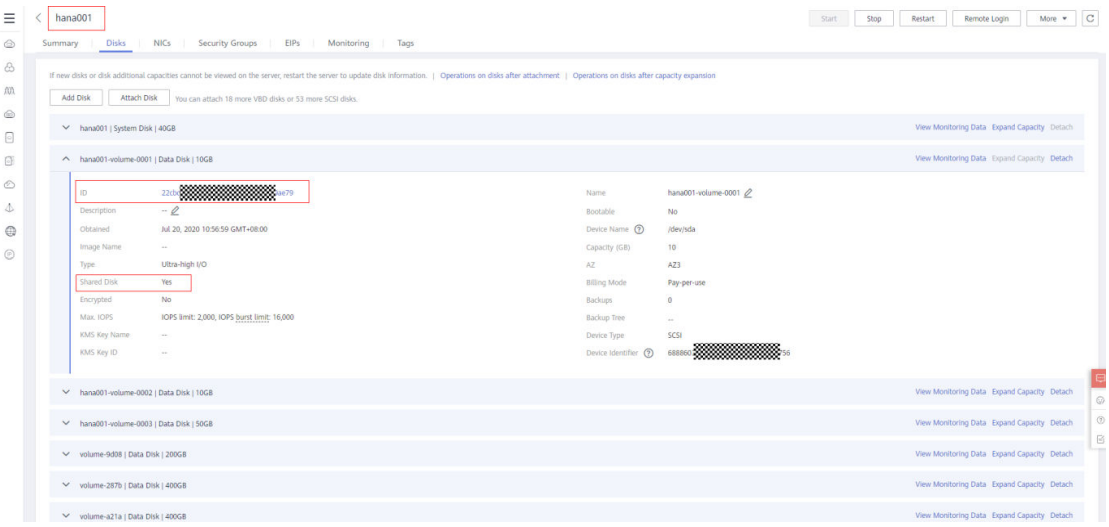
4.4.6 Mounting Shared Volumes

Mount the SBD shared volume created during the creation of the active SAP HANA ECS to the standby SAP HANA ECS, and mount the three shared volumes created during the creation of the active SAP S/4HANA ECS to the standby SAP S/4HANA ECS.

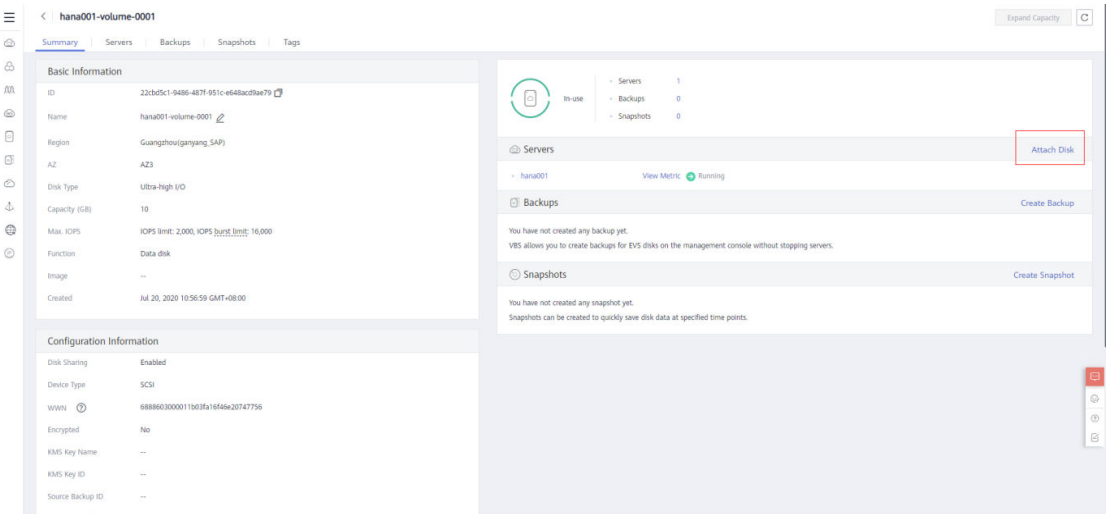
Procedure

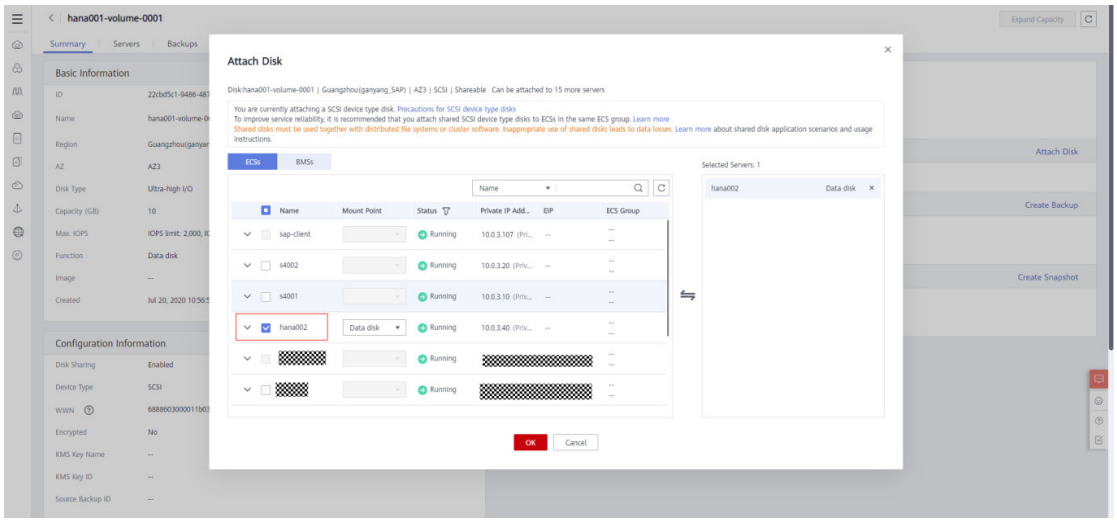
Step 1 Bind the SBD shared volume to the standby SAP HANA ECS.

1. Click ☰ in the navigation plane on the left of the management console, and choose **Computing** > **Elastic Cloud Server**.
2. Locate the created active SAP HANA ECS **hana001** on the displayed page and click its name to view its details.
3. Click the **Disks** tab. Locate the disk of the SBD volume and click the target data disk to view its details.



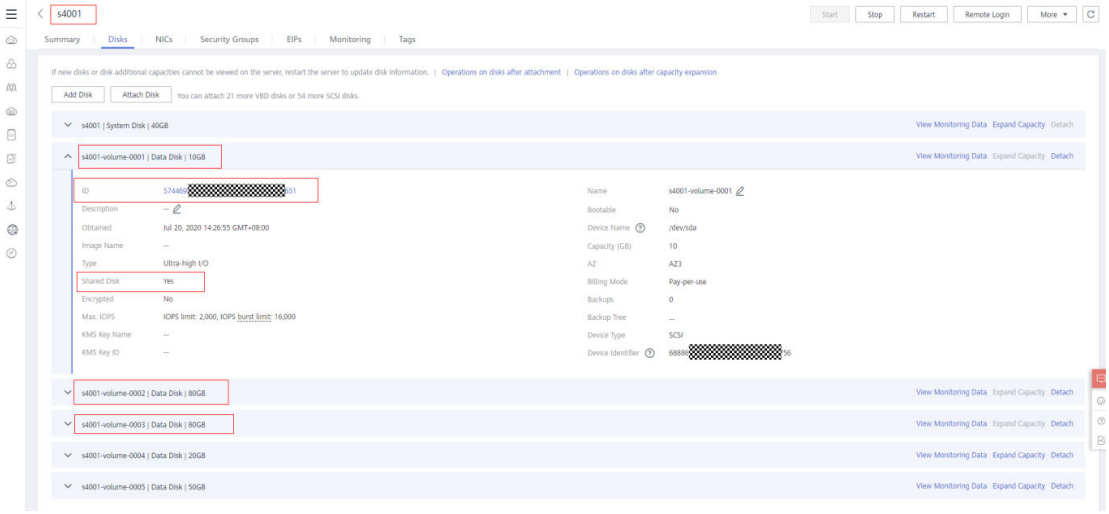
4. Click the data disk ID. On the displayed page, click **Attach Disk** in the **Servers** area. In the displayed dialog box, select the target ECS **hana002** (the standby SAP HANA node) and click **OK**.



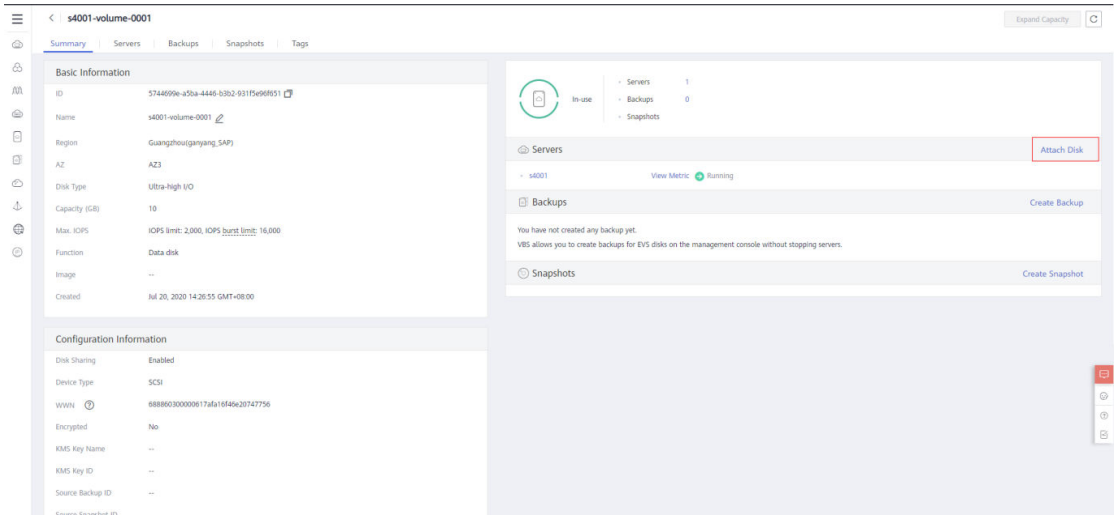


Step 2 Bind the three shared volumes created to the standby SAP S/4HANA ECS.

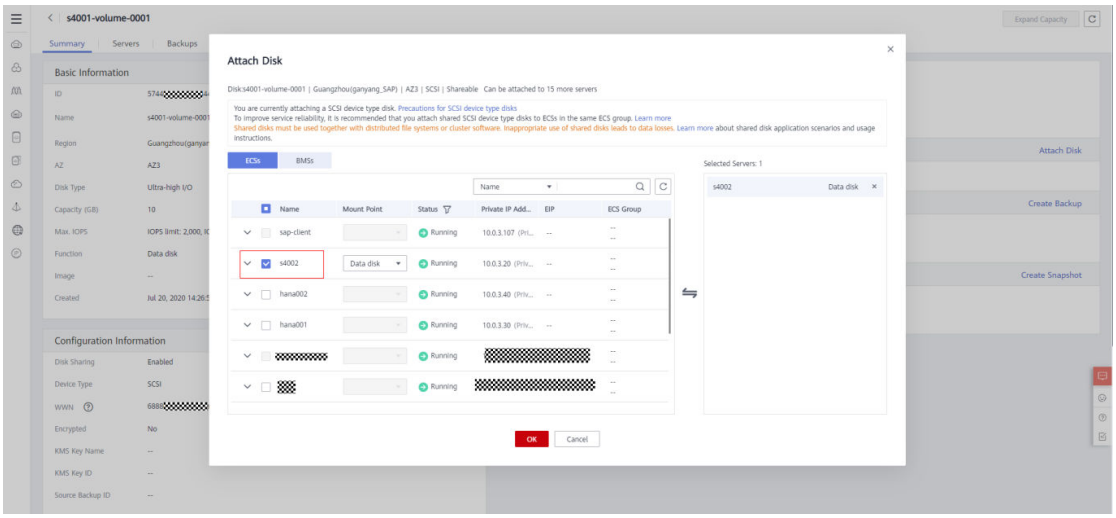
1. Locate the created active SAP S/4HANA ECS **s4001** on the ECS list page and click its name to view its details.
2. Click the **Disks** tab. Locate the shared disk and click the target data disk to view its details.



3. Click the data disk ID. On the displayed page, click **Attach Disk** in the **Servers** area.



4. In the displayed dialog box, select the target ECS **s4002** (the standby SAP S/4HANA node) and click **OK**.



5. Repeat **Step 2.1** to **Step 2.4** to mount the rest two shared volumes to the standby SAP S/4HANA ECS.

----End

4.4.7 Formatting File Systems

4.4.7.1 Formatting the File System for Active and Standby SAP HANA ECSs

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

Log in to ECS **hana001** where SAP HANA is to be installed and check the unformatted disks. Determine the disks of the **/usr/sap** volume, data volume (two physical disks are used to make a data volume in using LVM), log volume, shared volume, and swap volume according to the disk capacity. For details about the disk capacity planning, see **Table 4-4**. Then, format the disks, create directories which disks are to be attached to, and attach the disks.

Procedure

Step 1 Log in to the active SAP HANA ECS, run the following commands shown in the following figure on CLI to query the disk size, determine mount points of disks based on the disk capacity, and format the disks. For the data volume, two physical disks are used to make a data volume in using LVM. For details about how to creating a logical volume using LVM, see **Creating a Logical Volume Using LVM**.

NOTE

There is no need to format the SBD volume attached to the active and standby SAP HANA ECSs.

```
hana001:~ # lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0   10G  0 disk
vda    253:0    0   40G  0 disk
└─vda1 253:1    0   40G  0 part /
vdb    253:16   0   10G  0 disk  SWAP
vdc    253:32   0  400G  0 disk  /hana/shared
vdd    253:48   0   50G  0 disk  /usr/sap
vde    253:64   0  200G  0 disk /hana/log
vdf    253:80   0  200G  0 disk /hana/data
vdg    253:96   0  200G  0 disk
hana001:~ # mkswap /dev/vdb
Setting up swapspace version 1, size = 10 GiB (10737414144 bytes)
no label, UUID=47967aa7-105b-43a0-8532-9a2d1e42c2c2
hana001:~ # swapon /dev/vdb
hana001:~ # pvcreate /dev/vdf /dev/vdg
  Physical volume "/dev/vdf" successfully created.
  Physical volume "/dev/vdg" successfully created.
hana001:~ # vgcreate vghana /dev/vdf /dev/vdg
  Volume group "vghana" successfully created
hana001:~ # lvcreate -i 2 -l 100%VG -n lvhanadata vghana
  Using default stripesize 64.00 KiB.
  Logical volume "lvhanadata" created.
hana001:~ # lvdisplay
  --- Logical volume ---
  LV Path                /dev/vghana/lvhanadata
  LV Name                lvhanadata
  VG Name                vghana
  LV UUID                GyPOtn-Lfr1-9Lzz-xFvm-S7JJ-E9VW-6t4WGv
  LV Write Access        read/write
  LV Creation host, time hana001, 2023-01-30 11:14:50 +0800
  LV Status              available
  # open                 0
  LV Size                399.99 GiB
  Current LE             102398
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
```

```
hana001:~ # mkfs.xfs /dev/vdc
meta-data=/dev/vdc               isize=512    agcount=4, agsize=26214400 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=0, rmapbt=0
         =                       reflink=0
data     =                       bsize=4096   blocks=104857600, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=51200, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
hana001:~ # mkfs.xfs /dev/vdd
meta-data=/dev/vdd               isize=512    agcount=4, agsize=3276800 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=0, rmapbt=0
         =                       reflink=0
data     =                       bsize=4096   blocks=13107200, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=6400, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
hana001:~ # mkfs.xfs /dev/vde
meta-data=/dev/vde               isize=512    agcount=4, agsize=13107200 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=0, rmapbt=0
         =                       reflink=0
data     =                       bsize=4096   blocks=52428800, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=25600, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
hana001:~ # mkfs.xfs /dev/mapper/vghana-lvhanadata
meta-data=/dev/mapper/vghana-lvhanadata isize=512    agcount=16, agsize=6553456 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=0, rmapbt=0
         =                       reflink=0
```

Step 2 Check the UUID of each disk and write mappings between UUIDs and mount points to the **/etc/fstab** file. Then, obtain the shared path of the created SFS file system and write the mapping between the shared path and the **backup** volume to the **/etc/fstab** file.

NOTE

UUID is the unique character string for disk partitions in a Linux system.

```
hana001:~ # lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                   8:0    0   10G  0 disk
vda                 253:0    0   40G  0 disk
└─vda1              253:1    0   40G  0 part /
vdb                 253:16   0   10G  0 disk [SWAP]
vdc                 253:32   0  400G  0 disk /hana/shared
vdd                 253:48   0   50G  0 disk /usr/sap
vde                 253:64   0  200G  0 disk /hana/log
vdf                 253:80   0  200G  0 disk
└─vghana-lvhanadata 254:0    0  400G  0 lvm
vdg                 253:96   0  200G  0 disk /hana/data
└─vghana-lvhanadata 254:0    0  400G  0 lvm
hana001:~ # blkid
/dev/vda1: UUID="77fc659f-66a4-43d7-a210-2ddb7320f1a1" BLOCK_SIZE="4096" TYPE="ext4" PARTUUID="701f202e-01"
/dev/vdb: UUID="47967aa7-105b-43a0-8532-9a2d1e42c2c2" TYPE="swap"
/dev/vdc: UUID="a5ce503c-4e97-4e42-8891-841685a6b98f" BLOCK_SIZE="512" TYPE="xfs"
/dev/vdd: UUID="13d2523e-147f-47ac-a007-7cb1d5f548bb" BLOCK_SIZE="512" TYPE="xfs"
/dev/vde: UUID="f1252e44-b8e7-43f2-8cda-5bf969ce3d99" BLOCK_SIZE="512" TYPE="xfs"
/dev/vdf: UUID="zPlS7G-0jB3-ZPNQ-RkyW-tYhq-4jJt-qC4Hql" TYPE="LVM2_member"
/dev/vdg: UUID="4HCEwO-tMbw-TZBz-S4TK-OWND-sYN0-MHfSCc" TYPE="LVM2_member"
/dev/mapper/vghana-lvhanadata: UUID="be8012c3-8226-4386-bbd8-537e9896dbd3" BLOCK_SIZE="512" TYPE="xfs"
hana001:~ # echo "UUID=47967aa7-105b-43a0-8532-9a2d1e42c2c2 swap swap defaults 0 0" >> /etc/fstab
hana001:~ # echo "UUID=a5ce503c-4e97-4e42-8891-841685a6b98f /hana/shared xfs defaults 0 0" >> /etc/fstab
hana001:~ # echo "UUID=13d2523e-147f-47ac-a007-7cb1d5f548bb /usr/sap xfs defaults 0 0" >> /etc/fstab
hana001:~ # echo "UUID=f1252e44-b8e7-43f2-8cda-5bf969ce3d99 /hana/log xfs defaults 0 0" >> /etc/fstab
hana001:~ # echo "UUID=be8012c3-8226-4386-bbd8-537e9896dbd3 /hana/data xfs defaults 0 0" >> /etc/fstab
hana001:~ # echo "sfs-nas1.cn-south-1c.myhuaweicloud.com:[redacted] /hana/backup nfs vers=3,timeo=600,nolock 0 0" >> /etc
/fstab
```

Step 3 Create the directories which the disks are to be attached to and attach the disks.


```
hana001:~ # mkdir -p /usr/sap /hana/shared /hana/log /hana/data /hana/backup
hana001:~ # mount -a
hana001:~ # df -Th
Filesystem                                          Type      Size  Used Avail Use% Mounted on
devtmpfs                                            devtmpfs  4.0M  8.0K  4.0M   1% /dev
tmpfs                                               tmpfs     189G     0  189G   0% /dev/shm
tmpfs                                               tmpfs      51G  9.8M   51G   1% /run
tmpfs                                               tmpfs     4.0M     0  4.0M   0% /sys/fs/cgroup
/dev/vda1                                           ext4       40G  4.4G   33G  12% /
tmpfs                                               tmpfs      26G   56K   26G   1% /run/user/466
tmpfs                                               tmpfs      26G   64K   26G   1% /run/user/0
/dev/vdc                                            xfs       400G  441M  400G   1% /hana/shared
/dev/vdd                                            xfs        50G   84M   50G   1% /usr/sap
/dev/vde                                            xfs       200G  237M  200G   1% /hana/log
/dev/mapper/vghana-lvhanadata                       xfs       400G  441M  400G   1% /hana/data
sfs-nas1.cn-south-1c.myhuaweicloud.com:[redacted]   nfs        10P  3.2T   10P   1% /hana/backup
hana001:~ #
```

Step 4 Repeat **Step 1** to **Step 3** to format the file system of the standby SAP HANA ECS.

----End

4.4.7.2 Formatting the File System for Active and Standby SAP S/4HANA ECSs

The data disks of SAP S/4HANA nodes can be used only after they are formatted and attached to required directories.

Log in to ECS **s4001** where SAP S/4HANA is to be installed and check the unformatted disks. Determine the disks of the /usr/sap volume, ASCS volume, ERS volume, SBD volume, and swap volume according to the disk capacity. Then, format the disks, create directories which disks are to be attached to, and attach the disks. For details about the disk capacity and mount point, see **SAP S/4HANA File System Planning**.

Procedure

Step 1 Log in to the active SAP S/4HANA ECS, run the following commands shown in the following figure on CLI to query the disk size, determine mount points of disks based on the disk capacity, and format the disks.

NOTE

There is no need to format the SBD volume attached to the active and standby SAP S/4HANA ECSs.


```
s4001:~ # lsblk
NAME   MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda      8:0    0  10G  0 disk  SBD
sdb      8:16   0  80G  0 disk ASCS
sdc      8:32   0  80G  0 disk ERS
vda    253:0    0  40G  0 disk
└─vda1 253:1    0  40G  0 part /
vdb    253:16   0  20G  0 disk SWAP
vdc    253:32   0  50G  0 disk /usr/sap
s4001:~ # mkfs.xfs /dev/sdb
meta-data=/dev/sdb               isize=512    agcount=4, agsize=5242880 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=0, rmapbt=0
         =                       reflink=0
data     =                       bsize=4096   blocks=20971520, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=10240, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
s4001:~ # mkfs.xfs /dev/sdc
meta-data=/dev/sdc               isize=512    agcount=4, agsize=5242880 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=0, rmapbt=0
         =                       reflink=0
data     =                       bsize=4096   blocks=20971520, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=10240, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

```
s4001:~ # mkswap /dev/vdb
Setting up swapspace version 1, size = 20 GiB (21474832384 bytes)
no label, UUID=34cf0dff-f053-4703-91fc-ecd4c37a0bda
s4001:~ # swapon /dev/vdb
s4001:~ # mkfs.xfs /dev/vdc
meta-data=/dev/vdc               isize=512    agcount=4, agsize=3276800 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=0, rmapbt=0
         =                       reflink=0
data     =                       bsize=4096   blocks=13107200, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=6400, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
s4001:~ #
```

Step 2 Check the UUIDs of the disks and write them to the **/etc/fstab** file. The mounting information of ASCS and ERS volumes does not need to be written to the **/etc/fstab** file. You only need to run the commands to mount volumes.

NOTE

- Do not write the attaching information of partitions **sda** and **sdb** to the **fstab** file because the two partitions will be automatically attached when the HA function of SAP S/4HANA is configured. Otherwise, the VM may fail to be restarted. Write the attaching information of other partitions to the **fstab** file.
- **S01** indicates the SID of SAP S/4HANA, and **01** is the instance number of ASCS.


```
s4001:~ # lsblk
NAME   MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda      8:0    0  10G  0 disk
sdb      8:16   0  80G  0 disk
sdc      8:32   0  80G  0 disk
vda    253:0    0  40G  0 disk
└─vda1 253:1    0  40G  0 part /
vdb    253:16   0  20G  0 disk [SWAP]
vdc    253:32   0  50G  0 disk
s4001:~ # blkid
/dev/vda1: UUID="71177627-4cbd-4b0a-8188-133a453214d2" TYPE="ext4" PARTUUID="45884f8c-01"
/dev/vdb: UUID="34cf0dff-f053-4703-91fc-ecd4c37a0bda" TYPE="swap"
/dev/vdc: UUID="5e962c31-5c34-4dd4-b407-6f03544257c7" TYPE="xfs"
/dev/sdb: UUID="197b2f51-de7c-4436-9079-85d90ec0e906" TYPE="xfs"
/dev/sdc: UUID="a5f654f3-c28b-4f90-9bf5-f98f0ce6f637" TYPE="xfs"
s4001:~ # echo "UUID=34cf0dff-f053-4703-91fc-ecd4c37a0bda swap swap defaults 0 0" >> /etc/fstab
s4001:~ # echo "UUID=5e962c31-5c34-4dd4-b407-6f03544257c7 /usr/sap xfs defaults 0 0" >> /etc/fstab
s4001:~ #
s4001:~ # mkdir /usr/sap
s4001:~ # mount -a
s4001:~ # mkdir -p /usr/sap/S01/ASCS01
s4001:~ # mount /dev/sdb /usr/sap/S01/ASCS01/
s4001:~ # lsblk
NAME   MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda      8:0    0  10G  0 disk
sdb      8:16   0  80G  0 disk /usr/sap/S01/ASCS01
sdc      8:32   0  80G  0 disk
vda    253:0    0  40G  0 disk
└─vda1 253:1    0  40G  0 part /
vdb    253:16   0  20G  0 disk [SWAP]
vdc    253:32   0  50G  0 disk /usr/sap
s4001:~ #
```

Step 3 Mount the SFS file system. Obtain the three mounting addresses on the active SAP S/4HANA ECS and mount the SFS file system.

```
s4001:~ # echo "sfs-nas3.cn-east-2.myhuaweicloud.com:/[redacted]c /sapcd nfs defaults 0 0" >> /etc/fstab
s4001:~ # echo "10.0.3.[redacted]:/ /sapmnt nfs defaults 0 0" >> /etc/fstab
s4001:~ # echo "10.0.3.[redacted]:/ /usr/sap/trans nfs defaults 0 0" >> /etc/fstab
s4001:~ #
s4001:~ # mkdir /sapmnt /sapcd /usr/sap/trans
s4001:~ # mount -a
Created symlink from /run/systemd/system/remote-fs.target.wants/rpc-statd.service to /usr/lib/systemd/system/rpc
-statd.service.
s4001:~ # df -Th
Filesystem                                          Type      Size  Used Avail Use% Mounted on
devtmpfs                                            devtmpfs  3.9G  4.0K  3.9G   1% /dev
tmpfs                                               tmpfs     5.9G   76K  5.9G   1% /dev/shm
tmpfs                                               tmpfs     3.9G  9.9M  3.9G   1% /run
tmpfs                                               tmpfs     3.9G     0  3.9G   0% /sys/fs/cgroup
/dev/vda1                                           ext4       40G  6.7G   32G  18% /
tmpfs                                               tmpfs     797M   12K  797M   1% /run/user/0
sfs-nas3.cn-east-2.myhuaweicloud.com:/[redacted]c nfs        10P     0   10P   0% /sapcd
10.0.3.[redacted]:/                                 nfs       500G     0  500G   0% /sapmnt
10.0.3.[redacted]:/                                 nfs       500G     0  500G   0% /usr/sap/trans
s4001:~ #
```

Step 4 Log in to the standby SAP S/4HANA ECS and initialize the file system. You only need to format the local swap and /usr/sap volumes. Follow the operations described in **Step 1** and **Step 2**.

NOTE

S01 indicates the SID of SAP S/4HANA, and **10** is the instance number of ERS.


```
s4002:~ # lsblk
NAME   MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda      8:0    0  10G  0 disk  SBD
sdb      8:16   0  80G  0 disk  ASCS
sdc      8:32   0  80G  0 disk  ERS
vda    253:0    0  40G  0 disk
└─vda1 253:1    0  40G  0 part /
vdb    253:16   0  20G  0 disk SWAP
vdc    253:32   0  50G  0 disk /usr/sap
s4002:~ # mkswap /dev/vdb
Setting up swapspace version 1, size = 20 GiB (21474832384 bytes)
no label, UUID=99989ee2-b20c-4382-8c7a-c3859a0610aa
s4002:~ # swapon /dev/vdb
s4002:~ # mkfs.xfs /dev/vdc
meta-data=/dev/vdc               isize=512    agcount=4, agsize=3276800 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=0, rmapbt=0
         =                       reflink=0
data     =                       bsize=4096   blocks=13107200, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=6400, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
s4002:~ # lsblk
NAME   MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda      8:0    0  10G  0 disk
sdb      8:16   0  80G  0 disk
sdc      8:32   0  80G  0 disk
vda    253:0    0  40G  0 disk
└─vda1 253:1    0  40G  0 part /
vdb    253:16   0  20G  0 disk [SWAP]
vdc    253:32   0  50G  0 disk
```

```
s4002:~ # blkid
/dev/vda1: UUID="71177627-4cbd-4b0a-8188-133a453214d2" TYPE="ext4" PARTUUID="45884f8c-01"
/dev/vdb: UUID="99989ee2-b20c-4382-8c7a-c3859a0610aa" TYPE="swap"
/dev/vdc: UUID="453a065d-36ab-4033-87c9-e3c7ea7db60a" TYPE="xfs"
/dev/sdb: UUID="197b2f51-de7c-4436-9079-85d90ec0e906" TYPE="xfs"
/dev/sdc: UUID="a5f654f3-c28b-4f90-9bf5-f98f0ce6f637" TYPE="xfs"
s4002:~ # echo "UUID=99989ee2-b20c-4382-8c7a-c3859a0610aa swap swap defaults 0 0" >> /etc/fstab
s4002:~ # echo "UUID=453a065d-36ab-4033-87c9-e3c7ea7db60a /usr/sap xfs defaults 0 0" >> /etc/fstab
s4002:~ #
s4002:~ # mkdir /usr/sap
s4002:~ # mount -a
s4002:~ # mkdir -p /usr/sap/S01/ERS10
s4002:~ # mount /dev/sdc /usr/sap/S01/ERS10/
s4002:~ # lsblk
NAME   MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda      8:0    0  10G  0 disk
sdb      8:16   0  80G  0 disk
sdc      8:32   0  80G  0 disk /usr/sap/S01/ERS10
vda    253:0    0  40G  0 disk
└─vda1 253:1    0  40G  0 part /
vdb    253:16   0  20G  0 disk [SWAP]
vdc    253:32   0  50G  0 disk /usr/sap
s4002:~ #
```

Step 5 Mount the SFS file system. Obtain the three mounting addresses on the standby SAP S/4HANA ECS and mount the SFS file system.

NOTE

For details about the SFS mounting addresses, see **Step 3**.

```
s4002:~ # echo "sfs-nas3.cn-east-2.myhuaweicloud.com:/s[redacted] /sapcd nfs defaults 0 0" >> /etc/fstab
s4002:~ # echo "10.0.3.[redacted]:/ /sapmnt nfs defaults 0 0" >> /etc/fstab
s4002:~ # echo "10.0.3.[redacted]:/ /usr/sap/trans nfs defaults 0 0" >> /etc/fstab
s4002:~ # mkdir /sapmnt /sapcd /usr/sap/trans
s4002:~ # mount -a
Created symlink from /run/systemd/system/remote-fs.target.wants/rpc-statd.service to /usr/lib/systemd/system/rpc
-statd.service.
s4002:~ # df -Th
Filesystem                                          Type      Size  Used Avail Use% Mounted on
devtmpfs                                            devtmpfs  3.9G     0  3.9G   0% /dev
tmpfs                                               tmpfs     5.9G   76K  5.9G   1% /dev/shm
tmpfs                                               tmpfs     3.9G  9.9M  3.9G   1% /run
tmpfs                                               tmpfs     3.9G     0  3.9G   0% /sys/fs/cgroup
/dev/vda1                                           ext4       40G  6.7G   32G  18% /
tmpfs                                               tmpfs     797M   12K  797M   1% /run/user/0
sfs-nas3.cn-east-2.myhuaweicloud.com:/[redacted]c nfs        10P     0   10P   0% /sapcd
10.0.3.[redacted]:/                                 nfs       500G     0  500G   0% /sapmnt
10.0.3.[redacted]:/                                 nfs       500G     0  500G   0% /usr/sap/trans
s4002:~ #
```

----End

4.4.8 Configuring the Mappings Between IP Addresses and Hostnames

4.4.8.1 SAP HANA ECS Configuration

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

Procedure

Step 1 Log in to the active SAP HANA ECS **hana001**, edit the **/etc/hosts** file, and write the mappings between the names and IP addresses of all SAP HANA ECSs to the file.

NOTE

- If the mapping between **127.0.0.1** and the ECS name exists in the **/etc/hosts** file, delete it. For details, see **What Should I Do If an SAP Application on an ECS Cannot Be Started?**
- The IP address mentioned in this section is the IP address of the system replication/ heartbeat network plane.
- When configuring the mapping between the private IP address of the active node and the hostname, add a virtual hostname after the hostname. The virtual hostname will be used during SAP S/4HANA installation.

```
#
# hosts         This file describes a number of hostname-to-address
#               mappings for the TCP/IP subsystem.  It is mostly
#               used at boot time, when no name servers are running.
#               On small systems, this file can be used instead of a
#               "named" name server.
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#


# special IPv6 addresses
::1     localhost       ipv6-localhost  ipv6-loopback

fe00::0 ipv6-localnet

ff00::0 ipv6-mcastprefix
ff02::1 ipv6-allnodes
ff02::2 ipv6-allrouters
ff02::3 ipv6-allhosts



127.0.0.1       localhost
127.0.0.1       localhost       localhost
#127.0.0.1      suse15  suse15
#127.0.0.1      hana001 hana001

10.0.3.30       hana001         hanaha
10.0.3.40       hana002
~
~
~
~
"/etc/hosts" 32L, 722C                                                31,19-32      All
```

Step 2 Log in to the standby SAP HANA ECS **hana002**, edit the **/etc/hosts** file, and write the mappings between the names and IP addresses of all SAP HANA ECSs to the file.

----End

4.4.8.2 SAP S/4HANA ECS Configuration

During the SAP S/4HANA installation, installation programs use ECS names for communication. Therefore, you must configure the mappings between ECS names and IP addresses.

Procedure

Step 1 Log in to the active SAP S/4HANA ECS **s4001** and write the mappings between IP addresses and names of all SAP S/4HANA ECSs to the **/etc/hosts** file.

The following uses the mappings between the IP addresses and names of the active and standby ASCS nodes as an example.

- **ascsha** indicates the virtual hostname of the active ASCS node and **ersha** indicates the virtual hostname of the standby ASCS node. Virtual hostnames can be customized.
- You do not need to write the mappings between the virtual IP addresses and virtual hostnames. The virtual IP addresses take effect only after the HA is configured. Do not bind virtual IP addresses to virtual hostnames before the virtual IP addresses take effect. After the ASCS and ERS instances are installed, write the mappings between the virtual IP addresses and virtual hostnames to the hosts file.
- Add the mapping between the private IP address and name of the active SAP HANA ECS. Then, change the private IP address to the virtual IP address of SAP HANA.

```
#
# hosts         This file describes a number of hostname-to-address
#               mappings for the TCP/IP subsystem.  It is mostly
#               used at boot time, when no name servers are running.
#               On small systems, this file can be used instead of a
#               "named" name server.
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#


# special IPv6 addresses
::1     localhost       ipv6-localhost  ipv6-loopback

fe00::0 ipv6-localnet

ff00::0 ipv6-mcastprefix
ff02::1 ipv6-allnodes
ff02::2 ipv6-allrouters
ff02::3 ipv6-allhosts



127.0.0.1       localhost
127.0.0.1       localhost       localhost
#127.0.0.1      suse15  suse15
#127.0.0.1      s4001   s4001

10.0.3.10       s4001
10.0.3.20       s4002
10.0.3.10       ascsha
10.0.3.20       ersha

10.0.3.30       hanaha
~
                                                          35,16-22      All
```

Step 2 Log in to the standby SAP S/4HANA ECS **s4002**, modify the **/etc/hosts** file, and write the mappings between IP addresses and names of all SAP S/4HANA ECSs to the file.

----End

4.4.9 Configuring SSH Switching Permissions

To allow switching between active and standby SAP HANA ECSs as well as between active and standby SAP S/4HANA ECSs using SSH, you must configure the ECSs to be trusty. The following procedure applies to the scenario where password is used for login.

Procedure

Step 1 Log in to the active SAP HANA ECS, generate a key pair, and write the public key information to the **authorized_keys** file.

The command is in the following format:

ssh-keygen -t rsa

Press **Enter** for three consecutive times to generate a key pair.

Step 2 Configure the generated key pair on the standby SAP HANA ECS.

The command is in the following format:

ssh-copy-id -i /root/.ssh/id_rsa.pub root@*IP address of the standby SAP HANA ECS*

Enter the password of the standby ECS.

For example, if the IP address of the standby ECS is **10.0.3.31**, run the following command:

ssh-copy-id -i /root/.ssh/id_rsa.pub root@10.0.3.31

Step 3 Run the following command to log in to the standby ECS without a password:

ssh root@*IP address of the standby ECS*

For example, if the IP address of the standby ECS is **10.0.3.31**, run the following command:

ssh root@10.0.3.31


```
hana01:~ # ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:DFscIo6P4z3ODDFiPQgKj9KjGZj3roHh9h7Gkwku5bs root@hana01
The key's randomart image is:
+---[RSA 3072]----+
|    . . .        |
|   o . o .       |
|o . . . o        |
|==oo   =         |
|X+@o. . S        |
|=%oB+            |
|=+=B+            |
|o oOo.           |
|  E==            |
+----[SHA256]-----+
hana01:~ # ssh-copy-id -i /root/.ssh/id_rsa.pub root@hana02
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id
The authenticity of host 'hana02 (172.18.12.201)' can't be established.
ECDSA key fingerprint is SHA256:/IGFaljiwMtJ6pweTvmJsGkO6vwQ+gLhlfhngWV7QhU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to fil
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are pr
Password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@hana02'"
and check to make sure that only the key(s) you wanted were added.

hana01:~ # ssh root@hana02

        Welcome to Elastic Cloud Service
```

Step 4 Run the following command to generate a key pair for the standby ECS:

ssh-keygen -t rsa

Press **Enter** for three consecutive times to generate a key pair.

Step 5 Run the following command to configure the generated key pair on the active SAP HANA ECS:

ssh-copy-id -i /root/.ssh/id_rsa.pub root@*IP address of the active SAP HANA ECS*

Enter the password of the active ECS.

For example, if the IP address of the active ECS is **10.0.3.30**, run the following command:

ssh-copy-id -i /root/.ssh/id_rsa.pub root@10.0.3.30

Step 6 Run the following command to log in to the active ECS without a password:

ssh root@*IP address of the active ECS*

For example, if the IP address of the standby ECS is **10.0.3.30**, run the following command:

ssh root@10.0.3.30

```
hana02:~ # ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:PqIJIWz0+7TrI1GtedcUoqm02Vle7GJnF5V+/E3qryI root@hana02
The key's randomart image is:
+---[RSA 3072]----+
|                 .|
|          . .   o |
| .     . o o . o. |
|o .  o + . + . .+|
|.o..o B S =   .o+|
|.. o.* = = = .. o|
|  ....o = + ..   |
|   oo+.. .E . .  |
|    ==o    . ..o.|
+----[SHA256]-----+
hana02:~ # ssh-copy-id -i /root/.ssh/id_rsa.pub root@hana01
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id
The authenticity of host 'hana01 (172.18.12.200)' can't be established.
ECDSA key fingerprint is SHA256:R88arVmOx5XYUSBCDuyHSLIyt9mt7LDadrM2beH8flM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to fil
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are pr
Password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@hana01'"
and check to make sure that only the key(s) you wanted were added.

hana02:~ # ssh root@hana01
Last login: Thu Aug  3 03:16:28 2023 from localhost
```


The trust relationship between the active and standby SAP HANA ECSs has been configured.

```
hana01:~ # ssh root@hana02
Last login: Thu Aug  3 03:19:41 2023 from 172.18.12.200

        Welcome to Elastic Cloud Service

hana02:~ # ssh root@hana01
Last login: Thu Aug  3 03:26:27 2023 from 172.18.12.201

        Welcome to Elastic Cloud Service

hana01:~ #
```

Step 7 Repeat the preceding steps to configure the trust relationship between the active and standby SAP S/4HANA ECSs.

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)?". Enter **yes** and continue the switching.

----End

4.5 Software Installation

4.5.1 Installing SAP HANA

SAP HANA must be deployed on ECSs. This section uses the SAP HANA 2.0 installation package as an example. You can download the installation package from the official website and upload the installation package to the **/hana/shared** directory of ECSs **hana001** and **hana002** where SAP HANA is to be installed.

Procedure

Step 1 Run the following commands to decompress the installation package:


```
hana001:~ # cd /hana/shared/
hana001:/hana/shared # ll
total 13308308
-rw-r--r-- 1 root root 4000000000 Feb  3 13:35 51053381_part1.exe
-rw-r--r-- 1 root root 4000000000 Feb  3 13:35 51053381_part2.rar
-rw-r--r-- 1 root root 4000000000 Feb  3 13:35 51053381_part3.rar
-rw-r--r-- 1 root root 1627698107 Feb  3 13:36 51053381_part4.rar
hana001:/hana/shared # unrar x  51053381_part1.exe

UNRAR 5.00 freeware      Copyright (c) 1993-2013 Alexander Roshal


Extracting from 51053381_part1.exe

Creating    51053381                                                  OK
Creating    51053381/DATA_UNITS                                       OK
Creating    51053381/DATA_UNITS/HCO_INA_FILELOAD_10                   OK
Extracting  51053381/DATA_UNITS/HCO_INA_FILELOAD_10/PD.XML            OK
Extracting  51053381/DATA_UNITS/HCO_INA_FILELOAD_10/STACK.XML         OK
Extracting  51053381/DATA_UNITS/HCO_INA_FILELOAD_10/HCOINAFILELOAD03_1.ZIP  OK
Extracting  51053381/DATA_UNITS/HCO_INA_FILELOAD_10/LABEL.ASC         OK
Extracting  51053381/DATA_UNITS/HCO_INA_FILELOAD_10/SIGNATURE.SMF     OK
Creating    51053381/DATA_UNITS/HDB_CLIENT_SOLARIS_SPARC              OK
Extracting  51053381/DATA_UNITS/HDB_CLIENT_SOLARIS_SPARC/LABEL.ASC    OK
Creating    51053381/DATA_UNITS/HDB_CLIENT_SOLARIS_SPARC/licenses     OK
Extracting  51053381/DATA_UNITS/HDB_CLIENT_SOLARIS_SPARC/licenses/lz4.txt  OK
Extracting  51053381/DATA_UNITS/HDB_CLIENT_SOLARIS_SPARC/licenses/intel_bid.txt  OK
Extracting  51053381/DATA_UNITS/HDB_CLIENT_SOLARIS_SPARC/hdbclientreg  OK
Creating    51053381/DATA_UNITS/HDB_CLIENT_SOLARIS_SPARC/instruntime  OK
Extracting  51053381/DATA_UNITS/HDB_CLIENT_SOLARIS_SPARC/instruntime/Cwd.so  OK
Extracting  51053381/DATA_UNITS/HDB_CLIENT_SOLARIS_SPARC/instruntime/FCGI.so  OK
Extracting  51053381/DATA_UNITS/HDB_CLIENT_SOLARIS_SPARC/instruntime/lcm_pm_ext.tgz  OK
Extracting  51053381/DATA_UNITS/HDB_CLIENT_SOLARIS_SPARC/instruntime/version.pm  OK
Extracting  51053381/DATA_UNITS/HDB_CLIENT_SOLARIS_SPARC/instruntime/sdbrun  OK
Extracting  51053381/DATA_UNITS/HDB_CLIENT_SOLARIS_SPARC/instruntime/Carp.pm  OK
Extracting  51053381/DATA_UNITS/HDB_CLIENT_SOLARIS_SPARC/instruntime/libperl.so  OK
```

Step 2 Go to the directory where the installation package is stored and perform the installation.

```
hana001:/hana/shared # ll
total 13308308
drwxr-xr-x 3 root root        245 Sep 21  2018 51053381
-rw-r--r-- 1 root root 4000000000 Feb  3 13:35 51053381_part1.exe
-rw-r--r-- 1 root root 4000000000 Feb  3 13:35 51053381_part2.rar
-rw-r--r-- 1 root root 4000000000 Feb  3 13:35 51053381_part3.rar
-rw-r--r-- 1 root root 1627698107 Feb  3 13:36 51053381_part4.rar
hana001:/hana/shared # cd 51053381/DATA_UNITS/HDB_SERVER_LINUX_X86_64/
hana001:/hana/shared/51053381/DATA_UNITS/HDB_SERVER_LINUX_X86_64 # ll
total 180
-rwxr-xr-x 1 root root    97 Jul 18  2018 LABEL.ASC
-rwxr-xr-x 1 root root 36108 Sep 11  2018 SIGNATURE.SMF
drwxr-xr-x 2 root root    55 Sep  4  2018 adapters.d
drwxr-xr-x 2 root root    56 Sep  4  2018 descriptors.d
-rwxr-xr-x 1 root root   602 Aug 31  2018 filelist.hdbinst_remote_check
-rwxr-xr-x 1 root root   601 Aug 31  2018 filelist.hdblcm_remote_check
-rwxr-xr-x 1 root root  1262 Aug 31  2018 filelist.install
-rwxr-xr-x 1 root root  2693 Aug 31  2018 filelist.resident
-rwxr-xr-x 1 root root 14600 Aug 31  2018 hdbinst
-rwxr-xr-x 1 root root 14600 Aug 31  2018 hdblcm
-rwxr-xr-x 1 root root 14600 Aug 31  2018 hdblcmgui
-rwxr-xr-x 1 root root 14600 Aug 31  2018 hdblcmweb
-rwxr-xr-x 1 root root 14600 Aug 31  2018 hdbsetup
-rwxr-xr-x 1 root root 14600 Aug 31  2018 hdbuninst
-rwxr-xr-x 1 root root 14600 Aug 31  2018 hdbupd
drwxr-xr-x 7 root root  4096 Sep  4  2018 instruntime
drwxr-xr-x 2 root root  4096 Sep  4  2018 operations.d
drwxr-xr-x 6 root root    92 Sep  4  2018 resources
drwxr-xr-x 3 root root  4096 Sep  4  2018 server
hana001:/hana/shared/51053381/DATA_UNITS/HDB_SERVER_LINUX_X86_64 # ./hdblcm
```



```
Choose an action

  Index | Action             | Description
  ------------------------------------------------
  1     | install            | Install new system
  2     | extract_components | Extract components
  3     | Exit (do nothing)  |

Enter selected action index [3]: 1


SAP HANA Database version '2.00.033.00.1535711040' will be installed.

Select additional components for installation:

  Index | Components | Description
  ------------------------------------------------------------------------------------------
  1     | all        | All components
  2     | server     | No additional components
  3     | client     | Install SAP HANA Database Client version 2.3.119.1535661774
  4     | studio     | Install SAP HANA Studio version 2.3.41.000000
  5     | smartda    | Install SAP HANA Smart Data Access version 2.00.3.000.0
  6     | xs         | Install SAP HANA XS Advanced Runtime version 1.0.88.12598
  7     | afl        | Install SAP HANA AFL (incl.PAL,BFL,OFL) version 2.00.033.0000.1535724035
  8     | eml        | Install SAP HANA EML AFL version 2.00.033.0000.1535724035
  9     | epmmds     | Install SAP HANA EPM-MDS version 2.00.033.0000.1535724035

Enter comma-separated list of the selected indices [3]: 2
Enter Installation Path [/hana/shared]:
Enter Local Host Name [hana001]:
Do you want to add hosts to the system? (y/n) [n]:
Enter SAP HANA System ID: S00
Enter Instance Number [00]:
Enter Local Host Worker Group [default]:
```

```
  Index | System Usage | Description
  -------------------------------------------------------------------------------
  1     | production   | System is used in a production environment
  2     | test         | System is used for testing, not production
  3     | development  | System is used for development, not production
  4     | custom       | System usage is neither production, test nor development

Select System Usage / Enter Index [4]:
Enter Location of Data Volumes [/hana/data/S00]:
Enter Location of Log Volumes [/hana/log/S00]:
Restrict maximum memory allocation? [n]:
Enter Certificate Host Name For Host 'hana001' [hana001]:
Enter SAP Host Agent User (sapadm) Password:
Confirm SAP Host Agent User (sapadm) Password:
Enter System Administrator (s00adm) Password:
Confirm System Administrator (s00adm) Password:
Enter System Administrator Home Directory [/usr/sap/S00/home]:
Enter System Administrator Login Shell [/bin/sh]:
Enter System Administrator User ID [1000]:
Enter ID of User Group (sapsys) [79]:
Enter System Database User (SYSTEM) Password:
Confirm System Database User (SYSTEM) Password:
Restart system after machine reboot? [n]:

Summary before execution:
=========================
```



```
SAP HANA Database System Installation
   Installation Parameters
      Remote Execution: ssh
      Database Isolation: low
      Installation Path: /hana/shared
      Local Host Name: hana001
      SAP HANA System ID: S00
      Instance Number: 00
      Local Host Worker Group: default
      System Usage: custom
      Location of Data Volumes: /hana/data/S00
      Location of Log Volumes: /hana/log/S00
      Certificate Host Names: hana001 -> hana001
      System Administrator Home Directory: /usr/sap/S00/home
      System Administrator Login Shell: /bin/sh
      System Administrator User ID: 1000
      ID of User Group (sapsys): 79
   Software Components
      SAP HANA Database
         Install version 2.00.033.00.1535711040
         Location: /hana/shared/51053381/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
      SAP HANA AFL (incl.PAL,BFL,OFL)
         Do not install
      SAP HANA EML AFL
         Do not install
      SAP HANA EPM-MDS
         Do not install
      SAP HANA Database Client
         Do not install
      SAP HANA Studio
         Do not install
      SAP HANA Smart Data Access
         Do not install
      SAP HANA XS Advanced Runtime
         Do not install

Do you want to continue? (y/n): y
```

Step 3 Verify the installation.

- Switch to the database system administrator. The administrator account is **s00adm** displayed on the page during the installation.

  su - s00adm

- Query the database version.

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

  HDB -version

- Check whether the database process is running properly.

  Run the following command to check whether the process is normal (**00** is the SAP HANA instance ID):

  sapcontrol -nr 00 -function GetProcessList

  In the command output, if the value of **dispstatus** is **GREEN**, the process is normal.

- Run the following command to return to user **root**:

  exit


```
hana001:/hana/shared/51053381/DATA_UNITS/HDB_SERVER_LINUX_X86_64 # su - s00adm
s00adm@hana001:/usr/sap/S00/HDB00> HDB -version
HDB version info:
  version:             2.00.033.00.1535711040
  branch:              fa/hana2sp03
  machine config:      linuxx86_64
  git hash:            83714f37479a86233127c092c9e295c72d727b8b
  git merge time:      2018-08-31 12:24:00
  weekstone:           0000.00.0
  cloud edition:       0000.00.00
  compile date:        2018-08-31 12:31:44
  compile host:        ld4550
  compile type:        rel

s00adm@hana001:/usr/sap/S00/HDB00> sapcontrol -nr 00 -function GetProcessList

21.07.2020 10:10:04
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
hdbdaemon, HDB Daemon, GREEN, Running, 2020 07 21 10:06:05, 0:03:59, 5402
hdbcompileserver, HDB Compileserver, GREEN, Running, 2020 07 21 10:06:28, 0:03:36, 5593
hdbnameserver, HDB Nameserver, GREEN, Running, 2020 07 21 10:06:05, 0:03:59, 5418
hdbpreprocessor, HDB Preprocessor, GREEN, Running, 2020 07 21 10:06:28, 0:03:36, 5595
hdbwebdispatcher, HDB Web Dispatcher, GREEN, Running, 2020 07 21 10:07:10, 0:02:54, 5963
hdbindexserver, HDB Indexserver-S00, GREEN, Running, 2020 07 21 10:06:29, 0:03:35, 5634
hdbxsengine, HDB XSEngine-S00, GREEN, Running, 2020 07 21 10:06:29, 0:03:35, 5636
s00adm@hana001:/usr/sap/S00/HDB00> exit
logout
hana001:/hana/shared/51053381/DATA_UNITS/HDB_SERVER_LINUX_X86_64 #
```

Step 4 Log in to the other ECS where SAP HANA is to be installed, decompress the installation package, and install SAP HANA. The installation procedure is the same as the aforementioned. All parameters except ECS name must be consistent with preceding ones.

----End

4.5.2 Installing SAP S/4HANA

4.5.2.1 Adding a Virtual IP Address

Download the SAP S/4HANA (1809) installation package to the shared directory **/sapcd** and perform the installation.

If you use the SAP ASCS HA script provided by HUAWEI CLOUD, the virtual IP address is automatically configured in the installation script. Before installing SAP ASCS and ERS, you need to manually add the virtual IP addresses of ASCS and ERS on the active and standby nodes.

Command for adding virtual IP address on the active node:

ip addr add <ASCS VIP>/24 broadcast dev eth0:0

Example: ip addr add 172.16.0.12/24 broadcast 172.16.0.255 dev eth0:0

Command for adding virtual IP address on the standby node:

ip addr add <ERS VIP>/24 broadcast dev eth0:1

Example: ip addr add 172.16.0.13/24 broadcast 172.16.0.255 dev eth0:1

4.5.2.2 Installing ASCS Instance1

Procedure

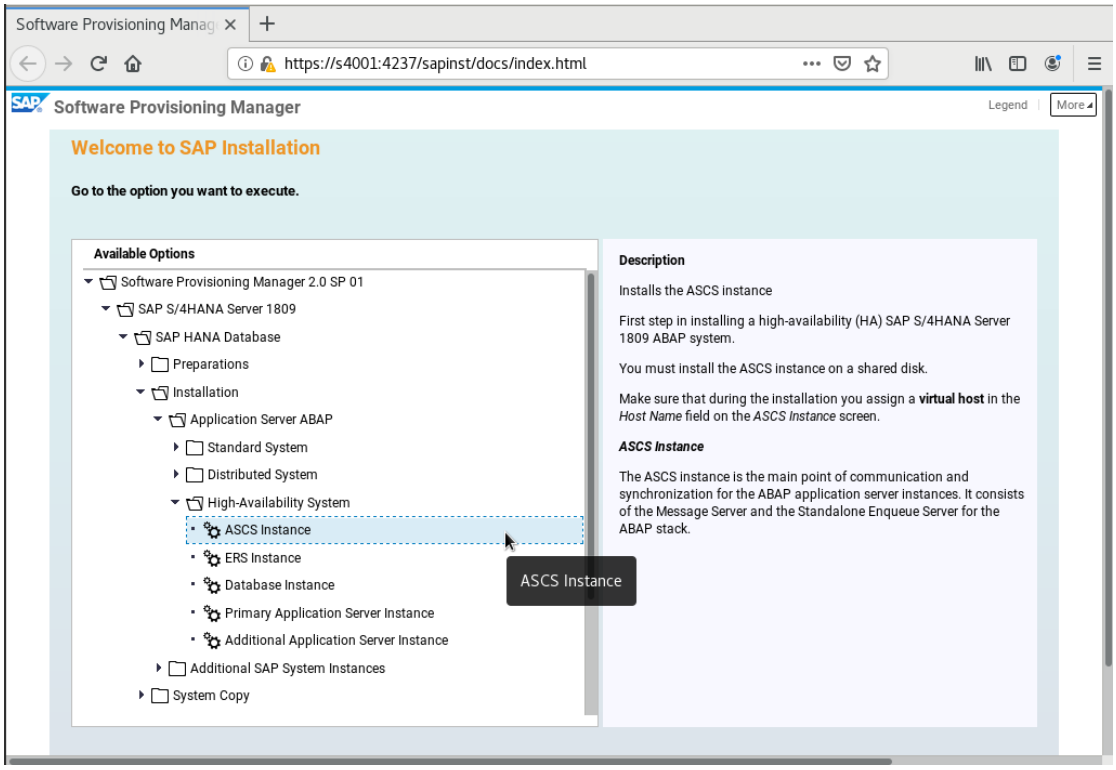
Step 1 Log in to the active SAP S/4HANA ECS **s4001**, and use Software Provisioning Manager (SWPM) to install ASCS Instance on the VM ascsha.

```
s4001:/sapcd/SWPM # ./sapinst
[==============================] | extracting...  done!
INFO       2020-07-21 11:21:13.365 (mainThread) [sixxcreate.cpp:347]
********************************************************************************
Initial log directory: /root/.sapinst/s4001/4379
********************************************************************************


SAPinst build information:
--------------------------
Version:          749.0.62
Build:            1875603
Compile time:     Oct 08 2018 - 14:01:31
Make type:        optU
Codeline:         749_REL
Platform:         linuxx86_64
Kernel build:     749, patch 611, changelist 1875937
SAP JRE build:    SAP Java Server VM (build 8.1.044 9.0.4+011, Sep  6 2018 16:58:06 - 81_REL - optU - linux amd64
 - 6 - bas2:309656 (mixed mode))
SAP JCo build:    3.0.18
SL-UI version:    2.6.28
SAP UI5 version: 1.50.4
Exe directory: /tmp/sapinst_exe.4378.1595301670

SAPinst process information:
----------------------------
Pid:         4379

INFO       2020-07-21 11:21:13.720 (root/sapinst) (startInstallation) [CSiManagerInterfaces.cpp:2348]
Problem with the DNS configuration: could not determine the DNS domain of host s4001

INFO       2020-07-21 11:21:13.722 (root/sapinst) (guiWatchdog) [CSLPCommunicationServer.cpp:349]
Problem with the DNS configuration: could not determine the DNS domain of host s4001

INFO       2020-07-21 11:21:15.749 (root/sapinst) (SLPCommunicator) [SLPMonitoringStatemachine.cpp:1392]
********************************************************************************
```

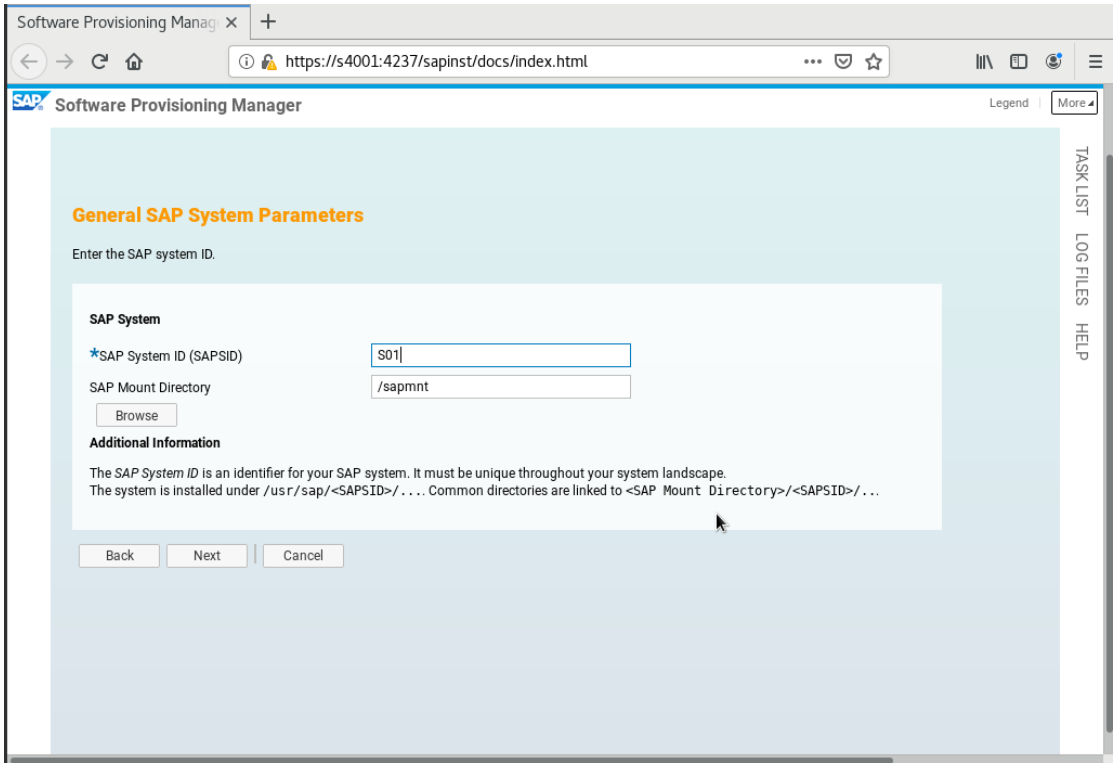
```
Open your browser and paste the following URL address to access the GUI
https://s4001:4237/sapinst/docs/index.html
Logon users: [root]
********************************************************************************

=>sapparam(1c): No Profile used.
=>sapparam: SAPSYSTEMNAME neither in Profile nor in Commandline
load resource pool /sapcd/SWPM/resourcepool.xml
```

Step 2 Enter **https://s4001:4237/sapinst/docs/index.html** in the address box of a browser, and then log in to the SWPM system as the **root** user and install ASCS Instance.

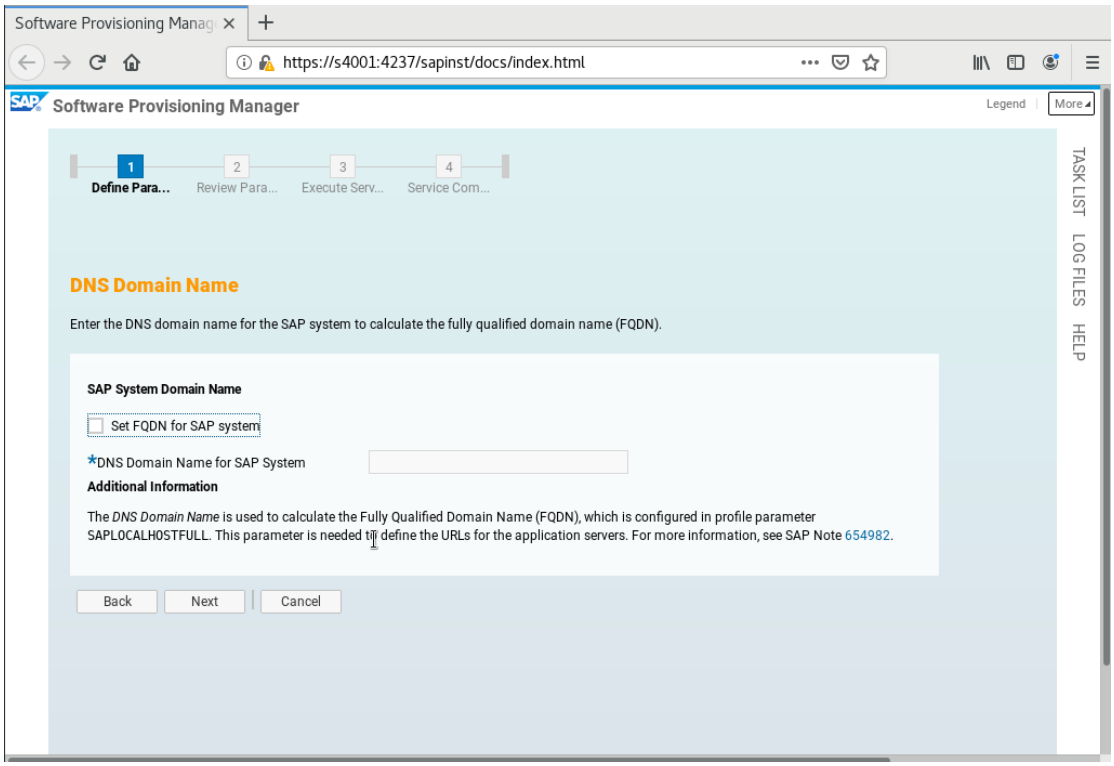
Select **ASCS Instance** and click **Next**.



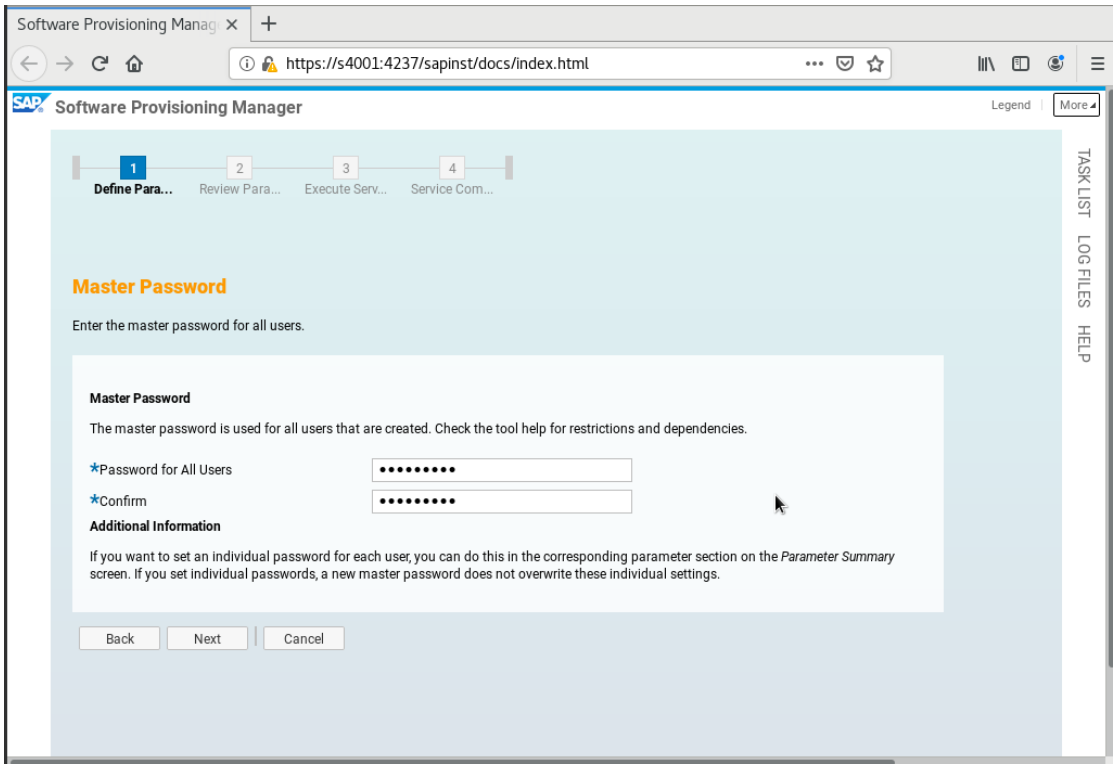
Step 3 Enter the planned SID for **SAP System ID** and **sapmnt** for SAP Mount Directory.



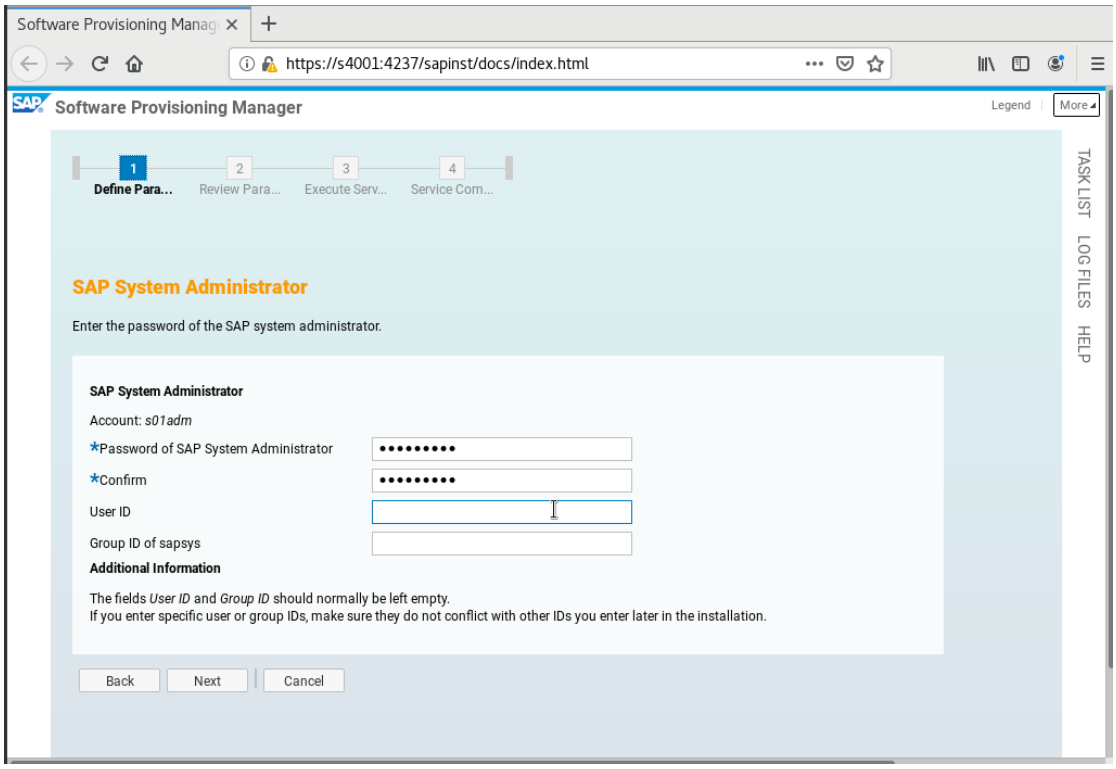
Step 4 Deselect **Set FQDN for SAP System**.



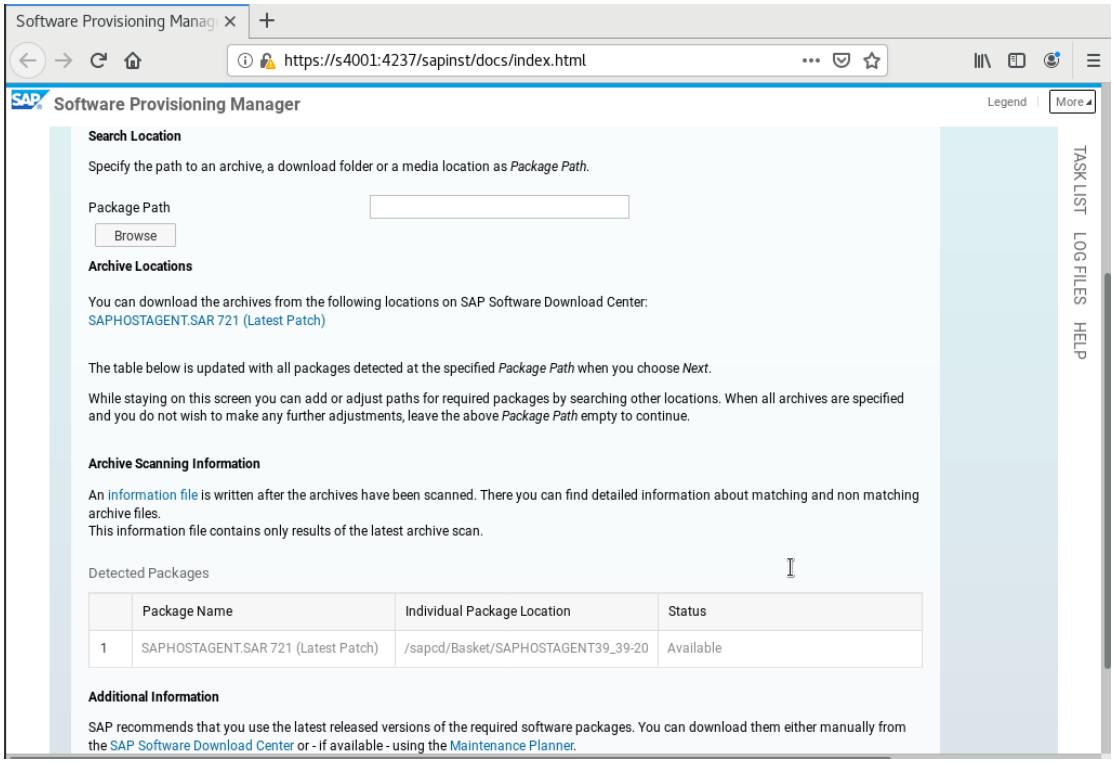
Step 5 Enter the master password for all users.



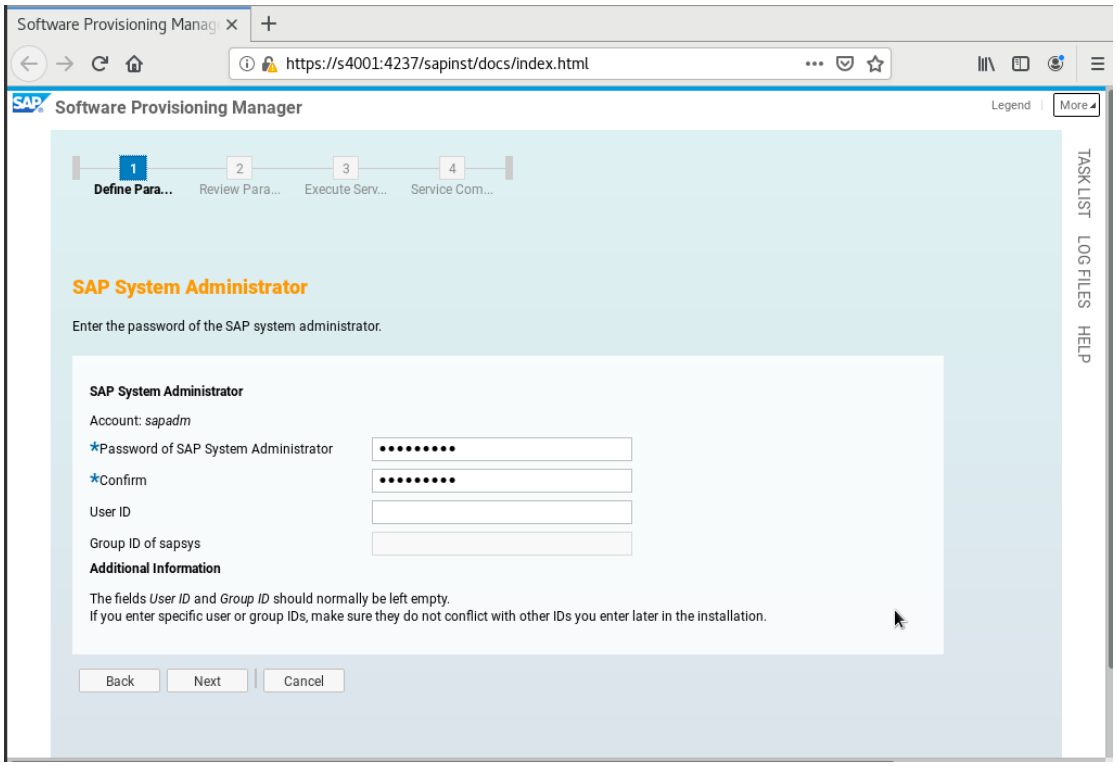
Step 6 Click **Next**.



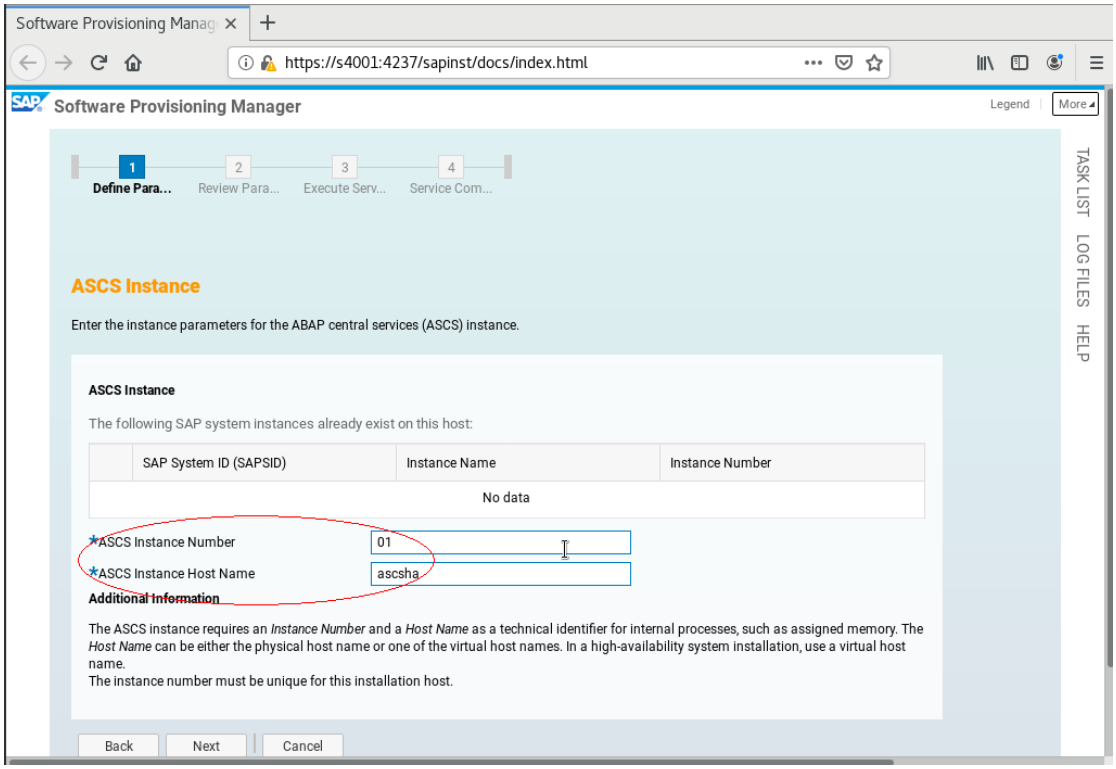
Step 7 Select a package path.



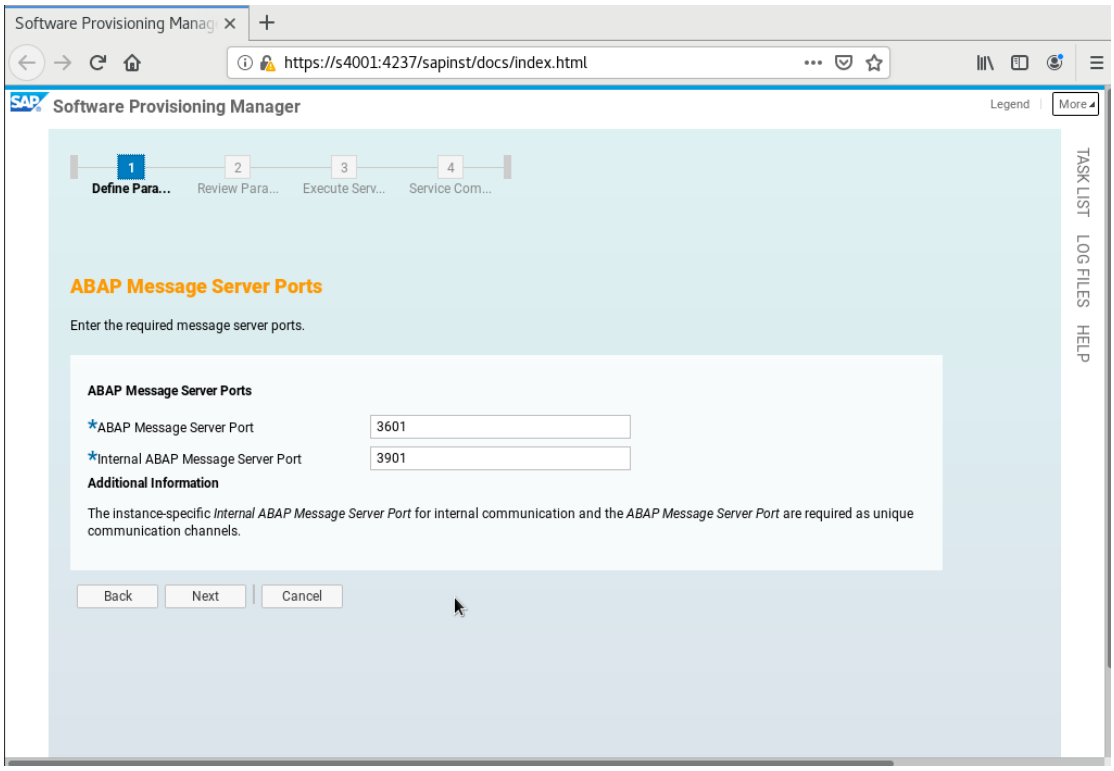
Step 8 Enter and confirm the password.



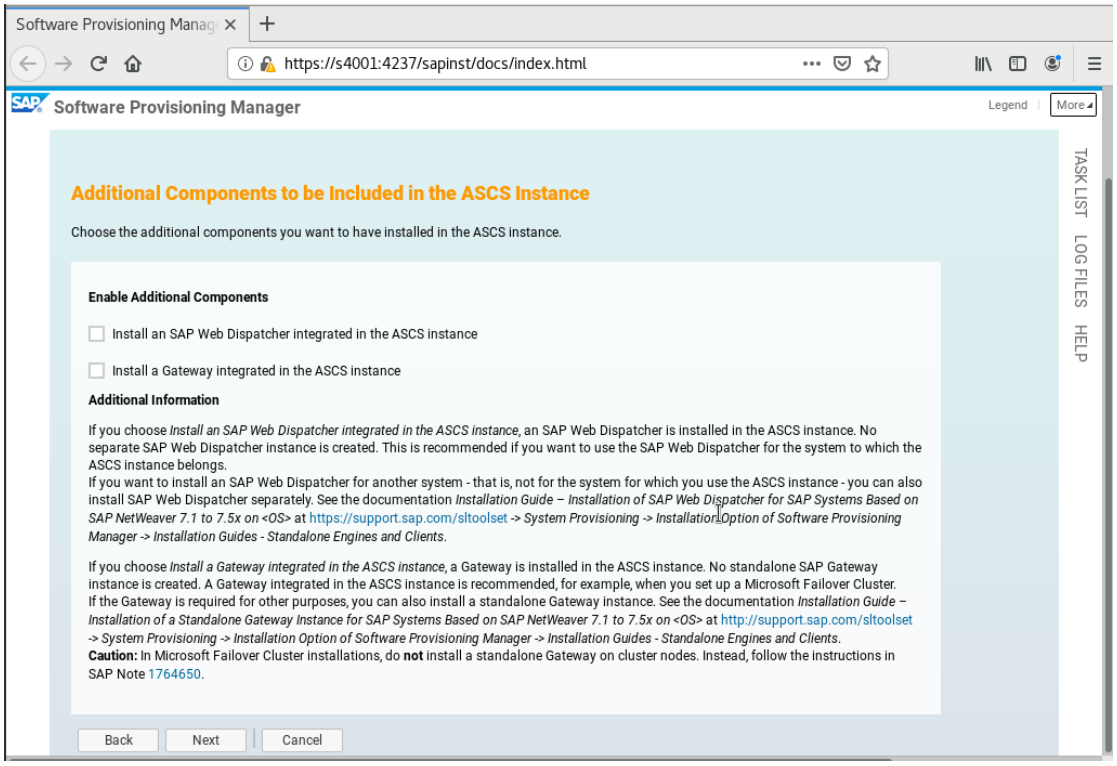
Step 9 Set **ASCS Instance Number** and **ASCS Instance Host Name** according to the installation planning. Enter the VM name (**ascsha**) of the active SAP S/4HANA ECS for **ASCS Instance Host Name**.



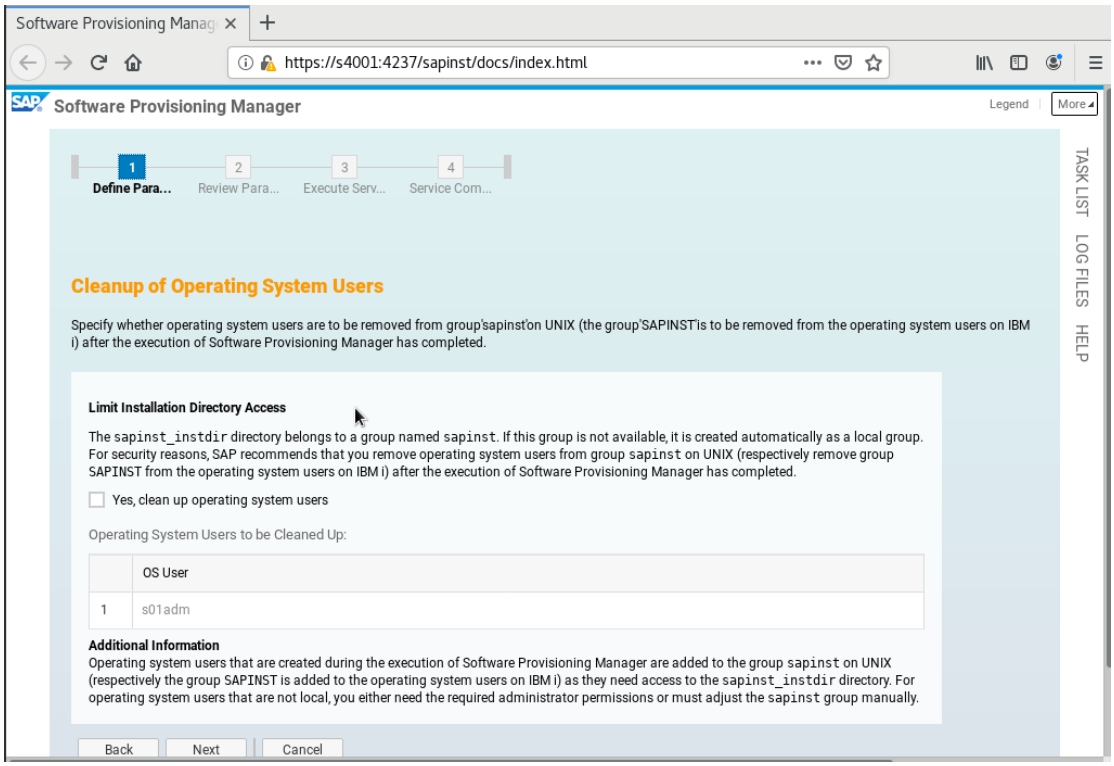
Step 10 Click **Next**.



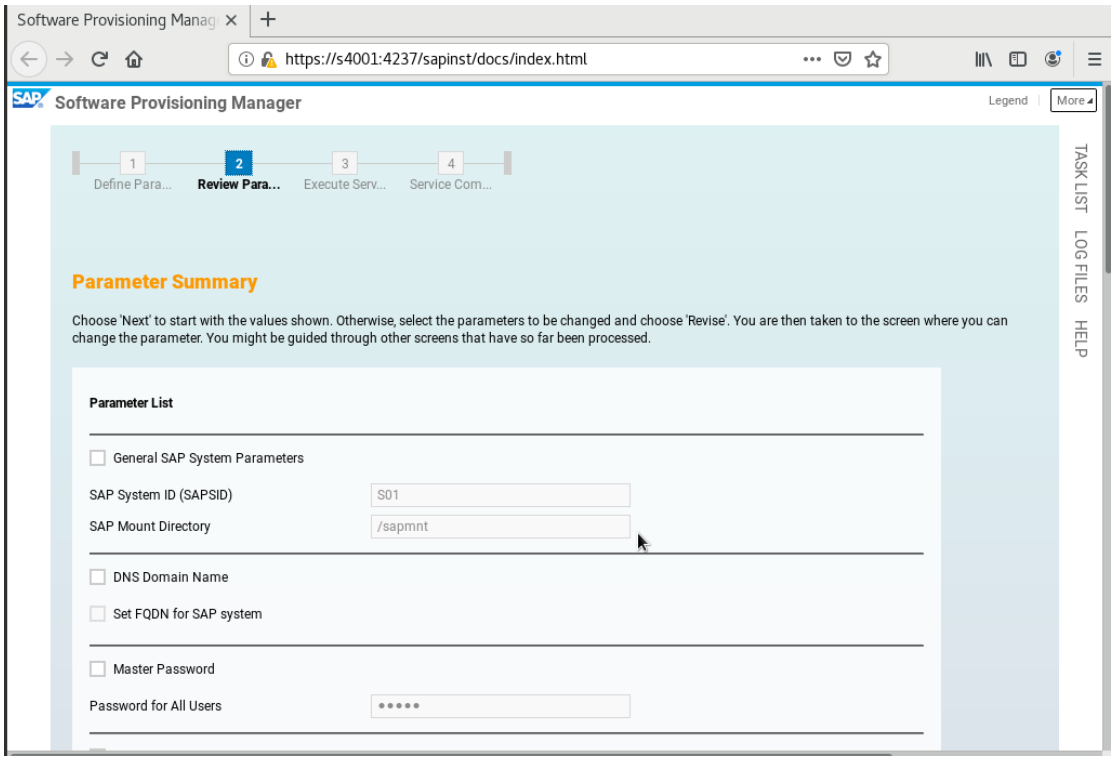
Step 11 Click **Next**.



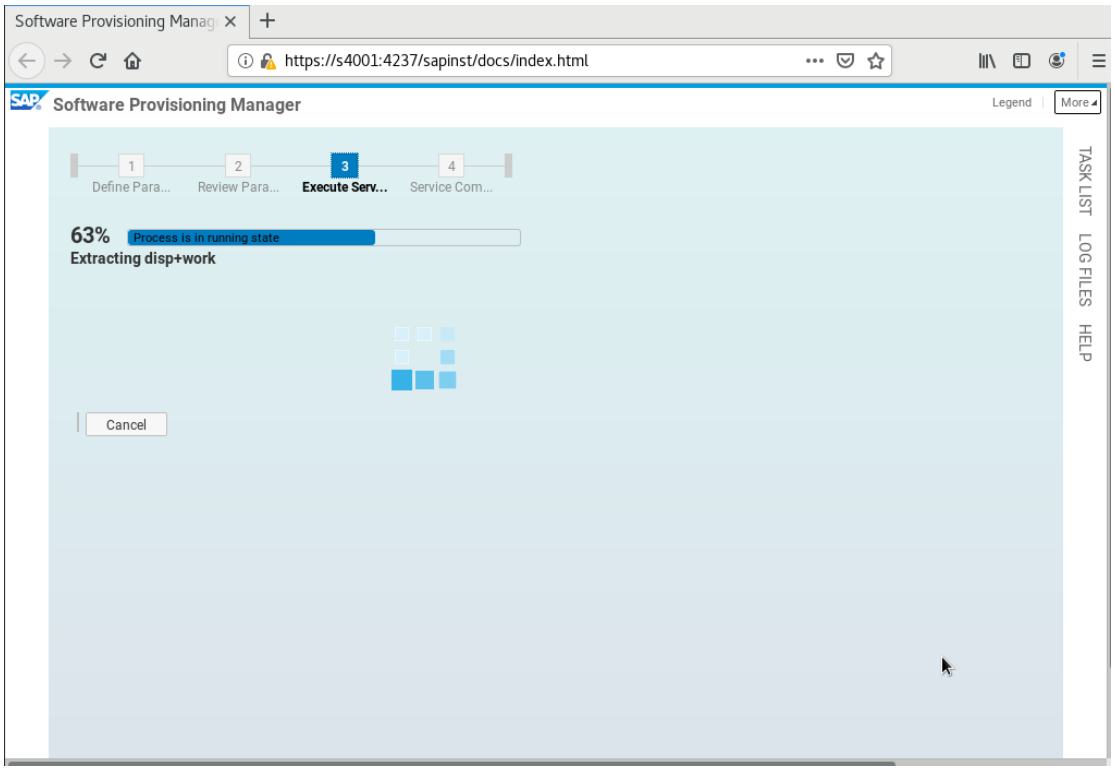
Step 12 Click **Next**.

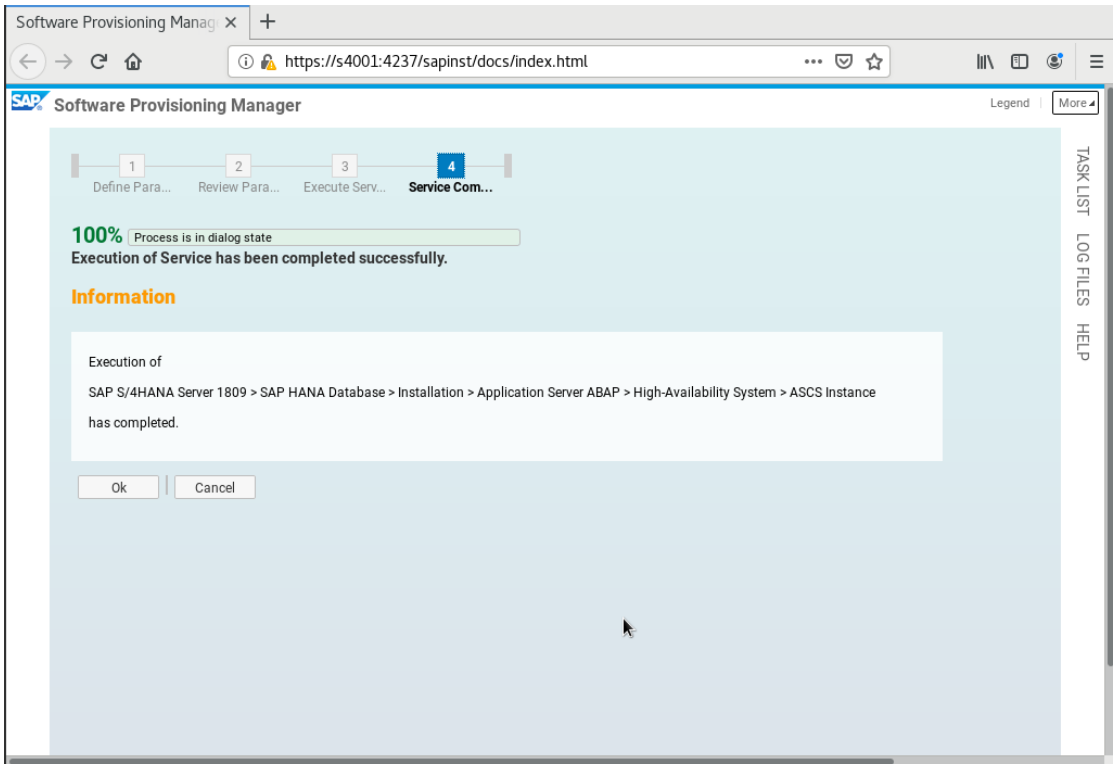


Step 13 Check your parameter settings. If they are all correct, click **Next**.



Step 14 The installation starts.





----End

4.5.2.3 Copying Files

After installing ASCS on the active SAP S/4HANA ECS **s4001**, you need to copy some files from **s4001** to the standby SAP S/4HANA ECS **s4002** where ERS is to be installed.

Procedure

Step 1 Log in to **s4001**, compress the SYS file of the **/usr/sap/S01** directory, and copy the file package to the **/usr/sap/S01** directory on **s4002**.

```
s4001:/sapcd/SWPM # cd /usr/sap/S01/
s4001:/usr/sap/S01 # ll
total 0
drwxr-xr-x 7 s01adm sapsys 63 Jul 21 11:54 ASCS01
drwxr-xr-x 5 s01adm sapsys 68 Jul 21 11:54 SYS
s4001:/usr/sap/S01 # tar -cvf SYS.tar SYS/
SYS/
SYS/exe/
SYS/exe/uc
SYS/exe/nuc
SYS/exe/opt/
SYS/exe/dbg
SYS/exe/run
SYS/gen/
SYS/gen/dbg/
SYS/src/
SYS/profile
SYS/global
s4001:/usr/sap/S01 # scp SYS.tar s4002:/usr/sap/S01/
SYS.tar                                                    100%   20KB   7.6MB/s   00:00
s4001:/usr/sap/S01 #
s4001:/usr/sap/S01 #
```

Step 2 Log in to **s4002** and decompress the **SYS.tar** file.

```
s4002:~ # cd /usr/sap/S01/
s4002:/usr/sap/S01 # ll
total 20
drwxr-xr-x 2 root root     6 Jul 20 15:55 ERS10
-rw-r--r-- 1 root root 20480 Jul 21 14:06 SYS.tar
s4002:/usr/sap/S01 # tar -xvf SYS.tar
SYS/
SYS/exe/
SYS/exe/uc
SYS/exe/nuc
SYS/exe/opt/
SYS/exe/dbg
SYS/exe/run
SYS/gen/
SYS/gen/dbg/
SYS/src/
SYS/profile
SYS/global
s4002:/usr/sap/S01 # ll
total 20
drwxr-xr-x 2 root root     6 Jul 20 15:55 ERS10
drwxr-xr-x 5 1000 1001    68 Jul 21 11:54 SYS
-rw-r--r-- 1 root root 20480 Jul 21 14:06 SYS.tar
s4002:/usr/sap/S01 #
```

Step 3 Install ERS.

----End

4.5.2.4 Installing ERS Instance

Procedure

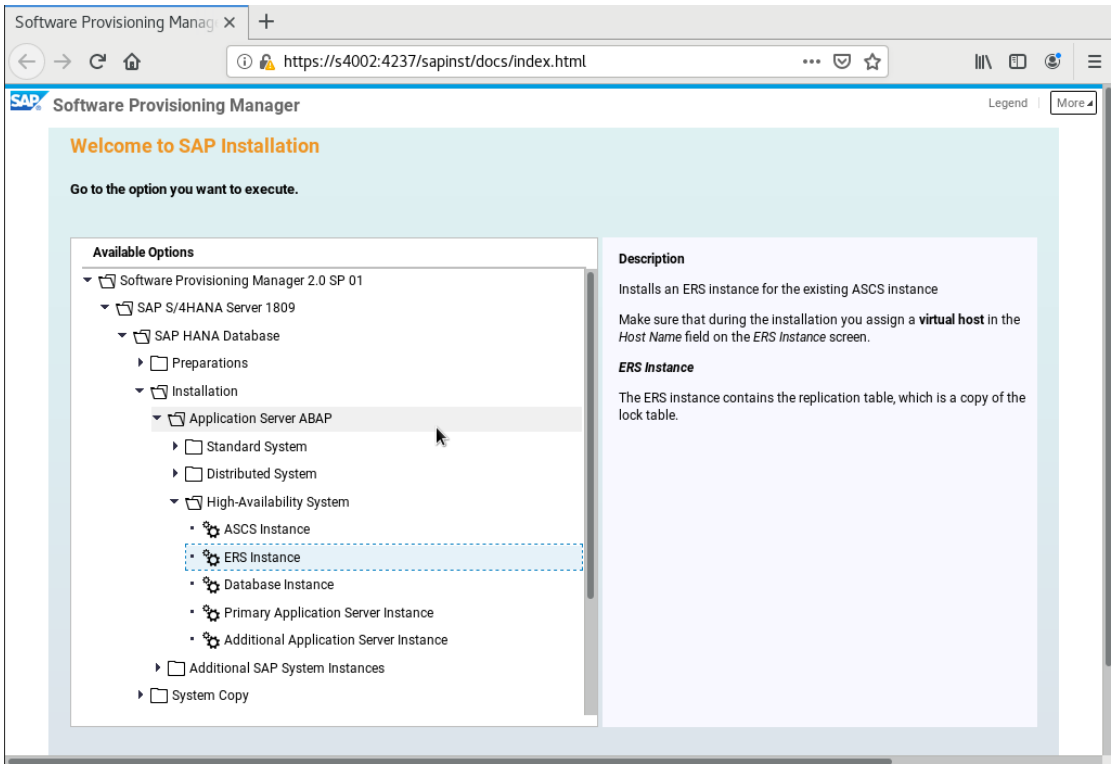
Step 1 Log in to the standby SAP S/4HANA ECS s4002 and go to the directory where the ERS installation package is stored to install it.


```
s4002:~ # cd /sapcd/SWPM/
s4002:/sapcd/SWPM # ./sapinst
[============================] | extracting...  done!
INFO       2020-07-21 14:10:33.597 (mainThread) [sixxcreate.cpp:347]
********************************************************************************
Initial log directory: /root/.sapinst/s4002/4783
********************************************************************************


SAPinst build information:
--------------------------
Version:          749.0.62
Build:            1875603
Compile time:     Oct 08 2018 - 14:01:31
Make type:        optU
Codeline:         749_REL
Platform:         linuxx86_64
Kernel build:     749, patch 611, changelist 1875937
SAP JRE build:    SAP Java Server VM (build 8.1.044 9.0.4+011, Sep  6 2018 16:58:06 - 81_REL - optU - linux amd64
 - 6 - bas2:309656 (mixed mode))
SAP JCo build:    3.0.18
SL-UI version:    2.6.28
SAP UI5 version: 1.50.4
Exe directory: /tmp/sapinst_exe.4782.1595311831

SAPinst process information:
----------------------------
Pid:         4783
```

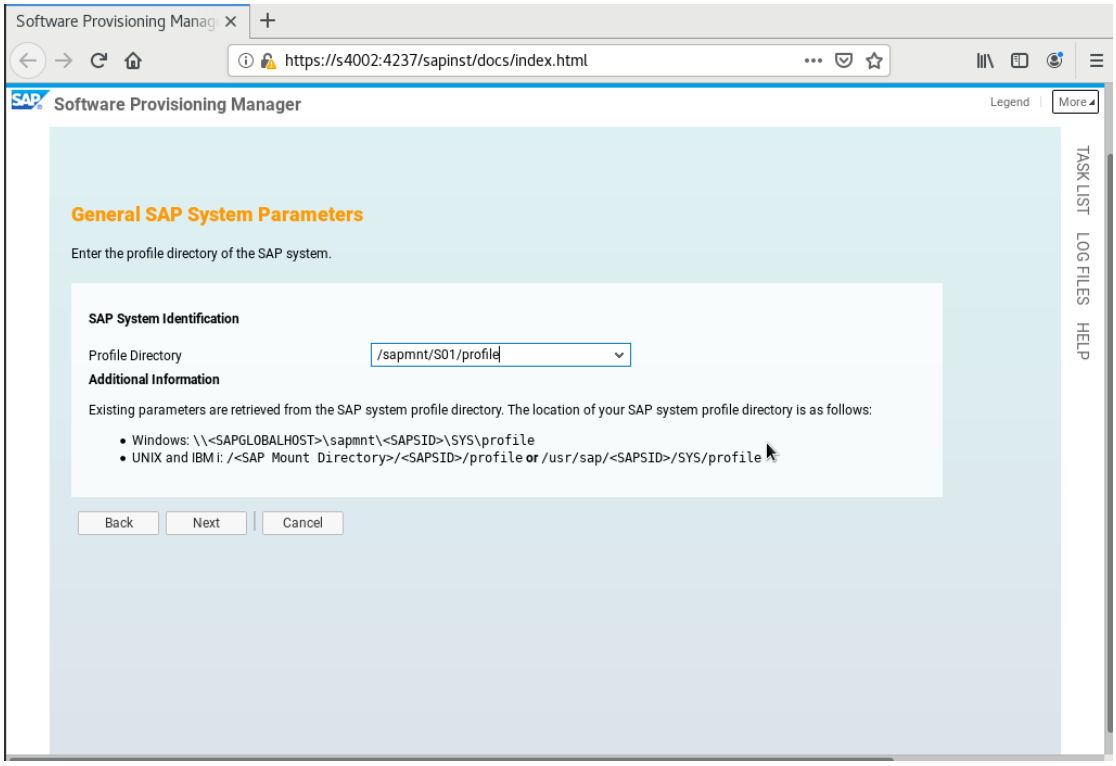
```
INFO       2020-07-21 14:10:33.959 (root/sapinst) (startInstallation) [CSiManagerInterfaces.cpp:2348]
Problem with the DNS configuration: could not determine the DNS domain of host s4002

INFO       2020-07-21 14:10:33.961 (root/sapinst) (guiWatchdog) [CSLPCommunicationServer.cpp:349]
Problem with the DNS configuration: could not determine the DNS domain of host s4002

INFO       2020-07-21 14:10:36.188 (root/sapinst) (SLPCommunicator) [SLPMonitoringStatemachine.cpp:1392]
********************************************************************************
Open your browser and paste the following URL address to access the GUI
https://s4002:4237/sapinst/docs/index.html
Logon users: [root]
********************************************************************************

=>sapparam(1c): No Profile used.
=>sapparam: SAPSYSTEMNAME neither in Profile nor in Commandline
load resource pool /sapcd/SWPM/resourcepool.xml
```

Step 2 Enter **https://s4002:4237/sapinst/docs/index.html** in the address box of a browser, and then log in to the SWPM system as the **root** user and install ERS Instance.

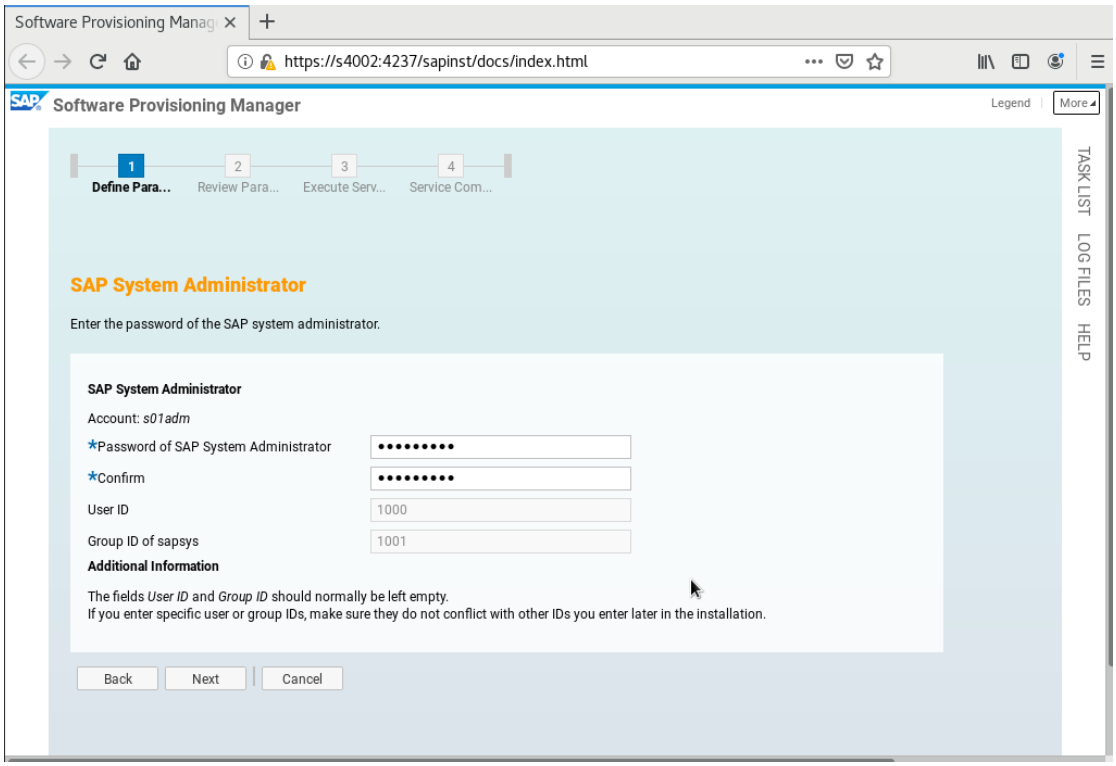
Select **ERS Instance** and click **Next**.



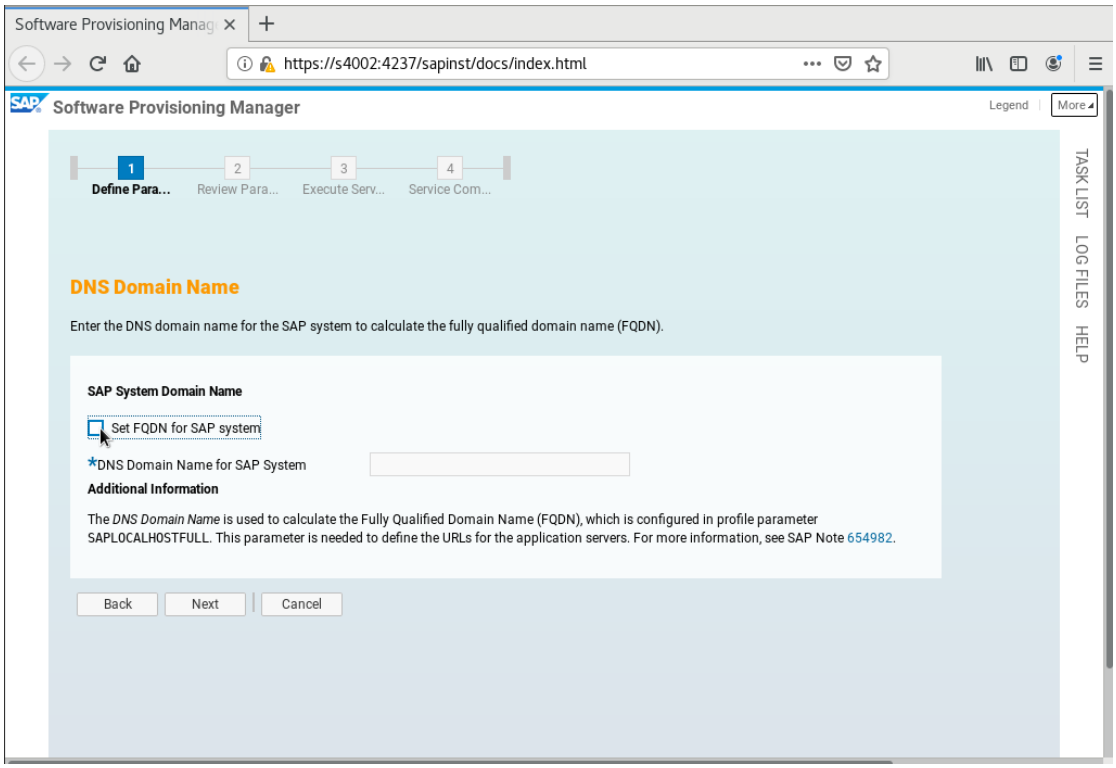
Step 3 Enter the directory where the **porfile** file is stored.



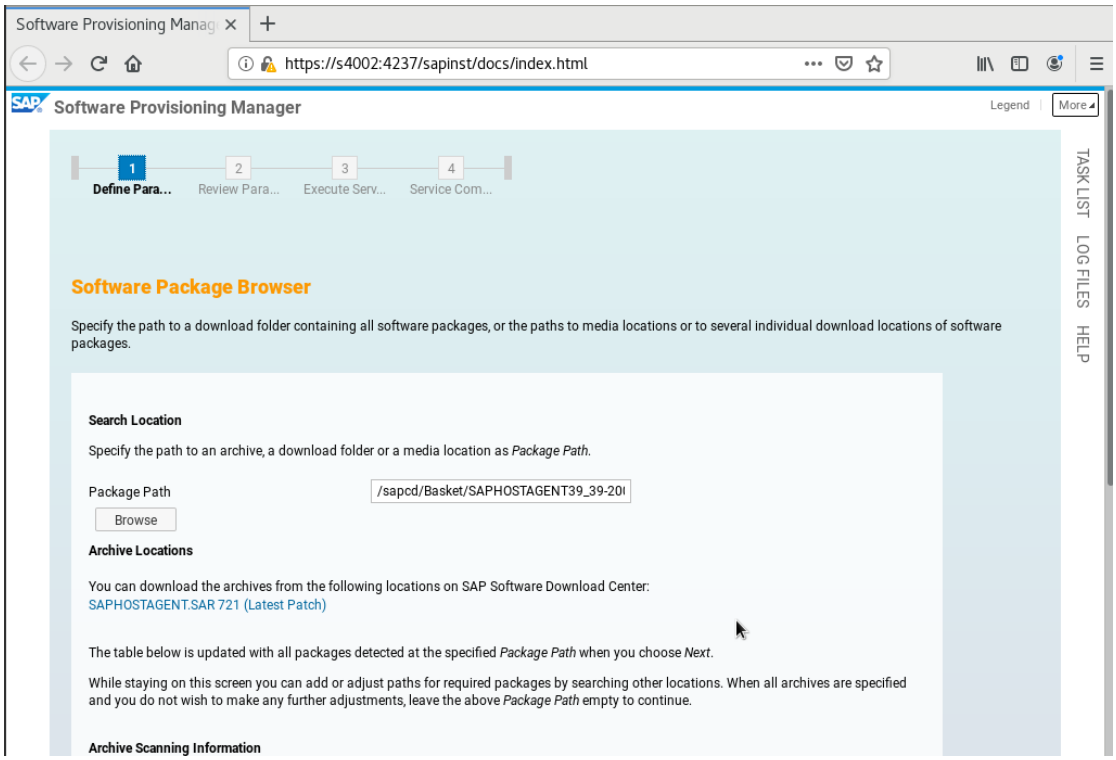
Step 4 Enter the password of the SAP system administrator.



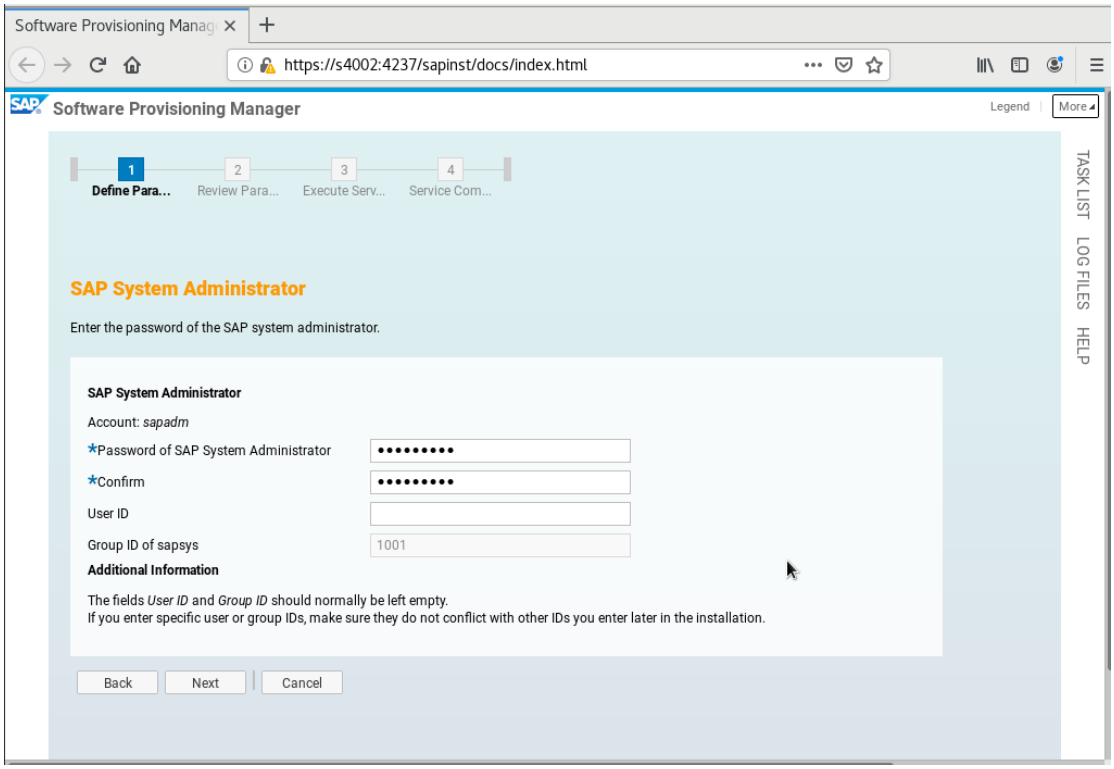
Step 5 Deselect **Set FQDN for SAP System**.



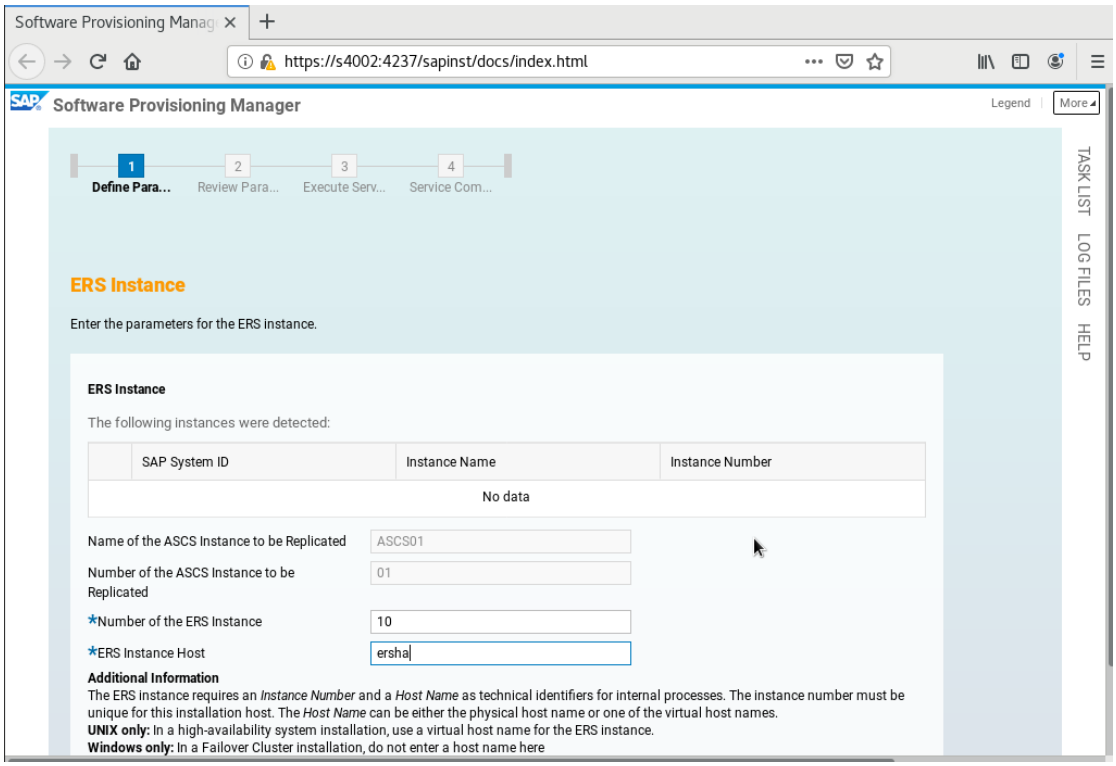
Step 6 Select a package path.



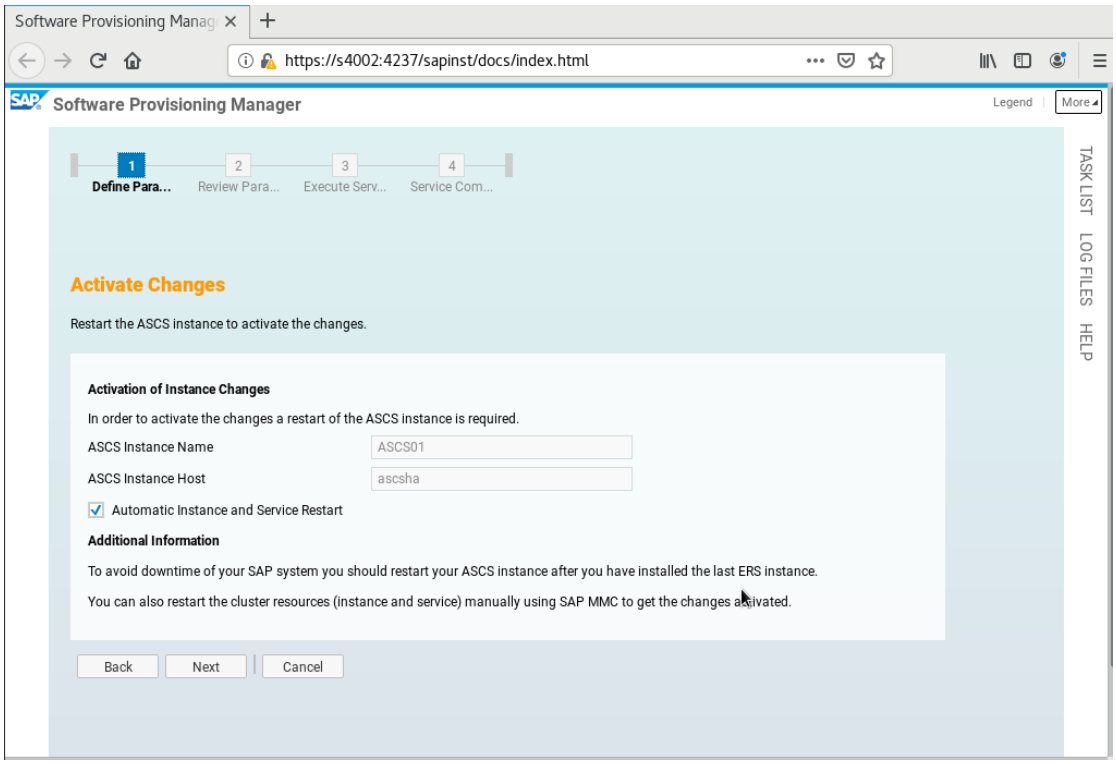
Step 7 Enter the password of the SAP system administrator.



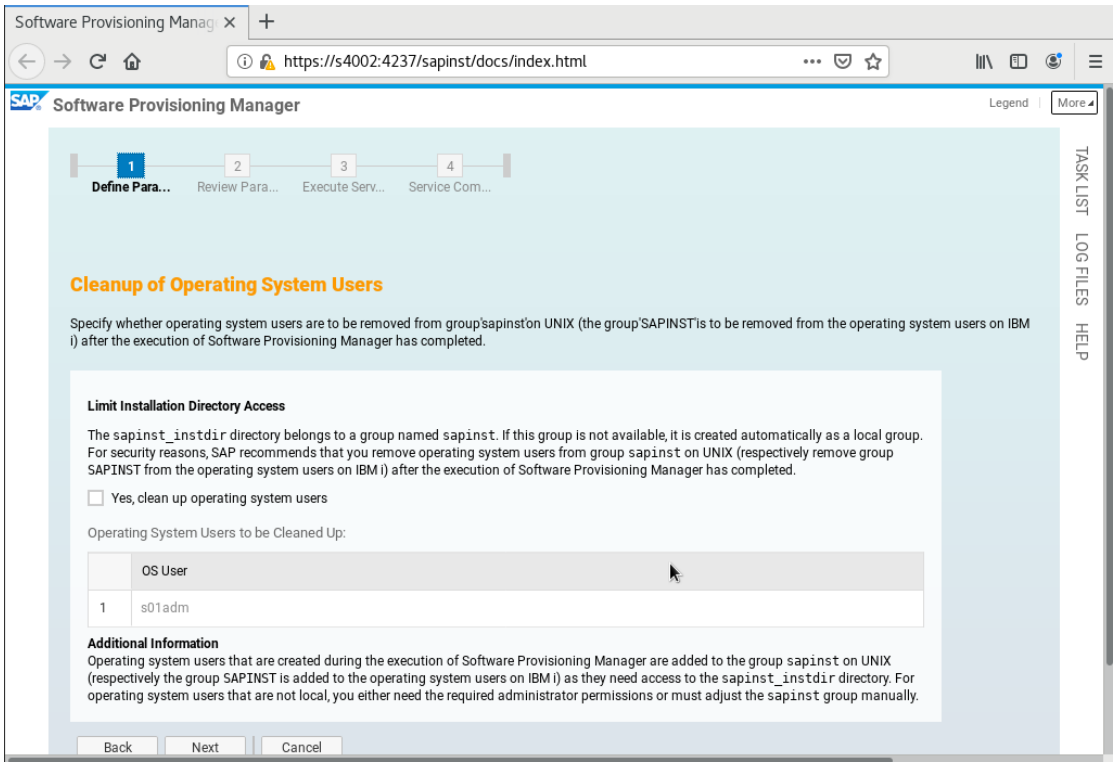
Step 8 Set **Number of the ERS Instance** and **ERS Instance Host** according to the installation planning. Enter the VM name (**ersha**) of the standby SAP S/4HANA node for **ERS Instance Host**.



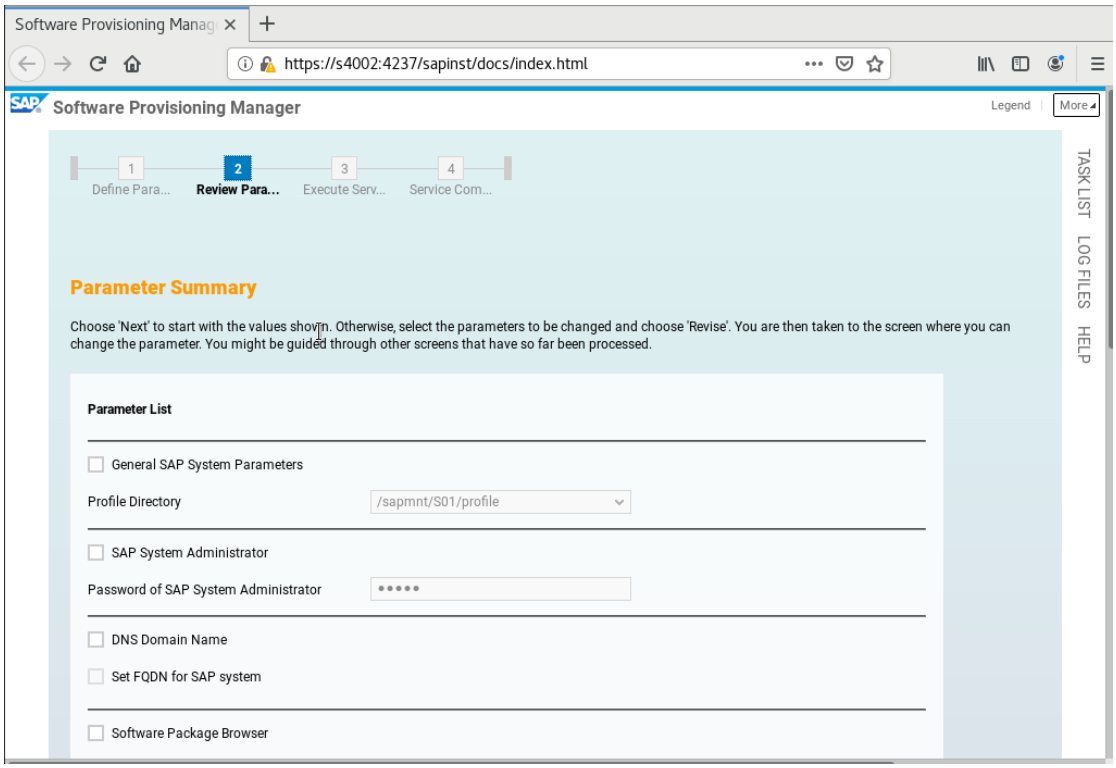
Step 9 Click **Next**.



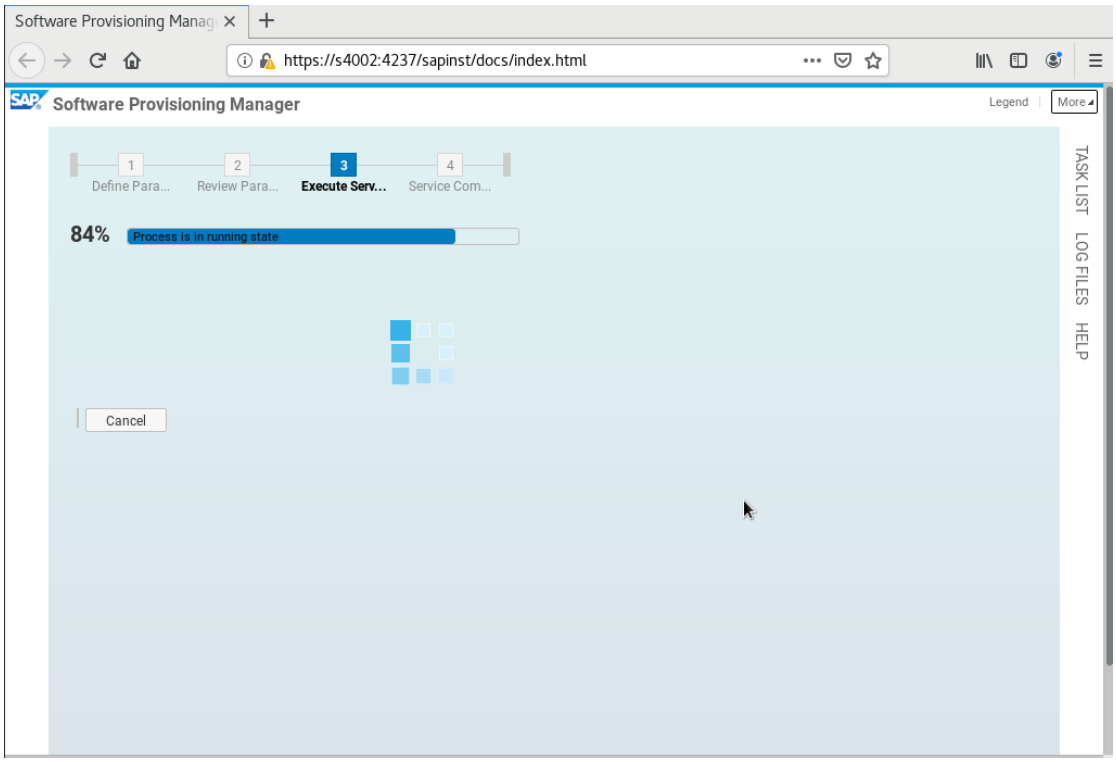
Step 10 Click **Next**.

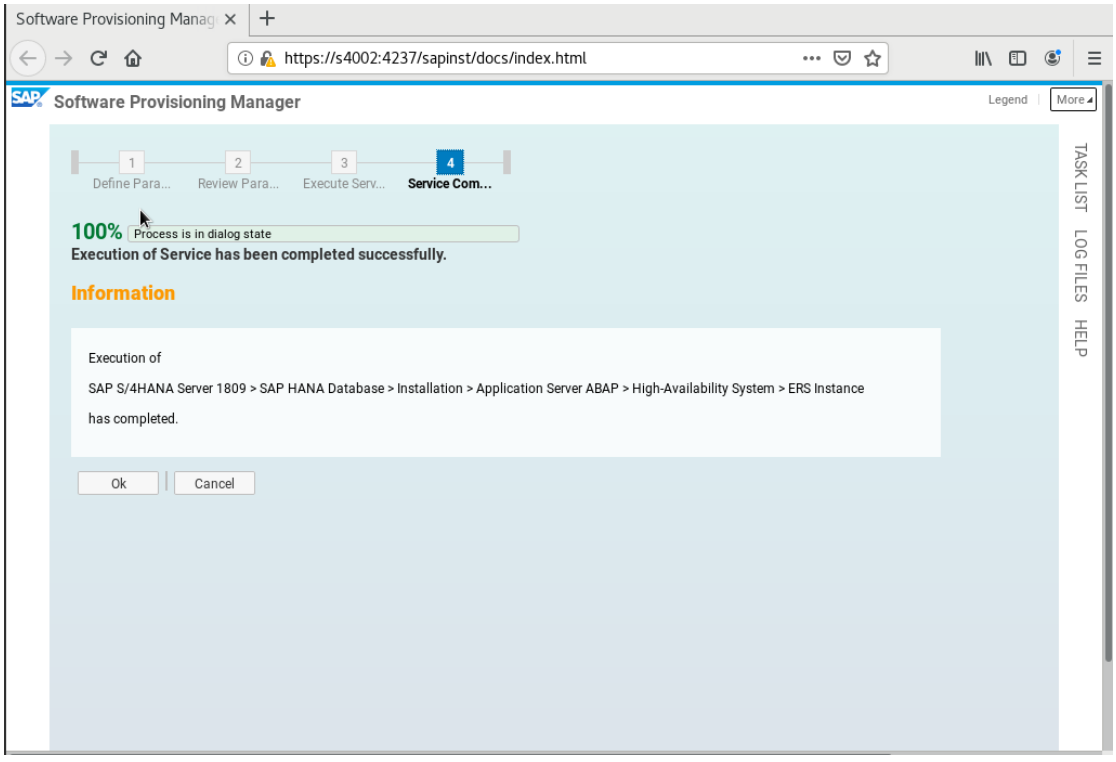


Step 11 Check your parameter settings. If they are all correct, click **Next**.



Step 12 The installation starts.





----End

4.5.2.5 Installing DB Instance

Procedure

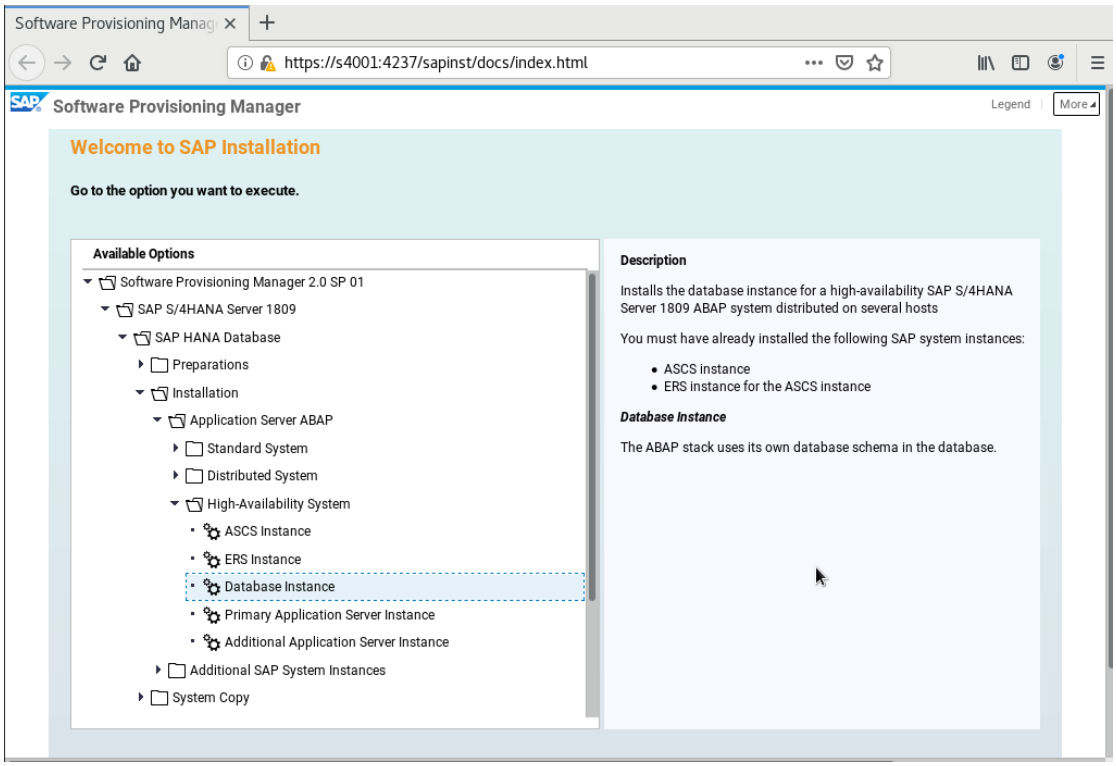
Step 1 Log in to the active SAP S/4HANA ECS **s4001** and go to the directory where the DB Instance installation package is stored to install it.

```
s4001:~ # cd /sapcd/SWPM/
s4001:/sapcd/SWPM # ./sapinst
[============================] | extracting...  done!
INFO       2020-07-21 14:35:21.276 (mainThread) [sixxcreate.cpp:347]
********************************************************************************
Initial log directory: /root/.sapinst/s4001/21815
********************************************************************************


SAPinst build information:
--------------------------
Version:         749.0.62
Build:           1875603
Compile time:    Oct 08 2018 - 14:01:31
Make type:       optU
Codeline:        749_REL
Platform:        linuxx86_64
Kernel build:    749, patch 611, changelist 1875937
SAP JRE build:   SAP Java Server VM (build 8.1.044 9.0.4+011, Sep  6 2018 16:58:06 - 81_REL - optU - linux amd64
 - 6 - bas2:309656 (mixed mode))
SAP JCo build:   3.0.18
SL-UI version:   2.6.28
SAP UI5 version: 1.50.4
Exe directory: /tmp/sapinst_exe.21814.1595313318

SAPinst process information:
----------------------------
Pid:        21815
```

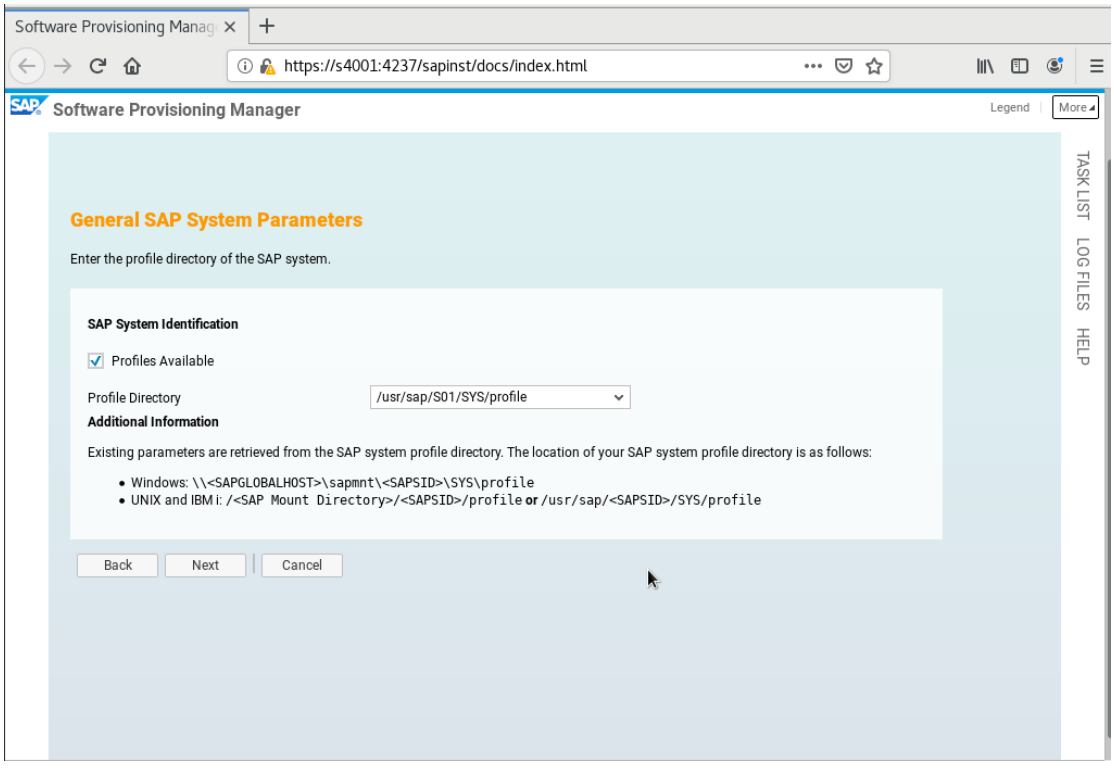
```
INFO       2020-07-21 14:35:21.579 (root/sapinst) (startInstallation) [CSiManagerInterfaces.cpp:2348]
Problem with the DNS configuration: could not determine the DNS domain of host s4001

INFO       2020-07-21 14:35:21.581 (root/sapinst) (guiWatchdog) [CSLPCommunicationServer.cpp:349]
Problem with the DNS configuration: could not determine the DNS domain of host s4001

INFO       2020-07-21 14:35:22.393 (root/sapinst) (SLPCommunicator) [SLPMonitoringStatemachine.cpp:1392]
********************************************************************************
Open your browser and paste the following URL address to access the GUI
https://s4001:4237/sapinst/docs/index.html
Logon users: [root]
********************************************************************************

=>sapparam(1c): No Profile used.
=>sapparam: SAPSYSTEMNAME neither in Profile nor in Commandline
load resource pool /sapcd/SWPM/resourcepool.xml
```

Step 2 Enter **https://s4002:4237/sapinst/docs/index.html** in the address box of a browser, and then log in to the SWPM system as the **root** user and install DB Instance.

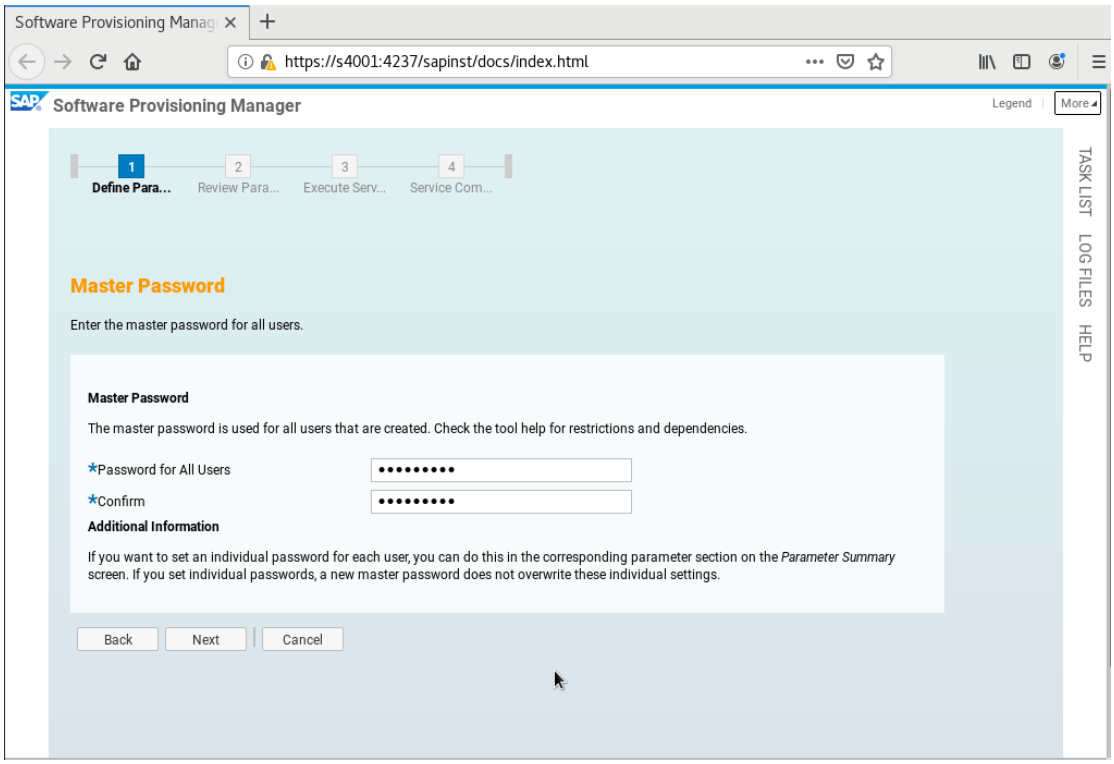
Select **Database Instance** and click **Next**.



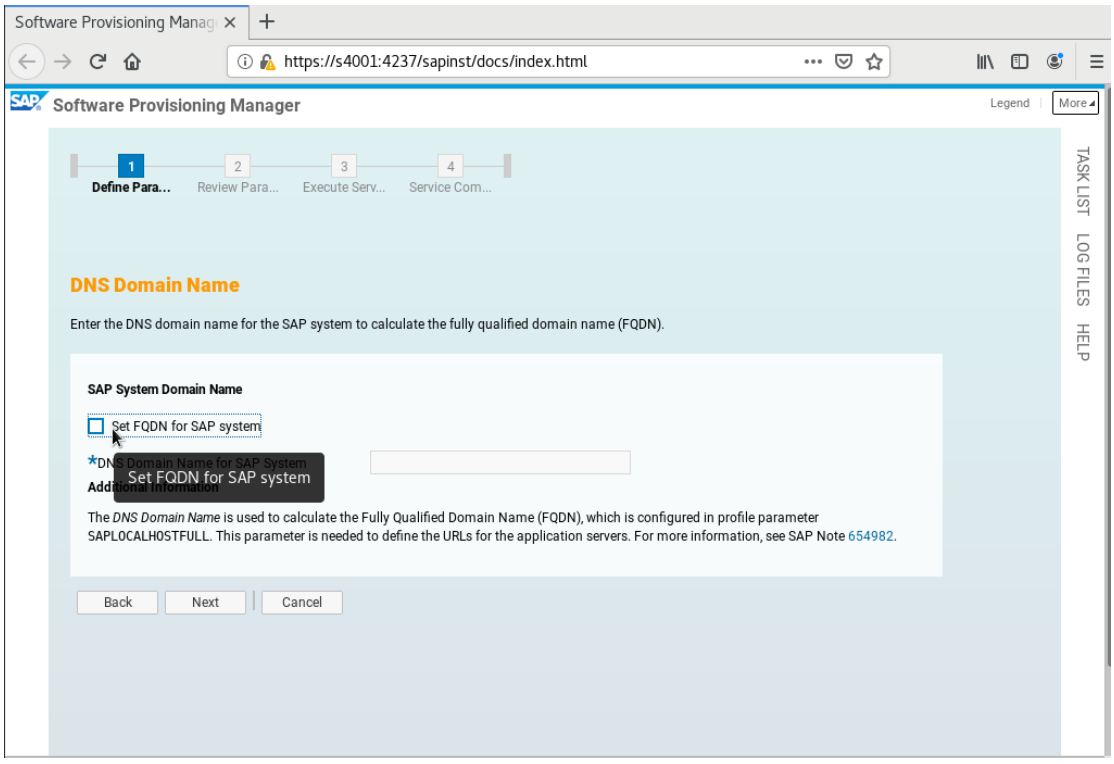
Step 3 Retain the default values, and click **Next**.



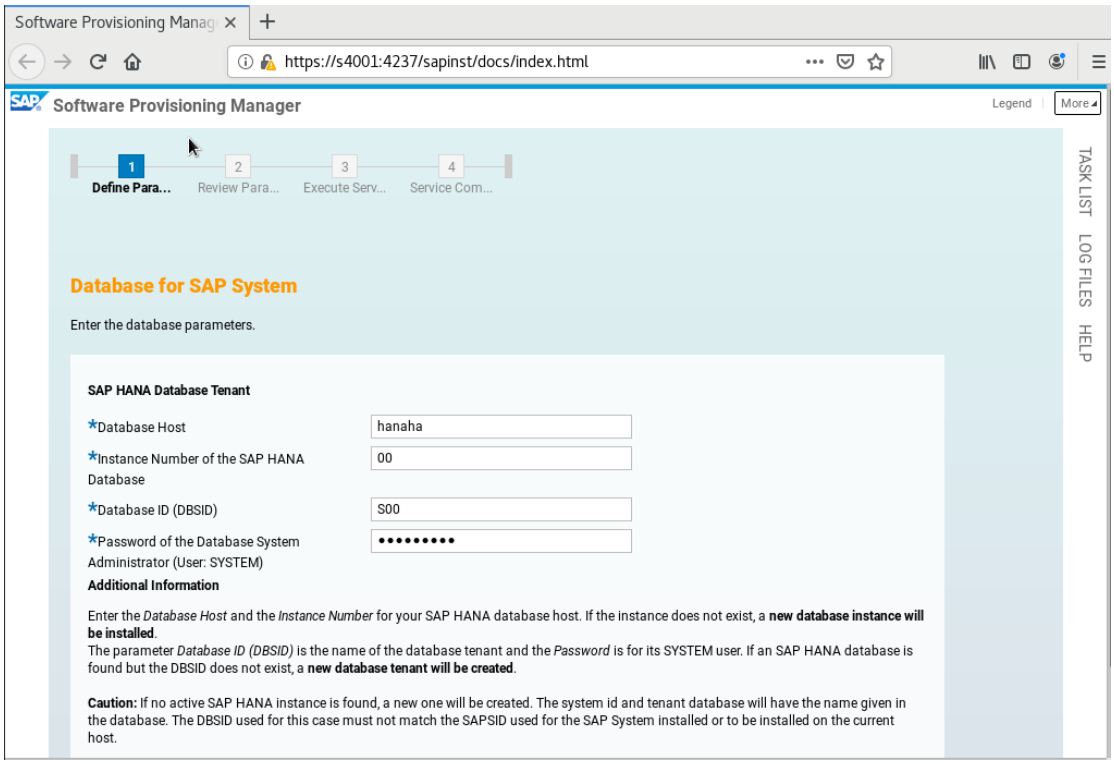
Step 4 Enter the master password for all users.



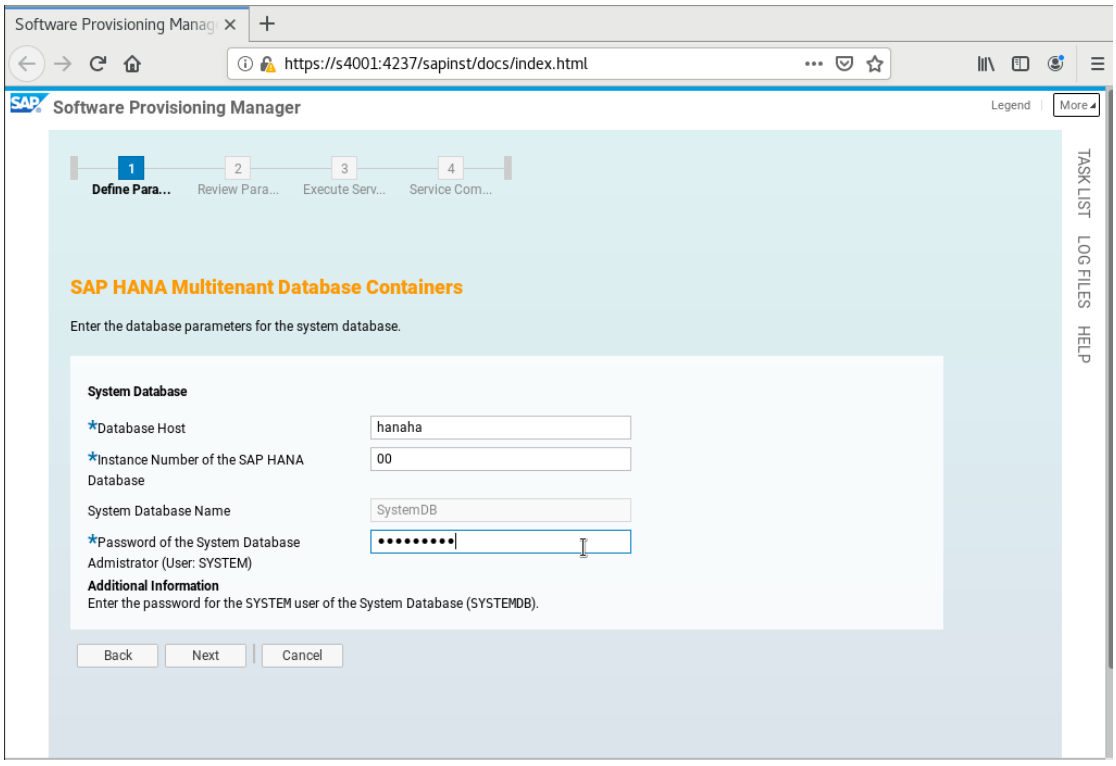
Step 5 Deselect **Set FQDN for SAP System**.



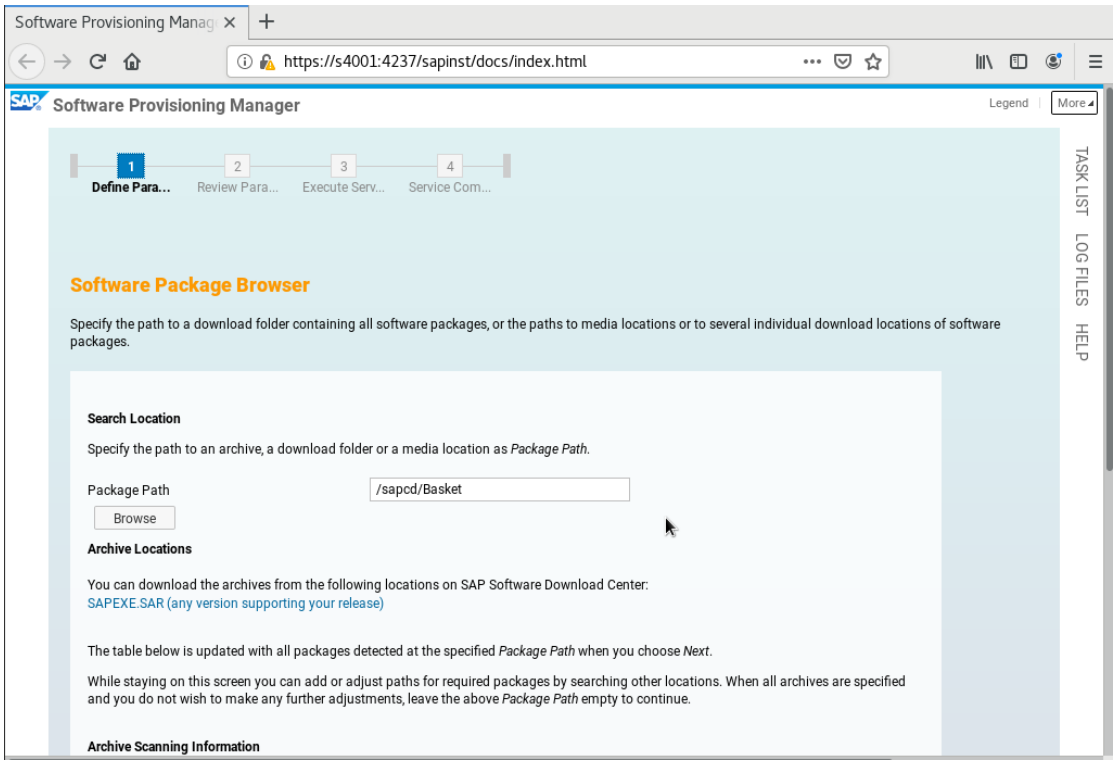
Set required parameters such as **Database Host**, **Instance Number of the SAP HANA Database**, and **Database ID (DBSID)**. Set **Database Host** to the VM name of the active SAP HANA node.



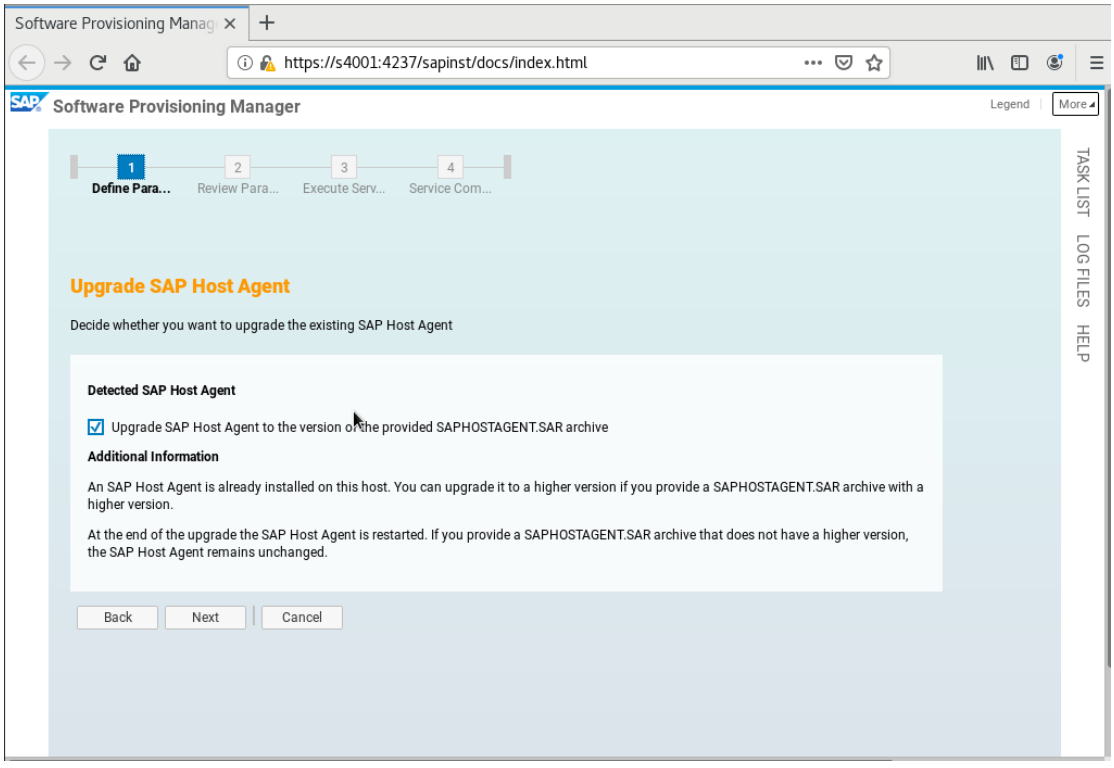
Step 6 Enter the password of the **SYSTEM** user.



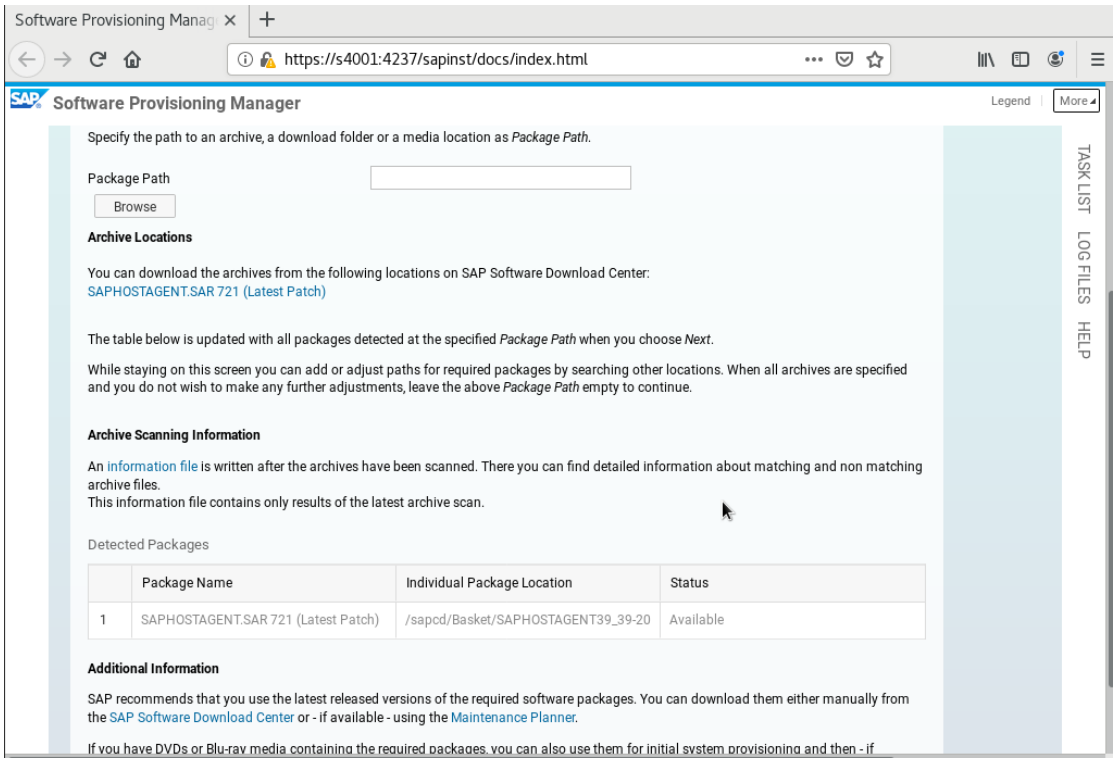
Step 7 Select a package path.



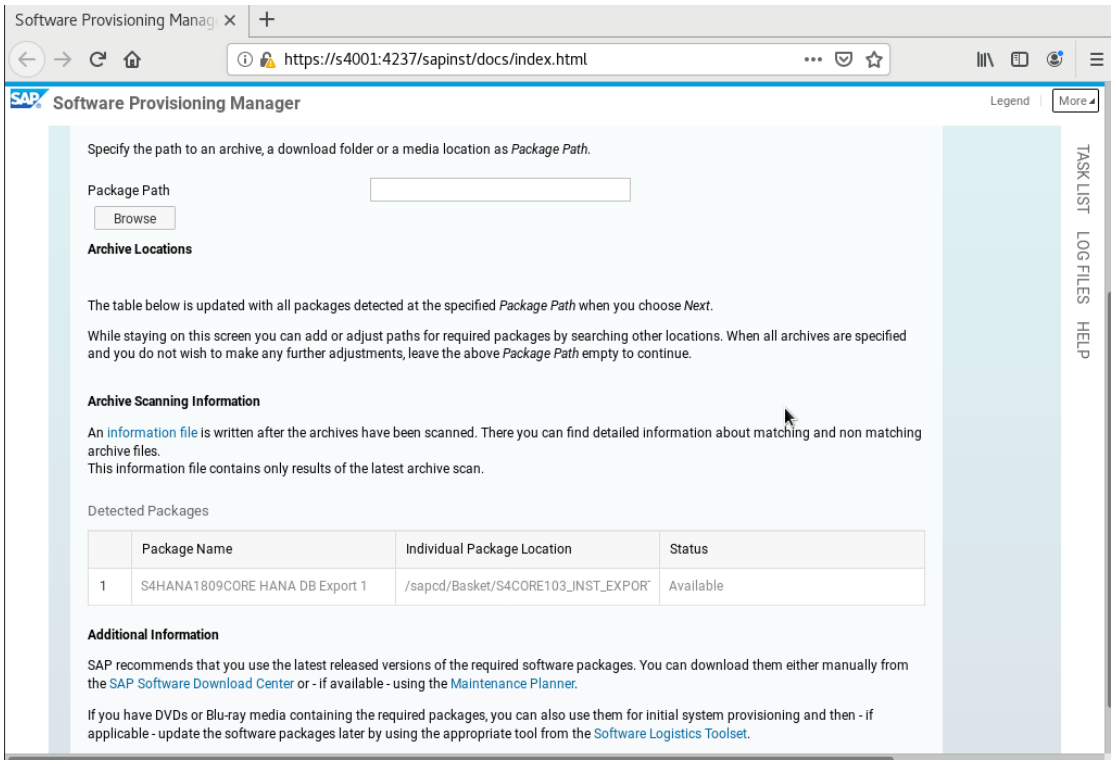
Step 8 Click **Next**.

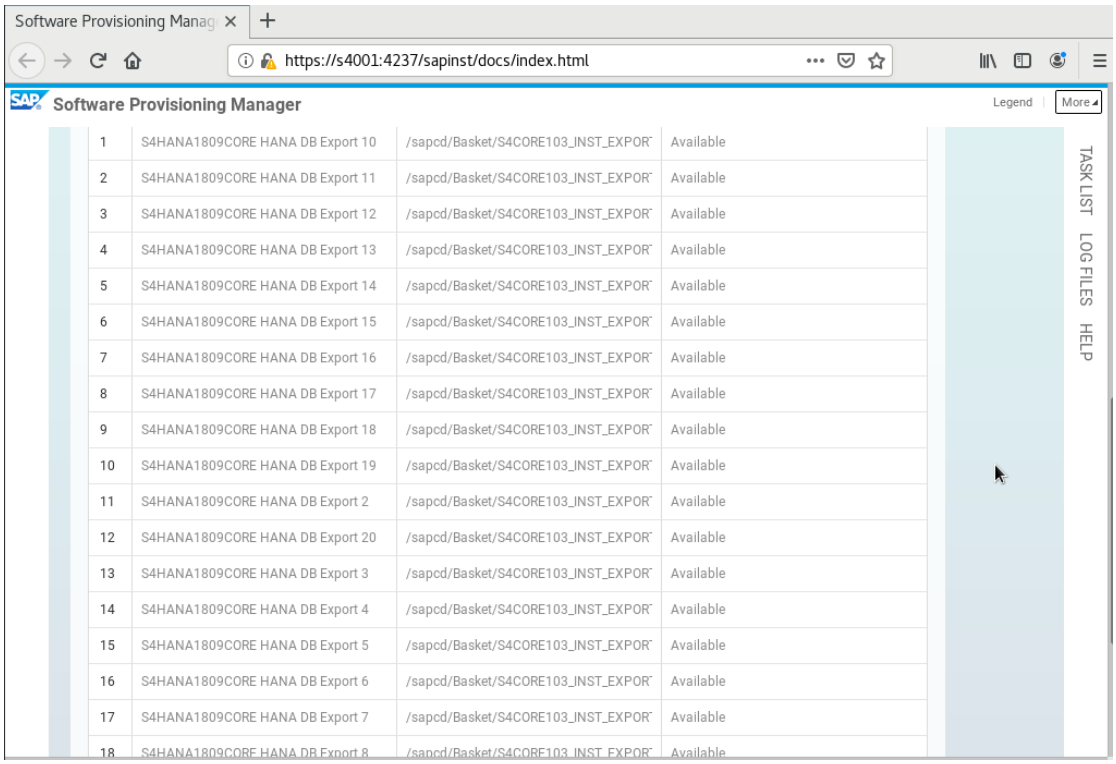


Step 9 Select a package path.

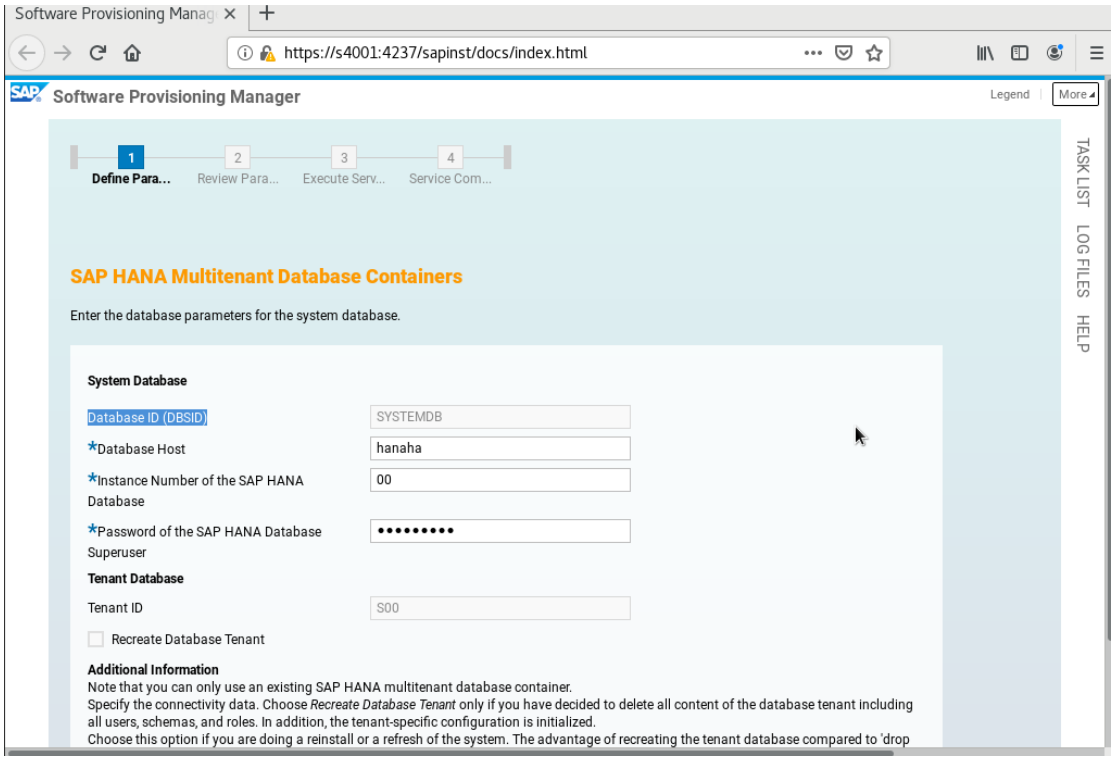


Step 10 Select a package path.

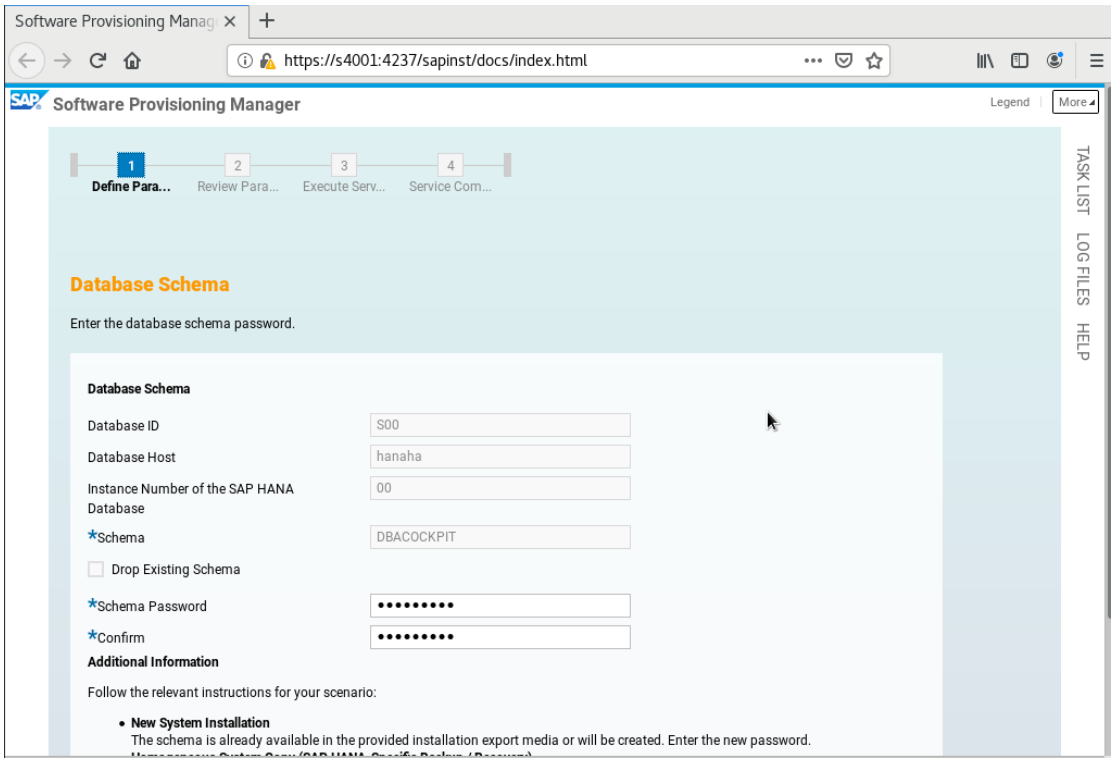


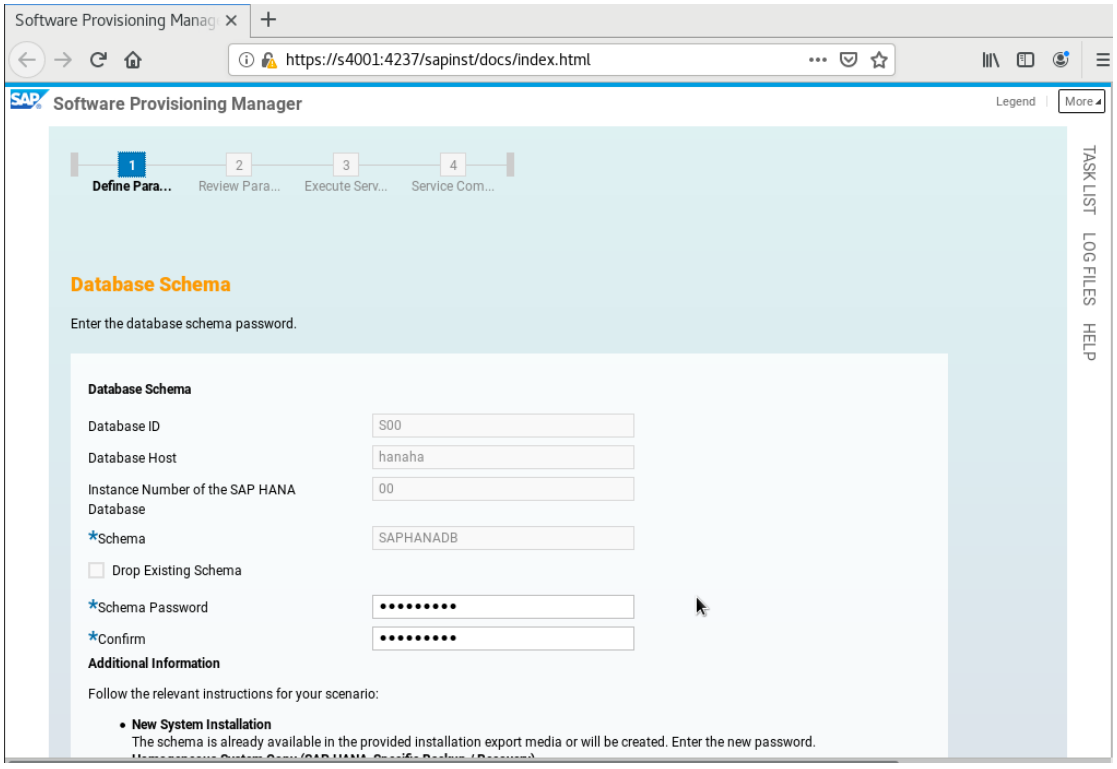


Step 11 Confirm the configuration information.

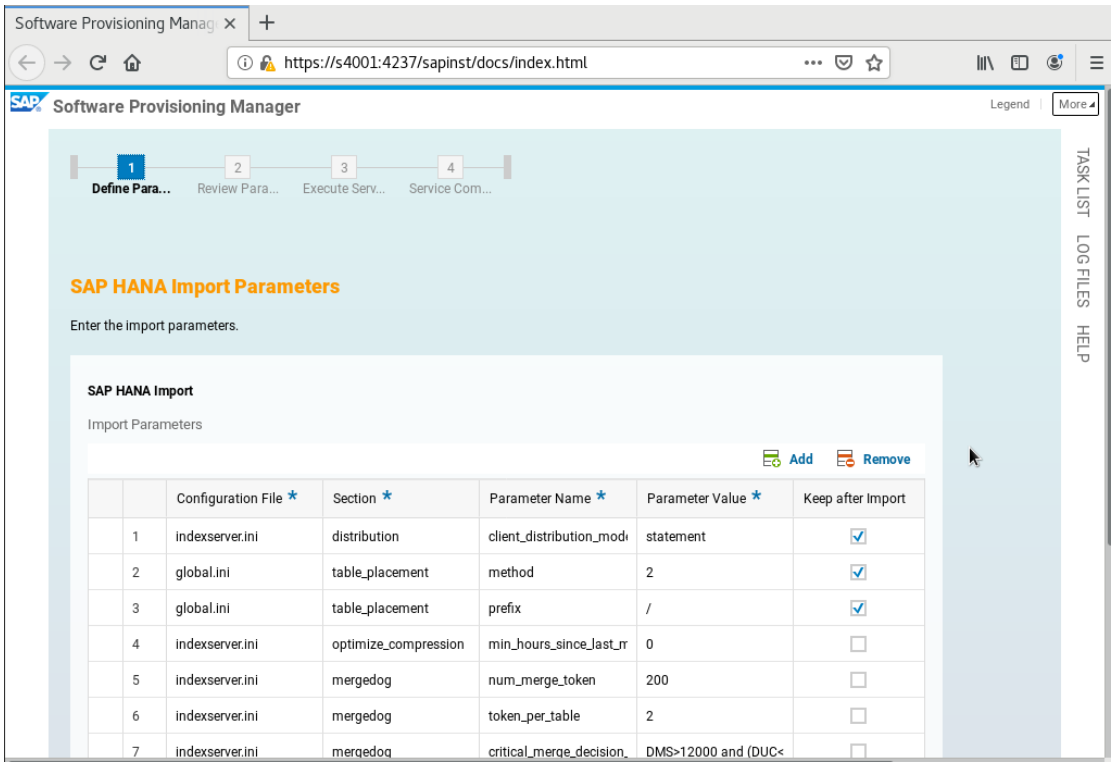


Step 12 Click **Next**.

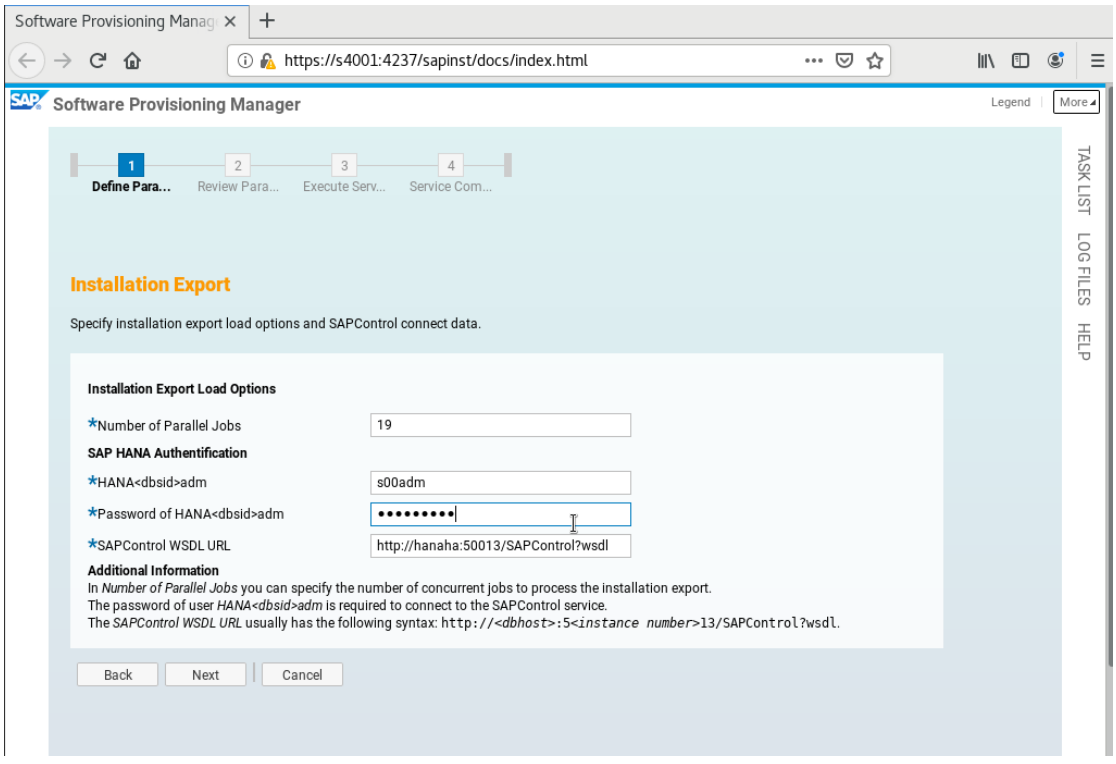




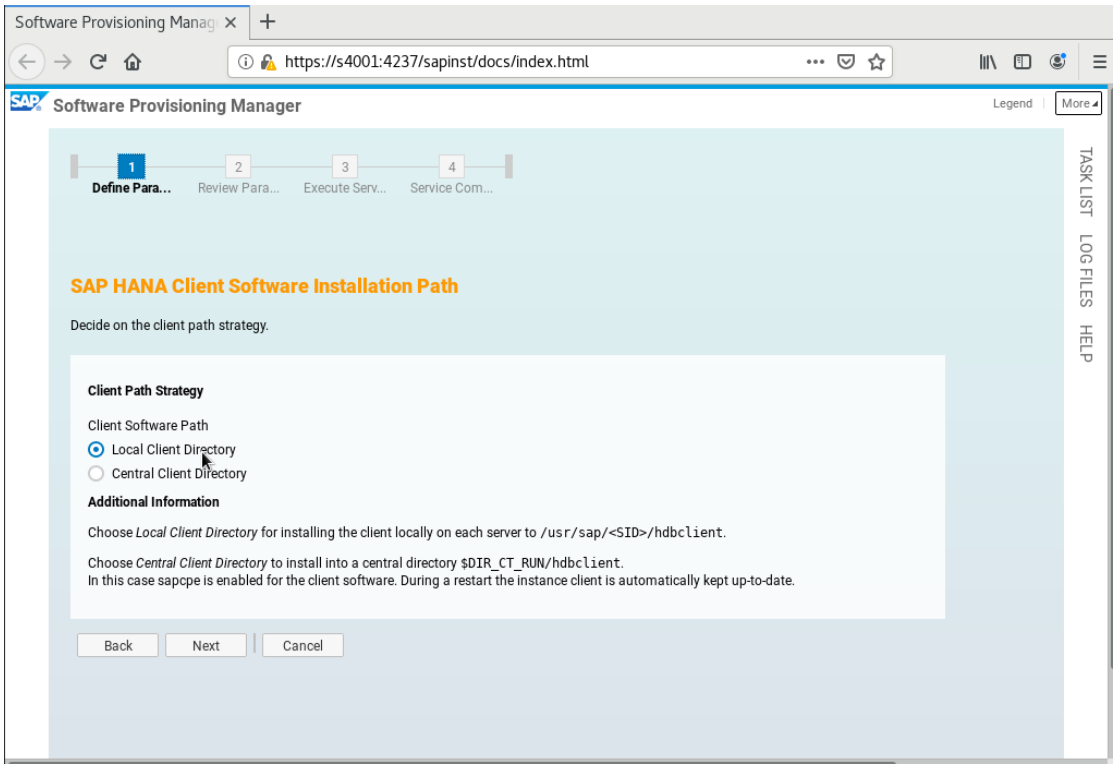
Step 13 Click **Next**.



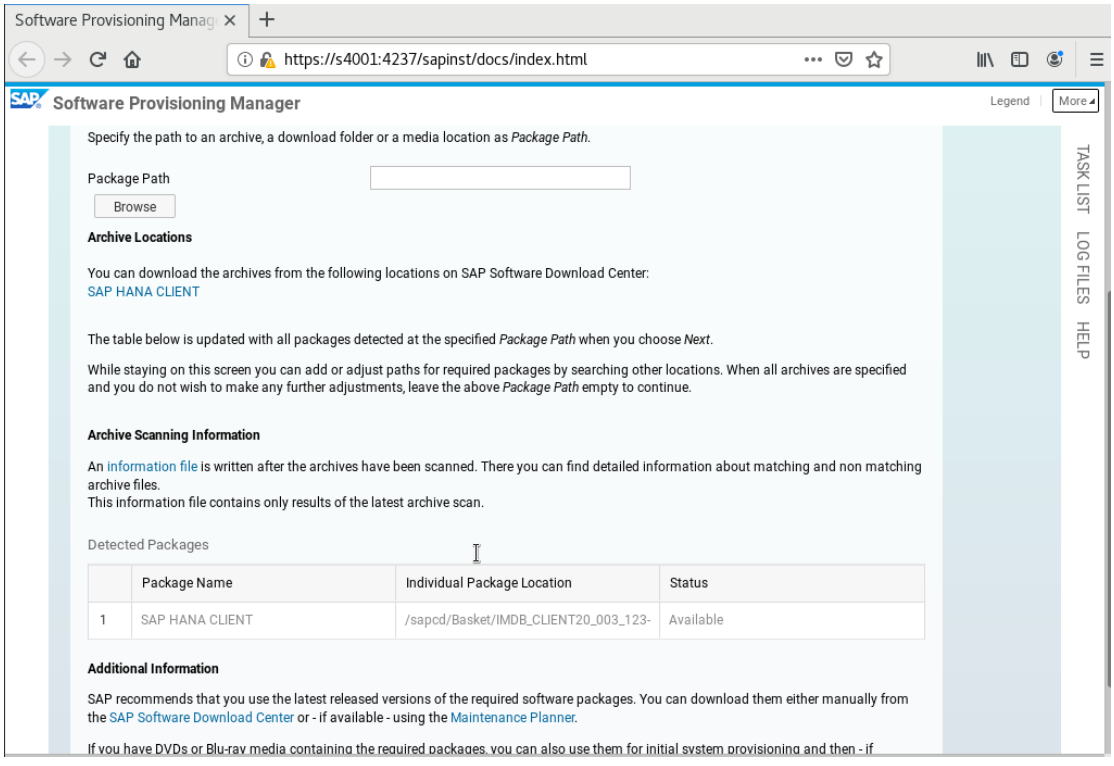
Step 14 Enter the password of **HANA<dbsid>admin**.



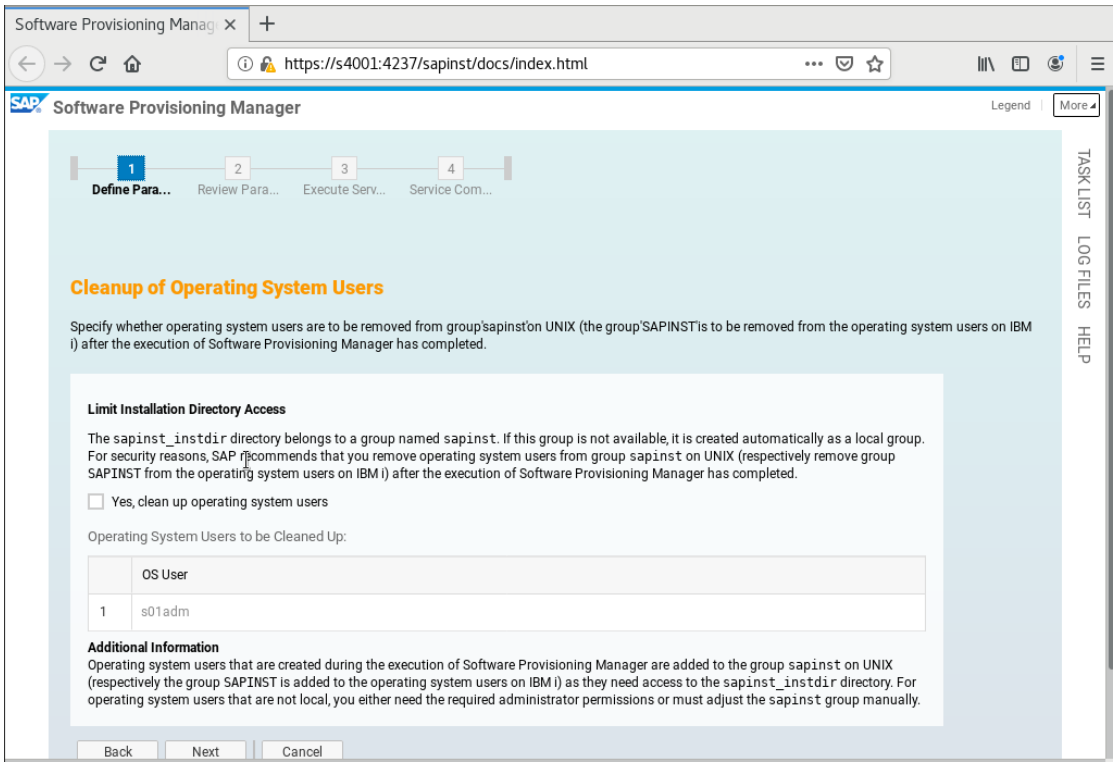
Step 15 Click **Next**.



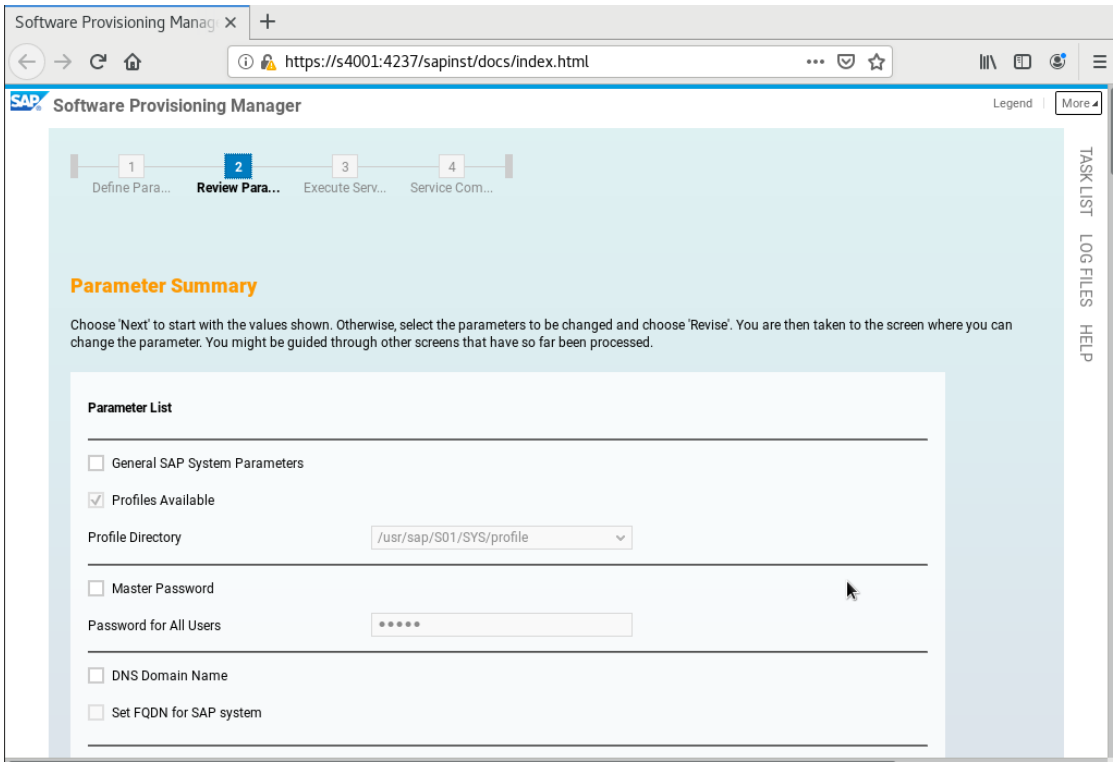
Step 16 Select a package path.



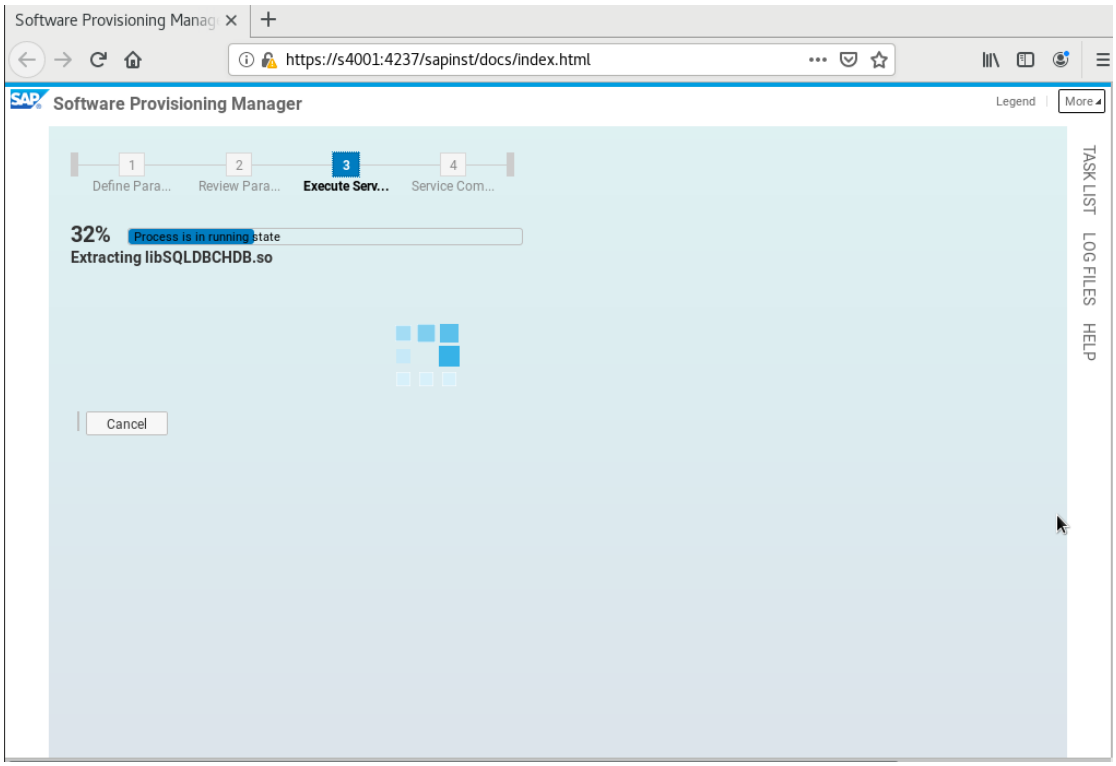
Step 17 Click **Next**.

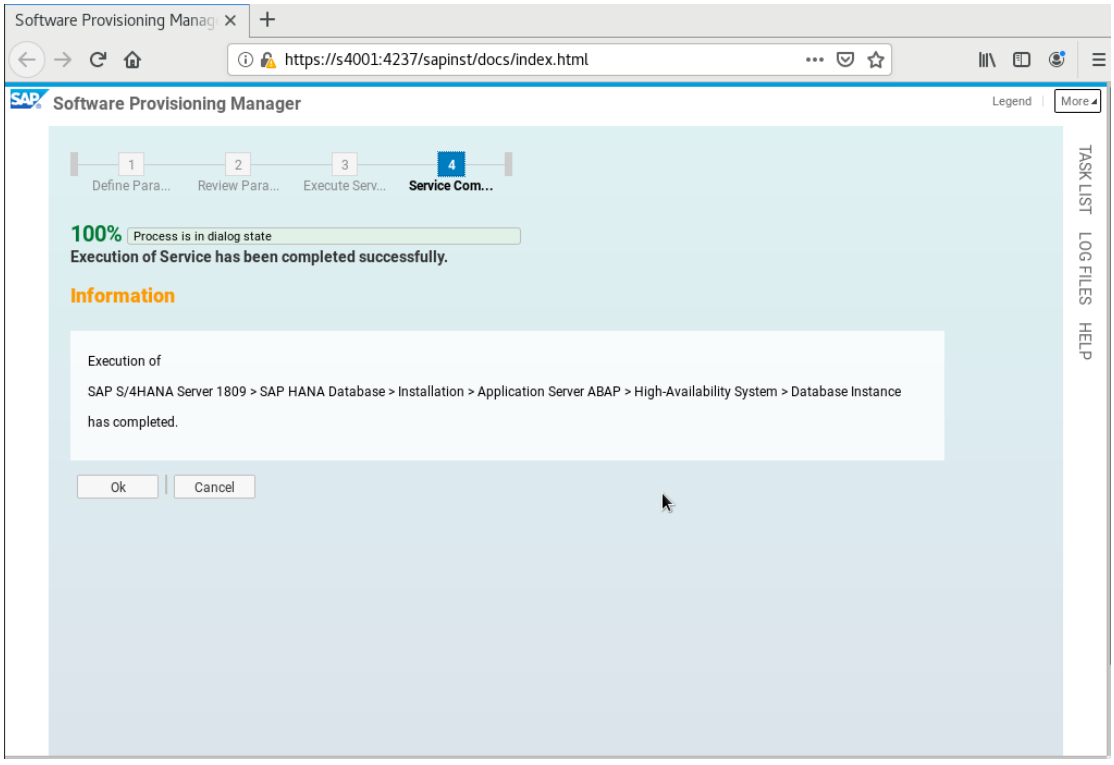


Step 18 Check your parameter settings. If they are all correct, click **Next**.



Step 19 The installation starts.





----End

4.5.2.6 Installing Primary Application Server (PAS) Instance

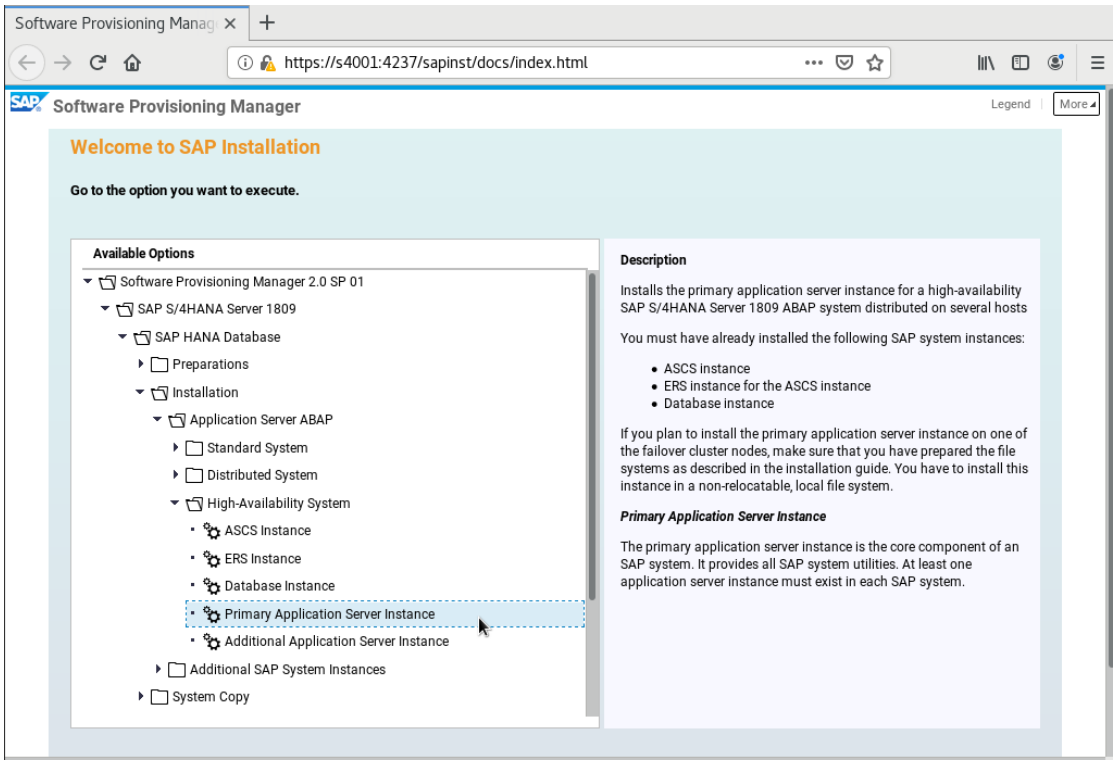
Procedure

Step 1 Go to the directory where the PAS Instance installation package is stored and install it on the active SAP S/4HANA node.

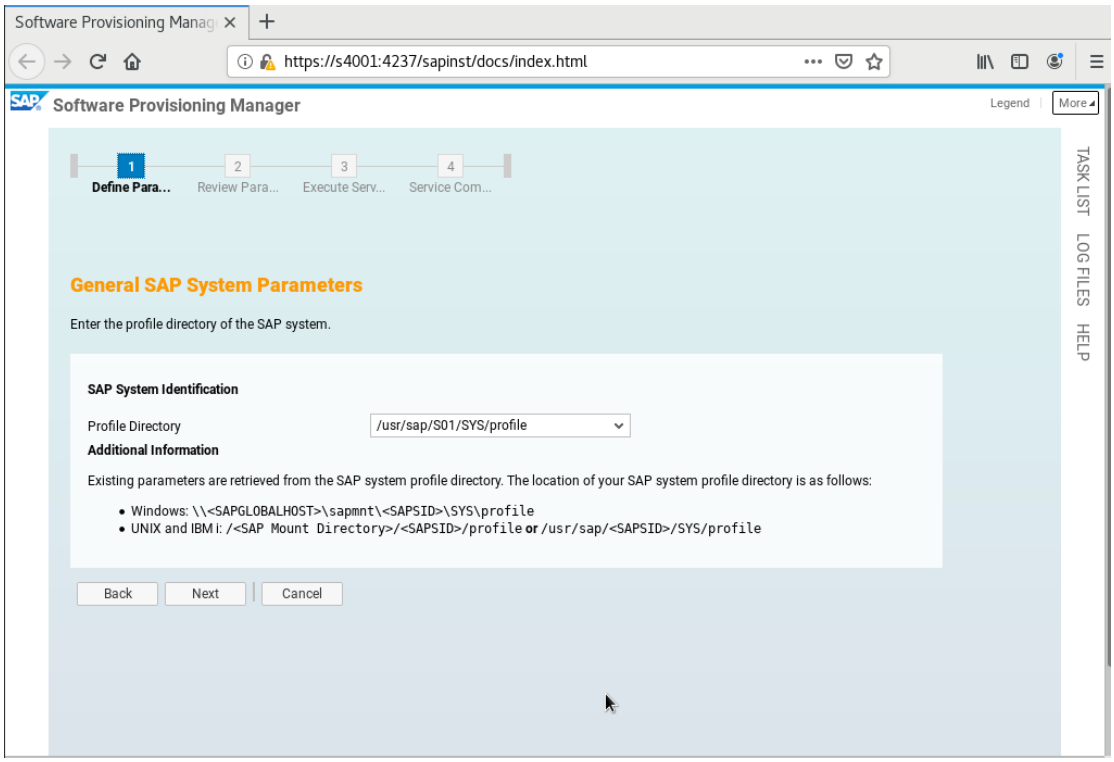
```
s4001:/sapcd/SWPM # ./sapinst
[==============================] | extracting...  done!
INFO       2020-07-21 16:57:17.209 (mainThread) [sixxcreate.cpp:347]
********************************************************************************
Initial log directory: /root/.sapinst/s4001/18980
********************************************************************************


SAPinst build information:
--------------------------
Version:          749.0.62
Build:            1875603
Compile time:     Oct 08 2018 - 14:01:31
Make type:        optU
Codeline:         749_REL
Platform:         linuxx86_64
Kernel build:     749, patch 611, changelist 1875937
SAP JRE build:    SAP Java Server VM (build 8.1.044 9.0.4+011, Sep  6 2018 16:58:06 - 81_REL - optU - linux amd64
 - 6 - bas2:309656 (mixed mode))
SAP JCo build:    3.0.18
SL-UI version:    2.6.28
SAP UI5 version: 1.50.4
Exe directory: /tmp/sapinst_exe.18979.1595321834

SAPinst process information:
----------------------------
Pid:         18980
```

```
INFO       2020-07-21 16:57:17.514 (root/sapinst) (startInstallation) [CSiManagerInterfaces.cpp:2348]
Problem with the DNS configuration: could not determine the DNS domain of host s4001

INFO       2020-07-21 16:57:17.516 (root/sapinst) (guiWatchdog) [CSLPCommunicationServer.cpp:349]
Problem with the DNS configuration: could not determine the DNS domain of host s4001

INFO       2020-07-21 16:57:18.328 (root/sapinst) (SLPCommunicator) [SLPMonitoringStatemachine.cpp:1392]
********************************************************************************
Open your browser and paste the following URL address to access the GUI
https://s4001:4237/sapinst/docs/index.html
Logon users: [root]
********************************************************************************

=>sapparam(1c): No Profile used.
=>sapparam: SAPSYSTEMNAME neither in Profile nor in Commandline
load resource pool /sapcd/SWPM/resourcepool.xml
```

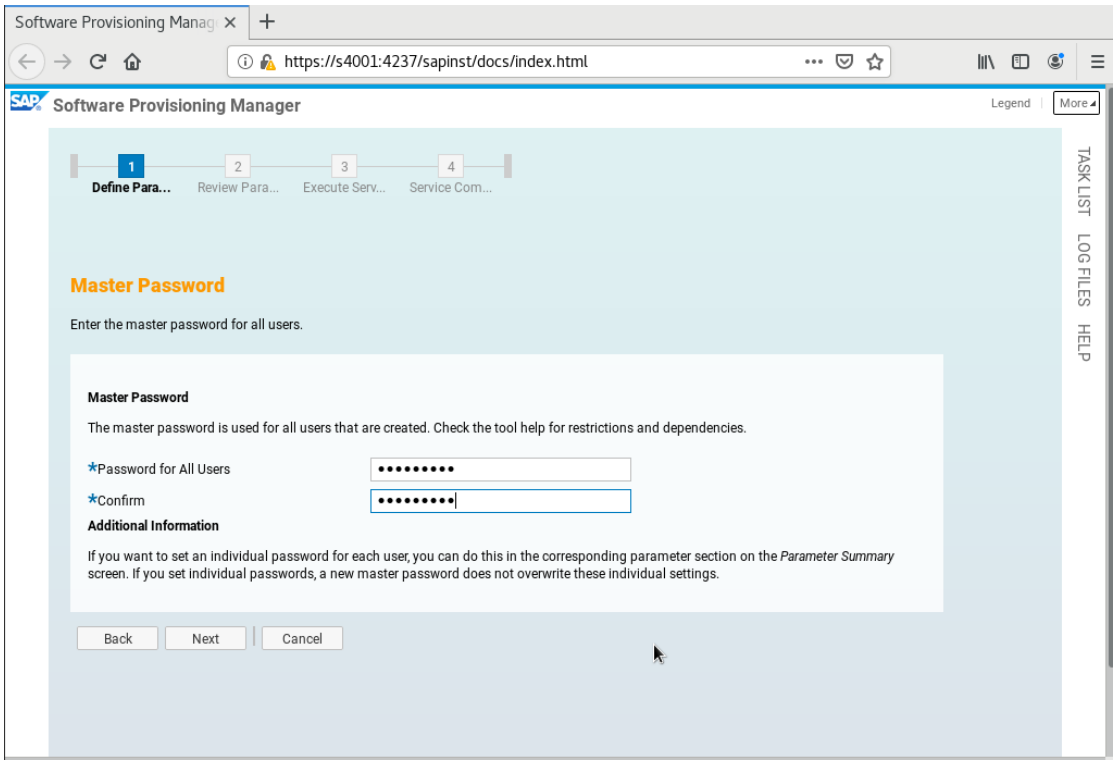
Step 2 Enter **https://s4002:4237/sapinst/docs/index.html** in the address box of a browser, and then log in to the SWPM system as the **root** user and install PAS Instance. Select **Primary Application Server Instance** and click **Next**.



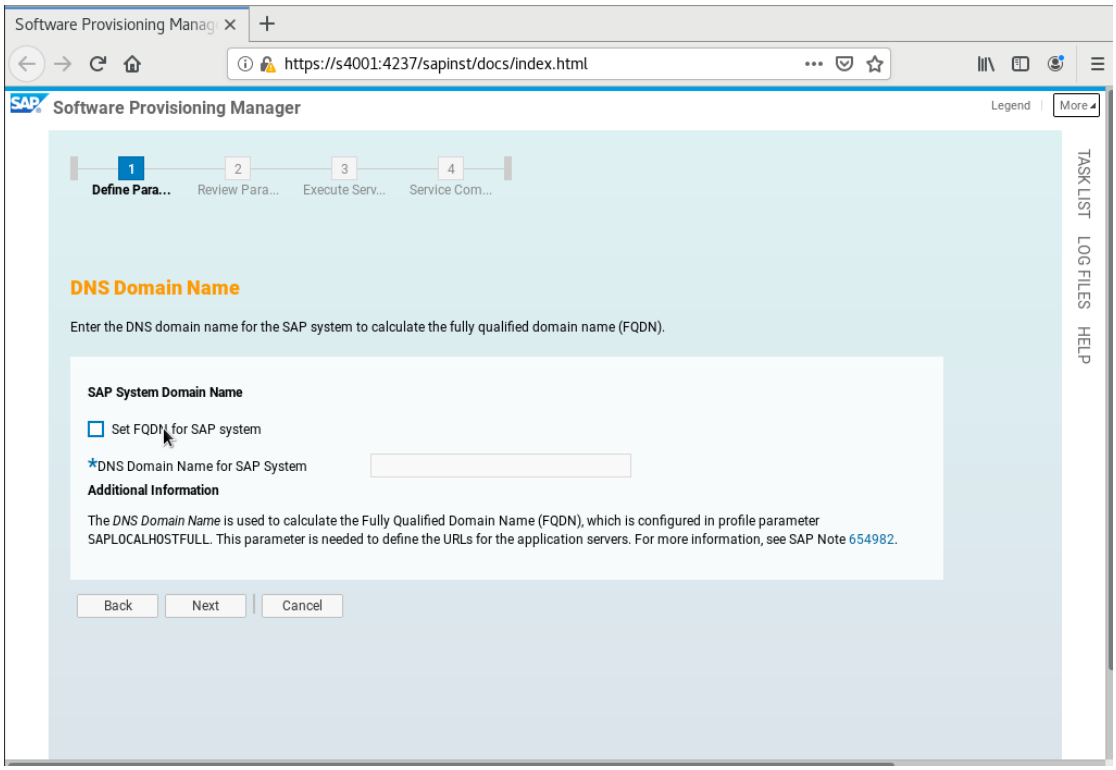
Step 3 Click **Next**.



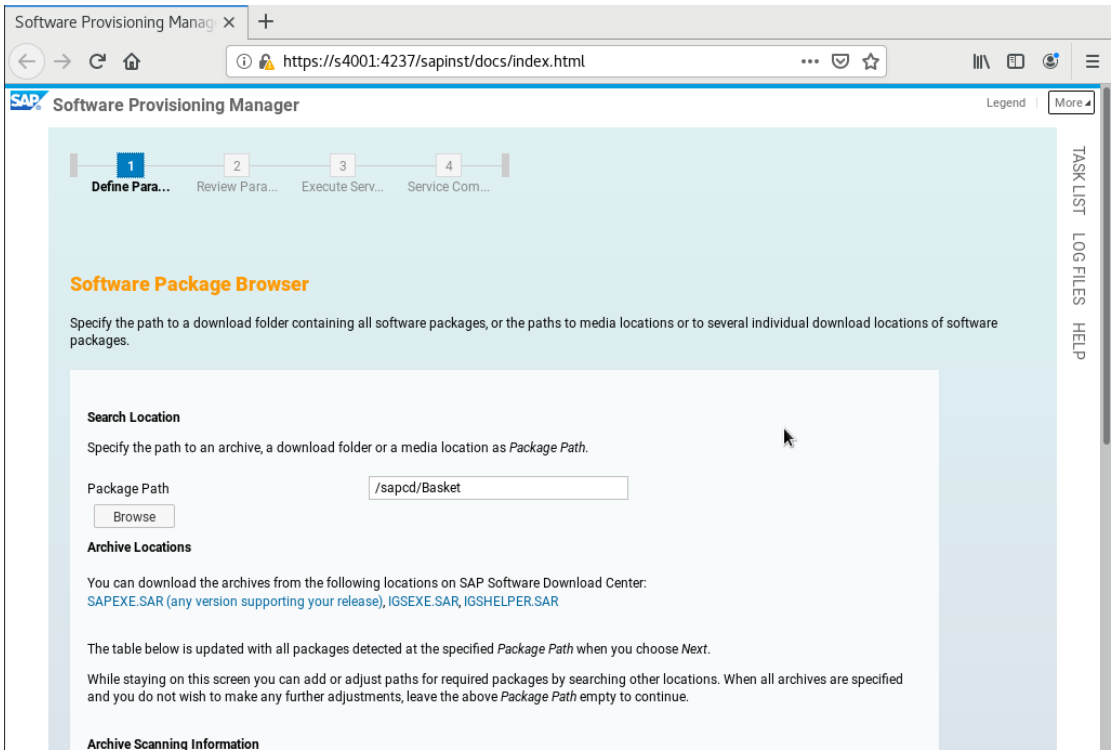
Step 4 Enter the master password for all users.



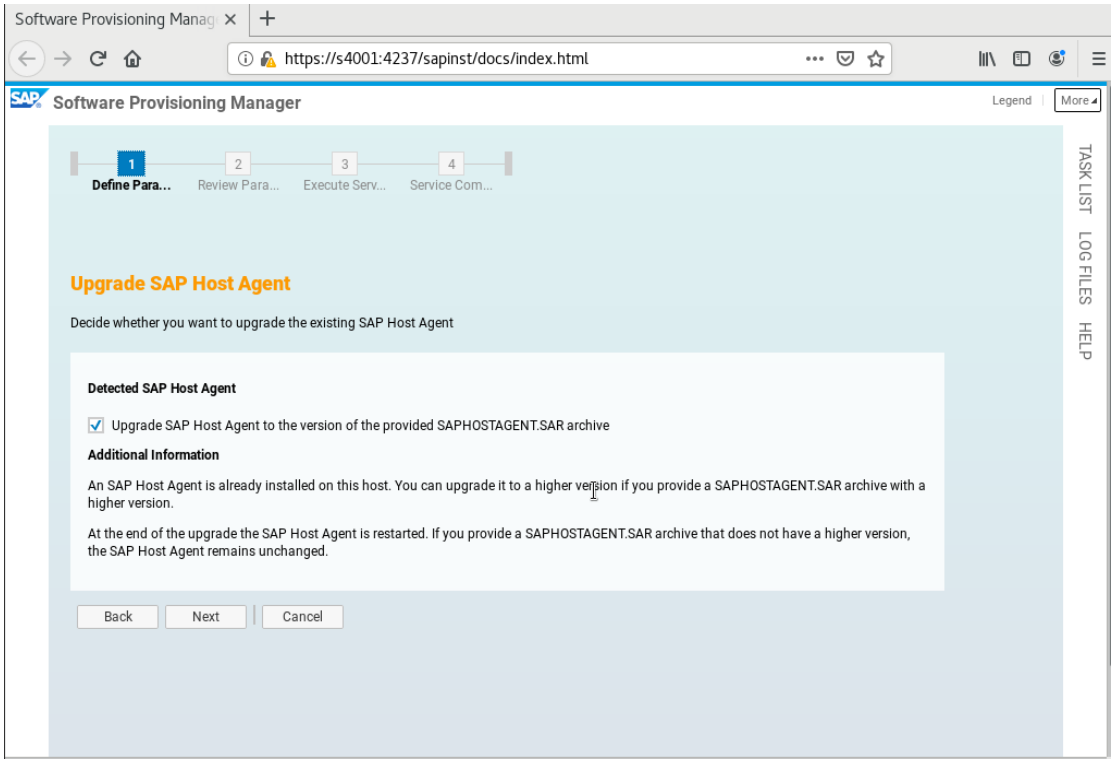
Step 5 Deselect **Set FQDN for SAP System**.



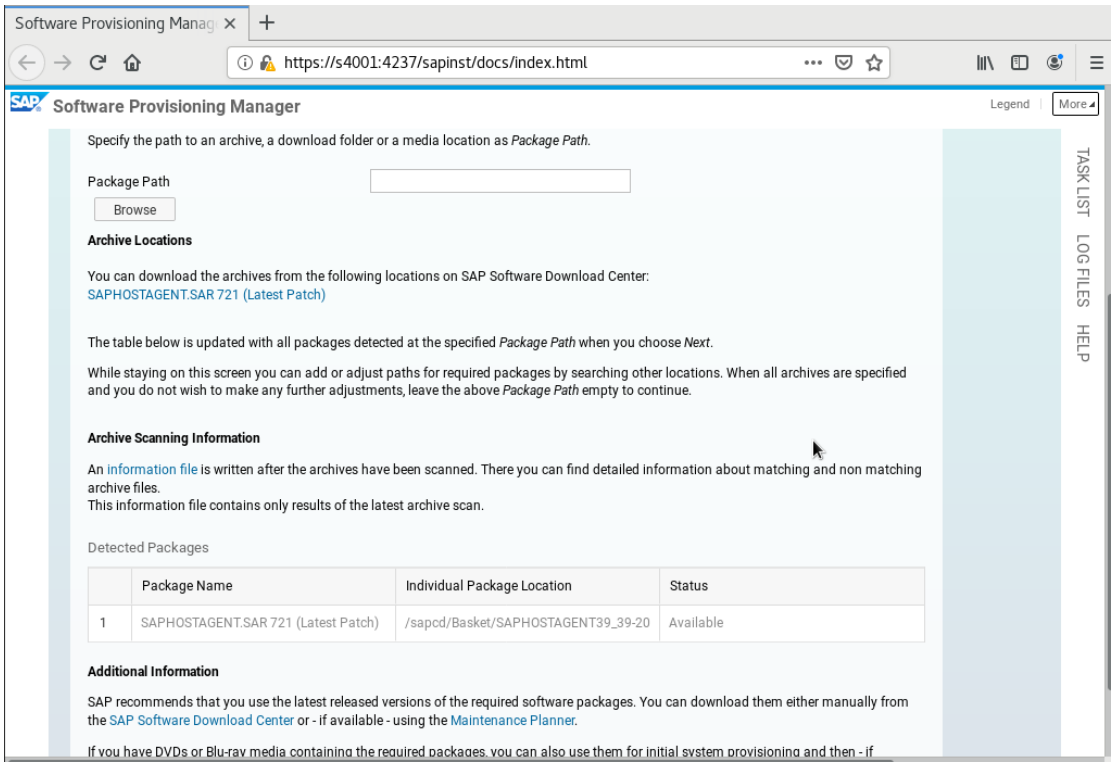
Select a package path.



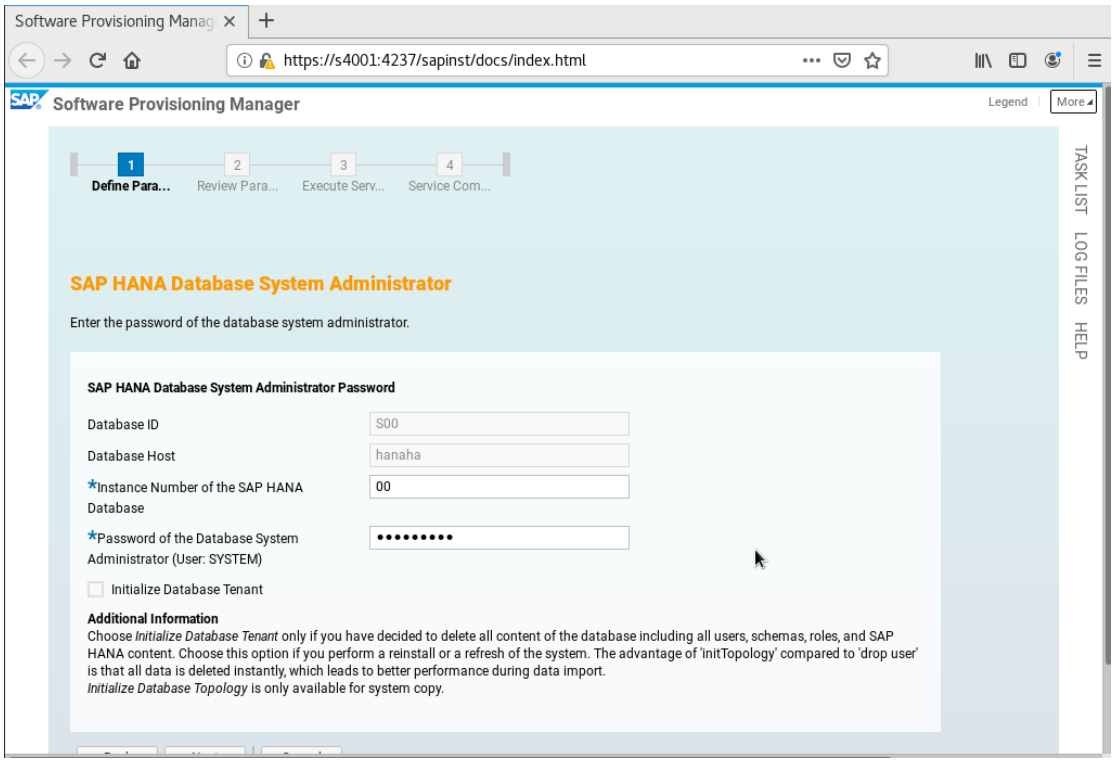
Step 6 Click **Next**.



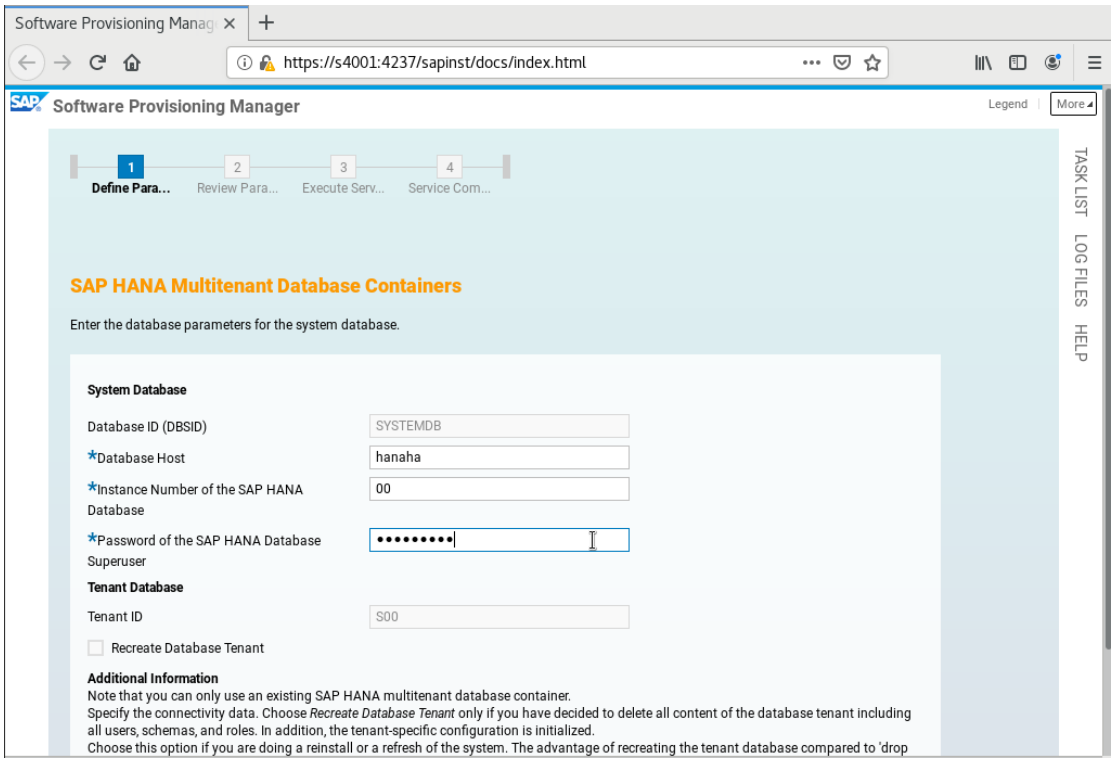
Step 7 Select a package path.



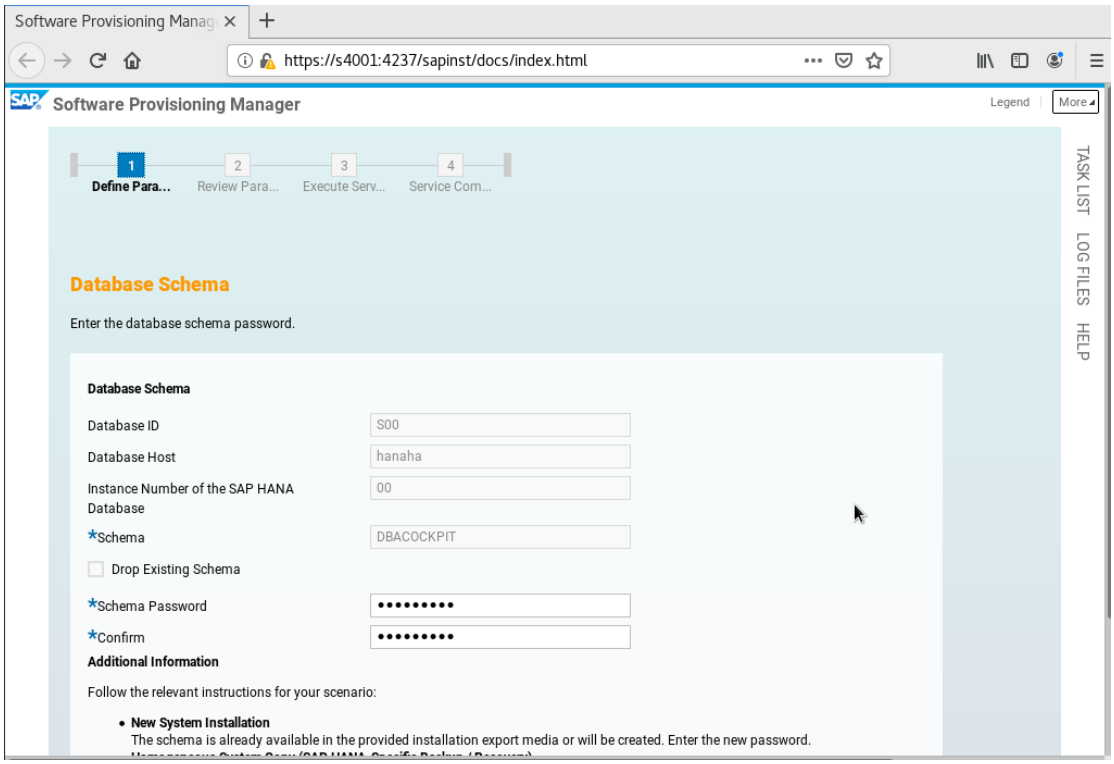
Step 8 Set **Instance Number of the SAP HANA Database**.

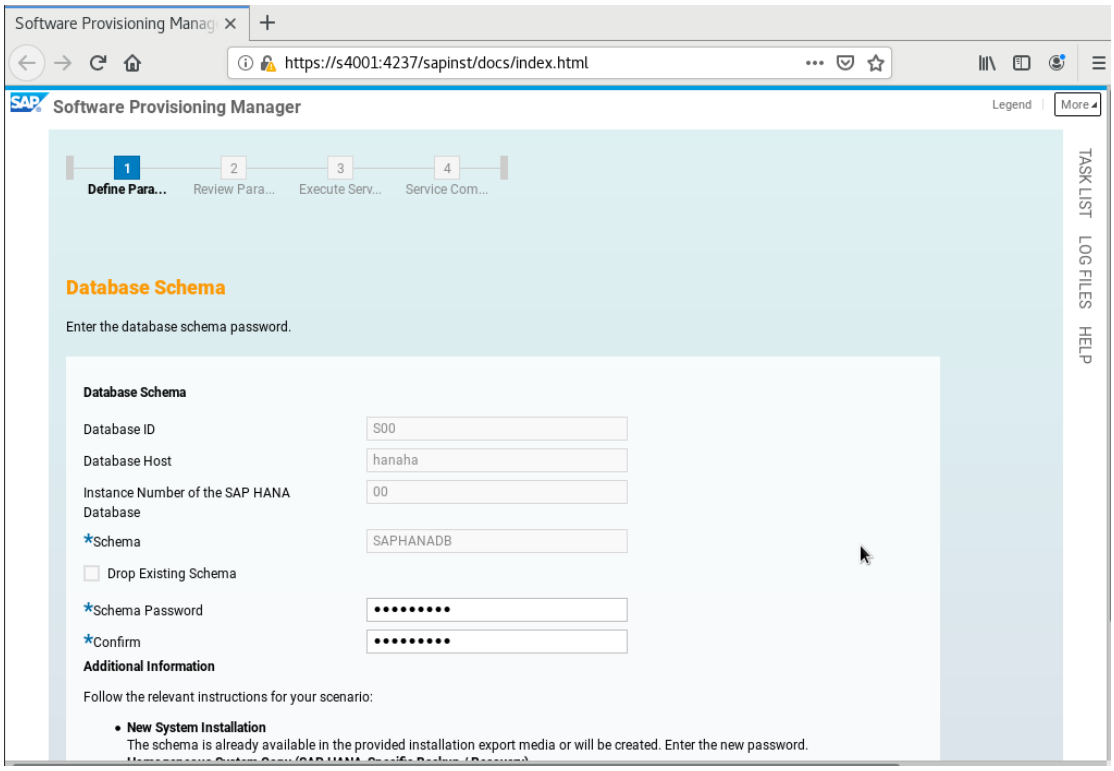


Step 9 Enter the password of the SAP HANA database superuser.

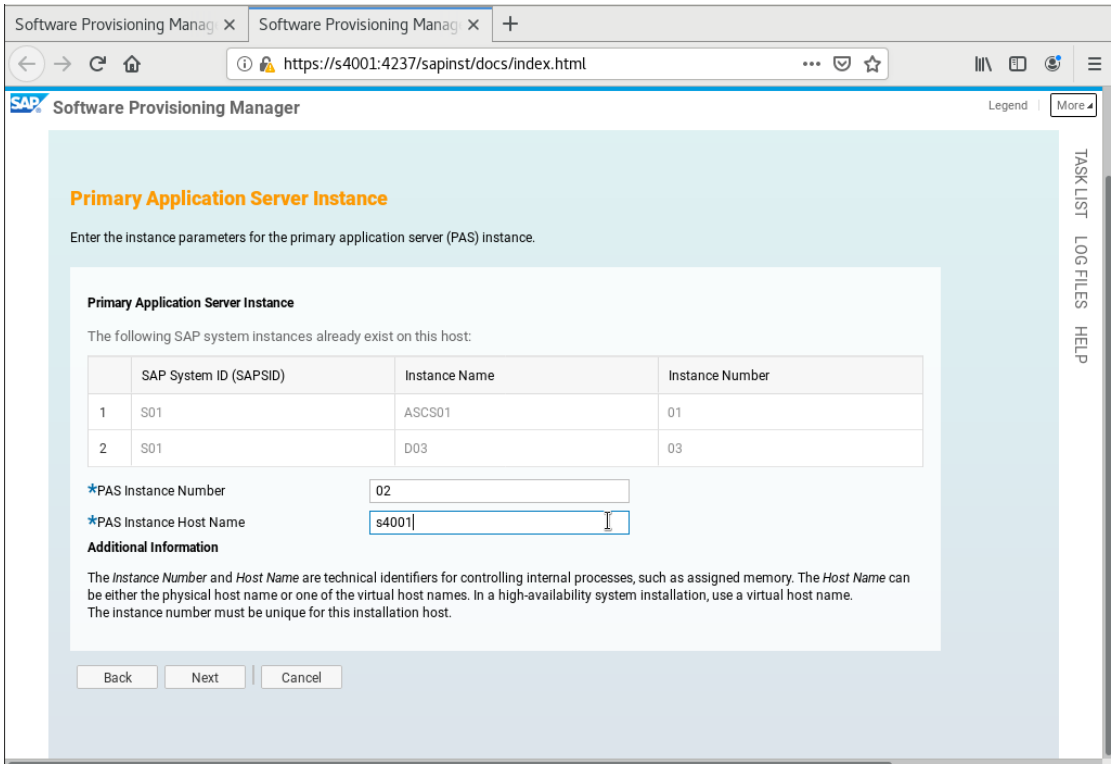


Step 10 Enter the database schema password.

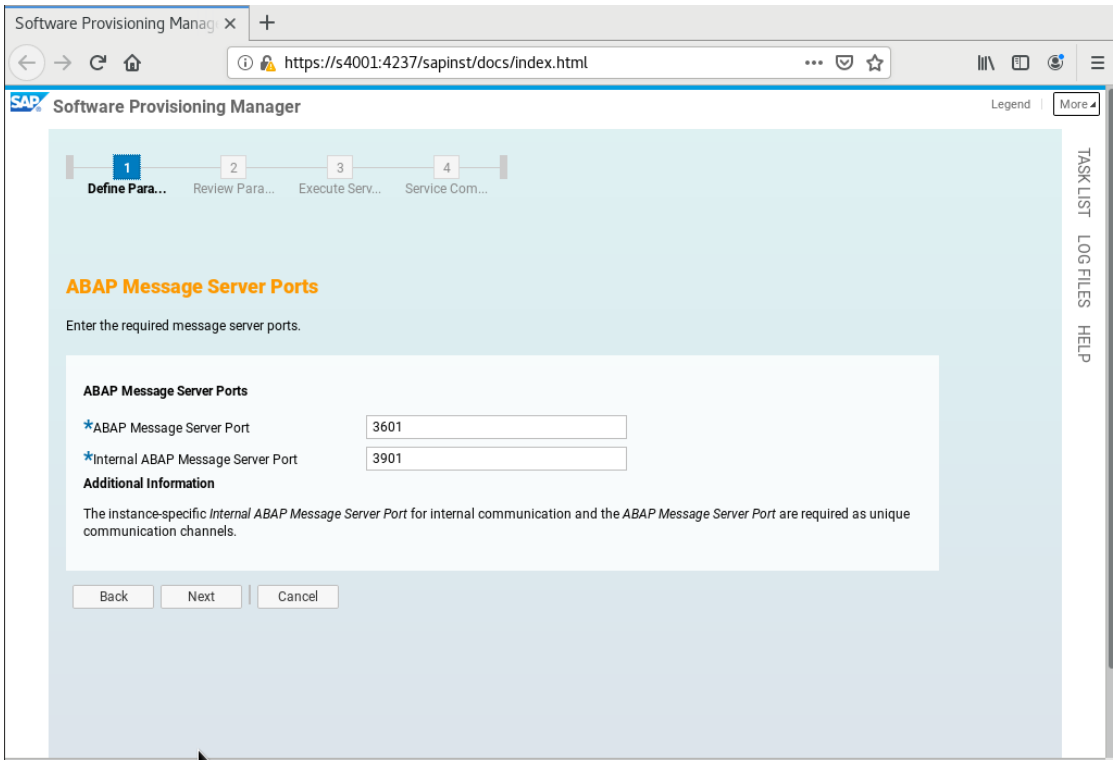




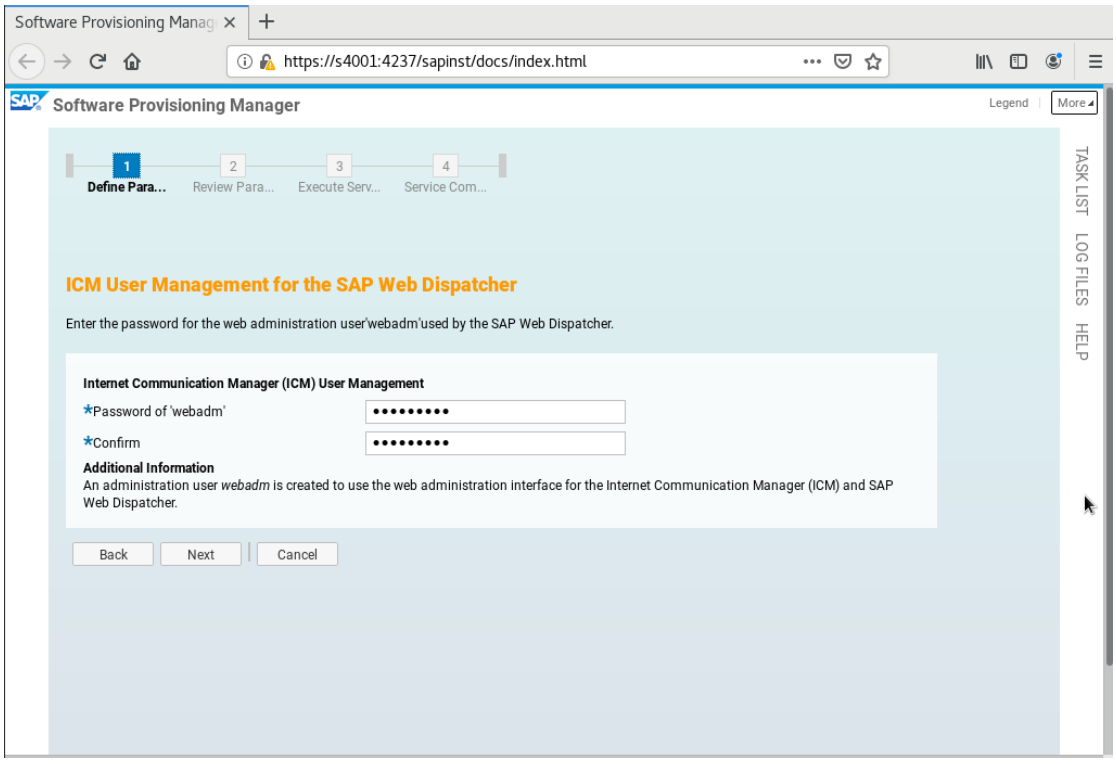
Step 11 Set **PAS Instance Number** and **PAS Instance Host Name** based on the installation planning. Set **PAS Instance Host Name** to the physical hostname of the active node.



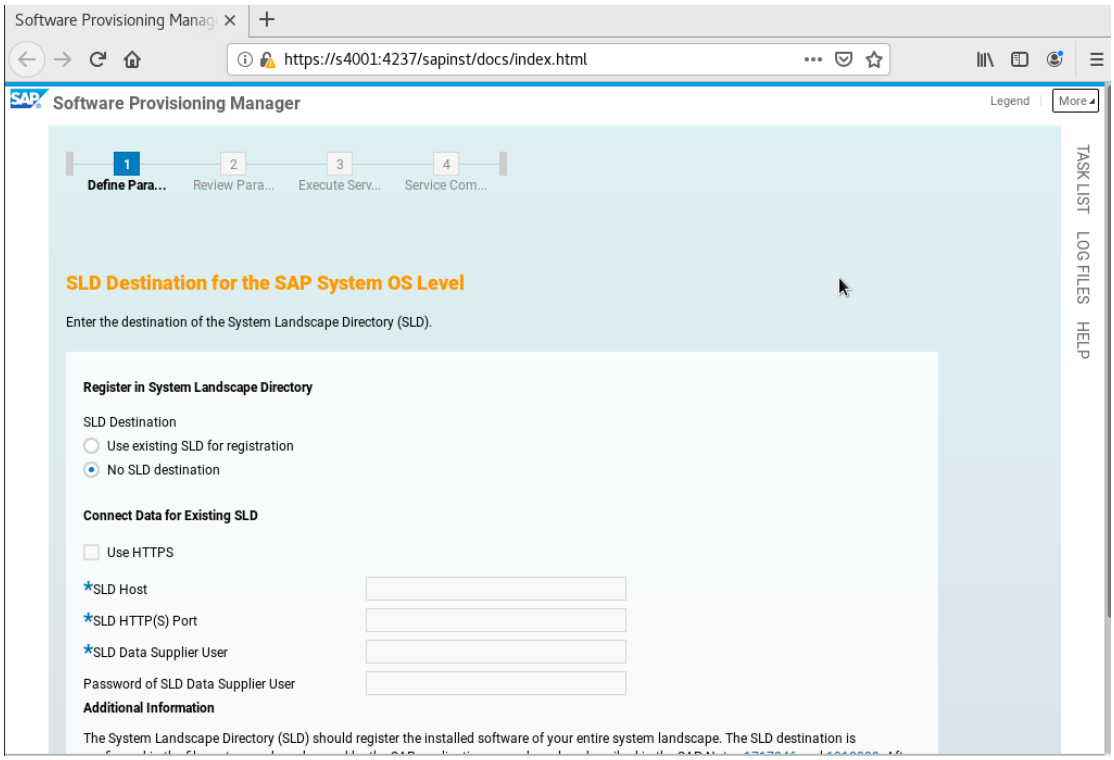
Step 12 Click **Next**.



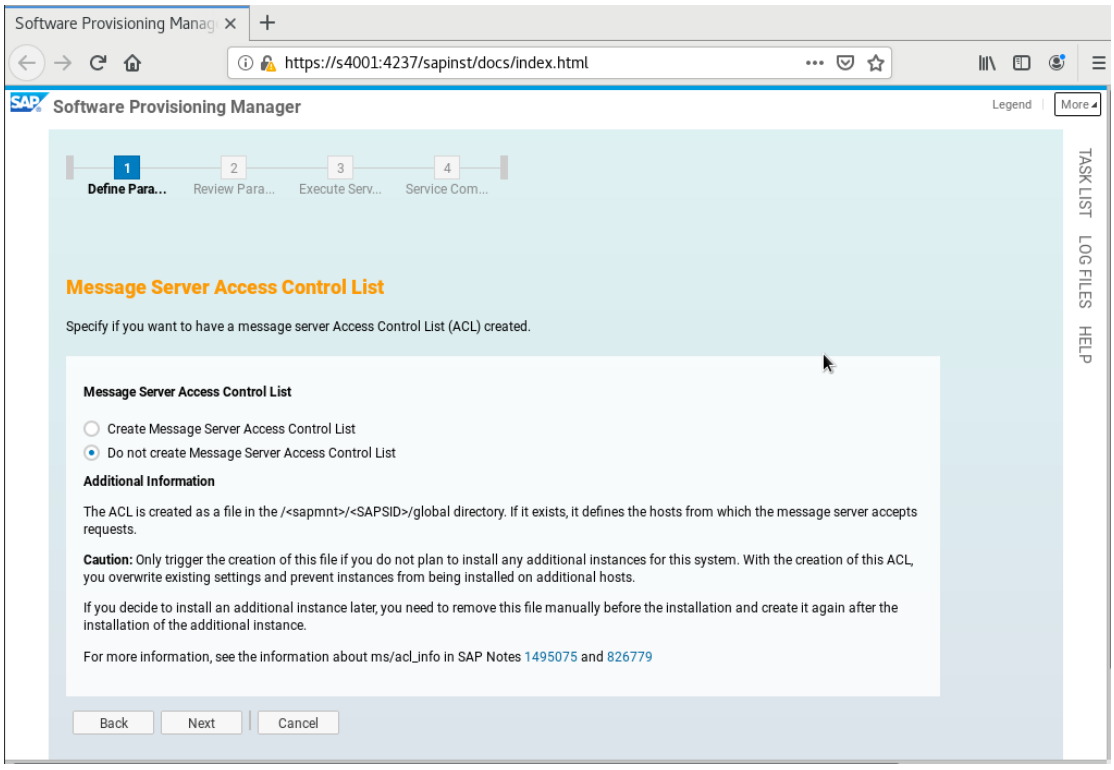
Step 13 Enter the password of the web administrator.



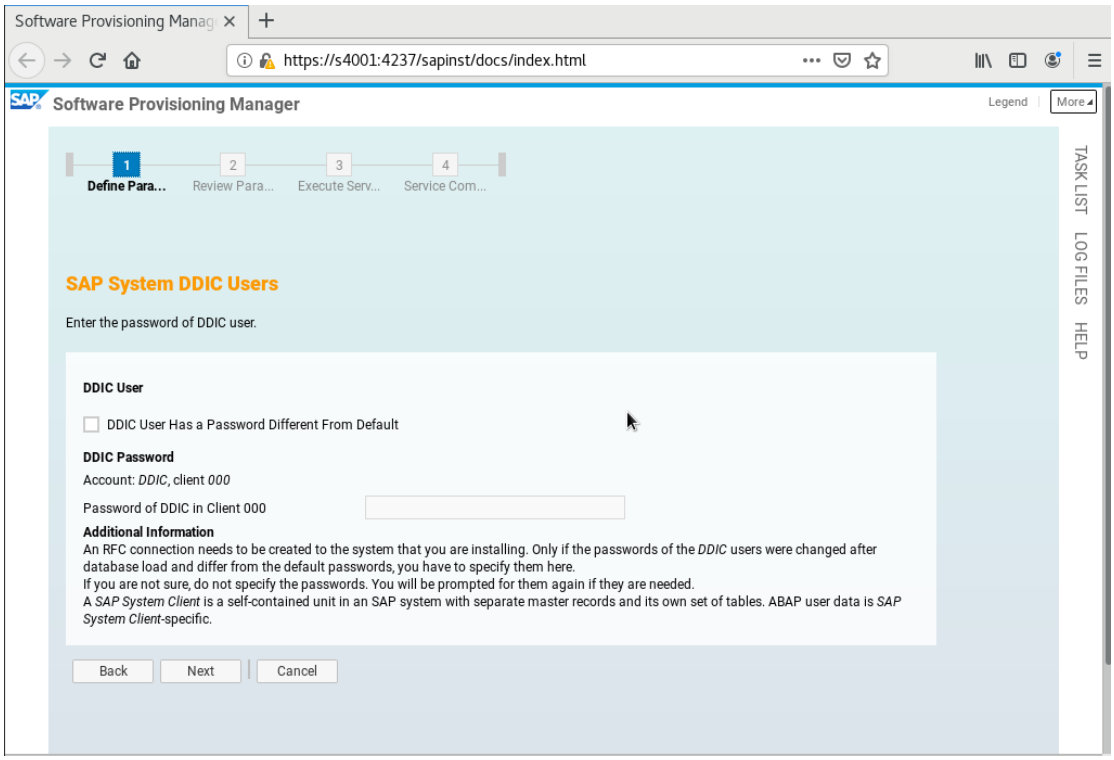
Step 14 Click **Next**.



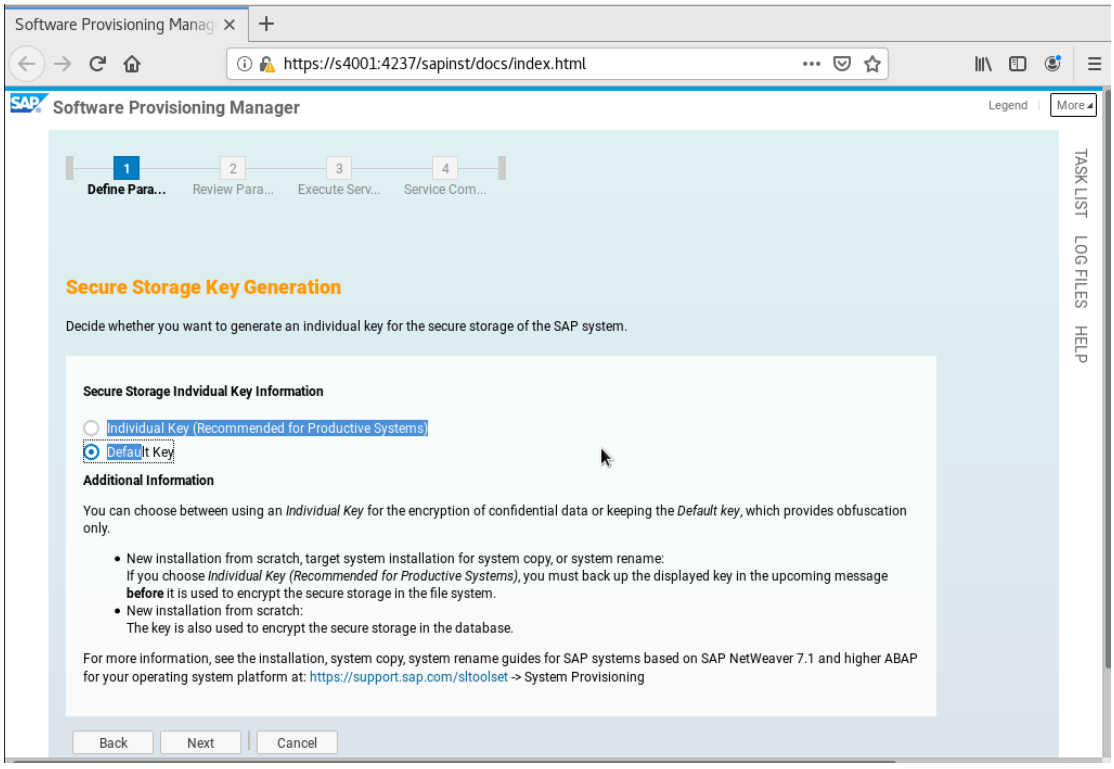
Step 15 Click **Next**.



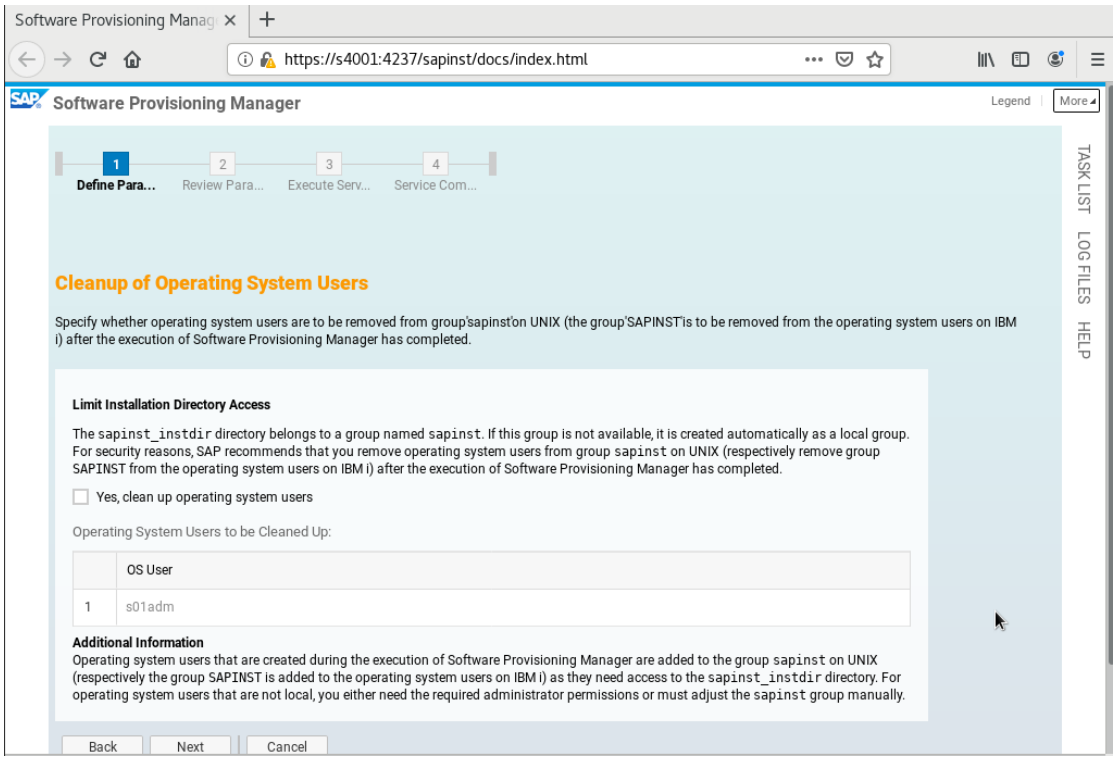
Step 16 Click **Next**.



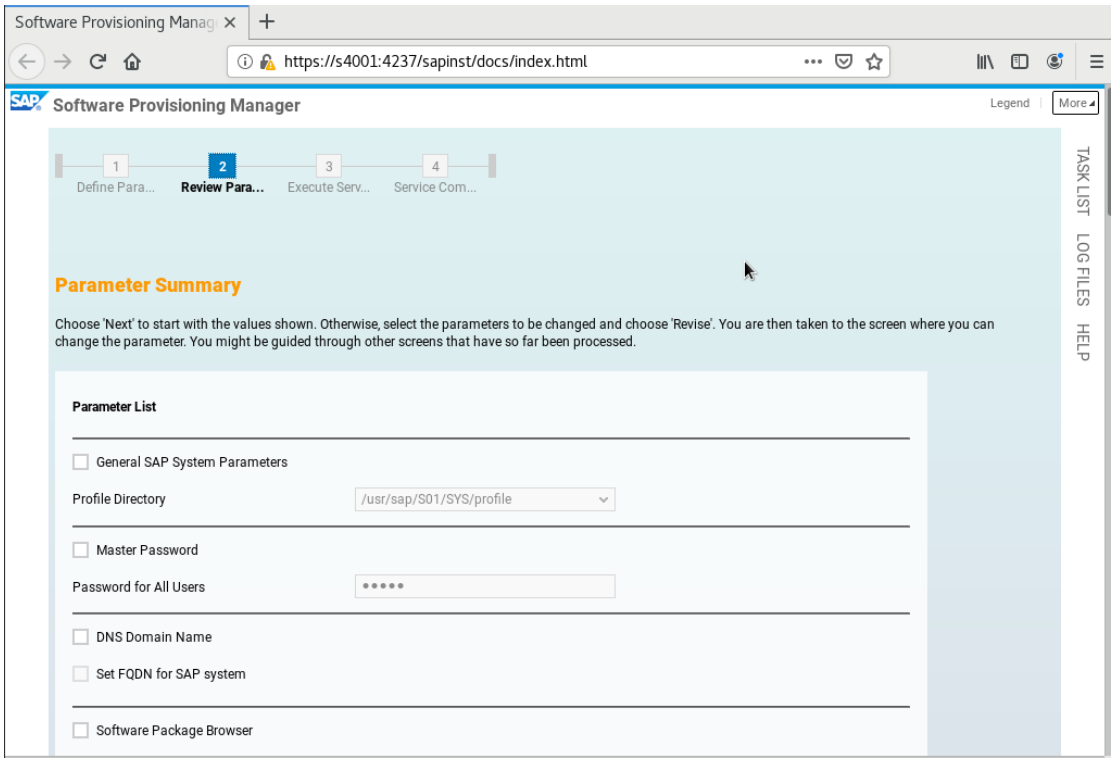
Step 17 Select **Default Key** and click **Next**.



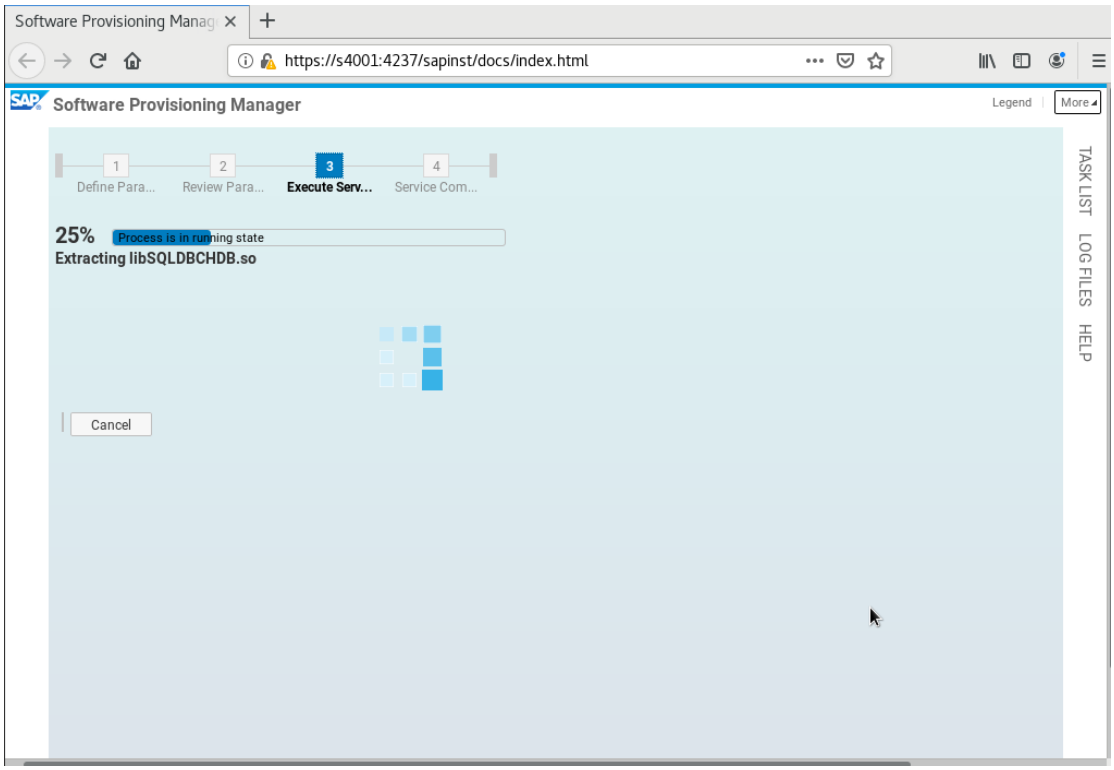
Step 18 Click **Next**.

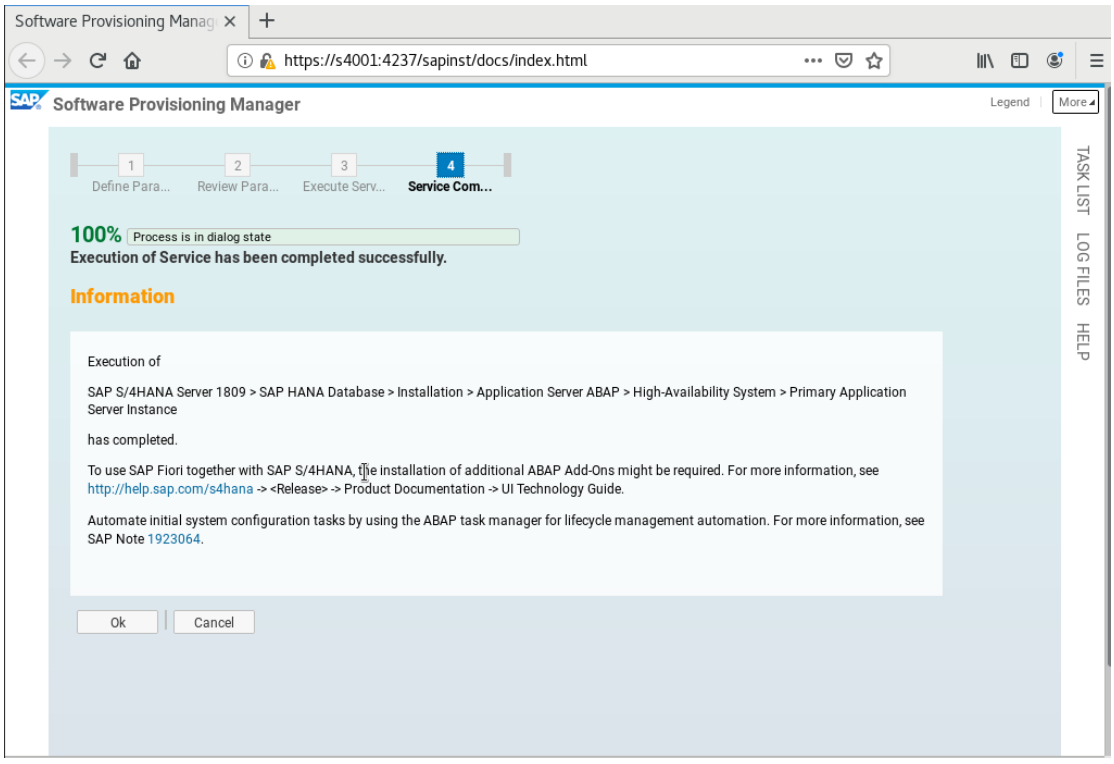


Step 19 Check your parameter settings. If they are all correct, click **Next**.



Step 20 The installation starts.


Software Provisioning Manag
https://s4001:4237/sapinst/docs/index.html
Software Provisioning Manager
Legend
More
1 Define Para...
2 Review Para...
3 Execute Serv...
4 Service Com...
25%
Process is in running state
Extracting libSQLDBCHDB.so
Cancel
TASK LIST
LOG FILES
HELP


Software Provisioning Manag
https://s4001:4237/sapinst/docs/index.html
Software Provisioning Manager
Legend
More
1 Define Para...
2 Review Para...
3 Execute Serv...
4 Service Com...
100%
Process is in dialog state
Execution of Service has been completed successfully.
Information
Execution of
SAP S/4HANA Server 1809 > SAP HANA Database > Installation > Application Server ABAP > High-Availability System > Primary Application Server Instance
has completed.
To use SAP Fiori together with SAP S/4HANA, the installation of additional ABAP Add-Ons might be required. For more information, see http://help.sap.com/s4hana -> <Release> -> Product Documentation -> UI Technology Guide.
Automate initial system configuration tasks by using the ABAP task manager for lifecycle management automation. For more information, see SAP Note 1923064.
Ok
Cancel
TASK LIST
LOG FILES
HELP

----End

4.5.2.7 Installing Additional Application Server (AAS) Instance

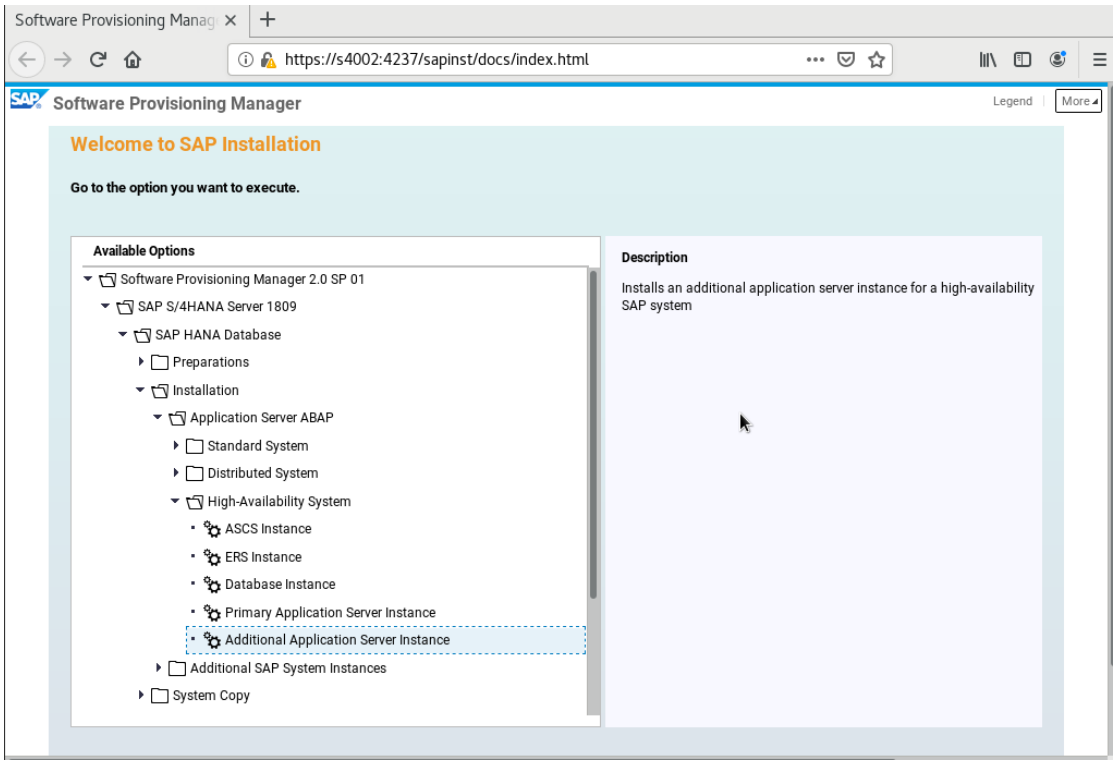
Procedure

Step 1 Go to the directory where the AAS Instance installation package is stored and install it on the standby SAP S/4HANA node.

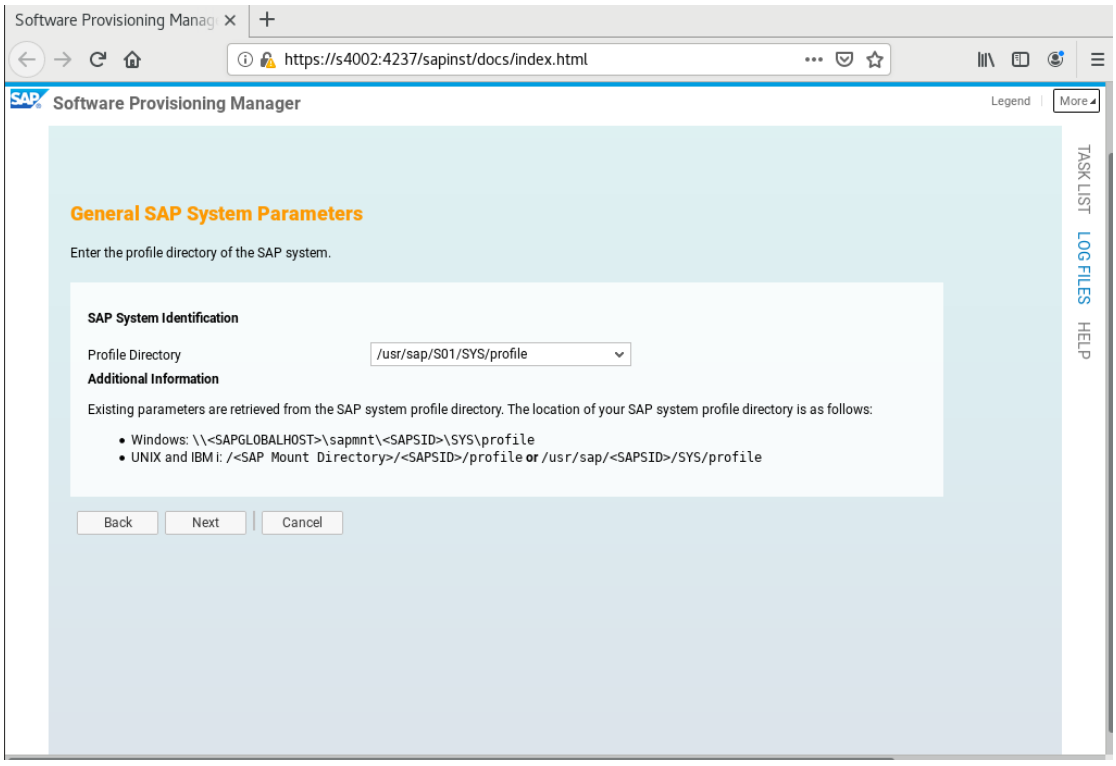
```
s4002:~ # cd /sapcd/SWPM/
s4002:/sapcd/SWPM # ./sapinst
[============================] | extracting...  done!
INFO       2020-07-21 19:13:00.706 (mainThread) [sixxcreate.cpp:347]
********************************************************************************
Initial log directory: /root/.sapinst/s4002/13913
********************************************************************************


SAPinst build information:
--------------------------
Version:          749.0.62
Build:            1875603
Compile time:     Oct 08 2018 - 14:01:31
Make type:        optU
Codeline:         749_REL
Platform:         linuxx86_64
Kernel build:     749, patch 611, changelist 1875937
SAP JRE build:    SAP Java Server VM (build 8.1.044 9.0.4+011, Sep  6 2018 16:58:06 - 81_REL - optU - linux amd64
 - 6 - bas2:309656 (mixed mode))
SAP JCo build:    3.0.18
SL-UI version:    2.6.28
SAP UI5 version: 1.50.4
Exe directory: /tmp/sapinst_exe.13912.1595329978

SAPinst process information:
----------------------------
Pid:         13913
```

```
INFO       2020-07-21 19:13:01.041 (root/sapinst) (startInstallation) [CSiManagerInterfaces.cpp:2348]
Problem with the DNS configuration: could not determine the DNS domain of host s4002

INFO       2020-07-21 19:13:01.043 (root/sapinst) (guiWatchdog) [CSLPCommunicationServer.cpp:349]
Problem with the DNS configuration: could not determine the DNS domain of host s4002

INFO       2020-07-21 19:13:01.855 (root/sapinst) (SLPCommunicator) [SLPMonitoringStatemachine.cpp:1392]
********************************************************************************
Open your browser and paste the following URL address to access the GUI
https://s4002:4237/sapinst/docs/index.html
Logon users: [root]
********************************************************************************

=>sapparam(1c): No Profile used.
=>sapparam: SAPSYSTEMNAME neither in Profile nor in Commandline
load resource pool /sapcd/SWPM/resourcepool.xml
```

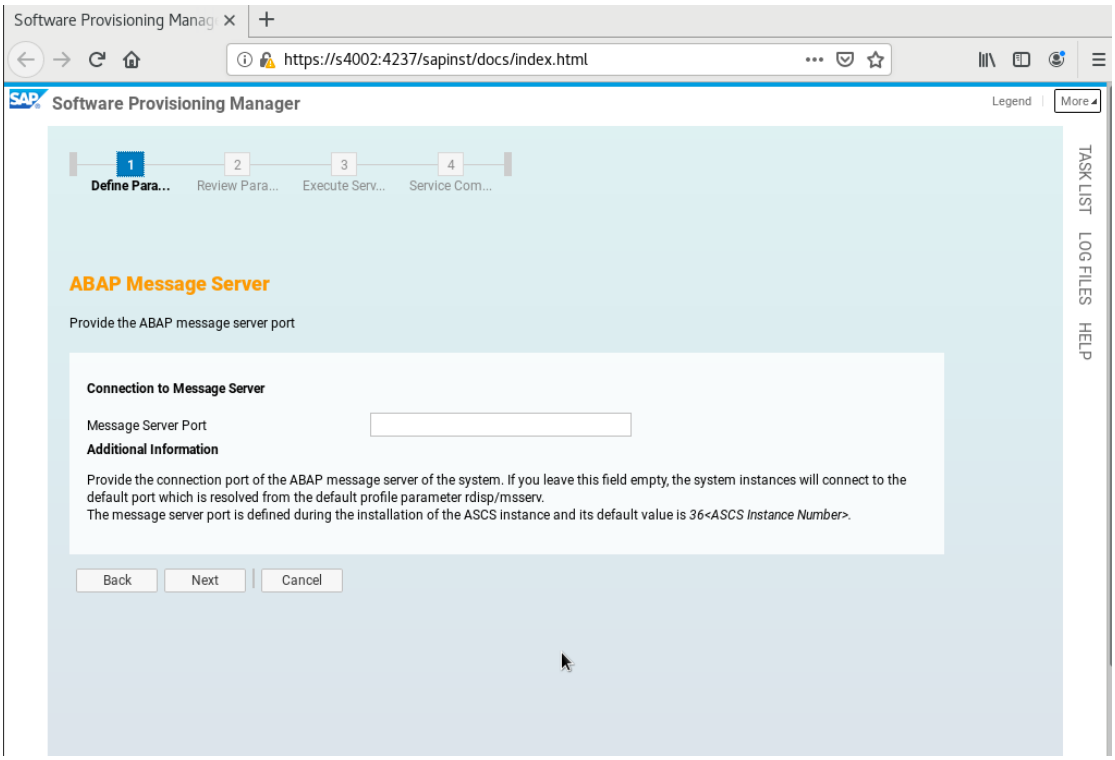
Step 2 Select **Additional Application Server Instance** and click **Next**.



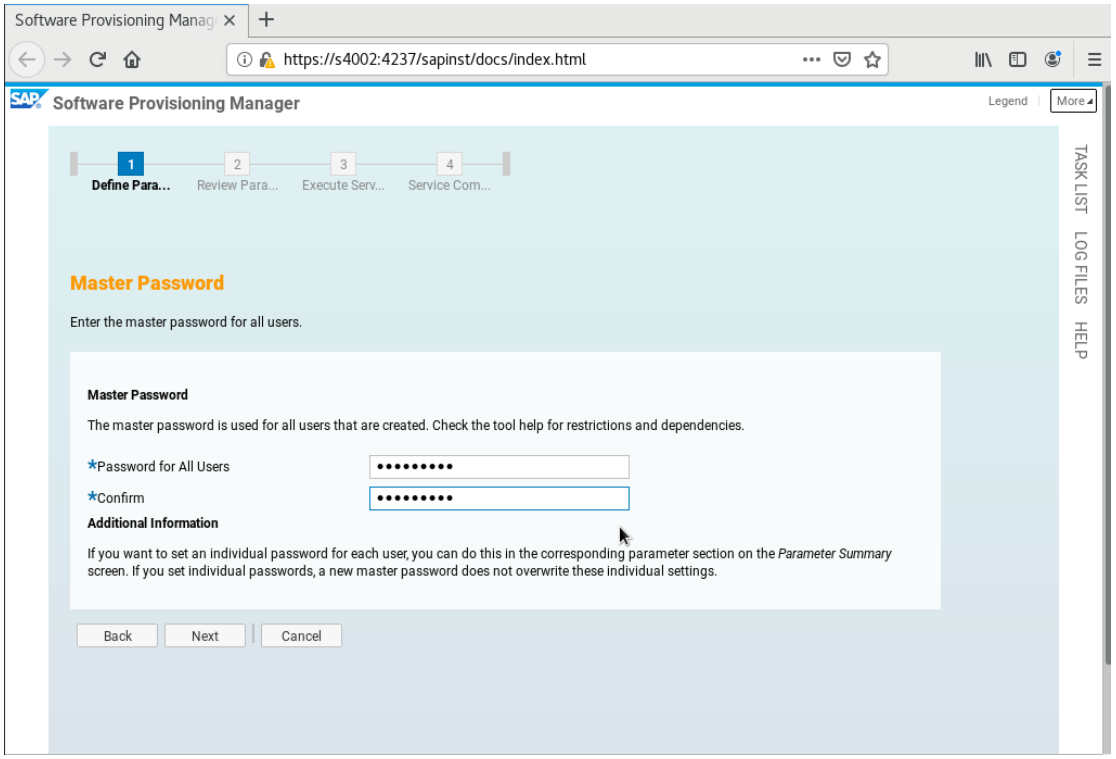
Step 3 Click **Next**.



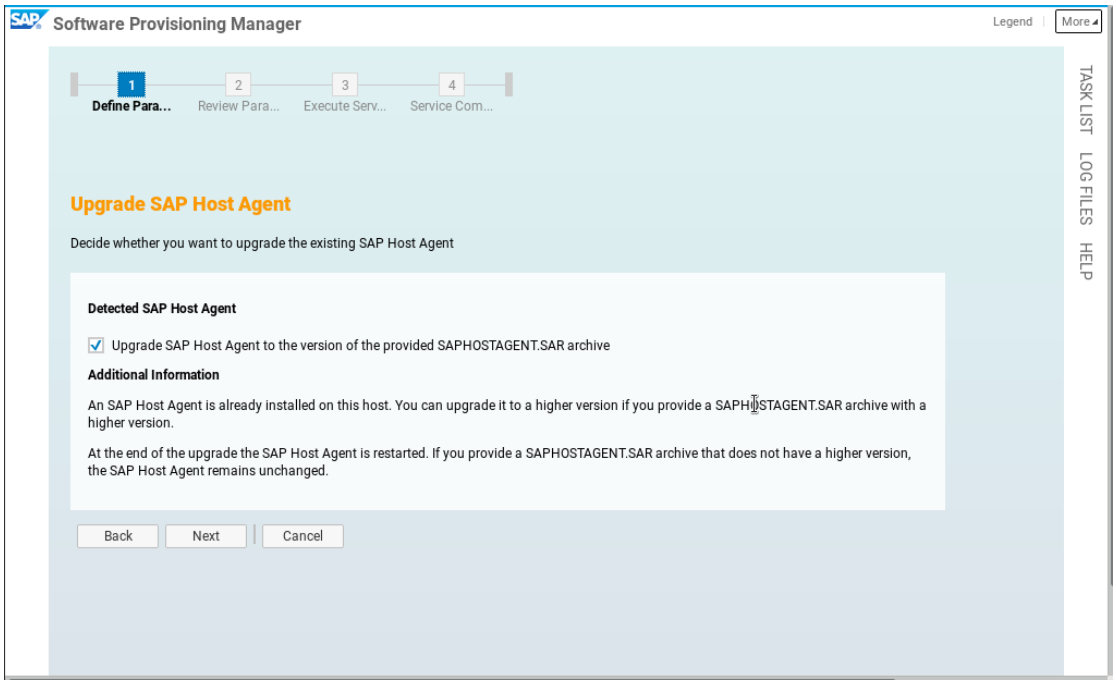
Step 4 Click **Next**.



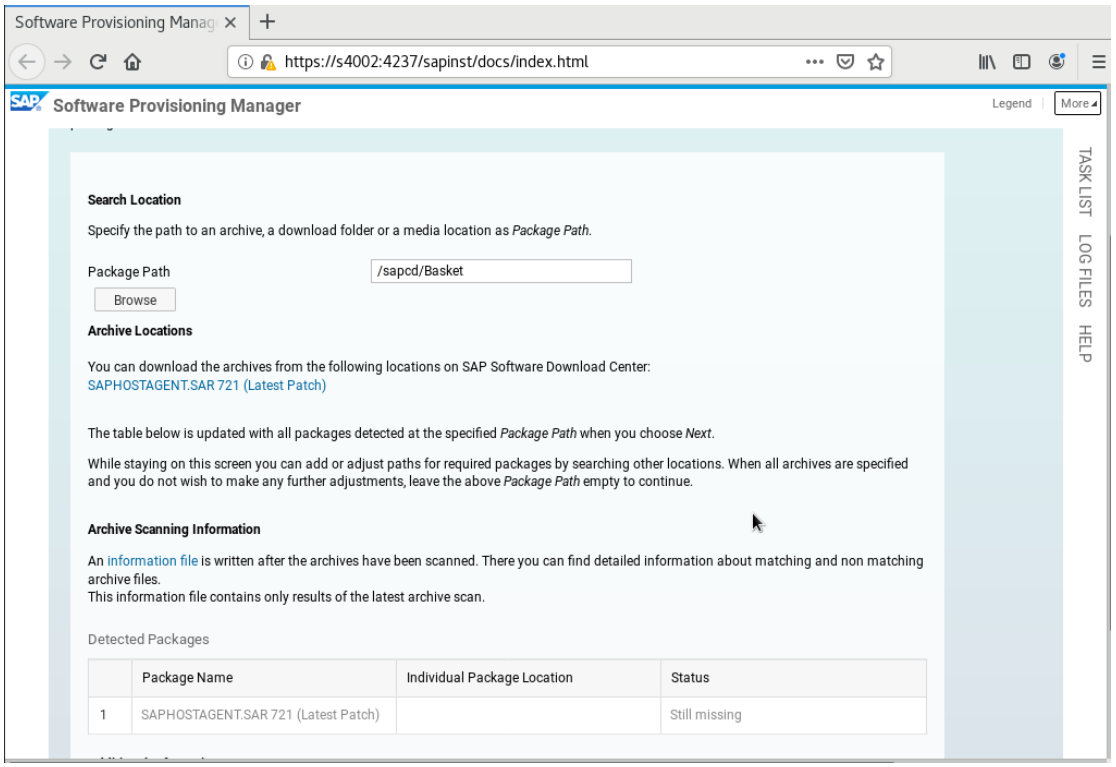
Enter the master password fo all users.



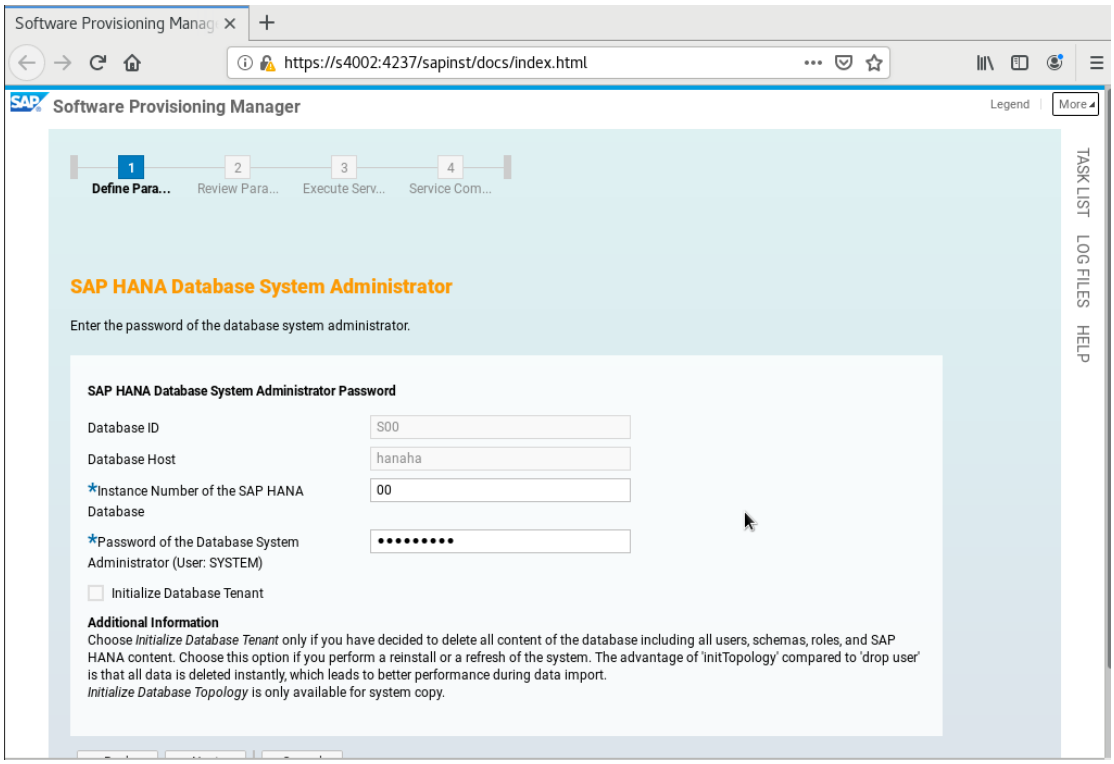
Step 5 Click **Next**.



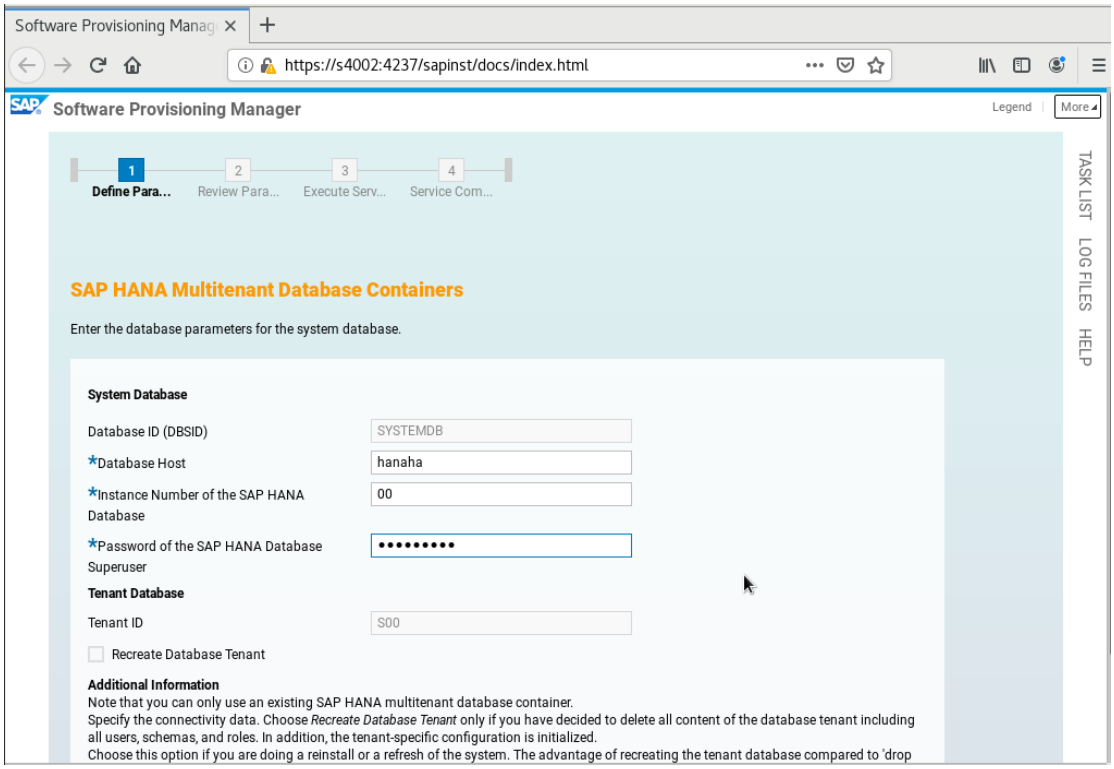
Step 6 Select a package path.



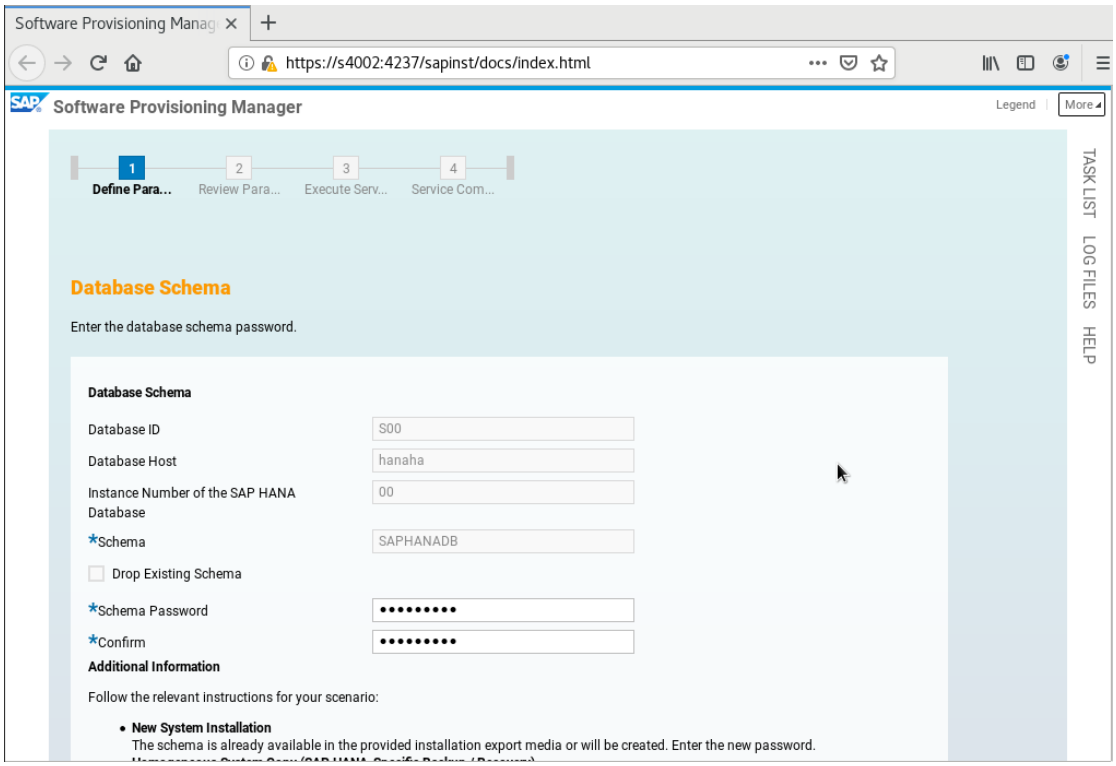
Step 7 Set the instance number and enter the password of the **SYSTEM** user.



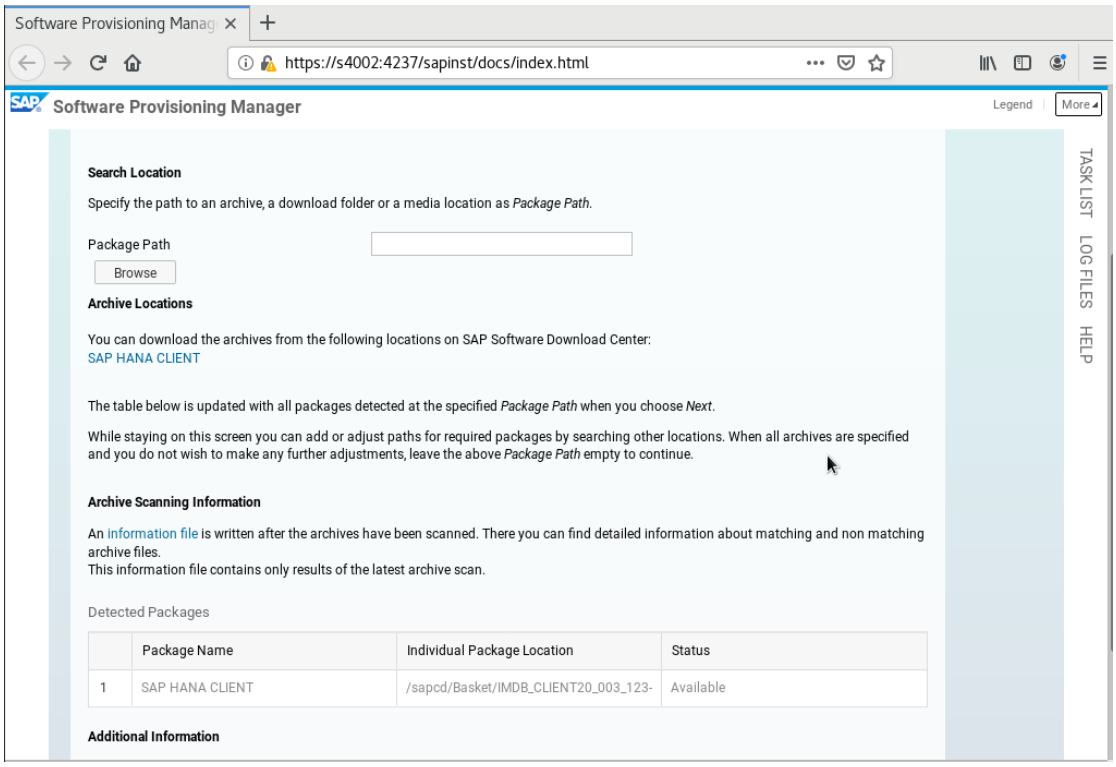
Step 8 Enter the password of SAP HANA database superuser.



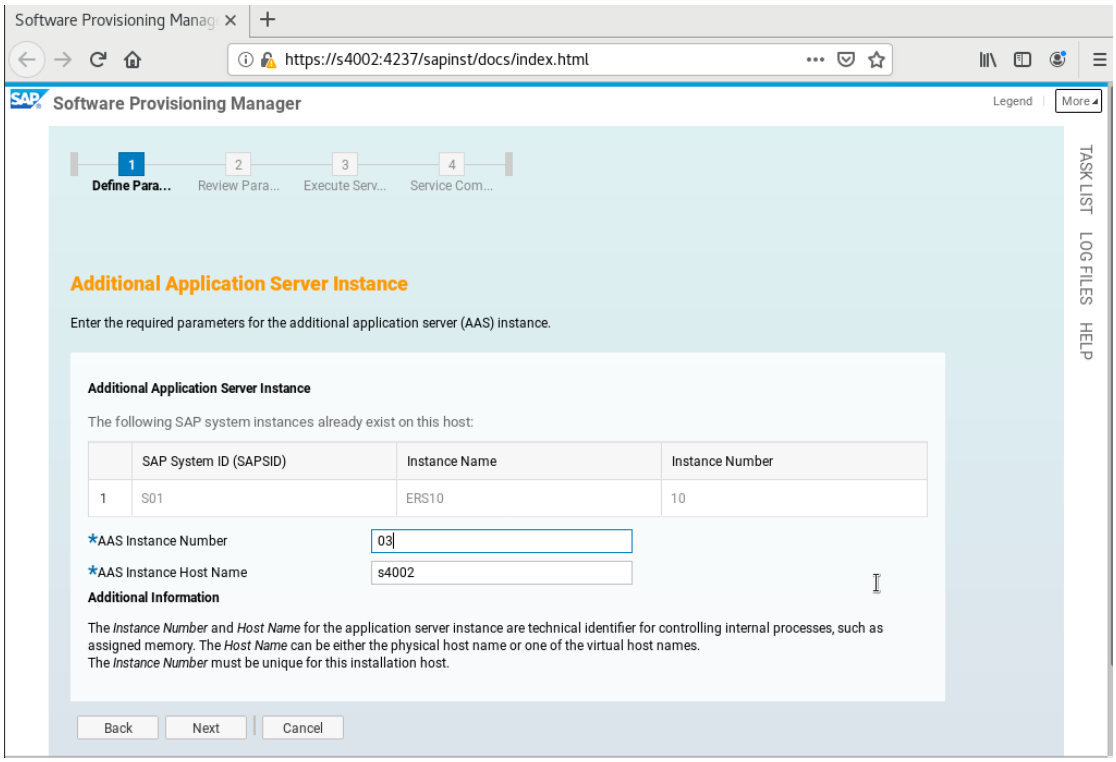
Step 9 Enter the database schema password.



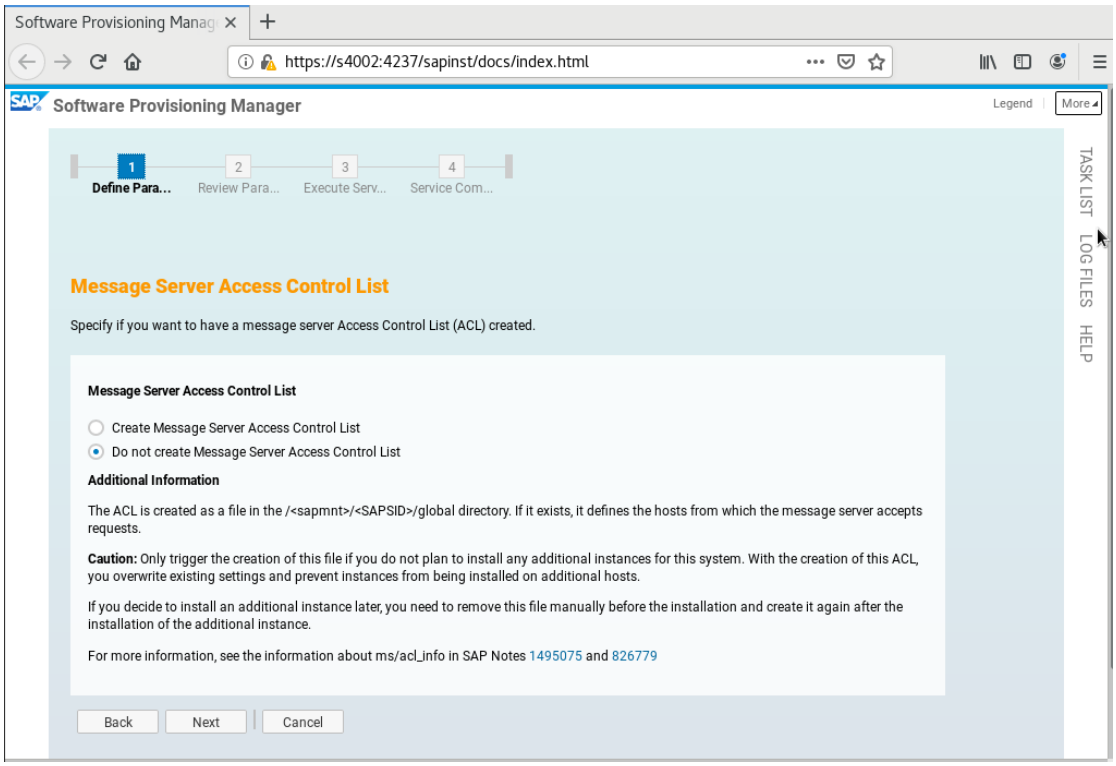
Step 10 Select a package path.



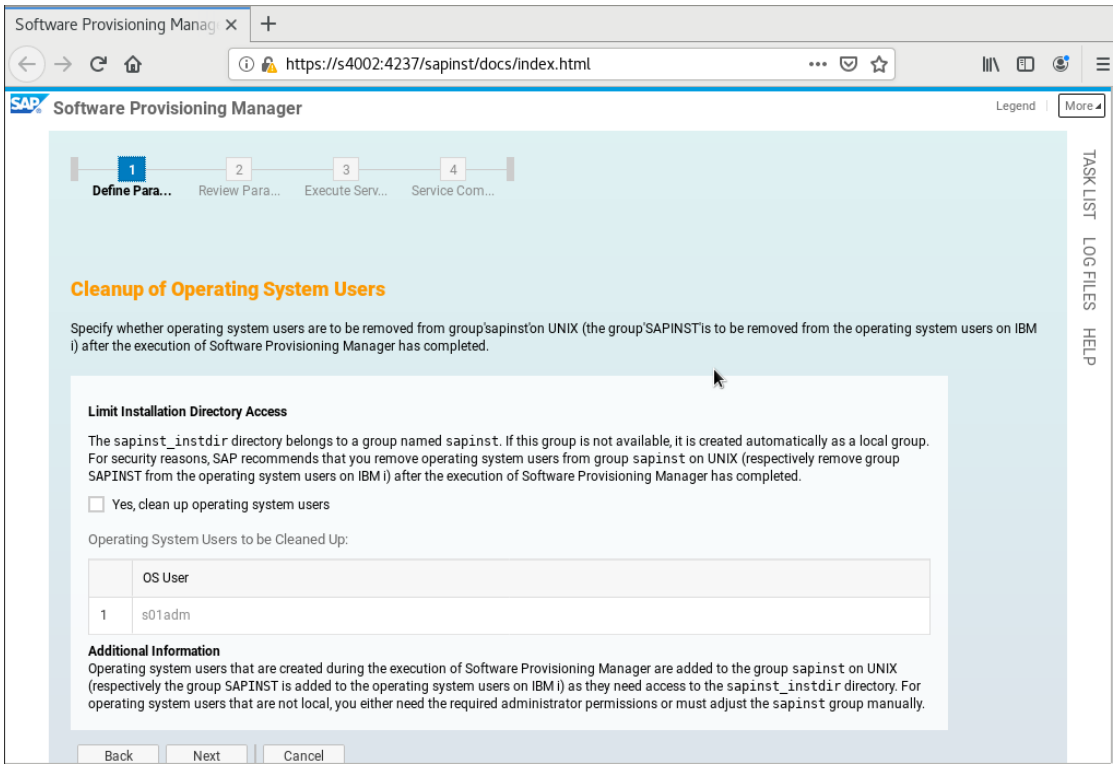
Step 11 Set **AAS Instance Number** and **AAS Instance Host Name** based on the installation planning. Set **AAS Instance Host Name** to the physical hostname of the standby node.



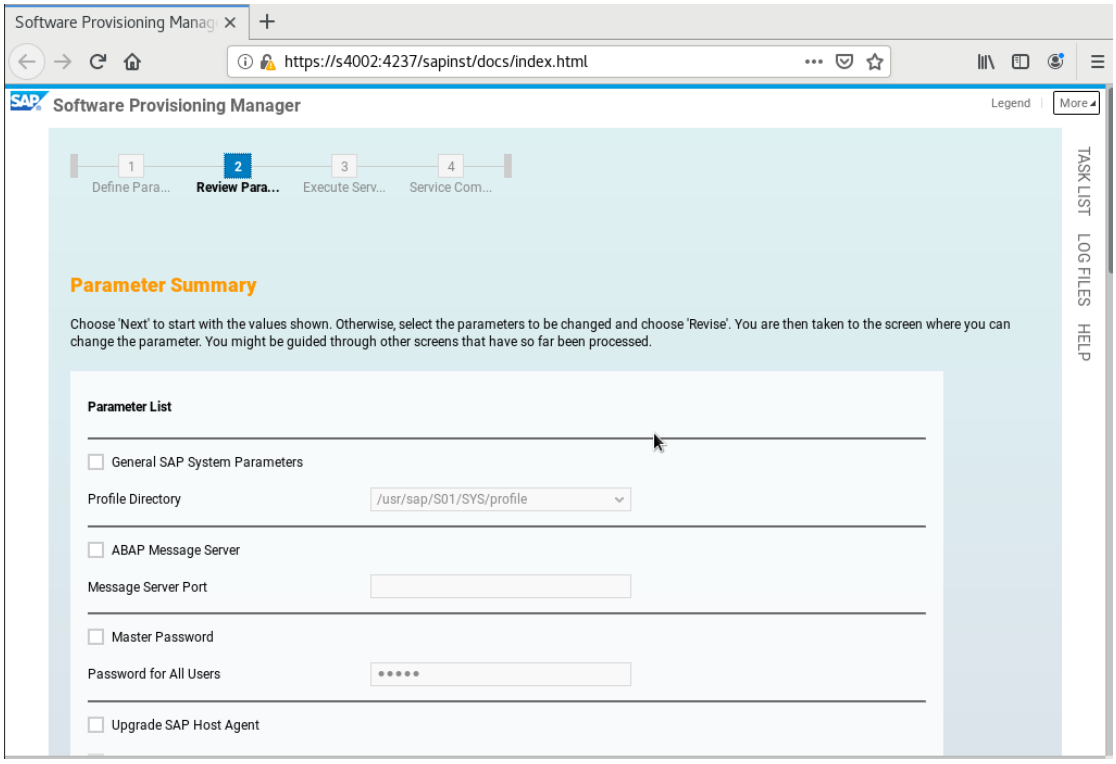
Step 12 Click **Next**.



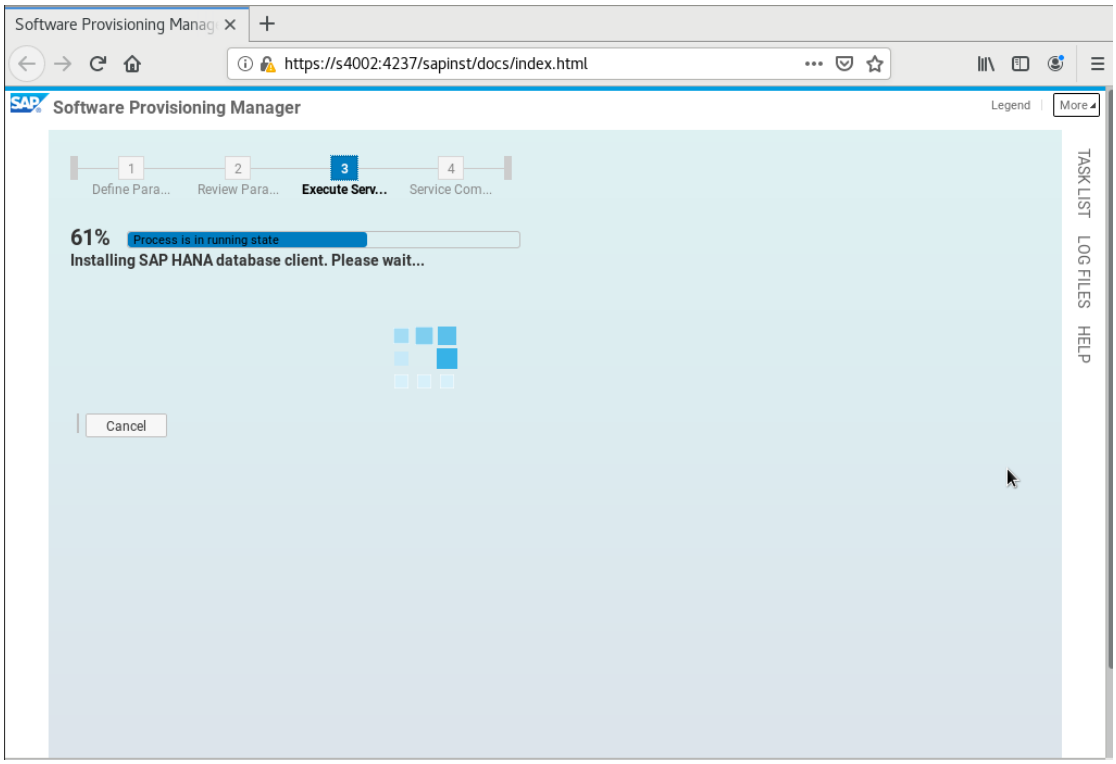
Step 13 Click **Next**.

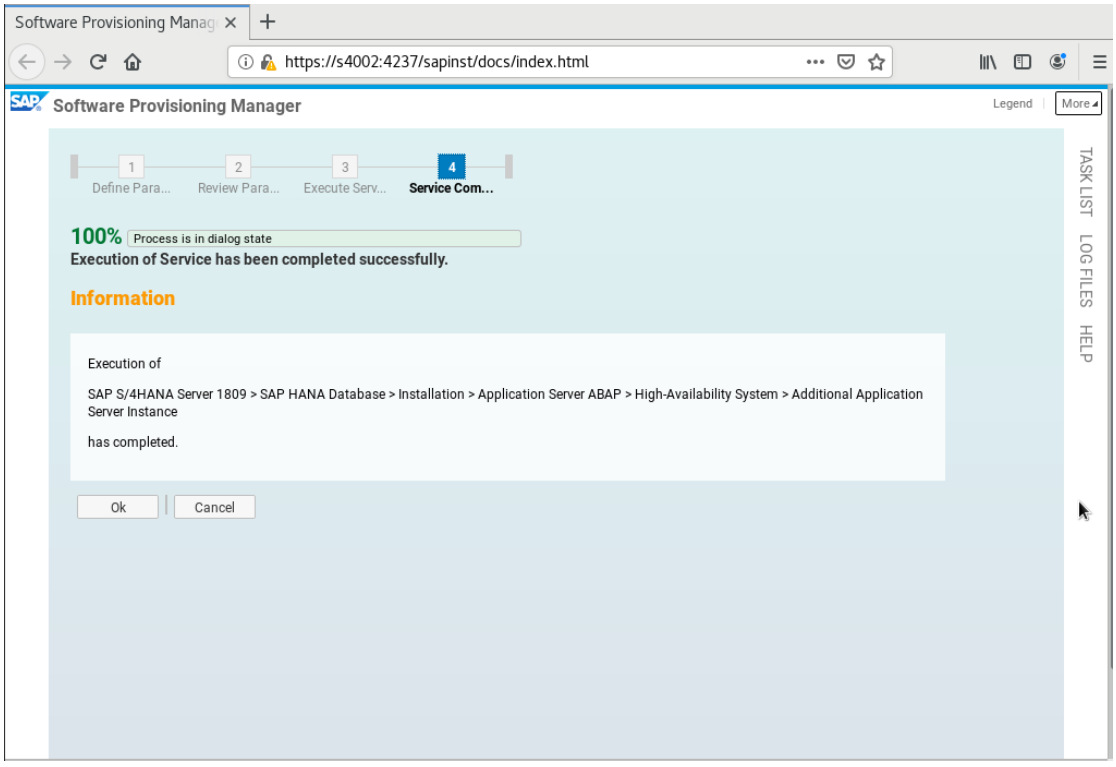


Step 14 Check your parameter settings. If they are all correct, click **Next**.



Step 15 The installation starts.





----End

4.6 High Availability Configuration

4.6.1 SAP HANA HA Configurations

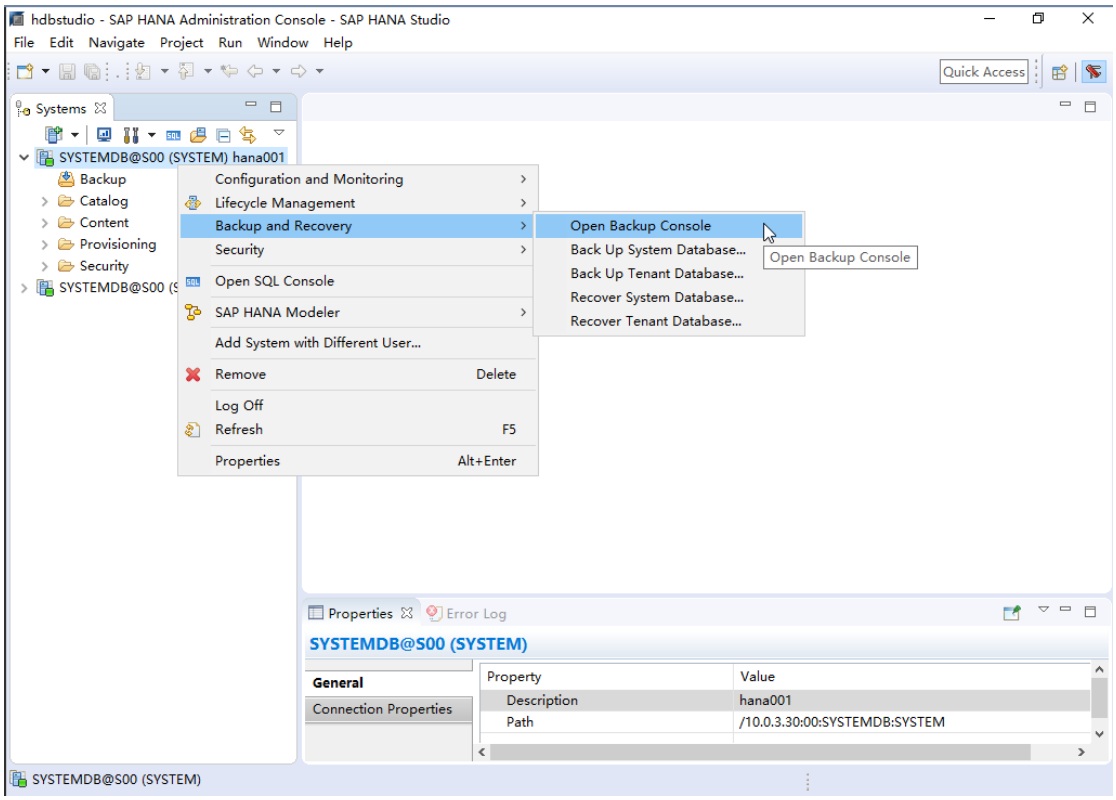
4.6.1.1 Configuring the Backup Path

A path is required for backing up SAP HANA data. This section uses SAP HANA Studio deployed on a Windows ECS as an example to describe how to configure backup settings and perform backup when SAP HANA 2.0 is used.

Procedure

Step 1 Start SAP HANA Studio.

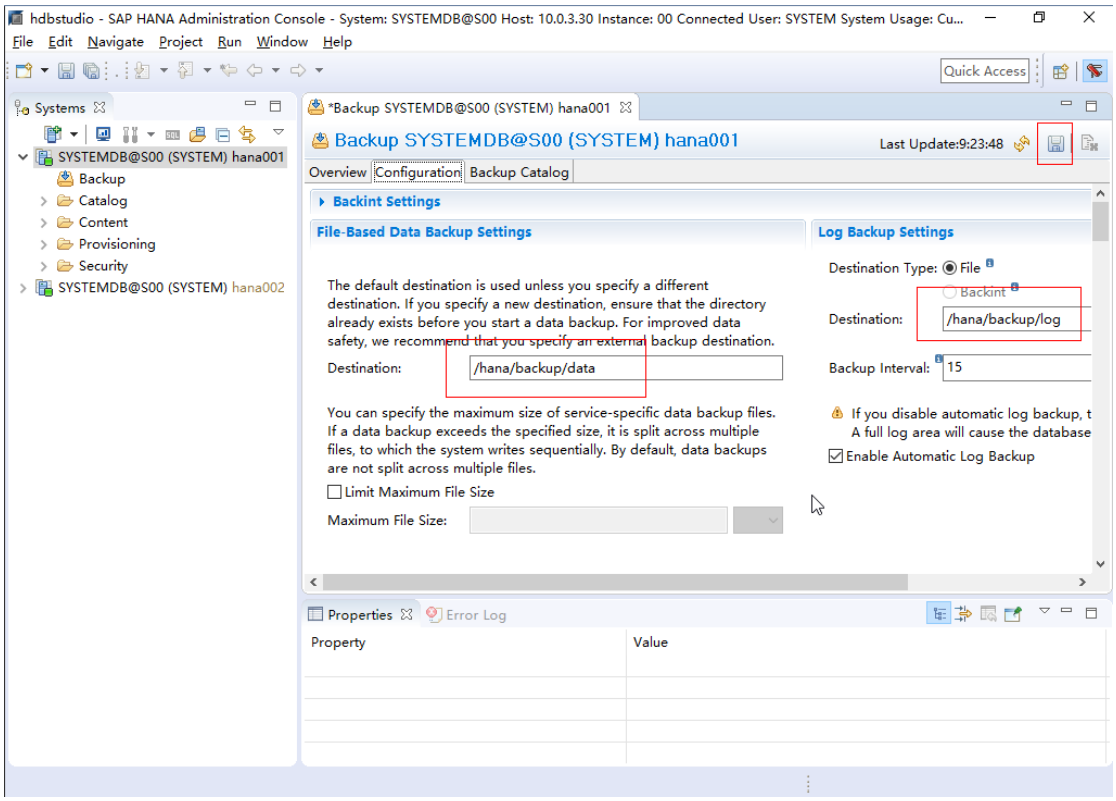
Step 2 In the **System** area on the left, right-click the database node **hana001** and choose **Backup and Recovery** > **Open Backup Console**.



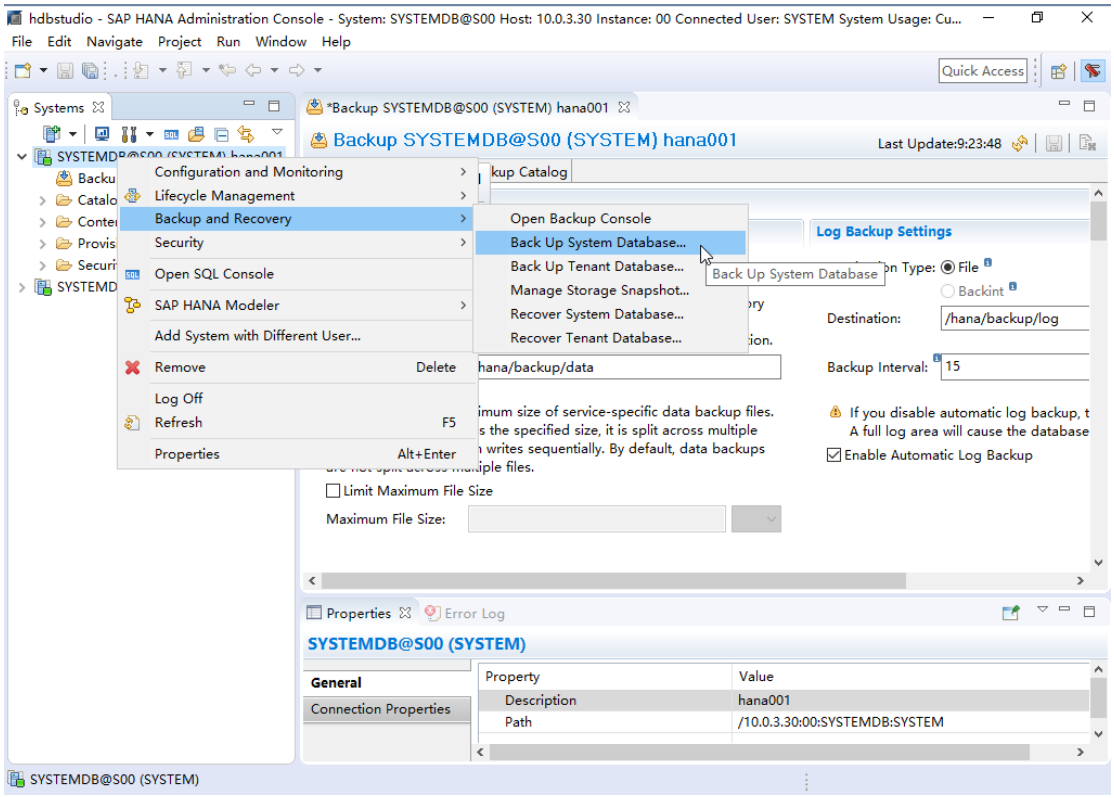
Step 3 Click the **Configuration** tab in the right pane and configure the backup paths.

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

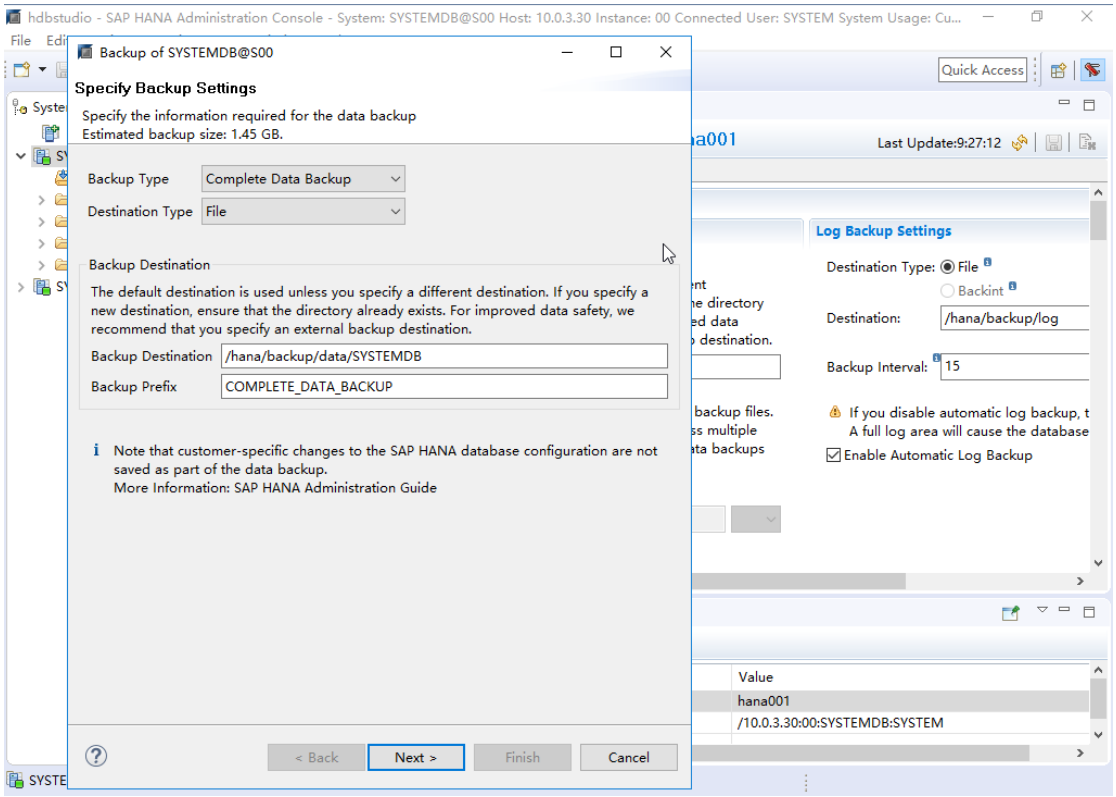
Click the save icon in the upper right corner to save the configuration.



Step 4 In the **System** area on the left, right-click the database node and choose **Backup and Recovery** > **Back Up System Database...** to back up the system database.

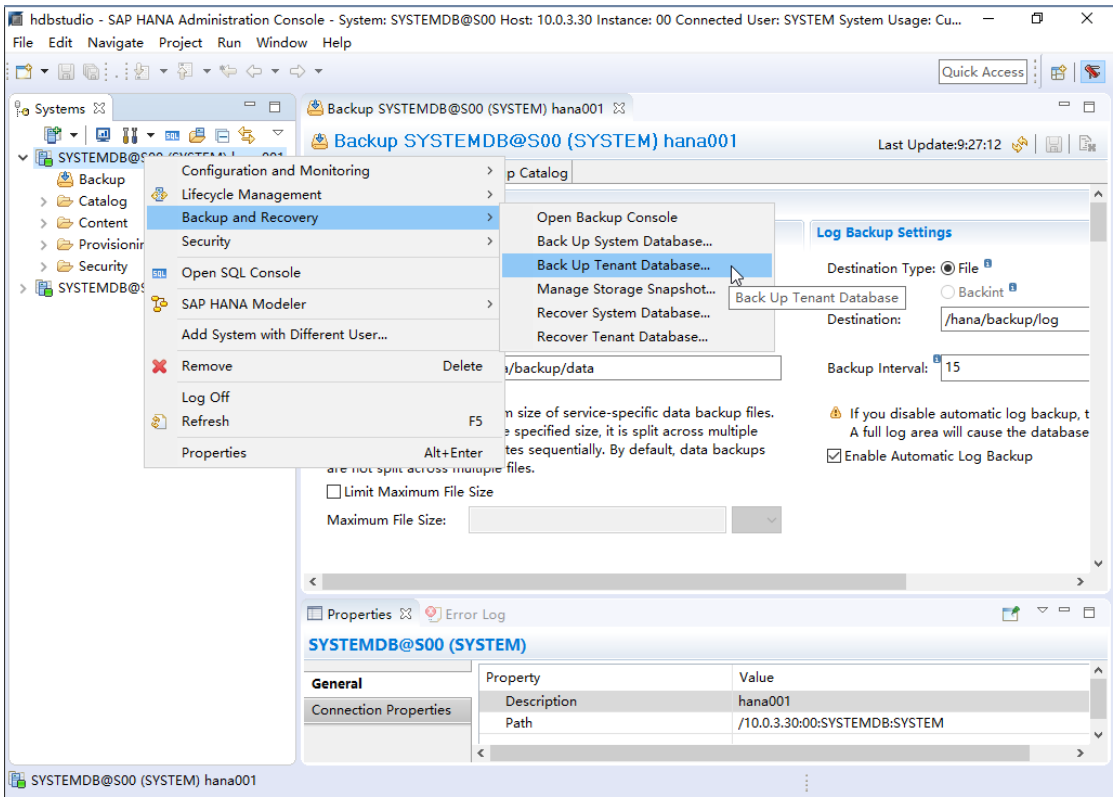


The **Backup Settings** dialog box is displayed.

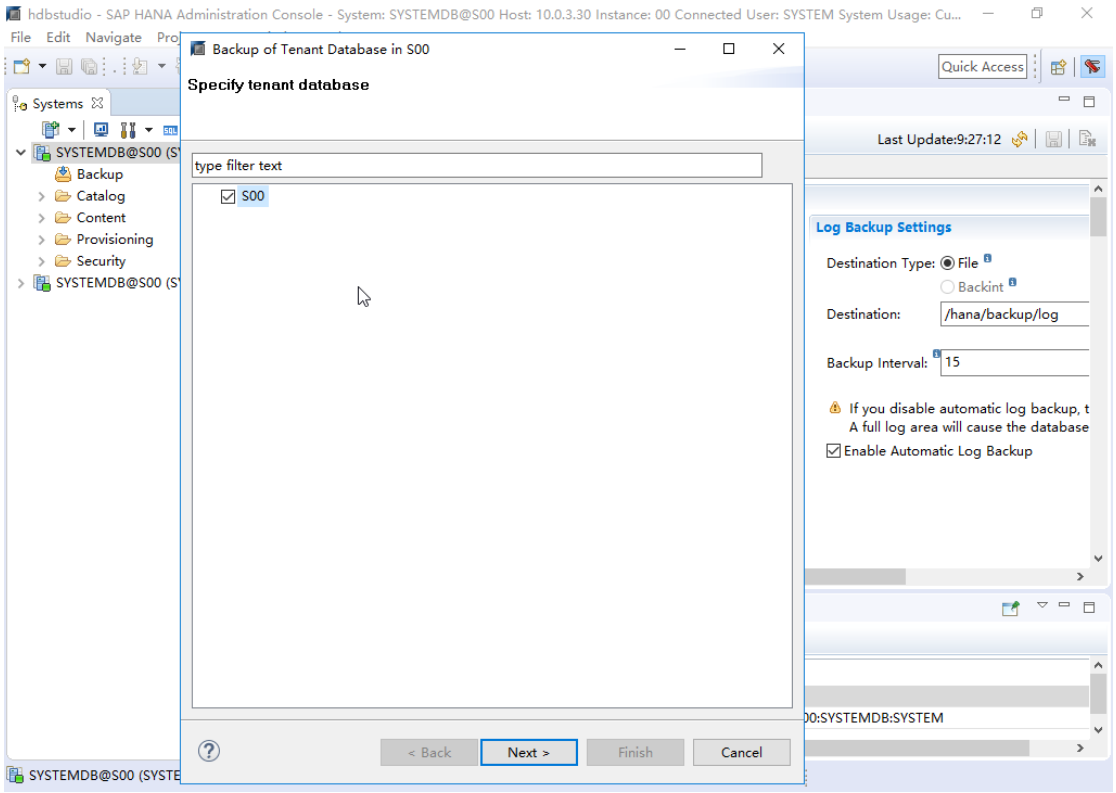


Step 5 Use default settings and click **Next**. The **Review Backup Settings** page is displayed. Confirm configurations and click **Finish**. The system starts the backup task.

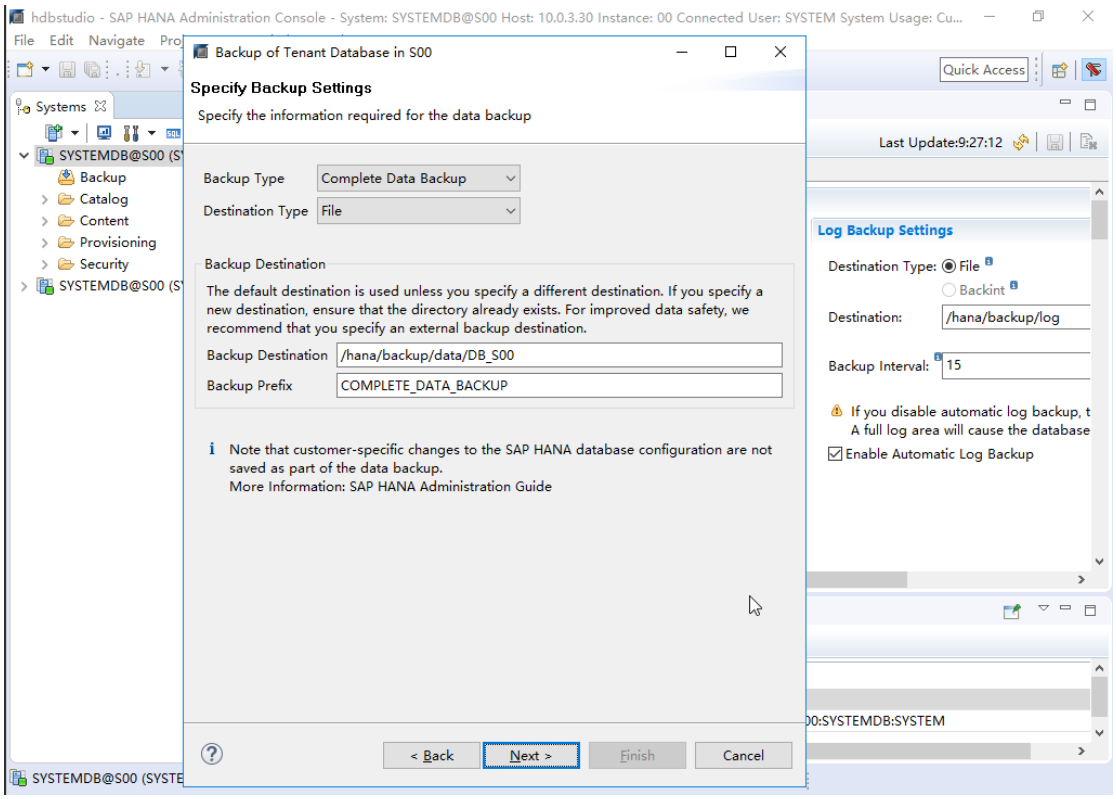
Step 6 In the **System** area on the left, right-click the database node and choose **Backup and Recovery** > **Back Up Tenant Database...** to back up the tenant database.



Step 7 Select the tenant database and click **Next**.



Step 8 Use default settings and click **Next**. The **Review Backup Settings** page is displayed. Confirm configurations and click **Finish**. The system starts the backup task.



Step 9 Repeat the preceding procedure to configure backup settings and perform backup for the database node **hana002**.

----End

4.6.1.2 Configuring the System Replication

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 **Configuring the Backup Path**.
- Before configuring HA, make sure that you have written the mappings between the IP addresses and names of the two SAP HANA ECSs to the **/etc/hosts** files of the two ECSs in **Configuring the Mappings Between IP Addresses and Hostnames**.

Procedure

Step 1 Configure the System Replication for the active SAP HANA node.

1. Log in to the active SAP HANA ECS **hana001**.
2. Run the following command to set the node as the active node:

   hdbnsutil -sr_enable --name=siteA

   In the preceding command, *siteA* indicates the node name, which can be customized.

   Example: **hdbnsutil -sr_enable --name=hana001**


```
hana001:~ # su - s00adm
s00adm@hana001:/usr/sap/S00/HDB00> hdbnsutil -sr_enable --name=hana001
nameserver is active, proceeding ...
successfully enabled system as system replication source site
done.
s00adm@hana001:/usr/sap/S00/HDB00>
```

Step 2 Copy the files on the active node to the standby node.

1. Log in to the active SAP HANA ECS **hana001**.
2. Run the following commands to copy the **/usr/sap/S00/SYS/global/security/rsecssfs/data/SSFS_S00.DAT** and **/usr/sap/S00/SYS/global/security/rsecssfs/key/SSFS_S00.KEY** files from the active node to the standby node. Ensure that the user group and user to which the copied file belongs are the same as those of the original file. If they are not consistent, make a manual adjustment.

   scp hana001:**/usr/sap/S00/SYS/global/security/rsecssfs/data/SSFS_S00.DAT**

   scp hana001:**/usr/sap/S00/SYS/global/security/rsecssfs/key/SSFS_S00.KEY**

```
hana002:~ # scp hana001:/usr/sap/S00/SYS/global/security/rsecssfs/data/SSFS_S00.DAT /usr/sap/S00/SYS/global/secu
rity/rsecssfs/data/SSFS_S00.DAT
SSFS_S00.DAT                                                                  100% 2960     9.8MB/s   00:00
hana002:~ # scp hana001:/usr/sap/S00/SYS/global/security/rsecssfs/key/SSFS_S00.KEY /usr/sap/S00/SYS/global/secur
ity/rsecssfs/key/SSFS_S00.KEY
SSFS_S00.KEY                                                                  100%  187   719.0KB/s   00:00
hana002:~ # ll /usr/sap/S00/SYS/global/security/rsecssfs/data/SSFS_S00.DAT
-rw-r--r-- 1 s00adm sapsys 2960 Jul 22 09:49 /usr/sap/S00/SYS/global/security/rsecssfs/data/SSFS_S00.DAT
hana002:~ # ll /usr/sap/S00/SYS/global/security/rsecssfs/key/SSFS_S00.KEY
-rw-r----- 1 s00adm sapsys 187 Jul 22 09:49 /usr/sap/S00/SYS/global/security/rsecssfs/key/SSFS_S00.KEY
```

```
hana001:~ #
hana001:~ # ll /usr/sap/S00/SYS/global/security/rsecssfs/data/SSFS_S00.DAT
-rw-r--r-- 1 s00adm sapsys 2960 Jul 21 10:06 /usr/sap/S00/SYS/global/security/rsecssfs/data/SSFS_S00.DAT
hana001:~ # ll /usr/sap/S00/SYS/global/security/rsecssfs/key/SSFS_S00.KEY
-rw-r----- 1 s00adm sapsys 187 Jul 21 10:05 /usr/sap/S00/SYS/global/security/rsecssfs/key/SSFS_S00.KEY
hana001:~ #
```

Step 3 Configure the System Replication for the standby HANA node.

1. Run the following command to enter the administrator mode:

   su – s00adm

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

   HDB stop

3. Run the following command to enable System Replication:

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

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


```
hana002:~ # su - s00adm
s00adm@hana002:/usr/sap/S00/HDB00> HDB stop
hdbdaemon will wait maximal 300 seconds for NewDB services finishing.
Stopping instance using: /usr/sap/S00/SYS/exe/hdb/sapcontrol -prot NI_HTTP -nr 00 -function Stop 400

22.07.2020 09:55:09
Stop
OK
Waiting for stopped instance using: /usr/sap/S00/SYS/exe/hdb/sapcontrol -prot NI_HTTP -nr 00 -function WaitforSt
opped 600 2


22.07.2020 09:55:41
WaitforStopped
OK
hdbdaemon is stopped.
s00adm@hana002:/usr/sap/S00/HDB00> hdbnsutil -sr_register --remoteHost=hana001 --remoteInstance=00 --replication
Mode=sync --name=hana002
adding site ...
--operationMode not set; using default from global.ini/[system_replication]/operation_mode: logreplay
nameserver hana002:30001 not responding.
collecting information ...
updating local ini files ...
done.
s00adm@hana002:/usr/sap/S00/HDB00>
```

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

   HDB start

```
s00adm@hana002:/usr/sap/S00/HDB00> HDB start


StartService
Impromptu CCC initialization by 'rscpCInit'.
  See SAP note 1266393.
OK
OK
Starting instance using: /usr/sap/S00/SYS/exe/hdb/sapcontrol -prot NI_HTTP -nr 00 -function StartWait 2700 2


22.07.2020 09:57:26
Start
OK

22.07.2020 09:57:53
StartWait
OK
s00adm@hana002:/usr/sap/S00/HDB00>
```

Step 4 Query the System Replication status in the SAP HANA system.

Run the following command in the administrator mode on the active node:

hdbnsutil -sr_state

Information similar to the following is displayed:


```
hana001:~ # su - s00adm
s00adm@hana001:/usr/sap/S00/HDB00> hdbnsutil -sr_state

System Replication State
~~~~~~~~~~~~~~~~~~~~~~~~

online: true

mode: primary
operation mode: primary
site id: 1
site name: hana001


is source system: true
is secondary/consumer system: false
has secondaries/consumers attached: true
is a takeover active: false

Host Mappings:
~~~~~~~~~~~~~~

hana001 -> [hana002] hana002
hana001 -> [hana001] hana001


Site Mappings:
~~~~~~~~~~~~~~
hana001 (primary/primary)
    |---hana002 (sync/logreplay)

Tier of hana001: 1
Tier of hana002: 2
```

```
Replication mode of hana001: primary
Replication mode of hana002: sync

Operation mode of hana001: primary
Operation mode of hana002: logreplay

Mapping: hana001 -> hana002
done.
s00adm@hana001:/usr/sap/S00/HDB00>
```

----End

4.6.1.3 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 SUSE Linux Enterprise Server (SLES) 12 SP1 for SAP or later for automatic active/standby switchovers.

Prerequisites

- SSH switching between SAP HANA nodes has been allowed.
- The SBD volume has been mounted to the two SAP HANA ECSs.
- A floating IP address has been created and bound to the two SAP HANA ECSs.

Procedure

Step 1 Log in to the active SAP HANA ECS **hana001**.

Step 2 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


```
hana001:~ # rpm -qa | grep patterns-ha-ha_sles
patterns-ha-ha_sles-12-15.7.x86_64
hana001:~ # rpm -qa | grep sap-suse-cluster-connector
sap-suse-cluster-connector-3.0.1-5.1.noarch
hana001:~ #
```

- If yes, skip this step.
- If no, run the following commands to install the dependency packages:

  zypper in -y patterns-ha-ha_sles

  zypper in -y sap-suse-cluster-connector

Step 3 Download scripts and configure the file.

1. Select the region where the SAP HANA software is installed and download the script.

   The following uses 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

   The script download addresses for different regions are as follows:

   - **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
   - **AF-Johannesburg**: https://obs-sap-af-south-1.obs.af-south-1.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip
   - LA-Santiago: https://obs-sap-la-south-2.obs.la-south-2.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip
   - LA-Sao Paulo1: https://obs-sap-sa-brazil-11.obs.sa-brazil-1.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip
   - LA-Mexico City1: https://obs-sap-na-mexico-1.obs.na-mexico-1.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip
   - LA-Mexico City2: https://obs-sap-la-north-2.obs.la-north-2.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip

2. Run the following commands to decompress the script package.

   cd /hana/shared

   unzip ha_auto_script.zip


```
hana001:~ # wget https://obs-sap-cn-south-1.obs.myhwclouds.com/ha_auto_script/ha_auto_script.zip -P /hana/shared
--2020-07-22 16:06:42--  https://obs-sap-cn-south-1.obs.myhwclouds.com/ha_auto_script/ha_auto_script.zip
Resolving obs-sap-cn-south-1.obs.myhwclouds.com (obs-sap-cn-south-1.obs.myhwclouds.com)... 100.125.24.34, 100.12
5.24.91, 100.125.24.3
Connecting to obs-sap-cn-south-1.obs.myhwclouds.com (obs-sap-cn-south-1.obs.myhwclouds.com)|100.125.24.34|:443..
. connected.
HTTP request sent, awaiting response... 200 OK
Length: 23657 (23K) [application/zip]
Saving to: '/hana/shared/ha_auto_script.zip'

100%[=====================================================================>] 23,657      --.-K/s   in 0.001s

2020-07-22 16:06:42 (21.1 MB/s) - '/hana/shared/ha_auto_script.zip' saved [23657/23657]

hana001:~ # cd /hana/shared/
hana001:/hana/shared # ll
total 13308332
drwxr-xr-x 3 root   root          245 Sep 21  2018 51053381
-rw-r--r-- 1 root   root   4000000000 Feb  3 13:35 51053381_part1.exe
-rw-r--r-- 1 root   root   4000000000 Feb  3 13:35 51053381_part2.rar
-rw-r--r-- 1 root   root   4000000000 Feb  3 13:35 51053381_part3.rar
-rw-r--r-- 1 root   root   1627698107 Feb  3 13:36 51053381_part4.rar
drwxr-xr-x 9 s00adm sapsys        117 Jul 22 11:56 S00
-rw-r--r-- 1 root   root        23657 Jan 22 12:06 ha_auto_script.zip

hana001:/hana/shared # unzip ha_auto_script.zip
Archive:  ha_auto_script.zip
   creating: ha_auto_script/
  inflating: ha_auto_script/basic_ha.cfg
   creating: ha_auto_script/templates/
  inflating: ha_auto_script/templates/scs_res.template
  inflating: ha_auto_script/templates/ascs_col.template
  inflating: ha_auto_script/templates/scs_col.template
  inflating: ha_auto_script/templates/hana_rsc.template
  inflating: ha_auto_script/templates/corosync_template
  inflating: ha_auto_script/templates/properties.template
  inflating: ha_auto_script/templates/corosync_2heartbeat_template
  inflating: ha_auto_script/templates/ascs_res.template
  inflating: ha_auto_script/templates/sbd_res.template
  inflating: ha_auto_script/templates/ers_res.template
  inflating: ha_auto_script/ascs_ha.cfg
  inflating: ha_auto_script/hana_ha.cfg
  inflating: ha_auto_script/helper.sh
  inflating: ha_auto_script/basic_auto_ha.sh
 extracting: ha_auto_script/version
  inflating: ha_auto_script/ascs_auto_ha.sh
  inflating: ha_auto_script/hana_auto_ha.sh
hana001:/hana/shared #
```

Step 4 Run the following command to modify the configuration file:

vi /hana/shared/ha_auto_script/hana_ha.cfg

Set the parameters in the configuration file based on the site requirements.


```
[masterNode]
# Host name of the active node
masterName=hana001
# Heartbeat IP address of the active node
masterHeartbeatIP1=10.0.4.130
masterHeartbeatIP2=10.0.3.30

[slaveNode]
# Host name of the standby node
slaveName=hana002
# Heartbeat IP address of the standby node
slaveHeartbeatIP1=10.0.4.140
slaveHeartbeatIP2=10.0.3.40

[trunkInfo]
# Floating IP address of SAP HANA
hanaBusinessIP=10.0.3.100

[hanaInfo]
# SBD volume path
SBDDevice=/dev/sda
# SAP HANA administrator account
hanaUser=s00adm
# SAP HANA instance number
InstanceNumber=00
~
~
~
~
~
~
~
~
~
~
~
                                                                    25,17         All
```

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.

Step 5 Run the following command to execute the script:

sh hana_auto_ha.sh

```
hana001:/hana/shared # sh ha_auto_script/hana_auto_ha.sh
Running on SLES 12.
ssh to slave node from master node.
ssh to master node from slave node.
s00adm exists.
SID: S00, Instnace Number: 00 are valid.
HANA is running on both nodes.
HANA system replication configured.
corosync.conf                                                 100% 2690     2.6KB/s   00:00
Configure softdog on master node success
softdog.conf                                                  100%    8     0.0KB/s   00:00
  Configuring csync2
  Generating csync2 shared key (this may take a while)...done
  csync2 checking files...done
  Done (log saved to /var/log/ha-cluster-bootstrap.log)
  Hawk cluster interface is now running. To see cluster status, open:
    https://10.0.3.30:7630/
  Log in with username 'hacluster', password 'linux'
WARNING: You should change the hacluster password to something more secure!
  Waiting for cluster........done
  Loading initial cluster configuration
  Done (log saved to /var/log/ha-cluster-bootstrap.log)
Master node ha-cluster-init successfully.
Removed symlink /etc/systemd/system/multi-user.target.wants/pacemaker.service.
Successfully calling ha-cluster-init in master node.
# 10.0.4.130:22 SSH-2.0-OpenSSH_7.2
# 10.0.4.130:22 SSH-2.0-OpenSSH_7.2
# 10.0.4.130:22 SSH-2.0-OpenSSH_7.2
```



```
.
Created symlink from /etc/systemd/system/corosync.service.requires/sbd.service to /usr/lib/systemd/system/sbd.se
rvice.
Created symlink from /etc/systemd/system/pacemaker.service.requires/sbd.service to /usr/lib/systemd/system/sbd.s
ervice.
Created symlink from /etc/systemd/system/dlm.service.requires/sbd.service to /usr/lib/systemd/system/sbd.service
.
Waiting for cluster...done
Stack: corosync
Current DC: hana001 (version 1.1.19+20181105.ccd6b5b10-3.10.1-1.1.19+20181105.ccd6b5b10) - partition with quorum
Last updated: Wed Jul 22 16:14:08 2020
Last change: Wed Jul 22 16:14:08 2020 by root via crm_attribute on hana002

2 nodes configured
6 resources configured

Online: [ hana001 hana002 ]

Full list of resources:

 stonith-sbd    (stonith:external/sbd): Starting hana001
 rsc_ip_SLE_HDB (ocf::heartbeat:IPaddr2):       Started hana002
 Master/Slave Set: msl_SAPHana_SLE_HDB [rsc_SAPHana_SLE_HDB]
     Slaves: [ hana001 hana002 ]
 Clone Set: cln_SAPHanaTopology_SLE_HDB [rsc_SAPHanaTopology_SLE_HDB]
     Stopped: [ hana001 hana002 ]
Successfully configure HA.
hana001:/hana/shared #
```


CAUTION

- If the script execution fails, you have to run the command **sh hana_auto_ha.sh unconf** to manually perform rollback 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. Run the following command to stop the database of standby node.

   HDB stop

3. Register the hostname of the standby node to the active node.

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

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

4. Run the following commands to start the database of 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

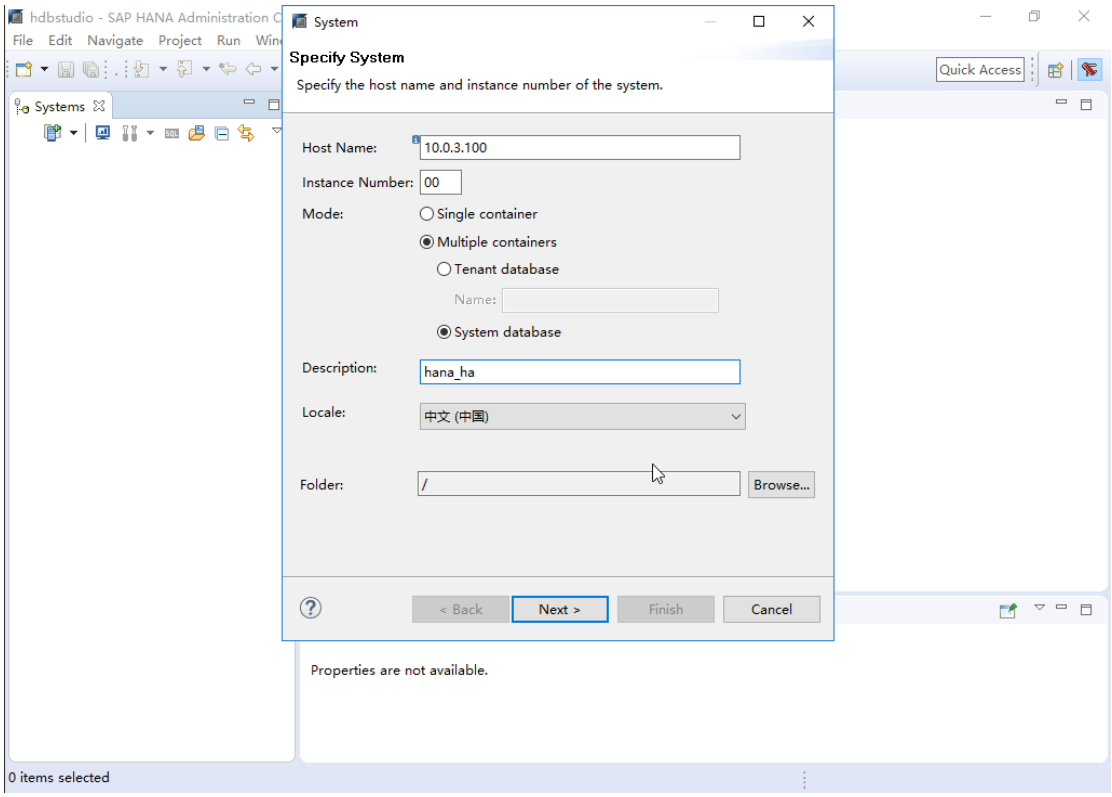
6. Clear resources on the original active node (current standby node).

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

   crm resource cleanup <rsc_SAPHana_SLE_HDB00> <primary>

Step 6 Connect SAP HANA nodes to the SAP HANA Studio again.

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

4.6.1.4 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 indicies 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 - *s00*adm

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

4.6.2 SAP S/4HANA HA Configurations

4.6.2.1 Modifying the Hosts Configuration File

To ensure that the communication between the active and standby ASCS nodes is normal, add the mappings between the virtual IP addresses and virtual hostnames to the hosts file after installing the SAP S/4HANA instance.

Procedure

Step 1 Log in to the active and standby SAP S/4HANA nodes and modify the **/etc/hosts** file.

- Change the physical IP address of the active ASCS node to virtual IP address of the active node.
- Change the physical IP address of the standby ASCS node to virtual IP address of the standby node.
- Change the physical IP address of the active SAP HANA node to the virtual IP address shared by the active and standby SAP HANA nodes.

The hosts file before the modification is as follows:


```
#
# hosts         This file describes a number of hostname-to-address
#               mappings for the TCP/IP subsystem.  It is mostly
#               used at boot time, when no name servers are running.
#               On small systems, this file can be used instead of a
#               "named" name server.
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#


# special IPv6 addresses
::1     localhost       ipv6-localhost  ipv6-loopback

fe00::0 ipv6-localnet

ff00::0 ipv6-mcastprefix
ff02::1 ipv6-allnodes
ff02::2 ipv6-allrouters
ff02::3 ipv6-allhosts




127.0.0.1       localhost

10.0.3.10       s4001
10.0.3.20       s4002
10.0.3.10       ascsha
10.0.3.20       ersha

10.0.3.30       hanaha
~
~
~
"/etc/hosts" 33L, 677C                                                27,0-1        All
```

Change the physical IP addresses to the virtual IP addresses.

```
#
# hosts         This file describes a number of hostname-to-address
#               mappings for the TCP/IP subsystem.  It is mostly
#               used at boot time, when no name servers are running.
#               On small systems, this file can be used instead of a
#               "named" name server.
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#


# special IPv6 addresses
::1     localhost       ipv6-localhost  ipv6-loopback

fe00::0 ipv6-localnet

ff00::0 ipv6-mcastprefix
ff02::1 ipv6-allnodes
ff02::2 ipv6-allrouters
ff02::3 ipv6-allhosts




127.0.0.1       localhost

10.0.3.10       s4001
10.0.3.20       s4002
10.0.3.110      ascsha
10.0.3.120      ersha

10.0.3.100      hanaha
~
~
"/etc/hosts" 33L, 680C                                                33,9          All
```

NOTE

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

Step 2 Log in to the standby SAP S/4HANA node and modify the /etc/hosts file to be the same as that of the active node.

----End

4.6.2.2 Checking the Directory

Check whether the **/var/log/cluster** directory exists on the active and standby ASCS nodes. If it does not exist, run the following command to create it:

mkdir /var/log/cluster

```
s4001:~ # ll /var/log/ | grep cluster
drwxr-xr-x 2 root root   4096 Apr 17  2018 cluster
s4001:~ #
```

4.6.2.3 Installing SAP Resource Agents

Install SAP resource agents on the active and standby SAP S/4HANA nodes.

Procedure

Step 1 Run the following command to check whether the **resource-agents** package has been installed:

sudo grep 'parameter name="IS_ERS"' /usr/lib/ocf/resource.d/heartbeat/SAPInstance

- If the information similar to the following is displayed, the patch package has been installed. No further action is required.

```
s4001:~ # sudo grep 'parameter name="IS_ERS"' /usr/lib/ocf/resource.d/heartbeat/SAPInstance
 <parameter name="IS_ERS" unique="0" required="0">
s4001:~ #
```

- If no command output is displayed, go to **Step 2** to install the patch package.

Step 2 Install the **resource-agents** package.

- If the image is SLES 12 SP1, run the following command:

  sudo zypper in -t patch SUSE-SLE-HA-12-SP1-2017-885=1
- If the image is SLES 12 SP2, run the following command:

  sudo zypper in -t patch SUSE-SLE-HA-12-SP2-2018-1923=1
- If the image is SLES 12 SP3, run the following command:

  sudo zypper in -t patch SUSE-SLE-HA-12-SP3-2018-1922=1

----End

4.6.2.4 Updating sap_suse_cluster_connector

Update sap_suse_cluster_connector on the active and standby SAP S/4HANA nodes.

Procedure

Step 1 Run the following command to uninstall sap_suse_cluster_connector of the earlier version. The software package name uses underscores (_).

zypper remove sap_suse_cluster_connector

Step 2 Run the following command to install sap_suse_cluster_connector of the latest version. The software package name uses hyphens (-):

zypper install sap-suse-cluster-connector

Step 3 Run the following command to obtain the version information about the newly installed **sap-suse-cluster-connector**:

/usr/bin/sap_suse_cluster_connector gvi --out version

Step 4 Run the following command to check the **version** file and verify that the sap_suse_cluster_connector version is 3.1.0 or later:

cat /usr/bin/version

```
s4001:~ # /usr/bin/sap_suse_cluster_connector gvi --out version
s4001:~ # cat /usr/bin/version
3
SUSE Linux Enterprise Server for SAP Applications 12 SP4
SUSE Linux Enterprise Server for SAP Applications 12 SP4 (sap_suse_cluster_connector 3.0.1)
https://www.suse.com/products/sles-for-sap/resource-library/sap-best-practices/
s4001:~ #
```

----End

4.6.2.5 Configuring the HA Function for SAP S/4HANA Nodes

Procedure

Step 1 Log in to the active SAP S/4HANA node, obtain the **ha_auto_script.zip** package, and decompress it to any directory.

1. Select the region where SAP S/4HANA is to be installed and download the script.

   Select the region where SAP S/4HANA is to be installed and download the script. The following uses 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 /sapcd

   The script download addresses for different regions are as follows:

   - **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
   - **AF-Johannesburg**: https://obs-sap-af-south-1.obs.af-south-1.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip
   - LA-Santiago: https://obs-sap-la-south-2.obs.la-south-2.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip

- LA-Sao Paulo1: https://obs-sap-sa-brazil-11.obs.sa-brazil-1.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip
- LA-Mexico City1: https://obs-sap-na-mexico-1.obs.na-mexico-1.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip
- LA-Mexico City2: https://obs-sap-la-north-2.obs.la-north-2.myhuaweicloud.com/ha_auto_script/ha_auto_script.zip

2. Run the following commands to decompress the obtained script package:

   cd /sapcd

   unzip ha_auto_script.zip

```
s4001:~ # wget https://obs-sap.obs.myhwclouds.com/ha_auto_script/ha_auto_script.zip -P /sapcd
--2020-07-22 16:50:59--  https://obs-sap.obs.myhwclouds.com/ha_auto_script/ha_auto_script.zip
Resolving obs-sap.obs.myhwclouds.com (obs-sap.obs.myhwclouds.com)... 122.112.208.64, 122.112.208.67
Connecting to obs-sap.obs.myhwclouds.com (obs-sap.obs.myhwclouds.com)|122.112.208.64|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 23657 (23K) [application/zip]
Saving to: '/sapcd/ha_auto_script.zip'

100%[======================================================================>] 23,657      --.-K/s   in 0.03s

2020-07-22 16:50:59 (798 KB/s) - '/sapcd/ha_auto_script.zip' saved [23657/23657]

s4001:~ # cd /sapcd/
s4001:/sapcd # ll
total 36
drwxrwxrwx  2 root root  4096 Jul 22 14:22 backup
drwxrwxrwx 14 root root  4096 Jul 22 15:35 SWPM
drwxrwxrwx  2 root root  4096 Jul 22 16:46 cluster_rpm
-rwxrwxrwx  1 root root 23657 Jan 22 12:12 ha_auto_script.zip

s4001:/sapcd # unzip ha_auto_script.zip
Archive:  ha_auto_script.zip
   creating: ha_auto_script/
  inflating: ha_auto_script/basic_ha.cfg
   creating: ha_auto_script/templates/
  inflating: ha_auto_script/templates/scs_res.template
  inflating: ha_auto_script/templates/ascs_col.template
  inflating: ha_auto_script/templates/scs_col.template
  inflating: ha_auto_script/templates/hana_rsc.template
  inflating: ha_auto_script/templates/corosync_template
  inflating: ha_auto_script/templates/properties.template
  inflating: ha_auto_script/templates/corosync_2heartbeat_template
  inflating: ha_auto_script/templates/ascs_res.template
  inflating: ha_auto_script/templates/sbd_res.template
  inflating: ha_auto_script/templates/ers_res.template
  inflating: ha_auto_script/ascs_ha.cfg
  inflating: ha_auto_script/hana_ha.cfg
  inflating: ha_auto_script/helper.sh
  inflating: ha_auto_script/basic_auto_ha.sh
 extracting: ha_auto_script/version
  inflating: ha_auto_script/ascs_auto_ha.sh
  inflating: ha_auto_script/hana_auto_ha.sh
s4001:/sapcd # cd ha_auto_script/
s4001:/sapcd/ha_auto_script # ll
total 92
-rw-r--r-- 1 root root 24661 Dec 23  2019 ascs_auto_ha.sh
-rw-r--r-- 1 root root   869 Dec 23  2019 ascs_ha.cfg
-rw-r--r-- 1 root root  3940 Dec 23  2019 basic_auto_ha.sh
-rw-r--r-- 1 root root   381 Dec 23  2019 basic_ha.cfg
-rw-r--r-- 1 root root  7687 Dec 23  2019 hana_auto_ha.sh
-rw-r--r-- 1 root root   546 Dec 23  2019 hana_ha.cfg
-rw-r--r-- 1 root root 29157 Dec 23  2019 helper.sh
drwxr-xr-x 2 root root  4096 Dec 23  2019 templates
-rw-r--r-- 1 root root     5 Dec 23  2019 version
s4001:/sapcd/ha_auto_script #
```

Step 2 Set parameters in the **ascs_ha.cfg** file based on the site requirements. **Table 4-18** describes the parameters in the file.

Table 4-18 Parameters in the **ascs_ha.cfg** file

Type	Name	Description
masterNode	masterName	ASCS instance node name

Type	Name	Description
	masterHeartbeatIP1	Heartbeat plane IP address 1 of the ASCS instance node
	masterHeartbeatIP2	Service plane IP address of the ASCS instance node
slaveNode	slaveName	ERS instance node name
	slaveHeartbeatIP1	Heartbeat plane IP address 1 of the ERS instance node
	slaveHeartbeatIP2	Service plane IP address of the ERS instance node
ASCSInstance	ASCSFloatIP	Service IP address of the ASCS instance node
	ASCSInstanceDir	Directory of the ASCS instance
	ASCSDevice	Disk partition used by the ASCS instance directory
	ASCSProfile	Profile file of the ASCS instance
ERSInstance **NOTE** You need to log in to the ERS instance node to obtain the information about the **ERSInstanceDir**, **ERSDevice**, and **ERSProfile** parameters.	ERSFloatIP	Service IP address of the ERS instance node
	ERSInstanceDir	Directory of the ERS instance
	ERSDevice	Disk partition used by the ERS instance directory
	ERSProfile	Profile file of the ERS instance
trunkInfo	SBDDevice	Independent disk used by the SBD. One or three disks are supported. Every two disks are separated by a comma (,), for example, **/dev/sda**, **/dev/sdb**, **/dev/sdc**.


```
[masterNode]
# Host name of the active node
masterName=s4001
# Heartbeat IP address of the active node
masterHeartbeatIP1=10.0.4.110
masterHeartbeatIP2=10.0.3.10

[slaveNode]
# Host name of the standby node
slaveName=s4002
# Heartbeat IP address of the standby node
slaveHeartbeatIP1=10.0.4.120
slaveHeartbeatIP2=10.0.3.20

[ASCSInstance]
# Float IP for ASCS instance or SCS instance
ASCSFloatIP=10.0.3.110
# Instance directory of ASCS instance or SCS isntance
ASCSInstanceDir=/usr/sap/S01/ASCS01
# Device of ASCS or SCS
ASCSDevice=/dev/sdb
# Profile of ASCS or SCS
ASCSProfile=/usr/sap/S01/SYS/profile/S01_ASCS01_ascsha


[ERSInstance]
UseERS=True
# Float IP for ERS instance
ERSFloatIP=10.0.3.120
ERSInstanceDir=/usr/sap/S01/ERS10
ERSDevice=/dev/sdc
ERSProfile=/usr/sap/S01/SYS/profile/S01_ERS10_ersha

[trunkInfo]
# disk or partition for SBD
SBDDevice=/dev/sda
"ascs_ha.cfg" 36L, 864C                                                    36,18         All
```

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

sh ascs_auto_ha.sh

```
s4001:/sapcd/ha_auto_script # sh ascs_auto_ha.sh
Running on SLES 12.
ssh to slave node from master node.
ssh to master node from slave node.
10.0.3.110      ascsha
10.0.3.120      ersha
Resource-agents installed on both nodes.
ASCS/SCS disk attached to both nodes.
Appending ERS entry to sapservices
Appending ASCS/SCS entry to sapservices in salve node.
Setting Start_Program for Enqueue Server.
Restarting ASCS/SCS instance.
Restarting ERS instance.
corosync.conf                                                 100% 2690     2.6KB/s   00:00
Configure softdog on master node success
softdog.conf                                                  100%    8     0.0KB/s   00:00
  Configuring csync2
  Generating csync2 shared key (this may take a while)...done
  csync2 checking files...done
  Done (log saved to /var/log/ha-cluster-bootstrap.log)
  Hawk cluster interface is now running. To see cluster status, open:
    https://10.0.3.10:7630/
  Log in with username 'hacluster', password 'linux'
WARNING: You should change the hacluster password to something more secure!
  Waiting for cluster........done
  Loading initial cluster configuration
  Done (log saved to /var/log/ha-cluster-bootstrap.log)
Master node ha-cluster-init successfully.
Removed symlink /etc/systemd/system/multi-user.target.wants/pacemaker.service.
Successfully calling ha_cluster_init in master node.
# 10.0.4.110:22 SSH-2.0-OpenSSH_7.2
# 10.0.4.110:22 SSH-2.0-OpenSSH_7.2
# 10.0.4.110:22 SSH-2.0-OpenSSH_7.2
Calling 'ha-cluster-join -y -c 10.0.4.110 csync2' in slave node.
  Configuring csync2...done
```



```
Created symlink from /etc/systemd/system/pacemaker.service.requires/sbd.service to /usr/lib/systemd/system/sbd.s
ervice.
Created symlink from /etc/systemd/system/dlm.service.requires/sbd.service to /usr/lib/systemd/system/sbd.service
.
INSTANCE_NAME = ASCS01
INSTANCE_NAME = ASCS01
Waiting for cluster...done
Stack: corosync
Current DC: s4001 (version 1.1.19+20181105.ccd6b5b10-3.10.1-1.1.19+20181105.ccd6b5b10) - partition with quorum
Last updated: Wed Jul 22 17:01:16 2020
Last change: Wed Jul 22 17:01:03 2020 by root via cibadmin on s4001

2 nodes configured
7 resources configured

Online: [ s4001 s4002 ]

Full list of resources:

 stonith-sbd    (stonith:external/sbd): Started s4001
 Resource Group: grp_ASCS
     rsc_ip_ASCS        (ocf::heartbeat:IPaddr2):       Stopped
     rsc_fs_ASCS        (ocf::heartbeat:Filesystem):    Started s4001
     rsc_sap_ASCS       (ocf::heartbeat:SAPInstance):   Stopping s4001
 Resource Group: grp_ERS
     rsc_ip_ERS (ocf::heartbeat:IPaddr2):       Stopped
     rsc_fs_ERS (ocf::heartbeat:Filesystem):    Started s4002
     rsc_sap_ERS        (ocf::heartbeat:SAPInstance):   Started s4002
Successfully configure HA.
s4001:/sapcd/ha_auto_script #
```

Step 4 Run the following command to check the resource status:

crm status

```
s4001:/sapcd/ha_auto_script # crm status
Stack: corosync
Current DC: s4001 (version 1.1.19+20181105.ccd6b5b10-3.10.1-1.1.19+20181105.ccd6b5b10) - partition with quorum
Last updated: Wed Jul 22 17:03:52 2020
Last change: Wed Jul 22 17:01:03 2020 by root via cibadmin on s4001

2 nodes configured
7 resources configured

Online: [ s4001 s4002 ]

Full list of resources:

 stonith-sbd    (stonith:external/sbd): Started s4001
 Resource Group: grp_ASCS
     rsc_ip_ASCS        (ocf::heartbeat:IPaddr2):       Started s4001
     rsc_fs_ASCS        (ocf::heartbeat:Filesystem):    Started s4001
     rsc_sap_ASCS       (ocf::heartbeat:SAPInstance):   Started s4001
 Resource Group: grp_ERS
     rsc_ip_ERS (ocf::heartbeat:IPaddr2):       Started s4002
     rsc_fs_ERS (ocf::heartbeat:Filesystem):    Started s4002
     rsc_sap_ERS        (ocf::heartbeat:SAPInstance):   Started s4002

s4001:/sapcd/ha_auto_script #
```


NOTE

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

crm configure property maintenance-mode=true

Exit the maintenance mode after the modification is complete.

crm configure property maintenance-mode=false

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

systemctl stop pacemaker

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

systemctl start pacemaker

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

sh ascs_auto_ha.sh unconf

----End

4.6.2.6 Verifying the Configuration

Prerequisites

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

Procedure

Step 1 Enter the IP address or hostname of the active or standby node as the URL. The login port is 7630.

Example: https://s4001:7630/

NOTE

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

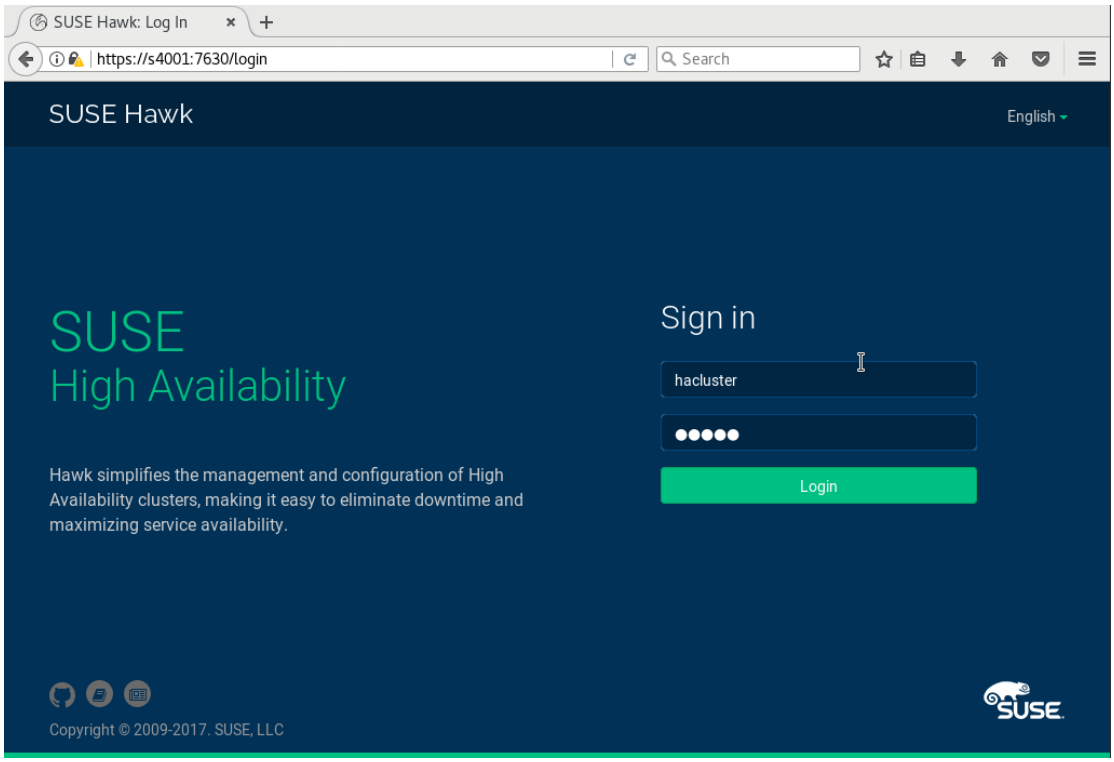
Click **Continue to this website (not recommended)** or add an exception in the browser to eliminate the warning message.

Remarks:

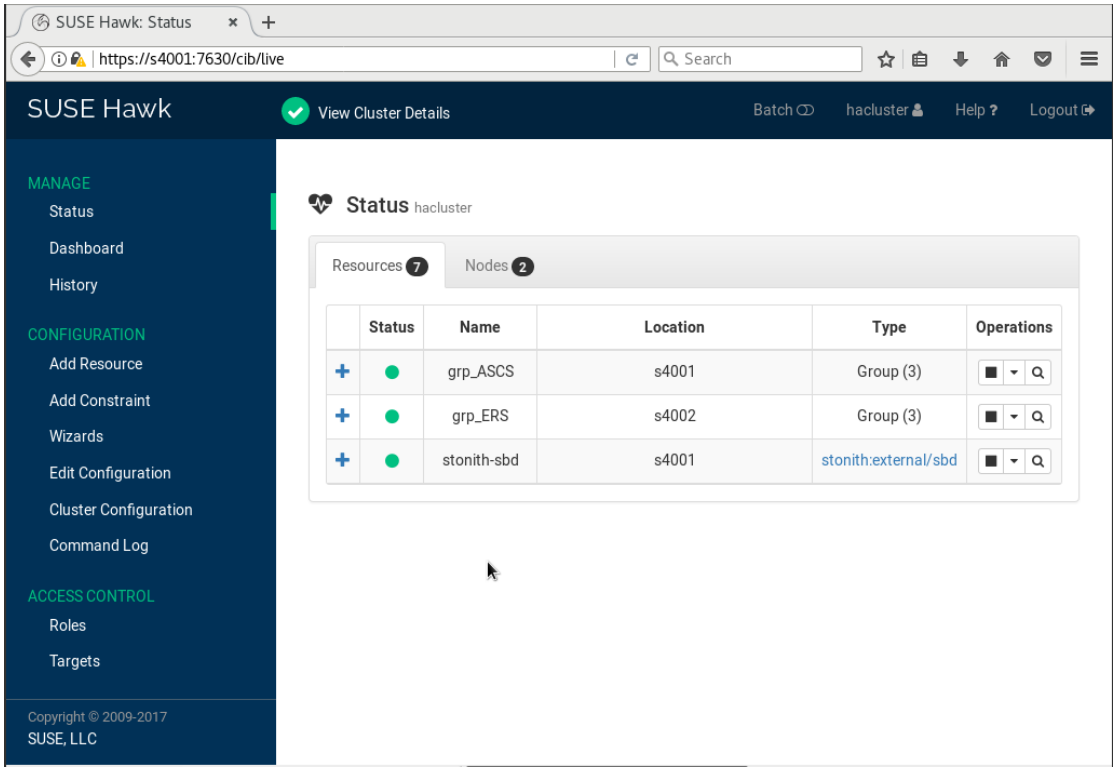
Step 2 On the login page, enter the username and password of user **hacluster** or any other user who belongs to the haclient group.

NOTE

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



Step 3 Click **Login**. You can view the statuses of cluster nodes and resources on the displayed page.



----End

4.7 Change History

Description	Released On
This issue is the first official release.	2020-10-30
This issue is the second official release, which incorporates the following change: Added section "5.2.1 Adding a Virtual IP Address".	2022-12-05
This issue is the third official release. which incorporates the following change: Modified sections "3.3 File System Planning" and "4.7.1 Formatting the File System for Active and Standby SAP HANA ECSs".	2023-03-01

5 HUAWEI CLOUD SAP Business One on HANA Installation Best Practice

5.1 Introduction

This document provides guidance for preparing resources (such as cloud servers and network resources) on the HUAWEI CLOUD platform and installing SAP Business One on HANA. SAP is authorized in Bring Your Own License (BYOL) mode. You need to log in at **SAP Support Portal** to purchase licenses.

The document conventions are as follows:

This document describes how to install and deploy SAP Business One (SAP HANA as the database).

This document cannot replace the standard SAP document. If you have any trouble in installing and using SAP Business One due to its own problems, contact the SAP technical support.

This document is written based on the OS SUSE Linux Enterprise Server. The deployment modes mentioned in the document are only for reference. Install SAP Business One by referring to the standard SAP installation manual or based on sizing results and site requirements.

For details about the official SAP installation guide and related notes, see the following documents:

- **SAP Installation Guides**
- **SAP Library**
- **https://partneredge.sap.com**

For details about SAP Business One, see **SAP Business One User Guide**.

5.2 Pre-installation Preparations

Logging in to Huawei Cloud

Before deploying the SAP system on Huawei Cloud, register a HUAWEI ID and enable Huawei Cloud services. Through this account, you can use Huawei Cloud services and pay only for the services you use.

For details, see **Registering a HUAWEI ID and Enabling Huawei Cloud Services**.

You can log in to Huawei Cloud using any of the methods described in **Logging In to Huawei Cloud**.

SAP License

SAP is authorized in Bring Your Own License (BYOL) mode. In this mode, you need to log in to the **SAP Support Portal** and apply for a license.

NAT Server

Prepare a Network Address Translation (NAT) server on which SAP HANA and SAP Business One clients and SAP HANA Studio are installed.

5.3 Resource Planning

5.3.1 Network Planning

The network information needs to be planned based on application scenarios and SAP planning. The following table lists the network segments and IP addresses required for installing standard standalone SAP Business One on HANA. You can configure it based on site requirements.

Parameter	Description	Example Value
IP address of the server/client plane	Specifies the IP address of the primary NIC plane. The SAP Business One node communicates communicate with the SAP HANA and SAP Business One clients and the SAP databases using this IP address.	SAP Business One node: 10.10.1.178 SAP HANA node: 10.10.1.178

5.3.2 Security Group Planning

SAP Security Group Planning

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

You can configure the security group by referring to the following table.

NOTE

- Plan the network segments and IP addresses based on the site requirements. The following security group rules are for reference only. You can configure your own security group rules as needed.
- In the following table, *##* stands for the SAP instance number, which must be consistent with the instance number specified when the SAP software is installed. If there are multiple instance numbers, enter them in sequence.

Source	Protocol	Port Range	Description
Inbound			
10.10.1.0/24	TCP	1-65535	Allows instances to communicate with each other in the subnet.
10.10.1.0/24	TCP	5##13 to 5##14	Allows the SAP HANA Studio to access SAP HANA.
10.10.1.0/24	TCP	3##00 to 3##10	Communication in the database
10.10.1.0/24	TCP	3##15 and 3##17	DB Client access port
10.10.1.0/24	TCP	111,2049,4000-4002	For NFS communication
10.10.1.0/24	TCP	40000~40001	SAP Business One server port
10.10.1.0/24	TCP	22	Allows SAP to be accessed using SSH.
10.10.1.0/24	TCP	43##	Allows access to XS Engine from the 10.0.0.0/24 subnet using HTTPS.

Source	Protocol	Port Range	Description
10.10.1.0/24	TCP	80##	Allows access to XS Engine from the 10.0.0.0/24 subnet using HTTP.
10.10.1.0/24	TCP	8080 (HTTP)	Allows Software Update Manager (SUM) to access SAP HANA using HTTP.
10.10.1.0/24	TCP	8443 (HTTPS)	Allows Software Update Manager (SUM) to access SAP HANA using HTTPS.
10.10.1.0/24	TCP	1128-1129	Allows access to SAP Host Agent using SOAP/HTTP.
Automatically specified by the system	ANY	ANY	Security group rule created by the system by default Allows ECSs in the same security group to communicate with each other.
Outbound			
ANY	ANY	ANY	Security group rule created by the system by default Allows SAP HANA to access all peers.

5.3.3 File System Planning

The following table describes the specifications of the file system planned for SAP Business One.

Mount Point	File System Size	File System Type	Shared	Description
/	40 GB	-	No	OS volume
/hana/data	400 GB	xfs	No	Data volume. Use two physical disks to make a data volume in using Logical Volume Manager (LVM).
/hana/log	## GB	xfs	No	Log volume. When the memory is less than or equal to 512 GB, the log volume capacity is half of the memory and rounded up for decimal places. When the memory is greater than 512 GB, the log volume capacity is 512 GB.
/hana/shared	## GB	xfs	No	Shared volume. It is recommended that the capacity of the Shared volume be at least 1.2 times the size of the memory.
/hana/backup	Auto capacity expansion	SFS	No	Create an SFS file system as the backup volume.
/usr/sap	50 GB	xfs	No	/usr/sap volume
/sapcd	Auto capacity expansion	SFS	Yes	Stores the SAP installation package, which is shared to all nodes in the SAP system.
-	20 GB	swap	No	Swap volume

5.3.4 ECS Planning

- SAP ECS specifications

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

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

SAP-certified ECSs must be used for installing the SAP application. For details, see **SAP Notes**.

- OS

  The following table lists the OS required for SAP ECSs. This document uses SAP Business One 9.3 as an example.

  SAP ECS OS

Name	Specifications
OS	SUSE Linux Enterprise Server 12 SP4

- SAP node planning

ECS Name	Server/ Client IP Address	Flavor	Type	Image
b123	10.10.1.178	m6.2xlarge.8	Business One HANA	SUSE Linux Enterprise Server 12 SP4
ecswindows	10.10.1.176	c6.4xlarge.2	Business One/HANA Client	Windows Server 2016 Standard 64bit Chinese

5.4 Preparing for the Installation

5.4.1 Creating a VPC

A VPC is logically isolated, configurable, and manageable virtual network for cloud servers, cloud containers, and cloud databases. It improves resource security and simplifies network deployment on the cloud. With a VPC, you can configure and manage the networks in the VPC, and make changes to these networks as needed, quickly and securely. For more information about VPC, see **VPC Overview**.

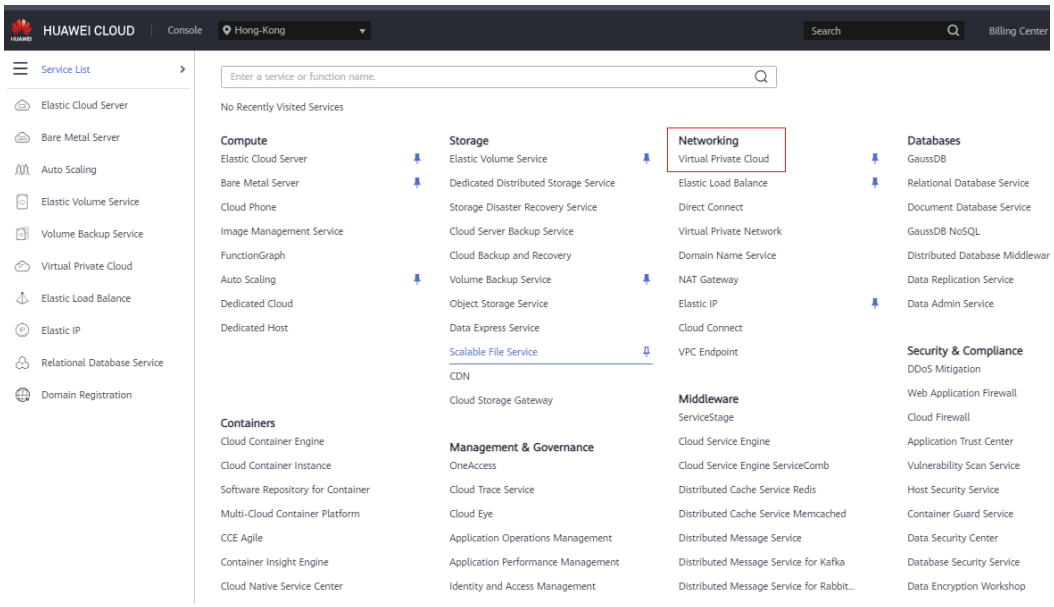
When creating a VPC, create the subnet 10.10.1.0 and use it as the server/client plane IP address of SAP Business One.

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 pane on the left, click and choose **Networking** > **Virtual Private Cloud**.



Step 4 Click **Create VPC** on the right of the page.

Step 5 Configure required parameters as prompted based on **Table 5-1**.

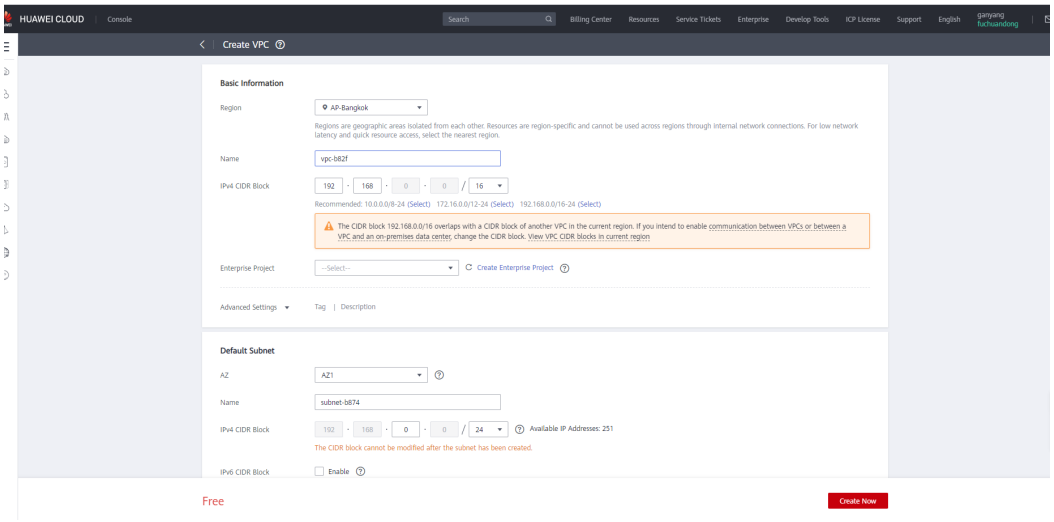


Table 5-1 VPC configuration parameters

Item	Parameter	Description
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 on the upper left of the page to change the region.

Item	Parameter	Description
	Name	VPC name.
	CIDR Block	CIDR block of 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 in the VPC). Choose one from the following CIDR blocks: 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 **Network Planning**.
	Enterprise Project	Enterprise project to which the VPC belongs. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**. For details about creating and managing enterprise projects, see the **Enterprise Management User Guide**.
	Tag	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. For details about the tag naming rules, see **VPC Tag Naming Rules**.
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 private networks.
	Name	Subnet name
	CIDR Block	CIDR block for the subnet. This value must be within the VPC CIDR block. Configure the subnet CIDR block based on the information provided in **Network Planning**.

Item	Parameter	Description
	Advanced Settings	Click **Advanced Settings** to set parameters such as **Gateway** and **DNS Server Address**.
	Gateway	Gateway address of the subnet.
	DNS Server Address	External DNS server addresses are used by default. To change the DNS server address, ensure that the DNS server addresses you configured are available.
	DHCP Lease Time	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.
	Tag	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**.
Add Subnet	You can click **Add Subnet** to add a subnet.	

Step 6 Click **Create Now**.

----End

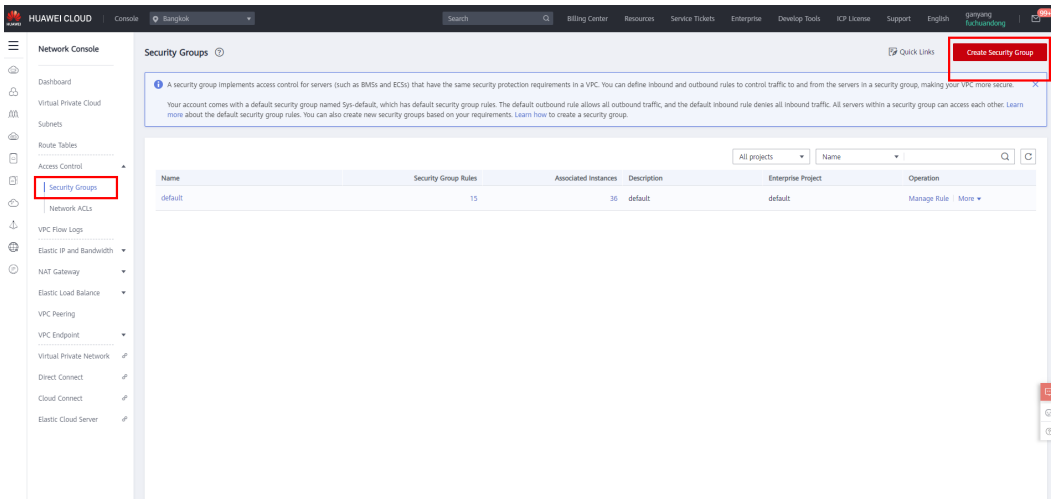
5.4.2 Creating a Security Group

A security group is a collection of access control rules for ECSs that have the same security protection requirements and are mutually trusted. You can define inbound and outbound rules to control traffic to and from the ECSs in a security group, making your VPC more secure. For more information about security groups, see **Security Group Overview**.

Procedure

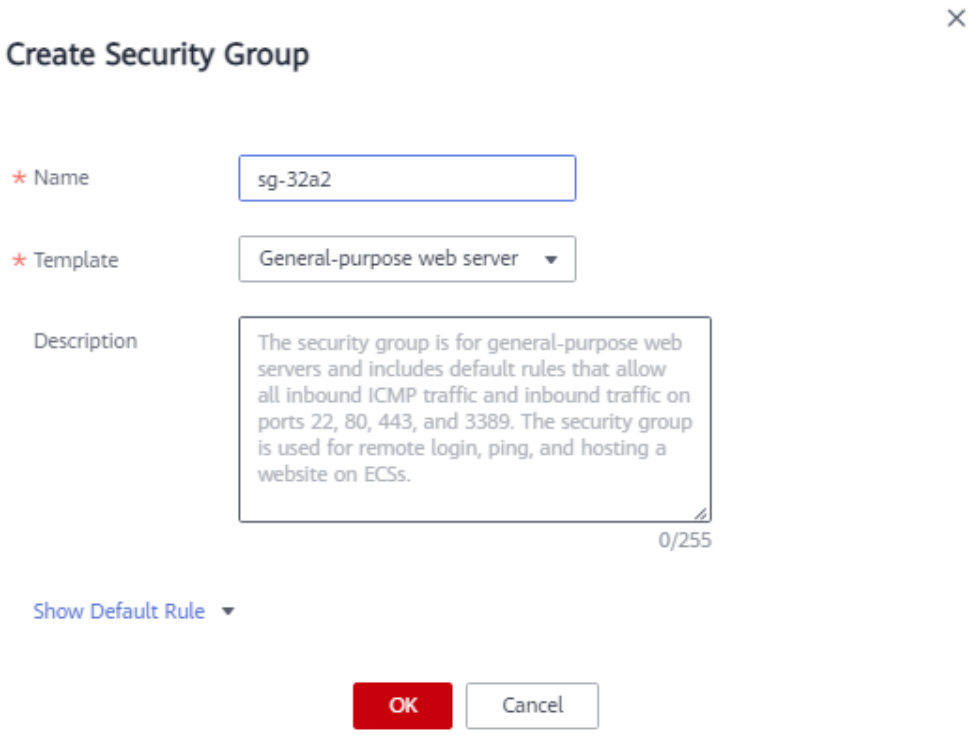
Step 1 Create a SAP security group.

Choose **Access Control** > **Security Groups** in the navigation pane on the left of the VPC console. On the **Security Groups** page, click **Create Security Group**.



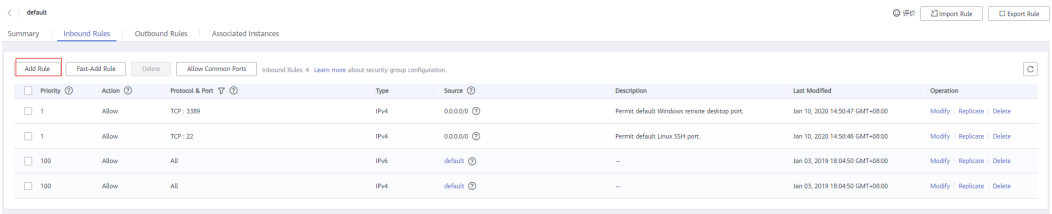
Step 2 Set required parameters to create a security group.

- **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 you create 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 you create using this template includes default rules that allow inbound traffic on any port. Note that allowing inbound traffic on any port poses security risks.
- **Name**: specifies the name of the security group. Name the security group that is easy to identify, for example, **sg_sap_**.
- **Enterprise Project**: You can add the security group to an enabled enterprise project. You can select an enterprise project from the drop-down list, for example, **SAP**.



Step 3 Click **OK**.

Locate the row that contains the newly created security group, and click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, add the desired ports listed in **Security Group Planning**.



----End

5.4.3 Creating ECSs

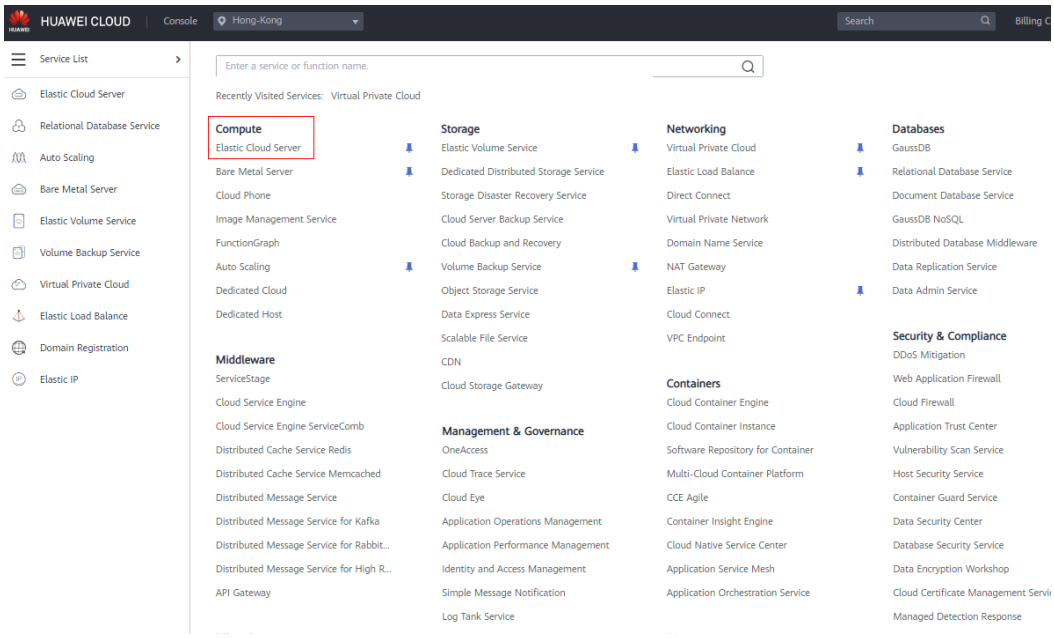
You need to create two ECSs. One is used to install SAP Business One and HANA, and the other is used to install the clients of SAP Business One and SAP HANA. The ECS specifications shown in the following table and figure are just for reference. Configure the specifications based on the site requirements.

ECS Name	Server/Client IP Address	Flavor	Type	Image
b123	10.10.1.178	m6.2xlarge.8	Business One	SUSE Enterprise 12 SP4

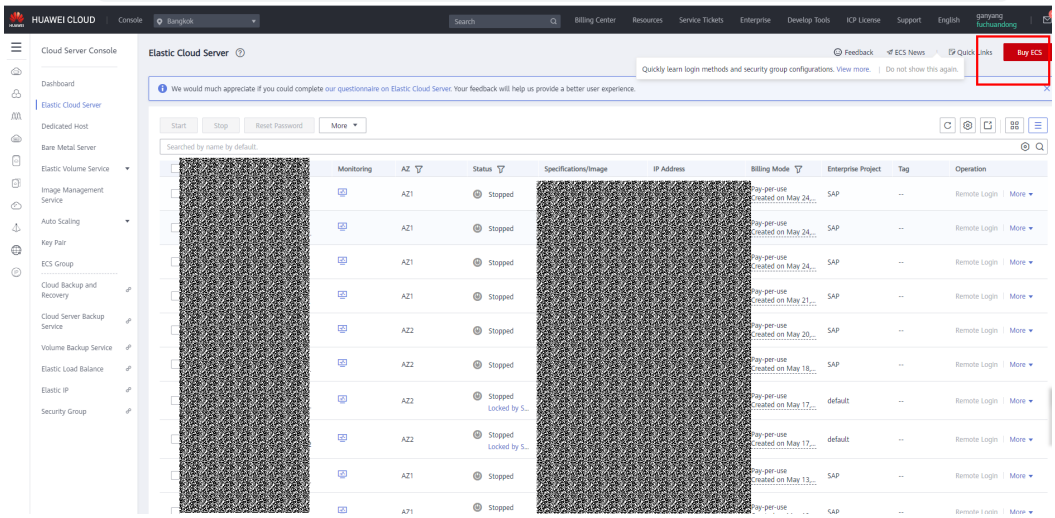
ECS Name	Server/Client IP Address	Flavor	Type	Image
			HANA	
ecswindows	10.10.1.176	c6.4xlarge.2	Business One/HANA Client	Windows Server 2016 Standard 64bit Chinese

ECS Flavor	Specifications	File System Size (GB)	Disk Size (GB)		Storage Class	OS
m6.2xlarge.8	12 vCPUs, 24 GB	1049	System disk	100	High I/O	SUSE Enterprise 12 SP4
			/usr/sap	80	High I/O	
			/hana/data	200 * 2	Ultra-high I/O	
			SWAP	17	High I/O	
			/hana/log	252	Ultra-high I/O	
			/hana/shared	300	High I/O	
			/sapcd	N/A	SFS	
c6.4xlarge.2	16 vCPUs | 32 GB	700	System disk	200	High I/O	Windows Server 2016 Standard 64bit Chinese
			D:	500	High I/O	

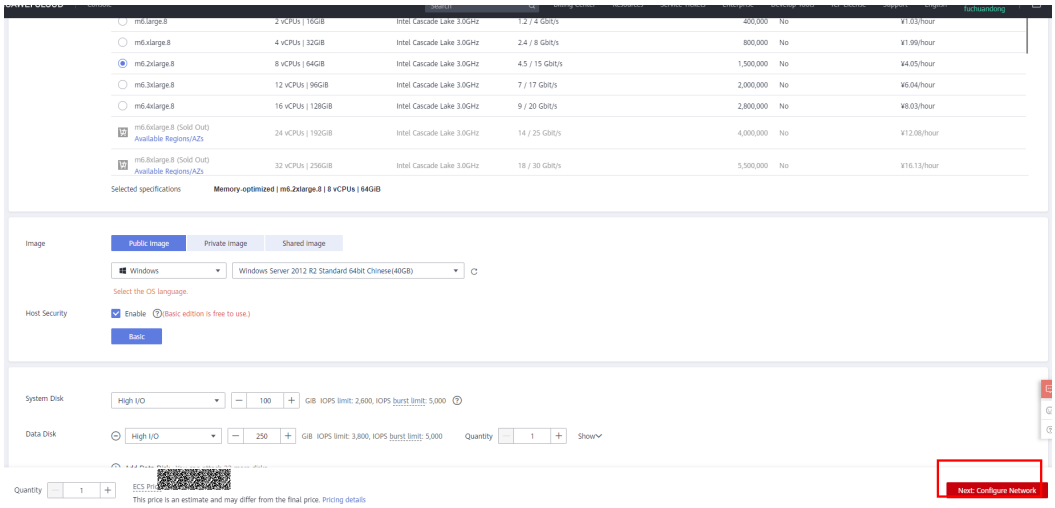
Step 1 Log in to the HUAWEI CLOUD management console, click the service list icon, and choose **Compute** > **Elastic Cloud Server**.



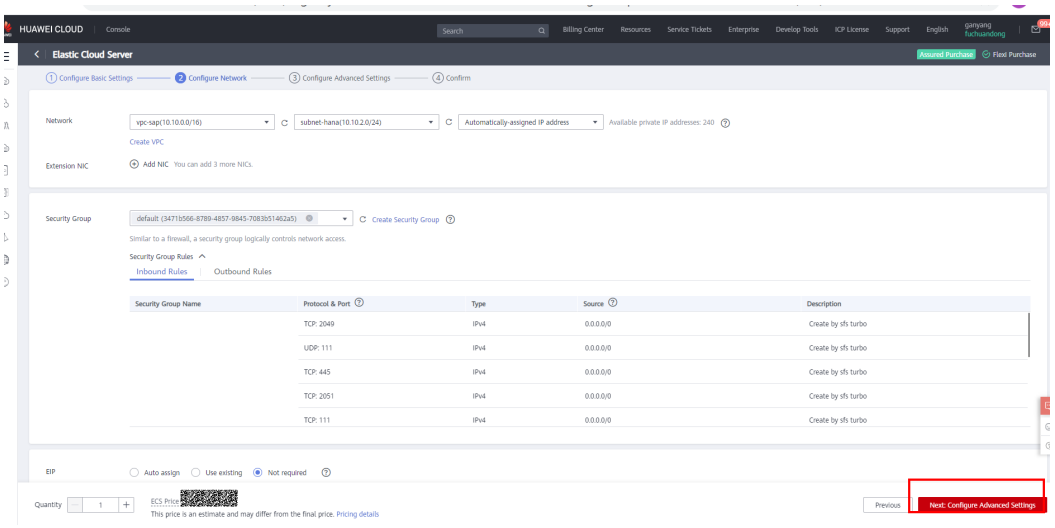
Step 2 Click **Buy ECS**.



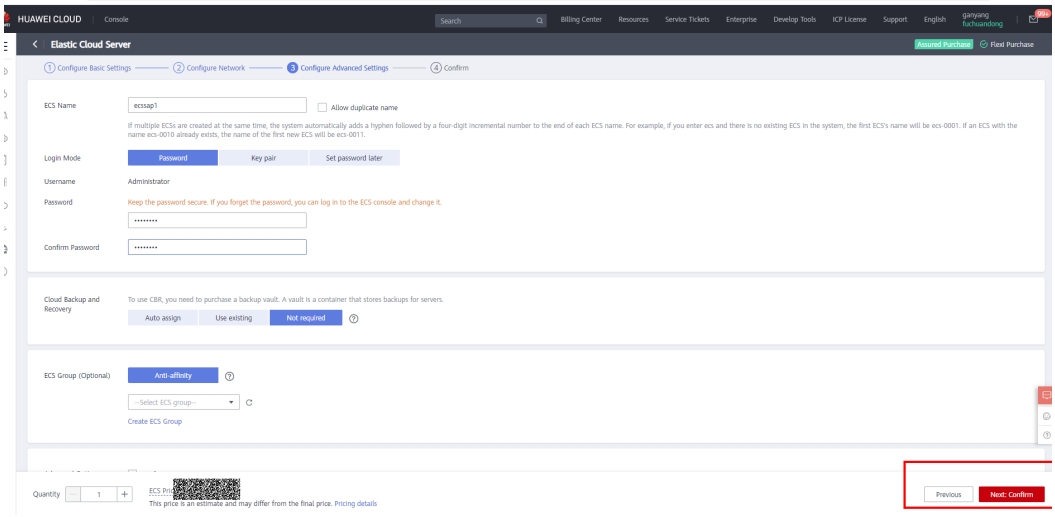
Step 3 Select the ECS flavor, image, and disk size based on #EN-US_TOPIC_0000001143628972/table127451133151718.



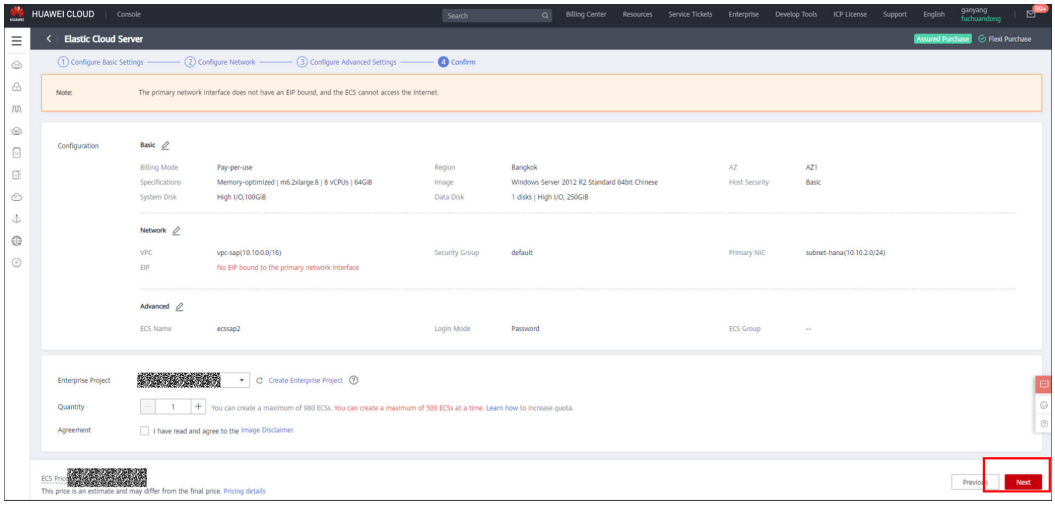
Step 4 Click **Next: Configure Network**. Select the created VPC and security group, confirm the configuration, and click **Next: Configure Advanced Settings**.



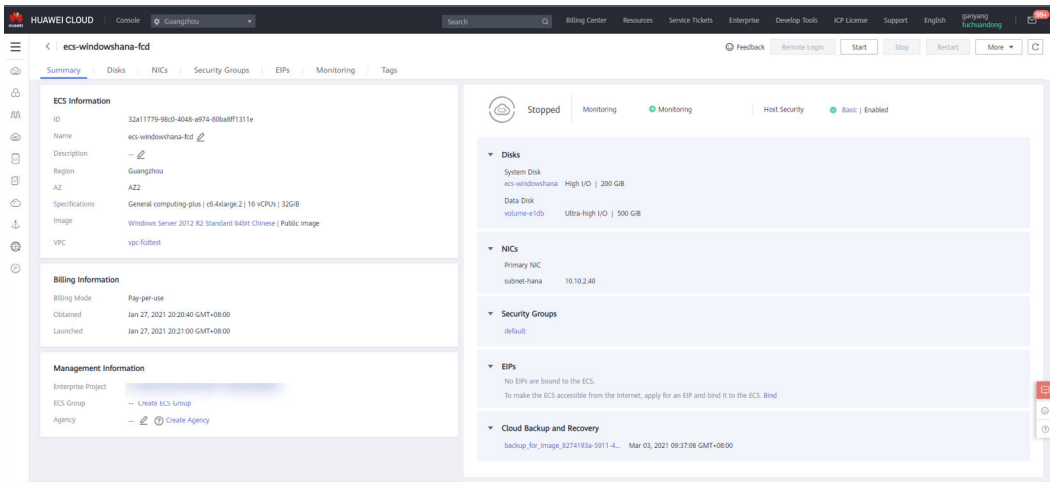
Step 5 Enter the ECS name and password of the **root** user, and click **Next: Confirm**.



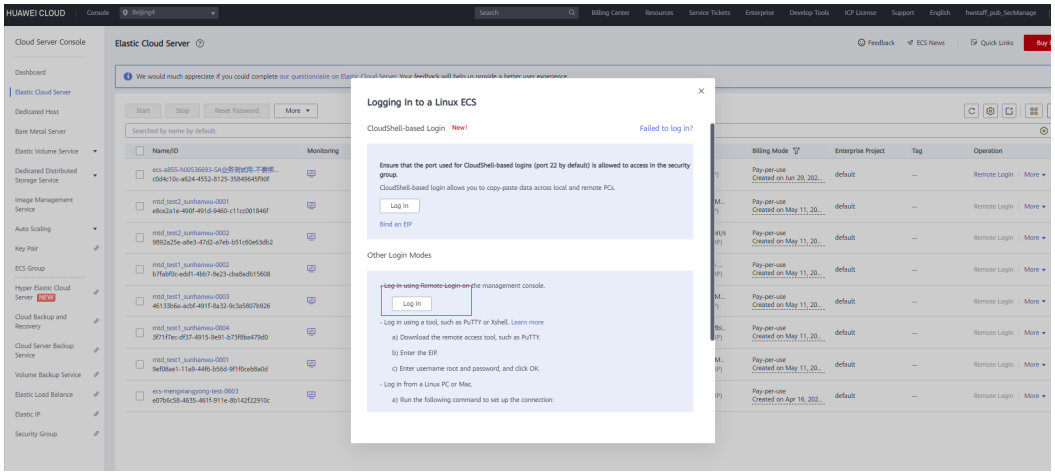
Step 6 Select an enterprise project and click **Next**.



Step 7 Create and purchase a Windows jump server.



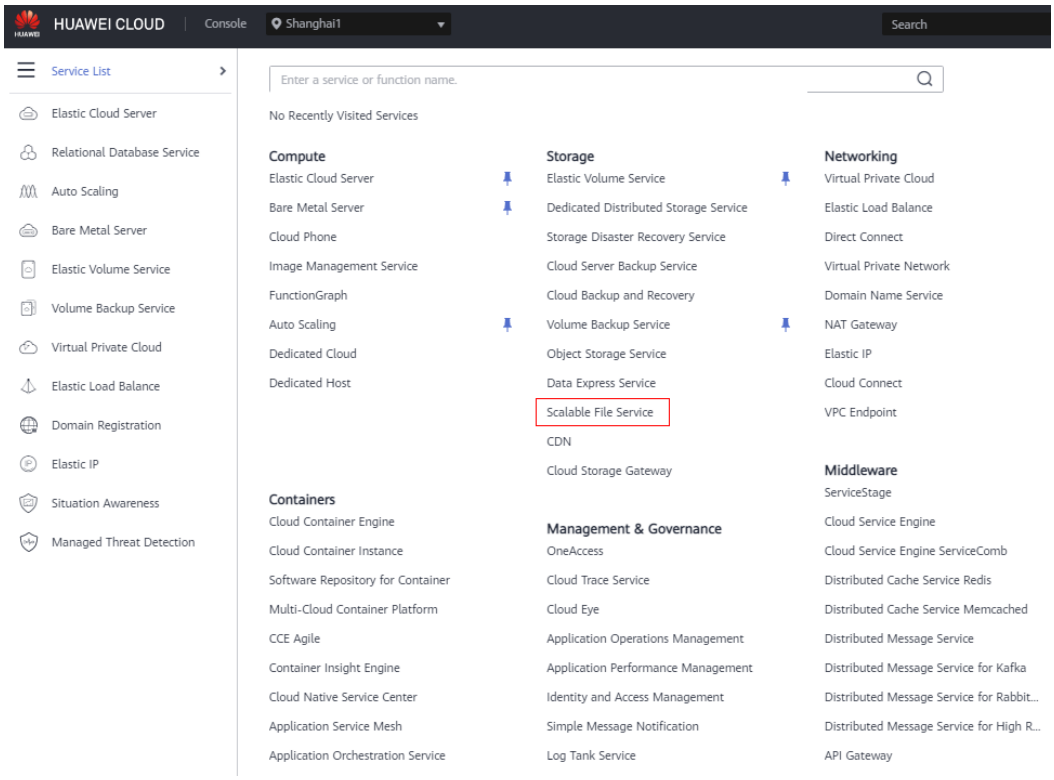
Step 8 After ECSs are created, locate the created ECSs in the ECS list and click **Remote Login** in the **Operation** column. Log in to the ECSs as user **root** using VNC.



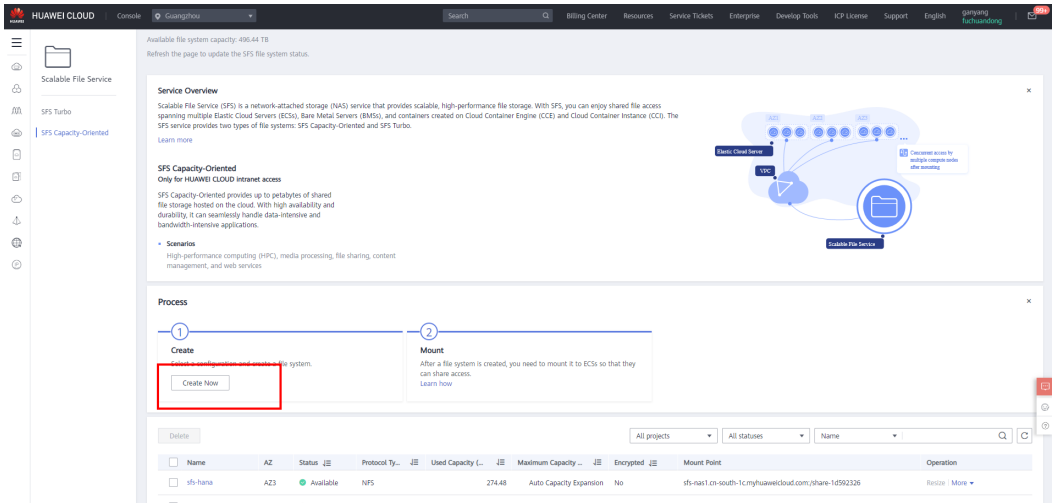
----End

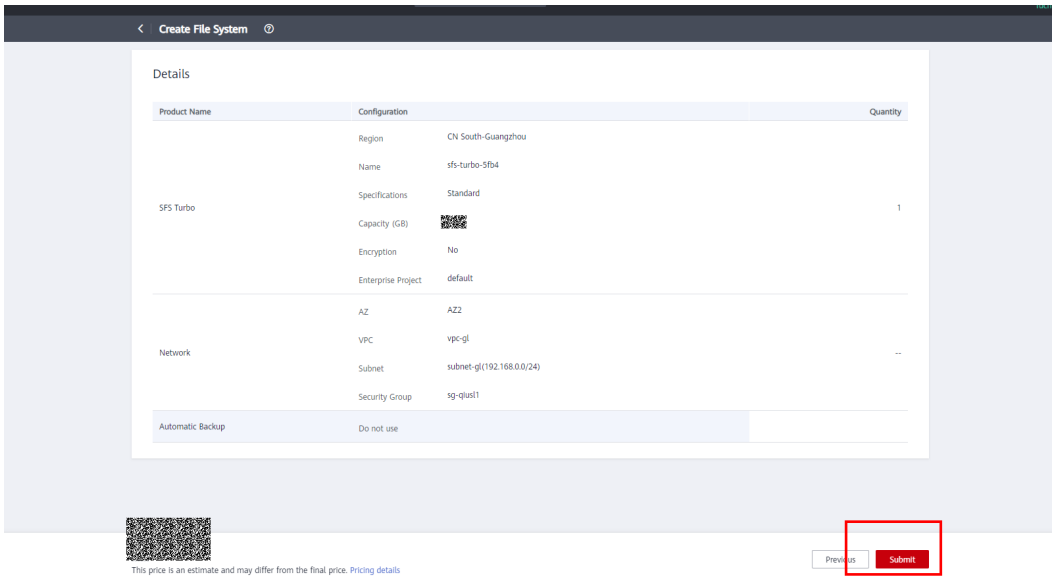
5.4.4 Purchasing and Mounting an SFS Disk

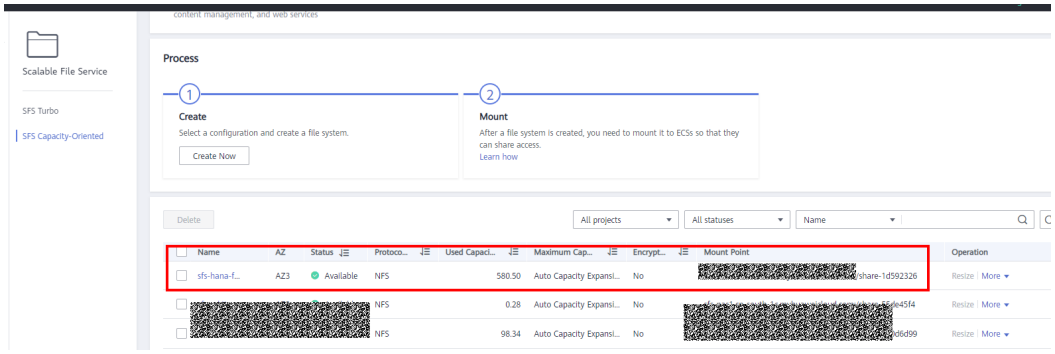
Step 1 Log in to the HUAWEI CLOUD management console, click the service list icon, and choose **Storage** > **Scalable File Service**.



Step 2 Create a file system and record the mount address.







Step 3 Log in to an ECS and create a folder.

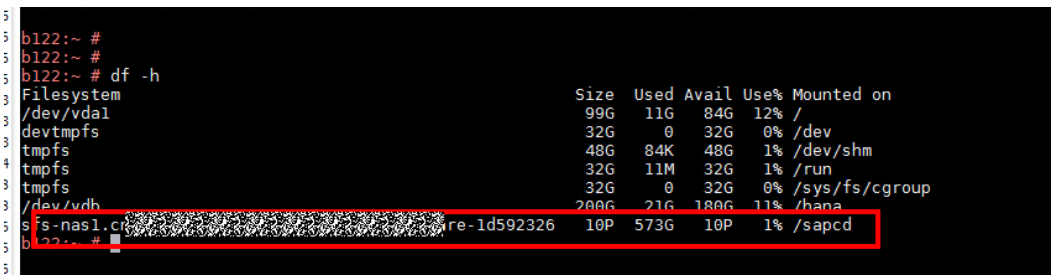
mkdir /sapcd

Step 4 Mount the **/db2sfs** directory to SFS.

echo "sfs-nas1.*:/share-cd3dc3c2 /sapcd nfs vers=3,timeo=600,nolock 1 2" >>/etc/fstab**

Run the **mount -a** command to mount the directory.

Step 5 Run the **df -h** command to view the mounting result.



----End

5.4.5 Creating a File System

Step 1 Run the **fdisk -l** command to check the unformatted disks.

Step 2 Format disks and logical volumes.

mkfs.xfs /dev/vdb

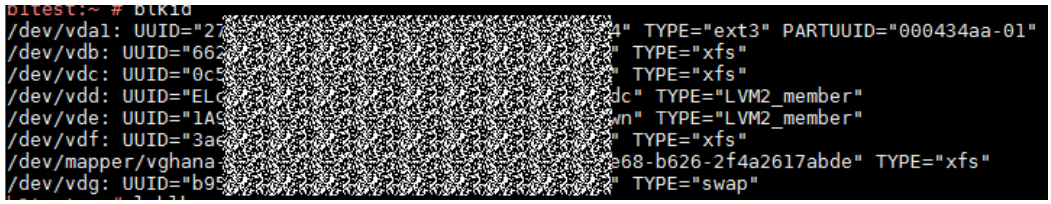
mkfs.xfs /dev/vdc

mkfs.xfs /dev/vde

Create a file system directory.

mkdir -p /usr/sap /hana/log /hana/data /hana/share

Run the **blkid** command to obtain the UUID of the disk.



Create mount points in **/etc/fstab**.

echo "UUID=662****81dbf9783 /usr/sap xfs defaults 0 0" >>/etc/fstab**

echo "UUID=0c5******19734f /hana/log xfs defaults 0 0" >>/etc/fstab**

echo "UUID=3ae****05166 /hana/share xfs defaults 0 0" >>/etc/fstab**

Step 3 Create LVM volumes.

Run the following commands:

pvcreate /dev/vdd /dev/vde

vgcreate vghana /dev/vdd /dev/vde

vgdisplay vghana

```
bltest:~ # vgdisplay vghana
  --- Volume group ---
  VG Name               vghana
  System ID
  Format                lvm2
  Metadata Areas        2
  Metadata Sequence No  4
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                1
  Open LV               1
  Max PV                0
  Cur PV                2
  Act PV                2
  VG Size               399.99 GiB
  PE Size               4.00 MiB
  Total PE              102398
  Alloc PE / Size       102398 / 399.99 GiB
  Free  PE / Size       0 / 0
  VG UUID               YN762R-Oo0S-gl8F-w42n-Jf07-UM2m-MkMnA2
```


lvcreate -i 2 -l 100%VG -n lvhanadata vghana

mkfs.xfs /dev/mapper/vghana-lvhanadata

uuid3=`blkid /dev/mapper/vghana-lvhanadata | awk '{print $2}'|awk -F"\"" '{print $2}'`

echo "UUID=$uuid3 /hana/data xfs defaults 0 0" >> /etc/fstab

Run the **mount -a** command to mount all disks and run the **df -h** command to check the disk mounting results.

```
/dev/vdg: UUID="b95b3d83-7ad6-444d-9cf2-1fee92fbc49f" TYPE="
[redacted] # lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
vda                 254:0    0  100G  0 disk
└─vda1              254:1    0  100G  0 part /
vdb                 254:16   0   80G  0 disk /usr/sap
vdc                 254:32   0  252G  0 disk /hana/log
vdd                 254:48   0  200G  0 disk
└─vghana-lvhanadata 253:0    0  400G  0 lvm  /hana/data
vde                 254:64   0  200G  0 disk
└─vghana-lvhanadata 253:0    0  400G  0 lvm  /hana/data
vdf                 254:80   0  300G  0 disk /hana/shared
vdg                 254:96   0   17G  0 disk [SWAP]
```

----End

5.4.6 Creating a SWAP Partition

Step 1 Use partitions/disks as the swap partition.

Run the following command to configure the swap partition.

mkswap /dev/vdg

Step 2 Run the following command to enable the swap partition.

swapon /dev/vdg

Step 3 Write the following information to **/etc/fstab**.

echo "UUID=43a73********d1f433 swap swap defaults 0 0" >> /etc/fstab**

Step 4 Run the following command to check the size of the current memory and swap space. The default unit is KB, and the unit of **-m** is MB

free -m

```
vdg                 254:96   0   17G  0 disk [SWAP]
[redacted] # free -m
             total       used       free     shared    buffers     cached
Mem:         64559       1227      63331         49         27        532
-/+ buffers/cache:        667      63892
Swap:        17407          0      17407
```

Step 5 Run the following command to check swap information, including detailed information about files and partitions.

swapon -s


```
[redacted]:~ # swapon -s
Filename                                Type            Size    Used    Priority
/dev/vdg                                partition       17825788        0       -1
b1test:~ #
```

----End

5.4.7 Configuring the hosts File

Configure the **hosts** file. During SAP software installation, the SAP software automatically maps host names to IP addresses.

Step 1 Run the **vi /etc/hosts** command to add the IP addresses mapped to the host names.

```
#
127.0.0.1       localhost

# special IPv6 addresses
::1             localhost ipv6-localhost ipv6-loopback

fe00::0         ipv6-localnet

ff00::0         ipv6-mcastprefix
ff02::1         ipv6-allnodes
ff02::2         ipv6-allrouters
ff02::3         ipv6-allhosts
10.10.1.178    b122
```

----End

5.5 Installing Software

5.5.1 Installing SAP HANA

For details about how to install and deploy SAP HANA, see the SAP standard documents and **SAP HANA User Guide (Single-Node Deployment)**.

Note: The client, server, and afl components need to be installed during SAP HANA installation.

Step 1 Install the server component.

Download the SAP HANA installation package from the official website and decompress it. Go to the **DATA_UNITS/HDB_SERVER_LINUX_X86_64** directory, and run the **./hdblcm --ignore=check_signature_file** command. During the installation, configure required parameters.


```
b122:/sapcd/B1/HANA/51050929/DATA_UNITS/SAPHANADATABASE1.0FORB1/LINX64SUSE/SAP_HANA_DATABASE # vi /etc/hosts
b122:/sapcd/B1/HANA/51050929/DATA_UNITS/SAPHANADATABASE1.0FORB1/LINX64SUSE/SAP_HANA_DATABASE # ./hdblcm --ignore=check_signature_file


SAP HANA Lifecycle Management - SAP HANA 1.00.122.03.1475845474
************************************************************


Scanning Software Locations...
Detected components:
    SAP HANA Database (1.00.122.03.1475845474) in /sapcd/B1/HANA/51050929/DATA_UNITS/SAPHANADATABASE1.0FORB1/LINX64SUSE/SAP_HANA_DATABASE/server



Choose installation

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

Enter selected system index [3]: 1

Enter Installation Path [/hana/shared]:
Enter Local Host Name [b122]:
Do you want to add additional hosts to the system? (y/n) [n]:
Enter SAP HANA System ID: HDX
Enter Instance Number [00]:

  Index | Database Mode       | Description
  ------------------------------------------------------------------------------------------
  1     | single_container    | The system contains one database
  2     | multiple_containers | The system contains one system database and 1..n tenant databases

Select Database Mode / Enter Index [1]: 1

  Index | System Usage | Description
  ---------------------------------------------------------------------------
  1     | production   | System is used in a production environment
  2     | test         | System is used for testing, not production
  3     | development  | System is used for development, not production
  4     | custom       | System usage is neither production, test nor development

Select System Usage / Enter Index [4]: 1
Enter Location of Data Volumes [/hana/data/HDX]:
Enter Location of Log Volumes [/hana/log/HDX]:
```

```
Select System Usage / Enter Index [4]: 1
Enter Location of Data Volumes [/hana/data/HDX]:
Enter Location of Log Volumes [/hana/log/HDX]:
Restrict maximum memory allocation? [n]:
Enter Certificate Host Name For Host 'b122' [b122]:
Enter SAP Host Agent User (sapadm) Password:
Confirm SAP Host Agent User (sapadm) Password:
Enter System Administrator (hdxadm) Password:
Confirm System Administrator (hdxadm) Password:
Enter System Administrator Home Directory [/usr/sap/HDX/home]:
Enter System Administrator Login Shell [/bin/sh]:
Enter System Administrator User ID [1001]:
Enter ID of User Group (sapsys) [79]:
Enter Database User (SYSTEM) Password:
Confirm Database User (SYSTEM) Password:
Restart system after machine reboot? [n]:

Summary before execution:
=========================

SAP HANA Components Installation
   Installation Parameters
      Remote Execution: ssh
      Installation Path: /hana/shared
      Local Host Name: b122
      SAP HANA System ID: HDX
      Instance Number: 00
      Database Mode: single_container
      System Usage: production
      Location of Data Volumes: /hana/data/HDX
      Location of Log Volumes: /hana/log/HDX
      Certificate Host Names: b122 -> b122
      System Administrator Home Directory: /usr/sap/HDX/home
      System Administrator Login Shell: /bin/sh
      System Administrator User ID: 1001
      ID of User Group (sapsys): 79
   Software Components
      SAP HANA Database
         Install version 1.00.122.03.1475845474
         Location: /sapcd/B1/HANA/51050929/DATA_UNITS/SAPHANADATABASE1.0FORB1/LINX64SUSE/SAP_HANA_DATABASE/server

Do you want to continue? (y/n): y
```



```
  Installing package 'Kr05 Runtime'...
  Installing package 'Installer'...
  Installing package 'Ini Files'...
  Installing package 'HWCCT'...
  Installing package 'Emergency Support Package'...
  Installing package 'EPM'...
  Installing package 'Documentation'...
  Installing package 'Delivery Units'...
  Installing package 'DAT Languages'...
  Installing package 'DAT Configfiles'...
  Creating instance...
  Starting SAP HANA Database system...
  Starting 7 processes on host 'b122' (worker):
      Starting on 'b122': hdbcompileserver, hdbdaemon, hdbindexserver, hdbnameserver, hdbpreprocessor, hdbwebdispatcher, hdbxsengine
      Starting on 'b122': hdbdaemon, hdbindexserver, hdbwebdispatcher, hdbxsengine
      Starting on 'b122': hdbdaemon, hdbwebdispatcher, hdbxsengine
      Starting on 'b122': hdbdaemon, hdbwebdispatcher
    All server processes started on host 'b122' (worker).
  Importing delivery units...
  Importing delivery unit HCO_INA_SERVICE
  Importing delivery unit HANA_DT_BASE
  Importing delivery unit HANA_IDE_CORE
  Importing delivery unit HANA_TA_CONFIG
  Importing delivery unit HANA_UI_INTEGRATION_SVC
  Importing delivery unit HANA_UI_INTEGRATION_CONTENT
  Importing delivery unit HANA_XS_BASE
  Importing delivery unit HANA_XS_DBUTILS
  Importing delivery unit HANA_XS_EDITOR
  Importing delivery unit HANA_XS_IDE
  Importing delivery unit HANA_XS_LM
  Importing delivery unit HDC_ADMIN
  Importing delivery unit HDC_BACKUP
  Importing delivery unit HDC_IDE_CORE
  Importing delivery unit HDC_SEC_CP
  Importing delivery unit HDC_XS_BASE
  Importing delivery unit HDC_XS_LM
  Importing delivery unit SAPUI5_1
  Importing delivery unit SAP_WATT
  Importing delivery unit HANA_BACKUP
  Importing delivery unit HANA_HDBLCM
  Importing delivery unit HANA_SEC_BASE
  Importing delivery unit HANA_SEC_CP
  Importing delivery unit HANA_ADMIN
  Importing delivery unit HANA_WKLD_ANLZ
Installing Resident hdblcm...
Updating SAP HANA Instance Integration on Local Host...
  Regenerating SSL certificates...
  Deploying SAP Host Agent configurations...
Creating Component List...
SAP HANA system installed
You can send feedback to SAP with this form: https://b122:1129/lmsl/HDBLCM/HDX/feedback/feedback.html
Log file written to '/var/tmp/hdb_HDX_hdblcm_install_2021-08-06_09.43.07/hdblcm.log' on host 'b122'.
```

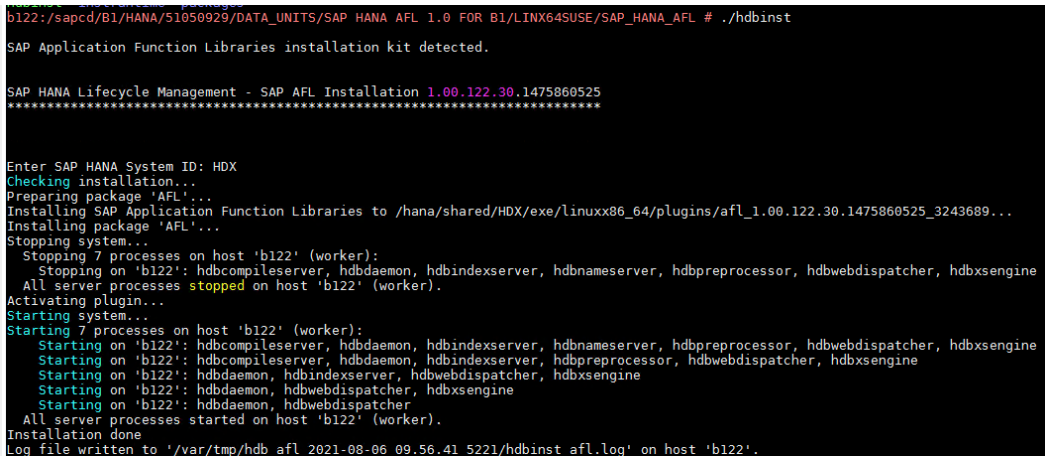
Step 2 Install the client component.

Run the **./hdbinst** command in the installation directory.

```
b122:/sapcd/B1/HANA/51050929/DATA_UNITS/SAPHANACLIENT1.0FORB1/LINX64SUSE/SAP_HANA_CLIENT # ./hdbinst

SAP HANA Database Client installation kit detected.


SAP HANA Lifecycle Management - Client Installation 1.00.120.042.1474657934
************************************************************************



Enter Installation Path [/usr/sap/hdbclient]:
Checking installation...
Preparing package 'Python Runtime'...
Preparing package 'Product Manifest'...
Preparing package 'SQLDBC'...
Preparing package 'REPOTOOLS'...
Preparing package 'Python DB API'...
Preparing package 'ODBC'...
Preparing package 'JDBC'...
Preparing package 'HALM Client'...
Preparing package 'Client Installer'...
Installing SAP HANA Database Client to /usr/sap/hdbclient...
Installing package 'Python Runtime'...
Installing package 'Product Manifest'...
Installing package 'SQLDBC'...
Installing package 'REPOTOOLS'...
Installing package 'Python DB API'...
Installing package 'ODBC'...
Installing package 'JDBC'...
Installing package 'HALM Client'...
Installing package 'Client Installer'...
Installation done
Log file written to '/var/tmp/hdb_client_2021-08-06_09.52.49_4878/hdbinst_client.log' on host 'b122'.
```

Step 3 Install the afl component.

In the installation directory, run the **./hdbinst** command and enter **SID**.



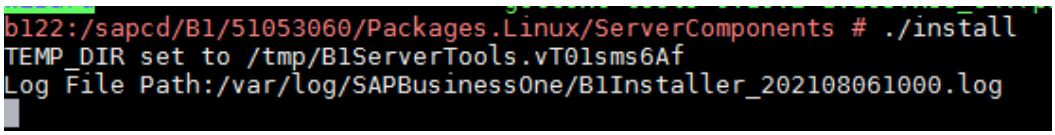
----End

5.5.2 Installing SAP Business One

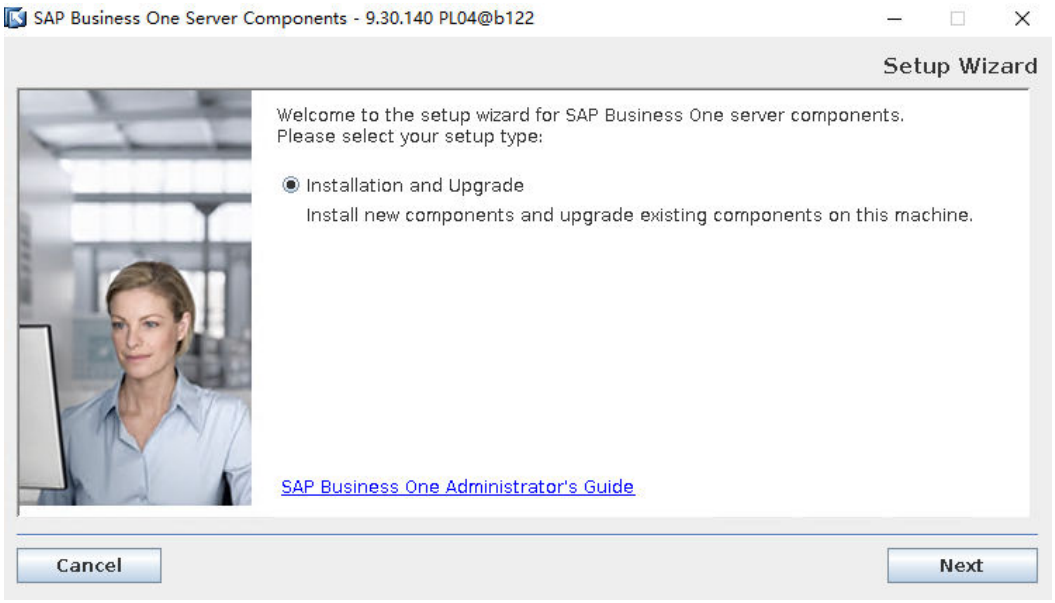
Before installing SAP Business One, modify the configurations on the target server. For details, see **What Should I Do If a SAP Application on an ECS Cannot Be Started?**.

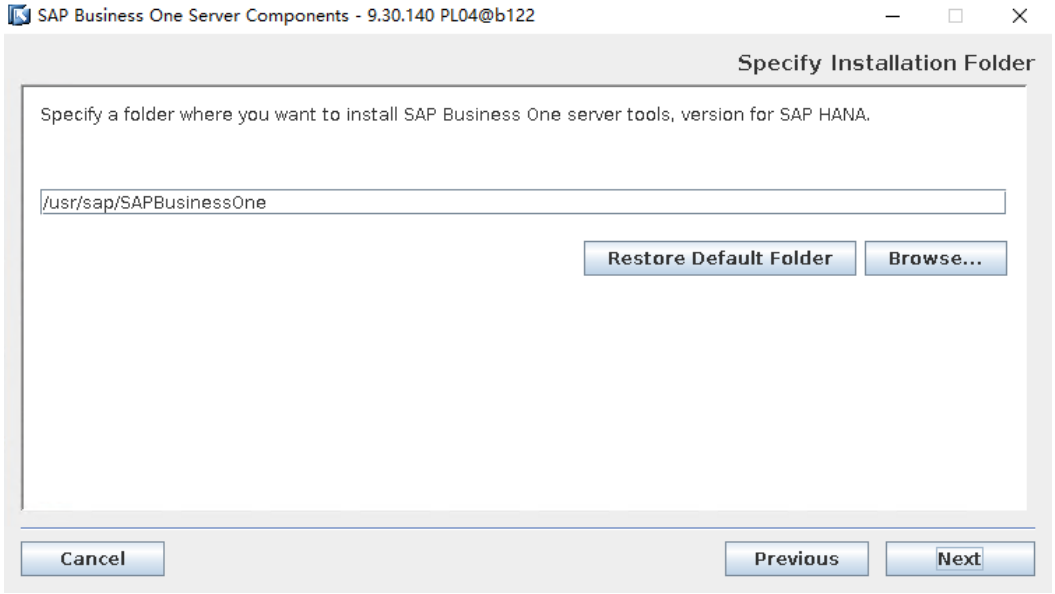
For details about how to install SAP Business One, see standard SAP documents. For more information, visit **https://support.sap.com/en/offerings-programs/support-small-medium-enterprises/business-one.html**.

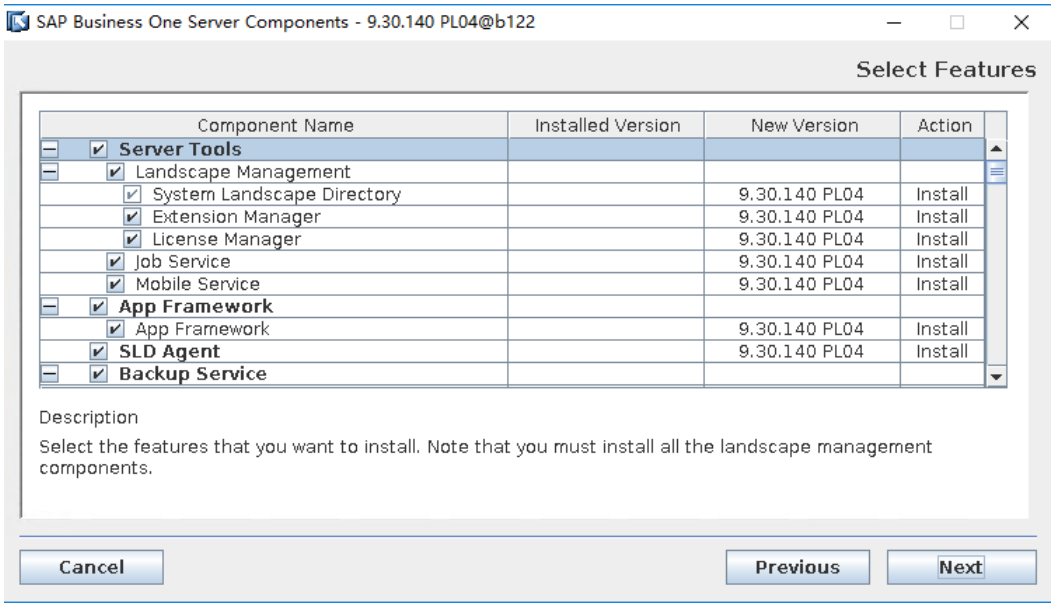
Step 1 Download the installation package from the SAP official website, decompress the package, go to the **Packages.Linux/ServerComponents** directory, and run the **./install** command to install SAP Business One.

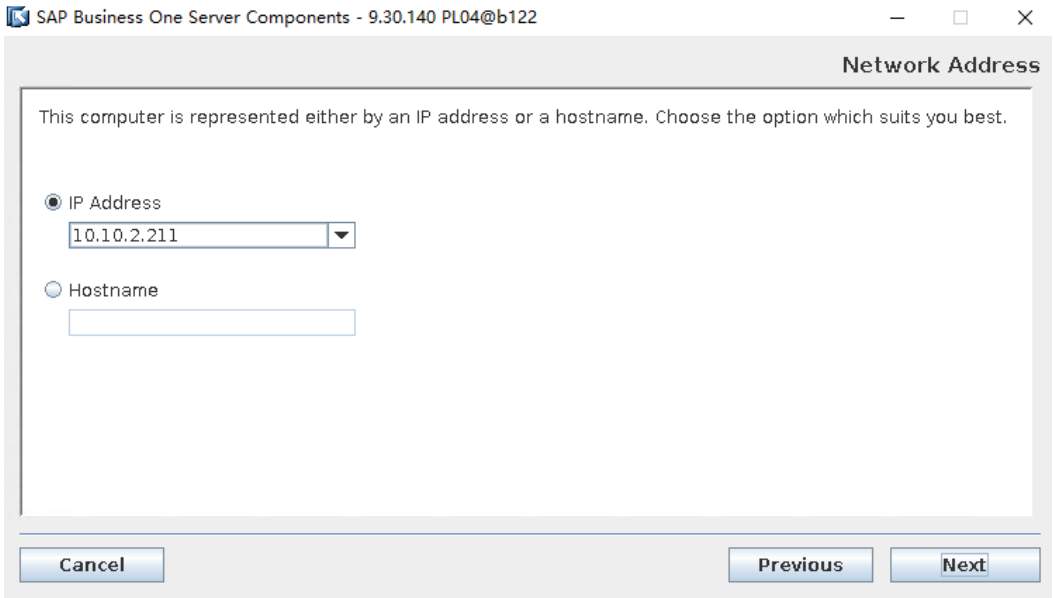


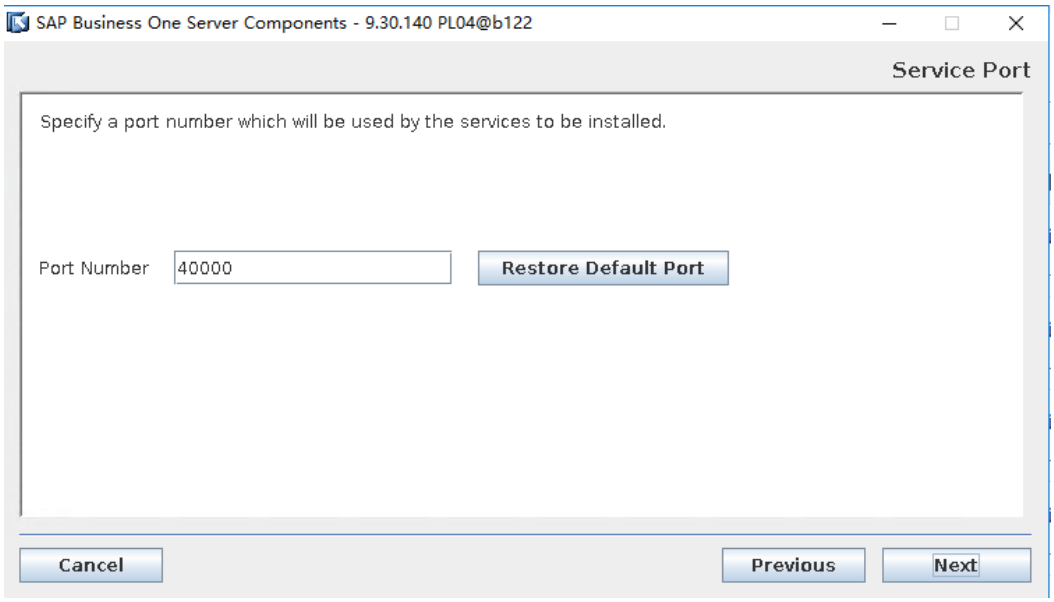
Step 2 The graphical installation interface is displayed. Configure the required parameter based on the site requirements.

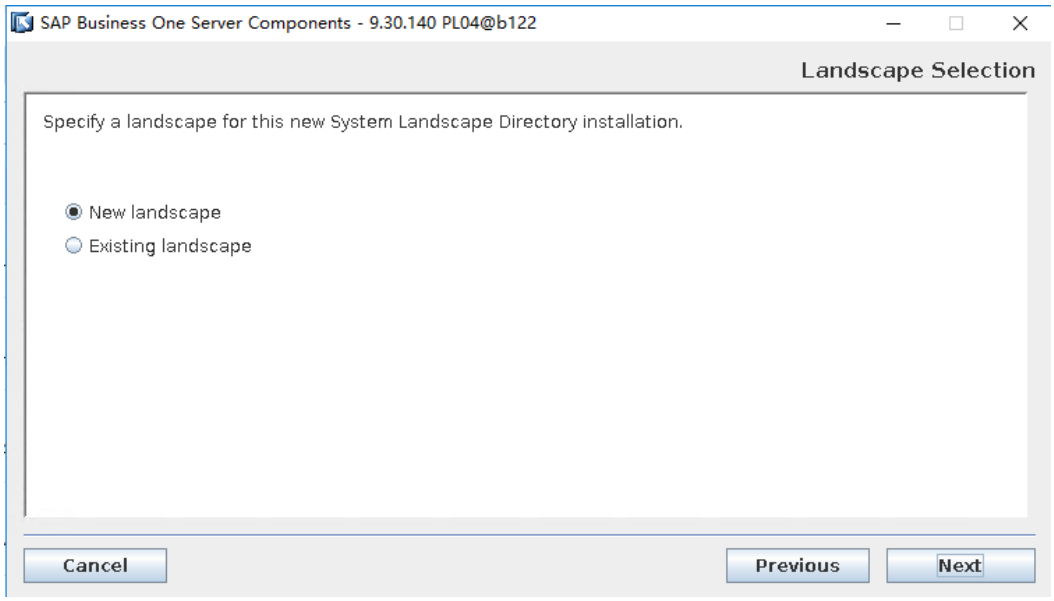


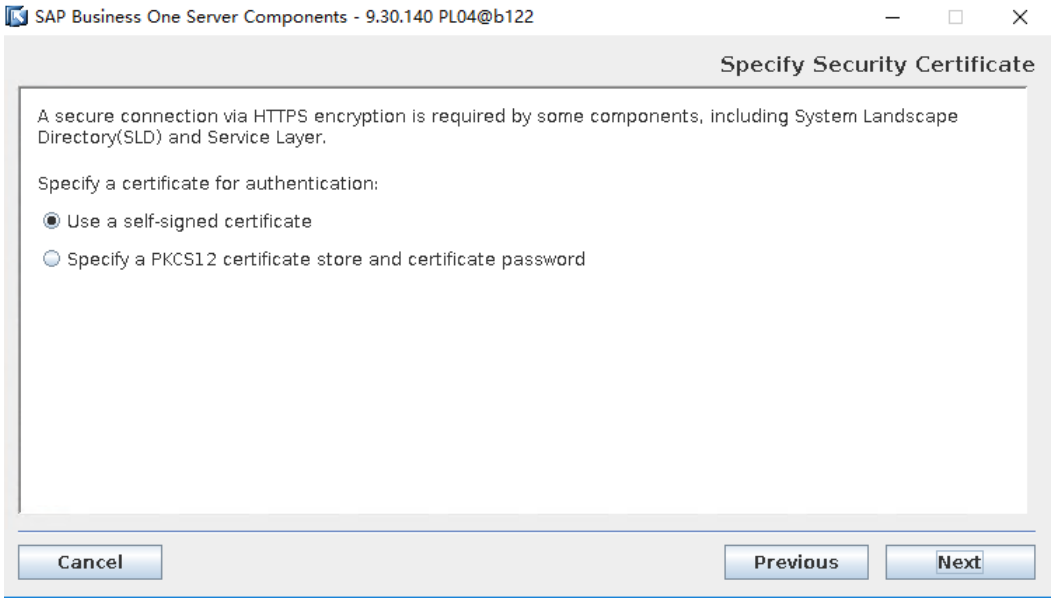


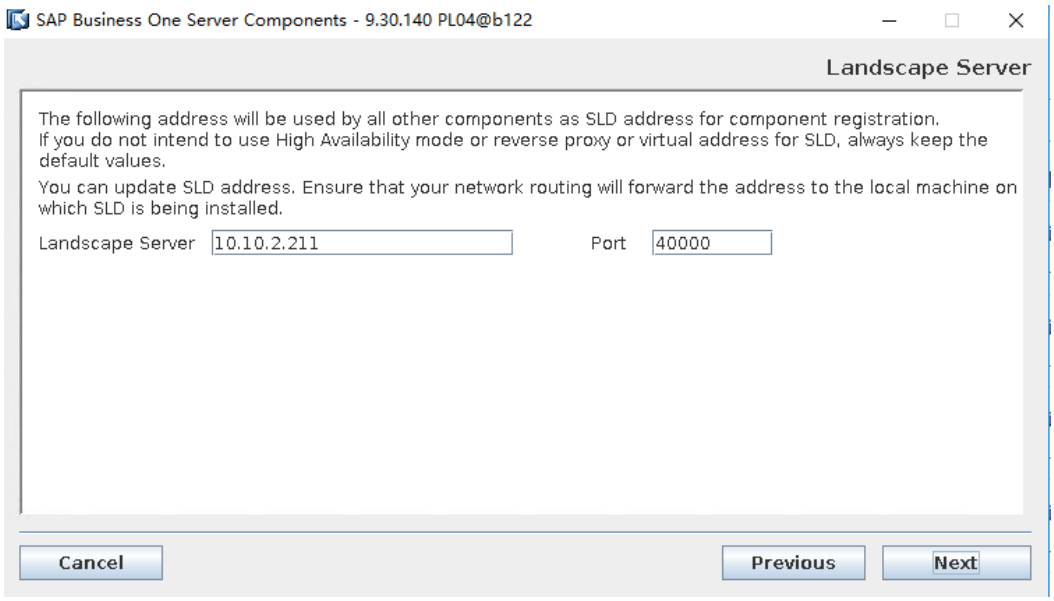


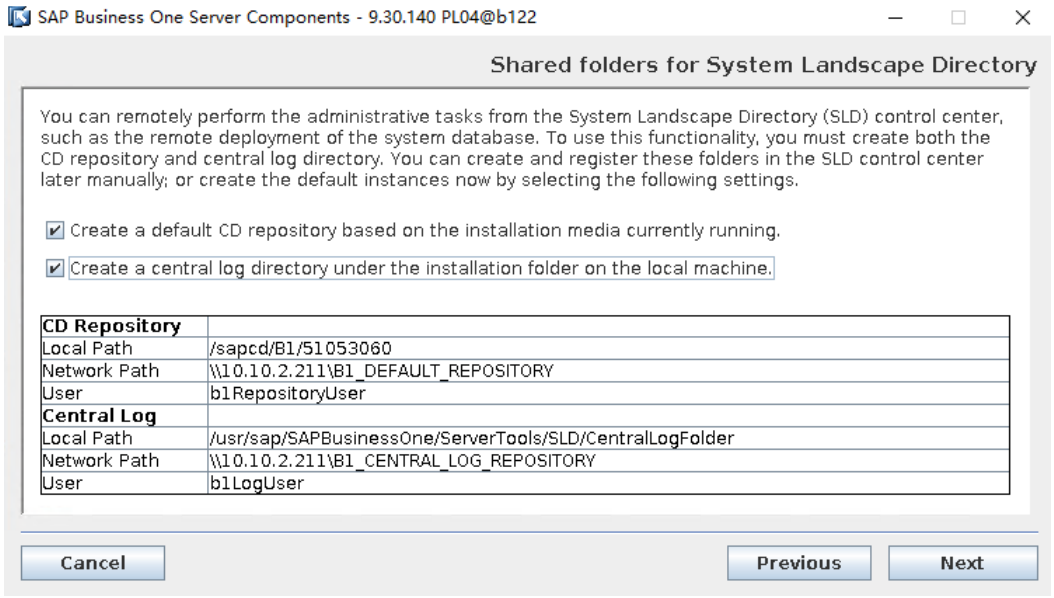


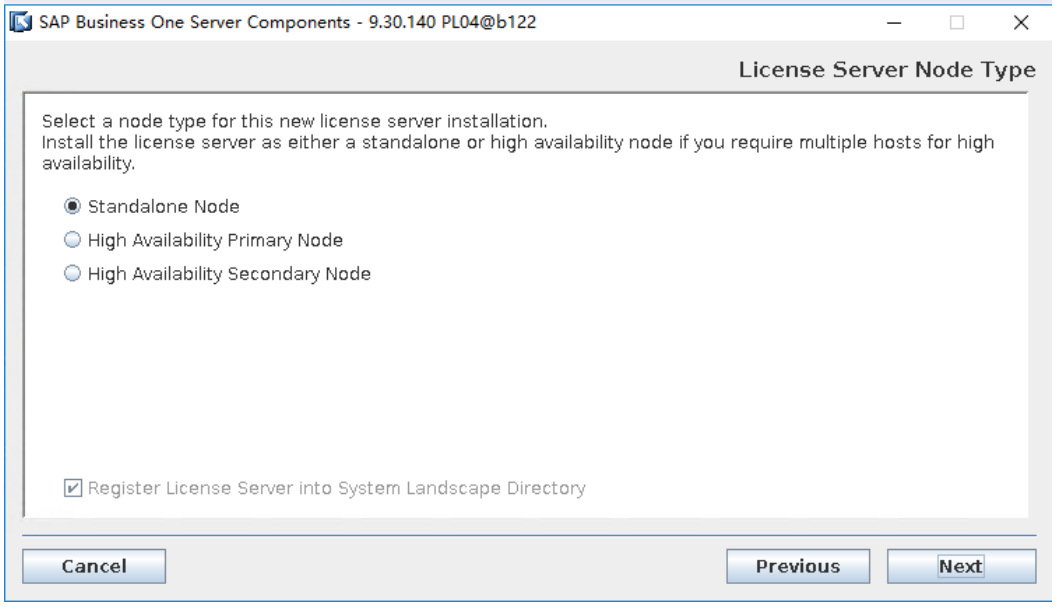


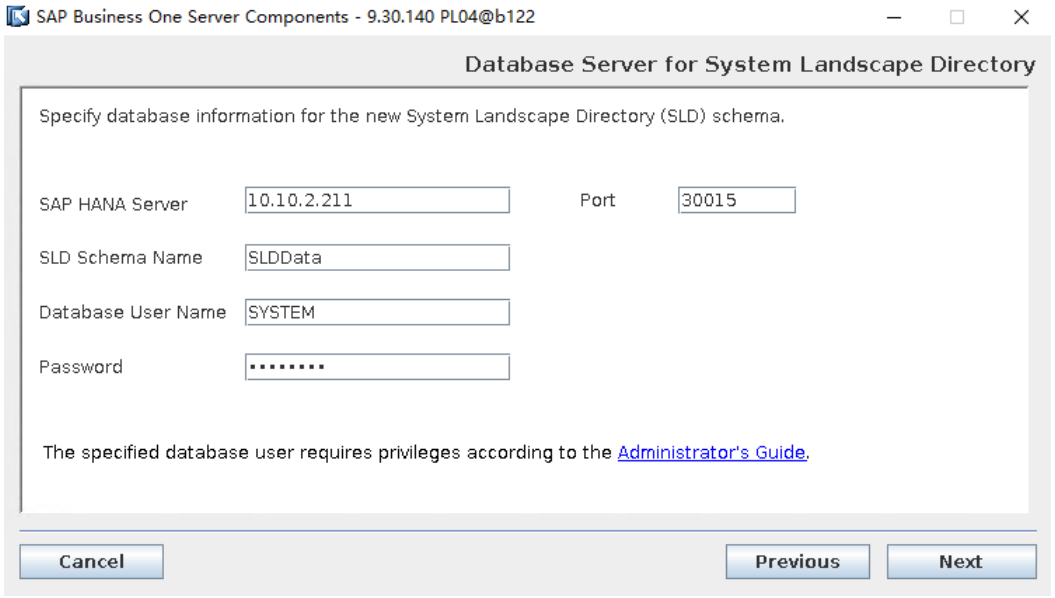


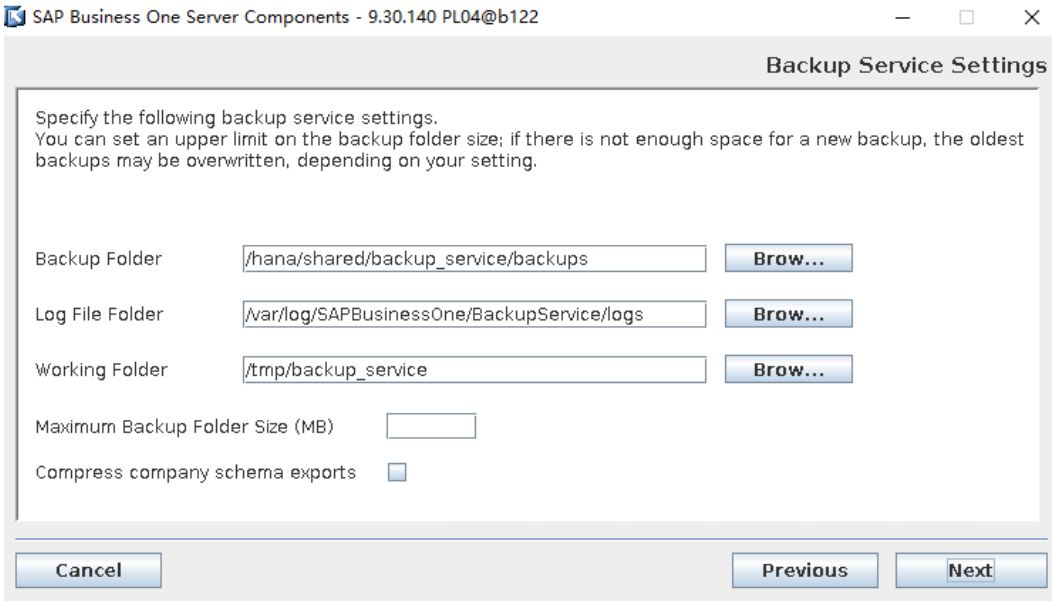


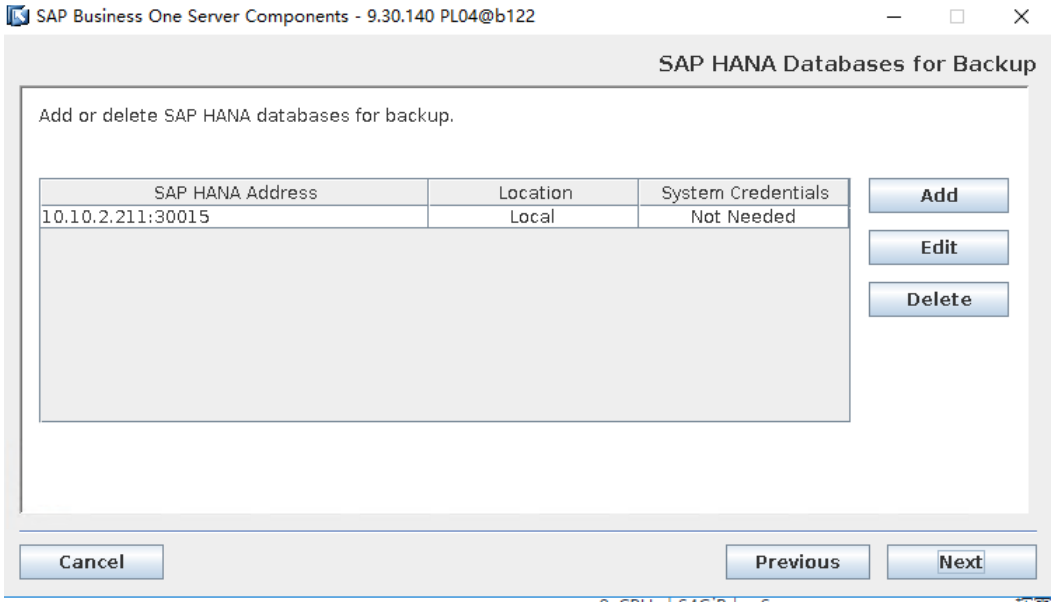


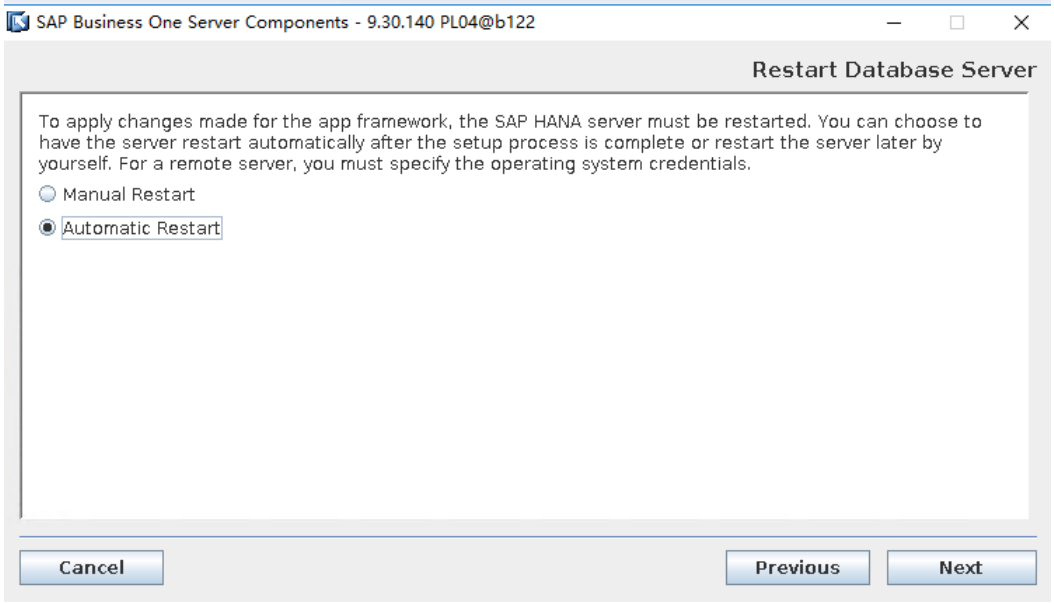


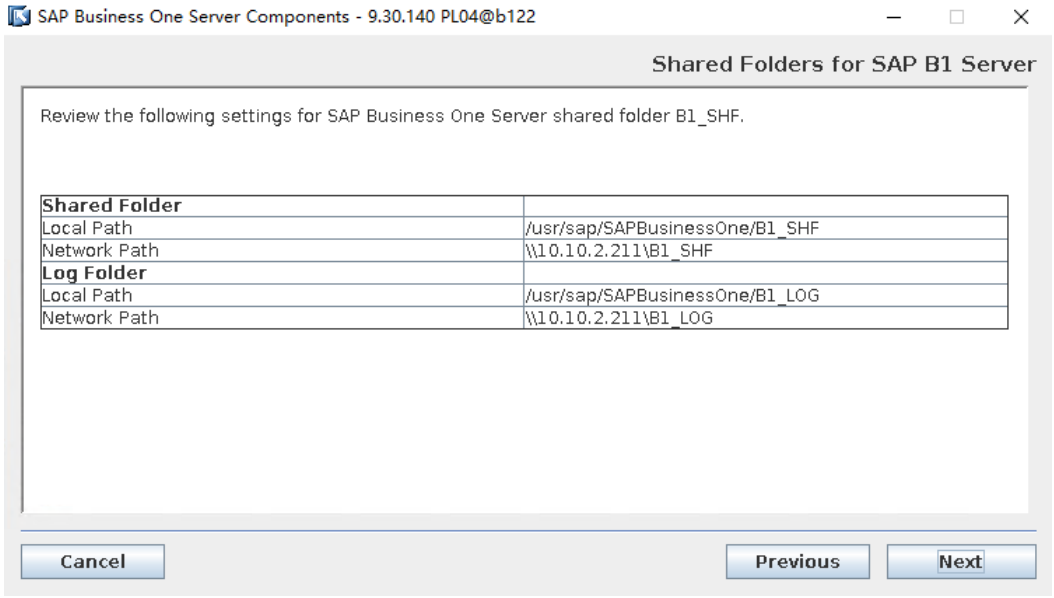


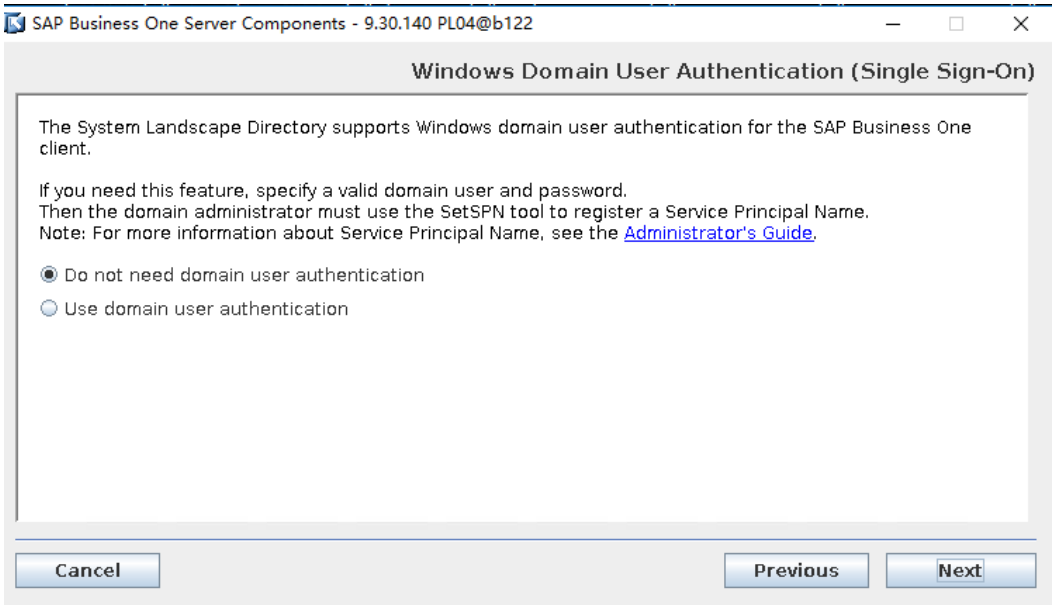


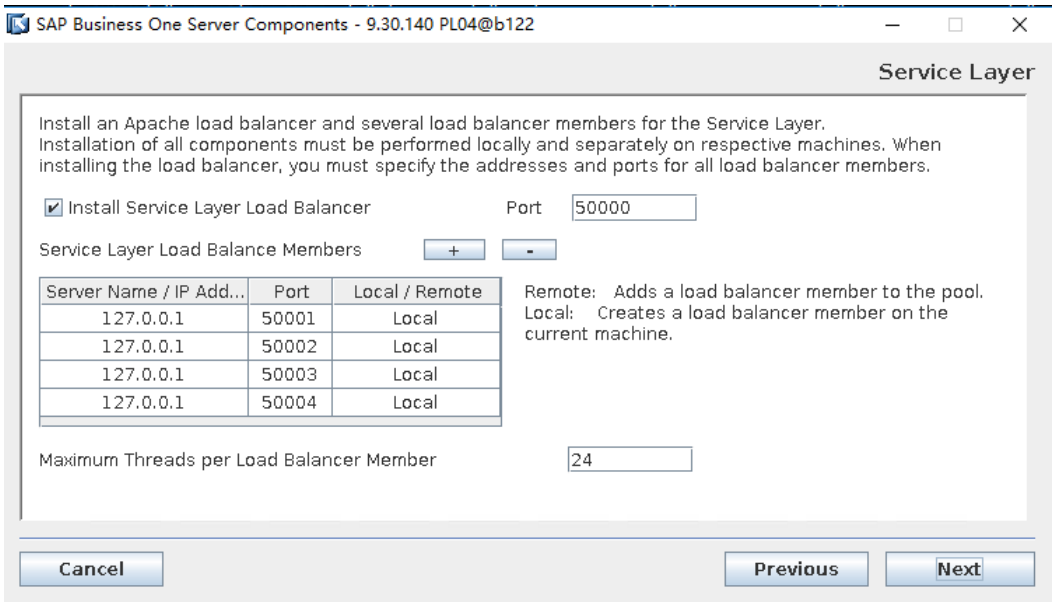


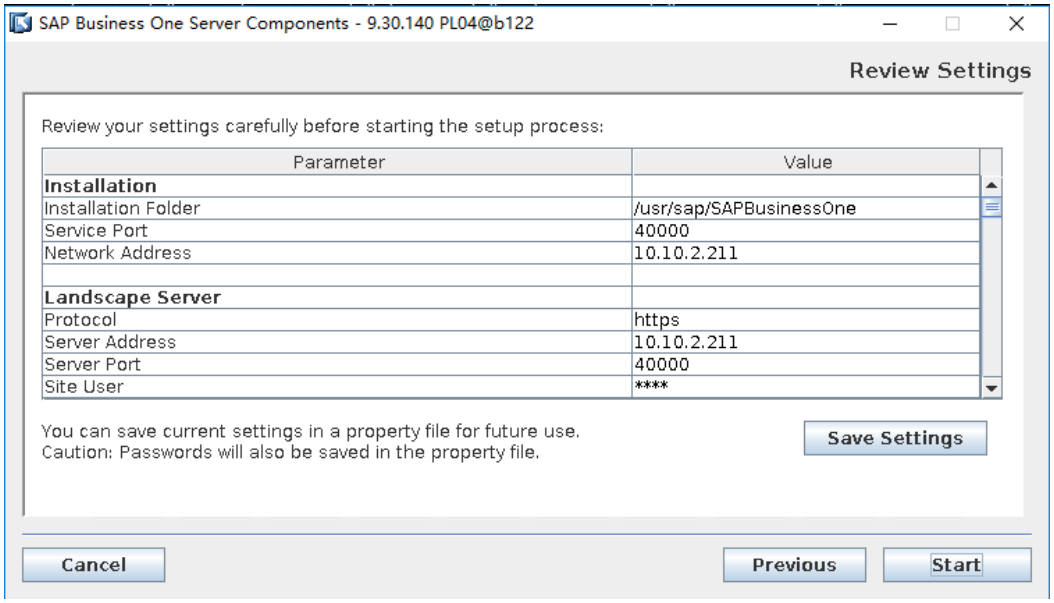


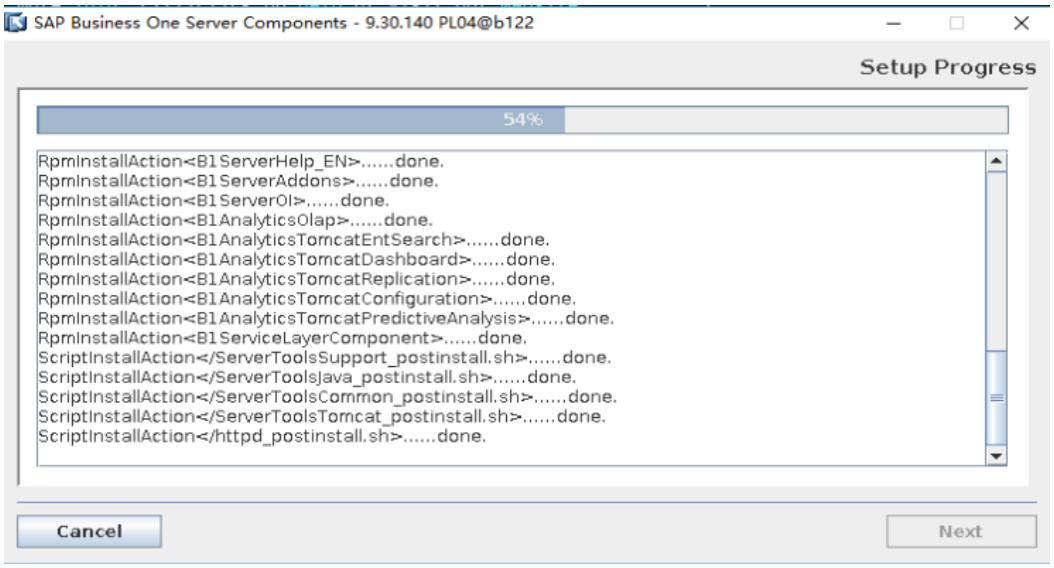


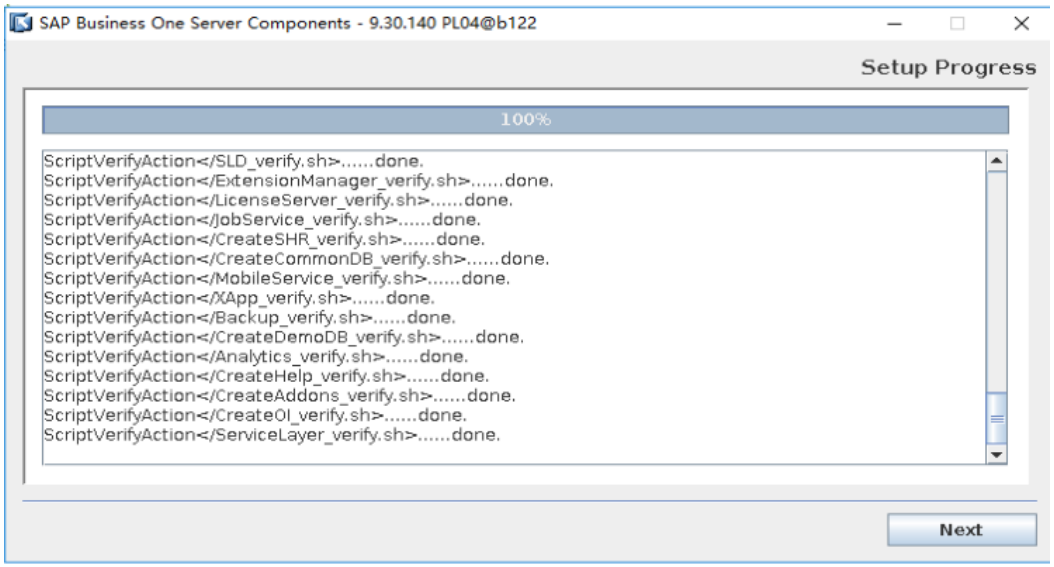


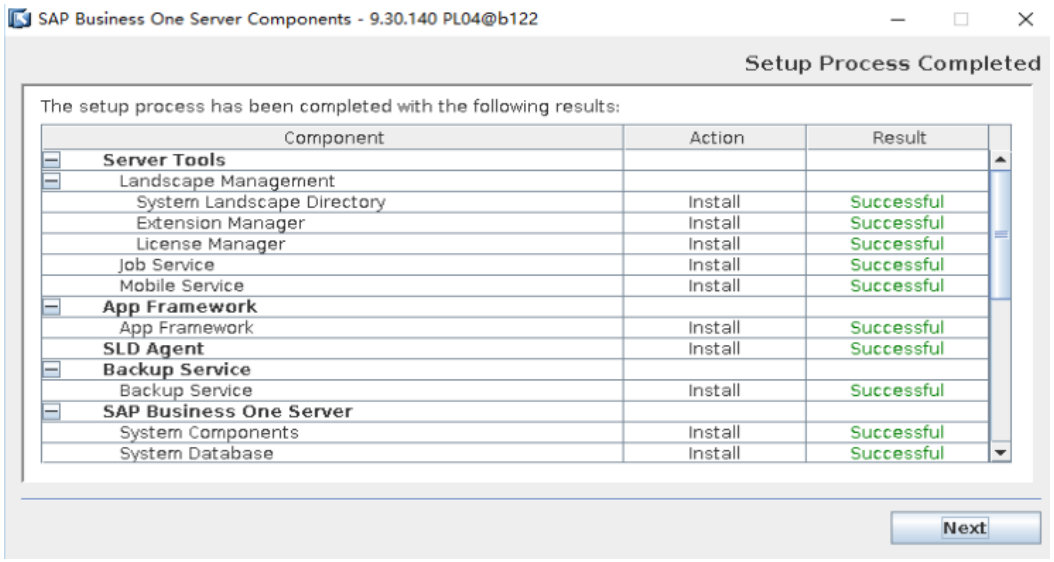


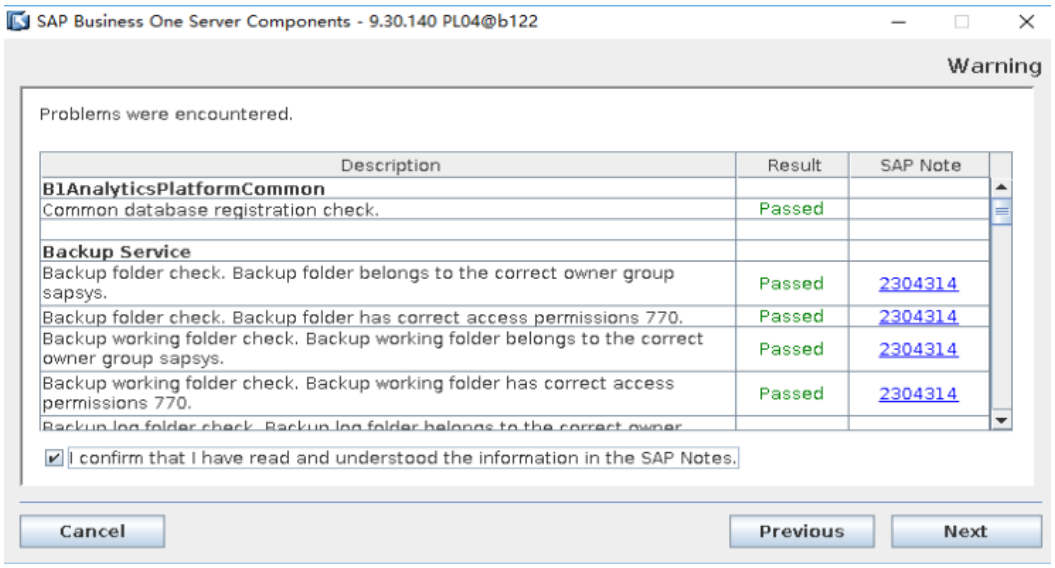


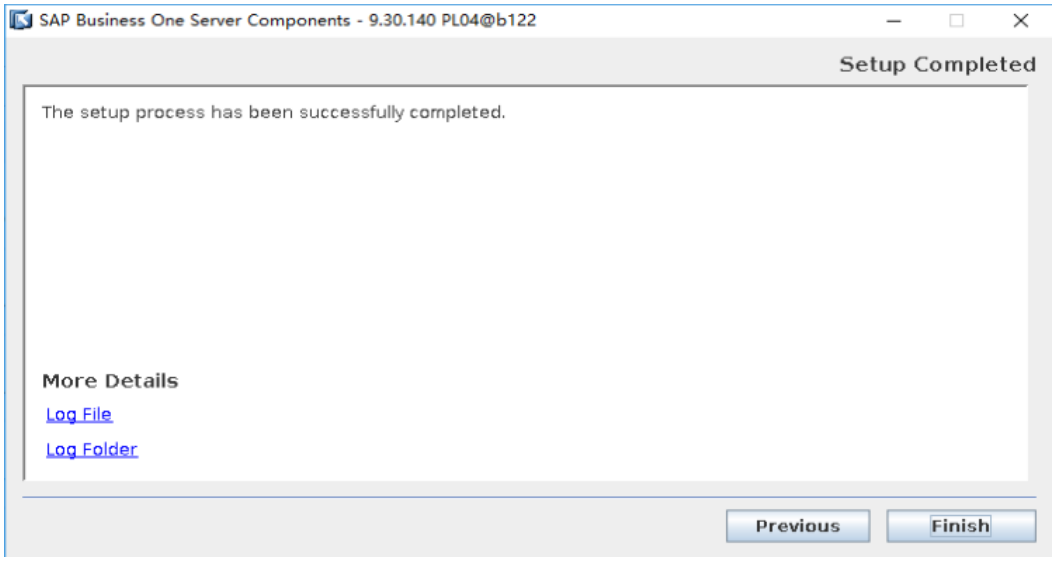










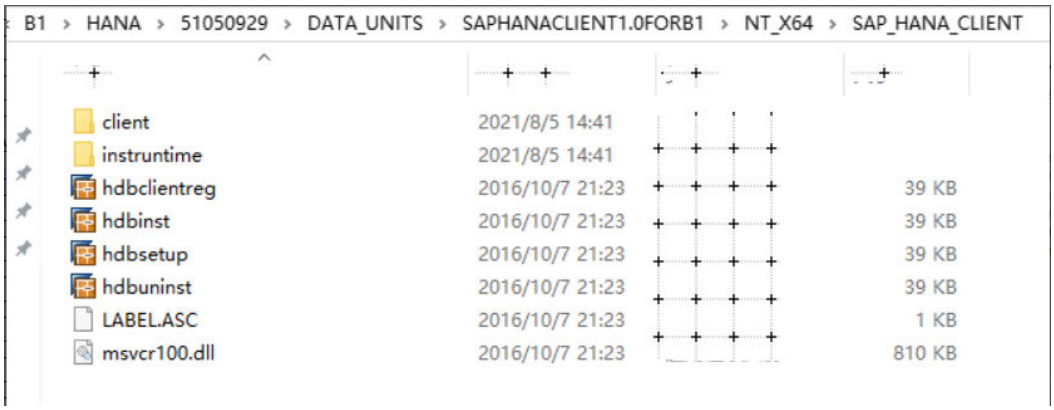


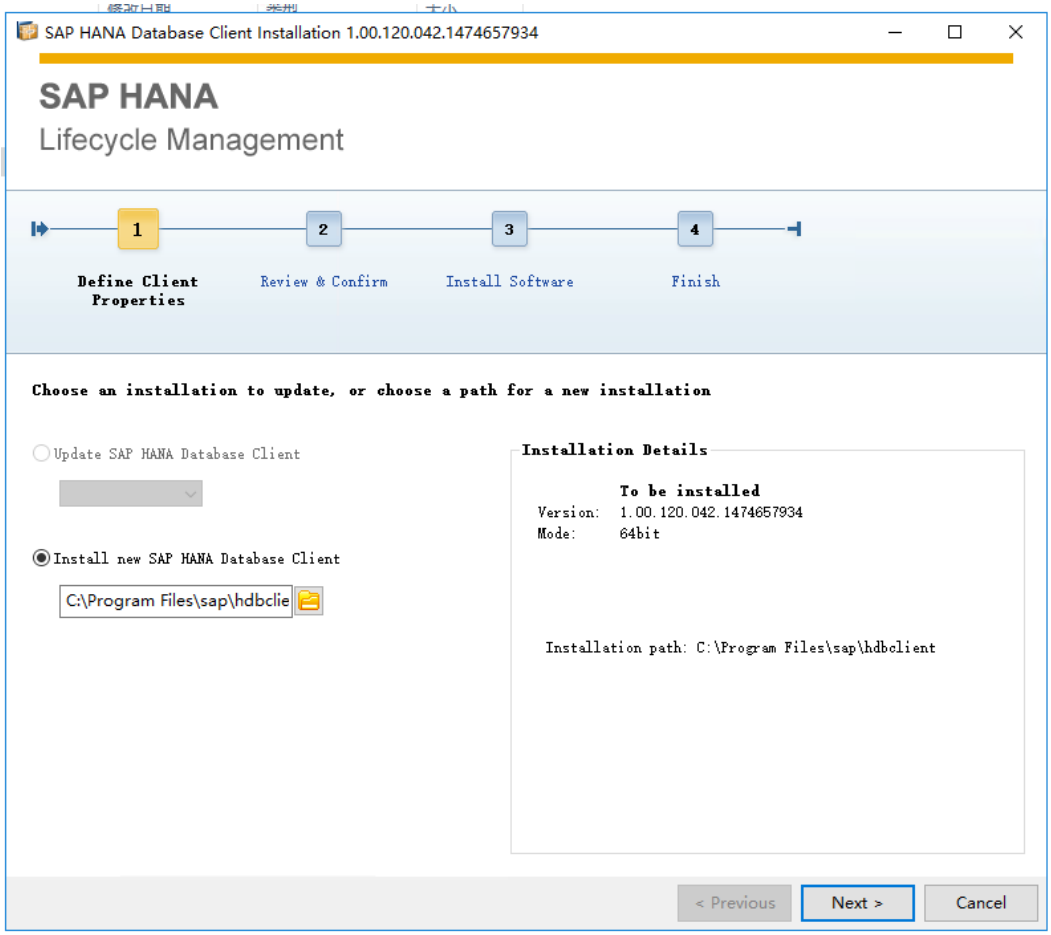
----End

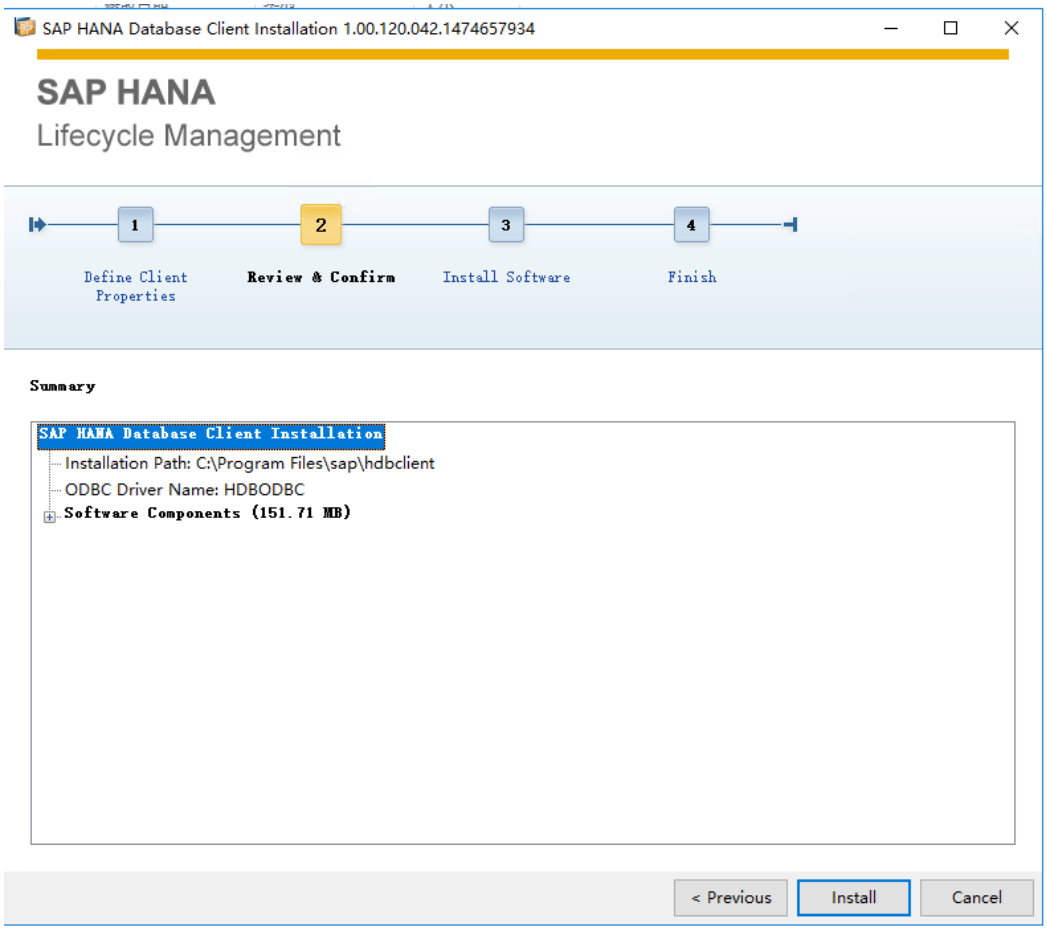
5.5.3 Installing the SAP HANA and SAP Business One Clients

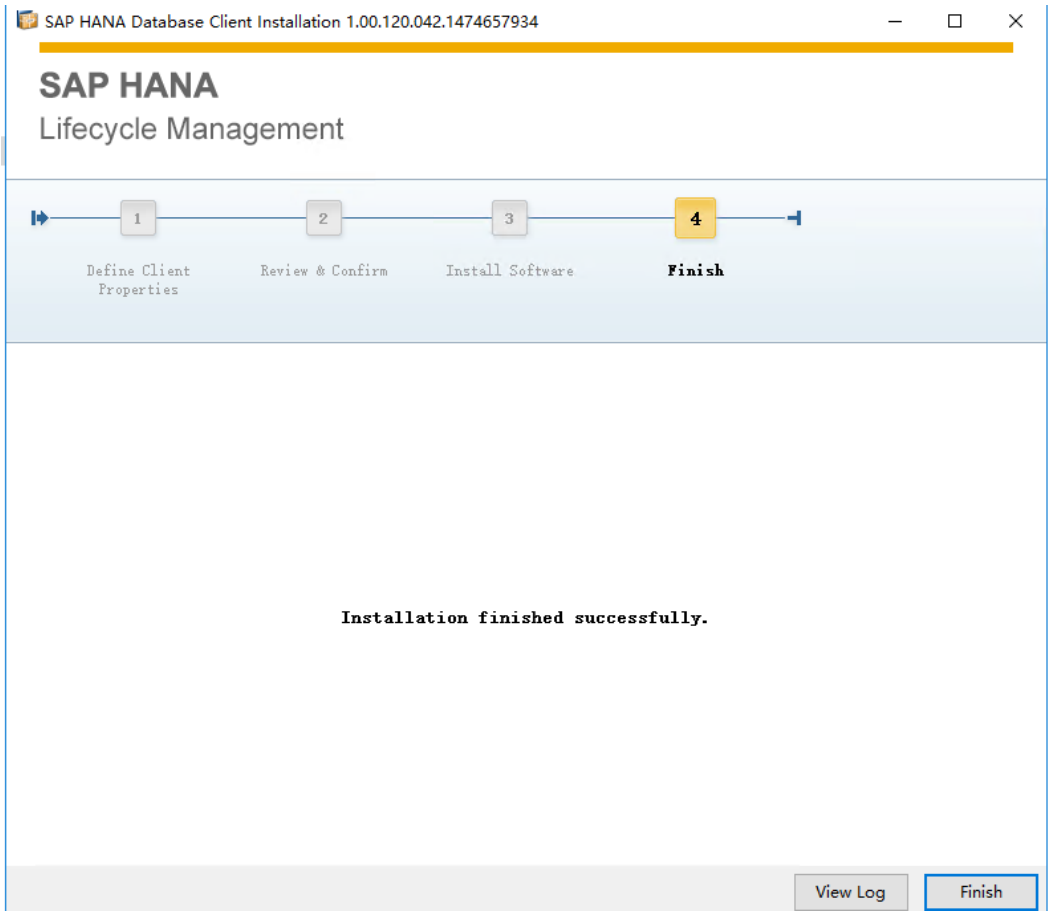
Step 1 Install the SAP HANA client.

On the Windows client, go to the **SAP_HANA_CLIENT** directory and double-click **hdbsetup** to start the installation.





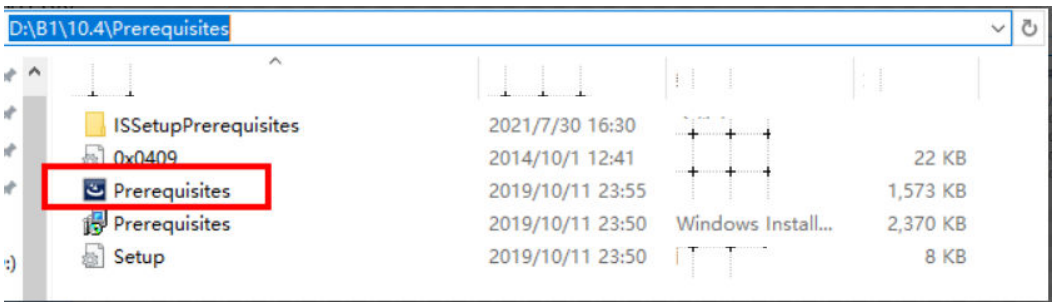




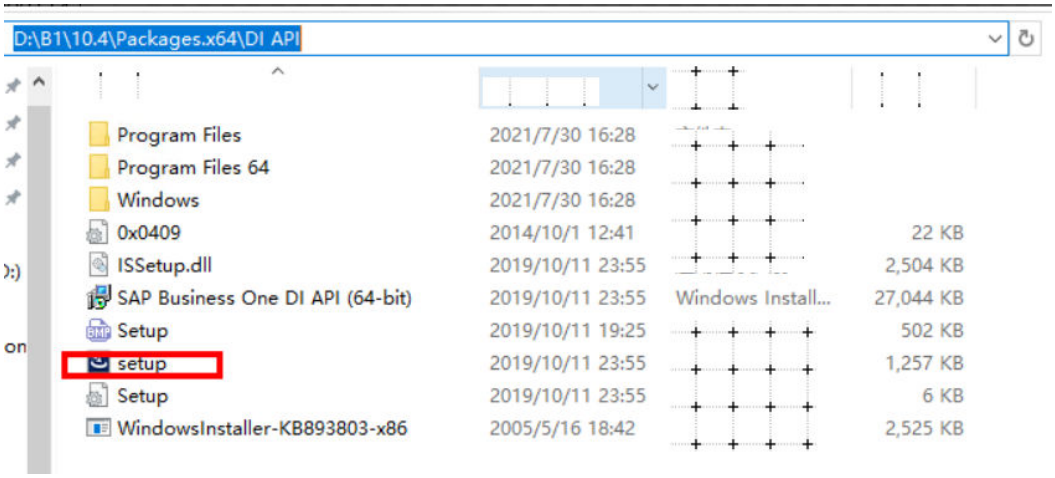
Step 2 Install the SAP Business One client.

1. Install Prerequisites and DI API (optional and required for SAP Business One 10.0).

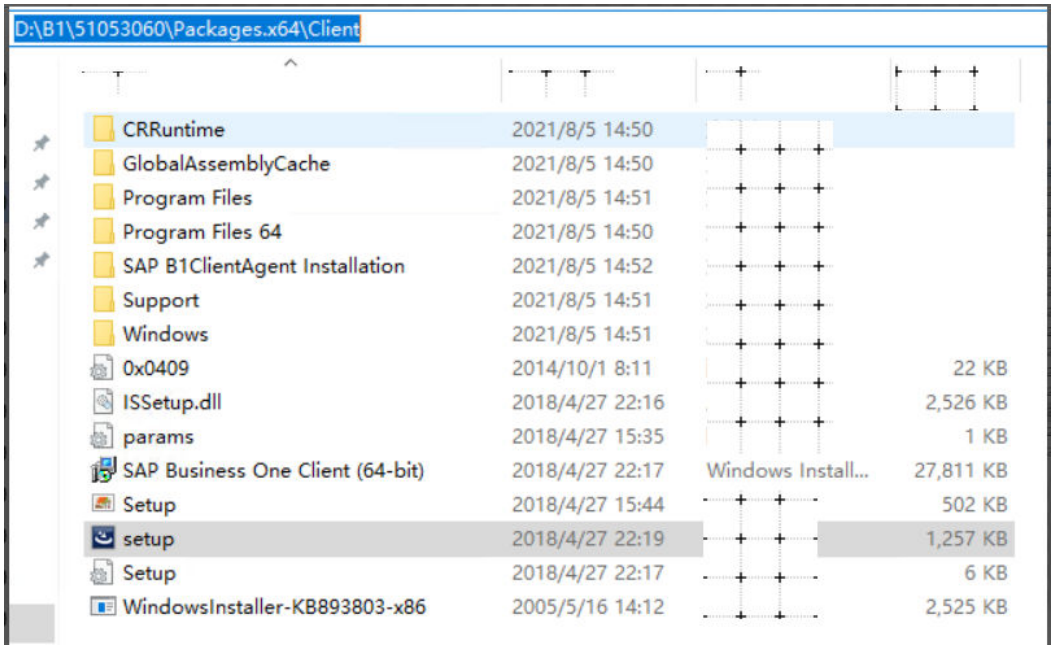
Go to the **Prerequisites** directory and double-click **Prerequisites** to start the installation.

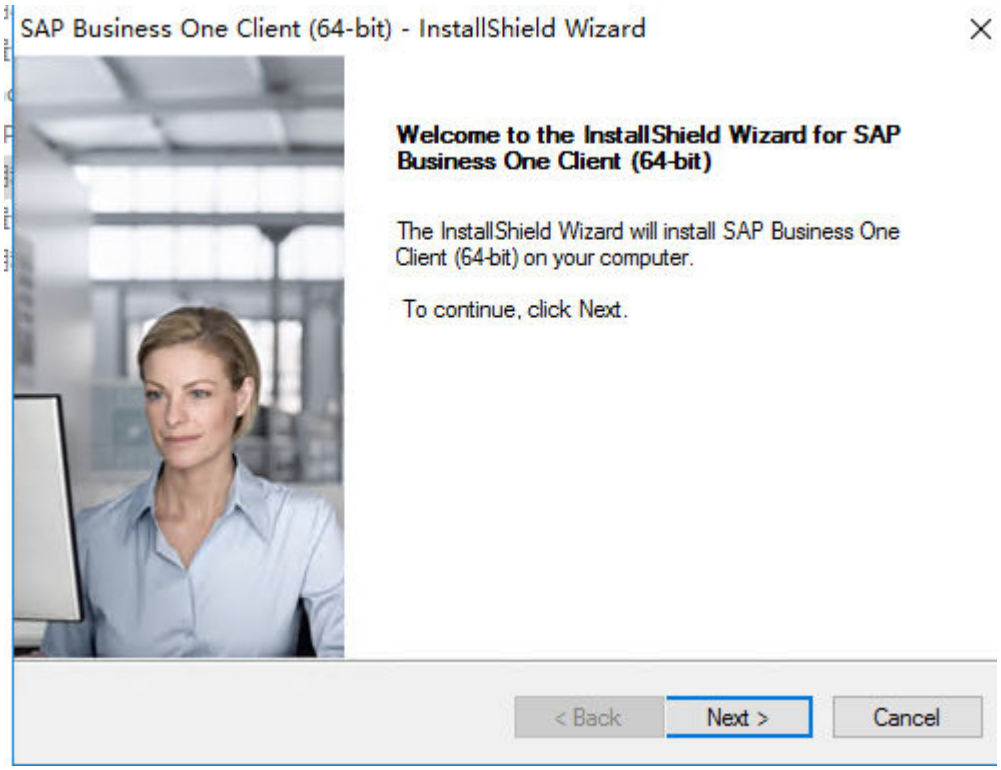


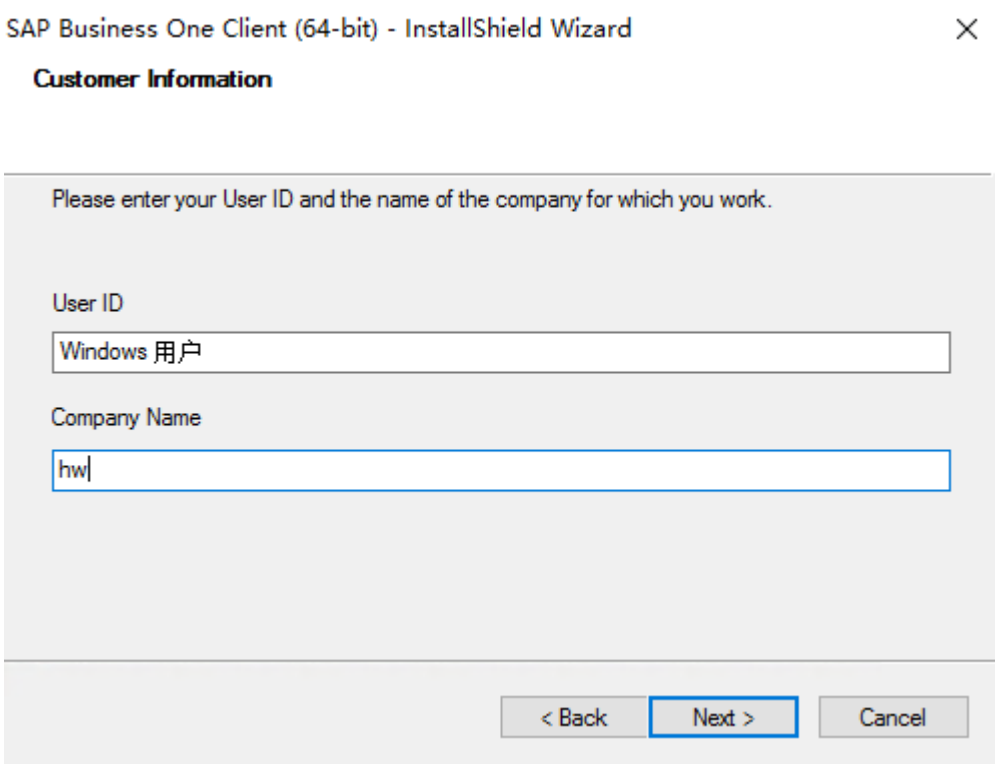
Go to the **DI API** directory and double-click **setup** to start the installation.

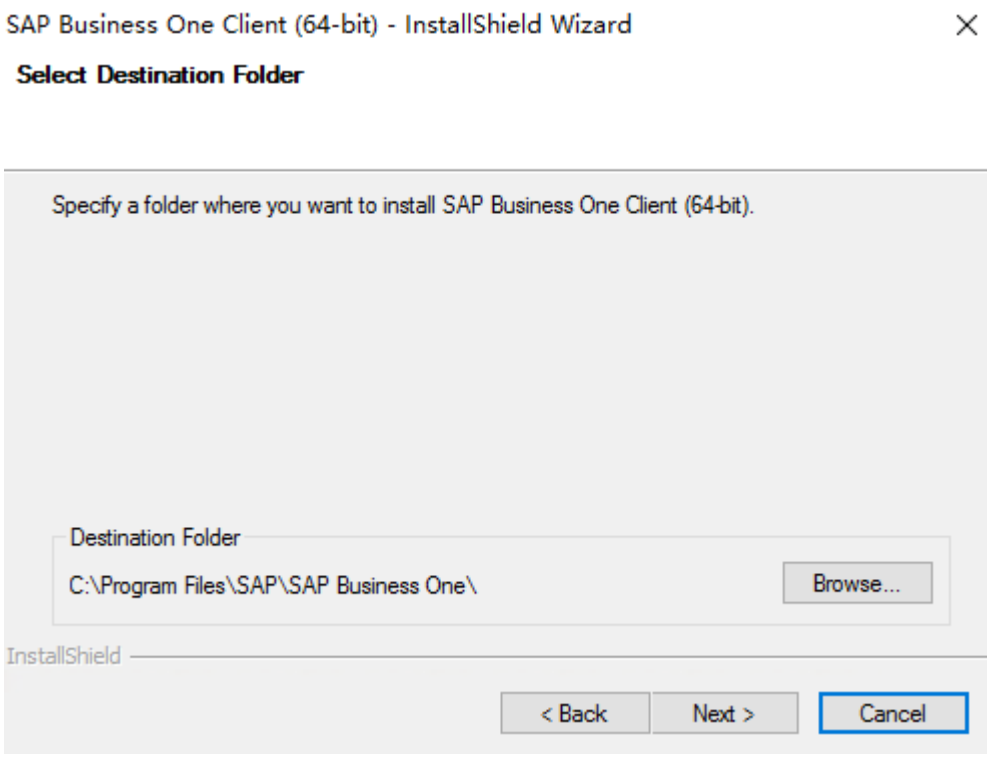


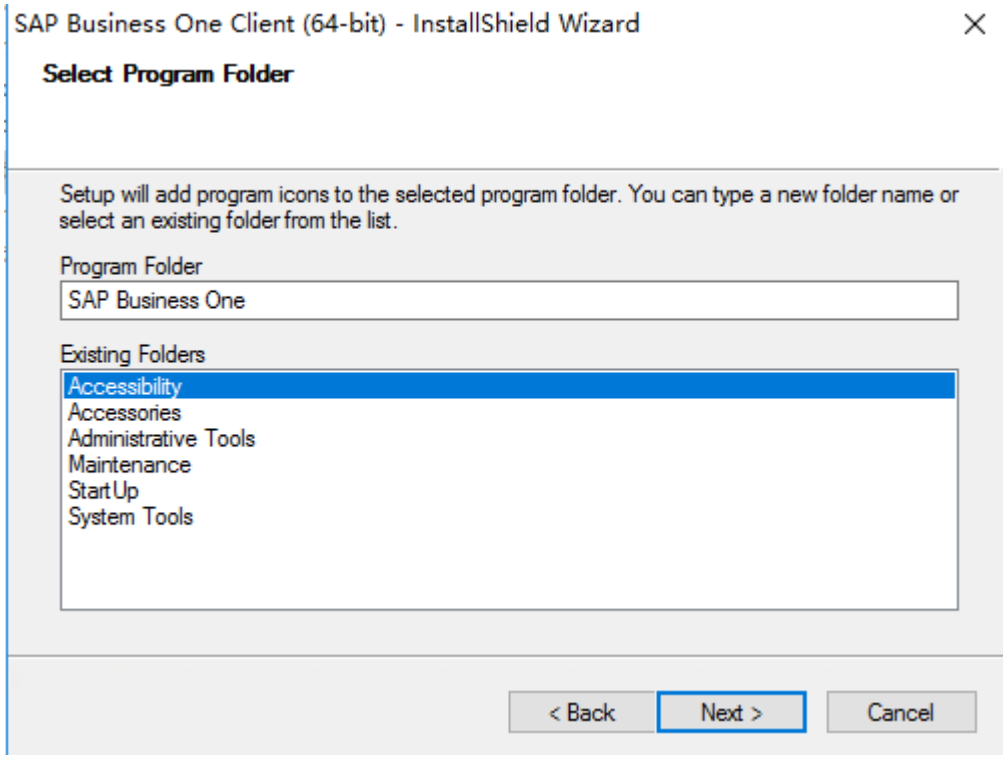
2. Go to the **Client** installation directory and double-click **setup** to install the client.

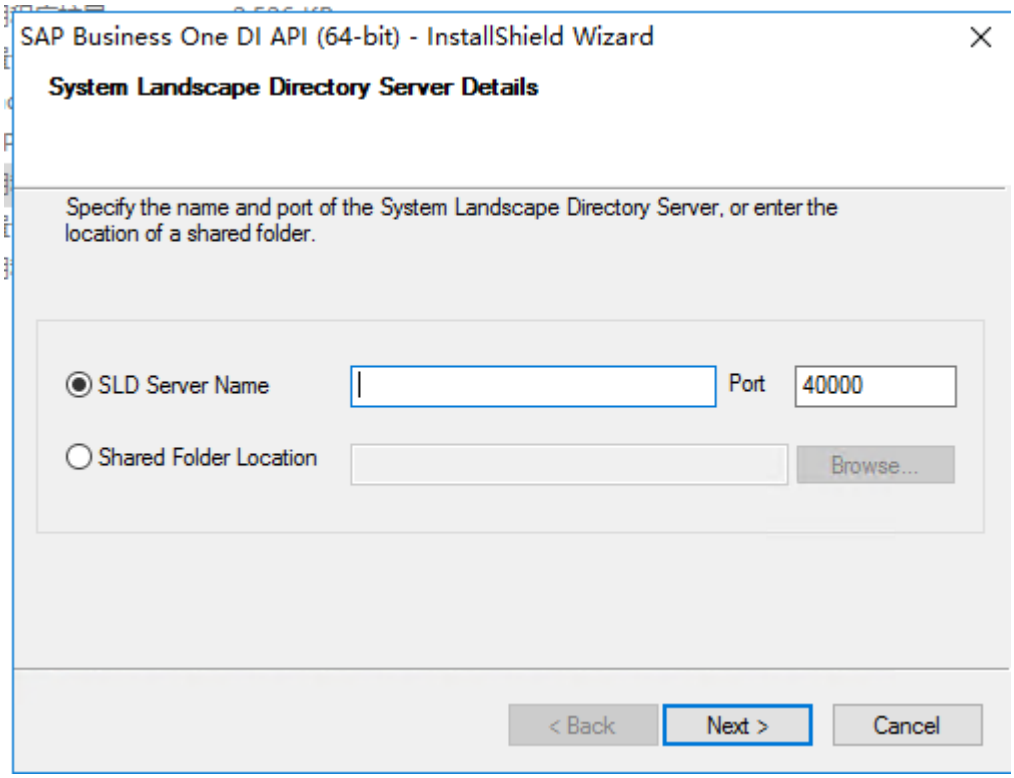


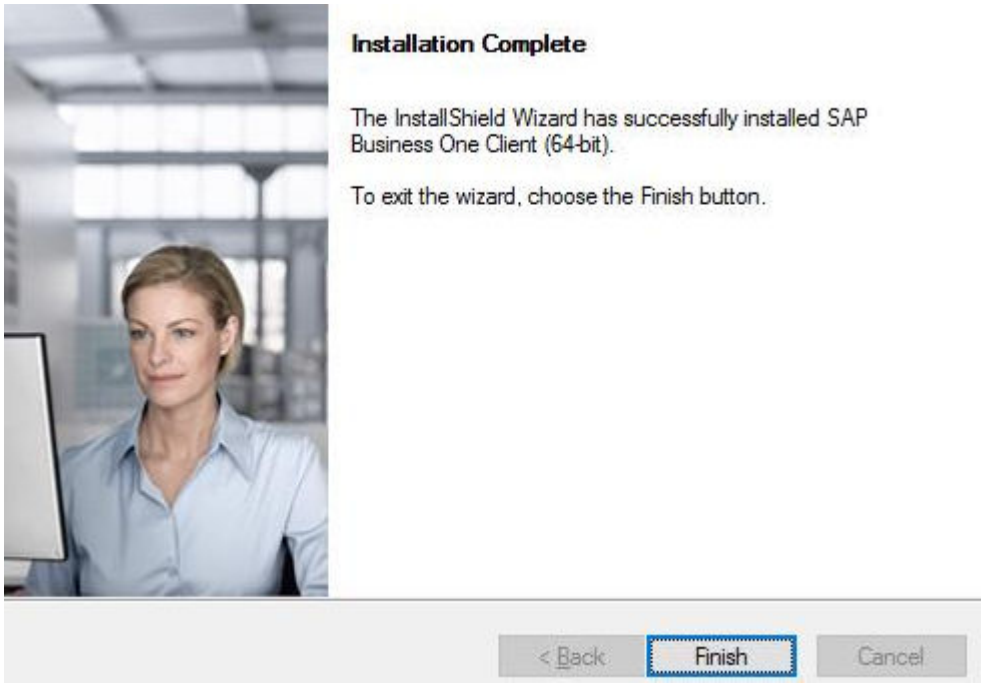






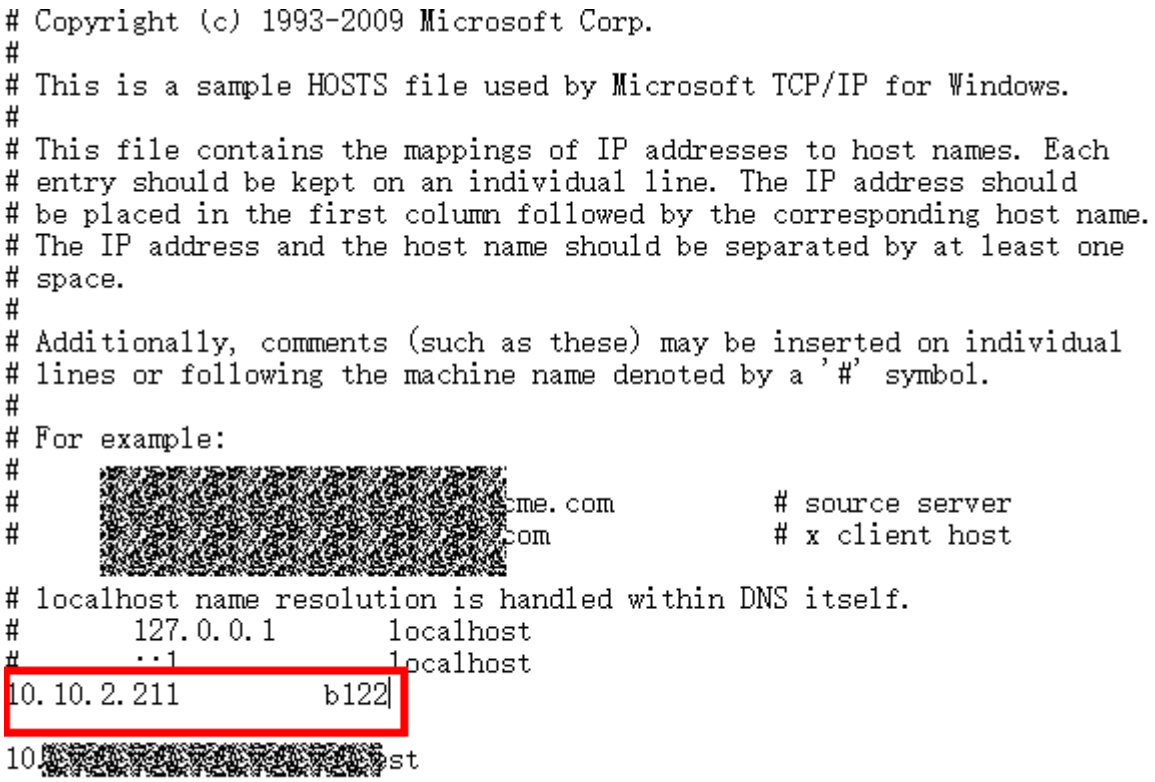






Step 3 Connect to SAP Business One.

1. Add the mapping between the SAP Business One ECS and its EIP to the local hosts file in the **C:/Windows/system32/drivers/etc/** directory.



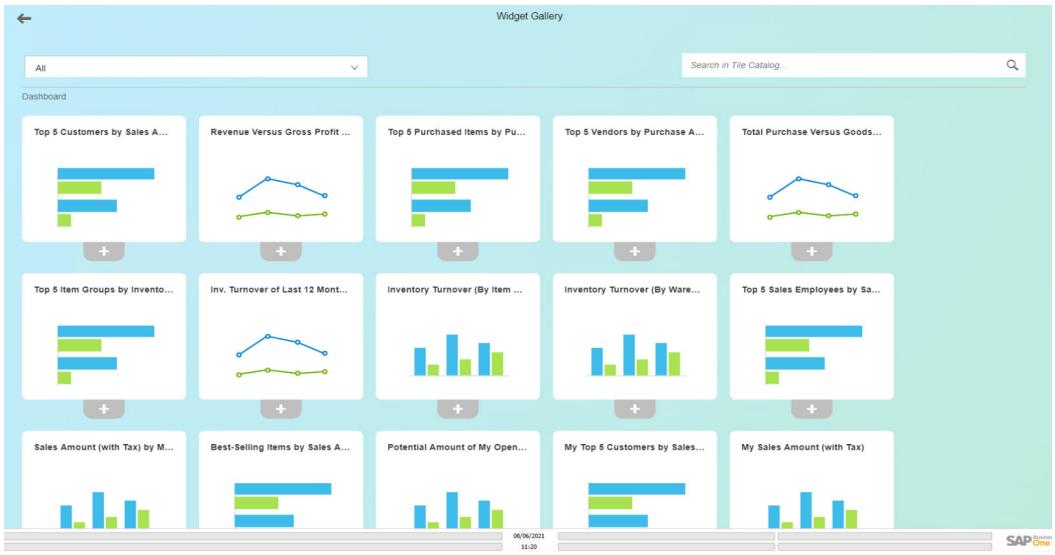
2. Run the SAP Business One client, enter the name of the SAP Business One ECS, and click **OK**.

3. Enter the username **manager** and password **manager**.

4. Click **Refresh**, or click **Create** to create a company as required,

5. Select the created company and click **OK**.

Company connected



----End

5.6 FAQs

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

Symptom

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

NOTE

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

Procedure

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

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

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

   vi /etc/cloud/cloud.cfg

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

   Example: #manage_etc_hosts: localhost


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

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

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

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

   vi /etc/hosts

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

```
#
# hosts         This file describes a number of hostname-to-address
#               mappings for the TCP/IP subsystem.  It is mostly
#               used at boot time, when no name servers are running.
#               On small systems, this file can be used instead of a
#               "named" name server.
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#


# special IPv6 addresses
::1     localhost       ipv6-localhost  ipv6-loopback

fe00::0 ipv6-localnet

ff00::0 ipv6-mcastprefix
ff02::1 ipv6-allnodes
ff02::2 ipv6-allrouters
ff02::3 ipv6-allhosts


127.0.0.1       localhost
127.0.0.1       localhost       localhost
127.0.0.1       test-xiongp     test-xiongp

~
```

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

----End

5.6.2 What Should I Do If a Message Indicating System Landscape Directory (SLD) Failed To Be Connected Is Displayed During the Connection to SAP Business One?

Symptom

After the node is restarted, a message indicating System Landscape Directory (SLD) failed to be connected is displayed during the connection to SAP Business One.

After the node is restarted, you need to manually start SAP HANA and SLD. To start SLD, perform the following operation:

Run the following commands:

/etc/init.d/sapb1servertools restart

/etc/init.d/b1s restart

```
bltest:/etc/init.d # cd sapblservertools
-bash: cd: sapblservertools: Not a directory
bltest:/etc/init.d # /etc/init.d/sapblservertools restart
redirecting to systemctl restart sapblservertools.service
bltest:/etc/init.d # /etc/init.d/b1s restart
Restarting Service Layer...
Stopping service with port 50001.
Stopping service with port 50002.
Stopping service with port 50003.
Stopping service with port 50004.
Stopping service with port 50000.
Starting service with port 50001.
Starting service with port 50002.
Starting service with port 50003.
Starting service with port 50004.
Starting service with port 50000.
Restarted.
bltest:/etc/init.d #
```

Connect to SAP Business One again.

5.7 Change History

Table 5-2

Description	Date	Prepared By
This issue is the first official release.	2021-08-30	Fu Chuandong/00469497

6 SAP Monitoring Best Practices

6.1 Overview

SAP full-screen monitoring developed based on Enterprise Project Management Service (EPS) has been brought offline. SAP full-screen monitoring 2.0 with more powerful capabilities is provided. If you are now using the EPS-based SAP full-screen monitoring, you need to follow the instructions described in **(Optional) Upgrading the Monitoring Agent** to upgrade the monitoring plug-in accordingly. The SAP full screen monitoring 2.0 provides functions such as SAP system monitoring, alarm statistics, application overview, and overview of CPU usage, memory usage, disk I/O, and network traffic. The SAP full screen monitoring helps you better understand the application resource usage, alarms, and SAP system running status in real time.

Table 6-1 lists the OSs and product versions supported by the Agent used for collecting monitoring metrics. **Table 6-2** describes the system resource usage of the Agent.

Table 6-1 Supported OSs and product versions

Type	Version
OS	• SUSE Linux Enterprise Server (SLES) 12 SP3 for SAP • SUSE Linux Enterprise Server (SLES) 12 SP4 for SAP • SUSE Linux Enterprise Server (SLES) 12 SP5 for SAP • SUSE Linux Enterprise Server (SLES) 15 for SAP • SUSE Linux Enterprise Server (SLES) 15 SP1 for SAP • SUSE Linux Enterprise Server (SLES) 15 SP2 for SAP
SAP HANA	SAP HANA 1.0 SP12 or later and SAP HANA 2.0
SAP S/4HANA	SAP S/4HANA 1709, SAP S/4HANA 1809, and SAP S/4HANA 1909
SAP NetWeaver	SAP NetWeaver 7.4 or later
SAP ECC	EHP7 FOR SAP ERP 6.0 or later

Table 6-2 System resource usage

Resource Type	Usage
Memory	The memory usage of the monitoring metric collecting Agent is from 30 MB to 35 MB.
CPU	The CPU usage of the monitoring metric collecting Agent is from 0.03% to 2.3%.

6.2 Installing the Monitoring Agent

6.2.1 SAP HANA (Single-Node Deployment Without High Availability Required)

To view the SAP full screen monitoring, the SAP monitoring agent must be installed. In the SAP HANA (single-node deployment without high availability required) scenario, the SAP monitoring agent must be installed on the HANA nodes.

Prerequisites

Ensure that Application Operations Management (AOM) ICAgent has been installed.

- AOM ICAgent is used to collect host OS metrics, such as CPU, memory, and disk. If it has not been installed, install it by referring to **Installing an ICAgent**.

Ensure that the AOM FullAccess permission has been assigned to the agency created for the host.

- AOM FullAccess is used for the authentication of AOM metric reporting API. The following describes the procedure to configure the permission.

Step 1 Log in to the management console.

Step 2 In the navigation pane on the left, click ☰ and choose **Identity Access Management** under **Management & Governance**.

Step 3 Click **Agencies** in the left pane, and then click **Create Agency** in the upper right corner. The **Create Agency** page is displayed.

Step 4 Set agency parameters.

- **Agency Name**: AOMFullAccess (this name is only for reference)
- **Agency Type**: Select **Cloud service**.
- **Cloud Service**: Select **Elastic Cloud Server (ECS) and Bare Metal Server (BMS)**.
- **Validity Period**: Retain the default setting.
- Click **Next** to configure the permission:
  a. Select **Region-specific projects** for **Scope**.
  b. Select the region where the cloud server is located.
  c. Enter **AOM FullAccess** in the search box and select it in the search result.
  d. Click **OK**.

Step 5 Configure the agency created in the previous step for the ECS.

1. In the left navigation pane, click ☰ and choose **Computing** > **Elastic Cloud Server**.
2. Select the ECS for which you want to configure the agency and click its name to switch to the basic information page.
3. Click the edit button next to **Agency** in the **Management Information** area, select the agency created in **Step 4**, and save the modification.

----End

CAUTION

AOM 2.0 is now available in the CN-Hong Kong, AP-Bangkok, AP-Singapore, AF-Johannesburg, TR-Istanbul, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago regions. **Subscribe to AOM 2.0** and **Upgrade ICAgent** before installing the SAP full screen monitoring for these regions.

Procedure

Installing and Configuring the Monitoring Agent

Step 1 Run the following commands to obtain the installation script to install the monitoring agent:

cd /tmp

The download paths of the script vary depending on regions. For details about how to obtain the path, see **Table 6-3**. The following commands show the download path in AP-Bangkok.

cd /tmp

curl https://obs-sap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/sapmon/install.sh | sh

Table 6-3 Links to obtain the installation script

Script Name	Description	Download Link
install.sh	Installation script	AP-Bangkok: **https://obs-sap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/sapmon/install.sh** AP-Singapore: **https://obs-sap-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com/sapmon/install.sh** CN-Hong Kong: **https://obs-sap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/sapmon/install.sh** SA-Johannesburg: **https://obs-sap-af-south-1.obs.af-south-1.myhuaweicloud.com/sapmon/install.sh** TR-Istanbul: **https://obs-sap-tr-west-1.obs.tr-west-1.myhuaweicloud.com/sapmon/install.sh** LA-Santiago: **https://obs-sap-la-south-2.obs.la-south-2.myhuaweicloud.com/sapmon/install.sh** LA-Sao Paulo1: **https://obs-sap-sa-brazil-11.obs.sa-brazil-1.myhuaweicloud.com/sapmon/install.sh** LA-Mexico City1: **https://obs-sap-na-mexico-1.obs.na-mexico-1.myhuaweicloud.com/sapmon/install.sh** LA-Mexico City2: **https://obs-sap-la-north-2.obs.la-north-2.myhuaweicloud.com/sapmon/install.sh**

Step 2 Modify the configuration.

1. Run the following command to encrypt the password:
   /usr/local/sapmon/bin/ktool -e
2. Enter the password.
3. Run the following command to modify the configuration file:
   vim /usr/local/sapmon/config/sapmon.ini

Table 6-4 lists the parameters. Set the parameters based on the actual situation. Change the password to the encrypted password obtained in Step 2.1.

Table 6-4 Configuration parameters

Type	Name	Description	Example Value
DEFAULT	log_level	Log level	INFO
	log_file	Log file name. The log file path is **/var/log/huawei/sapmon/**.	sap_metrics.log
	hostname	OS hostname	hana-1709
database.hana	enable	Whether to obtain database metrics. The value can be **true** or **false**. **NOTE** In the SAP HANA (single-node deployment with high availability required) scenario, the parameter is set to **true** for the active node and to **false** for the standby node.	true
	ha_mode	Whether the database is deployed in high availability (HA) mode. If yes, set this parameter to **true**. If no, set it to **false**.	false
	sid	Database SID	S00
	instance_number	Database instance number	00
	tenant_database_name	Name of the tenant database. This parameter is used in the multi-tenant scenario. – If the HANA database is for single tenant, you do not need to set this parameter. – If the HANA database is for multiple tenants, enter the name of the tenant database.	-

Type	Name	Description	Example Value
	username	SAP HANA username **NOTE** You need to use the following SQL statements to grant required permissions to this user: **CREATE USER <*username*> PASSWORD <*password*> NO FORCE_FIRST_PASSWORD_CHANGE;** GRANT CATALOG READ to <username>; GRANT SELECT on SCHEMA _SYS_STATISTICS to <username>	-
	password	SAP HANA user password	-

NOTE

If you need to monitor multiple tenant databases, copy and paste parameters under **database.hana**, and change **database.hana** to **database.hana.***<tenantdb_name>*.

Replace *<tenantdb_name>* with the tenant database name, and change values of **username**, **password**, and other required parameters. **username** and **password** indicate the username and password for logging in to the tenant database.

4. Run the following command to restart the monitoring agent.

   systemctl restart sapmon

----End

(Optional) Uninstalling the Monitoring Agent

Step 1 Run the following command to uninstall the monitoring agent.

rpm -e sapmon

----End

6.2.2 SAP HANA (Single-Node Deployment With High Availability Required)

In the SAP HANA (single-node deployment with high availability required) scenario, you need to deploy the monitoring agent on both the active and standby nodes. For details, see **SAP HANA (Single-Node Deployment Without High Availability Required)**.

NOTE

- Set **hostname** to the names of hosts of active and standby nodes. On the active node, set the value of **enable** of **database.hana** to **true** to enable the monitoring function.
- After the HA switchover, set the value of **enable** of **database.hana** on the original active node to **false** to stop the monitoring for the original active node. On the original standby node, set the value of **enable** of **database.hana** to **true** to enable the monitoring for it (the new active node after HA switchover).

6.2.3 SAP S/4HANA (Single-Node Deployment Without High Availability Required)

In the SAP S/4HANA (single-node deployment without high availability required) scenario, you need to install the SAP monitoring agent on the node where both ASCS and PAS instances are deployed.

Prerequisites

Ensure that Application Operations Management (AOM) ICAgent has been installed.

- AOM ICAgent is used to collect host OS metrics, such as CPU, memory, and disk. If it has not been installed, install it by referring to **Installing an ICAgent**.

Ensure that the AOM FullAccess permission has been assigned to the agency created for the host.

- AOM FullAccess is used for the authentication of AOM metric reporting API. The following describes the procedure to configure the permission.

Step 1 Log in to the management console.

Step 2 In the navigation pane on the left, click ☰ and choose **Identity Access Management** under **Management & Governance**.

Step 3 Click **Agencies** in the left pane, and then click **Create Agency** in the upper right corner. The **Create Agency** page is displayed.

Step 4 Set agency parameters.

- **Agency Name**: AOMFullAccess (this name is only for reference)
- **Agency Type**: Select **Cloud service**.
- **Cloud Service**: Select **Elastic Cloud Server (ECS) and Bare Metal Server (BMS)**.
- **Validity Period**: Retain the default setting.
- Click **Next** to configure the permission:
  a. Select **Region-specific projects** for **Scope**.
  b. Select the region where the cloud server is located.
  c. Enter **AOM FullAccess** in the search box and select it in the search result.
  d. Click **OK**.

Step 5 Configure the agency created in the previous step for the ECS.

1. In the left navigation pane, click ☰ and choose **Computing** > **Elastic Cloud Server**.
2. Select the ECS for which you want to configure the agency and click its name to switch to the basic information page.
3. Click the edit button next to **Agency** in the **Management Information** area, select the agency created in **Step 4**, and save the modification.

----End

Procedure

Preparations

Step 1 Obtain SAP NW RFC SDK.

NOTE

To obtain SAP NW RFC SDK, log in at **https://support.sap.com/en/my-support/software-downloads.html**, access downloads of **Support Packages & Patches**, search for SAP NW RFC SDK 7.50, and download it.

Step 2 Log in to the cloud server as user **root**.

Step 3 Upload the obtained SAP NW RFC SDK installation package to the **/usr/sap** directory.

Step 4 Run the following commands to decompress the SAP NW RFC SDK package to the **/usr/sap** directory:

unzip nwrfc750P_7-70002752.zip

mv nwrfcsdk /usr/sap/

----End

Installing the Monitoring Agent

Step 1 Run the following commands to obtain the installation script to install the monitoring agent.

The download paths of the script vary depending on regions. For details about how to obtain the path, see **Table 6-5**. The following commands show the download path in AP-Bangkok.

cd /tmp

wget https://obs-sap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/sapmon/install.sh&& sh install.sh --nwrfcsdk-path /usr/sap/nwrfcsdk

/usr/sap/nwrfcsdk is the decompression path in **Step 4**.

Table 6-5 Link to obtain the installation script

Script Name	Description	Download Link
install.sh	Installation script	AP-Bangkok: **https://obs-sap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/sapmon/install.sh** AP-Singapore: **https://obs-sap-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com/sapmon/install.sh** CN-Hong Kong: **https://obs-sap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/sapmon/install.sh** SA-Johannesburg: **https://obs-sap-af-south-1.obs.af-south-1.myhuaweicloud.com/sapmon/install.sh** TR-Istanbul: **https://obs-sap-tr-west-1.obs.tr-west-1.myhuaweicloud.com/sapmon/install.sh** LA-Santiago: **https://obs-sap-la-south-2.obs.la-south-2.myhuaweicloud.com/sapmon/install.sh** LA-Sao Paulo1: **https://obs-sap-sa-brazil-11.obs.sa-brazil-1.myhuaweicloud.com/sapmon/install.sh** LA-Mexico City1: **https://obs-sap-na-mexico-1.obs.na-mexico-1.myhuaweicloud.com/sapmon/install.sh** LA-Mexico City2: **https://obs-sap-la-north-2.obs.la-north-2.myhuaweicloud.com/sapmon/install.sh**

Step 2 Modify the configuration.

1. Run the following command to encrypt the password:

   /usr/local/sapmon/bin/ktool -e

2. Enter the password.
3. Run the following command to enter the edit mode of the configuration file. Modify the file according to **Table 6-6**, save the file, and exit.

   vim /usr/local/sapmon/config/sapmon.ini

   Modify the parameters based on the actual situation. Change the password to the return code obtained in **Step 2.1**.

Table 6-6 Configuration parameters

Parameter Type	Name	Description	Example Value
DEFAULT	log_level	Log level	INFO
	log_file	Log file name. The log file path is **/var/log/huawei/sapmon/**.	sap_metrics.log
	hostname	OS hostname	s4hana-1709

Parameter Type	Name	Description	Example Value
application.netweaver	enable	Whether to obtain the application metrics. The value can be **true** or **false**. **NOTE** In the SAP S/4HANA (single-node deployment with HA required) scenario, set this parameter to **true** for the active node and to **false** for the standby node.	true
	ha_mode	Whether to deploy the application in high availability mode. If yes, set this parameter to **true**. If no, set this parameter to **false**.	true
	sid	Application SID	S4H
	instance_number	PAS instance ID	10
	client	SAP system ID	000
	username	Application username	ddic
	password	Application password. Enter the encrypted password.	-

NOTE

If you need to monitor multiple applications, copy and paste parameters under **application.netweaver**, and change **application.netweaver** to **application.netweaver.<*sid*>**.

sid indicates the application system ID.

4. Run the following command to restart the monitoring agent.

   systemctl restart sapmon

----End

(Optional) Uninstalling the Monitoring Agent

Step 1 Run the following command to uninstall the monitoring agent.

rpm -e sapmon

----End

6.2.4 SAP S/4HANA (Single-Node Deployment With High Availability Required)

In the SAP S/4HANA (with HA required) scenario, ASCS is deployed on the active node and ERS is deployed on the standby node. You need to deploy the monitoring agent on both the active and standby nodes. For details, see **SAP S/4HANA (Single-Node Deployment Without High Availability Required)**.

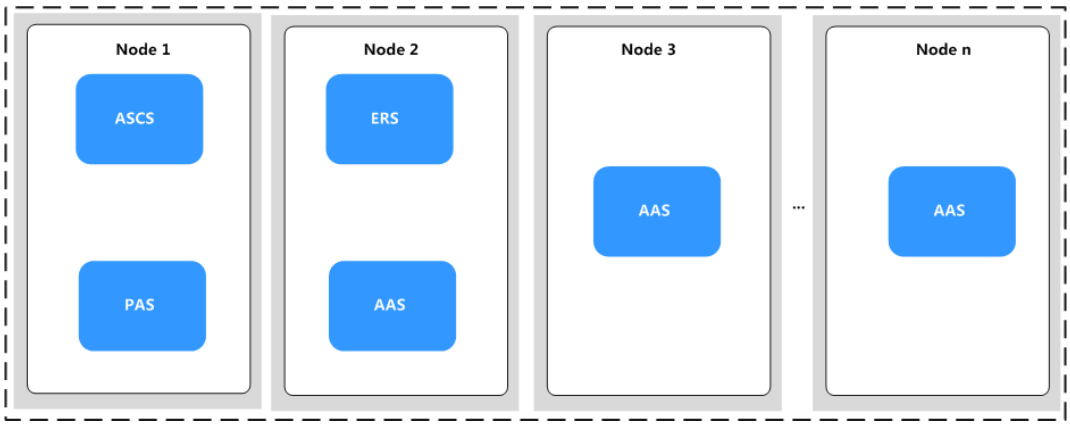
NOTE

- Set **hostname** to the names of hosts of active and standby nodes. On the active and standby nodes, set the value of **instance_number** to the PAS or AAS instance number. On the active node, set **enable** of **application.netweaver** to **true** to enable the monitoring function.
- AAS and PAS must be installed on both the active and standby nodes, and their processes must be started.
- After the HA switchover, set the value of **enable** of **application.netweaver** on the original active node to **false** to stop the monitoring for the original active node. On the original standby node, set the value of **enable** of **application.netweaver** to **true** to enable the monitoring for it (the new active node after HA switchover).

6.2.5 SAP S/4HANA (Distributed Deployment with High Availability Required)

In the SAP S/4HANA (distributed deployment with high availability required) scenario, you need to deploy the monitoring agent on node 1 and node 2, as shown in **Figure 6-1**. For details about the deployment of the monitoring agent, see **SAP S/4HANA (Single-Node Deployment With High Availability Required)**.

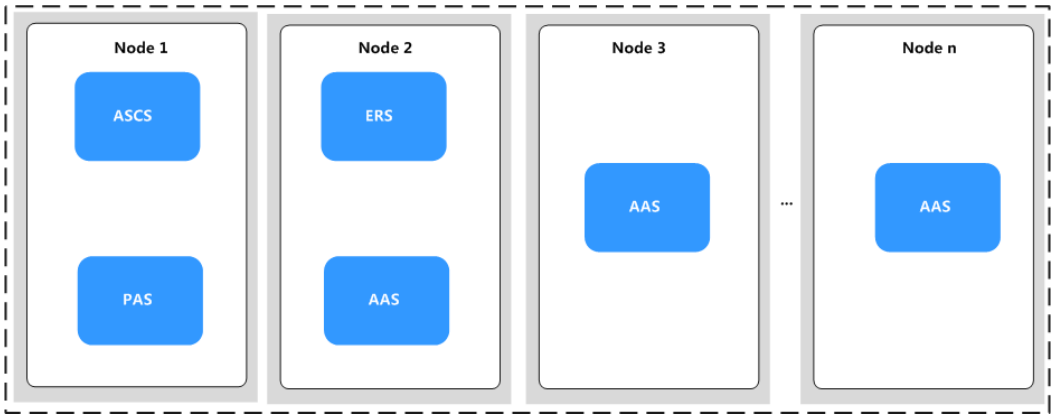
Figure 6-1 Deployment scheme



6.2.6 SAP S/4HANA (Distributed Deployment Without High Availability Required)

In the SAP S/4HANA (distributed deployment without high availability required) scenario, you need to deploy the monitoring agent on the node where ASCS is located (node 1 in **Figure 6-2**). For details about the deployment of the monitoring agent, see **SAP S/4HANA (Single-Node Deployment Without High Availability Required)**.

Figure 6-2 Deployment scheme



6.2.7 SAP ECC

To monitor SAP ECC metrics, you need to follow the operations descried in **SAP S/4HANA (Single-Node Deployment Without High Availability Required)** to deploy and configure the monitoring agent on the node where SAP ECC is located.

6.3 (Optional) Upgrading the Monitoring Agent

Uninstalling the EPS-based SAP Monitoring Plug-in and Installing the Monitoring Agent of the Latest Version

If the ERP-based SAP monitoring plug-in has been installed in your hosts, uninstall it and install the monitoring agent of the latest version.

Step 1 Log in to the node where the SAP monitoring plug-in is installed.

Step 2 Run the following command to uninstall the EPS-based monitoring plug-in:

rpm -e sapmon

Step 3 Follow the instructions described in **Installing Agent** to install the monitoring agent of the latest version.

----End

Upgrading the Monitoring Agent

If the ERP-based SAP monitoring plug-in has not been installed in your hosts, upgrade the monitoring agent due to updated monitoring metrics or monitoring agent optimization requirement to better monitoring the SAP metrics.

Step 1 Log in to the node where the monitoring agent is installed.

Step 2 Run the following command to upgrade the monitoring agent.

/usr/local/sapmon/upgrade.sh

----End

6.4 Viewing Monitoring Metrics

You can view the host OS metrics and SAP system metrics reported to AOM.

Procedure

Step 1 Log in to the management console.

Step 2 In the navigation pane on the left, click ☰ and choose **Management & Governance** > **Application Operations Management**.

Step 3 In the navigation pane on the left on the displayed page, choose **Monitoring** > **Metric Monitoring** to view the SAP system metrics and host OS metrics.

----End

Host OS Metrics

For details about the host OS metrics of AOM, see **Metric Overview**.

SAP System Metrics

SAP system metrics are classified into SAP HANA metrics as well as SAP NetWeaver ABAP and SAP NetWeaver Java application metrics, as shown in:

Table 6-7

Table 6-8

Table 6-7 SAP HANA metrics

Metric Group	Metric Name	Description	Unit
database_version	sap_hanadb_database_version_info	Database version	
service_quantity	sap_hanadb_service_quantity_count	Total number of instance processes	count
	sap_hanadb_active_service_quantity_count	Number of active processes in an instance	count
database_ha_active	sap_hanadb_database_ha_active_status	Database HA status	status
sr_active	sap_hanadb_sr_active_status	Database system replication status	status
threads	sap_hanadb_all_threads_count	Total number of threads	count
	sap_hanadb_active_threads_count	Number of active threads	count

Metric Group	Metric Name	Description	Unit
	sap_hanadb_blocked_threads_count	Number of blocked threads	count
	sap_hanadb_sqlexecutor_threads_count	Number of SQL execution threads	count
	sap_hanadb_sqlexecutor_threads_active_count	Number of active SQL execution threads	count
	sap_hanadb_jobworker_threads_count	Total number of job threads	count
	sap_hanadb_jobworker_threads_active_count	Number of active job threads	count
recent_data_backup	sap_hanadb_age_of_recent_data_backup_hours	Number of hours since the last successful full data backup If the backup fails, the value is **-1**.	hours
recent_savepoint	sap_hanadb_age_of_recent_savepoint_minutes	Number of minutes since last SAVEPOINT If the SAVEPOINT does not exist, the value is **-1**.	minutes
	sap_hanadb_recent_savepoint_duration_seconds	Duration (in seconds) of the last SAVEPOINT If the SAVEPOINT does not exist, the value is **-1**.	seconds
column_tables_used_memory	sap_hanadb_column_tables_used_memory_mb	Memory usage of the data table	mb
schema_used_memory	sap_hanadb_schema_used_memory_mb	Database schema memory usage	mb
disk_data_files	sap_hanadb_disk_data_files_used_size_mb	Used space per file and file type (in MB)	mb
	sap_hanadb_disk_data_files_total_size_mb	Total space per file and file type (in MB)	mb
	sap_hanadb_disk_data_files_available_size_mb	Available space per file and file type (in MB)	mb
	sap_hanadb_disk_data_files_fragmentation_percent	Percentage of unused space compared to total space in file	percent

Metric Group	Metric Name	Description	Unit
disk_usage	sap_hanadb_disk_total_device_size_mb	Total device size returned by the operating system (in MB). It will be repeated if the device is shared between usages_types.	mb
	sap_hanadb_disk_total_size_mb	Volume size in MB. It will be repeated if the volume is shared between usages_types.	mb
	sap_hanadb_disk_total_used_size_mb	Used volume size in MB. It will be repeated if the volume is shared between usages_types.	mb
	sap_hanadb_disk_used_size_mb	Used disk size calculated for each usage type (such as DATA and LOG)	mb
service_memory	sap_hanadb_memory_service_shared_allocated_mb	Shared memory in MB allocated from the memory pool to the service	mb
	sap_hanadb_memory_service_shared_used_size_mb	Used Shared Memory part of the memory pool per service in MB	mb
	sap_hanadb_memory_service_shared_used_percent	Percentage of used Shared Memory from the memory pool per service	percent
	sap_hanadb_memory_service_heap_allocated_mb	Heap memory allocated from the memory pool to the service	mb
	sap_hanadb_memory_service_heap_used_size_mb	Used Heap Memory part of the memory pool per service in MB	mb
	sap_hanadb_memory_service_heap_used_percent	Percentage of used Heap Memory part of the memory pool per service	percent
	sap_hanadb_memory_service_total_used_mb	Total memory that has been applied for from the memory pool for the service	mb
	sap_hanadb_memory_service_physical_total_mb	Total physical memory used by the service	mb

Metric Group	Metric Name	Description	Unit
	sap_hanadb_memory_service_virtual_total_mb	Total virtual memory used by the service	mb
	sap_hanadb_memory_service_code_size_mb	Size of the code snippet used by the service (including the dynamic link library)	mb
	sap_hanadb_memory_service_stack_size_mb	Size of the stack used by the service	mb
	sap_hanadb_memory_service_compactors_freeable_size_mb	Memory that can be freed during a memory shortage per service in MB	mb
	sap_hanadb_memory_service_compactors_allocated_size_mb	Potential memory that can be released by the memory pool when the memory is insufficient for the service	mb
	sap_hanadb_memory_service_alloc_limit_mb	Maximum size of the memory pool for the service	mb
	sap_hanadb_memory_service_effective_alloc_limit_mb	Maximum valid memory pool size for the service (calculated by taking other processes into account)	mb
host_memory	sap_hanadb_host_memory_physical_total_mb	Total physical memory of the host	mb
	sap_hanadb_host_memory_resident_mb	Physical memory used by processes on a host	mb
	sap_hanadb_host_memory_physical_free_mb	Idle physical memory of a host	mb
	sap_hanadb_host_memory_swap_free_mb	Idle swap memory of the host	mb
	sap_hanadb_host_memory_swap_used_mb	Used swap memory of the host	mb
	sap_hanadb_host_memory_alloc_limit_mb	Maximum memory in MB that can be allocated to all processes on a host	mb

Metric Group	Metric Name	Description	Unit
	sap_hanadb_host_memory_used_total_mb	Total memory size occupied by the SAP HANA process in the memory pool	mb
	sap_hanadb_host_memory_used_peak_mb	Maximum memory that can be occupied by the SAP HANA process in the memory pool after the instance is started	mb
	sap_hanadb_host_memory_pool_size_mb	Total memory pool size for the SAP HANA process	mb
	sap_hanadb_host_memory_code_size_mb	Total code snippet size of the SAP HANA process, including the dynamic link library	mb
	sap_hanadb_host_memory_shared_alloc_mb	Total shared memory size of the SAP HANA process	mb
sql_service	sap_hanadb_sql_service_executions_count	Total number of execution times of different types of SQL statements	count
	sap_hanadb_sql_service_elapsed_time_ms	Total execution time of different types of SQL statements	ms
	sap_hanadb_sql_service_elap_per_exec_avg_ms	Average execution time of different types of SQL statements	ms
	sap_hanadb_sql_service_lock_per_exec_ms	Average lock wait time for executing different types of SQL statements	ms
	sap_hanadb_sql_service_max_ela_time_ms	Maximum time required for executing different types of SQL statements	ms
sql_top_time	sap_hanadb_sql_top_time_consumers_execution_time_mu	Top 10 SQL statements with the longest execution duration	mu
	sap_hanadb_sql_top_time_consumers_execution_count	Total number of execution times of top 10 SQL statements with the longest execution duration	count

Metric Group	Metric Name	Description	Unit
sql_top_mem	sap_hanadb_sql_top_mem_consumers_total_execution_memory_size_byte	Top 10 SQL statements with the largest memory usage	byte
	sap_hanadb_sql_top_mem_consumers_execution_count	Total number of execution times of top 10 SQL statements with the largest memory usage	count
connections_total	sap_hanadb_connections_total_count	Total number of connections of different types	count
table_cs_top_mem	sap_hanadb_table_cs_top_mem_total_mb	Top 10 database tables with the largest memory usage	mb
	sap_hanadb_table_cs_top_mem_estimated_max_mb	Estimated maximum memory usage for the top 10 database tables with the largest memory usage	mb
	sap_hanadb_table_cs_top_mem_record_count	Number of data rows in the top 10 database tables with the largest memory usage	count
	sap_hanadb_table_cs_top_mem_disk_size_mb	Disk usage of the top 10 database tables with largest memory usage	mb
alerts	sap_hanadb_alerts_current_rating	Database alarm	rating

Table 6-8 SAP NetWeaver ABAP and SAP NetWeaver Java application metrics

Metric Group	Metric Name	Description	Unit
application_version	sap_netweaver_application_version_info	Application version	
instance_quantity	sap_netweaver_instance_quantity_count	Total number of instances in the application system	count
	sap_netweaver_active_instance_quantity_count	Number of active instances in the application system	count
application_ha_active	sap_netweaver_application_ha_active_status	Application HA status	status

Metric Group	Metric Name	Description	Unit
abap_short_dumps	sap_netweaver_abap_short_dumps_count	Number of ABAP Dumps in the last one hour	count
abap_short_dumps_5m	sap_netweaver_abap_short_dumps_5m_count	Number of ABAP Dumps in the last five minutes	count
jobs	sap_netweaver_canceled_jobs_count	Number of jobs deleted (canceled) in the last one hour	count
	sap_netweaver_finished_jobs_count	Number of jobs completed in the last one hour	count
logged_in_users	sap_netweaver_logged_in_users_count	Number of users who have logged in to the SAP application	count
lock_entries_usage	sap_netweaver_lock_entries_usage_percent	Lock entries usage	percent
extended_memory_utilization	sap_netweaver_extended_memory_utilization_percent	Extended memory usage (%)	percent
heap_memory_utilization	sap_netweaver_heap_memory_utilization_percent	Heap memory usage (%)	percent
dialog_response_time	sap_netweaver_dialog_response_time_ms	Dialog response duration	ms
dialog_db_request_time	sap_netweaver_dialog_db_request_time_ms	Time required for processing a request from Dialog to the database	ms
work_processes	sap_netweaver_work_processes_utilization_percent	Process usage (%). The types of processes are dialog, background, spool, update 1, and update 2.	percent
	sap_netweaver_number_of_total_work_processes_count	Total number of processes. The types of processes are dialog, background, spool, update 1, and update 2.	count

Metric Group	Metric Name	Description	Unit
	sap_netweaver_number_of_free_work_processes_count	Number of idle processes. The types of processes are dialog, background, spool, update 1, and update 2.	count
jobs	sap_netweaver_running_jobs_count	Number of running jobs	count
failed_idocs	sap_netweaver_failed_idocs_count	Number of failed Intermediate Documents (IDocs)	count
update_records	sap_netweaver_update_records_count	Number of update records in the last one minute	count
	sap_netweaver_failed_updates_count	Number of failed update records in the last one minute	count
rfc_ping	sap_netweaver_rfc_ping_ms	RFC ping latency from each instance to the PAS node	ms
j2ee_running_process	sap_netweaver_j2ee_running_process_count	Number of running Java processes	count
j2ee_thread	sap_netweaver_j2ee_thread_count	Number of Java threads	count
j2ee_session	sap_netweaver_j2ee_session_count	Number of Java sessions	count
j2ee_websession	sap_netweaver_j2ee_websession_count	Number of Java web sessions	count
j2ee_ejbsession	sap_netweaver_j2ee_ejbsession_count	Number of Java EJB sessions	count
j2ee_vm_heap_size	sap_netweaver_j2eevmheap_size_mb	Size of the **local classes** or **local objects** heap in the Java process	mb
	sap_netweaver_j2eevmheap_commitSize_mb	Commit size of the **local classes** or **local objects** heap in the Java process	mb

Metric Group	Metric Name	Description	Unit
	sap_netweaver_j2eevmheap_maxUsedSize_mb	Maximum used size of the **local classes** or **local objects** heap in the Java process	mb
	sap_netweaver_j2eevmheap_initialSize_mb	Initial size of the **local classes** or **local objects** heap in the Java process	mb
	sap_netweaver_j2eevmheap_maxSize_mb	Maximum size of the **local classes** or **local objects** heap in the Java process	mb

6.5 Configuring Grafana SAP Full Screen Monitoring

By configuring the Grafana SAP full screen monitoring, you can learn about the application resource usage, alarms, and SAP system running status in real time.

Prerequisites

- The monitoring agent has been installed. If it has not been installed, follow the instructions described in **Installing the Agent** to install it.
- Grafana has been installed and started. The SAP full screen monitoring is implemented based on Grafana. You need to prepare a host for running Grafana and install and start Grafana on the host. For details about how to install Grafana, see **Installing Grafana**. During the installation, you are directed to start the Grafana service.

Procedure

Step 1 Log in to Grafana and create an AOM data source on Grafana. For details, see **Viewing Metric Data in AOM Using Grafana**.

NOTE

If you have upgraded to AOM 2.0, create an AOM data source on Grafana. For details, see **Viewing Metric Data in AOM 2.0 Using Grafana**.

CAUTION

After Grafana has been installed and started, use a browser to access *Host IP address*:*Port number* to log in to Grafana. The default port number is **3000**. The default username for first-time login is **admin**. Change the password upon the first-time login. Grafana 9.0.0 is recommended.

Step 2 Download the Grafana full-screen monitoring template.

Use the following links to download the Grafana full-screen monitoring templates. Download all of the following templates that display system metrics from different dimensions.

Table 6-9

Template Name	Description
Overview of SAP System Metrics	Provides an overview of the SAP system metrics.
SAP HANA Metrics	Displays detailed information about SAP HANA metrics.
SAP NetWeaver Metrics	Displays detailed information about SAP NetWeaver metrics.
AOM Host Metrics	Displays details about host OS metrics collected by AOM.

The download path varies depending on the region. For details, see **Table 6-10**.

Table 6-10 Links to obtain the templates

Template	Download Link
Overview of SAP System Metrics	AP-Bangkok: **https://obs-sap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/sapmon/templates/en/SAP-Systems-Overview** AP-Singapore: **https://obs-sap-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com/sapmon/templates/en/SAP-Systems-Overview** CN-Hong Kong: **https://obs-sap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/sapmon/templates/en/SAP-Systems-Overview** SA-Johannesburg: **https://obs-sap-af-south-1.obs.af-south-1.myhuaweicloud.com/sapmon/templates/en/SAP-Systems-Overview** TR-Istanbul: **https://obs-sap-tr-west-1.obs.tr-west-1.myhuaweicloud.com/sapmon/templates/en/SAP-Systems-Overview** LA-Santiago: **https://obs-sap-la-south-2.obs.la-south-2.myhuaweicloud.com/sapmon/templates/en/SAP-Systems-Overview** LA-Sao Paulo1: **https://obs-sap-sa-brazil-11.obs.sa-brazil-1.myhuaweicloud.com/sapmon/templates/en/SAP-Systems-Overview** LA-Mexico City1: **https://obs-sap-na-mexico-1.obs.na-mexico-1.myhuaweicloud.com/sapmon/templates/en/SAP-Systems-Overview** LA-Mexico City2: **https://obs-sap-la-north-2.obs.la-north-2.myhuaweicloud.com/sapmon/templates/en/SAP-Systems-Overview**

Template	Download Link
SAP HANA Metrics	AP-Bangkok: **https://obs-sap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/sapmon/templates/en/SAP-HANA** AP-Singapore: **https://obs-sap-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com/sapmon/templates/en/SAP-HANA** CN-Hong Kong: **https://obs-sap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/sapmon/templates/en/SAP-HANA** SA-Johannesburg: **https://obs-sap-af-south-1.obs.af-south-1.myhuaweicloud.com/sapmon/templates/en/SAP-HANA** TR-Istanbul: **https://obs-sap-tr-west-1.obs.tr-west-1.myhuaweicloud.com/sapmon/templates/en/SAP-HANA** LA-Santiago: **https://obs-sap-la-south-2.obs.la-south-2.myhuaweicloud.com/sapmon/templates/en/SAP-HANA** LA-Sao Paulo1: **https://obs-sap-sa-brazil-11.obs.sa-brazil-1.myhuaweicloud.com/sapmon/templates/en/SAP-HANA** LA-Mexico City1: **https://obs-sap-na-mexico-1.obs.na-mexico-1.myhuaweicloud.com/sapmon/templates/en/SAP-HANA** LA-Mexico City2: **https://obs-sap-la-north-2.obs.la-north-2.myhuaweicloud.com/sapmon/templates/en/SAP-HANA**

Template	Download Link
SAP NetWeaver Metrics	AP-Bangkok: **https://obs-sap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/sapmon/templates/en/SAP-NetWeaver** AP-Singapore: **https://obs-sap-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com/sapmon/templates/en/SAP-NetWeaver** CN-Hong Kong: **https://obs-sap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/sapmon/templates/en/SAP-NetWeaver** SA-Johannesburg: **https://obs-sap-af-south-1.obs.af-south-1.myhuaweicloud.com/sapmon/templates/en/SAP-NetWeaver** TR-Istanbul: **https://obs-sap-tr-west-1.obs.tr-west-1.myhuaweicloud.com/sapmon/templates/en/SAP-NetWeaver** LA-Santiago: **https://obs-sap-la-south-2.obs.la-south-2.myhuaweicloud.com/sapmon/templates/en/SAP-NetWeaver** LA-Sao Paulo1: **https://obs-sap-sa-brazil-11.obs.sa-brazil-1.myhuaweicloud.com/sapmon/templates/en/SAP-NetWeaver** LA-Mexico City1: **https://obs-sap-na-mexico-1.obs.na-mexico-1.myhuaweicloud.com/sapmon/templates/en/SAP-NetWeaver** LA-Mexico City2: **https://obs-sap-la-north-2.obs.la-north-2.myhuaweicloud.com/sapmon/templates/en/SAP-NetWeaver**

Template	Download Link
AOM Host Metrics	AP-Bangkok: **https://obs-sap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/sapmon/templates/en/AOM-Hosts** AP-Singapore: **https://obs-sap-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com/sapmon/templates/en/AOM-Hosts** CN-Hong Kong: **https://obs-sap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/sapmon/templates/en/AOM-Hosts** SA-Johannesburg: **https://obs-sap-af-south-1.obs.af-south-1.myhuaweicloud.com/sapmon/templates/en/AOM-Hosts** TR-Istanbul: **https://obs-sap-tr-west-1.obs.tr-west-1.myhuaweicloud.com/sapmon/templates/en/AOM-Hosts** LA-Santiago: **https://obs-sap-la-south-2.obs.la-south-2.myhuaweicloud.com/sapmon/templates/en/AOM-Hosts** LA-Sao Paulo1: **https://obs-sap-sa-brazil-11.obs.sa-brazil-1.myhuaweicloud.com/sapmon/templates/en/AOM-Hosts** LA-Mexico City1: **https://obs-sap-na-mexico-1.obs.na-mexico-1.myhuaweicloud.com/sapmon/templates/en/AOM-Hosts** LA-Mexico City2: **https://obs-sap-la-north-2.obs.la-north-2.myhuaweicloud.com/sapmon/templates/en/AOM-Hosts**

Step 3 Log in to Grafana and import the downloaded template to Grafana. Hover the cursor over  in the upper right corner of the page, click **Import** > **Upload .json File**, and select the template file to be uploaded. The import details page is displayed.

Step 4 Configure import parameters.

- Prometheus: Select the AOM data source created in en-us_topic_0000001165750083.xml#EN-US_TOPIC_0000001165750083/li4243935211186.

Step 5 After the import parameters are configured, click **Import**.

Step 6 Check whether any data reported to AOM exists in the imported template.

----End

6.6 Alarm Configuration

After SAP monitoring metrics are reported to AOM, you can use the alarm management function of AOM to notify you of abnormal metrics by email or SMS. For details, see **Alarm Management Usage Description**.

6.7 FAQs

6.7.1 Why No Data Is Available After I Configured Application Monitoring Successfully on the SAP Full Screen Monitoring Page?

Rectify the fault based on the causes listed in **Table 6-11**.

Table 6-11 Troubleshooting

Possible Cause	Solution
The SAP full screen configuration is incorrect or the configured application has been deleted.	Enter the edit mode and check whether the application, application SID, database, and database SID are configured as required. If they are incorrect, correct them and update the configuration.
The Agent has not been installed on the cloud server in the application.	Install the Agent and wait for several minutes.
The Agent data is still within the reporting cycle.	The minimum reporting cycle of the SAP monitoring agent is one minute. Wait for one minute and then refresh the data.
The cloud server meta information is incorrectly modified.	Enter the edit mode, update the monitoring configuration, and wait for several minutes.
The parameters in the **metrics.ini** configuration file are incorrect.	Check whether the configuration file is consistent with the actual application parameters.
The Agent and daemon processes are abnormal.	Check whether the Agent process is normal.
The Agent has not obtained data.	Check **/var/log/huawei/sapmon/sap_metrics.log** and see whether an error is reported when metrics are obtained.

6.7.2 How Do I Change the Collection Period of SAP Monitoring Metrics?

1. Log in to the node where the monitoring agent is installed.
2. Run the following command to open the **metrics.ini** file:

   vim /usr/local/sapmon/config/metrics.ini

```
[interval]
# unit is minute 1,5,15
database_version = 1
service_quantity = 1
database_ha_active = 1
sr_active = 1
threads = 1
recent_data_backup = 5
recent_savepoint = 1
column_tables_used_memory = 15
schema_used_memory = 15
disk_data_files = 1
disk_usage = 1
service_memory = 1
host_memory = 1
sql_service = 1
sql_top_time = 1
sql_top_mem = 1
connections_total = 1
table_cs_top_mem = 15
system_replication = 1
system_replication_takeover = 1
alerts = 1


# FOR APPLICATION
logged_in_users = 1
application_version = 1
instance_quantity = 1
application_ha_active = 1
abap_short_dumps = 1
abap_short_dumps_5m = 5
jobs = 1
lock_entries_usage = 1
extended_memory_utilization = 1
heap_memory_utilization = 1
work_processes = 1
update_records = 1
rfc_ping = 1
failed_idocs = 1
dialog_response_time = 1
dialog_db_request_time = 1
j2ee_running_process = 1
j2ee_thread = 1
j2ee_session = 1
j2ee_websession = 1
j2ee_ejbsession = 1
j2ee_vm_heap_size = 1
```

3. Press **i** to enter the edit mode. Change the collection period of the monitoring metric group.

   Example command:

   database_ha_active = 5

   NOTE

   The collection periods of metrics in the same group are managed uniformly. The unit of the collection period is minute, and the collection period can be 1 minute, 5 minutes, or 15 minutes.

4. Press **Esc** and run the **wq!** command to save and exit.

7 Best Practices of SAP Migration to HUAWEI CLOUD

7.1 Overview

7.1.1 Migration Scenarios

If your SAP system uses old version software whose performance is poor, or the system is deployed on cloud servers of small specifications with an inflexible architecture, you are suffering from slow system running and high O&M costs, especially when the businesses running on the system are growing. An increasing number of customers are choosing to migrate SAP systems to HUAWEI CLOUD to reduce costs and improve efficiency. HUAWEI CLOUD SAP on Cloud solution provides comprehensive cloud deployment schemes, improving the efficiency and reducing costs.

SAP migration projects are much more complex than traditional IT migration projects. An SAP migration project involves hardware migration, software upgrade, service and interface testing, project management, and risk control. In addition, a SAP migration project involves personnel and organizations from multiple parties, including customer's IT team, service team, migration implementor, and infrastructure provider. A successful migration project requires close collaboration among all the parties. During the migration, HUAWEI CLOUD provides

infrastructure and assistants the migration. In addition, HUAWEI CLOUD platform will facilitate the project implementation.

This document is not a replacement of SAP's or database vendor's official documents. This document is intended for SAP migration consultants and SAP practitioners. The restrictions and specifications of SAP software and databases in this document are subject to the official documents.

This document assumes that you are familiar with SAP system deployment and operations on HUAWEI CLOUD. If you are new to HUAWEI CLOUD SAP on Cloud solution, read the following documents:

- **SAP Deployment Guide**
- **SAP S/4HANA Quick Deployment Guide**
- **SAP HANA User Guide (Single Node)**
- **SAP NetWeaver User Guide**

This document describes how to migrate SAP systems from on-premises or other cloud platforms to HUAWEI CLOUD in four typical migration scenarios, as described in **Table 7-1**. You can select a suitable migration solution based on the actual requirements.

Table 7-1 Migration scenarios

Scenario	Description	Solution
Migrating SAP systems from x86 platform to HUAWEI CLOUD	In this scenario, you migrate an SAP system that is deployed on an x86 physical machine in your on-premises data center or a VMWare virtual machine (VM). The supported operating systems (OSs) of servers are listed in **OSs Supported by Different Types of ECSs**. There is no restriction on the database. After the migration to HUAWEI CLOUD, the database and OSs remain unchanged.	Use the following services and tools to migrate the system: • Use HUAWEI CLOUD **Server Migration Service (SMS) to migrate SAP application servers without service interruption**, replicating off-cloud servers to HUAWEI CLOUD. • If there is no requirement on database downtime, **use the SMS to migrate the database** of a non-production system. • To reduce the service downtime, **use the native database migration tool** to move the production system database to the cloud. For example, use SystemReplication, Oracle DataGuard, or SQL Logging Shipping migrate HANA.

Scenario	Description	Solution
Migrating SAP systems form a third-party cloud to HUAWEI CLOUD	In this scenario, you migrate an SAP system that is deployed on a third-party cloud. The supported server OSs are listed in **OSs Supported by Different Types of ECSs**. There is no restriction on the database. In addition, other cloud services, such as object storage service, can be involved in. After the migration to HUAWEI CLOUD, the database, OSs, and system architecture remain unchanged. The involved cloud services of other cloud vendors will be changed to those of HUAWEI CLOUD.	The solution is similar to that of the previous scenario. However, there are some differences: • You can easily adjust the network bandwidth between the third-party cloud platform and HUAWEI CLOUD. The maximum bandwidth can be hundreds of Mbit/s. • Generally, the system architecture does not need adjustment. If the on-premises system architecture is complex, you need to replan the deployment architecture of the system on the cloud. • Generally, an on-premises system contains only physical servers or VMs. A system on a third-party cloud may contain cloud service resources.
Migrating SAP systems from IBM or HP midrange computers to HUAWEI CLOUD	In this scenario, you migrate an SAP system deployed on IBM or HP midrange computers. The OSs are not supported by HUAWEI CLOUD. There is no restriction on the database. After the migration, the OSs are changed to those supported by HUAWEI CLOUD, and the database remains unchanged.	You need to deployed application servers and the database server of the system on HUAWEI CLOUD. The target system is redeployed on HUAWEI CLOUD ECSs or BMSs. Solutions for database migration are as follows: • Use the **SAP R3load Export/ Import function** to migrate the database. • Or use some **native database tools**, such as Oracle GoldenGate or Oracle XTTS, to back up databases.

Scenario	Description	Solution
Migrating SAP applications running on a non-HANA database to HUAWEI CLOUD SAP HANA	In this scenario, you migrate an SAP system deployed in the local data center. The database is a non-HANA database (such as Sybase, Oracle, and DB2). The target end is HUAWEI CLOUD SAP HANA system. The server OSs may change.	The project includes system migration, software upgrade, and database and OS change. • Use the **database migration option (DMO) of SAP SUM** to upgrade and migrate the SAP system to HUAWEI CLOUD SAP HANA system. • Use the **Classical Migration to SAP HANA** solution. Use SUM to upgrade the system to a supported version, and then use the System Copy function of SWPM to migrate the system onto the HANA database.

Due to the complexity of a migration project, this section will not include the detailed migration processes, but only focuses on the part related to HUAWEI CLOUD. There are two types of migration:

- Homogeneous migration: The databases and OSs of the source and destination servers remain unchanged, and the software can be upgraded in the homogeneous migration.
- Heterogeneous migration: Either of databases and OSs are changed.

You can view the following examples:

- Homogeneous migration:
  - **Migrating the SAP System from the x86 Platform to HUAWEI CLOUD**
  - **Migrating from a Third-Party Cloud to HUAWEI CLOUD**
- Heterogeneous migration:
  - **Migrating from IBM or HP Midrange Computers to HUAWEI CLOUD**
  - **Migrating SAP Applications Running on a Non-HANA Database to HUAWEI CLOUD SAP HANA**

7.1.2 Migration Solutions

Table **Migration services and tools** describes the services and tools recommended by HUAWEI CLOUD to migrate an SAP system. The table compares the application scopes, downtime, and migration complexity of the solutions. You can select a solution that meets your requirements. For details about migration operations of each solution, see **Migration Solution Details**.

Table 7-2 Migration services and tools

Service/ Tool	Advantages and Disadvantages	Application Scope	Database Interruption Duration (Bandwidth: 100 Mbit/s)		Technical Support	Scenarios
			500 GB database	**2 TB database**		
Server Migration Service or Server Migration Tool (P2V and V2V migration tools)	**Advantages**: The migration of SAP application servers and database servers is easy. **Disadvantages**: The downtime is long. Only the X86 platform is supported.	Applies to homogeneous x86 platform migration. The service and tool can migrate SAP applications and databases. Interrupt the database service when you migrate the database using SMS.	About 18 hours	About 65 hours	HUAWEI CLOUD Server Migration Service	Migrating an SAP system from the X86 platform to HUAWEI CLOUD Migrating an SAP system from a third-party cloud to HUAWEI CLOUD
Database backup and restoration function	**Advantages**: Short downtime **Disadvantages**: Only homogeneous migration is supported.	Applies to the migration between databases of the same type.	**Full migration**: About 20 hours **Increment migration**: About 2 hours	**Full migration**: About 70 hours **Increment migration**: About 2 hours	Database provider	Migrating an SAP system from the X86 platform to HUAWEI CLOUD Migrating an SAP system from a third-party cloud to HUAWEI CLOUD

Service/ Tool	Advantages and Disadvantages	Application Scope	Database Interruption Duration (Bandwidth: 100 Mbit/s)		Technical Support	Scenarios
Database replication (including HANA SR and Oracle Data Guard)	**Advantages**: The downtime is shortened to minutes. **Disadvantages**: The operations are complex and require expertise.	Applies to the migration between databases of the same type.	Within 1 hour	Within 1 hour	Database provider	Migrating an SAP system from the X86 platform to HUAWEI CLOUD Migrating an SAP system from a third-party cloud to HUAWEI CLOUD Migrating an SAP system from IBM midrange computers to HUAWEI CLOUD (with database restrictions)

Service/ Tool	Advantages and Disadvantages	Application Scope	Database Interruption Duration (Bandwidth: 100 Mbit/s)		Technical Support	Scenarios
DMO of SAP SUM	**Advantages**: You can upgrade the SAP system while migrating the database. **Disadvantages**: The operations are complex and require expertise.	Applies to homogeneous and heterogeneous migration and supports SAP upgrade during the database migration. Migrates data from other databases to the HANA database.	About 10 hours	About 45 hours	SAP	Migrating an SAP system from the x86 platform to HUAWEI CLOUD Migrating an SAP system from a third-party cloud to HUAWEI CLOUD Migrating an SAP system from IBM midrange computers to HUAWEI CLOUD Migrating an SAP system running on a non-HANA database to HUAWEI CLOUD SAP HANA database

Service/ Tool	Advantages and Disadvantages	Application Scope	Database Interruption Duration (Bandwidth: 100 Mbit/s)		Technical Support	Scenarios
R3load (parallel import and export function)	**Advantages**: a standard SAP tool that is easy to use **Disadvantages**: The downtime is long, which depends on the database size.	Supports homogeneous and heterogeneous migration.	About 24 hours	About 48 hours	SAP	Migrating an SAP system from the x86 platform to HUAWEI CLOUD Migrating an SAP system from a third-party cloud to HUAWEI CLOUD Migrating an SAP system from IBM midrange computers to HUAWEI CLOUD Migrating an SAP system running on a non-HANA database to HUAWEI CLOUD SAP HANA database

7.1.3 Related Cloud Services

Public cloud refers to a cloud based on the standard cloud computing model, in which service providers make resources available to the general public over the Internet. The core attribute of a public cloud is its shared resources. HUAWEI CLOUD is a public cloud and provides the following cloud services to implement SAP system migration. You can use HUAWEI CLOUD services independently or together to meet your migration requirements. **Table 7-3** lists the cloud services that can be used during the migration.

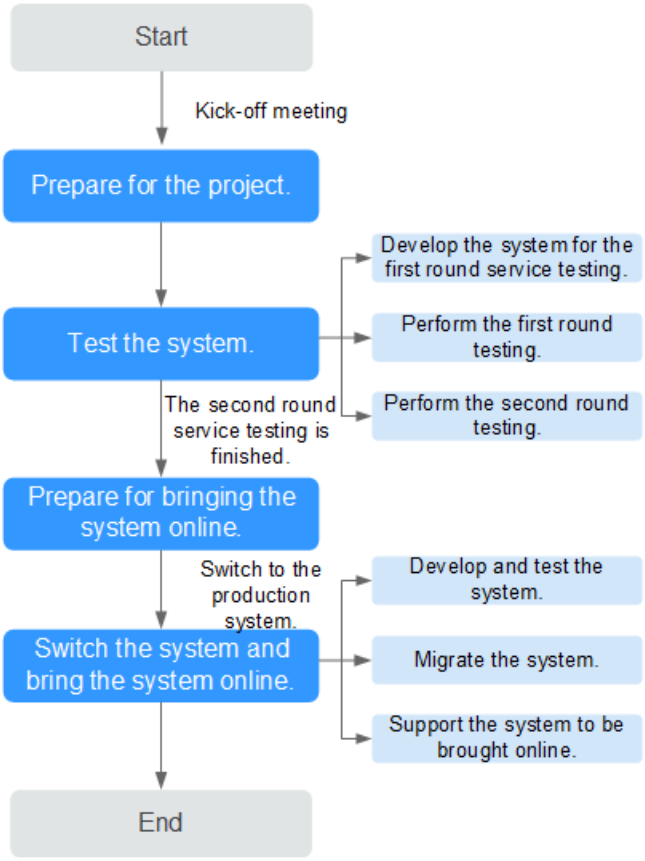
Table 7-3 HUAWEI CLOUD services

Service	Features
SMS	Server Migration Service provides P2V and V2V migration services to help you migrate applications and data from on-premises X86 physical servers or VMs on private or public clouds to HUAWEI CLOUD Elastic Cloud Servers (ECSs). SMS migrates SAP application servers while the applications are running, and migrates database servers after the database service is stopped. You can use SMS to migrate incremental data. For more information about SMS, see **What is Server Migration Service**.
IMS	If your SAP application servers can be converted into image files, and the types and OSs of the image files are listed in **Formats and OSs Supported for External Image Files**, you can create the SAP application server image files as private images on HUAWEI CLOUD, and use the images to quickly deploy new application servers. For details, see **Creating a Linux System Disk Image from an External Image File** and **Creating a Windows System Disk Image from an External Image File**.
OMS	Object Storage Migration Service is an online data migration service. If the source SAP system has object storage data (such as database backup files and software installation media) stored on a third-party cloud, the OMS can smoothly migrate the data from the third-party cloud to the HUAWEI CLOUD. Note: This service applies only to migrate objects storage from a third-party cloud. For details about how to use the OMS, see **Object Storage Migration Service Introduction**.
DES	Data Express Service is a massive data transmission solution. It allows transmitting a large amount of data using Teleport devices or disks (with external USB interfaces, SATA interfaces, or SAS interfaces) to HUAWEI CLOUD. DES helps to address issues facing massive data transmission such as high network costs and long transmission time. If the source SAP system has storage devices with a large amount of data, for example, the storage device where the database backup directory resides, you can use DES for migration. Whether to use DES depends on the amount of data and the network bandwidth. For details, see **DES Application Scenarios**. For more information about DES, see the **DES Product Overview**.

7.2 Migration Procedure

Figure 7-1 shows the implementation procedure of a typical SAP migration project.

Figure 7-1 Migration procedure



The implementation phases are as follows:

1. Project Preparation

   Based on specific requirements and application system information, assess the risks and feasibility of the cloud migration. Collect information and assessment results to plan the project and design the solution. Manage the project, for example, establish a project team and formulate team management regulations.

   HUAWEI CLOUD provides a system deployment solution and offers migration suggestions. The solution includes computing, network, and security resources on the cloud, and account systems.

2. Tests and Drills

   Set up the migration environment to ensure that the system will meet the requirements after the migration to HUAWEI CLOUD. Ensure that no problem remains unsolved in each phase of the migration project.

   HUAWEI CLOUD provides a series of user and deployment guides to help you migrate the system:

  - **SAP HANA User Guide (Single Node)**
  - **SAP NetWeaver User Guide**
  - **SAP Business One User Guide**
  - **SAP S/4HANA Quick Deployment Guide**
  - **SAP Business One Quick Deployment Guide**
  - **SAP Deployment Guide**

3. Preparations for Bringing the System Online

   Optimize the migration solution based on the drill and test results and determine the final solution. List known issues and transmission items. Test HA, switchover, and shutdown solutions, and decide the switchover and shutdown plan. Design and verify the rollback solution.

   This task is performed by the migration implementor and supported by HUAWEI CLOUD.

4. System Switchover

   Migrate the workload according to the final switchover plan and solution determined based on the system tests.

   This task is performed by the migration implementor and supported by HUAWEI CLOUD.

5. Bringing the System Online

   Continuously monitor the system after it is brought online and optimize the cloud architecture if necessary.

   This task is performed by the migration implementor and supported by HUAWEI CLOUD.

7.3 Migrating the SAP System from the x86 Platform to HUAWEI CLOUD

7.3.1 Description

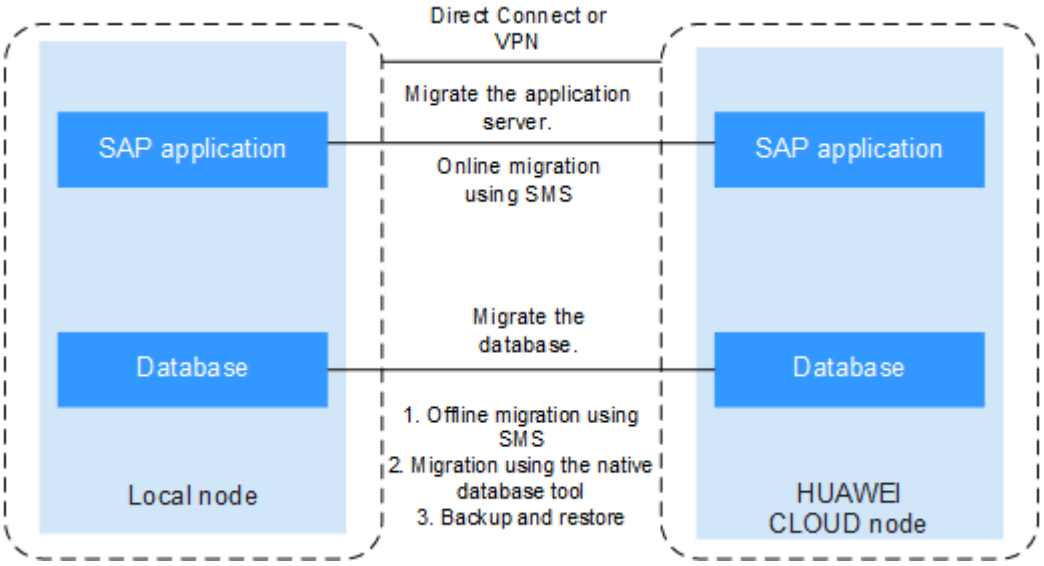
In this scenario, you migrate an SAP system that is deployed on an X86 physical machine in your on-premises data center or VMWare VM. The supported OSs of servers are listed in **OSs Supported by Different Types of ECSs**. There is no restriction on the database. After the migration to HUAWEI CLOUD, the database and OS remain unchanged.

Use HUAWEI CLOUD Server Migration Service to migrate SAP application servers without service interruption, replicating off-cloud servers to HUAWEI CLOUD. For database migration:

- Non-production system database: If there is no requirement on database downtime, use Server Migration Service to migrate the database offline.
- Production system database: To reduce the service downtime, use the native database migration tool to migrate the database.

Figure 7-2 shows the migration plan.

Figure 7-2 Migrating the SAP system from the x86 platform to HUAWEI CLOUD



7.3.2 Solution Design

Deployment Plan

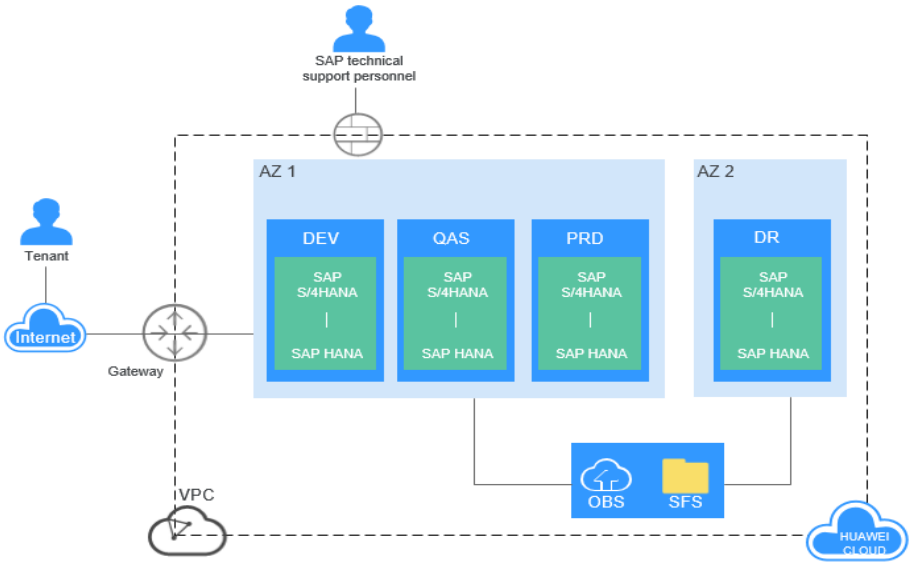
Use HUAWEI CLOUD services for the deployment. Specifically, use ECS or BMS for server computing resources, and EVS and SFS for storage.

Table 7-4 Deployment plan

Migrate Object	Source	Target
Application server	Physical server	ECS
Database server	Physical server	ECS or BMS
Storage	Physical hard disk	EVS

Figure 7-3 shows a typical SAP system deployment architecture on HUAWEI CLOUD. The architecture of a new deployment or that used in a migration to HUAWEI CLOUD is similar to this one.

Figure 7-3 SAP deployment architecture



For more features and details, see **SAP Deployment Guide**.

You can also visit the SAP official website to learn more about the SAP products related to HUAWEI CLOUD. **Table 7-5** lists the SAP notes.

Table 7-5 HUAWEI CLOUD-related SAP notes

SAP Note #	Title
2582296	SAP Applications on Huawei Cloud: Supported Products and Huawei Cloud VM types
2582305	SAP on Huawei Cloud: Support prerequisites
2570214	Linux on Huawei Cloud: Adaption of your SAP License
2570198	SAP on Linux with Huawei Cloud: Enhanced Monitoring
2644322	SAP Adaptive Server Enterprise (ASE) 16.0 Certification Report for Huawei Cloud

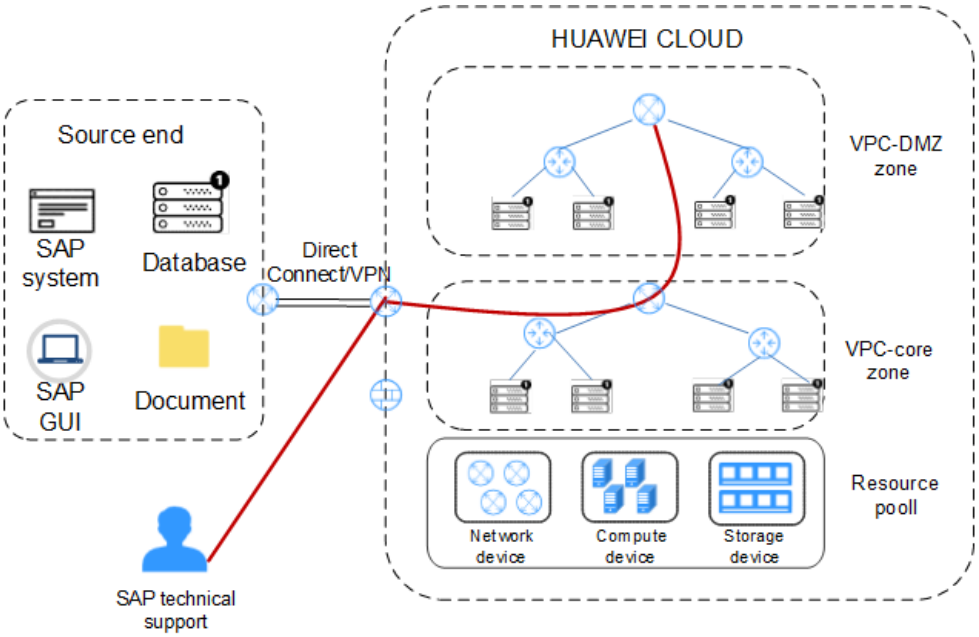
Determine the number and specifications of servers deployed on HUAWEI CLOUD based on the source system status, service requirements, and the preceding information. Then, design the HUAWEI CLOUD deployment plan. The deployment plan needs to contain the detailed information about cloud product selection and networking plan to guide subsequent resource provisioning.

Networking Plan

After the migration, a VPC is used on the cloud. For details about subnet planning, see the **VPC User Guide**. HUAWEI CLOUD is connected with the on-premises IDC using EIP, VPN, or Direct Connect.

HUAWEI CLOUD VPC is an isolated and private virtual network environment that users apply for on the HUAWEI CLOUD. You can configure IP address segments, subnets, and security groups, assign EIPs, and allocate bandwidths in a VPC. **Figure 7-4** shows the network architecture.

Figure 7-4 Network architecture



VPC 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. The SAP technical support personnel can access the system deployed on HUAWEI CLOUD using the public IP address.

- 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.

Security Design

Enterprises store core data in the SAP system. HUAWEI CLOUD ensures the security of the SAP system based on the cloud platform security and network configurations.

You are recommended to divide the cloud-based system (production environment and development and test environment) into zones of different security levels, including the management, application, SAP DB, and demilitarized zones (DMZ). The zones are isolated from each other using VPCs or subnets.

Figure 7-5 Production environment security solution

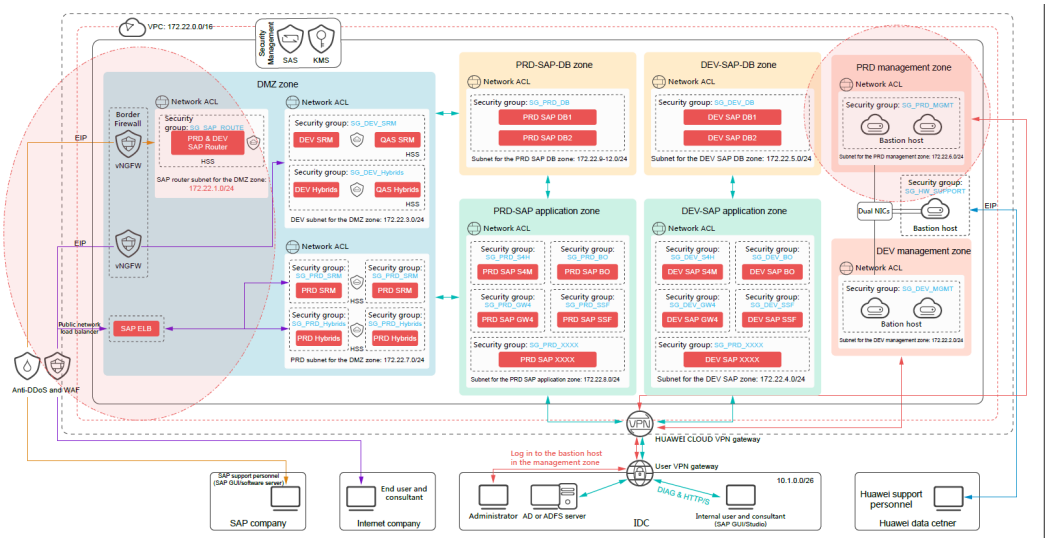
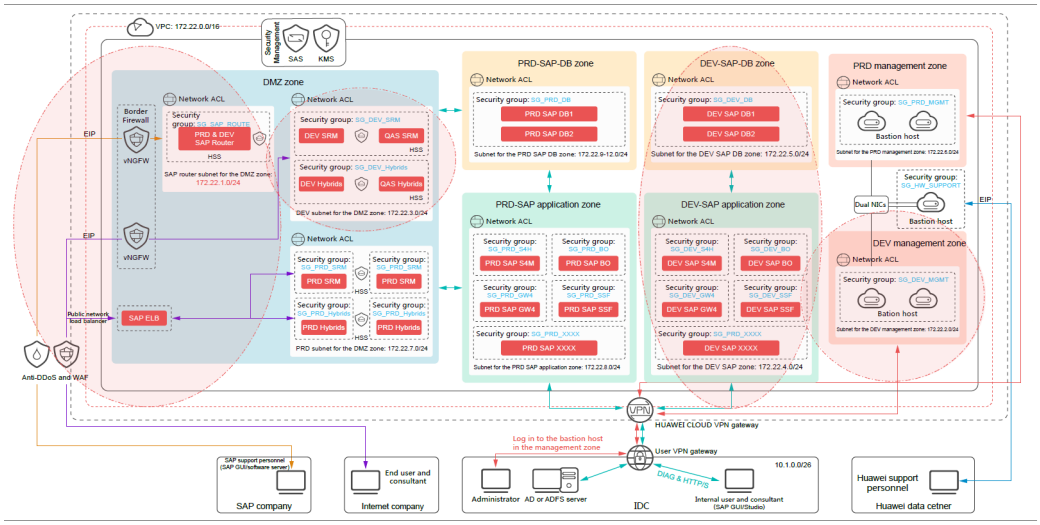


Figure 7-6 Development and test environment security solution

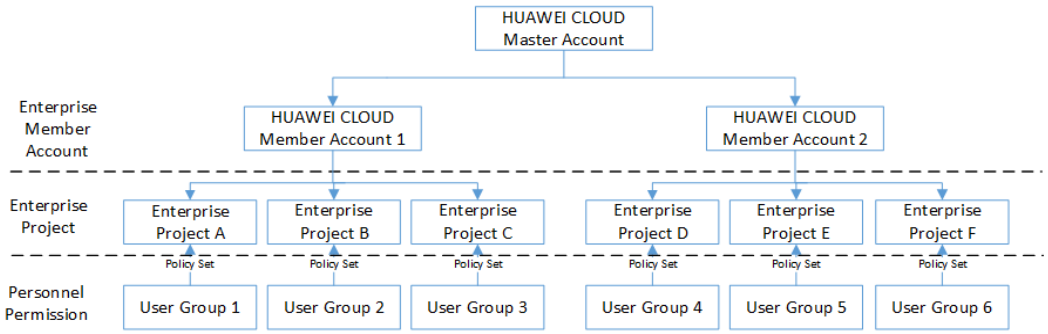


For details, see **SAP Security White Paper**.

Service Account System Design

After the system is deployed on the cloud, HUAWEI CLOUD provides enterprise management services for enterprise group uses to manage the employees, finance, and materials in multi-level organizations and multi-project mode and to standardize enterprise operation requirements on HUAWEI CLOUD. **Figure 7-7** shows the HUAWEI CLOUD enterprise accounts. For details, see **Enterprise Management**.

Figure 7-7 Enterprise accounts



Migration Solution

Table 7-6 lists the recommended migration solution. For details about the migration methods, see **Migration Solution Details**.

Table 7-6 Migration Solution

Migrate Object	Migration Plan	Description
Application server	SMS or SMT **NOTE** If the source server cannot access SMS, use SMT.	SMS supports online and incremental migration. You are recommended to migrate SAP application servers online in incremental mode for multiple times. **Data transmission time = Actual data volume/Actual network bandwidth** **Table 7-7** lists the estimated time for transmitting 1 TB data. Estimate the time required for transmitting data based on the actual data volume. If the data cannot be transmitted within the estimated time, increase the network bandwidth.

Migrate Object	Migration Plan	Description
Database server	• The non-production system database can be migrated offline using SMS. • The production system database is migrated using the native database tool, such as the database backup and restore tool.	If you use SMS to migrate the database, SMS performs online clone of the OS. All the data on the OS, such as the application software and system configurations, is replicated to the target system. Generally, the application software can be started at the target system. However, if the database is migrated when it is running, the database may fail to start after the migration. Therefore, you need to migrate the database offline when you use SMS.

Table 7-7 Theoretical time for transmitting 1 TB data

Network Bandwidth	2 Mbit/s	10 Mbit/s	50 Mbit/s	100 Mbit/s
Theoretical time (80% network utilization rate) **NOTE** Transmission time (days) = [Total capacity (KB)]/[Bandwidth (Mbit/s) x 125 x Network utilization rate x 60 (seconds) x 60 (minutes) x 24 (hours)]	106 days	13 days	60 hours	30 hours

Service Switchover Plan

The owner of the service switchover plan is the migration implementor. This section provides an example of the service switchover plan.

Table 7-8 Switchover plan example

Migration Plan	Switchover Plan	Impact
Use SMS to migrate application servers online, and use SMT to migrate database servers offline.	1. After using SMS to migrate the application servers to HUAWEI CLOUD, use incremental replication to synchronize the source end server changes to HUAWEI CLOUD online. 2. After stopping the database, use SMS to migrate the database servers to HUAWEI CLOUD.	The database servers are migrated offline, so the interruption will be long. This plan applies to the non-production system. Interruption duration = **Data transmission time for the database server + Commissioning time after the migration**
Deploy application servers on the cloud, and use the backup and restore plan for database servers.	1. Commission the application servers after the deployment. 2. Restore the database servers using full backup. 3. Stop the database at the source end. Upload the incremental data and necessary log files to the database on the cloud. Restore the database using the incremental data.	Stop the servers at the source end before the incremental backup of the last time. Compared with the offline migration plan, this plan causes shorter interruption, so it applies to the production system. Interruption duration = **Time for incremental backup + Time for transmitting incremental data + Time for restoring the incremental data**

7.3.3 Preparing the Migration Environment

7.3.3.1 Preparing Resources

To ensure smooth migration, you need to perform the following operations:

1. Prepare the network environment.
   a. Follow the descriptions in **Networking Plan** to interconnect the source server with HUAWEI CLOUD, establish network connectivity using Cloud Connect, and configure VPN. For details, see **SAP Deployment Guide**.
   b. Set up the HUAWEI CLOUD network environment, including creating VPCs, subnets, and security groups. For details, see the related section in the **SAP Deployment Guide**.
2. Prepare software tools required for the migration, such as SAP migration software and specific database migration tool.

3. Prepare resources at the source end.
   a. Back up the data at the source end, including important files and software installation packages. You are advised to back up the data to HUAWEI CLOUD OBS.
   b. Check the source server settings. Check whether the source server OS meets migration requirements by referring to **OSs Supported by Different Types of ECSs**, and check the data volume on the source server.
4. Prepare resources at the target end.
   a. Provision HUAWEI CLOUD server resources based on **Deployment Plan**.
   b. Set the security parameters based on **Security Design**.
   c. Purchase OBS, SFS, OMS, and DES on HUAWEI CLOUD as required.

7.3.3.2 Migrating Application Servers to HUAWEI CLOUD

You can migrate SAP application servers to HUAWEI CLOUD using either of the following methods:

- **Method 1: Using SMS**
- **Method 2: Importing Images**

Method 1: Using SMS is recommended. If VMs are at the source end, you can use **Method 2: Importing Images**.

Method 1: Using SMS

If you use SMS for migration, the systems at the source end and target end are basically the same. For details about the changes, see **What Are the Differences Between Target ECSs and Source Servers After the Migration?**.

The following uses an SAP HANA database server as an example to describe the migration procedure.

Step 1 Back up the source-end data and software.

Step 2 Obtain the AK/SK of the account to which the target server belongs.

- If you need to use an account to migrate servers, see **How Do I Obtain the AK and SK of an Account?**.
- If you have created an IAM user under this account, grant the permission to the IAM user and use the IAM user to create the AK/SK. For details, see **How Do I Obtain the AK and SK of an IAM User?**.

Step 3 Install the migration Agent on the source server. For details, see **How Can I Install the Migration Agent on Source Servers?**. Enter the AK/SK obtained in **Step 2** when they are required by SMS-Agent.

Step 4 After the migration Agent is started successfully, it automatically collects information about the source server and sends collected information to SMS. SMS automatically checks whether the source server information is valid and whether the source server can be migrated. After the migration Agent uploads source server information to SMS, you can log in to the HUAWEI CLOUD management console at any time to view information about the source server using the HUAWEI CLOUD account of the target server. For details, see **Viewing Check Results**.

Step 5 Start the migration task. For details, see **Creating and Starting a Migration Task**.

NOTE

- Ensure that source servers are on during the migration.
- When you migrate the database, stop the database before the last time synchronization and then migrate it offline.

Step 6 After the migration task is complete, log in to the target server using the source server login mode. Check whether the basic functions are normal, including the network and storage.

Step 7 Modify the basic OS settings of the target server to adapt to HUAWEI CLOUD.

1. Modify the DNS and NTP configurations. For details, see **How Can I Configure the NTP and DNS Servers for an ECS?**.
2. (Optional) Install and configure Cloud-Init. For details, see **Installing Cloud-Init** and **Configuring Cloud-Init**.

   For more about Cloud-Init, see **Cloud-init**.
3. (Optional) Install the HUAWEI CLOUD one-click password reset plug-in. For details, see **(Optional) Installing the One-Click Password Reset Plug-in**.
4. Modify the host name and the **hosts** file as required. For details, see **Changing Host Name**.
5. Install Data Provider.

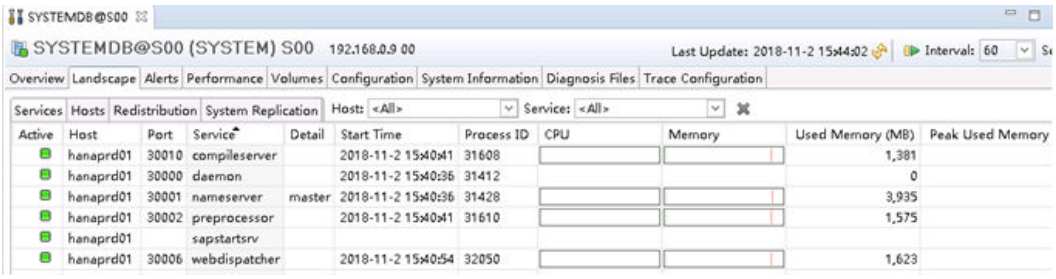
   Data Provider is the SAP metric collector on HUAWEI CLOUD. For details about how to install and configure Data Provider, see **Data Provider for SAP User Guide**.
6. Restart the server and check whether other OS errors occur.

Step 8 Check whether the SAP HANA database can start properly.

1. Switch to user *{$SID}***ADM** and run the **HDB start** command to start the database.
2. Run the **sapcontrol -nr 00 -function GetProcessList** command to query the status of all SAP HANA processes. The command output shows that all SAP HANA processes are in the GREEN state.

```
hanaprd01:HDB:s00adm /usr/sap/S00/HDB00 13> sapcontrol -nr 00 -function GetProcessList

02.11.2018 15:39:22
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
hdbdaemon, HDB Daemon, GREEN, Running, 2018 11 02 15:34:30, 0:04:52, 29652
hdbcompileserver, HDB Compileserver, GREEN, Running, 2018 11 02 15:34:36, 0:04:46, 29875
hdbindexserver, HDB Indexserver-S00, GREEN, Running, 2018 11 02 15:34:37, 0:04:45, 29918
hdbnameserver, HDB Nameserver, GREEN, Running, 2018 11 02 15:34:31, 0:04:51, 29679
hdbpreprocessor, HDB Preprocessor, GREEN, Running, 2018 11 02 15:34:36, 0:04:46, 29877
hdbwebdispatcher, HDB Web Dispatcher, GREEN, Running, 2018 11 02 15:34:51, 0:04:31, 30300
hdbxsengine, HDB XSEngine-S00, GREEN, Running, 2018 11 02 15:34:37, 0:04:45, 29920
```

3. Use SAP HANA Studio to connect to the SAP HANA database and check whether the connection is successful and whether all processes are in the normal state.



Step 9 (Optional) After a migration task is complete, you can use SMS to synchronize the incremental data from the source servers to the target servers as needed. For details about how to perform the incremental synchronization, see **Synchronizing Data After a Migration Task Is Complete**.

NOTE

After the incremental synchronization, the status of the target server becomes consistent with the source server. Perform **Step 6** to **Step 8** after the synchronization is complete.

Step 10 Connect the application with the database to test whether the system is functional.

----End

Method 2: Importing Images

If your source servers can be converted into image files, and the type and OS of the image files are listed in **Formats and OSs Supported for External Image Files**, you can create the source server image files as private images on HUAWEI CLOUD, and use the images to quickly deploy new servers on HUAWEI CLOUD.

Step 1 Export the source server as **images of formats supported by HUAWEI CLOUD**. You can use the recommended tool to convert the image format. For details, see **Converting the Image Format Using qemu-img**.

Step 2 Upload the external image file to the OBS bucket. For details, see **Uploading an External Image File**.

Step 3 Select the uploaded image file on the management console and register the image file as a private image. For details, see **Creating a Linux System Disk Image from an External Image File** and **Creating a Windows System Disk Image from an External Image File**.

Step 4 Use the created image to provision new servers in the planned environment based on the design.

----End

7.3.3.3 Migrating the Database to HUAWEI CLOUD

You can use either of the following methods to migrate the database:

- You can use SMS to migrate the database, but the migration must be performed offline. For details, see **Method 1: Using SMS**.
- If you have high database downtime requirements, you can use the database backup and restoration function or database synchronization technology to migrate the database.

This document uses the SAP HANA database as an example to describe how to reduce migration RTO. For details, see **Method 2: Using the Database Backup and Restore Function** and **Method 3: Using the Database Synchronization Technology**.

Method 1: Using SMS

To ensure data consistency between the target system and the source system, you need to stop services at the source end before the last time incremental synchronization. Then, repeat procedures in **Method 1: Using SMS**.

Method 2: Using the Database Backup and Restore Function

The database backup and restoration function uses the backup of the source system data and restore it in the target system.

The following uses the SAP HANA database as an example to describe how to use method to migrate the database to HUAWEI CLOUD.

Step 1 Migrate the source database to HUAWEI CLOUD by performing steps provided in **Migrating Application Servers to HUAWEI CLOUD**. Alternatively, deploy SAP HANA servers on HUAWEI CLOUD. For details, see **SAP HANA User Guide**.

Step 2 Stop the database service at the source end and perform a full backup for the database. Ensure that the necessary logs are retained. Transfer the backup file to the target server on HUAWEI CLOUD.

You can also use OBS to transfer files. OBS provides multiple tools to accelerate the file upload. For details, see **OBS Tools**.

Step 3 Log in to the target server and use HANA Studio or run the hdbsql command to restore the backup data to the database. For details, see **SAP HANA Administration Guide**.

NOTE

- If the size of a full backup file is large, data transmission and restoration will take a long time. To reduce the downtime, you can restore the data on the target system using a full backup without stopping services on the source system. After you stop the services at the source end, perform a differential or incremental backup and then restore the differential or incremental backup to the target system.
- Alternatively, you can use SMS to migrate source servers to HUAWEI CLOUD so that you do not need to deploy the system again, and part of the backup data can be migrated to the target server. You only need to perform a differential or incremental backup and then restore it to the target system.

Step 4 Start the SAP HANA database on the cloud and verify that the database is functional and the data is intact.

Step 5 Connect the application with the database to test whether the system is functional.

----End

Method 3: Using the Database Synchronization Technology

Databases have their native tools to support synchronous data replication, such as **HANA System Replication**, **Oracle Data Guard**, **On Availability Groups (SQL Server)**, and **Q Replication** of DB2.

The following uses the SAP HANA database as an example to describe how to use HANA System Replication to migrate the database to HUAWEI CLOUD.

Step 1 Migrate the source database to HUAWEI CLOUD by performing steps provided in **Migrating Application Servers to HUAWEI CLOUD**. Alternatively, you can deploy SAP HANA servers at HUAWEI CLOUD. For details, see **SAP HANA User Guide**.

Step 2 Configure asynchronous system replication from the source SAP HANA database to the target SAP HANA database. For details, see **SAP HANA Administration Guide**.

Step 3 Before the system switchover, check HANA System Replication to ensure that the data replication status is normal, and then stop the source SAP application system.

Step 4 Run the SAP HANA takeover command on the target database to check the database running status. For details, see **SAP HANA Administration Guide**.

Step 5 Start the target SAP application system on the cloud and ensure that the connection between the application system and HANA database is normal.

Step 6 Check the system availability and service data integrity on the service side.

----End

7.3.4 Tests and Drills

After setting up the environment required for the migration, you can perform tests on target system service functions and service migration drills.

Migration Drills

Use the designed service switchover plan to perform a drill to ensure that the plan meets the requirements. For details about the service switchover plan, see **Service Switchover Plan**.

Service Tests

Check the target system on the cloud and perform complete verification on key service processes. Ensure that the system after the migration can meet service requirements.

7.3.5 Switchover and Go-Live

Perform the official system migration according to the plan specified in the migration drill. You can switch over services of the development and test system first, verify that the development and test system is running properly, and then cut over services of the production system.

7.4 Migrating from a Third-Party Cloud to HUAWEI CLOUD

7.4.1 Scenario Description

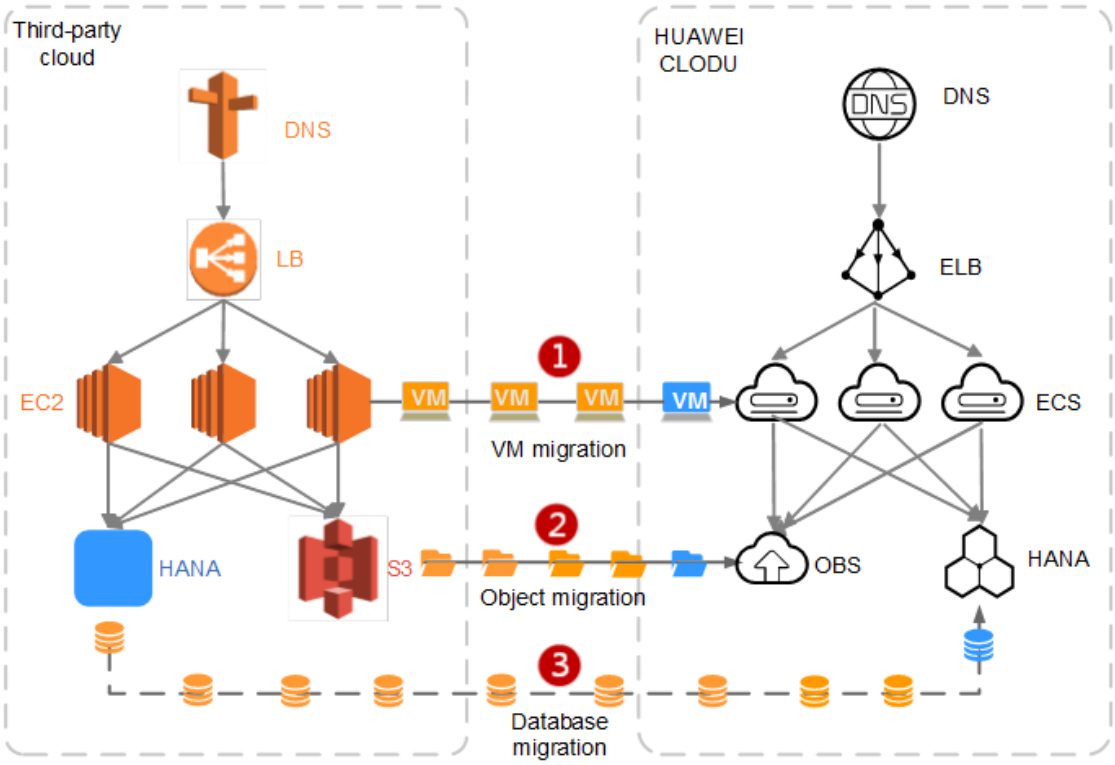
In this scenario, you migrate the SAP system that is deployed on a third-party cloud. The supported server OSs are listed in **OSs Supported by Different Types of ECSs**. There is no restriction on the database. In addition, other cloud services, such as object storage service, can be involved in. After the migration to HUAWEI CLOUD, the database, OS, and system architecture remain unchanged. The involved cloud services of other cloud vendors will be changed to those of HUAWEI CLOUD.

This scenario is similar to the previous one. However, there are some differences:

- You can easily adjust the network bandwidth between the third-party cloud platform and HUAWEI CLOUD. The maximum bandwidth can be hundreds of Mbit/s.
- Generally, the system architecture does not need adjustment. If the on-premises system architecture is complex, you need to replan the deployment architecture of the system on the cloud.
- Generally, an on-premises system contains only physical servers or VMs. A system on a third-party cloud may contain cloud service resources.

Figure 7-8 shows an example. You can use the same system architecture as the third-party cloud to reduce migration complexity.

Figure 7-8 Migrating from a third-party cloud



7.4.2 Solution Design

Deployment Plan

To deploy the system on HUAWEI CLOUD, keep the application architecture unchanged and replace third-party cloud services with HUAWEI CLOUD services.

For details about the deployment solution design, refer to section **Deployment Plan**.

Networking Plan

The system networking on HUAWEI CLOUD is the same as that of the source end. The system connects to a third-party cloud through EIP and VPN or Direct Connect.

For details, see **Networking Plan**.

Security Design

- For details, see **Security Design**. Find more information in the **SAP Security White Paper**.
- For details about permission management, see **Service Account System Design**.

Migration Plan

Table 7-9 lists the recommended migration solutions.

Table 7-9 Migration solutions

Object	Solution	Description
Application servers	Server Migration Service **NOTE** The source server must access HUAWEI CLOUD SMS. Bind a public IP address to the source server.	SMS supports online and incremental migration. You can migrate SAP application servers while the applications are running, and synchronize incremental data several times. **Data transmission time = Actual data volume/Actual network bandwidth** Table 7-10 lists the estimated time for transmitting 1 TB data. Estimate the time required for transmitting data based on the actual data volume. If the data cannot be transmitted within the estimated time, increase the network bandwidth.
Database	• You can migrate a non-production system database after stop the database service using SMS. • You can use the database backup and restoration function or other native database tools to migration the production system database.	When using SMS, you need to stop the database servcie before the migration to ensure data consistency. The service interruption duration of using native database tool is shorter than that of using the SMS. For details about the estimated interruption duration, see section Table 7-2.

Table 7-10 Theoretical time for transmitting 1 TB data

Network Bandwidth	2 Mbit/s	10 Mbit/s	50 Mbit/s	100 Mbit/s
Theoretical time (80% network utilization rate) **NOTE** Transmission time (days) = [Total capacity (KB)]/[Bandwidth (Mbit/s) x 125 x Network utilization rate x 60 (seconds) x 60 (minutes) x 24 (hours)]	106 days	13 days	60 hours	30 hours

Service Switchover Plan

The owner of the service switchover plan is the migration implementor. This section provides an example of the service switchover plan.

Table 7-11 Switchover plan example

Migration Solution	Switchover Plan	Impact
The application servers are redeployed on or migrated to HUAWEI CLOUD by importing images. The database is restored using backup data.	1. Redeploy and commission the application servers on HUAWEI CLOUD. 2. Back up the entire source database server and upload full backups to the target system to restore data to the target database. 3. Stop the source database, upload the incremental or differential data and required log files to HUAWEI CLOUD, and restore the backup data to the target database.	The service interruption duration = **the incremental backup duration + the incremental backup transmission duration + the incremental data restoration duration**
Use SMS to migrate the application servers, and the database replication function to synchronize database.	1. After the application servers are migrated to HUAWEI CLOUD using SMS, use incremental replication to synchronize the servers. 2. Configure synchronous replication from the on-premises database to the cloud database. Stop the services on the source end and perform the service takeover on the cloud database.	Stop source end services only after the last incremental synchronization is performed using SMS. After the cloud database takes over the services, the service switchover is complete. The service interruption duration is the **database switchover duration**.

7.4.3 Preparing the Migration Environment

7.4.3.1 Preparing Resources

For details, see **Preparing Resources**.

7.4.3.2 Migrating Application Servers to HUAWEI CLOUD

Perform operations provided in **Method 1: Using SMS** to migrate the application servers. You can also use the method described in **Method 2: Importing Images**.

The procedure is the same as that described in **Migrating Application Servers to HUAWEI CLOUD**.

7.4.3.3 Migrating the Database to HUAWEI CLOUD

The migration method is the same as that of scenario 1. For details, see **Migrating the Database to HUAWEI CLOUD**.

7.4.4 Tests and Drills

For details, see **Tests and Drills**.

7.4.5 Switchover and Go-Live

For details, see **Switchover and Go-Live**.

7.5 Migrating from IBM or HP Midrange Computers to HUAWEI CLOUD

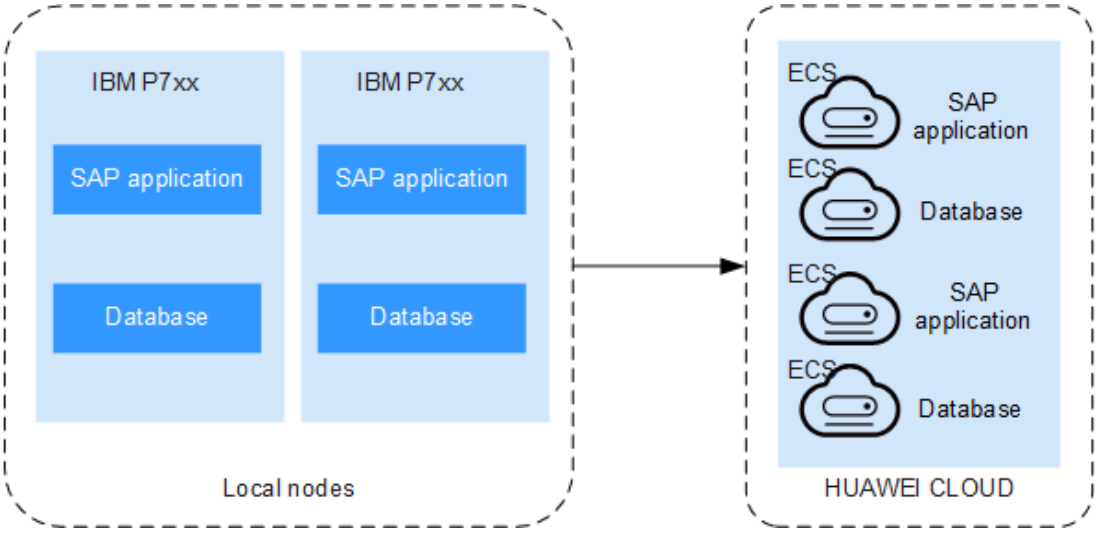
7.5.1 Scenario Description

In this scenario, you migrate the SAP system deployed on IBM or HP midrange computers. The OSs are not supported by HUAWEI CLOUD. After the migration, the OSs are changed to those supported by HUAWEI CLOUD, and the database remains unchanged.

You need to deployed application servers and the database servers of the system on HUAWEI CLOUD. The target system is redeployed on HUAWEI CLOUD ECSs or BMSs. Use the export and import functions of R3load to migrate database data. You can also use some native database tools, such as Oracle GoldenGate.

Figure 7-9 shows an example. For details, see section **Migrating from IBM or HP Midrange Computers to HUAWEI CLOUD**.

Figure 7-9 Migration from IBM midrange computers to HUAWEI CLOUD



7.5.2 Solution Design

Deployment Plan

Use HUAWEI CLOUD services for the deployment. Specifically, use ECS or BMS for server computing resources, and EVS and SFS for storage.

For the deployment solution design, refer to section **Deployment Plan**.

Networking Plan

A VPC is used on HUAWEI CLOUD, and subnets are created according to the networking best practices on HUAWEI CLOUD. On-premises IDC connects to HUAWEI CLOUD through EIP and VPN or Direct Connect.

For details, see **Networking Plan**.

Security Design

For details, see **Security Design**. Find more information in the **SAP Security White Paper**.

For details about permission management, see **Service Account System Design**.

Migration Solution

Table 7-12 shows the recommended solutions.

Table 7-12 Migration solutions

Object	Migration Solution	Description
Application servers	Redeployment	If the application servers running OSs that are not supported by HUAWEI CLOUD, you need to deploy the source system on the HUAWEI CLOUD.
Database	• System Copy option of SWPM (R3load import and export functions) • Heterogeneous database migration provided by a native database tool, such as Oracle GoldenGate and Oracle XTTS offline database data Export/ Import function	The R3load export and import function is used in a standard SAP migration solution. If any problem occurs during the migration, you can visit SAP official website to seek for SAP technical support. When using R3load, you need to shut down the servers before exporting the data, and the service interruption duration is long. If you requires shorter service interruption period, use heterogeneous migration provided by the database. For example, Oracle GoldeGate supports to reduce the downtime to almost zero. For more information, see **Oracle GoldeGate technical details**.

Service Switchover Plan

Table 7-13 shows an example.

Table 7-13 Switchover plan example

Migration Solution	Switchover Plan	Impact
The application servers and database server are redeployed on HUAWEI CLOUD. The database is migrated using the SWPM import and export function (R3load).	1. After the system is deployed on HUAWEI CLOUD, stop services on the source end and use the SWPM to export the source system. 2. Upload the exported files to the destination system through a private line, and then import the files to the destination system using SWPM.	The downtime is long, and the system needs to be shut down from the beginning. The service interruption duration = **Data exporting duration + File transferring duration+ Data importing duration**
The application servers and database server are redeployed on HUAWEI CLOUD. The Oracle database is migrated using the Oracle GoldeGate.	1. After the system is deployed on HUAWEI CLOUD, use the Oracle GoldeGate to configure data synchronization from the source to the destination. 2. Stop the services on the source end and perform the service takeover on the cloud database.	After the cloud database takes over the services, the service switchover is complete. The service interruption duration is the **database switchover duration**.

Migration Solution	Switchover Plan	Impact
The application servers and database server are redeployed on HUAWEI CLOUD. The Oracle database is migrated using Oracle XTTS.	1. After the system is successfully deployed on HUAWEI CLOUD, cross-platform transportable tablespaces (XTTS) and multiple incremental backups are used to synchronize data with the cloud. 2. After services on the source end are stopped, perform the data synchronization, and then the database on the cloud takes over the services. This greatly shortens the downtime.	After the cloud database takes over the services, the service switchover is complete. The service interruption duration is the time of the last incremental synchronization of the database.

7.5.3 Preparing the Migration Environment

7.5.3.1 Preparing Resources

For details, see **Preparing Resources**.

7.5.3.2 Migrating Application Servers to HUAWEI CLOUD

You need to redeploy the system on HUAWEI CLOUD because the OSs running on IBM Power midrange computers are not supported by HUAWEI CLOUD.

Redeploying the System

Deploy the servers on HUAWEI CLOUD. Redeploy the system on HUAWEI CLOUD. For details, see **SAP Deployment Guide**, **SAP HANA User Guide**, and **SAP NetWeaver User Guide**.

7.5.3.3 Migrating the Database to HUAWEI CLOUD

Heterogeneous migration may involve replication operations, such as data table splitting and ABAP code modification. These operations require SAP system and database management experience. You may spend more time adjusting the system and planning the migration. Do not change the database type. The following solutions are available:

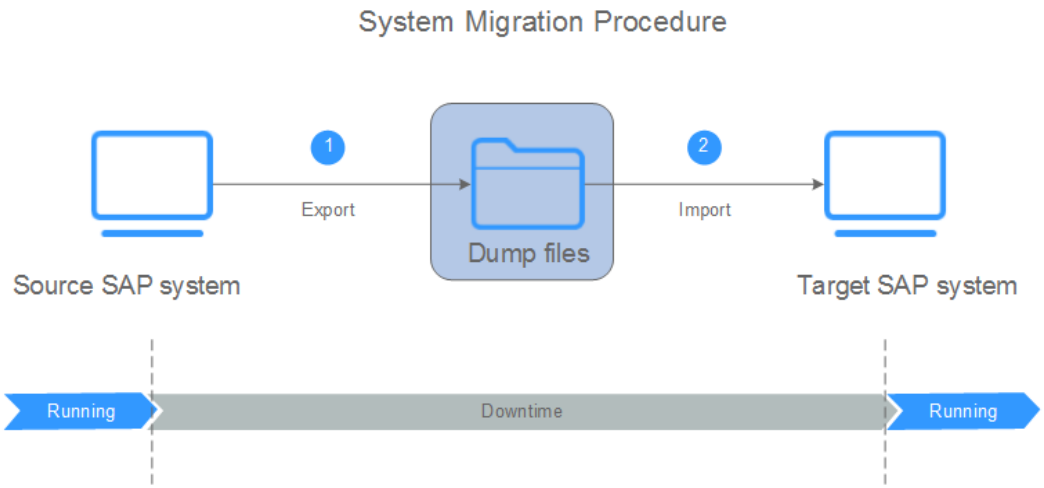
- Method 1: Use SAP System Copy that is a standard migration solution provided by SAP. If you have any questions during the migration, contact SAP technical support. For details, see **Method 1: Using SAP System Copy (R3load)**.
- Method 2: Use a database native tool. Different databases have their own heterogeneous migration solutions, for example, offline data Export/Import.

Method 1: Using SAP System Copy (R3load)

SAP System Copy is a standard migration solution supported by SAP's technical personnel. It can migrate data from your database to the HANA database (**System Copy - Target Database SAP HANA**) and other databases (**System Copy - Target Databases Other than SAP HANA**).

When using System Copy, stop the services before you start the export. The service interruption duration depends on the database size. Importing and exporting of over 1 TB data takes a long time, which has a great impact on services. **Figure 7-10** shows the procedure.

Figure 7-10 System migration



The procedure is described as follows:

Step 1 On HUAWEI CLOUD, create the a subnet, configure security group policies, and build the target system, including the database and application servers.

Step 2 Stop the source system services. Run the SWPM tool on the source server and use System Copy to export data. For details, see **SAP System Copy**.

Step 3 Upload the exported data to the file system of the target system.

Step 4 Run the SWPM tool in the target system and use System Copy to import data.

Step 5 Verify the system availability and data integrity.

----End

Method 2: Using the native migration function of your Products and installation programs required for Q Replication and SQL Replication on Linux, UNIX, and Windows - IBM DocumentationProducts and installation programs required for Q Replication and SQL Replication on Linux, UNIX, and Windows - IBM Documentationdatabase.

Databases have their own heterogeneous migration solutions. For example, the Oracle database has **Oracle GoldenGate**, and the DB2 has **Q Replication**, and the offline data Export/Import function. However, heterogeneous migration requires more careful planning and design. Consultants who are familiar with database migration tools are needed for implementing the migration.

7.5.4 Tests and Drills

For details, see **Tests and Drills**.

7.5.5 Switchover and Go-Live

For details, see **Switchover and Go-Live**.

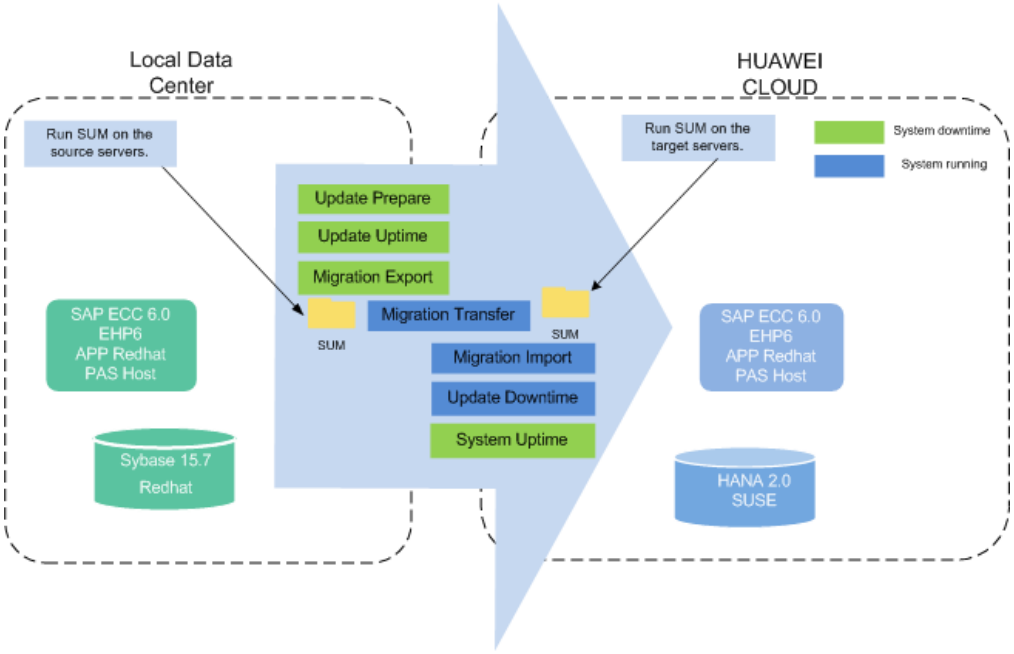
7.6 Migrating SAP Applications Running on a Non-HANA Database to HUAWEI CLOUD SAP HANA

7.6.1 Scenario Description

In this scenario, you migrate the source SAP system deployed in the local data center. The database is a non-HANA database (such as Sybase, Oracle, and DB2). The target end is HUAWEI CLOUD SAP HANA system. The server OSs may change.

The project includes system migration, software upgrade, database migration, and OS change. Use the DMO of SAP SUM to upgrade and migrate the SAP system to HUAWEI CLOUD SAP HANA system. Alternatively, use the **Classical Migration to SAP HANA** solution. Use SUM to upgrade the system to a supported version, and then use System Copy of SWPM to migrate the system onto the HANA database.

Figure 7-11 DMO Migration



7.6.2 Solution Design

Deployment Plan

Use HUAWEI CLOUD services for the deployment. Specifically, use ECS or BMS for server computing resources, and EVS and SFS for storage.

For the deployment solution design, refer to section **Deployment Plan**.

Networking Plan

A VPC is used on HUAWEI CLOUD, and subnets are created according to the networking best practices on HUAWEI CLOUD. On-premises IDC connects to HUAWEI CLOUD through EIP and VPN or Direct Connect.

For details, see **Networking Plan**.

Security Design

For details, see **Security Design**. Find more information in the **SAP Security White Paper**.

For details about permission management, see **Service Account System Design**.

Migration Solution

Redeploy the application servers and database server on HUAWEI CLOUD. For database migration, use the SAP solutions. **Table 7-14** describes the recommended solutions.

Table 7-14 Migration solutions

Object	Migration Solution	Description
Application servers	• Redeployment	Redeployment on HUAWEI CLOUD
Database	• DMO in SUM • Classic migration of SAP HANA (only applicable to Java systems)	• SAP provides the DMO in SUM to upgrade and migrate the SAP system to HUAWEI CLOUD SAP HANA. For details, see **Database Migration Option (DMO) of SUM**. • Alternatively, use the Classical Migration to SAP HANA solution. Use SUM to upgrade the system to a supported version, and then use System Copy of SWPM to migrate the system onto the HANA database. For details, see **Classical Migration to SAP HANA**.

Generally, data is transmitted over the network. The optimal network bandwidth is higher than 50 Mbit/s.

Service Switchover Plan

The migration implementor is responsible for the service switchover plan. **Table 7-15** shows an example plan.

Table 7-15 Switchover plan example

Migration Solution	Switchover Plan	Impact
Application servers are newly deployed, and database servers are migrated using DMO.	1. Deploy and commission the new system. 2. Stop source database services and use DMO to migrate data to the target system.	The downtime relates to the service data volume and network bandwidth. The service interruption time of this plan is long.

7.6.3 Preparing the Migration Environment

7.6.3.1 Preparing Resources

For details, see **Preparing Resources**.

7.6.3.2 Migrating Application Servers to HUAWEI CLOUD

You need to redeploy SAP application servers on HUAWEI CLOUD.

Redeploying the System

Redeploy the system on HUAWEI CLOUD. For details, see **SAP Deployment Guide**, **SAP HANA User Guide**, and **SAP NetWeaver User Guide**.

7.6.3.3 Migrating the Database to HUAWEI CLOUD

SAP provides the DMO in SUM and typical SAP migration methods to help you migrate data from non-HANA databases to the HANA database. If you are an experienced SAP migration consultants, use these methods to migrate your SAP system to HUAWEI CLOUD.

For details, see the official SAP documents **Classical Migration to SAP HANA** and **Database Migration Option (DMO) of SUM**.

7.6.4 Tests and Drills

For details, see **Tests and Drills**.

7.6.5 Switchover and Go-Live

For details, see **Switchover and Go-Live**.

7.7 Appendix

7.7.1 Migration Solution Details

Table 7-16 describes common SAP system migration methods.

Table 7-16 Migration tools and methods

Tool/Method	Description
Server Migration Service	SMS provides P2V and V2V migration services to help you migrate applications and data from on-premises X86 physical servers or VMs on private or public clouds to ECSs on HUAWEI CLOUD. For details about how to use SMS, see the **Server Migration Service Quick Guide**. **NOTE** HUAWEI CLOUD also provides the Server Migration Tool (SMT). The Server Migration Service is the SMT provided as a service, but the SMT has more powerful functions. If the SMS cannot meet your requirements, contact HUAWEI CLOUD technical support. The differences between the SMS and SMT are as follows: • Supported OSs: SMT supports more types and versions. For those supported by SMS, see **Supported Source Server OSs**. • Connections: For SMS, source servers need to access HUAWEI CLOUD SMS server through the Internet. If a source server and a target ECS are connected through Direct Connect or VPN, ensure that the source server to be migrated can access the SMS.
Image Export/ Import	If your servers can be converted into image files, and the type and OS of the image files are listed in **Formats and OSs Supported for External Image Files**, you can create server image files as private images on HUAWEI CLOUD, and use the images to quickly deploy new servers. For details, see **Creating a Linux System Disk Image from an External Image File** and **Creating a Windows System Disk Image from an External Image File**.
Database Backup and Restoration	This method uses the database backup function to export data from the source system, transfer the backup files to the destination system, and then use the database restoration function to restore the data. Proper use of the database backup and restoration feature reduces the migration downtime.
Database Synchronization and Replication	Database replication functions include **HANA System Replication**, **Oracle Data Guard**, **Always On Availability Groups (SQL Server)**, and DB2 **Q Replication**. They all have similar features that allow you to copy a database from one node to another. If you require shorter downtime, use database replication as the data migration tool.
SAP System Copy (R3load)	The System Copy in SAP Software Provisioning Manager (SWPM) can replicate the SAP system to a new system through the Export/Import function. This document does not describe this tool in detail. However, this is a solution to migrate the SAP system to HUAWEI CLOUD. You can visit SASP official website to find details about **System Copy** and **System Copy and Migration**.

Tool/Method	Description
DMO	Data Migration Option (DMO) is integrated in SAP Software Update Manager (SUM), which upgrades SAP systems and migrate SAP databases. This document does not describe this tool in detail. However, this is a solution to migrate an SAP system to HUAWEI CLOUD. For details, visit the SAP website at **Database Migration Option (DMO) of SUM**.
Classic migration to SAP HANA	This solution uses a series of processes and tools including heterogeneous System Copy to migrate data from a database to the HANA database. This document does not describe this solution in detail. However, you can use this solution to migrate the SAP system to HUAWEI CLOUD. For details about the solution, see **Classical Migration to SAP HANA**.
Object Storage Migration Service	OMS is an online data migration service that helps users easily and smoothly migrate object storage data from other public clouds to HUAWEI CLOUD. For details about how to use OMS, see the **Object Storage Migration Service Quick Start**.
Data Express Service	DES is a massive data transmission solution. It allows transmitting a large amount of data using Teleport devices or disks (with external USB interfaces, SATA interfaces, or SAS interfaces) to HUAWEI CLOUD. DES helps to address issues facing massive data transmission such as high network costs and long transmission time. For details about how to use DES, see **Data Express Service Quick Start**.

8 Best Practice of Using Block-Level Migration of SMS to Migrate SAP Applications and Databases Running on Linux Servers

8.1 Block-Level Migration of SMS

In block-level migrations, a block refers to a disk block. A disk block is the minimum logical unit of the file system for managing disk partitions. Disk blocks are similar to clusters in Windows. A block is also the minimum logic unit of disks used by OSs and software. The smallest unit for disk read or write is a sector. A sector is a physical area on the disk. The read and write operations to disk blocks are performed in sectors. Generally, a file is stored in several blocks, and one block maps to several physical sectors.

In block-level migrations, the file system is migrated by blocks. Therefore, if the network is interrupted during the migration, only impacted blocks need to be migrated again after the network is recovered. If files are modified during the migration, only modified blocks need to be synchronized after the migration. In file-level migrations, various tools like TAR and SSH or other transmission protocols are used for remote replication. Therefore, if the file is changed during decompression or the network is interrupted during migration, the migration fails. In addition, if the file is changed during incremental data synchronization, the file needs to be synchronized again. In this case, all the blocks of the file must be synchronized. So, the synchronization efficiency is low. Block-level migration of file systems can better meet the incremental data synchronization requirements of SAP databases.

For more information about SMS, see **Server Migration Service User Guide**.

8.2 Preparing for the Migration

8.2.1 Application Scenarios

The block-level migration of SMS can be used in the following SAP migration scenarios:

- SAP HANA independent databases
- Applications and SAP HANA database on the SAP ERP single node
- Applications and SAP HANA database on SAP ERP nodes deployed in HA mode (including the shared disks)

CAUTION

The block-level migration function of SMS cannot be used to migrate SFS and SFS Turbo. The migration of SFS and SFS Turbo must be completed at the file system level.

8.2.2 Preparations for Using SMS

The SMS of the latest version is used for the migration. Before using SMS, prepare the account and source and destination server environments, and obtain the required permissions. For details, see **Preparations Before Migration**.

SAP HANA and SAP S/4HANA1809 are installed on the source server used in this migration. After the migration is complete, SAP HANA and SAP S/4HANA1809 are also available on the destination server and can be started and run properly.

8.2.3 (Optional) Preparing a Destination ECS

For Linux block-level migration, you can choose to create an ECS or use the existing ECS as the destination server. Perform the following operations if you choose to use the existing ECS as the destination server.

Linux block-level migration of SMS is used here for the migration between different AZs in the same region. Before the migration, create a destination ECS with the same specifications, including disk quantity and size as well as OS, as those of the source server, and deploy it in the same VPC and region with but different AZs from the source server.

NOTE

The created destination ECS must meet the following requirements. Otherwise, the migration may fail.

- A target server running Windows must have at least 2 GB memory.
- The destination server must have at least as many disks as the source server, and the size of each disk on the destination server must be at least as large as those on the source server.
- The destination server must run the same OS as the source server, or there will be a server name conflict.
- The destination server must have been configured with an EIP, VPN, or Direct Connect connection.
- The security group of the VPC that the destination ECS is in must be correctly configured. If the destination ECS runs Windows, enable the TCP ports **8899** and **8900**. If the destination ECS runs Linux, enable ports **8900** and **22**.

For details, see **How Do I Configure the Security Group Rules for Target Servers?**

8.3 Performing the Migration

8.3.1 Installing the Migration Agent on the Source Server

You need to install the Agent on each Linux source server that you want to migrate. During the Agent installation, you need to enter the AK/SK pair of your HUAWEI CLOUD account of the destination ECS. After the Agent is started successfully, it automatically reports source server information to SMS.

Step 1 Log in to the source server to be migrated as user **root**.

Run the following command to download the Agent:

wget -t 3 -T 15 https://sms-agent-2-0-cn-north-1.obs.cn-north-1.myhuaweicloud.com/SMS-Agent.tar.gz

```
sms-saptest:~/SMS # wget -t 3 -T 15 https://sms-agent-2-0-cn-north-1.obs.cn-nort
h-1.myhuaweicloud.com/SMS-Agent.tar.gz
--2021-07-14 14:20:25--  https://sms-agent-2-0-cn-north-1.obs.cn-north-1.myhuawe
icloud.com/SMS-Agent.tar.gz
Resolving sms-agent-2-0-cn-north-1.obs.cn-north-1.myhuaweicloud.com (sms-agent-2
-0-cn-north-1.obs.cn-north-1.myhuaweicloud.com)... 114.115.192.27, 114.115.192.1
62, 114.115.192.98
Connecting to sms-agent-2-0-cn-north-1.obs.cn-north-1.myhuaweicloud.com (sms-age
nt-2-0-cn-north-1.obs.cn-north-1.myhuaweicloud.com)|114.115.192.27|:443... conne
cted.
HTTP request sent, awaiting response... 200 OK
Length: 90937990 (87M) [application/gzip]
Saving to: 'SMS-Agent.tar.gz'

SMS-Agent.tar.gz     19%[==>                 ]  17.02M  4.20MB/s    eta 14s
```

Step 2 Run the following command to decompress the downloaded package:

tar -zxvf SMS-Agent.tar.gz


```
sms-saptest:~/SMS # tar -zxvf SMS-Agent.tar.gz
SMS-Agent/
SMS-Agent/restart.sh
SMS-Agent/agent/
SMS-Agent/agent/x64/
SMS-Agent/agent/x64/sms-cmp
SMS-Agent/agent/x64/agent-cli
SMS-Agent/agent/x64/linuxmain
SMS-Agent/agent/cert/
SMS-Agent/agent/cert/srcAgent.pfx
SMS-Agent/agent/cert/ksa.file
SMS-Agent/agent/cert/ksb.file
SMS-Agent/agent/cert/destAgent.pfx
SMS-Agent/agent/x86/
SMS-Agent/agent/ioblock/
SMS-Agent/agent/ioblock/x64/
SMS-Agent/agent/ioblock/x64/2.6.32-573.1.1.el6.x86_64/
SMS-Agent/agent/ioblock/x64/2.6.32-573.1.1.el6.x86_64/iocapture.ko
SMS-Agent/agent/ioblock/x64/4.15.0-136-generic/
SMS-Agent/agent/ioblock/x64/4.15.0-136-generic/iocapture.ko
```

Step 3 Run the following command to switch to the **SMS-Agent** directory of the source server:

cd SMS-Agent

Step 4 (Optional) Perform this step if an HTTPS proxy server is used.

⚠ CAUTION

A proxy server is a special network service. If your source server cannot access HUAWEI CLOUD through the Internet, you can use a proxy server to access HUAWEI CLOUD. You need to configure a proxy server by yourself.

---

a. Run the following command to go to the **config** directory:

cd agent/config

b. Run the following command to open and edit the **auth.cfg** file:

vi auth.cfg

```
File  Edit  View  Search  Terminal  He
[proxy-config]
enable = true
proxy_addr = 10.10[redacted]
proxy_port = 808
proxy_user = Administrator
use_password = true
~
```

c. Run the following command to save the **auth.cfg** file and exit:

:wq

NOTE

- **proxy_addr** indicates the IP address of the proxy server. It is used by the source server to access SMS.
- If the HTTPS proxy is not used during the migration, you are not allowed to modify the **auth.cfg** file.
- The proxy is used for registering the source server with SMS when a Direct Connect or VPN connection is used. It is not used for data migration.
- **enable** controls if the proxy is used or not. To use the proxy, set this to **true**.
- If a username is required to use the proxy, set **proxy_user** to the username, for example, **root**. If the username is not required, leave this parameter blank.
- If a password is required to use the proxy, set **use_password** to **true**. If the password is not required, set it to **false**.
- The values shown here are for reference only. Actual values will depend on your server configuration,

Step 5 Modify the **g-property.cfg** file in the **config** directory to enable Linux block-level migration.

```
/SMS/SMS-Agent/agent/config # vi g-property.cfg
```

```
[ssl_config]
servercheck = False

[property]
times = 20
debug = False
file exist check = \Windows\system32\DRIVERS\atapi
RIVERS\intelide.sys
enablesync = True
enablesnapshot = True
enablelinuxblock = True
wmi = True
targetip =
heartmonitorday = 30
stopsync = 0
uefi2bios = False

[enviromentcheck]
vss depend service = VSS
```

Run the **:wq** command to exit.

Step 6 (Optional) If an SFS disk is mounted to the source server, run the following commands.

Modify the **g-property.cfg** file in the **config** directory.


```
sms-saptest:~/SMS/SMS-Agent/agent/config # ls
ErrorCode.ini           cloud-region.json  error.cfg      init.cfg
auth.cfg                commands.xml       g-property.cfg srcAgent
blocktransferlayer.cfg  disk.cfg           huaweiapi.pem
sms-saptest:~/SMS/SMS-Agent/agent/config # vi g-property.cfg
```

Add **nfs** to **exclude.filesystem**.

```
[linux.config]
linux.support.filesystem = ext2,ext3,ext4,xfs,vfat,reiserfs,btrfs
linux.unsupport.filesystem =
tar.exclude.dir = /proc/*,/sys/*,/lost+found/*,/var/lib/ntp/proc/*
tar.interval = 30
rsync.exclude.dir = /proc/*,/sys/*,/lost+found/*,/var/lib/ntp/proc/*,/boot/*,/bo
ot/efi/*,/etc/fstab,/etc/*,/etc/X11/*,/root/initrd_bak/*,lib/modules/*,/boot/gru
b2/x86_64-efi/*,/boot/grub2/i386-pc/*
rsync.interval = 30
network.dev =
network.gateway =
exclude.filesystem = tmpfs,devpts,devtmpfs,sysfs,proc,ramfs,nfs
installPwdAgent = true
-- INSERT --                                          28,64         Bot
```

Run the **:wq** command to exit.

Step 7 Run the following command to start the Agent:

./startup.sh

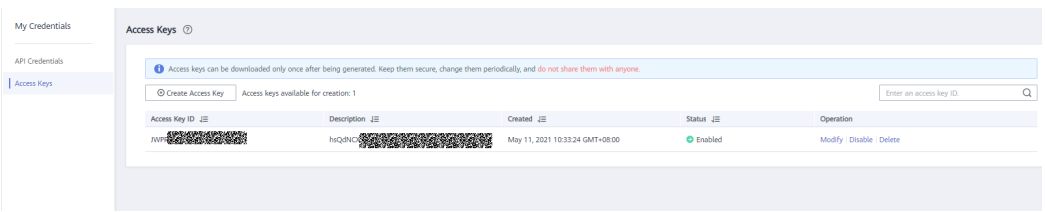
```
sms-saptest:~/SMS/SMS-Agent # ./startup.sh
After being started, the migration Agent collects system configuration informati
on and uploads the information to SMS for migration task creation. The informati
on to be collected includes server IP address and MAC address. For details, see
the Server Migration Service User Guide. Are you sure you want to collect the in
formation?(y/n)
```

Step 8 Carefully review the description of what information will be collected by the Agent, enter **y**, and press **Enter**.

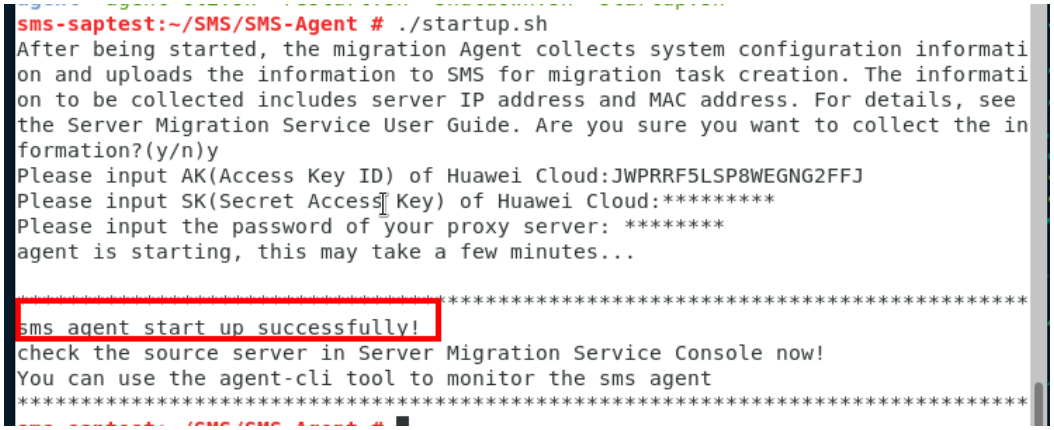
Enter the AK and SK of the HUAWEI CLOUD account of the destination ECS and the password of the HTTP proxy server as prompted.

```
sms-saptest:~/SMS/SMS-Agent # ./startup.sh
After being started, the migration Agent collects system configuration informati
on and uploads the information to SMS for migration task creation. The informati
on to be collected includes server IP address and MAC address. For details, see
the Server Migration Service User Guide. Are you sure you want to collect the in
formation?(y/n)y
Please input AK(Access Key ID) of Huawei Cloud:JWPRRF5LSP8WEGNG2FFJ
Please input SK(Secret Access Key) of Huawei Cloud:*********
Please input the password of your proxy server:
```

Create and view the AK and SK on the management console.



When the following information is displayed, the Agent has been started up and will automatically start reporting source server information to SMS.



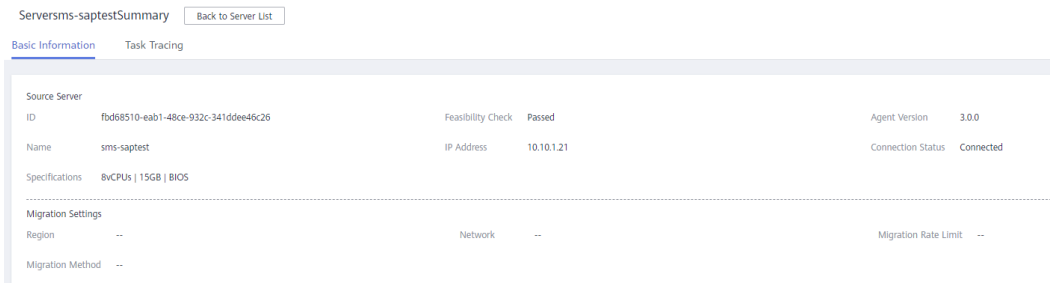
Repeat the preceding steps to install the Agent on the source server where SAP HANA and SAP applications are installed.

----End

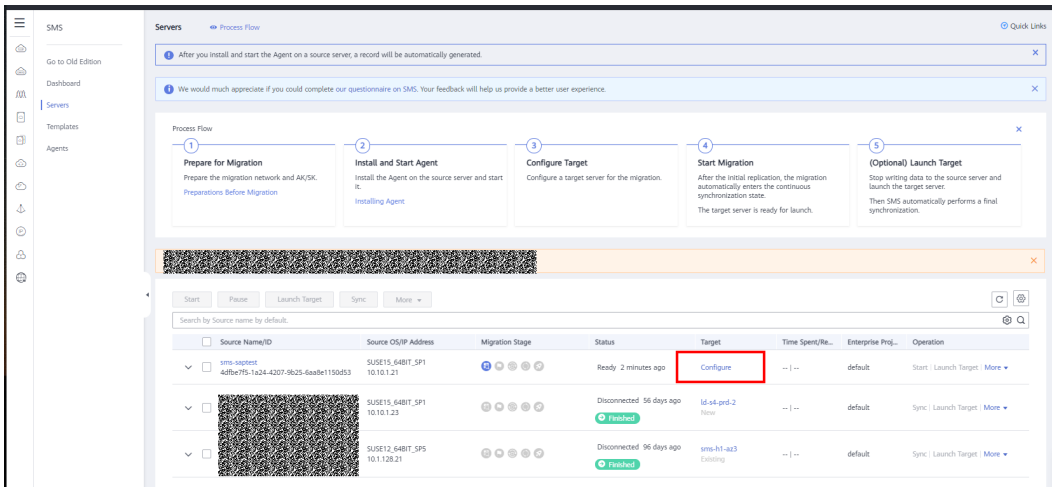
8.3.2 Configuring the Destination Server

Before the migration, you need to configure the destination server. The destination server is used to receive data from the source server. You can also use the it for migration test and launch the destination server. The destination server can be configured only after all migration items on the source server are checked and confirmed OK.

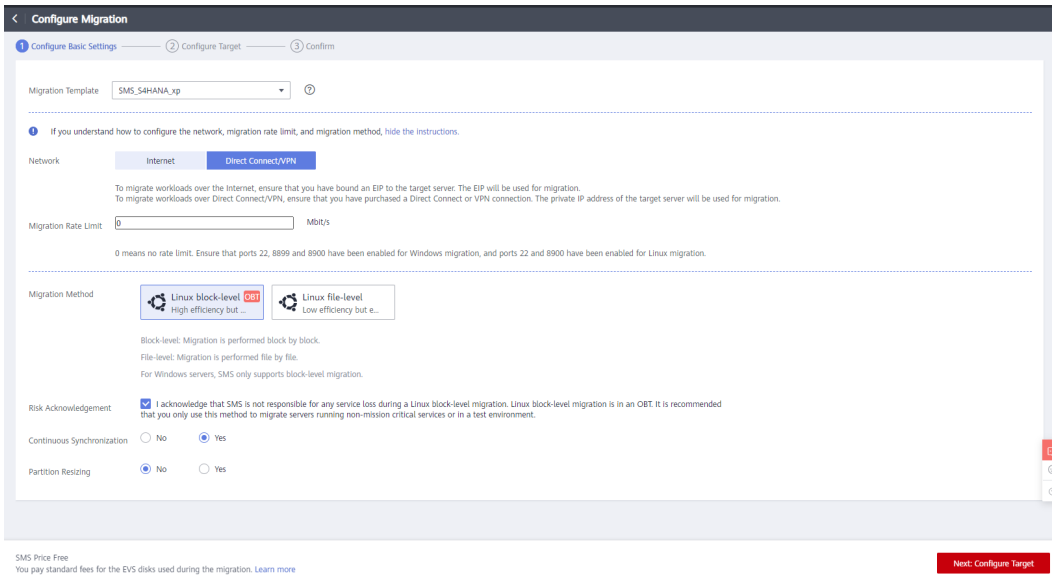
Step 1 Log in to the SMS management console and choose **Servers** in the left navigation pane. On the server list page, click the server to be migrated to go to the server details page. Select the **Source Server Details** tab to view check result for the migration items on the source server. You can perform the following steps only after all migration items are checked and confirmed OK. If there are some items found to be abnormal, locate the cause and rectify it on the current page.



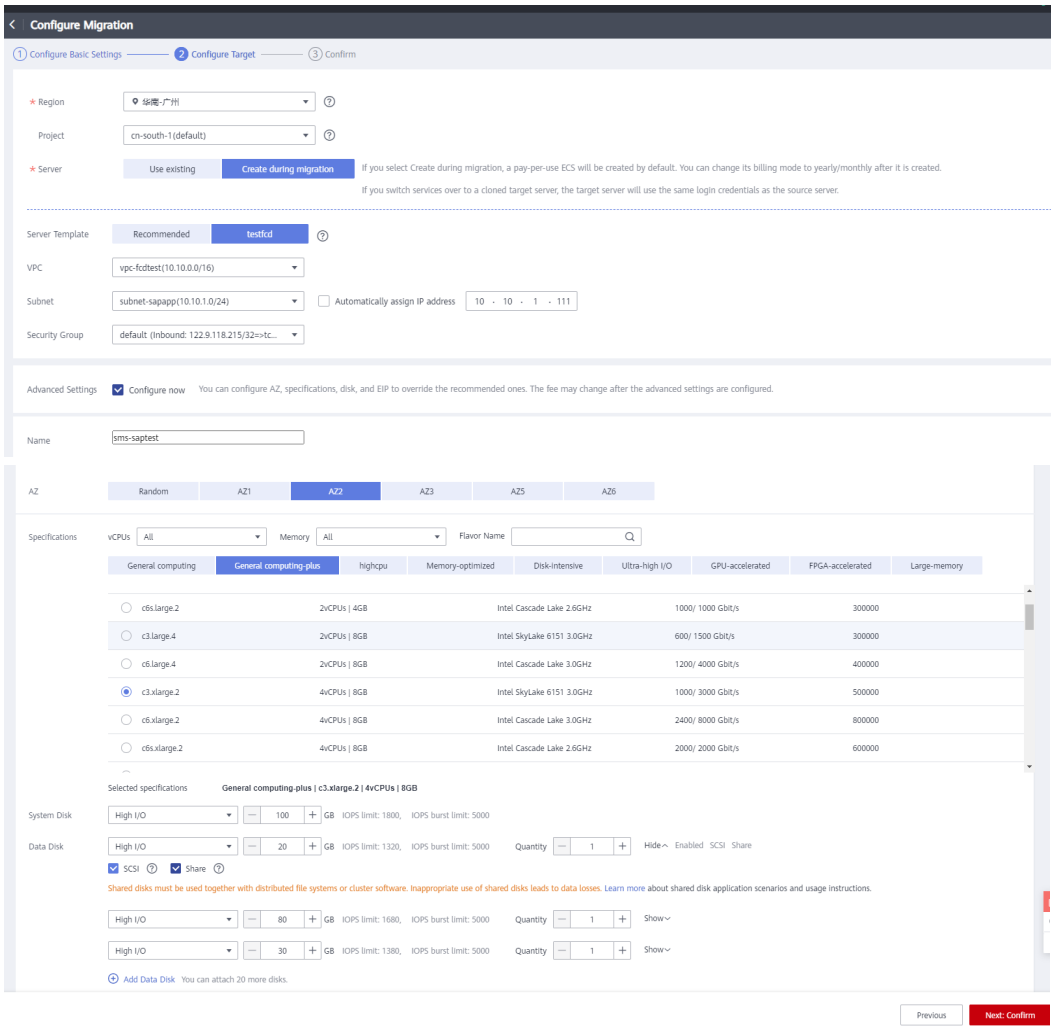
Step 2 Locate the server to be migrated and click **Configure** to configure the destination server.



Step 3 Configure basic settings as required. Select **Continuous Synchronization** and click **Next: Configure Target**.



Step 4 Select **Create during migration** or **Use existing** for **Server**, configure whether to create shared disks, and select the VPC and disk specifications based on the site requirements. Click **Next: Confirm**.

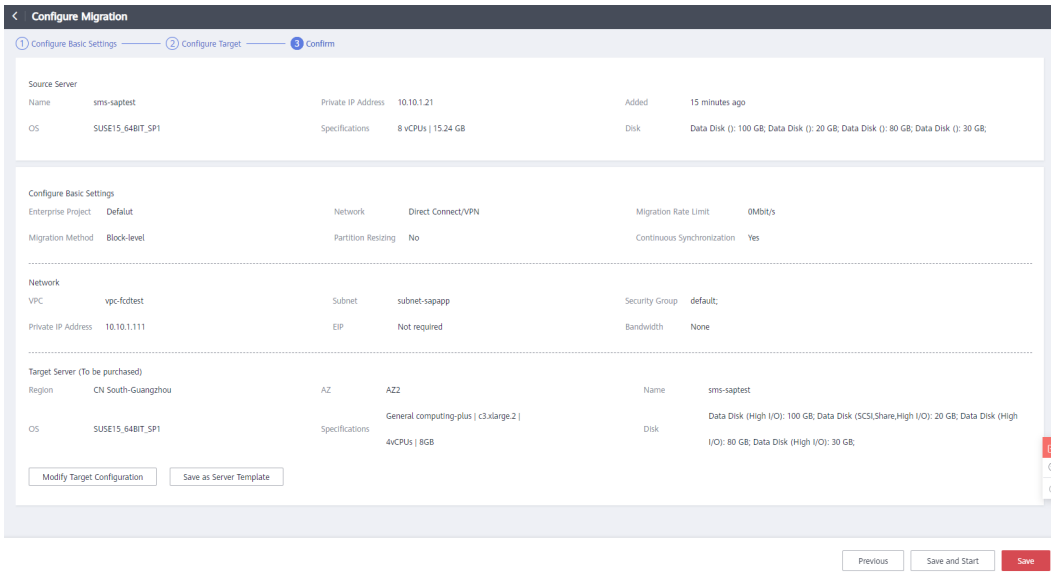


Parameter description

Name	Description	Example Value
Region	Select the region where the destination ECS is located. By default, the region is the one set for the current migration project, but you can select another region if needed.	CN East-Shanghai2
Migration Method	• **Linux block-level**: Migration is performed block by block. This method has high efficiency but poor compatibility. • **Linux file-level**: Migration is performed file by file. This method has low efficiency but excellent compatibility. • **Windows block-level**: Migration is performed block by block. For Windows servers, SMS only supports block-level migration. This method has high efficiency.	Linux block-level

Name	Description	Example Value
Network	• **Internet**: If you select this option, an elastic IP address must be assigned on the target ECS. **Network** is set to **Internet** by default. • **Direct Connect/VPN**: You need to create a Direct Connect or VPN connection between the source server and the VPC subnet where the target server is located in advance. • **Migration Rate Limit**: You can set the rate limits as needed based on the bandwidth size of the source server and service requirements. **NOTE** If the source and destination servers are in the same VPC, set **Network** to **Direct Connect/VPN**. Configure it based on the site requirements.	Direct Connect/VPN
Whether to perform a continuous synchronization after the full replication is complete.	• If you select **No**, after the full replication, SMS will not perform a continuous synchronization and will automatically start the target ECS. To synchronize incremental data, click **Start** in the **Operation** column. • If you select **Yes**, after the full replication, SMS will perform a continuous synchronization. To complete the migration, you need to manually launch or clone the target ECS.	Yes
Server	• Use existing • Create during migration	Use existing

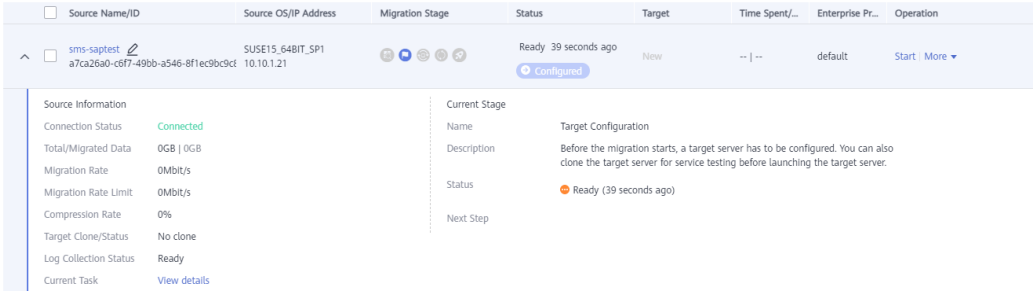
Step 5 Ensure that all parameters have been configured based on the site requirements and click **Save**.

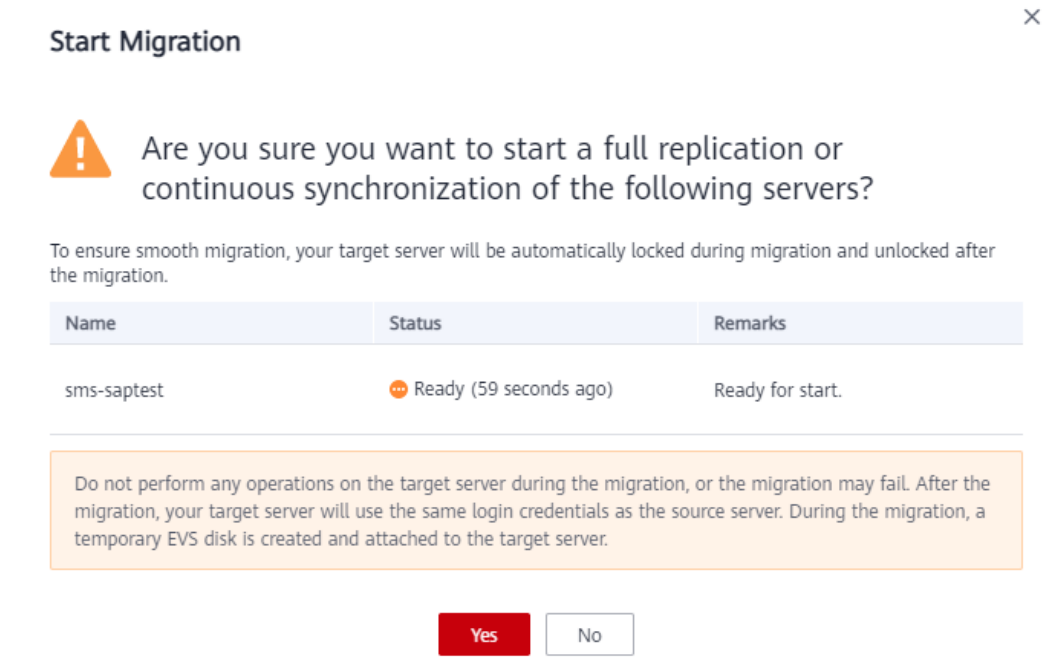


----End

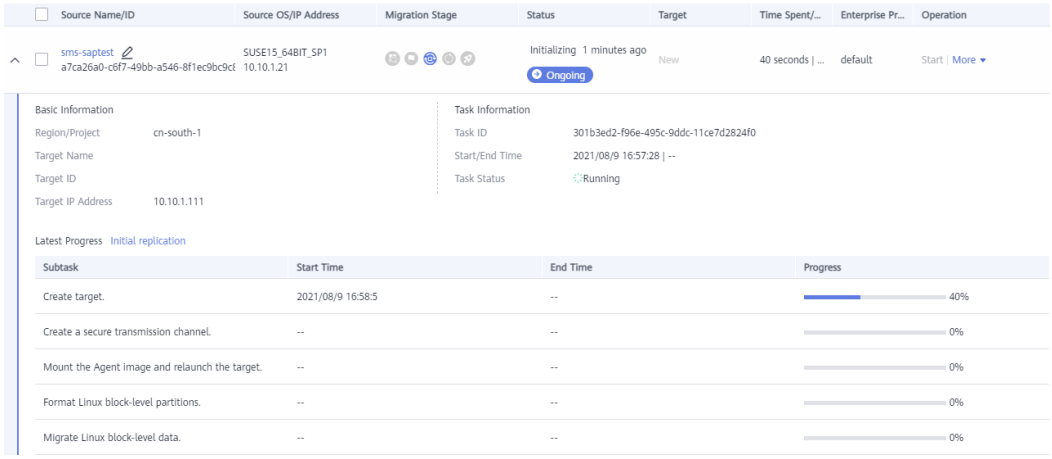
8.3.3 Starting the Migration

Step 1 Back to the SMS console, and view the migration task status. If it is **Ready**, click **Start** in the **Operation** column.

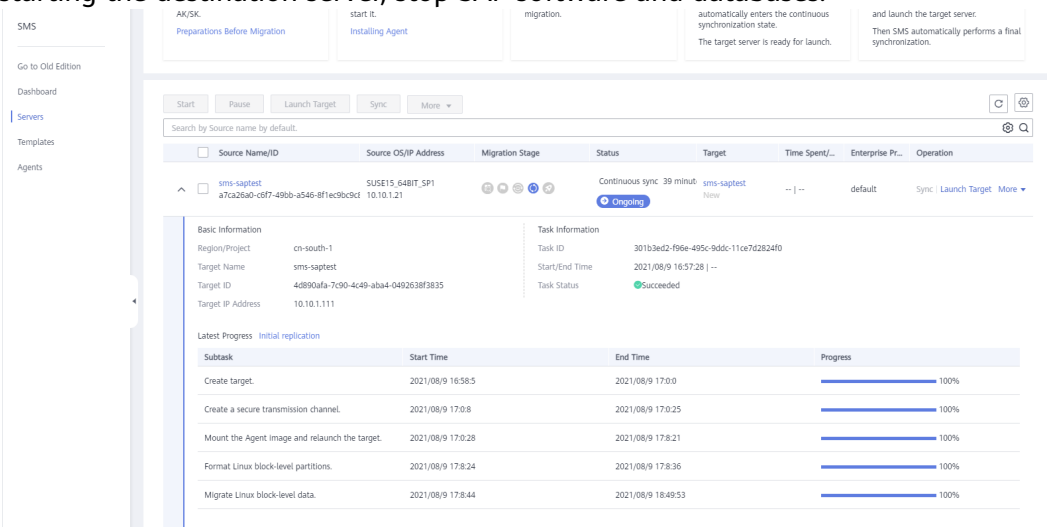




Step 2 Wait until the migration is completed.



Wait until the migration enters the continuous synchronization status. Before starting the destination server, stop SAP software and databases.



----End

8.3.4 Stopping the SAP Software

On the SMS manage console, view the migration status. When the migration enters the continuous synchronization status, the full replication is complete, and the system automatically synchronizes the I/O data from the source server to the destination server. To ensure that SAP-related data in the memory of the source server can be synchronized to the destination server, you need to stop SAP S/4HANA and SAP HANA so that the data in the memory of the source server is updated to the disk and then synchronized to the destination server by SMS.

Step 1 Log in to the SMS management console and view the migration progress. When the migration is in the continuous synchronization status, stop the SAP software.

Step 2 Log in to the source server and stop SAP S/4HANA.


```
sms-saptest:~ #
sms-saptest:~ # su - s01adm
sms-saptest:s01adm 2> sapcontrol -nr 01 -function GetProcessList

30.11.2020 09:21:22
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
disp+work, Dispatcher, GREEN, Running, 2020 11 28 16:48:15, 40:33:07, 22718
igswd_mt, IGS Watchdog, GREEN, Running, 2020 11 28 16:48:15, 40:33:07, 22719
gwrd, Gateway, GREEN, Running, 2020 11 28 16:48:16, 40:33:06, 22724
icman, ICM, GREEN, Running, 2020 11 28 16:48:16, 40:33:06, 22725
sms-saptest:s01adm 3> sapcontrol -nr 01 -function Stop

30.11.2020 09:21:29
Stop
OK
sms-saptest:s01adm 4> sapcontrol -nr 02 -function Stop

30.11.2020 09:21:34
Stop
OK
sms-saptest:s01adm 5> sapcontrol -nr 01 -function GetProcessList

30.11.2020 09:24:49
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
disp+work, Dispatcher, GRAY, Stopped, , , 22718
igswd_mt, IGS Watchdog, GRAY, Stopped, , , 22719
sms-saptest:s01adm 6>
```

Step 3 Stop SAP HANA.

```
sms-saptest:~ # su - s00adm
s00adm@sms-saptest:/usr/sap/S00/HDB00> sapcontrol -nr 00 -function GetProcessList

30.11.2020 09:27:15
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
hdbdaemon, HDB Daemon, GREEN, Running, 2020 11 28 15:34:20, 41:52:55, 4082
hdbcompileserver, HDB Compileserver, GREEN, Running, 2020 11 28 15:34:44, 41:52:31, 4272
hdbnameserver, HDB Nameserver, GREEN, Running, 2020 11 28 15:34:20, 41:52:55, 4098
hdbpreprocessor, HDB Preprocessor, GREEN, Running, 2020 11 28 15:34:44, 41:52:31, 4274
hdbwebdispatcher, HDB Web Dispatcher, GREEN, Running, 2020 11 28 15:35:26, 41:51:49, 4681
hdbindexserver, HDB Indexserver-S00, GREEN, Running, 2020 11 28 16:40:20, 40:46:55, 13117
hdbxsengine, HDB XSEngine-S00, GREEN, Running, 2020 11 28 16:40:30, 40:46:45, 13189
hdbdocstore, HDB DocStore-S00, GREEN, Running, 2020 11 28 16:40:30, 40:46:45, 13192
hdbdpserver, HDB DPserver-S00, GREEN, Running, 2020 11 28 16:40:30, 40:46:45, 13194
hdbdiserver, HDB Deployment Infrastructure Server-S00, GREEN, Running, 2020 11 28 16:46:49, 40:40:26, 20613
s00adm@sms-saptest:/usr/sap/S00/HDB00> HDB stop
hdbdaemon will wait maximal 300 seconds for NewDB services finishing.
Stopping instance using: /usr/sap/S00/SYS/exe/hdb/sapcontrol -prot NI_HTTP -nr 00 -function Stop 400

30.11.2020 09:27:24
Stop
OK
Waiting for stopped instance using: /usr/sap/S00/SYS/exe/hdb/sapcontrol -prot NI_HTTP -nr 00 -function WaitforSt
opped 600 2


30.11.2020 09:28:20
WaitforStopped
OK
hdbdaemon is stopped.
```

```
s00adm@sms-saptest:/usr/sap/S00/HDB00> sapcontrol -nr 00 -function GetProcessList

30.11.2020 09:29:37
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
hdbdaemon, HDB Daemon, GRAY, Stopped, , , 4082
s00adm@sms-saptest:/usr/sap/S00/HDB00>
```

Then, the SMS migration progress is still in the continuous synchronization status. In this case, you can click **Launch Target**.

----End

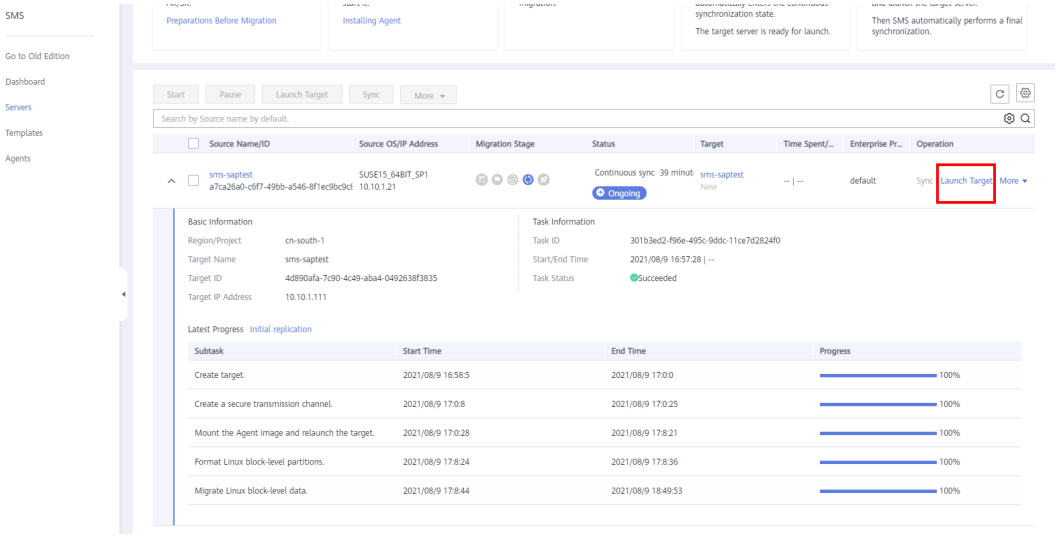
8.3.5 Launching the Destination Server

You can launch a server that is in the continuous synchronization state. After the server is launched, continuous synchronization is stopped. The destination server can only be launched if the migration is in the continuous synchronization state.

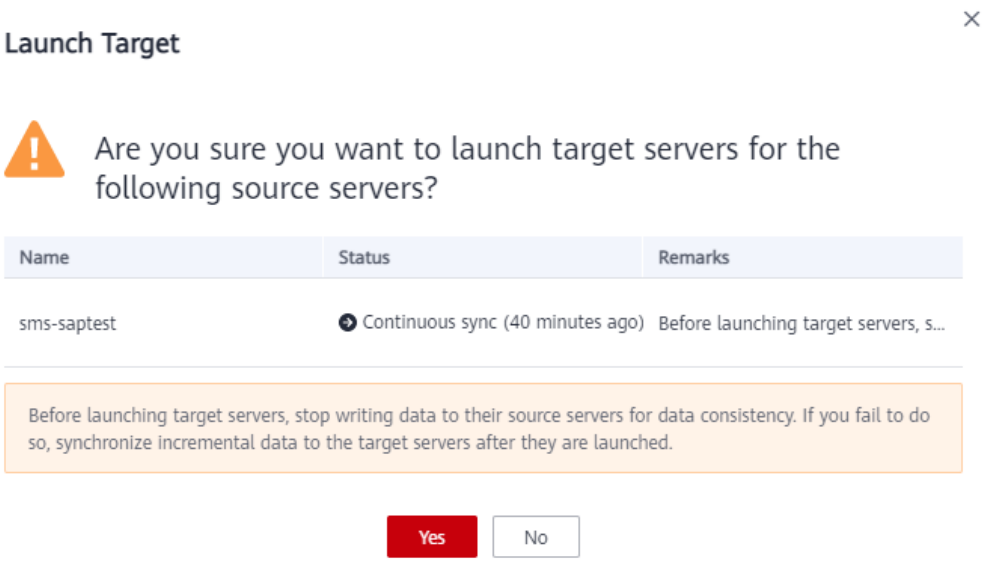
Before launching the destination server, you can clone the destination server for service testing. If there are no problems in the testing of cloned server, launch the destination server.

The cloned server must be in the same AZ as the destination server, but can be in a different VPC.

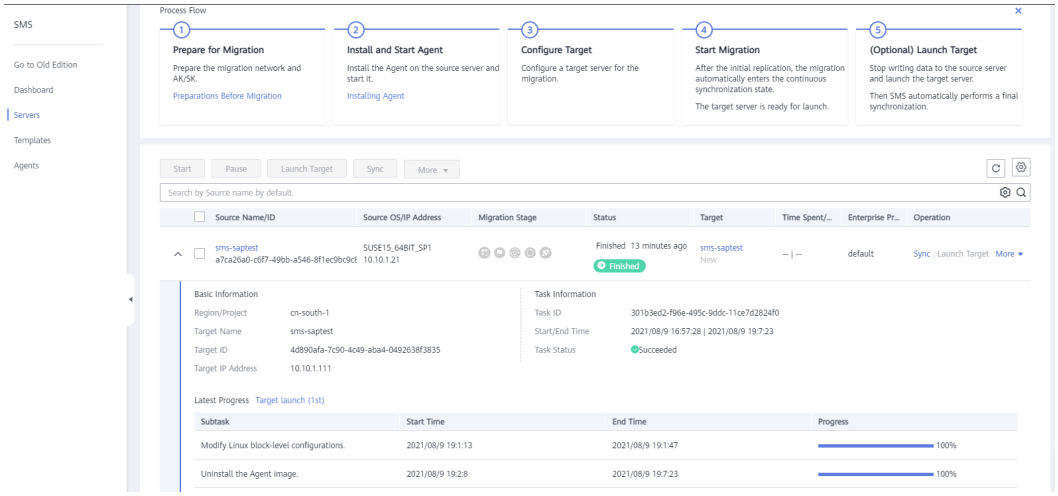
Step 1 Log in to the SMS management console. In the navigation pane on the left, choose **Servers**. Locate the target server you want to launch, and click **Launch Target** in the **Operation** column.



Step 2 In the displayed dialog box, click **Yes**.



Step 3 Wait until the destination server is launched. When the status changes to **Finished**, the destination server is launched and the migration is completed.



----End

8.3.6 Verifying the Migration

After the destination server is launched, you can log in to the destination server to check whether SAP S/4HANA and SAP HANA are running properly and whether the data in the database is consistent with that in the database of the source server.

Use the password of the source server to log in to the destination server.

After the migration, the information of the destination server is the same as that of the source server, including the host name and the content in the **/etc/hosts** file.

Step 1 Check the disk mounting status to ensure that all disks have been correctly mounted to the directories on the server.

```
sms-saptest:~ #
sms-saptest:~ # lsblk  -f
NAME   FSTYPE LABEL UUID                                 MOUNTPOINT
vda
└─vda1 ext4         6f154186-728a-477c-8d12-55ecf8487572 /
vdb    swap         c6de0ab2-a5ee-4ac4-a53e-a395de7c4085 [SWAP]
vdc    xfs          fe5a3926-2ad0-4f74-b1c4-2319e80f26c0 /usr/sap
vdd    xfs          1e7b1fba-030c-4b1b-bf18-9abf41338f64 /sapmnt
vde    xfs          9c73a9d9-b60c-45c3-8ab9-6a89f8469597 /hana/log
vdf    xfs          7eb4b38e-bc5f-4c6a-901c-97433cea8925 /hana/data
vdg    xfs          77cfc0ef-8e10-49d1-a129-3e969f6e8ffa /hana/shared
vdh    xfs          261d5228-5f62-4dd7-9674-826a6a52ab49 /hana/backup
sms-saptest:~ # ll /hana/
total 0
drwxr-xr-x 2 root root 35 Nov 25 20:58 backup
drwxr-xr-x 3 root root 46 Nov 25 20:58 data
drwxr-xr-x 3 root root 46 Nov 25 20:58 log
drwxr-xr-x 4 root root 67 Nov 25 20:58 shared
sms-saptest:~ # ll / | grep sap
drwxr-xr-x   3 root sapsys    46 Nov 25 20:58 sapmnt
sms-saptest:~ # ll /usr/ | grep sap
drwxr-xr-x   8 root sapsys   208 Nov 25 20:58 sap
sms-saptest:~ #
```

Step 2 Modify the **/etc/hosts** file on the destination server.

Modify the **/etc/hosts** file, and change the IP address mapped with the host name to the IP address of the destination server.


```
#
# hosts         This file describes a number of hostname-to-address
#               mappings for the TCP/IP subsystem.  It is mostly
#               used at boot time, when no name servers are running.
#               On small systems, this file can be used instead of a
#               "named" name server.
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#


# special IPv6 addresses
::1     localhost       ipv6-localhost  ipv6-loopback

fe00::0 ipv6-localnet

ff00::0 ipv6-mcastprefix
ff02::1 ipv6-allnodes
ff02::2 ipv6-allrouters
ff02::3 ipv6-allhosts

127.0.0.1       localhost
10.0.1.118      sms-saptest
~
~
~
~
~
~
~
~
~
~
~
"/etc/hosts" 25L, 614C                                                24,10         All
```

Step 3 Start SAP HANA.

```
sms-saptest:~ # su - s00adm
s00adm@sms-saptest:/usr/sap/S00/HDB00> sapcontrol -nr 00 -function GetProcessList

30.11.2020 10:26:36
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
hdbdaemon, HDB Daemon, GRAY, Stopped, , , 3888
s00adm@sms-saptest:/usr/sap/S00/HDB00> HDB start


StartService
Impromptu CCC initialization by 'rscpCInit'.
  See SAP note 1266393.
OK
OK
Starting instance using: /usr/sap/S00/SYS/exe/hdb/sapcontrol -prot NI_HTTP -nr 00 -function StartWait 2700 2


30.11.2020 10:26:41
Start
OK

30.11.2020 10:27:46
StartWait
OK
```

```
s00adm@sms-saptest:/usr/sap/S00/HDB00> sapcontrol -nr 00 -function GetProcessList

30.11.2020 10:27:56
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
hdbdaemon, HDB Daemon, GREEN, Running, 2020 11 30 10:26:42, 0:01:14, 5482
hdbcompileserver, HDB Compileserver, GREEN, Running, 2020 11 30 10:26:52, 0:01:04, 5753
hdbdiserver, HDB Deployment Infrastructure Server-S00, GREEN, Running, 2020 11 30 10:27:31, 0:00:25, 6525
hdbdocstore, HDB DocStore-S00, GREEN, Running, 2020 11 30 10:26:53, 0:01:03, 5796
hdbdpserver, HDB DPserver-S00, GREEN, Running, 2020 11 30 10:26:53, 0:01:03, 5798
hdbindexserver, HDB Indexserver-S00, GREEN, Running, 2020 11 30 10:26:53, 0:01:03, 5800
hdbnameserver, HDB Nameserver, GREEN, Running, 2020 11 30 10:26:42, 0:01:14, 5498
hdbpreprocessor, HDB Preprocessor, GREEN, Running, 2020 11 30 10:26:52, 0:01:04, 5755
hdbwebdispatcher, HDB Web Dispatcher, GREEN, Running, 2020 11 30 10:27:31, 0:00:25, 6527
hdbxsengine, HDB XSEngine-S00, GREEN, Running, 2020 11 30 10:26:53, 0:01:03, 5802
s00adm@sms-saptest:/usr/sap/S00/HDB00>
s00adm@sms-saptest:/usr/sap/S00/HDB00>
```

Step 4 Start SAP S/4HANA.

Run the following commands:

sapcontrol -nr 01 -function StartService S01

sapcontrol -nr 02 -function StartService S01

Then run the following commands:

sapcontrol -nr 01 -function Start

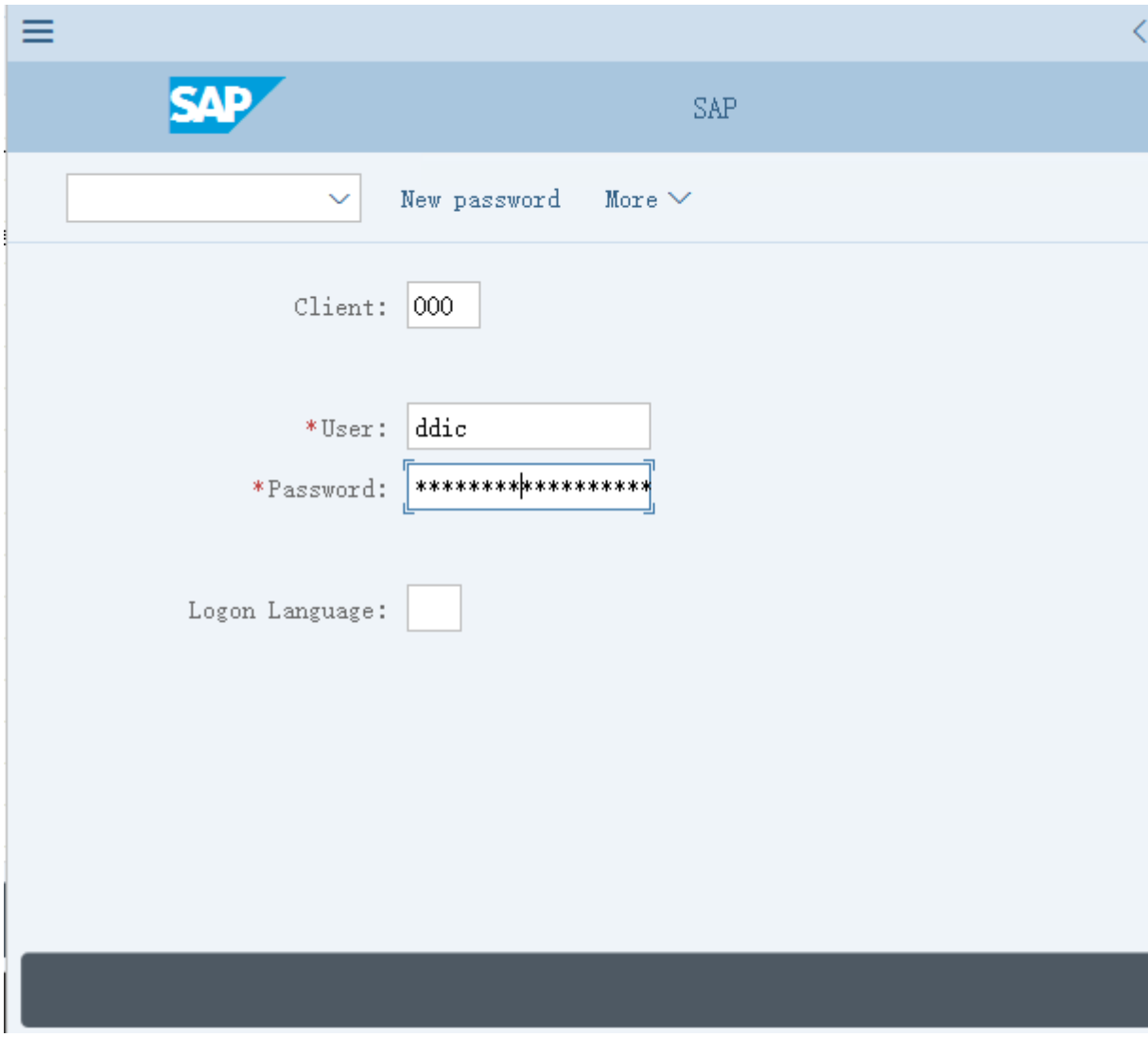
sapcontrol -nr 02 -function Start

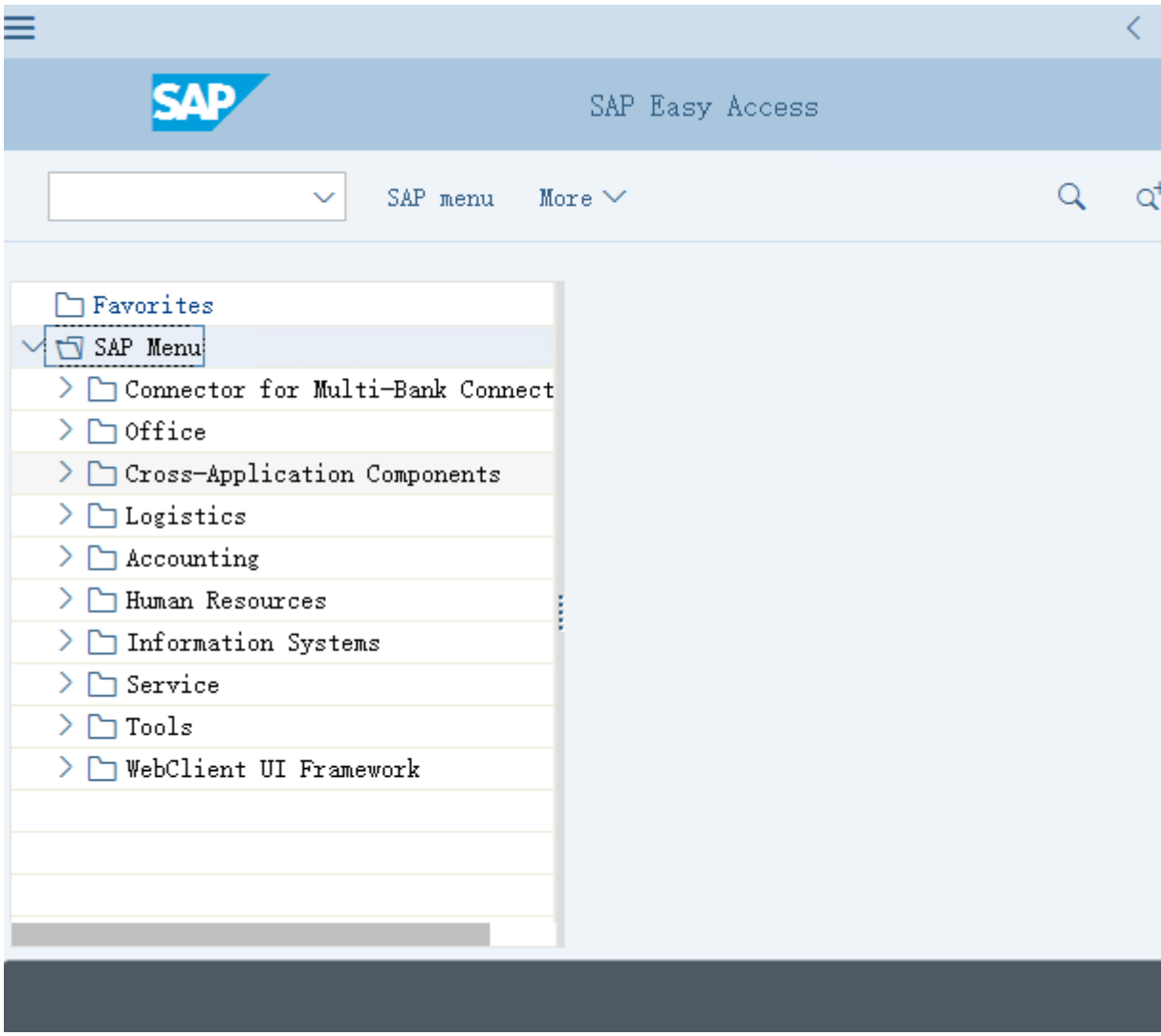
```
sms-saptest:~ # su - s01adm
sms-saptest:s01adm 52> sapcontrol -nr 01 -function GetProcessList

30.11.2020 10:30:28
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
disp+work, Dispatcher, GRAY, Stopped, , , 5411
igswd_mt, IGS Watchdog, GRAY, Stopped, , , 5412
sms-saptest:s01adm 52> sapcontrol -nr 01 -function Start

30.11.2020 10:30:35
Start
OK
sms-saptest:s01adm 53> sapcontrol -nr 02 -function Start

30.11.2020 10:30:40
Start
OK
sms-saptest:s01adm 54> sapcontrol -nr 01 -function GetProcessList

30.11.2020 10:31:27
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
disp+work, Dispatcher, GREEN, Running, 2020 11 30 10:30:36, 0:00:51, 7365
igswd_mt, IGS Watchdog, GREEN, Running, 2020 11 30 10:30:36, 0:00:51, 7366
gwrd, Gateway, GREEN, Running, 2020 11 30 10:30:37, 0:00:50, 7384
icman, ICM, GREEN, Running, 2020 11 30 10:30:37, 0:00:50, 7385
sms-saptest:s01adm 55>
```

Step 5 (Optional) Use SAP GUI to connect to SAP S/4HANA for verification.

Choose **Variable Logon** in the toolbar, enter the IP address of the SAP application server, PAS instance number, and system ID, and click **Next**.

Step 6 Click **Logon**. In the dialog box that is displayed, enter the username **ddic** and password, and press **Enter**.





Step 7 The check is completed and the results meet the expected requirements. SAP S/4HANA and SAP HANA on the destination server can start and run properly, and the SAP GUI can be used to connect to SAP S/4HANA.

----End

8.4 Change History

Description	Released On	Prepared By
This issue is the first official release.	2020-11-30	Xiong Peng/ 00508152
Updated the migration procedure of the latest SMS.	2021-08-30	Fu Chuandong/ 00469497

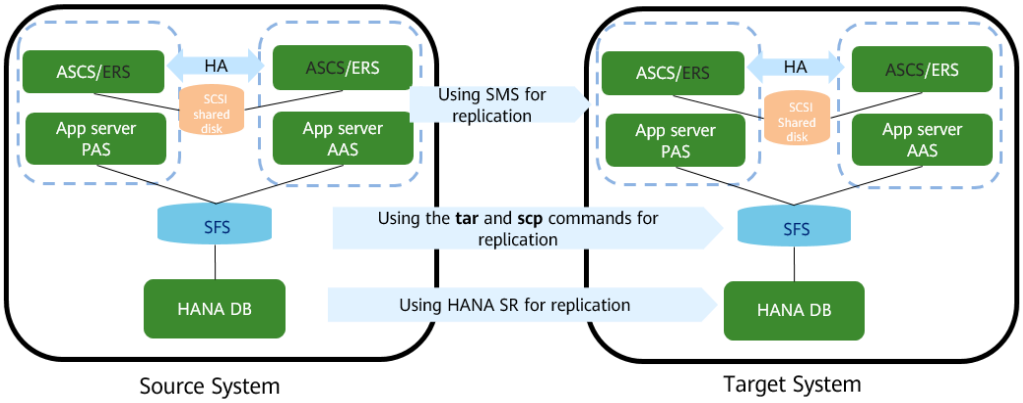
9 Best Practice of SAP Migration from XEN to KVM

9.1 Introduction

Xen PODs on HUAWEI CLOUD are gradually replaced by KVM PODs. In addition, AZs where Xen PODs reside are under inventory management and do not support new deployment and capacity expansion. This document guides SAP migration from the Xen POD to the KVM POD in two AZs isolated from each other in the same region. You can also refer to this document for other SAP migrations, such as migration from offline to online, or online migration.

9.2 Overall Solution

In this scenario, there are five servers, four of which are used to deploy applications and one is used to deploy database. The operating system (OS) of both the source and target systems needs to be the same. The HANA database version of the target system must be no earlier than that of the source system. The architecture and migration solution are shown in the following figure:



1. Use HUAWEI CLOUD Server Migration Service (SMS) to completely replicate and migrate the system image and disk data of the four application servers and the mounted storage disk to the target system.

2. Use the SFS shared storage and the **tar** and **scp** commands of the OS to copy data in the SAP directory to the target system.

3. Use SAP HANA System Replication (SR) to replicate data in HANA database to the target database.

9.3 Preparations

Before the migration, ensure that the following preparations are complete:

1. Obtain information about the OS version, network planning and design, and file system of the source system, and generated the delivery LLD of the target system based on the obtained information.

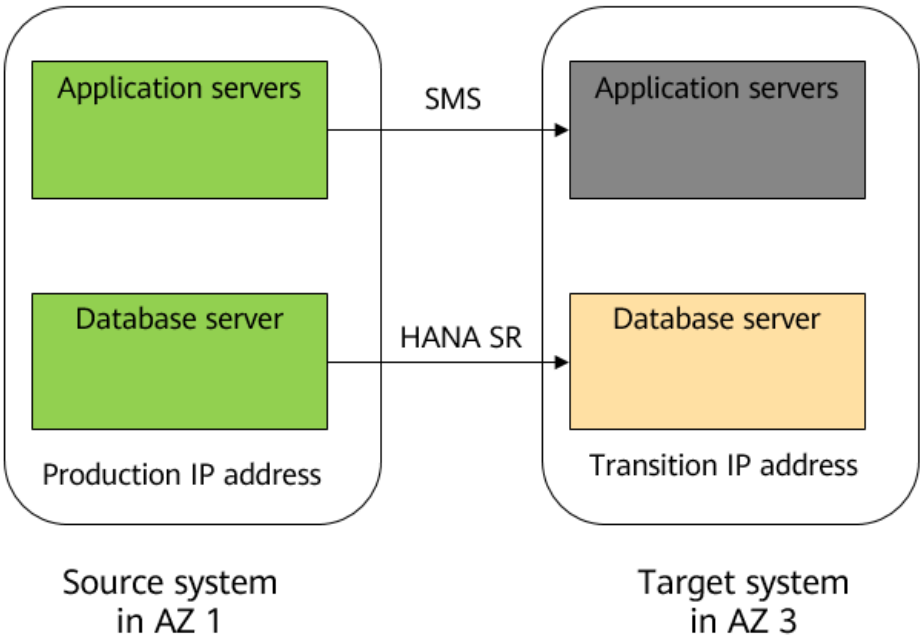
2. Confirm the HANA database version of the source and target systems, and obtain the OS image and installation package of the target database.

3. Ensure that your SMS account has sufficient balance for server creation and renewal.

9.4 Implementation

There are two phases for SAP migration. In the first phase, replicate files and data in the source system to the target system. In the second phase, stop the source system and bring the target system online.

9.4.1 Replication Procedures



In this phase, deploy new servers in AZ 3, use SMS for real-time replication of application servers, and use HANA SR for asynchronous database replication. In this case, the source system is running properly as the production system, while the target system is not running and has no impact on the production system.

9.4.1.1 Preparations

1. Before the replication, ensure that you have performed a full backup of the source system to restore the system in case of faults or misoperations. Back up the HANA database using HANA Studio or other methods. Back up the four application servers using the Cloud Backup and Recovery service of HUAWEI CLOUD.

2. Install the SMS migration Agent on the four application servers. For details, see **Preparations Before Migration** and **Installing the Agent on Linux Servers**.

9.4.1.2 Replicating the PAS and AAS

1. Configure target servers on SMS Console. For details, see **Configuring the Target ECS**.

2. Start server replication. For details, see **Starting Replication**.

3. Launch target servers. For details, see **Launching the Target ECS**.

Note: Before launching target servers, ensure that SAP in the source system is not set to automatically start upon power-on.

4. Check the target server configuration.

Step 1 Run the **dh -h** command to check whether the file system of the target system (except the NFS file system) is the same as that of the source system.

Step 2 Query the **/etc/fstab** configuration file to check whether the directories and items (except the NFS file system) mounted during startup are the same as those in the source system.

----End

9.4.1.3 Replicating the ASCS and ERS

1. Configure target servers by following the instructions provided in **Configuring the Target ECS**. The target servers must have same disks as the source servers have. The shared disk of the target ASCS is the same as that of the source ASCS, and that of the target ERS is the same as that of the source ERS.

2. Start server replication. For details, see **Starting Replication**.

3. Launch target servers. For details, see **Launching the Target ECS**.

Note: Before launching target servers, ensure that SAP in the source system is not set to automatically start upon power-on.

4. Check the target server configuration.

Step 1 On the HUAWEI CLOUD management console, mount the ERS shared disk to ASCS and the ASCS shared disk to ERS.

Step 2 Create an SBD shared disk and mount it to ASCS and ERS based on the delivery LLD.

Step 3 Run the **dh -h** command to check whether the file system of the target system (except the NFS file system) is the same as that of the source system.

Step 4 Query the **/etc/fstab** configuration file to check whether the directories and items (except the NFS file system) mounted during startup are the same as those in the source system.

----End

9.4.1.4 Replicating HANA Database

Step 1 Create an ECS for the target HANA database on HUAWEI CLOUD Console based on the delivery LLD.

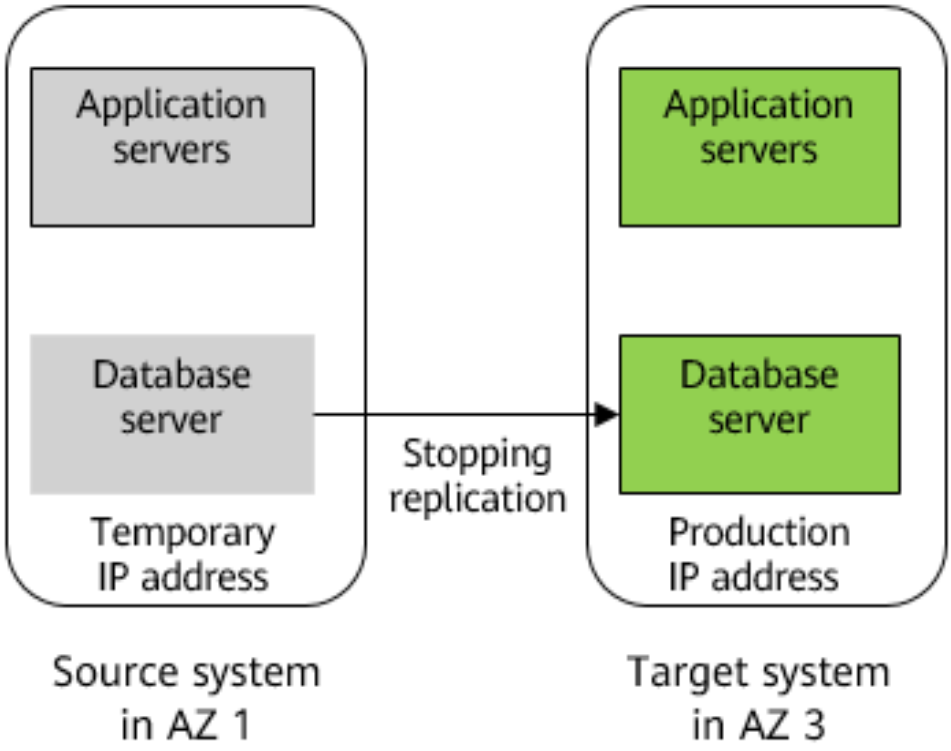
Step 2 Install the HANA database and upgrade it to the target version. The version must be no earlier than the HANA version of the source system.

Step 3 Configure the SR data synchronization between the source database and the target database on the backend.

```
hdbnsutil -sr_enable --name=[Server name of the target HANA DB]    //(Source HANA DB execution)
hdbnsutil -sr_register --remoteHost=[Server name of the target HANA DB] --remoteInstance=00 --
replicationMode=sync  --name=[Server name of the source HANA DB]      //(Target HANA DB execution)
HDB start  //(Target HANA DB execution)
```

----End

9.4.2 Go-online Procedures



In this phase, stop the source system, switch the production IP address to the target system in AZ 3, and start services in the target environment to take over production services.

9.4.2.1 Backup Before Going Online

Before going online, perform a full backup of the source system to restore the system in case of faults or misoperations. Back up the HANA database using HANA Studio or other methods. Back up the four application servers using the Cloud Backup and Recovery service of HUAWEI CLOUD.

9.4.2.2 Stopping the Source System

Step 1 Log in to SAP and lock all accounts except the DDIC and hand system accounts in the SU 10 mode.

Step 2 Create a test user in PFCG.

Step 3 Suspend backend tasks on SAP.

Step 4 Stop applications in the source system.

Log in to the PAS/AAS server as an application user and run the **sapcontrol -nr [***Instance ID***] -function Stop** command to stop PAS and AAS.

Log in to any ASCS/ERS node as the **root** user and run the **service pacemaker stop** command to stop ASCS and ERS.

Step 5 Shut down the source database. Ensure that no other services directly read data from or write data to the HANA database after applications are stopped.

Log in to the target database as a database user and run the following command to stop data synchronization with the source database:

```
hdbnsutil -sr_unregister
```

Log in to the source database as a database user and run the following command:

```
HDB stop
```

Step 6 Change the IP addresses of the source servers.

Log in to the HUAWEI CLOUD management console and change the physical IP addresses of the primary and extension NICs of the five source servers to temporary IP addresses.

Note: Before changing the IP addresses of the primary NICs, ensure that the servers are shut down.

----End

9.4.2.3 Starting the Target System

Step 1 On the management console, shut down the five servers of the target system.

Step 2 Change the physical IP addresses of the primary and extended NICs of the five servers in the target system from the transition IP addresses to the production IP addresses of the source system. Bind the virtual IP addresses of the ASCS/ERS servers in the source system to the primary NICs of the ASCS/ERS servers in the target system.

Step 3 On the management console, power on the five servers of the target system.

Step 4 Check the **/etc/hosts** files on the five servers in the target system and ensure that the IP addresses match the domain names or host names. Ensure that the target HANA host name is different from the source host name. Change the HANA host name if the target system uses the source one.

Step 5 Mount the SFS shared directory.

Mount the shared file system for database backup in the source system to the **/etc/fstab** file on the target database server.

Mount the shared file system for mounting **/sapmnt/** and **/usr/sap/trans** on the source application servers to the **/etc/fstab** file on the target application servers.

Step 6 Log in to the database server as a database user and run the **HDB start** command to start the database. After the database is started, log in to the database using HANA Studio and check whether the database is normal.

Step 7 Log in to each application server and run the following command as an application user to check the database connection. If **00** is displayed in the command output, the database connection is normal.

```
hdbuserstore list
R3trans –d
```

Step 8 Change the SBD device ID in **/etc/sysconfig/sbd** on the active and standby ASCS/ERS nodes to the actual device ID and rebuild the SBD disk.


```
sbd –d  /dev/disk/by-id/scsixxxxx   -4 30 -1 15 create
```

Step 9 Start the ASCS and ERS.

Start the two-node cluster and set it to the maintenance status.

```
service pacemaker start
crm configure property maintenance-mode=true
```

Run the **crm configure edit** command to access the two-node cluster configuration page and change the ASCS/ERS shared disk ID to the actual disk ID of the target system.

Stop the maintenance status of the cluster.

```
crm configure property maintenance-mode=false
```

Check the cluster resources. Ensure that the ASCS/ERS resources are in the **started** status.

```
crm status
```

Step 10 Log in to the PAS/AAS servers as an application user, start the PAS and AAS, check their process, and check the application status on SAP.

```
sapcontrol -nr [Instance ID] -function Start
sapcontrol -nr [Instance ID] –function GetProcessList
```

----End

9.4.2.4 Checking the System Status

Log in to SAP to check whether the test user created in **Step 2 in section 4.2.2** exists, whether the backend tasks are suspended, and whether the peripheral system integration is normal.

9.4.2.5 Applying for and Importing a New License

You need to apply for a new SAP license according to the new hardware ID.

1. If you use SR for database synchronization, you do not need to apply for a new license because SR can adjust the license synchronously.
2. If you need to apply for the S/4HANA license, refer to the ASCS hardware ID. If servers are deployed in a two-node cluster and the license information is obtained from SAP, perform a active/standby switchover to ensure that ASCS on both the active and standby nodes is running, and then apply for and import a license for each node.

9.4.2.6 Restoring and launching Services

Log in to SAP, unlock all backend tasks and users, and restore services.

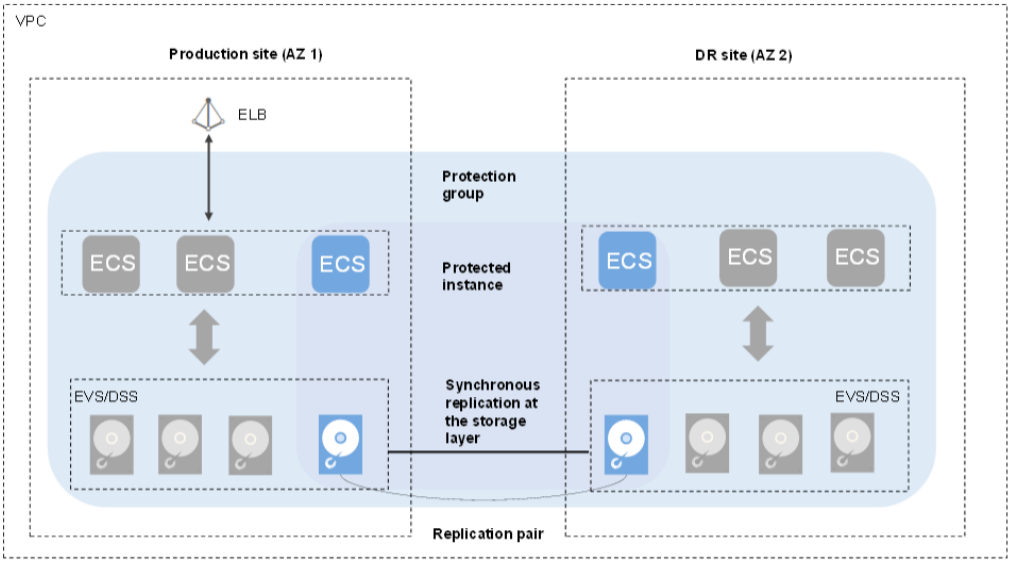
10 Best Practice of SAP Disaster Recovery with SDRS

10.1 About This Document

Storage Disaster Recovery Service (SDRS) provides disaster recovery (DR) services for many cloud services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), and Dedicated Distributed Storage Service (DSS). SDRS uses multiple technologies, such as storage replication, data redundancy, and cache acceleration, to provide you with high data reliability and service continuity.

SDRS protects service applications by replicating the server data and configurations to a DR site. It allows service applications to start at the DR site in the event that the server at the production site stops. This improves service availability and continuity.

For more information, see **Storage Disaster Recovery Service User Guide**.



10.2 Preparations for Using SDRS

This document applies to the deployment of SAP on SQL Server. Currently, Scalable File Service (SFS) file systems and SFS Turbo cannot be mounted to ECSs. Use SDRS based on the actual scenarios.

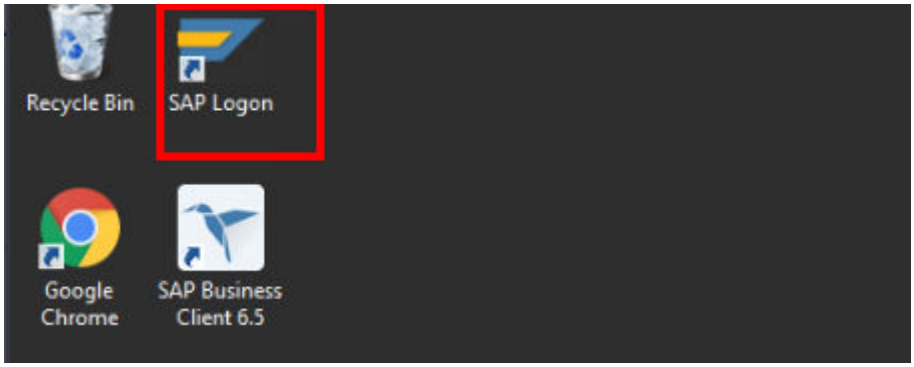
In this test, the production site and DR site are in AZ 2 and AZ 3, respectively, in the South China region. The production site uses two servers that have SAP PAS and AAS instances installed respectively, and uses the SQL Server database. After SDRS is used, the servers at the DR site are the same as those at the production site. After a failover, the IP address of the server at the DR site is exchanged with that of the server at the production site, and the server at the DR site takes over workloads from the server at the production site. The SAP system can be started and run properly, and the original production site becomes the DR site. Specifications of the ECS at the production site in this test are as follows:

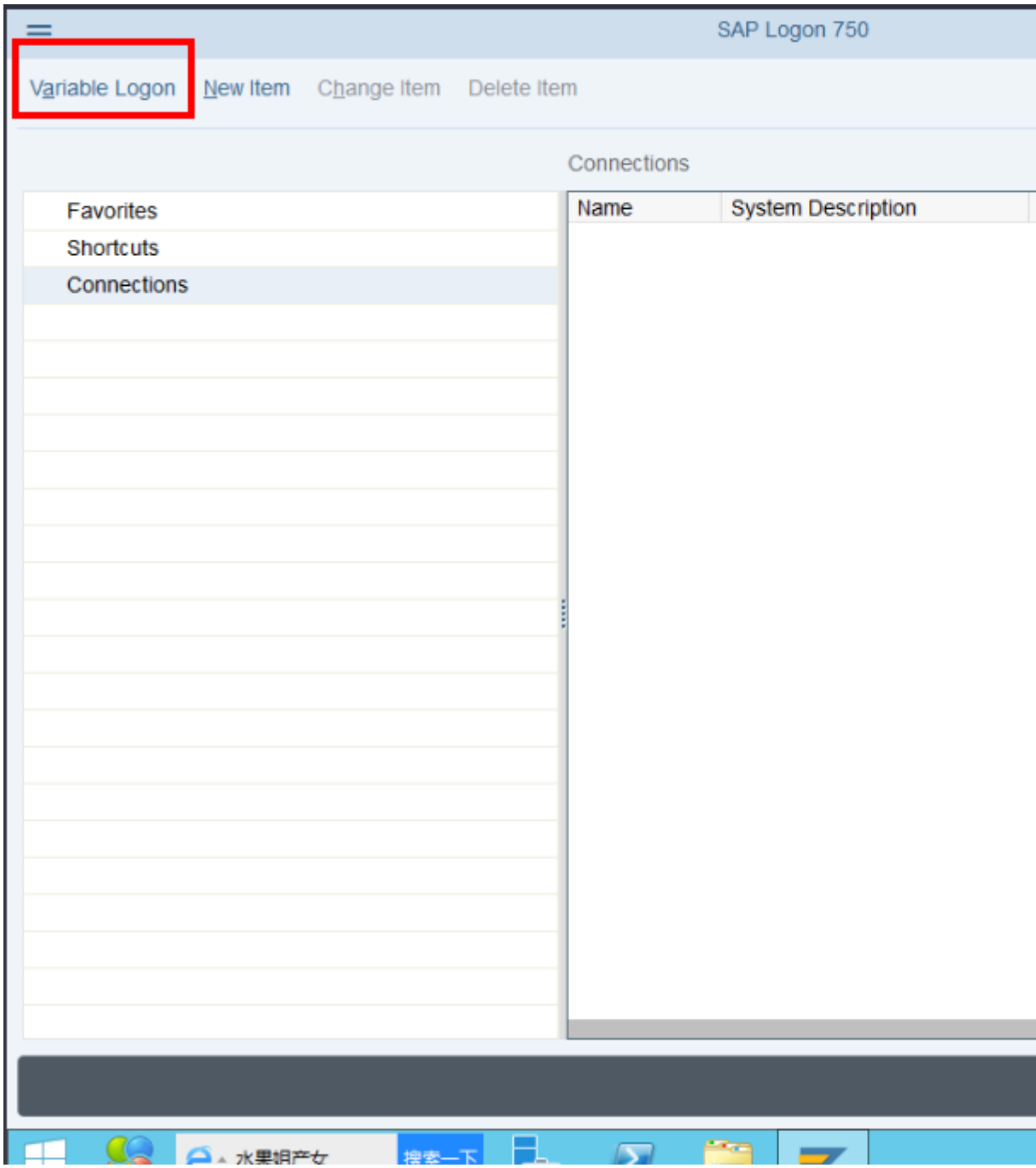
ECS Name	Flavor	Disk	Image	Remarks
ecssap1	m6.2xlarge.8	System disk: 100 GB, high I/O Data disk: 250 GB, high I/O	Windows Server 2012 R2 Standard 64-bit English (40 GB)	Used for installing SAP ERP and SQL Server
ecssap2	m6.xlarge.8			Used for installing AAS and SAP GUI

Viewing the Hardware Key at the Production Site

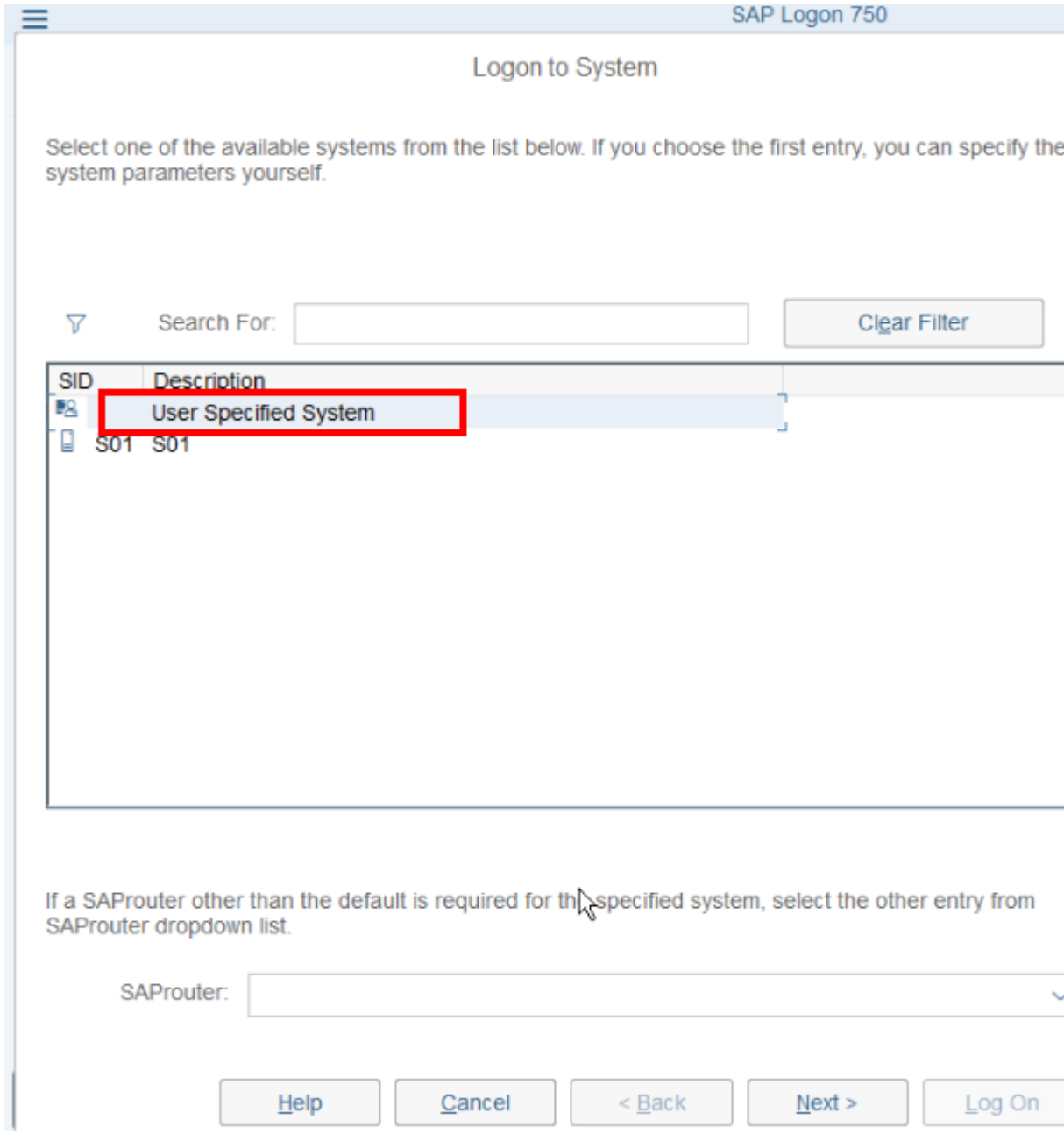
Use the SAP GUI to connect to an SAP application, check and save the SAP hardware key, compare the key with the hardware key after the failover, and ensure that SAP is started.

Step 1 Log in to **ecssap2** at the production site, run SAP Logon, and click **Variable Logon**.

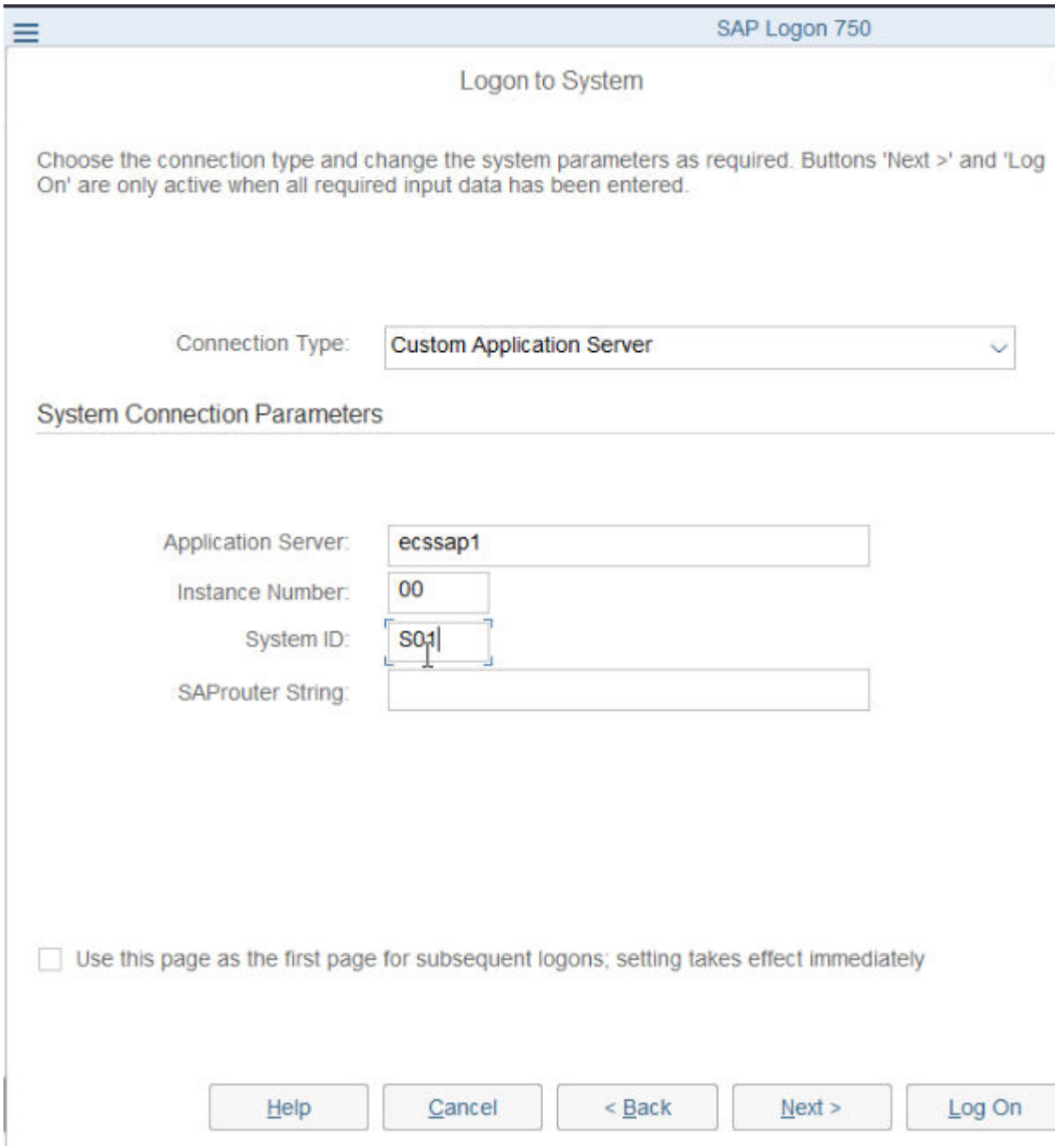


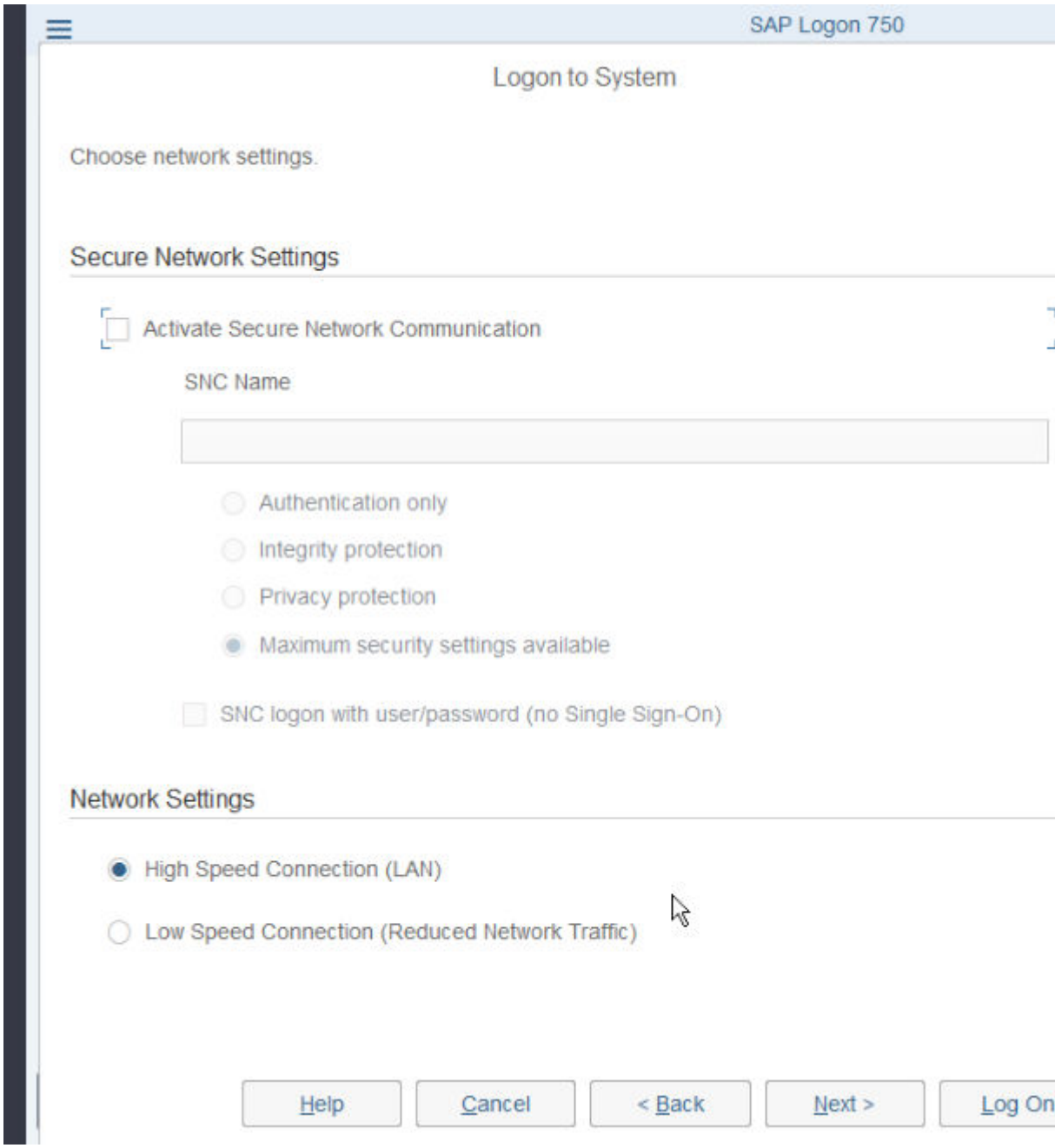


Step 2 Double-click **User Specified System**.

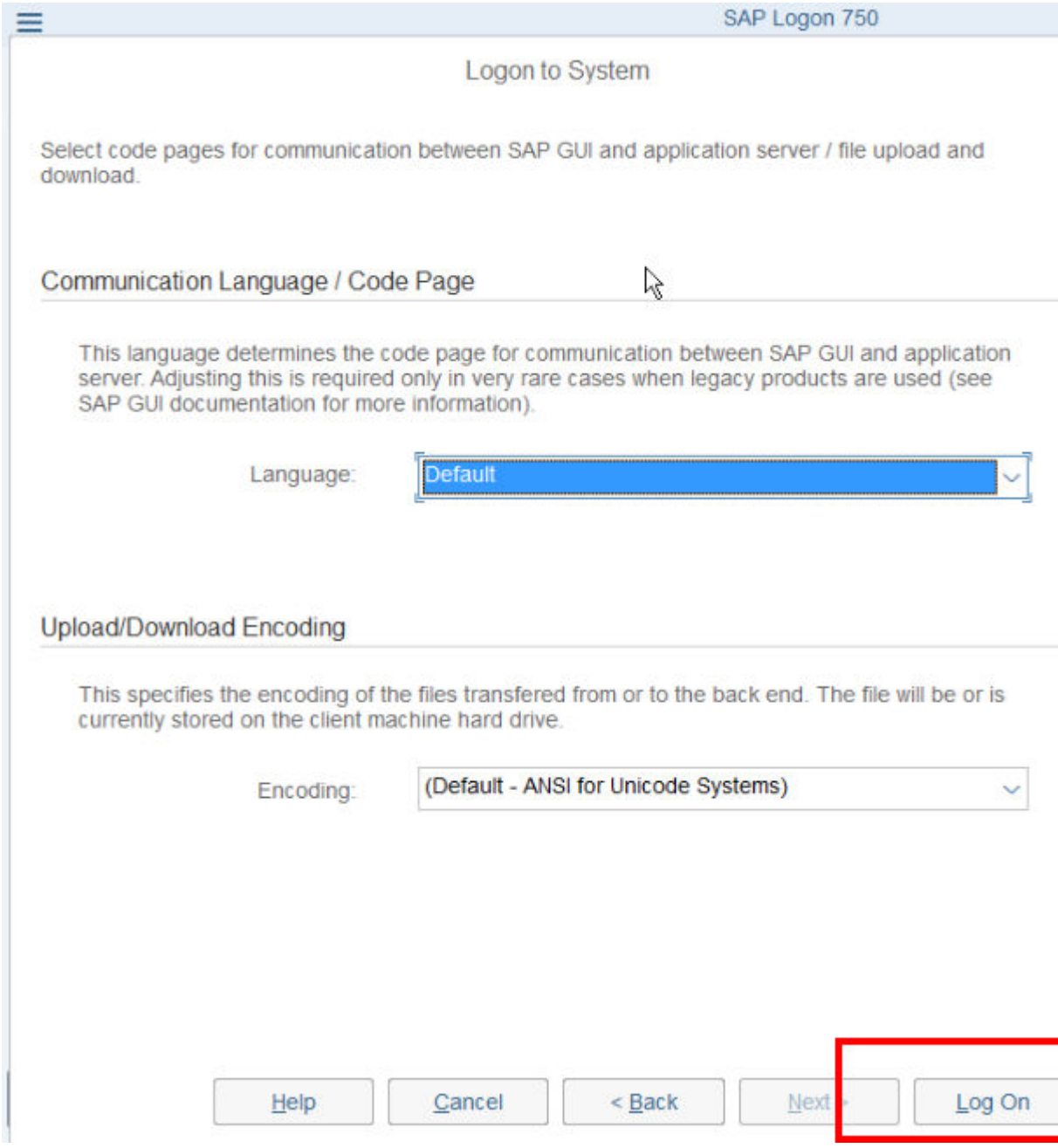


Step 3 Configure required parameters based on the site requirements and click **Next**.

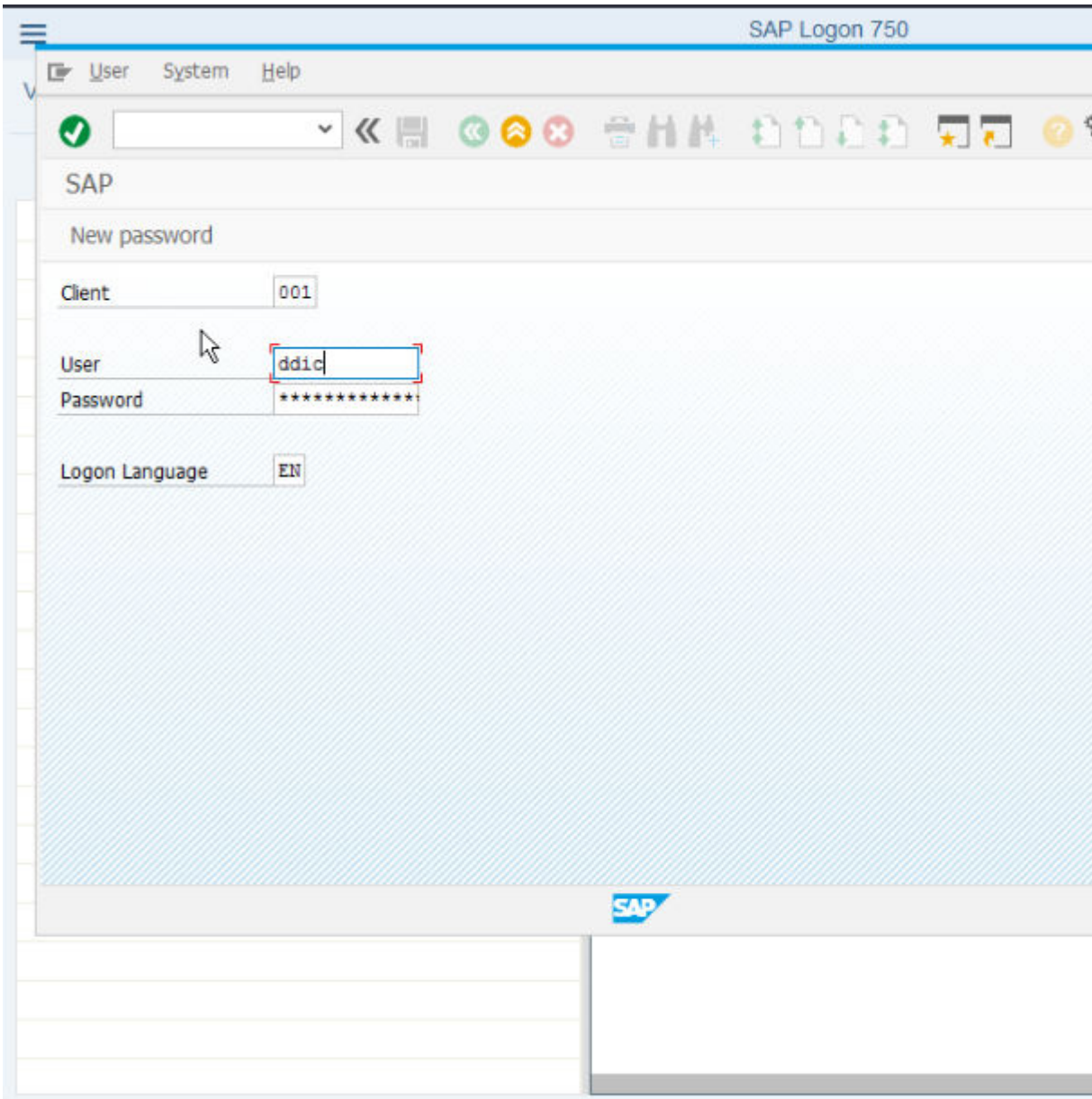


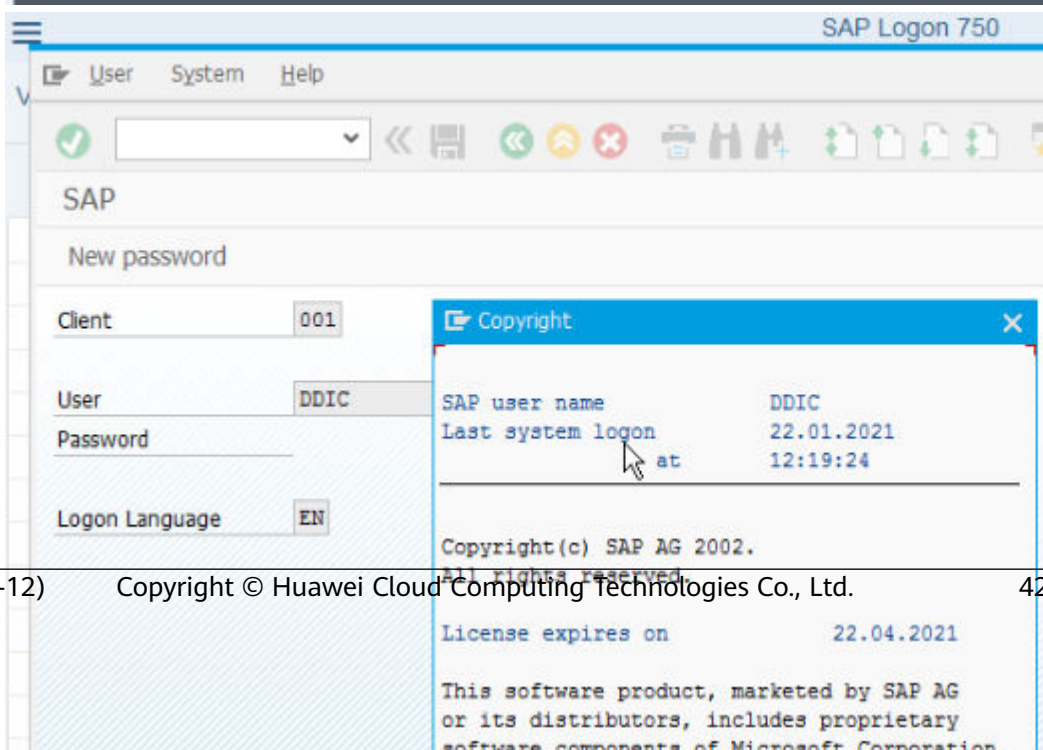


Step 4 Click **Log On**.

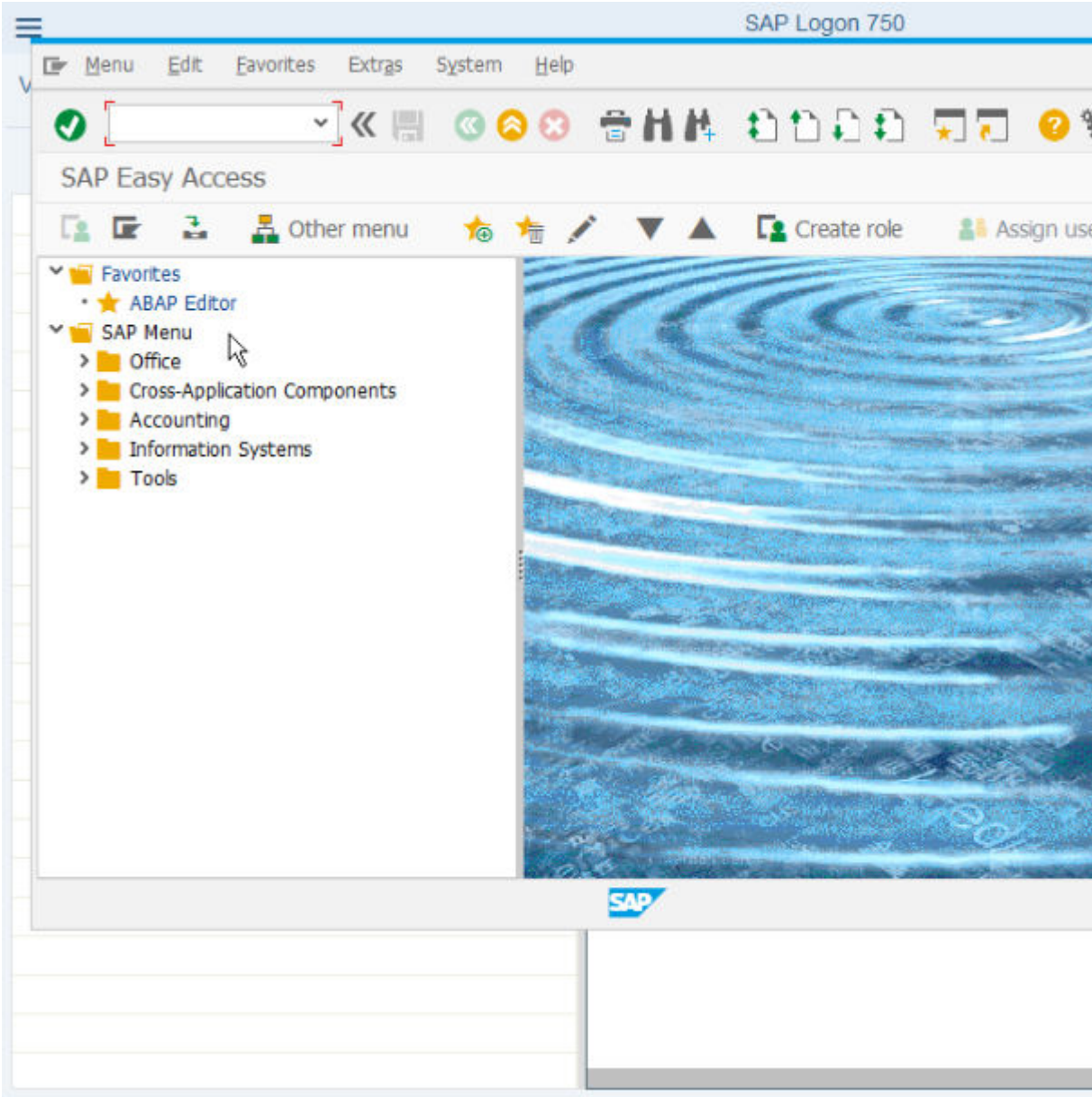


Step 5 Enter username **ddic** and the password, and then press **Enter**.

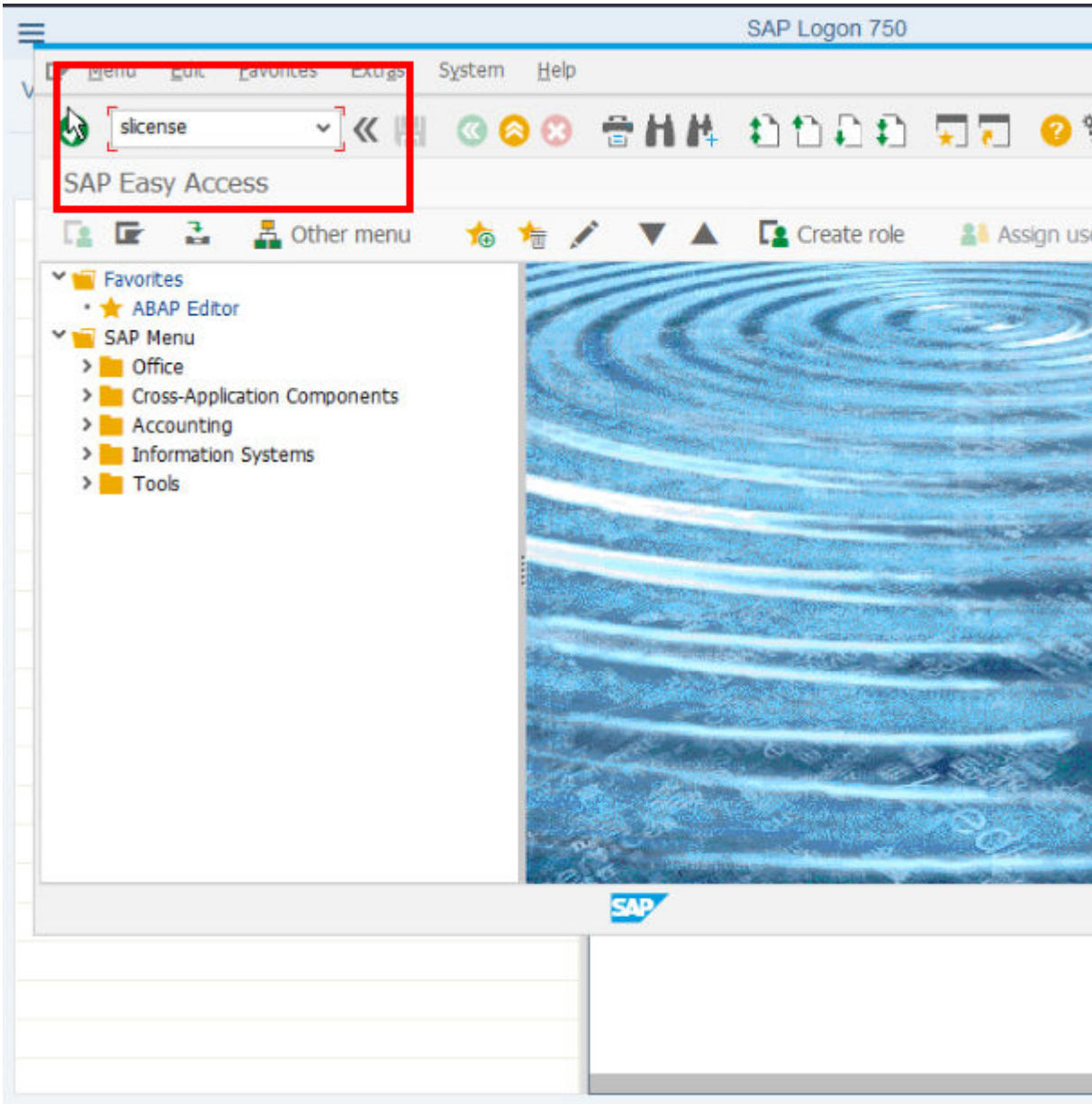

SAP Logon 750
User System Help
SAP
New password
Client 001
User ddic
Password
Logon Language EN

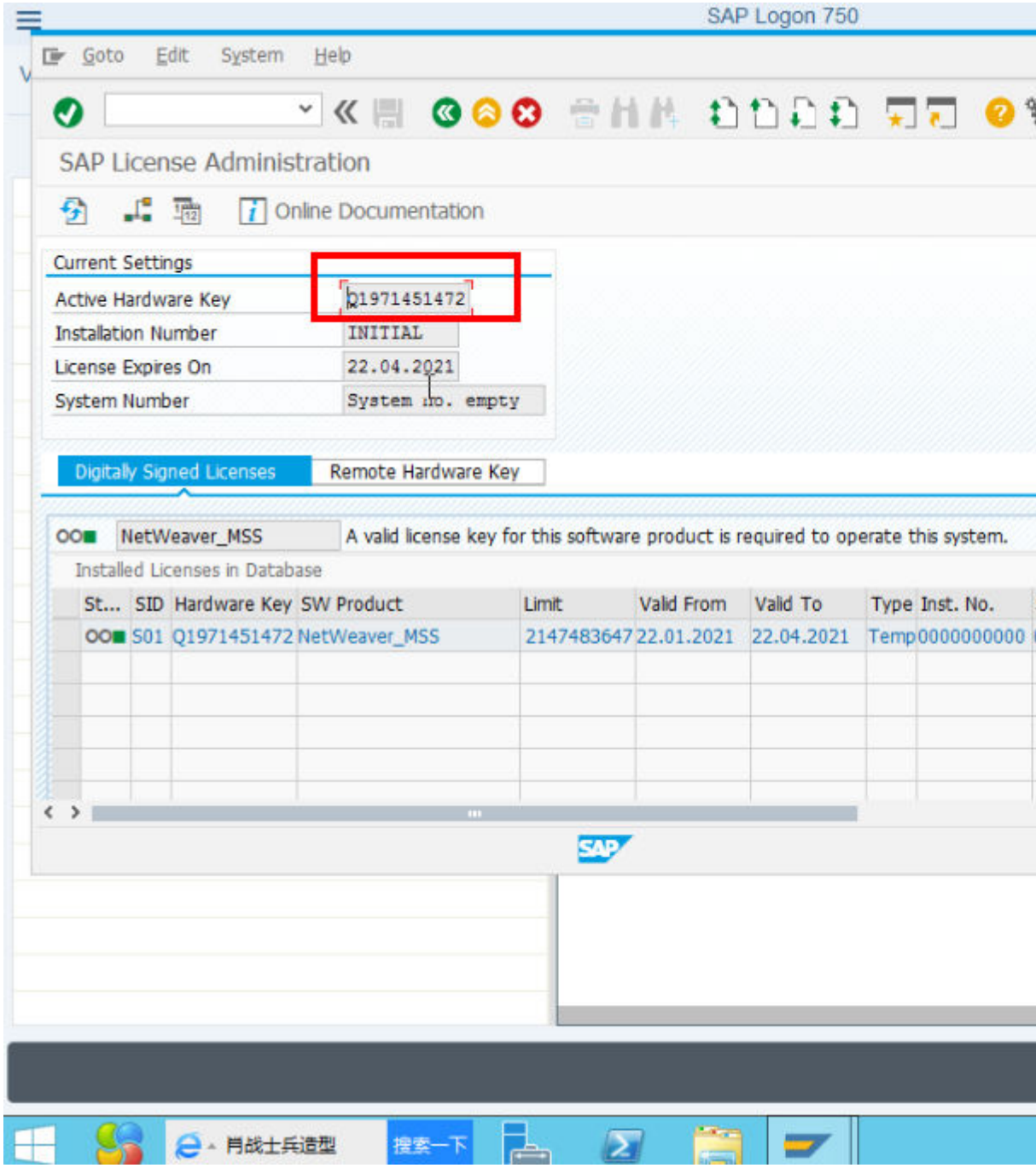

SAP Logon 750
User System Help
SAP
New password
Client 001
User DDIC
Password
Logon Language EN
Copyright
SAP user name DDIC
Last system logon 22.01.2021
at 12:19:24
Copyright(c) SAP AG 2002.
All rights reserved.
License expires on 22.04.2021
This software product, marketed by SAP AG
or its distributors, includes proprietary

Step 6 The login to SAP GUI is successful.



Step 7 Enter **slicense** in the search box and press **Enter** to view the value of **Active Hardware Key** and record it.





----End

10.3 DR Configurations

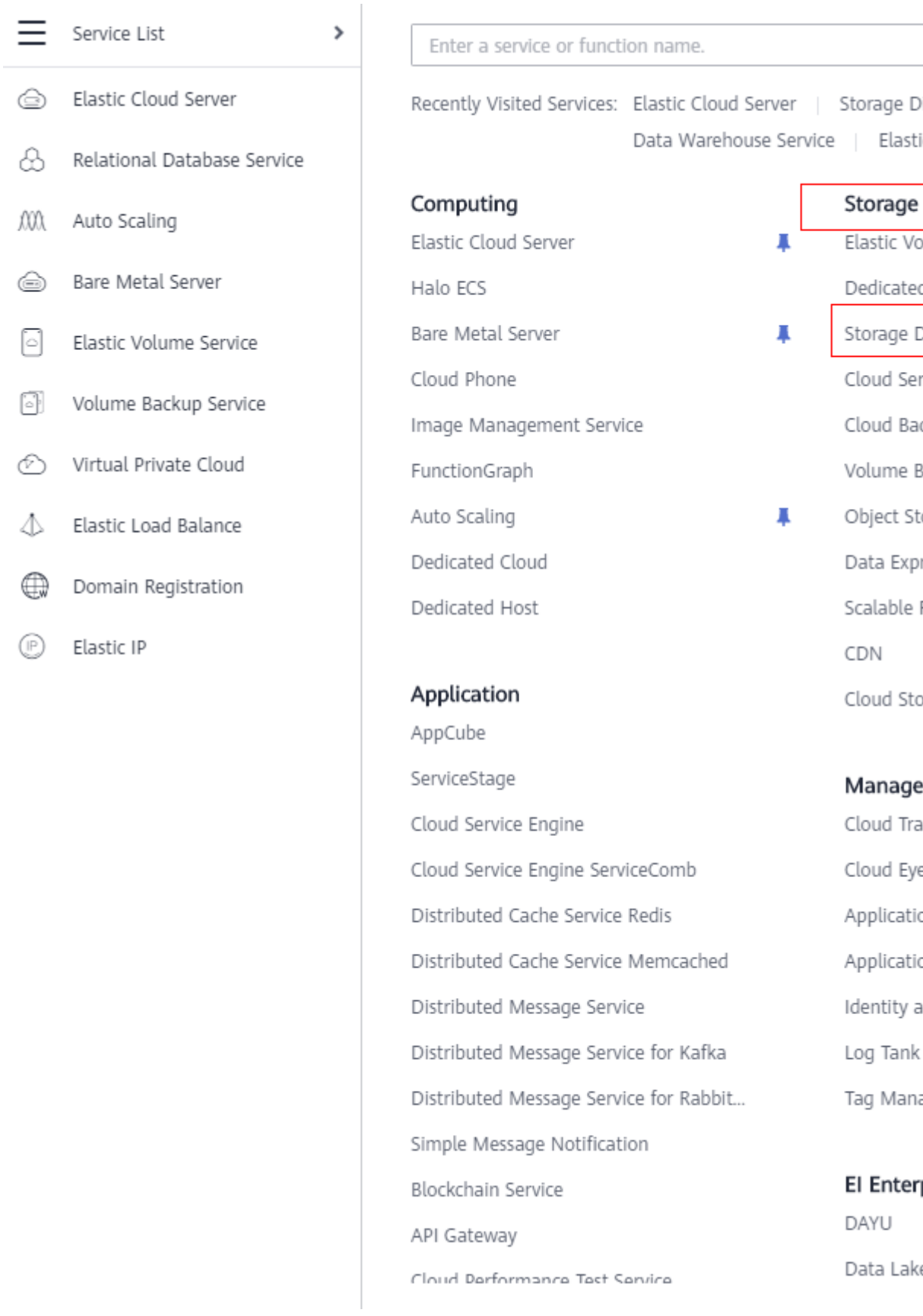
10.3.1 Creating a Protected Group

Specify two AZs as the source and target AZs, and create a protection group. Then, you can create protected instances and replication pairs in this protection group.

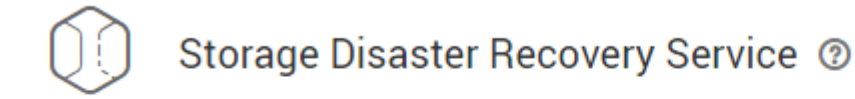
Determine the production and DR sites before you create a protection group. In this version, only the VPC migration deployment model is supported. Specifically,

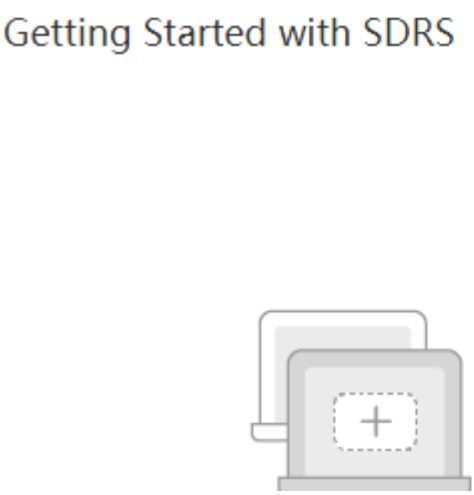
the servers at the production and DR sites must be in different AZs but in the same VPC.

Step 1 Log in to the management console and choose **Storage** > **Storage Disaster Recovery Service**.

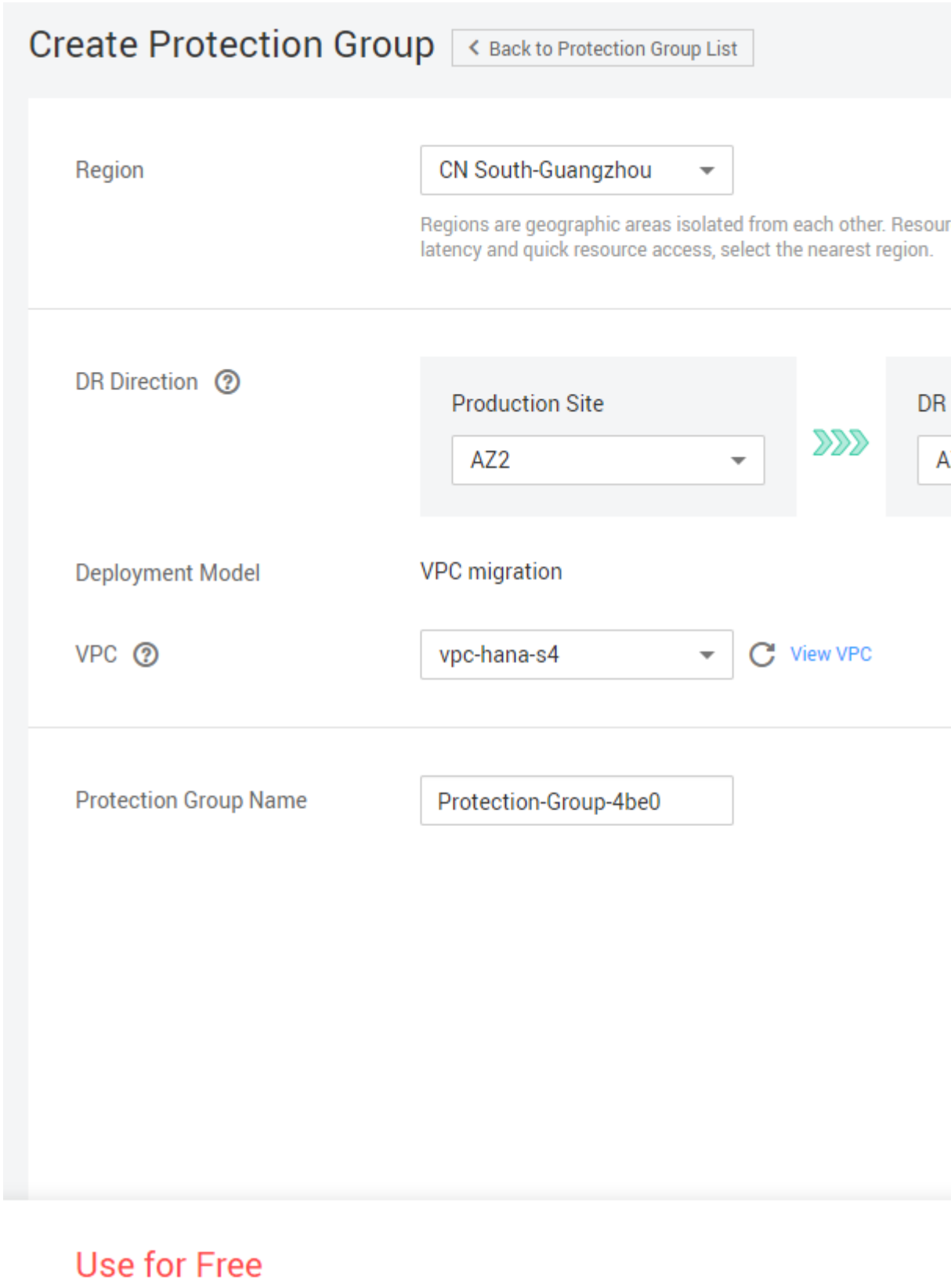


Step 2 Click **Create Protection Group**.



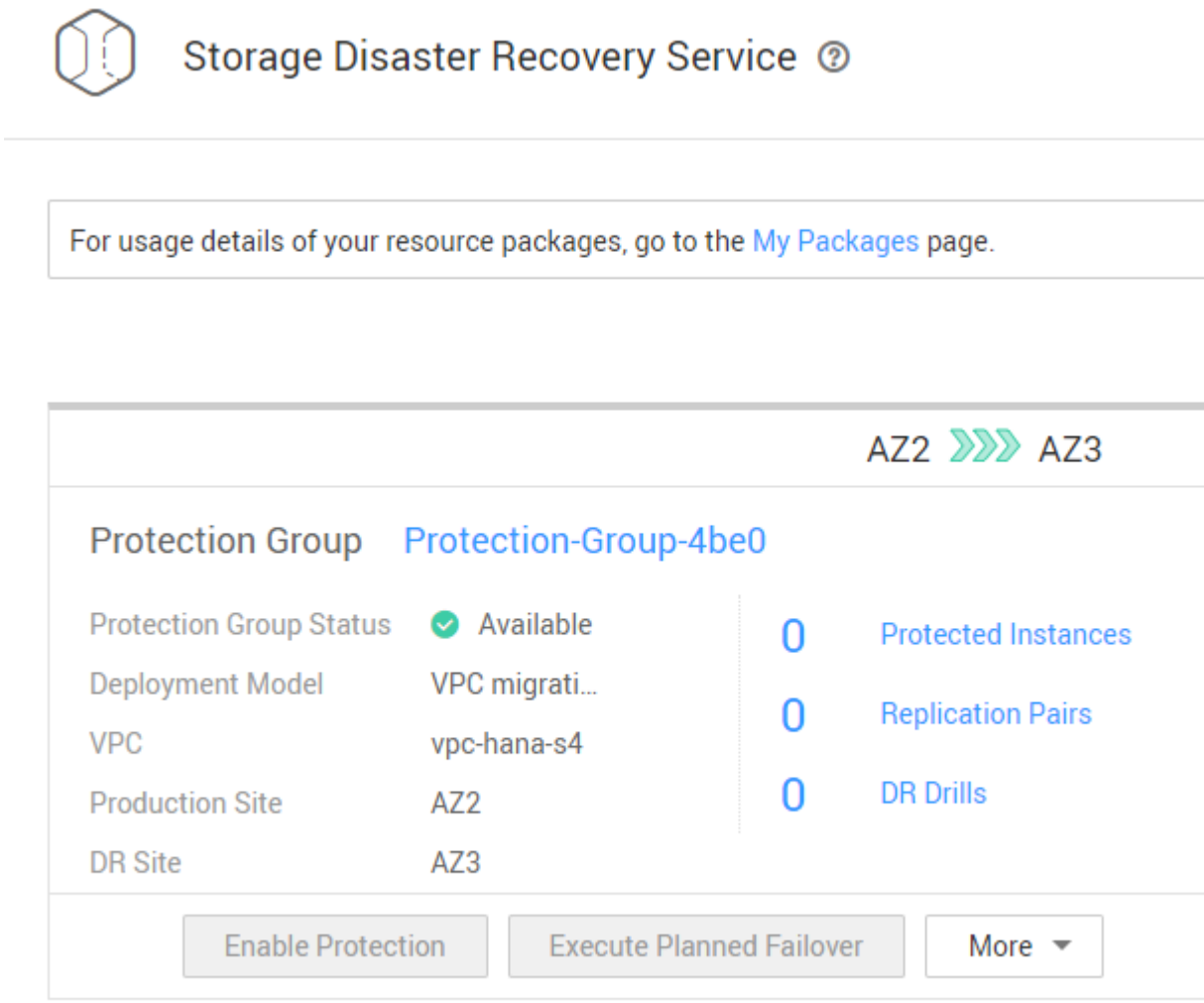


Step 3 Configure the basic information about the protection group as prompted. (Set **Production Site** and **VPC** to the actual AZ and VPC where the production server is located, respectively.)

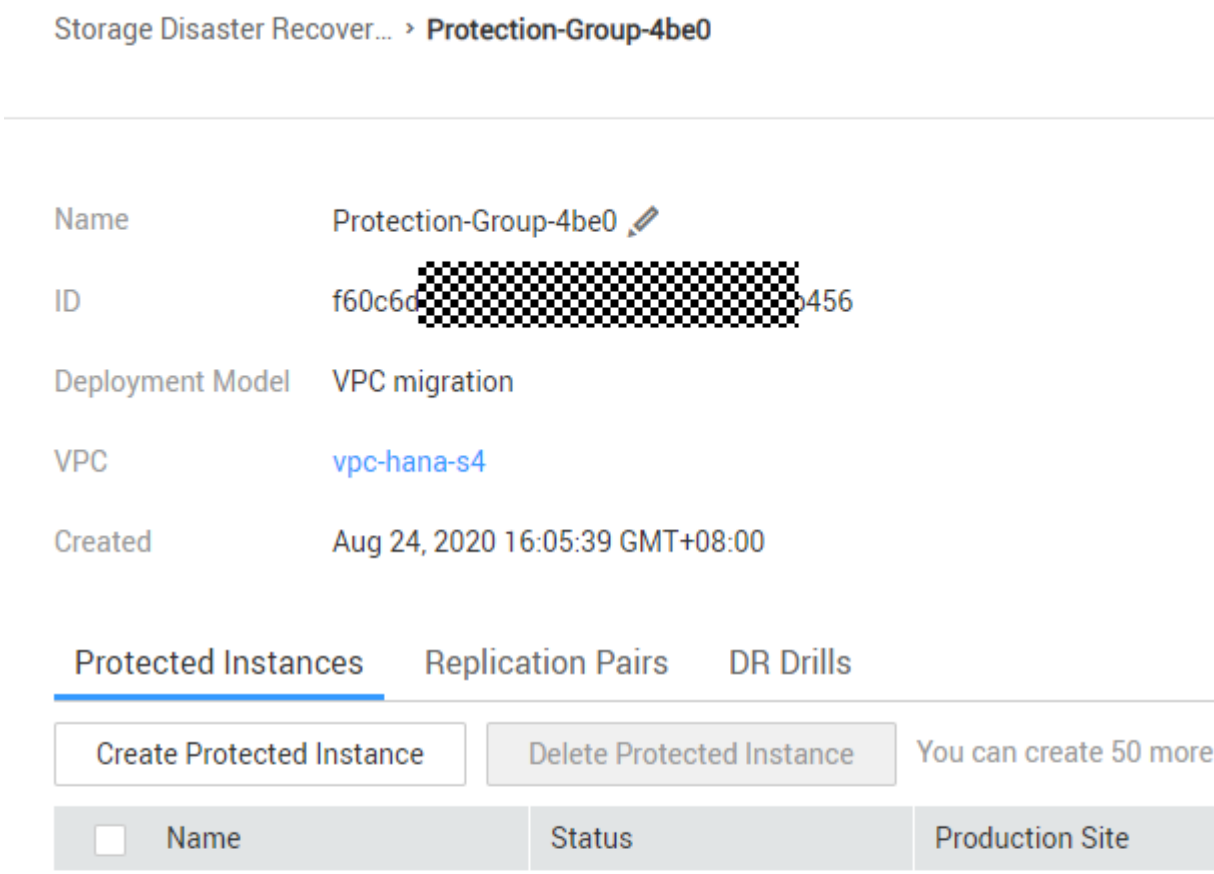


Step 4 Click **Create Now**.

Step 5 Click **Back to Protection Group List** to return to the SDRS homepage and query the protection group status.



Step 6 Click the name of the protected group to view its details.



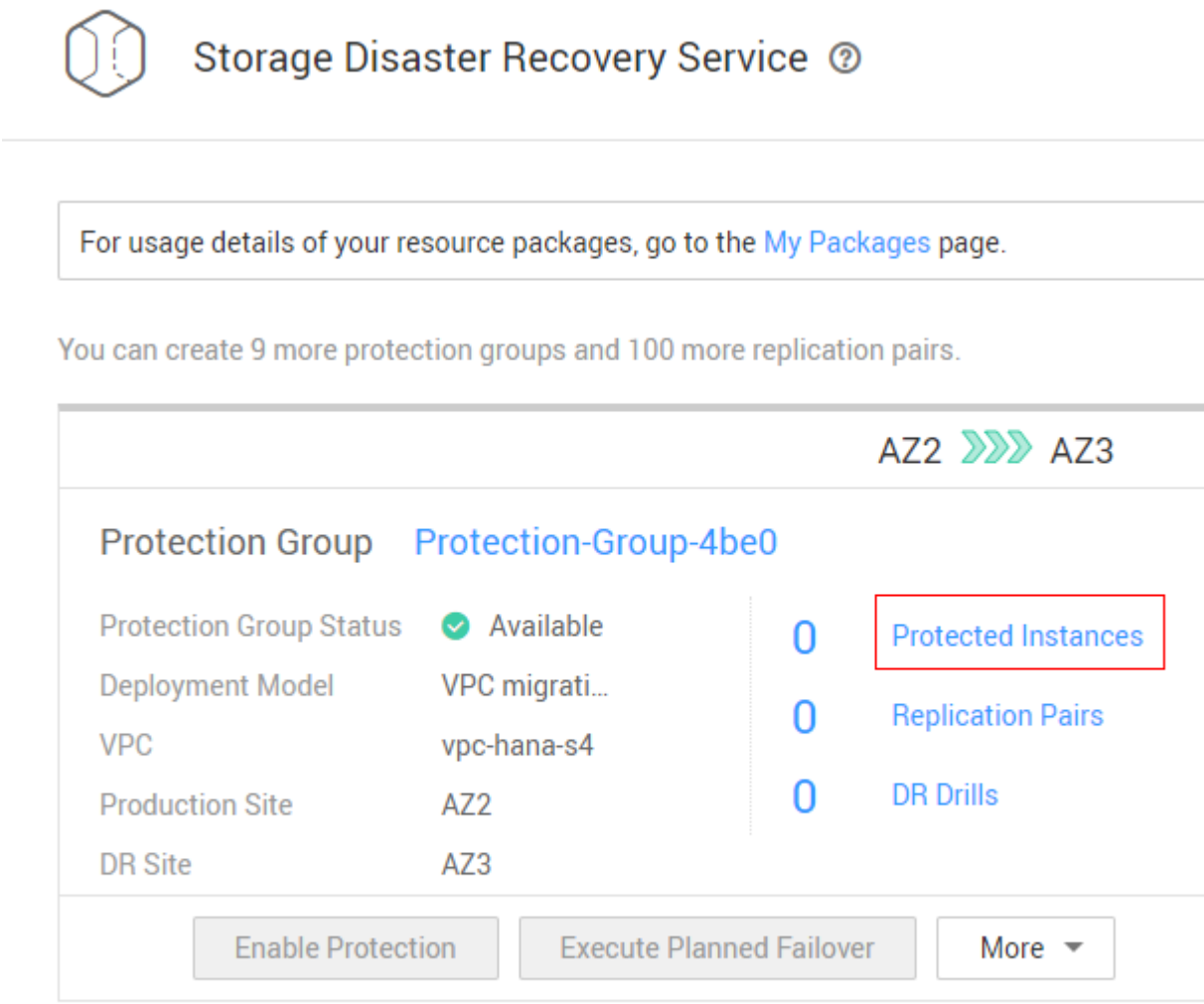
----End

10.3.2 Creating a Protected Instance

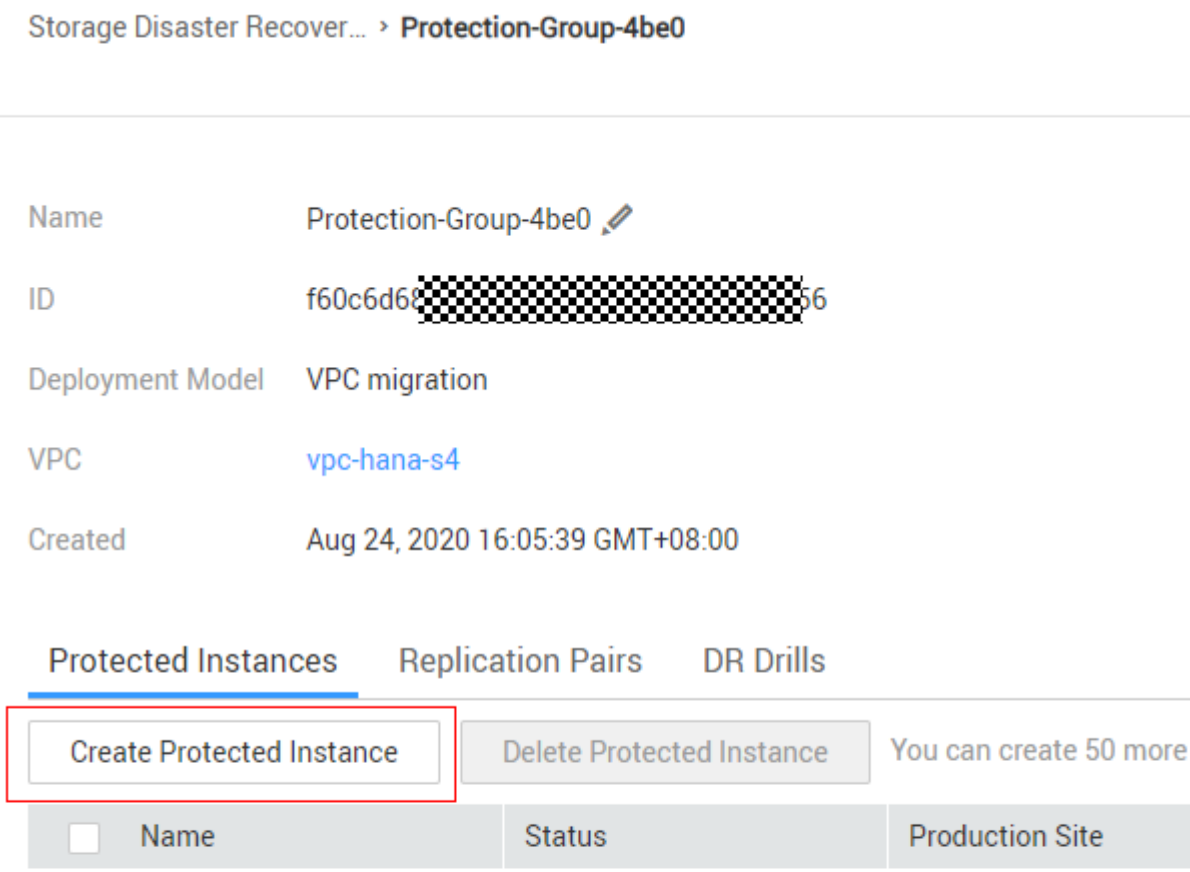
Select a protection group for each server to be replicated and create a protected instance using the server. When you create a protected instance, the server and disk will be created at the DR site for the production site server and disk. The server specifications can be configured as required. Specifically, the specifications of the DR site server can be different from those of the production site server. The disks of the production site and DR site are of the same specifications and can automatically form a replication pair.

The server at the DR site is in the **Stopped** state after the protected instance created. These automatically created resources, including the DR site servers and disks, cannot be used before a planned failover or failover.

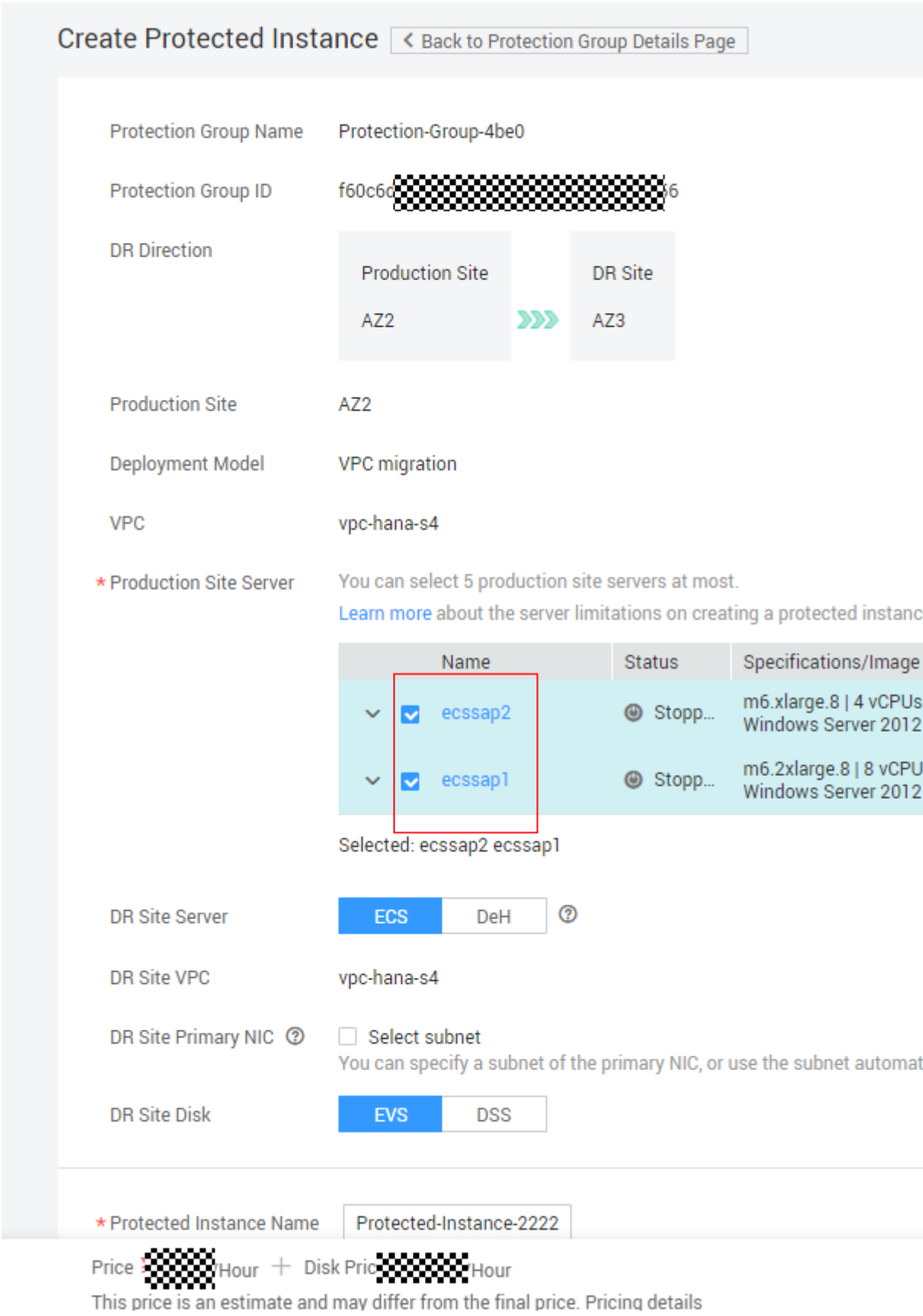
Step 1 On the **Storage Disaster Recovery Service** page, click **Protected Instances** in the created protection group.



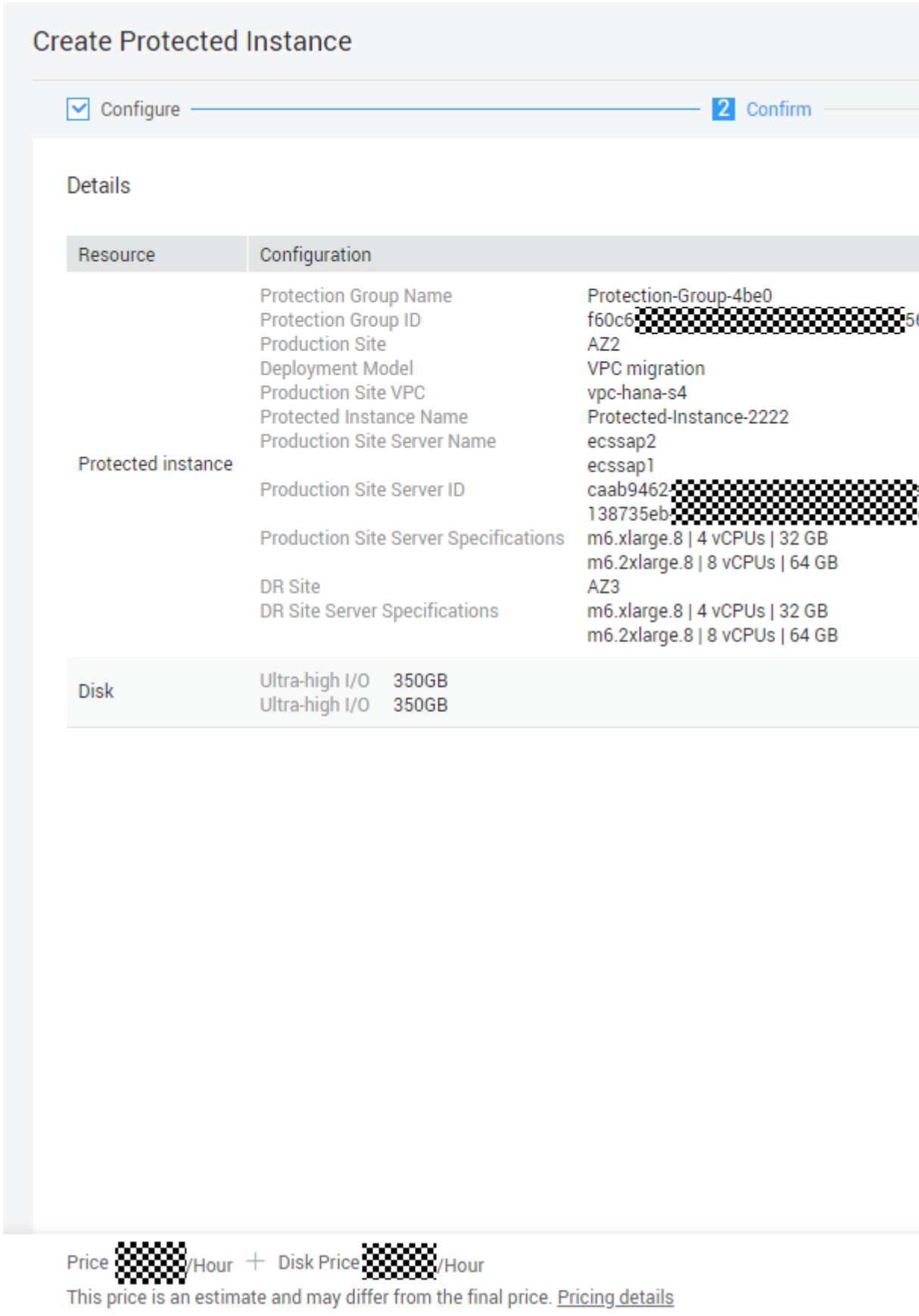
Step 2 Click **Create Protected Instance** under the **Protected Instances** tab.



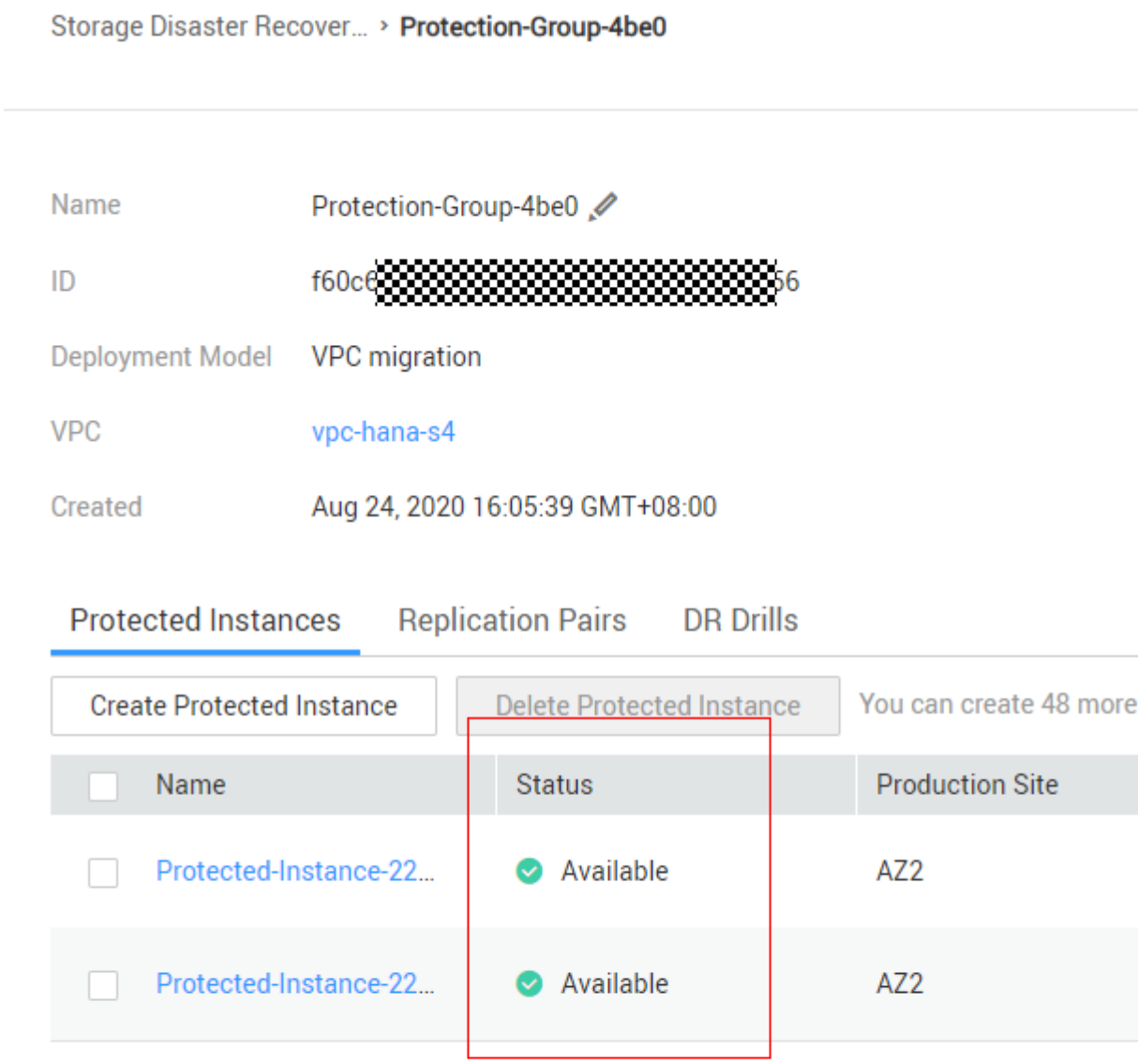
Step 3 Configure the basic information about the protected instance as prompted. The specifications of the server can be modified.



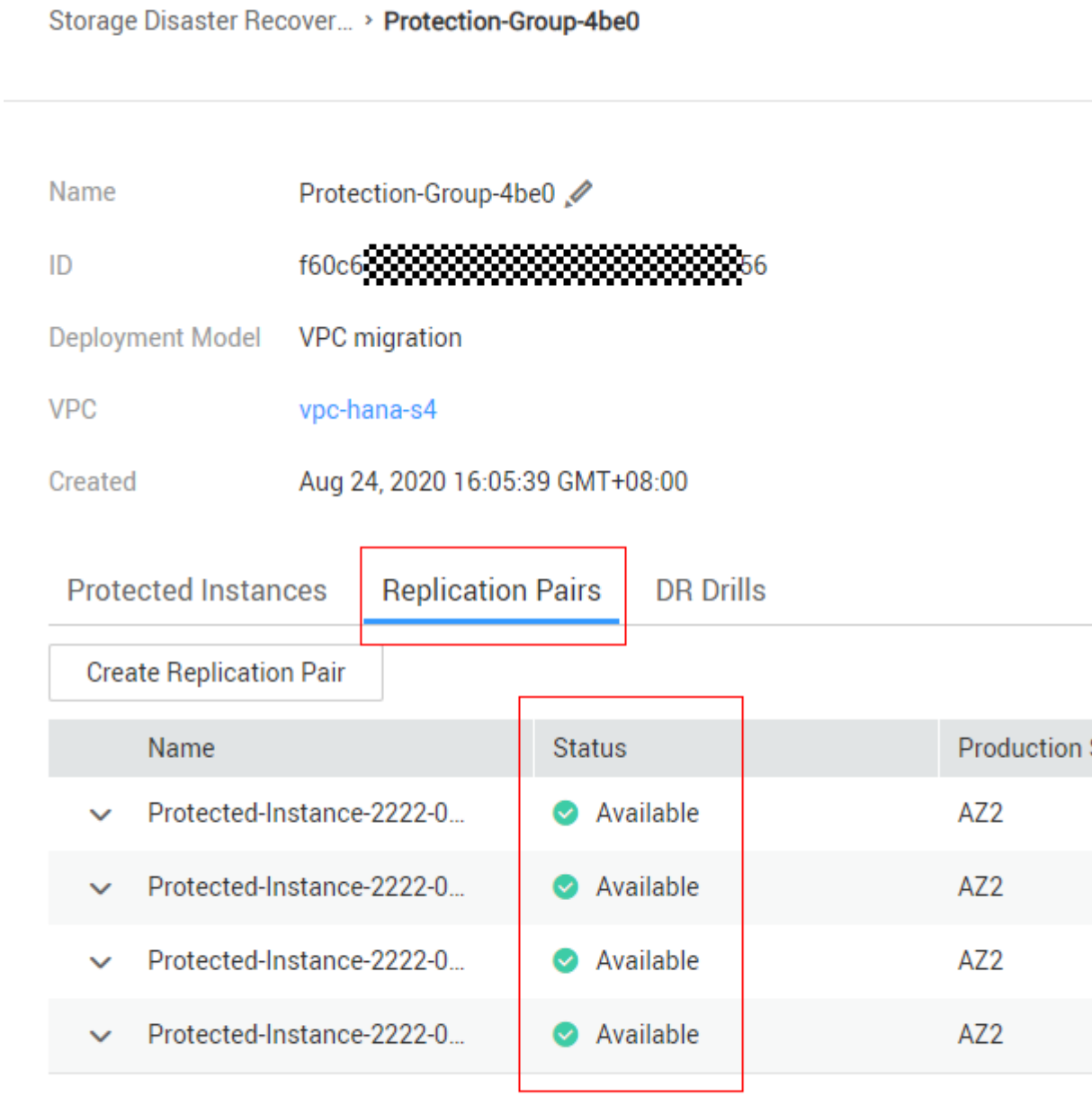
Step 4 Click **Create Now**, confirm the configuration parameters, and click **Submit**.



Step 5 Click **Back to Protection Group Details Page** and view the protected instances of the protection group. If the protected instance status changes to **Available** or **Protecting**, the protected instance has been created successfully.



Step 6 After a protected instance is created, the system automatically creates replication pairs for the disks of the protected instance and backs up all the disks. To view the replication pair details, click the **Replication Pairs** tab.

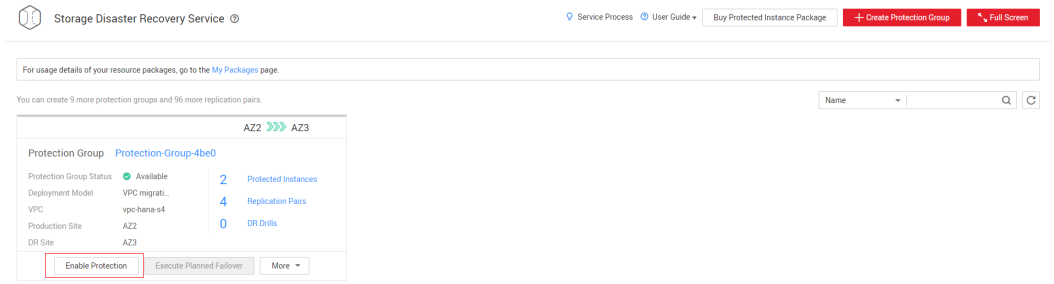


----End

10.3.3 Enabling Protection

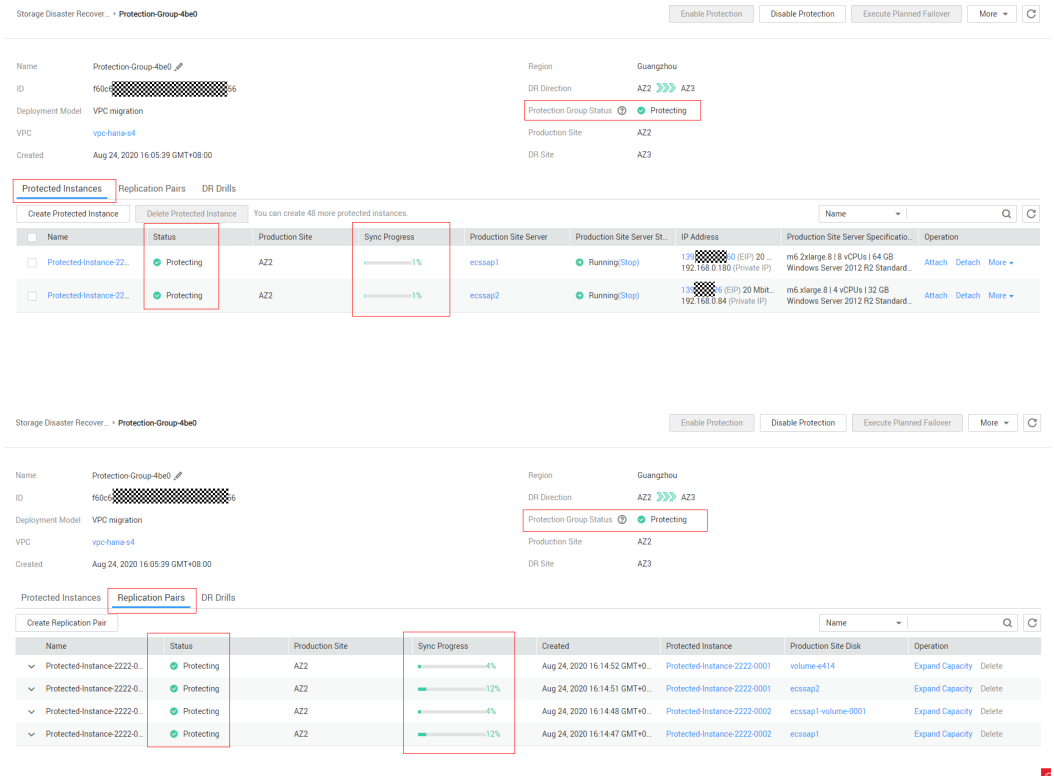
When data is written to the disks of the server at the production site, SDRS synchronizes the data to the disks of the server at DR site in real time.

Step 1 On the **Storage Disaster Recovery Service** page, click **Enable Protection** in the pane of the desired protection group.

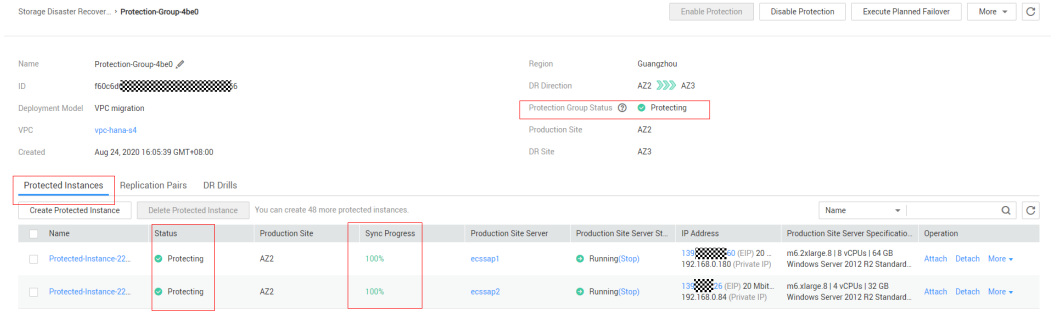


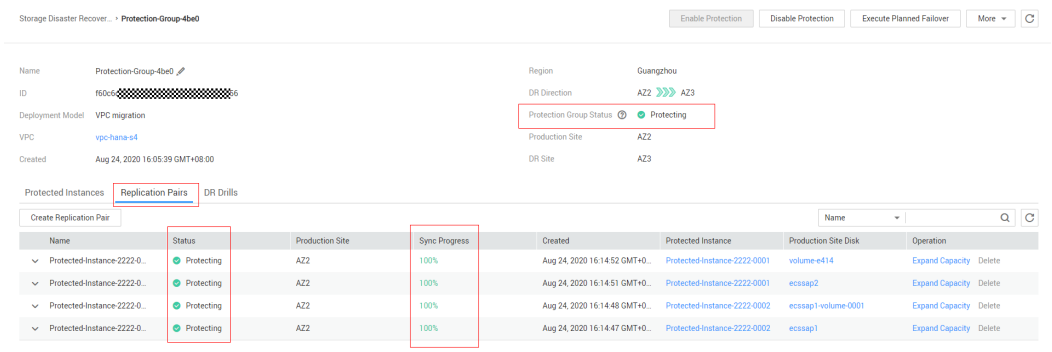
Step 2 In the displayed dialog box, confirm the protection group information, and click **Yes**. Once protection is enabled, data synchronization starts.

Step 3 Click the protected group to view the data synchronization progress.

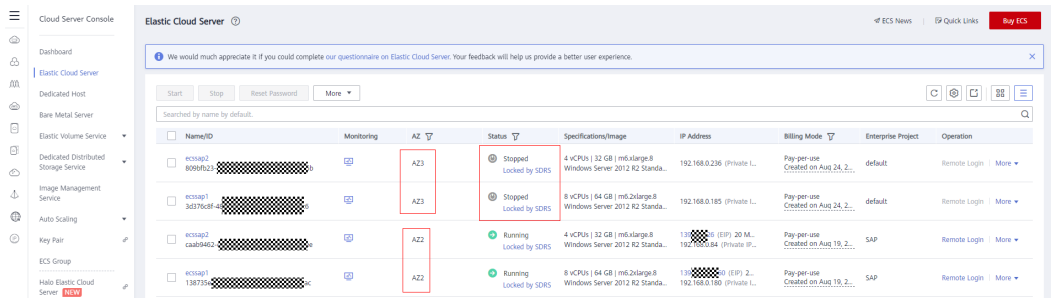


Step 4 View the data synchronization results.





Step 5 Log in to the ECS console, and you can see that two ECSs with the same specifications as those at the DR site are created, the AZ of the two ECSs is the AZ selected when the protection group is created, and the two ECSs are in the **Stopped** state.

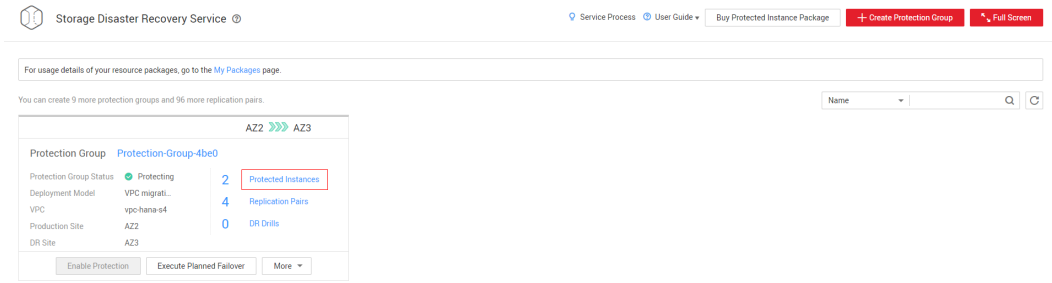


----End

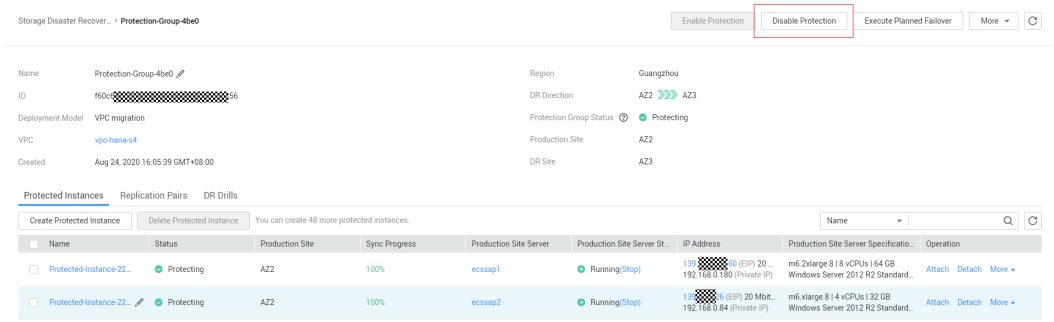
10.3.4 Disabling Protection

If you want to disable protection for all resources in a specified protection group, you can perform steps provided in this section. Once the protection is disabled, data synchronization for all protected instances in the protection group will stop.

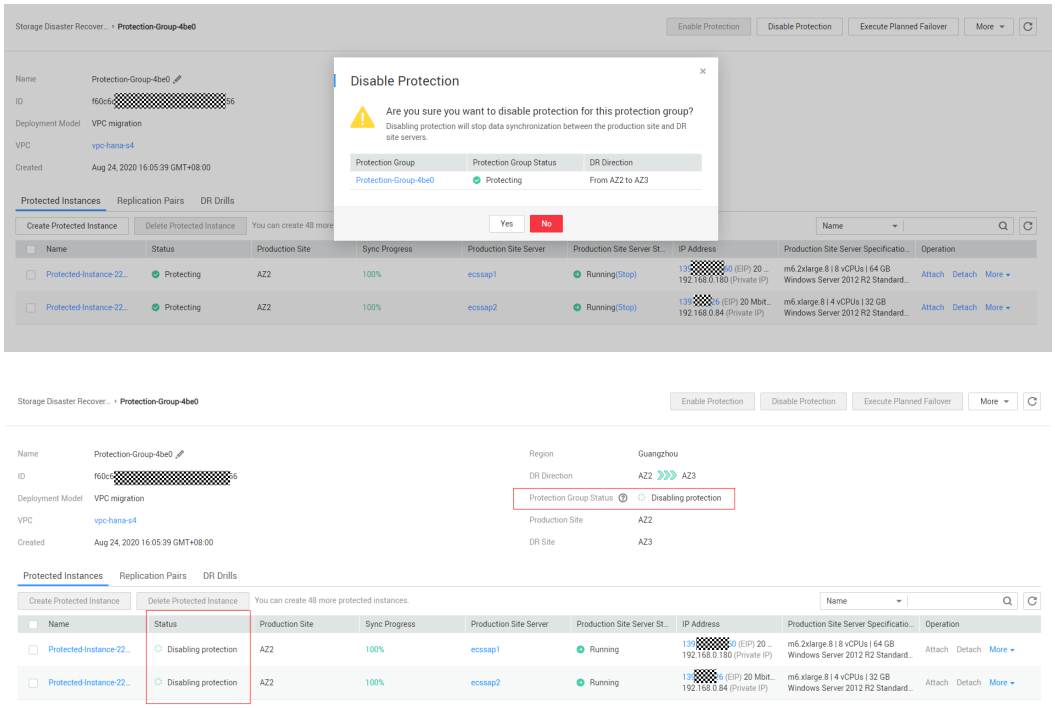
Step 1 Log in to the **Storage Disaster Recovery Service** page. In the pane of the protection group to be disabled, click **Protected Instances**.



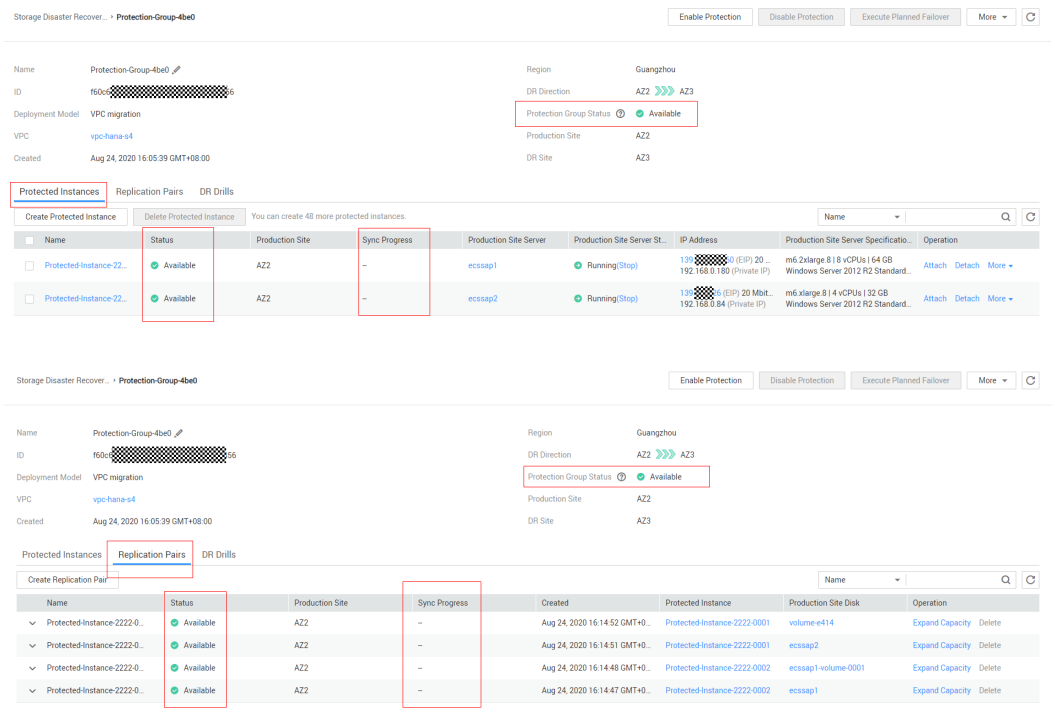
Step 2 In the upper right corner of the page, click **Disable Protection**.



Step 3 In the displayed dialog box, confirm the protection group information, and click **Yes**.



After protection is disabled, data synchronization between the production site and DR site for all protected instances in the protection group will stop.



Step 4 To enable protection again, perform the steps described in **Enabling Protection**.

----End

10.3.5 Performing a Planned Failover

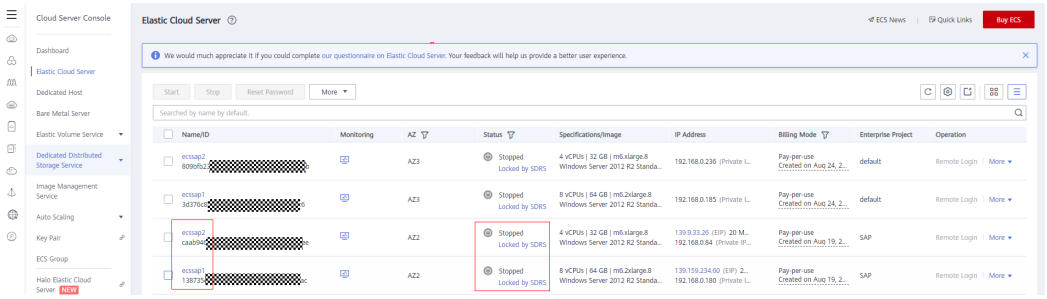
A planned failover changes the disaster recovery direction of a protection group. After the planned failover, data synchronization continues, but the DR direction is changed from the DR site to the production site. Perform planned failovers based on your planned outages to ensure no data loss. For example, if the production site (AZ 2) is going to encounter a power failure, you can perform a planned failover to switch the services in AZ 2 to the DR site (AZ 3). The planned failover will not affect data synchronization of the protection group.

SDRS will migrate NICs on the server during the planned failover. After the planned failover, the IP, EIP, and MAC addresses of the production site server will be migrated to the DR site server, so that the IP, EIP, and MAC addresses remain the same.

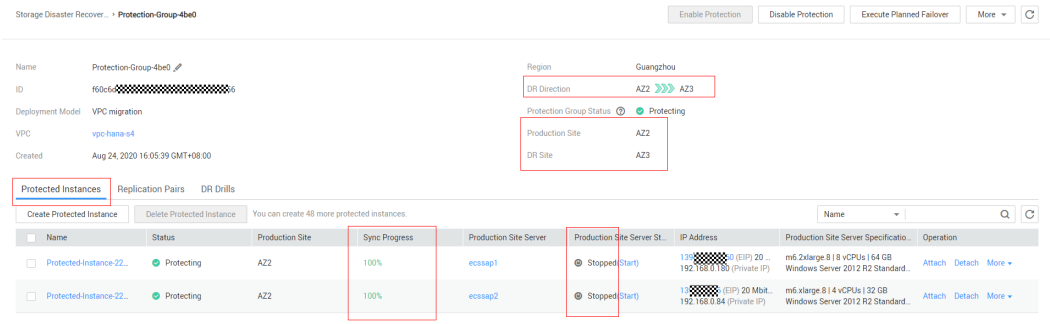
NOTE

- Ensure that all the servers in the protection group are stopped before the planned failover.
- During the planned failover, do not start the servers in the protection group. Otherwise, the planned failover may fail.
- Once a planned failover is complete, data synchronization will not stop, only the synchronization direction will reverse.
- After the planned failover is complete, the status of the protection group changes to **Protecting**. Switch to the protected instance details page and start the server at the production site.

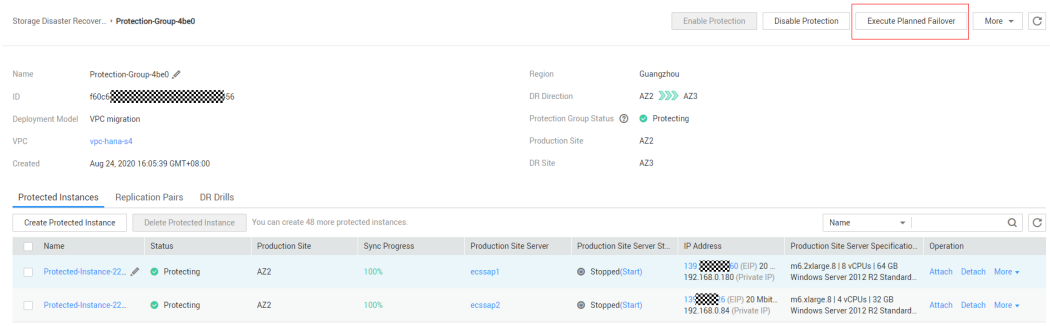
Step 1 Log in to the ECS management console and stop the target server at the production site.



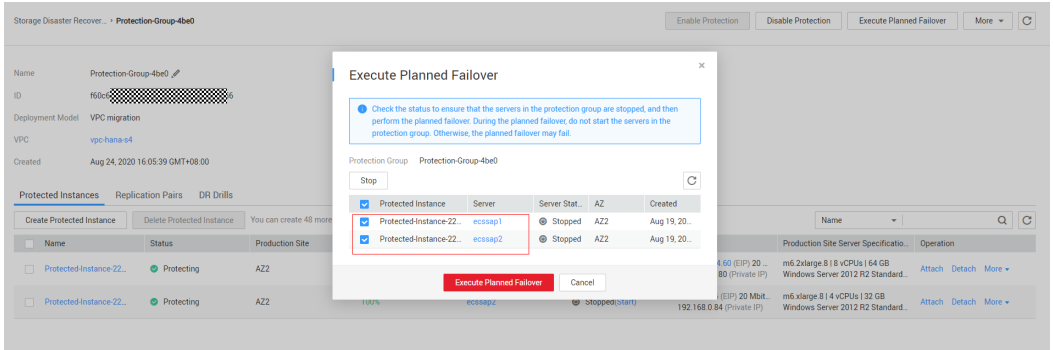
Step 2 Log in to the **Storage Disaster Recovery Service** page, click the protected group for which you want to perform a planned failover, and check the synchronization result and whether the server in the protected group is stopped.



Step 3 Click **Execute Planned Failover**.

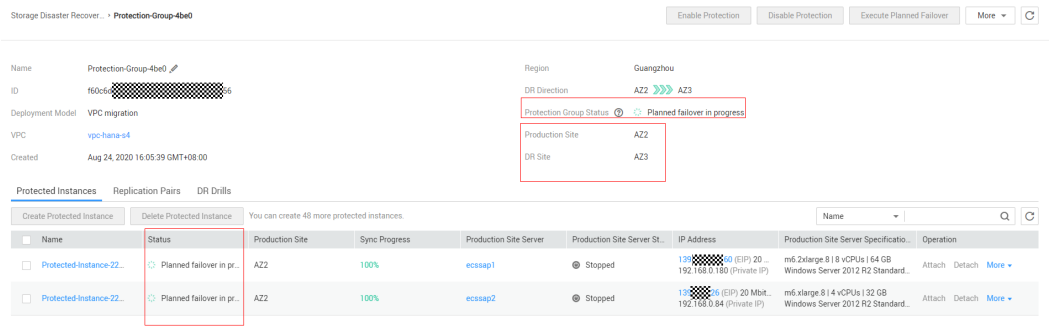


Step 4 Select the protected instance for which you want to perform a planned failover and click **Execute Planned Failover**.



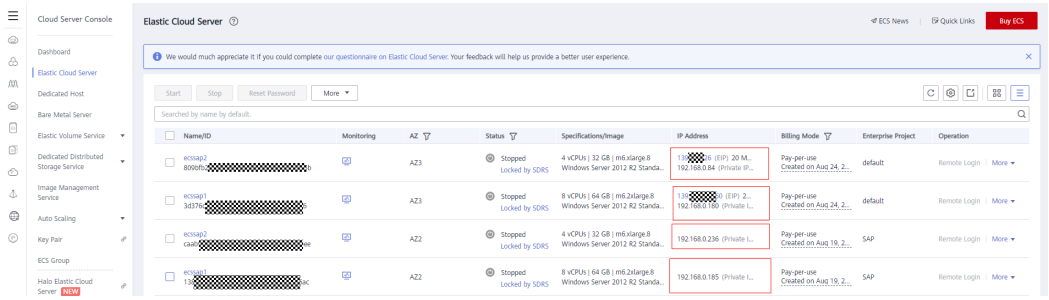
Step 5 Check the protection group status.

Step 6 Check whether the failover is complete. (The failover usually takes several minutes. The time required depends on the actual situation.)



After the failover, the previous production site becomes the new DR site, the previous DR site becomes the new production site, and the status of the protected group and protected instance changes from **Planned failover in progress** to **Protected**.

Step 7 Log in to the ECS management console and view server details at the new production site and DR site.

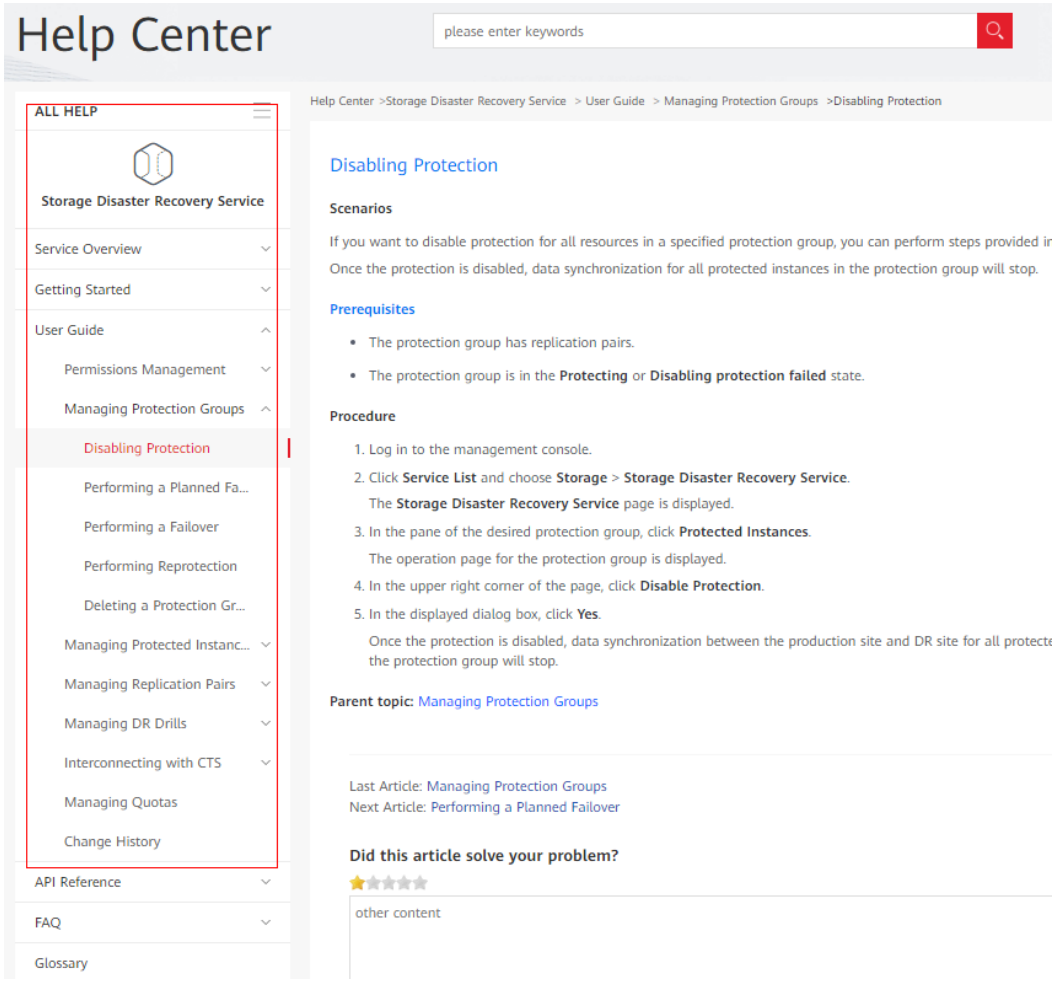


----End

Compare the ECS details before and after the failover. It is found that the private and public IP addresses of the production site server before the failover are the same as the private and public IP address of the DR site server after the failover. In this case, manually start the new DR server. (Note that the server at the DR site cannot be manually started. Only the server at the production site can be manually started.)

10.3.6 Performing Other Operations on SDRS

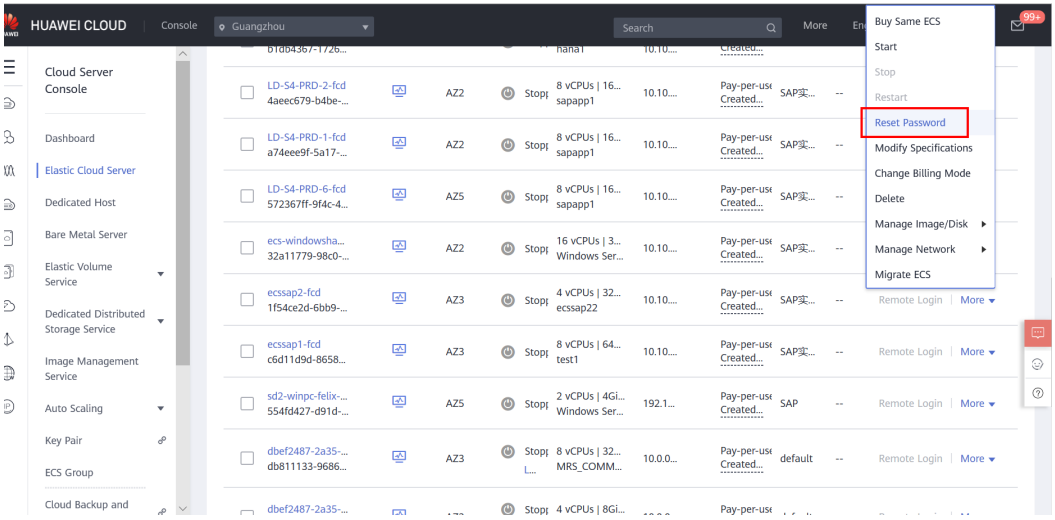
For details, see **Storage Disaster Recovery Service User Guide**.



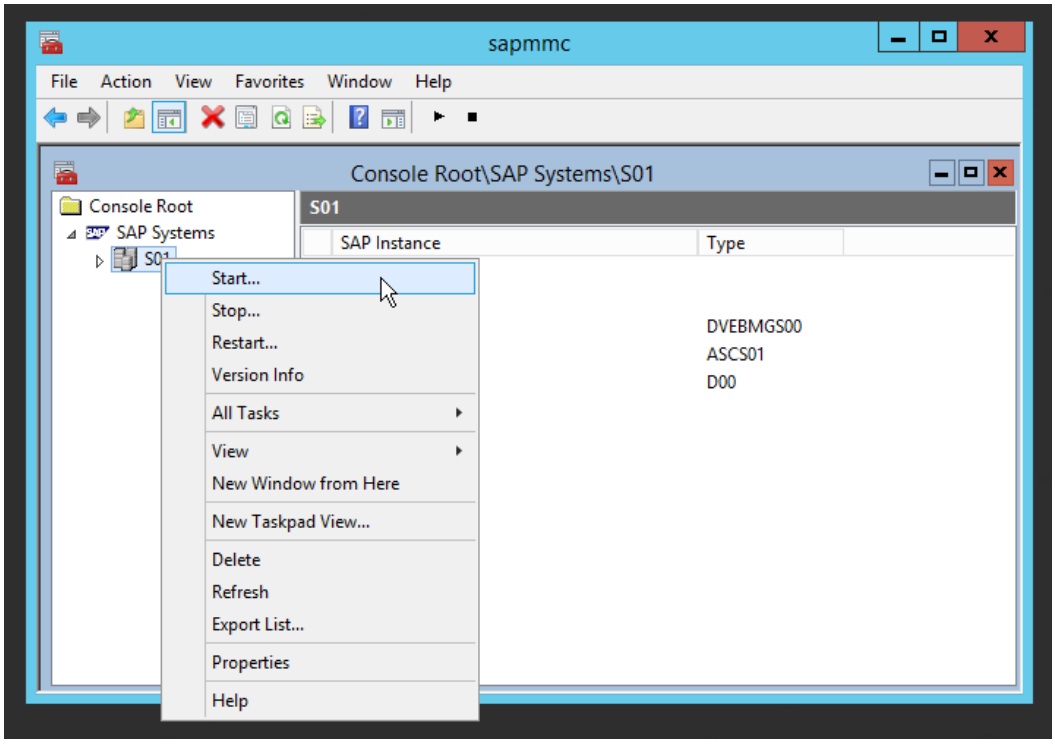
10.3.7 Checking SAP Applications

After the failover, the production site and DR site are switched. Log in to the servers at the new production site to check whether the applications can start properly and whether the SAP hardware key is changed.

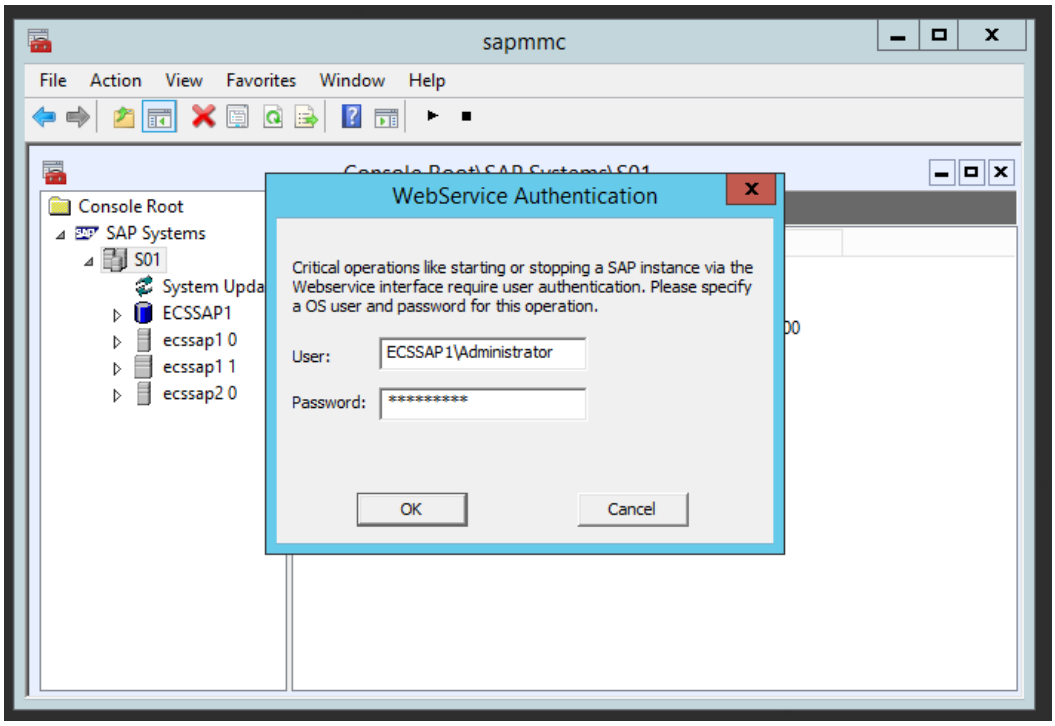
Step 1 After the failover, the servers at the new production site are still in the stopped state and you need to manually start them. If the startup passwords of the servers at the new production site are different from those at the current DR site, manually change the passwords of the servers at the new production site on the ECS console, restart the ECSs, and the new passwords will take effect.



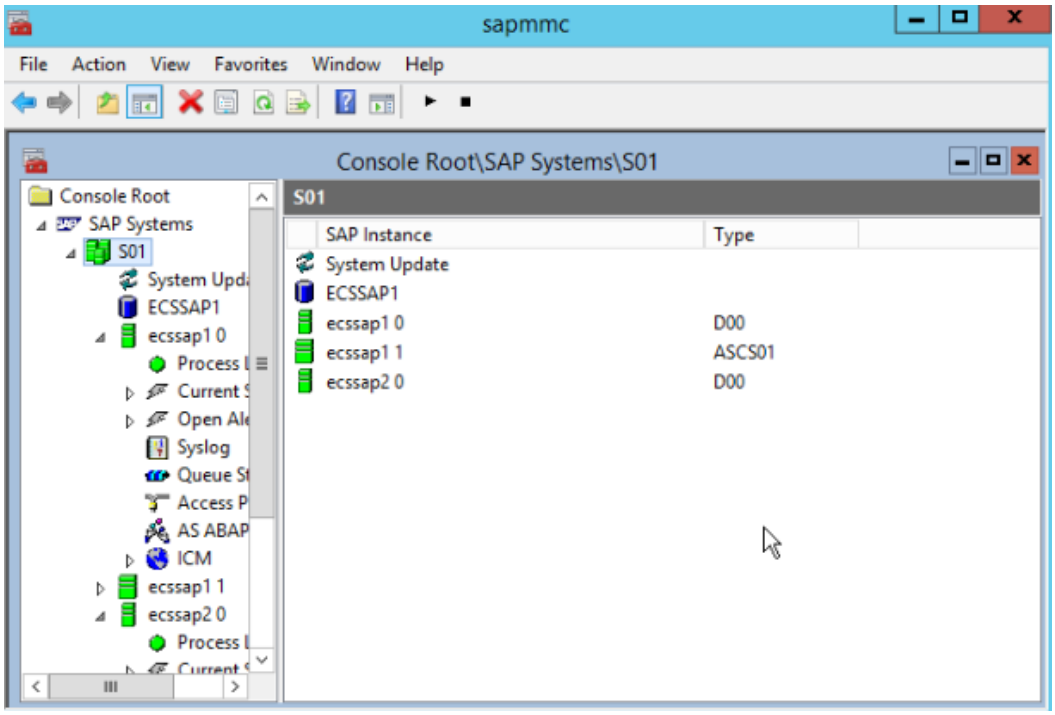
Step 2 Log in to the **ecssap1** server at the new production site, click **SAP Management Console** on the desktop, right-click **S01**, and choose **Start** from the shortcut menu.



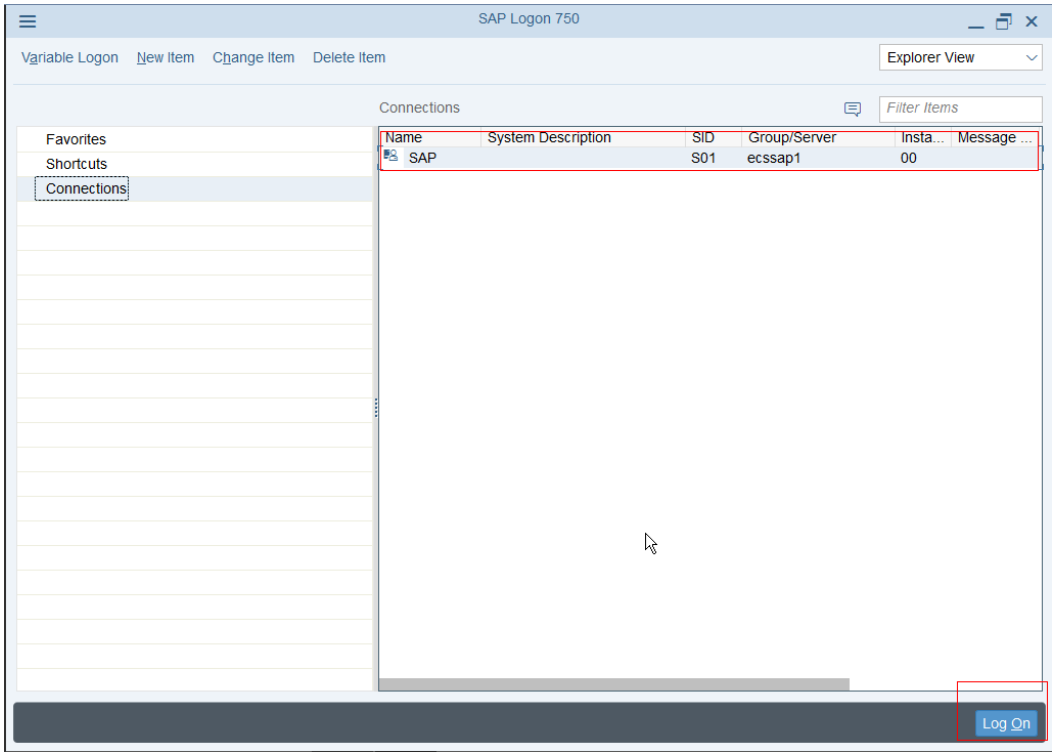
Step 3 Enter the password to start the SAP application and click **OK**.



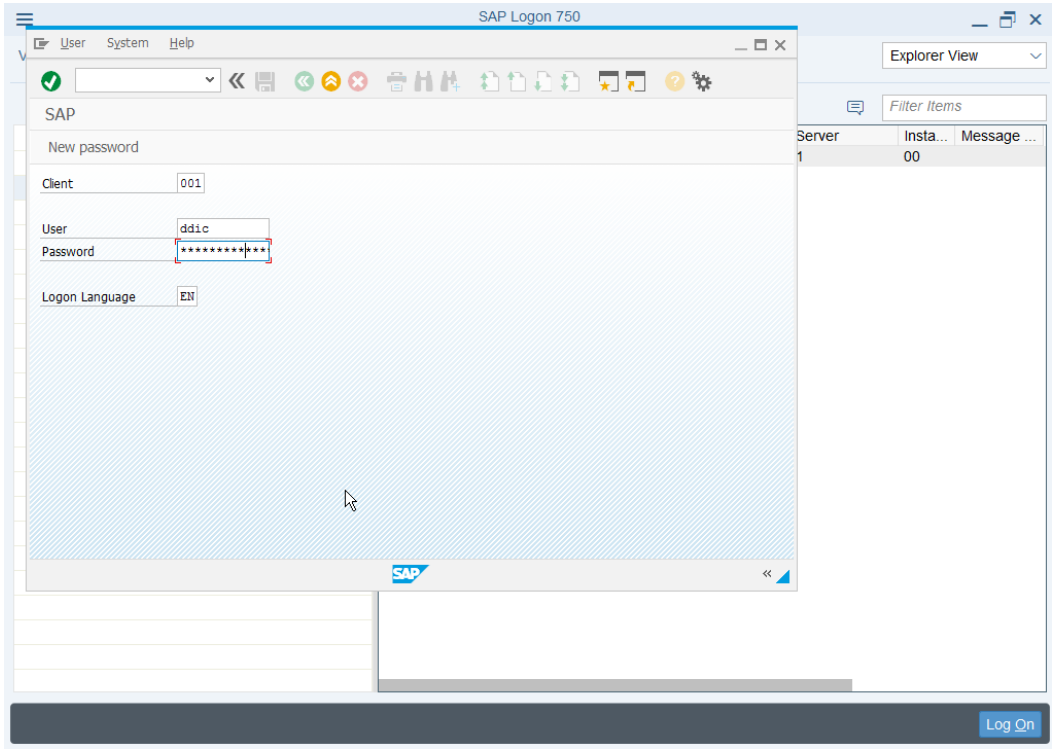
Step 4 Click the refresh button to view the SAP startup information.



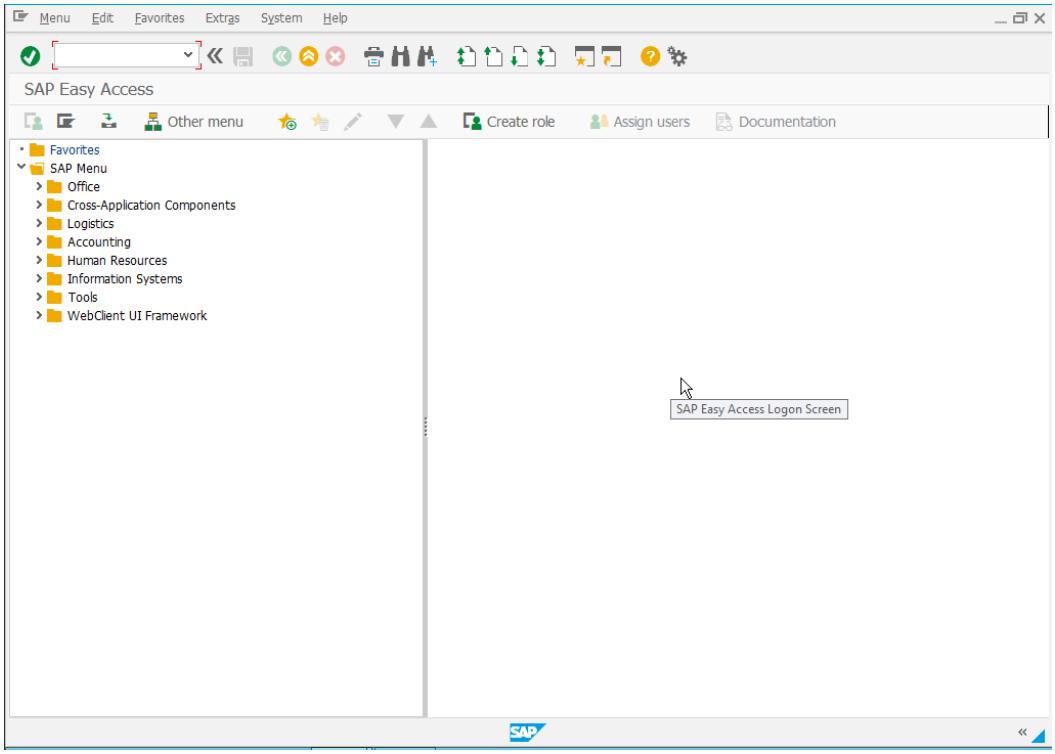
Step 5 Click **SAP Logon** to run the SAP GUI.



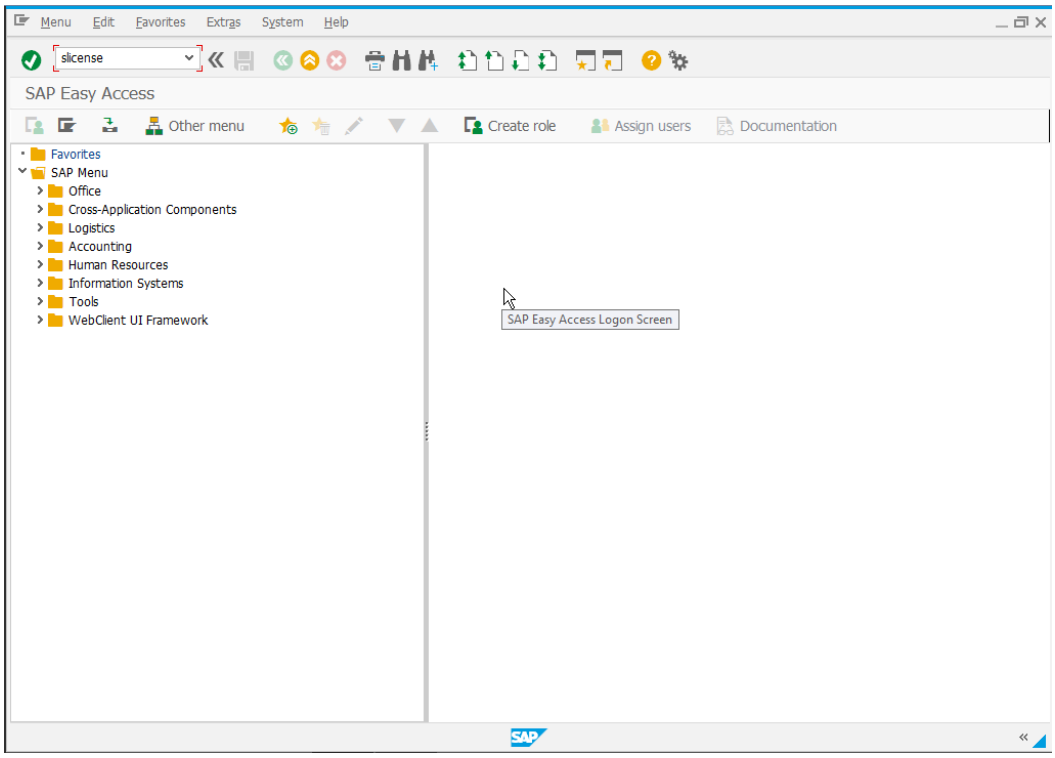
Step 6 Enter username **ddic** and the password, and then press **Enter**.



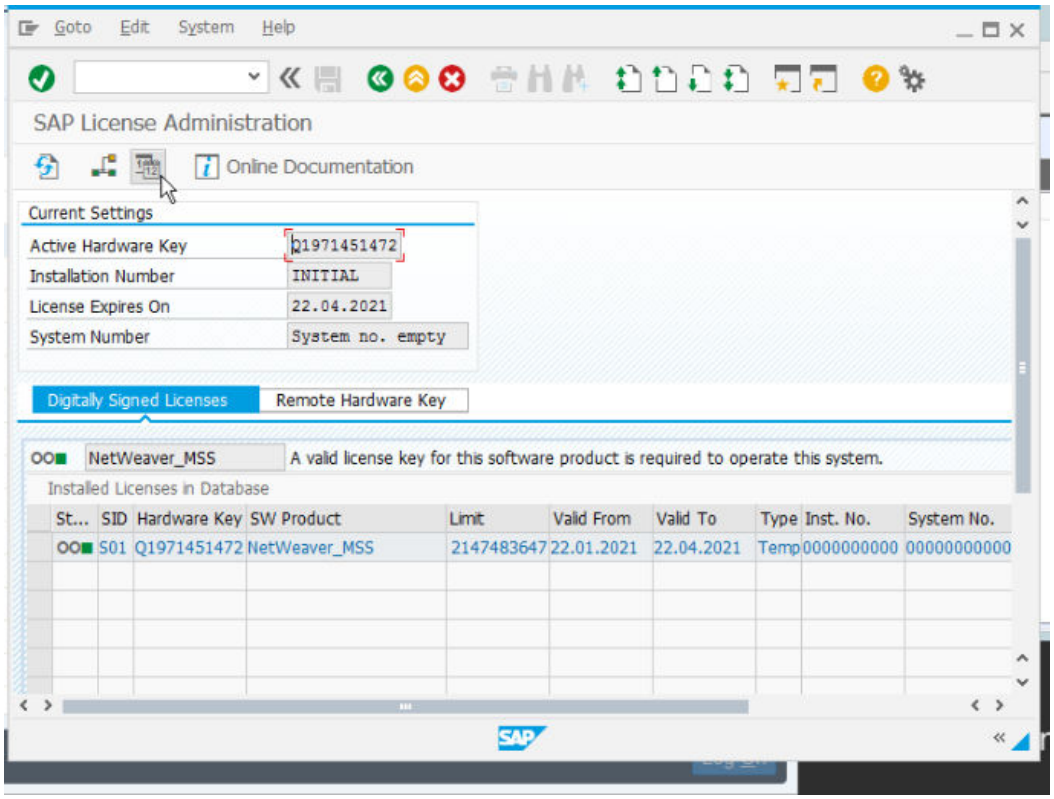
Step 7 Check whether the SAP GUI login is successful, and whether the SAP application is running smoothly.



Step 8 Enter **slicense** and press **Enter** to view the SAP license.



Step 9 Compare the SAP hardware key before and after the DR failover to ensure that the SAP hardware key keeps unchanged before and after the failover. That is, the SAP license keeps unchanged.



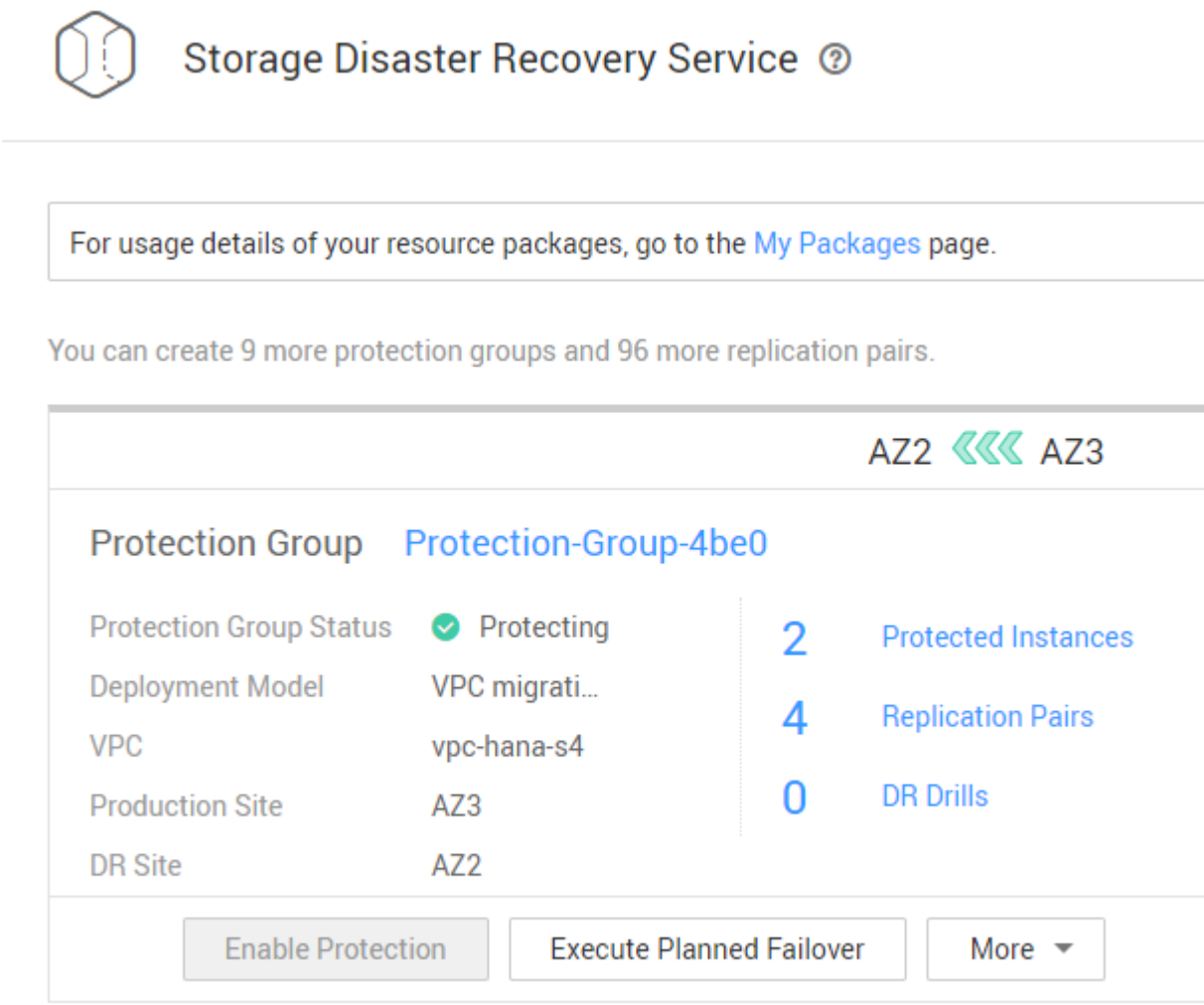
----End

10.4 SDRS Performance Test

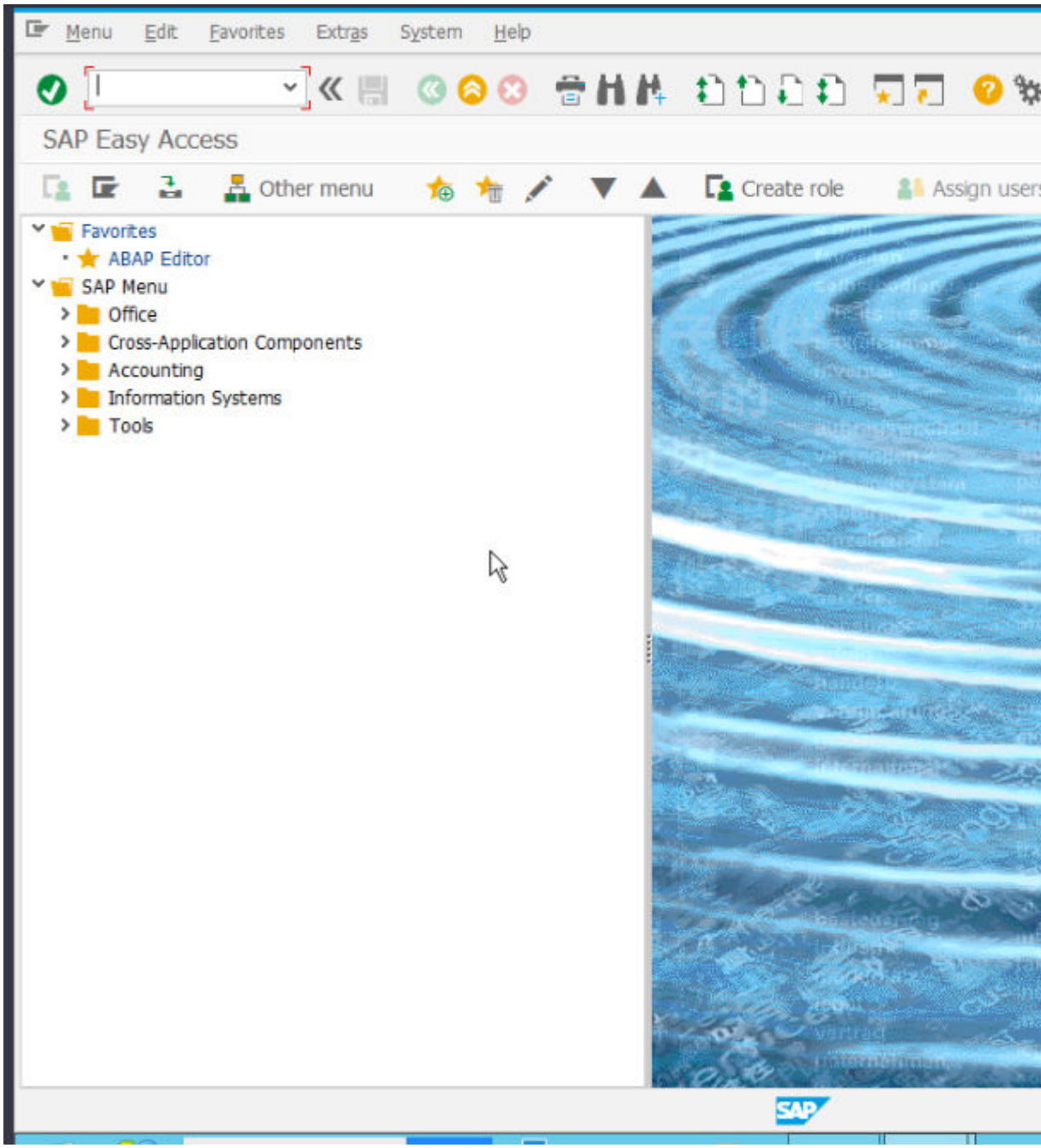
10.4.1 Testing Performance of SAP Applications

This section describes how to test the SDRS performance by comparing the time required for performing the Client Copy operations before and after SDRS protection is enabled.

Step 1 Click **Enable Protection** on the **Storage Disaster Recovery Service** page.

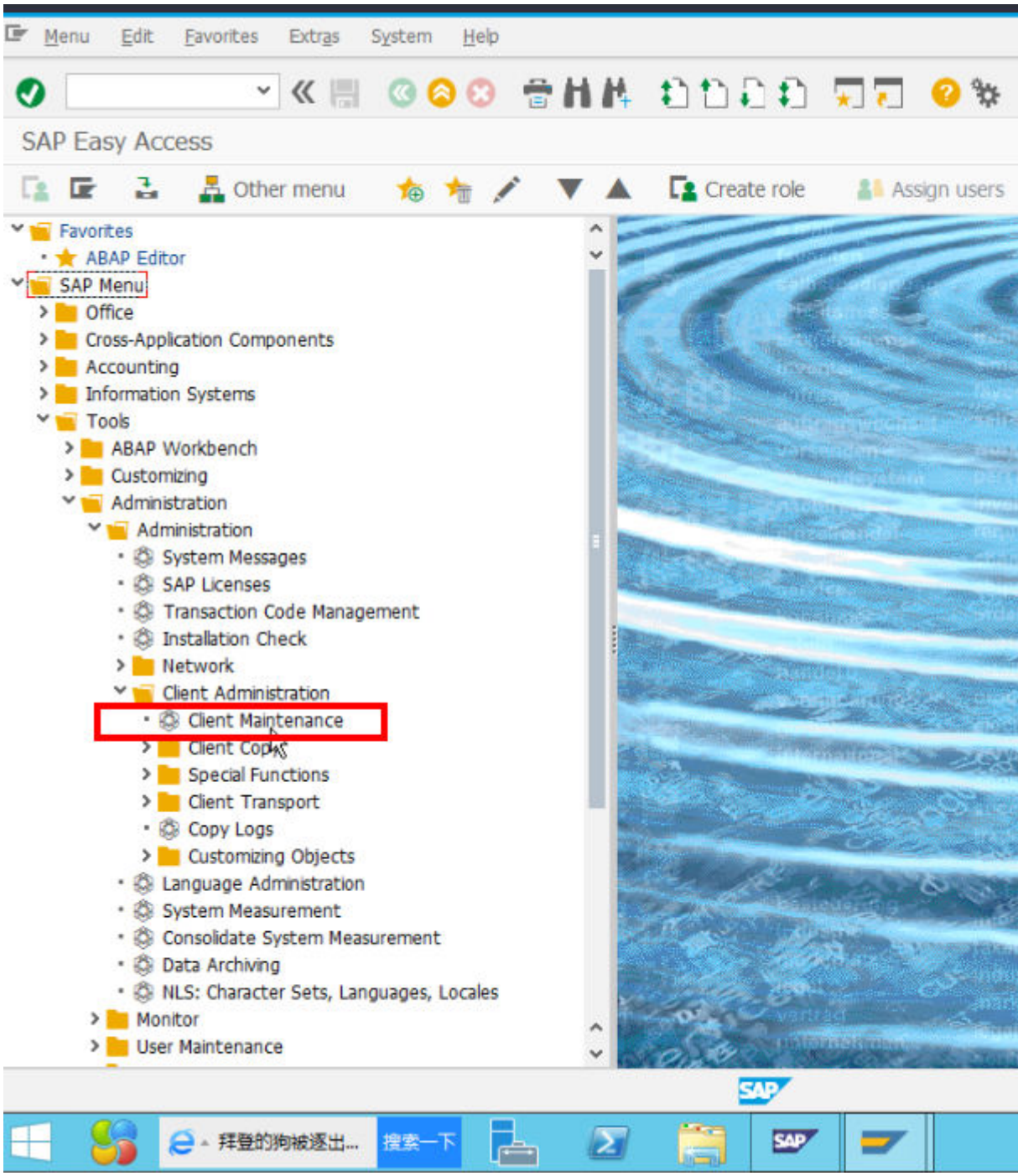


Step 2 Log in to the SAP system as user **ddic**. For details, see **Checking SAP Applications**.

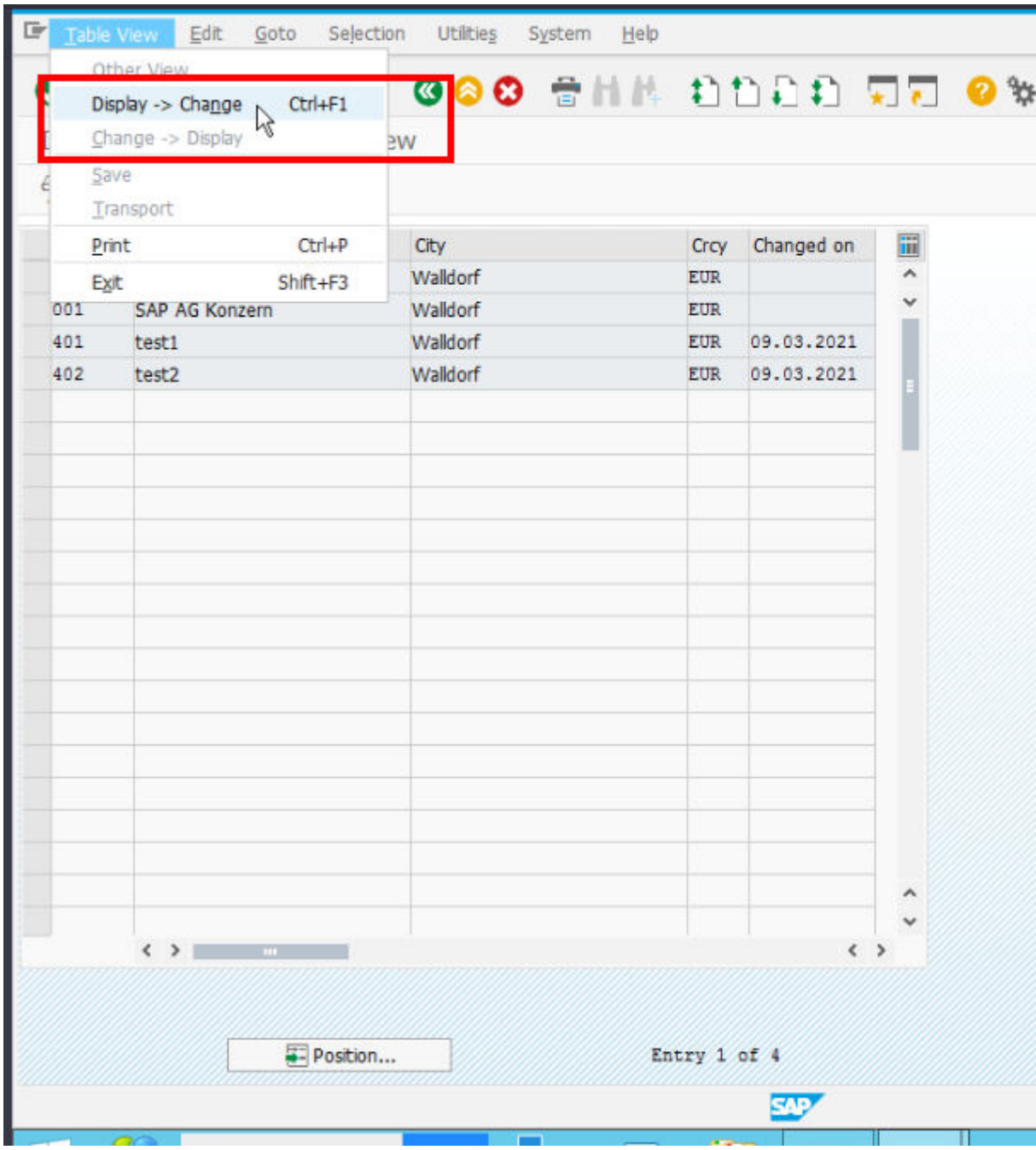


Step 3 Create a client.

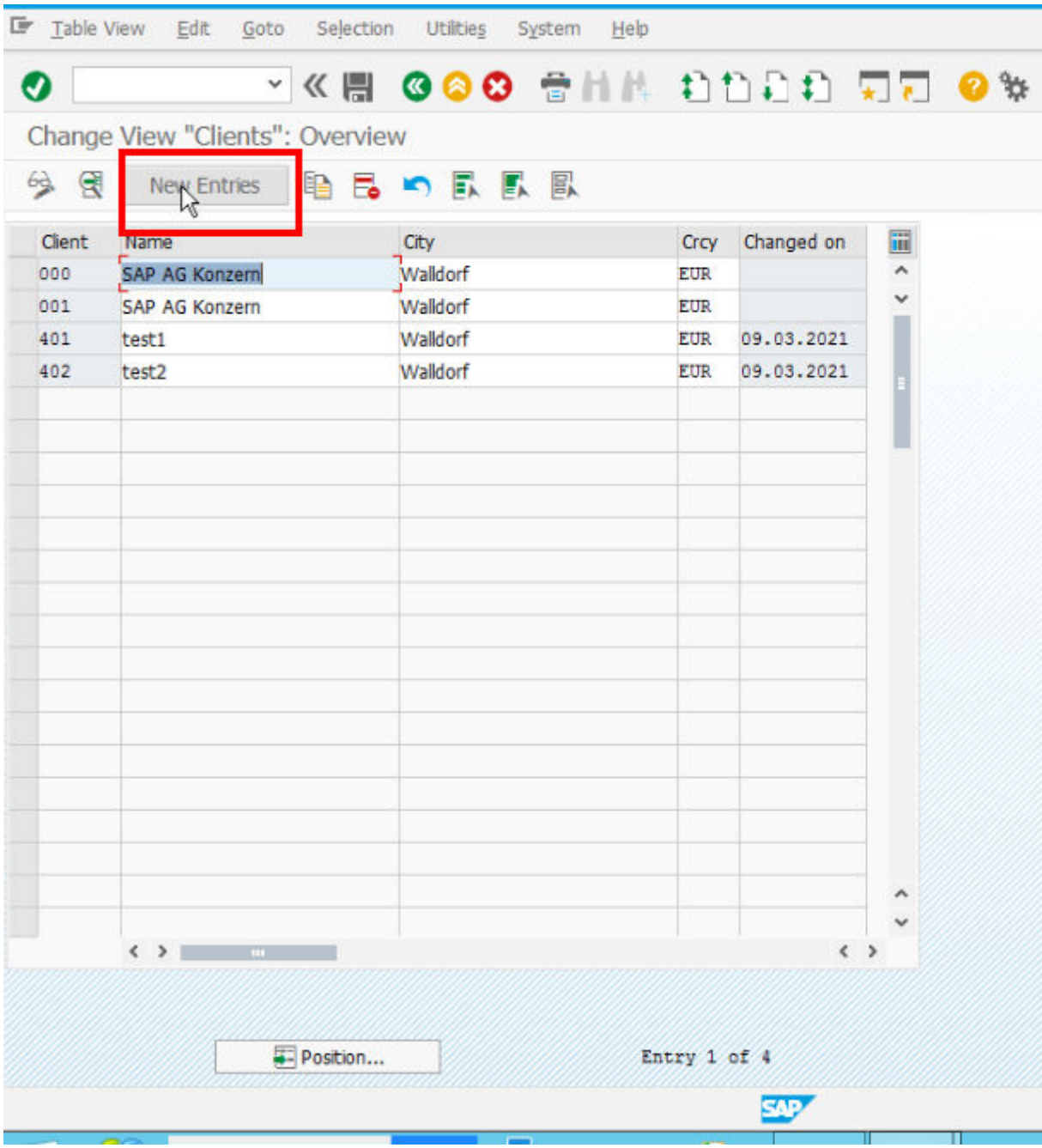
Choose **SAP Menu** > **Tools** > **Administration** > **Administration** > **Client Administration** > **Client Maintenance**.



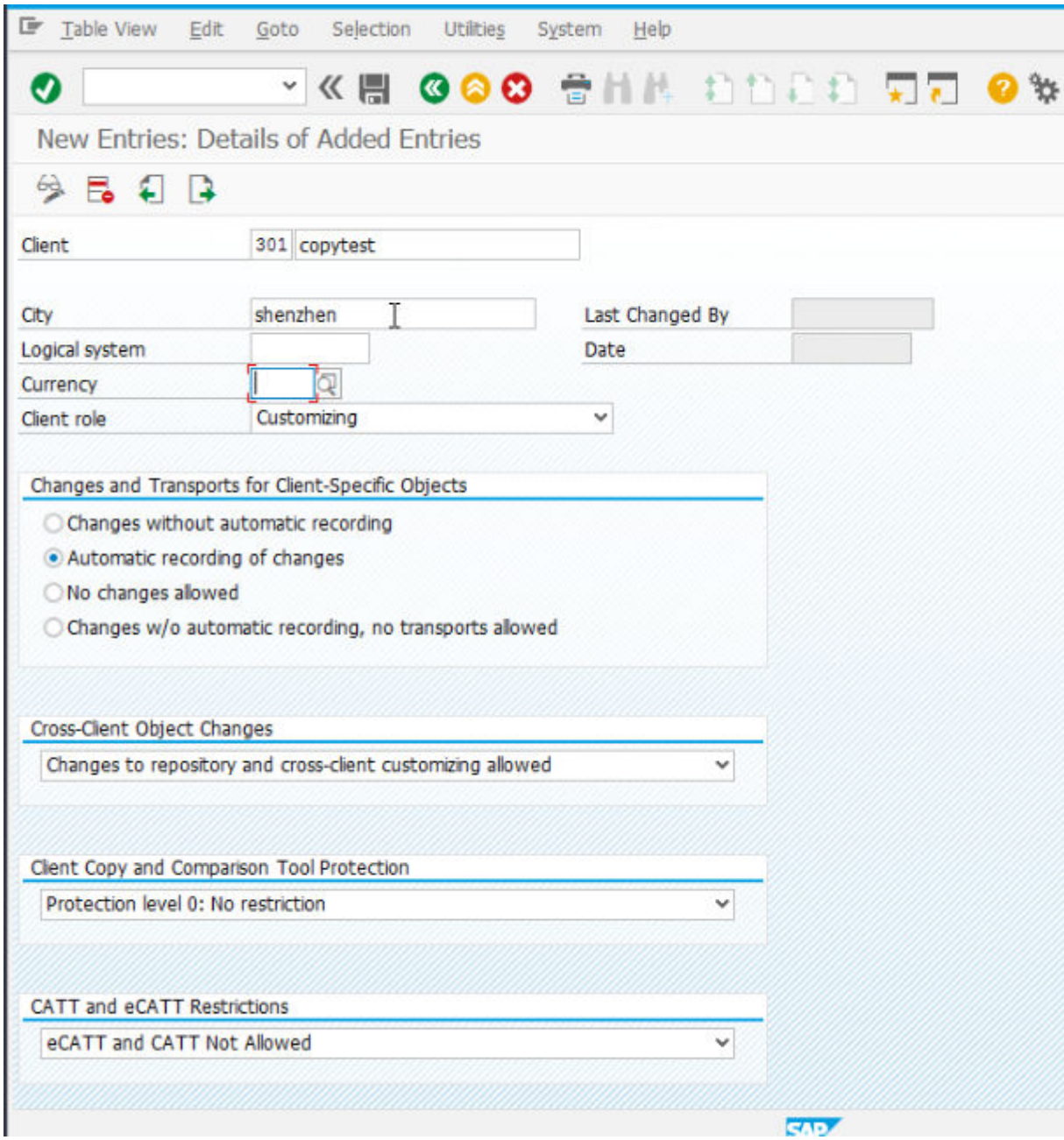
Step 4 In the dialog box that is displayed, choose **Table View** > **Display-Change**.



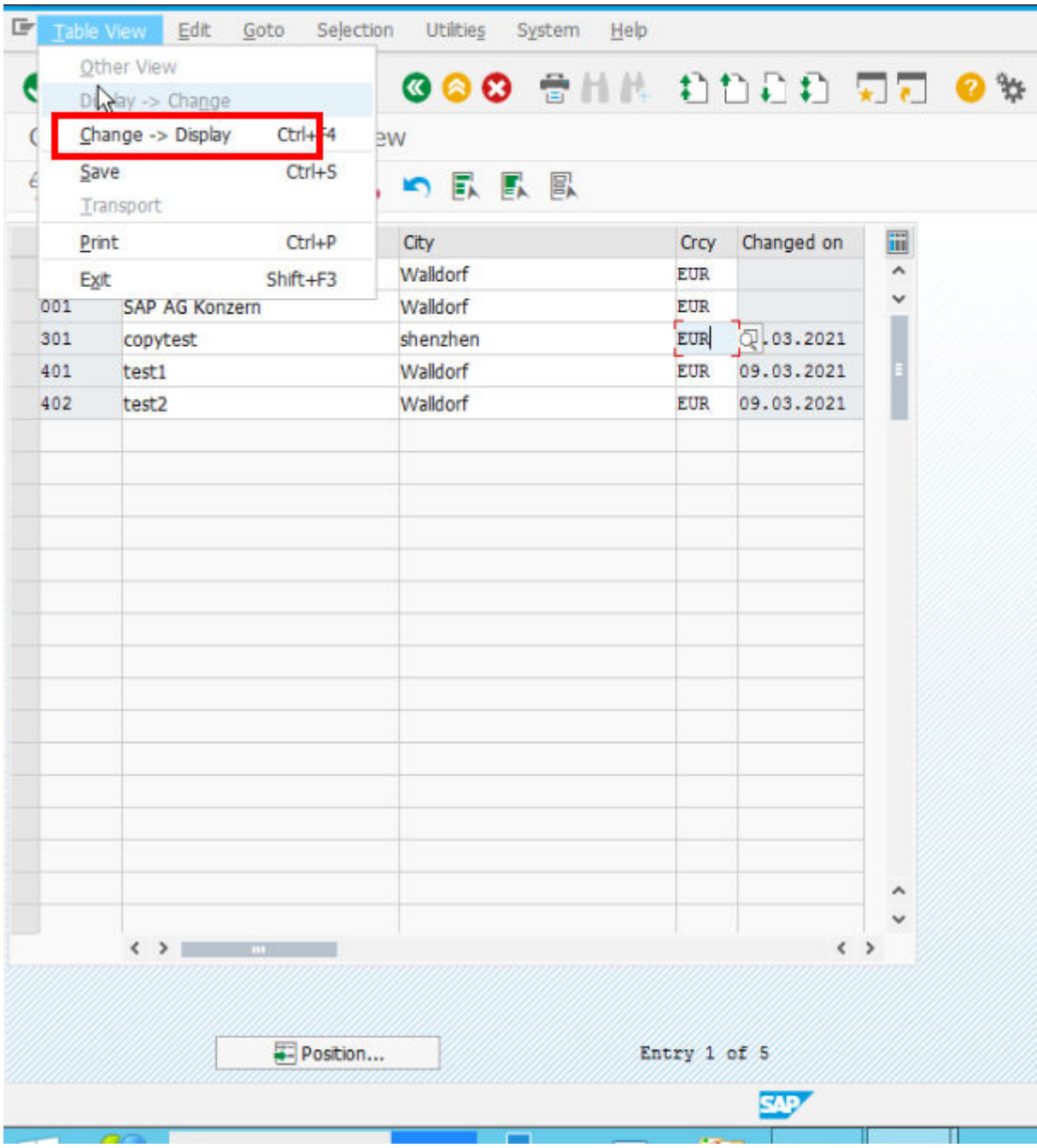
Step 5 Click **New Entries**.



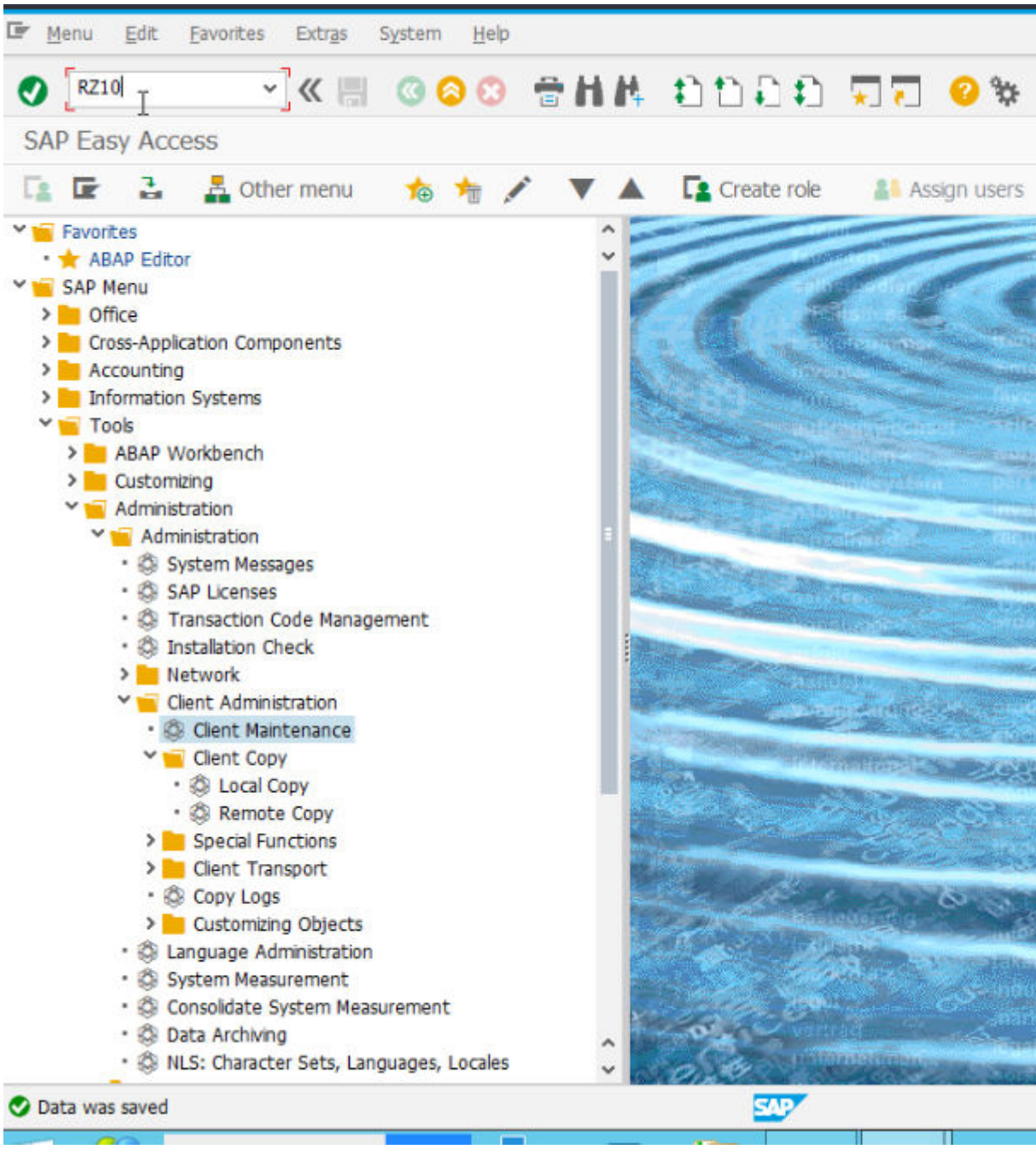
Step 6 Enter the client parameters, save the settings, and exit.



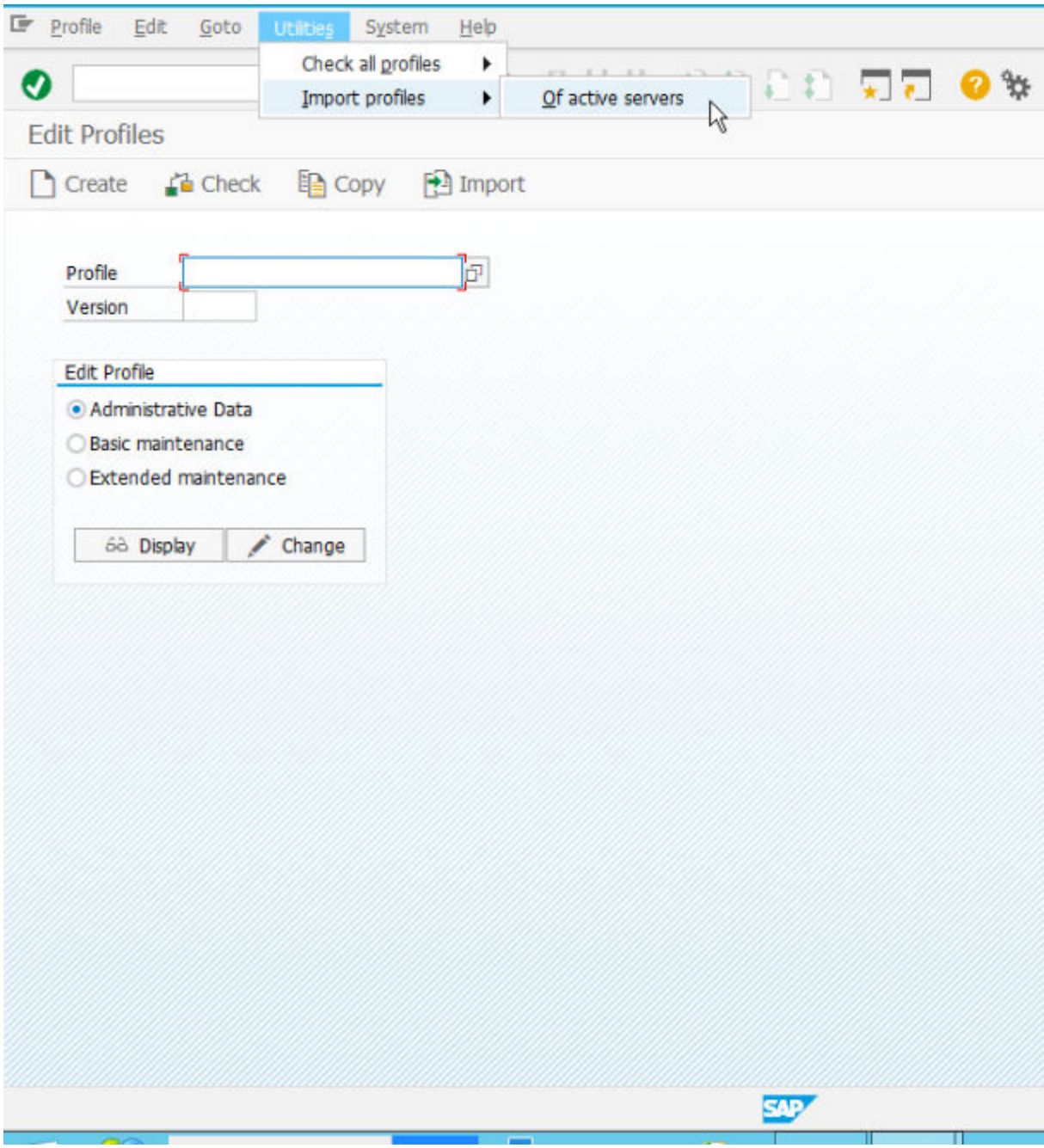
Step 7 Choose **Table View** > **Change-Display** to save the settings.

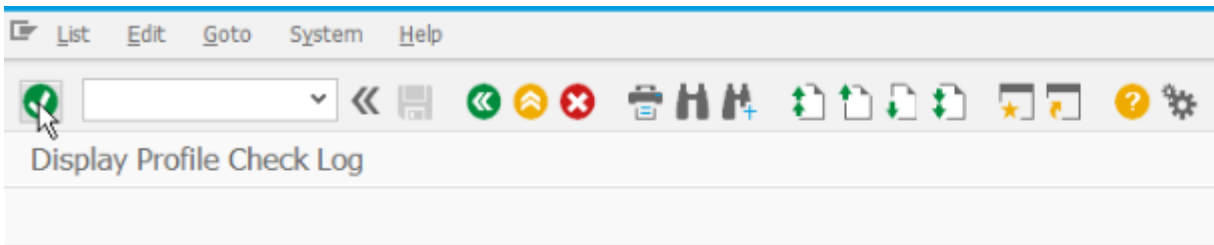


Step 8 Assign the login permission to the new client, return to the home page, enter **RZ10** in the search box, and press **Enter**.



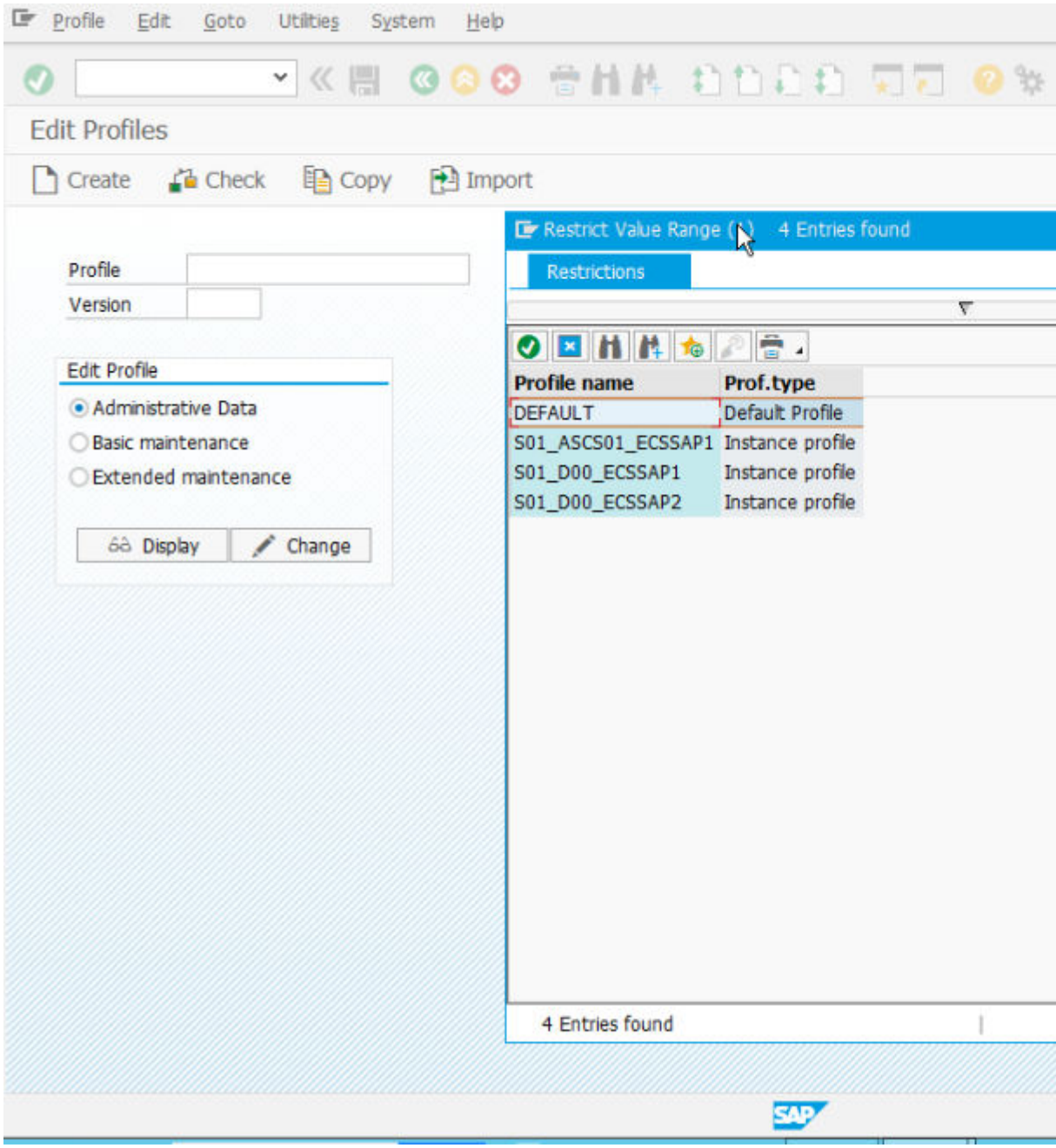
Step 9 The initial profile cannot be selected. In the dialog box that is displayed, choose **Utilities** > **Import profiles** > **Of active servers**.



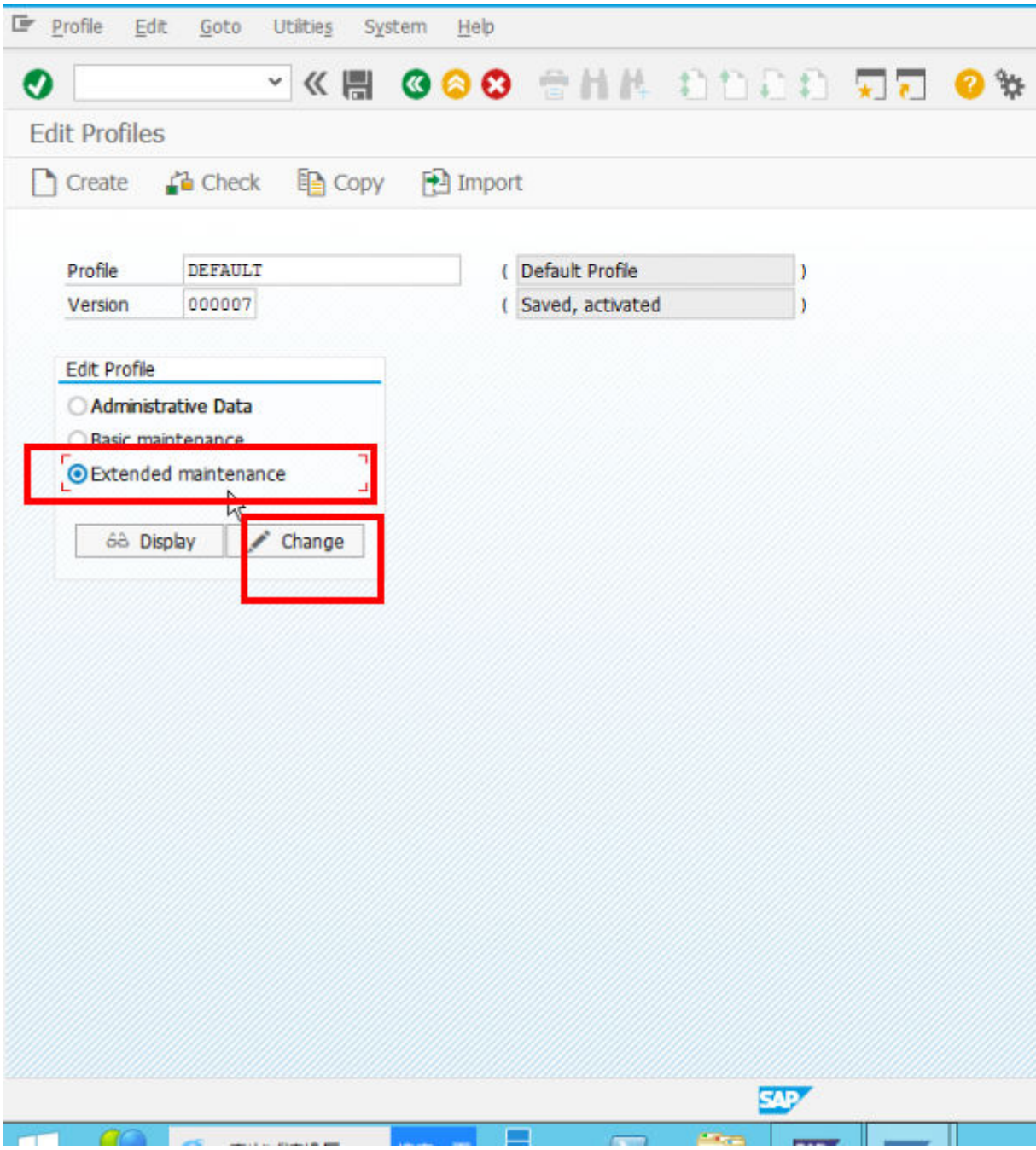



```
Import the start and instance profiles of all active servers

The following default profile is imported:

ecssap1_S01_00:\\ecssap1\sapmnt\S01\SYS\profile\DEFAULT.PFL

The following instance profiles are imported:

ecssap2_S01_00:\\ecssap1\sapmnt\S01\SYS\profile\S01_D00_ecssap2
ecssap1_S01_00:\\ecssap1\sapmnt\S01\SYS\profile\S01_D00_ecssap1

Log for the import of profiles

Instance profile \\ecssap1\sapmnt\S01\SYS\profile\S01_D00_ecssap2
```

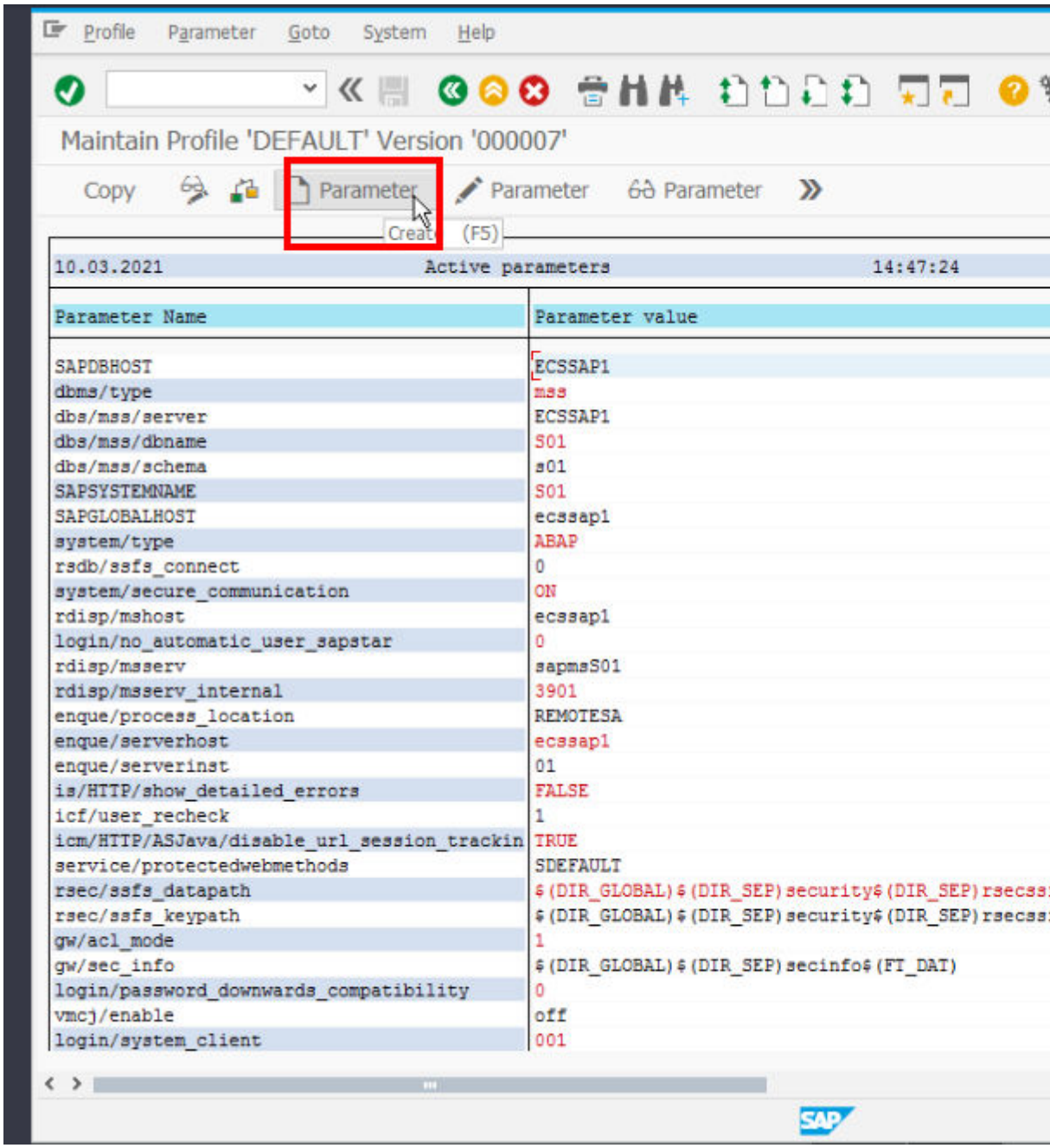

Step 10 Select **DEFAULT** for **Profile name** and **Default Profile** for **Prof.type**.



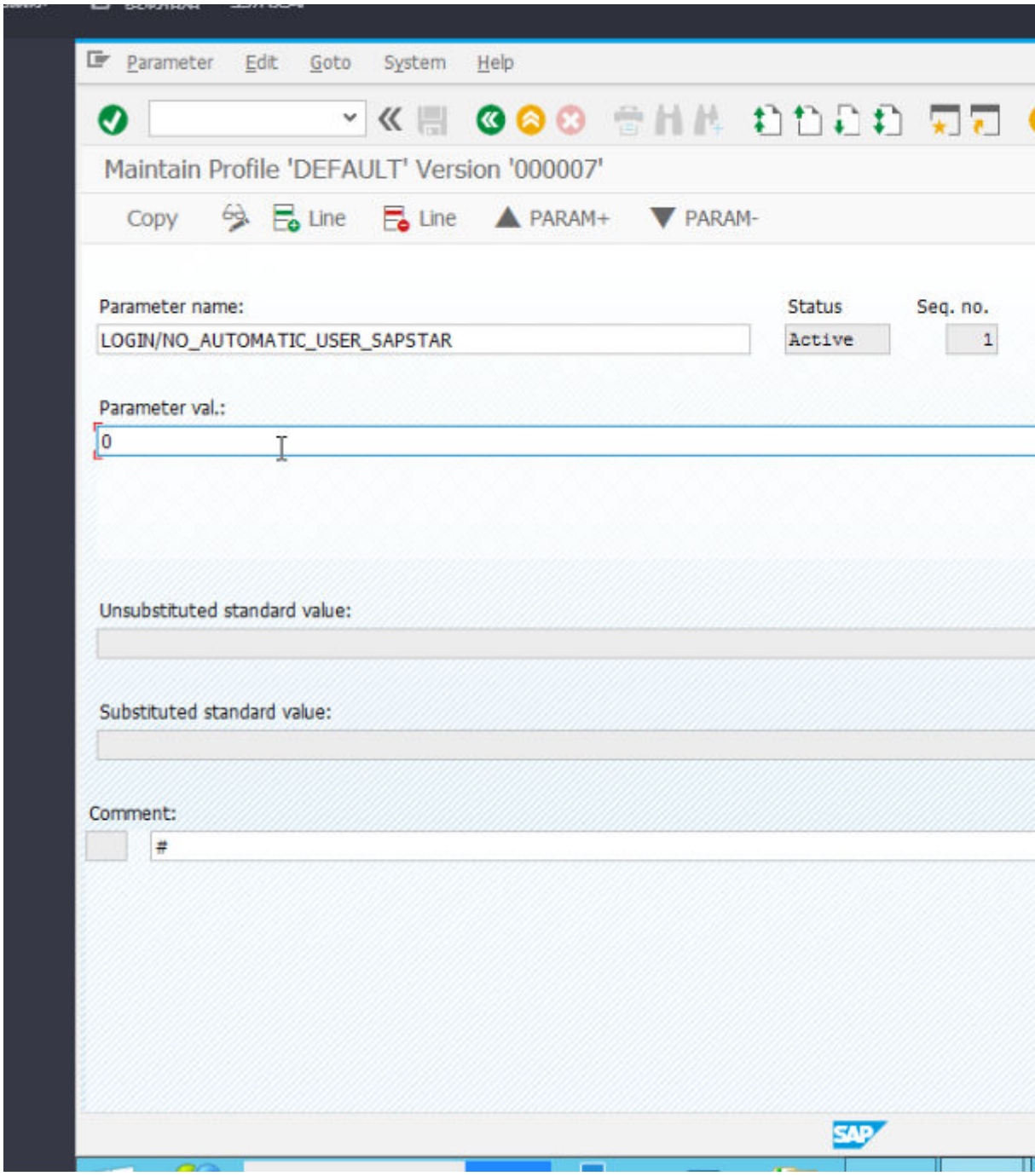
Step 11 Select **Extended maintenance** and click **Change**.



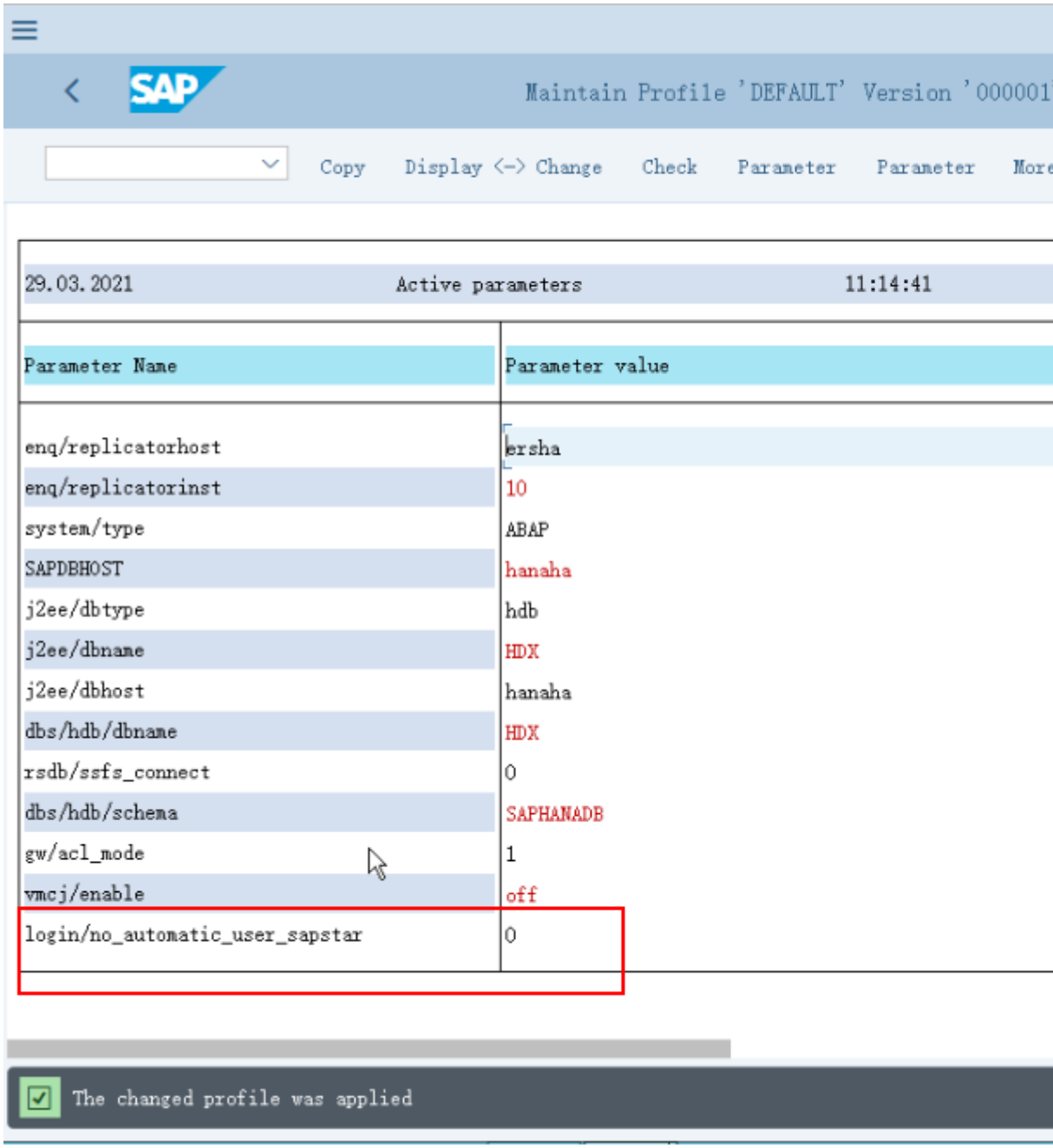
Step 12 Click **Parameter**.



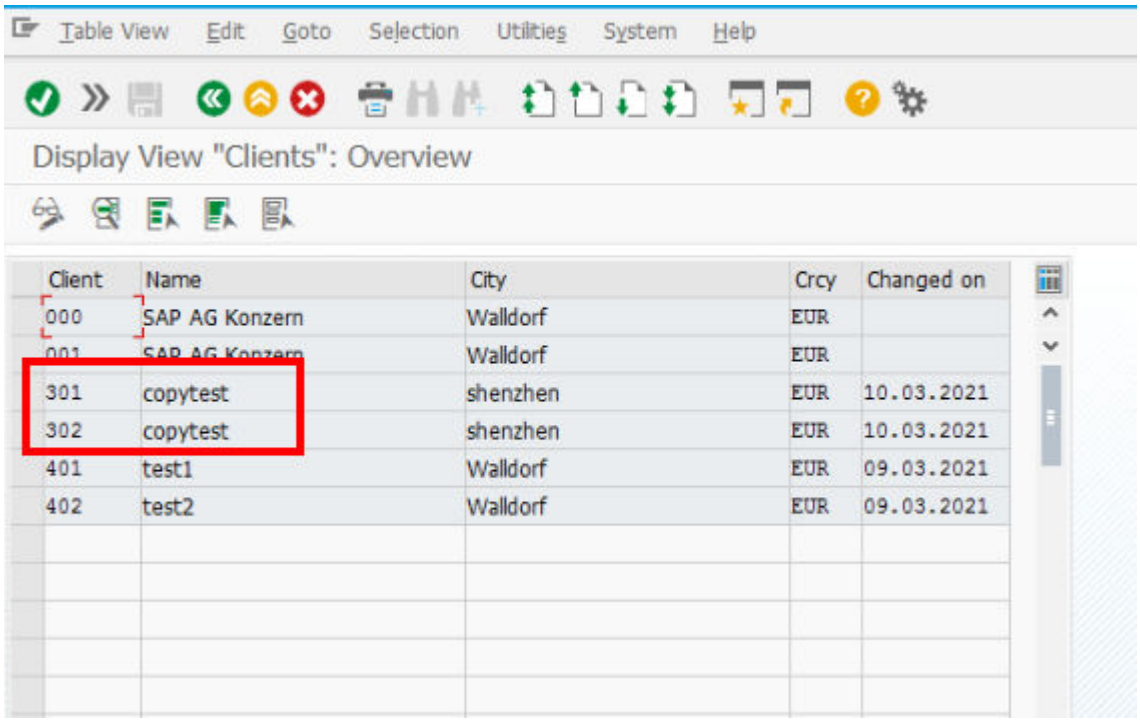
Step 13 Enter the parameter name **LOGIN/NO_AUTOMATIC_USER_SAPSTART**, set it to **0**, and click **Copy** to save the setting and exit.



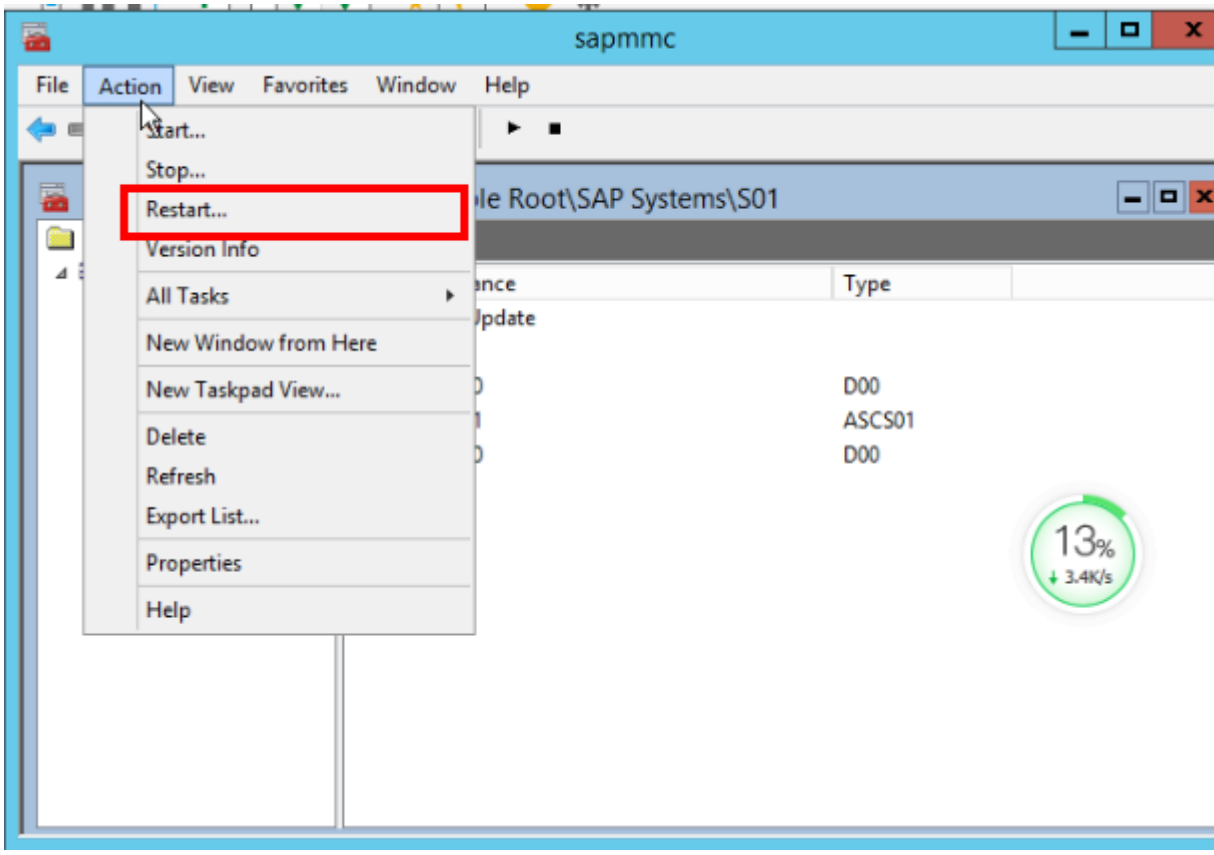
Step 14 Save the settings and exit.



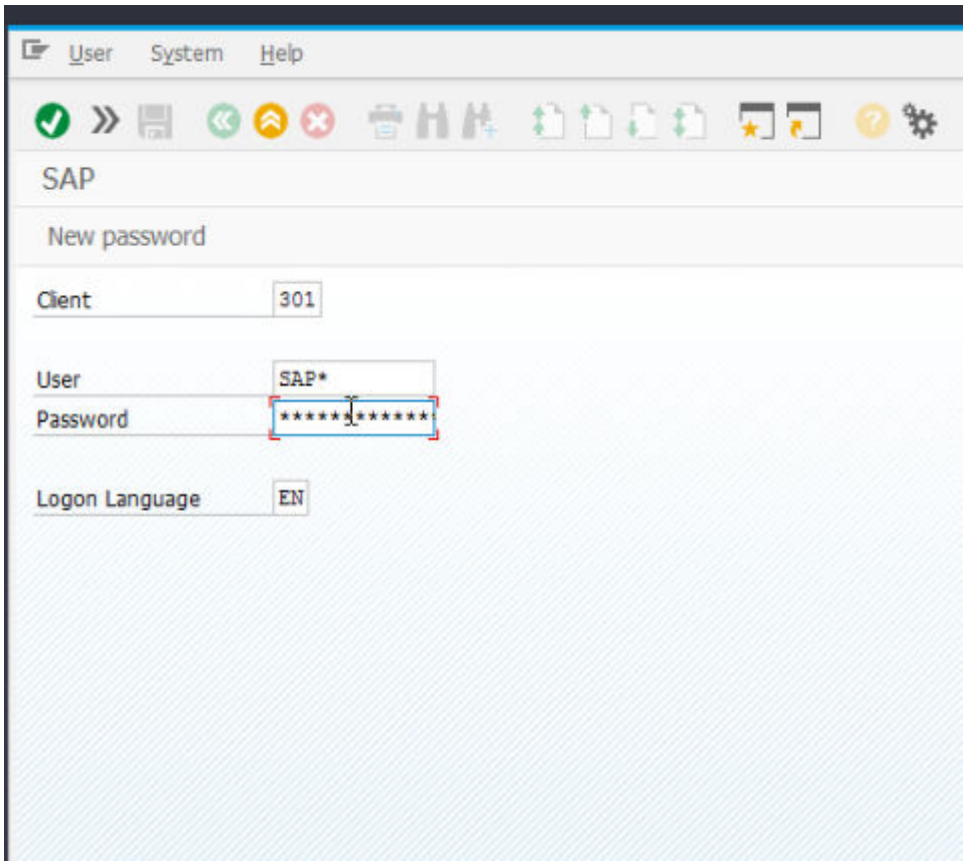
Step 15 Repeat the preceding steps to create the second client.

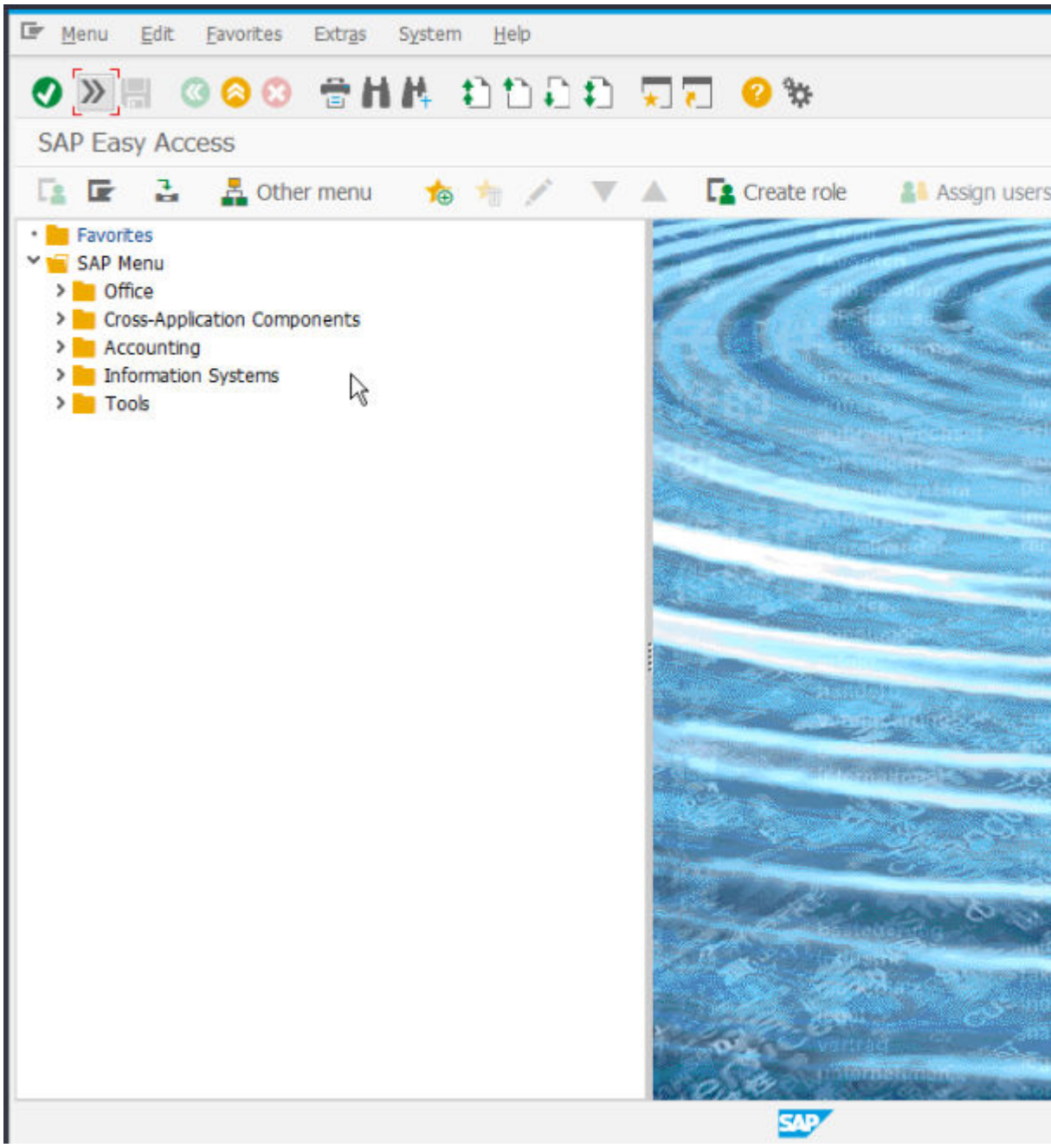


Step 16 Restart SAP.

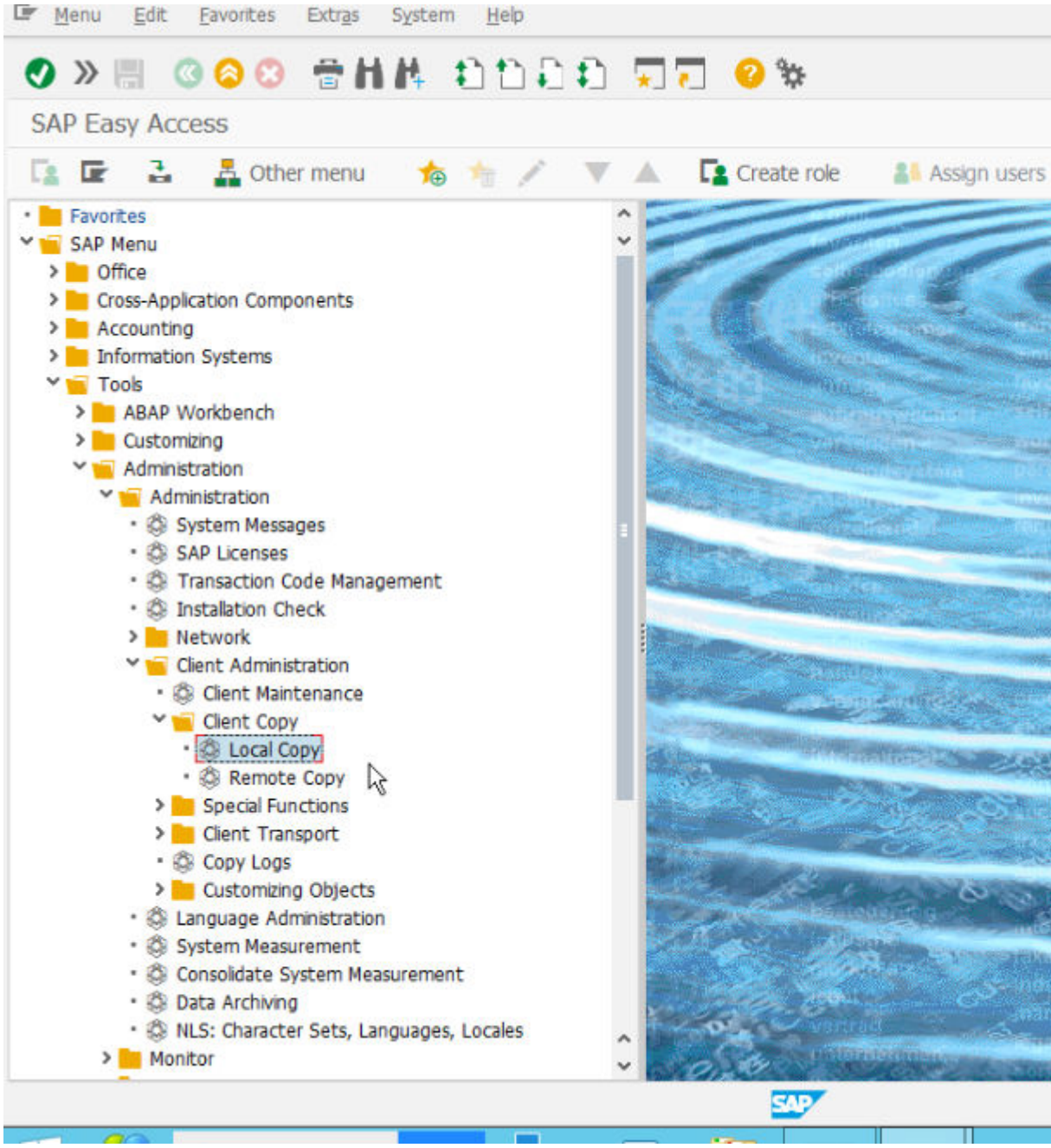


Step 17 Log in to the SAP GUI using the created client. The username is **SAP*** and the password is **pass**.

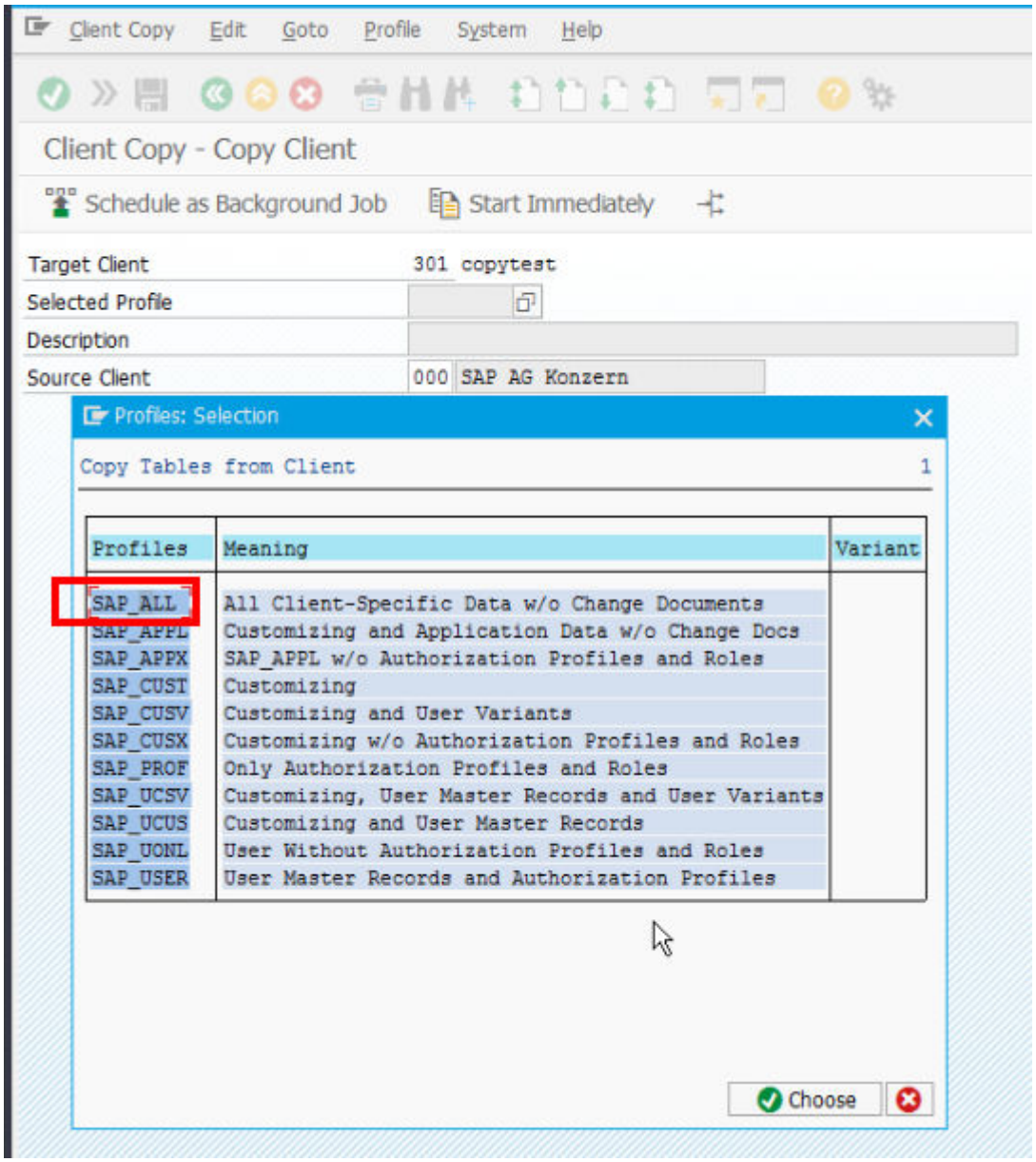


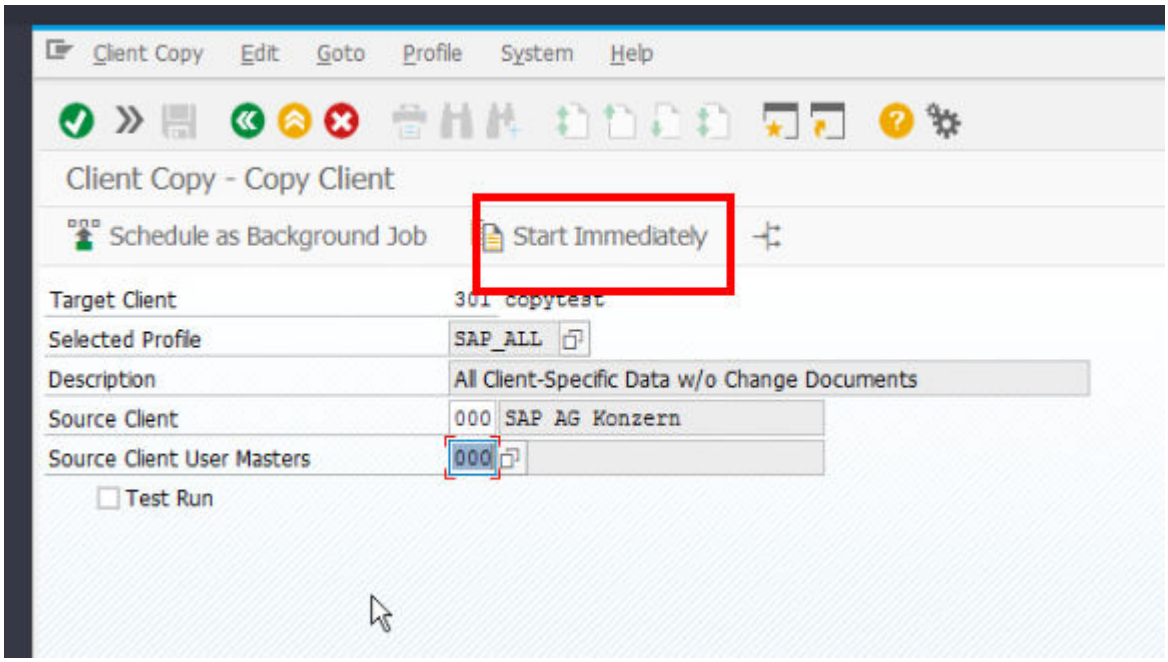


Step 18 Choose **SAP Menu** > **Tools** > **Administration** > **Administration** > **Client Administration** > **Client Copy** > **Local Copy**.

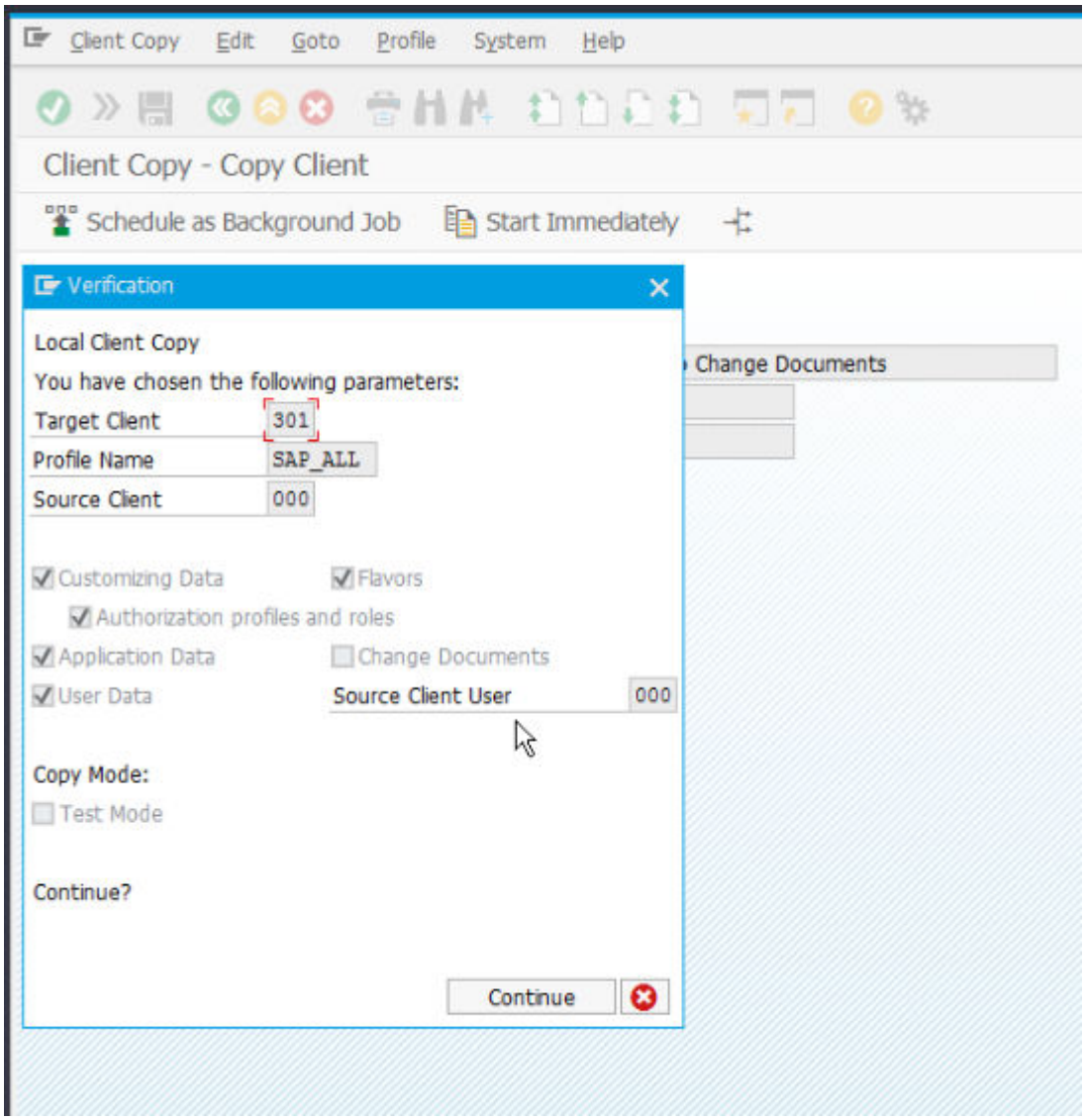


Step 19 Enter **000** for **Source Client**, select **SAP_ALL** under **Profiles**, and click **Start Immediately**.

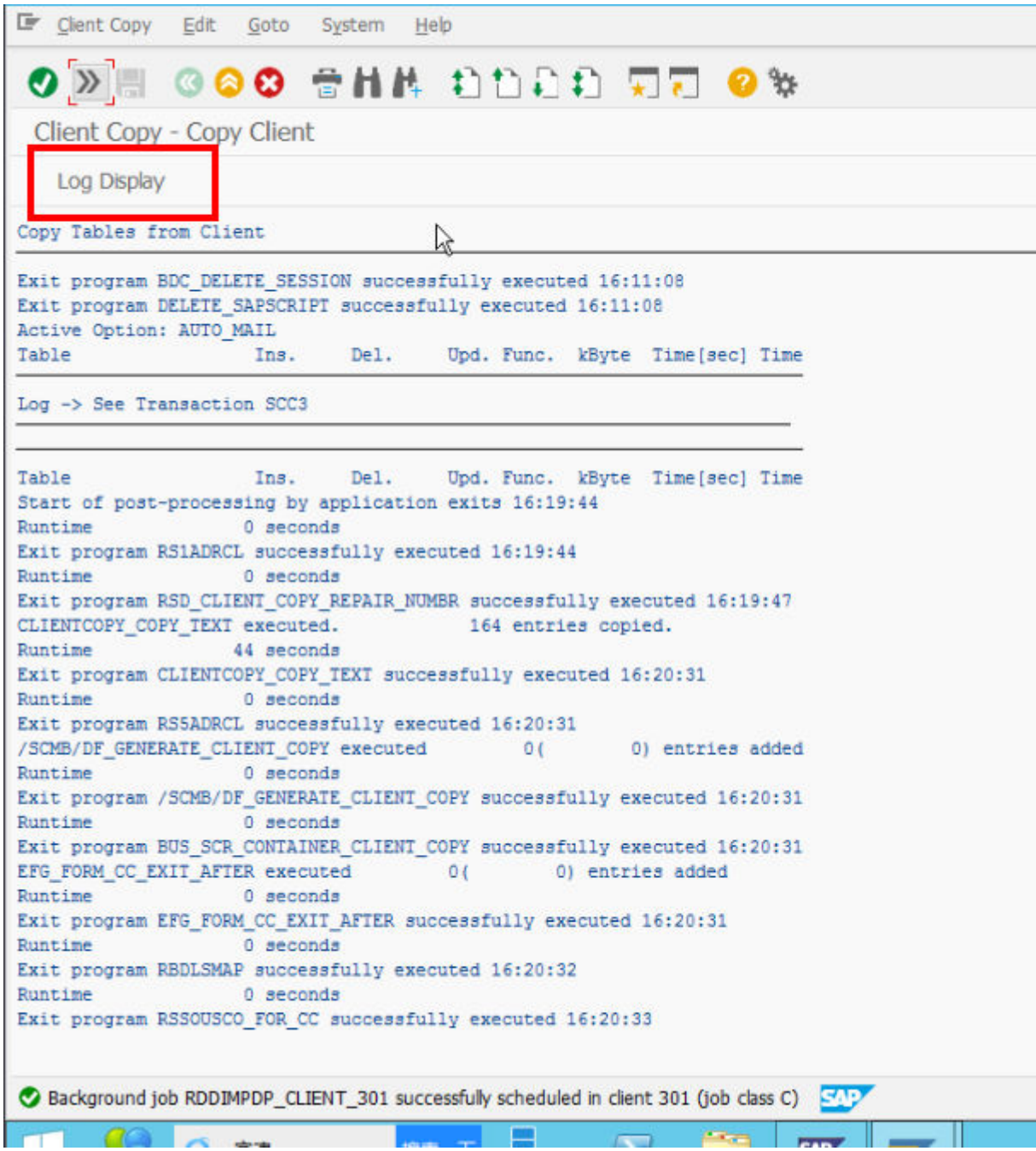




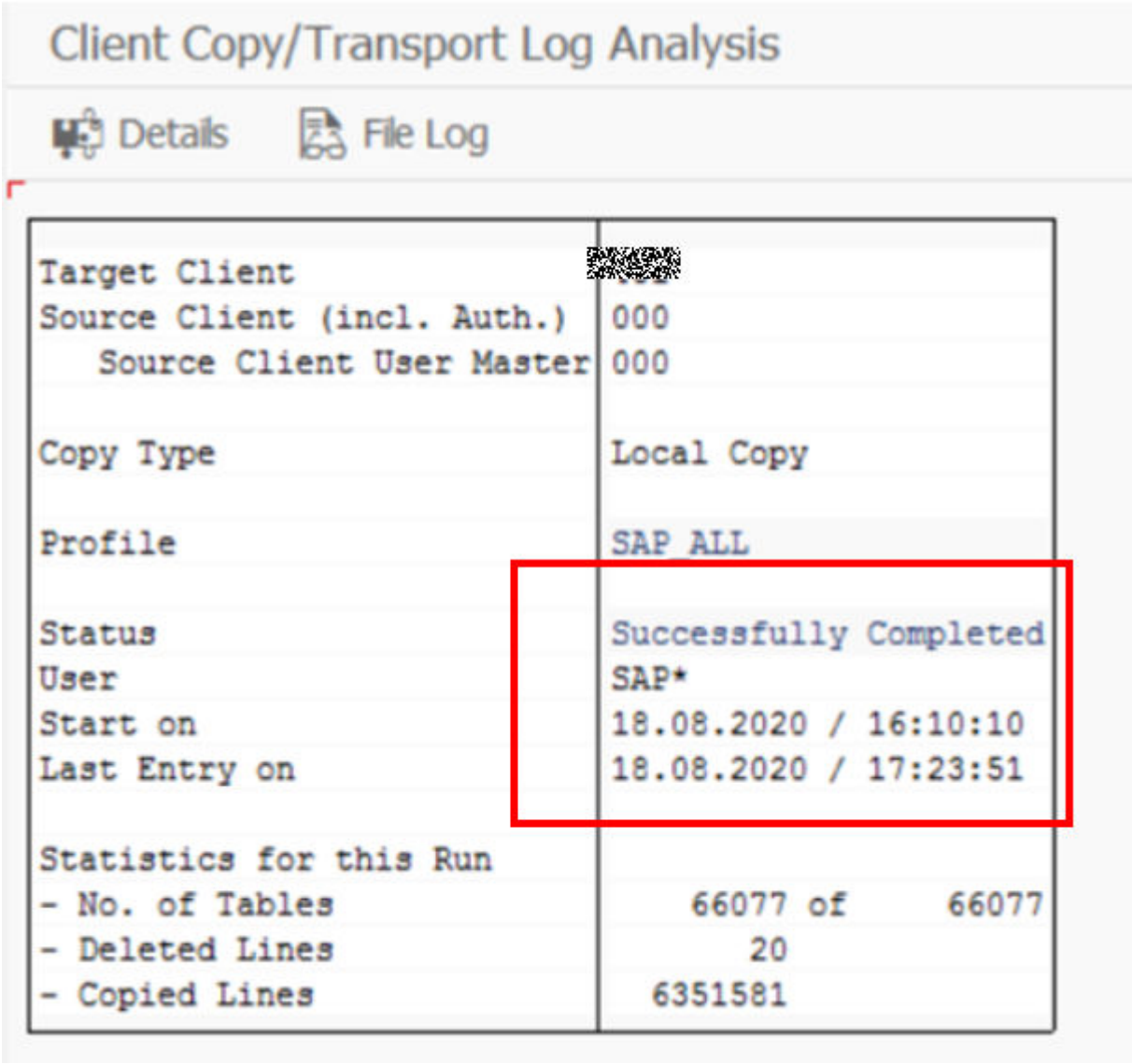
Step 20 Click **Continue** to start the replication.



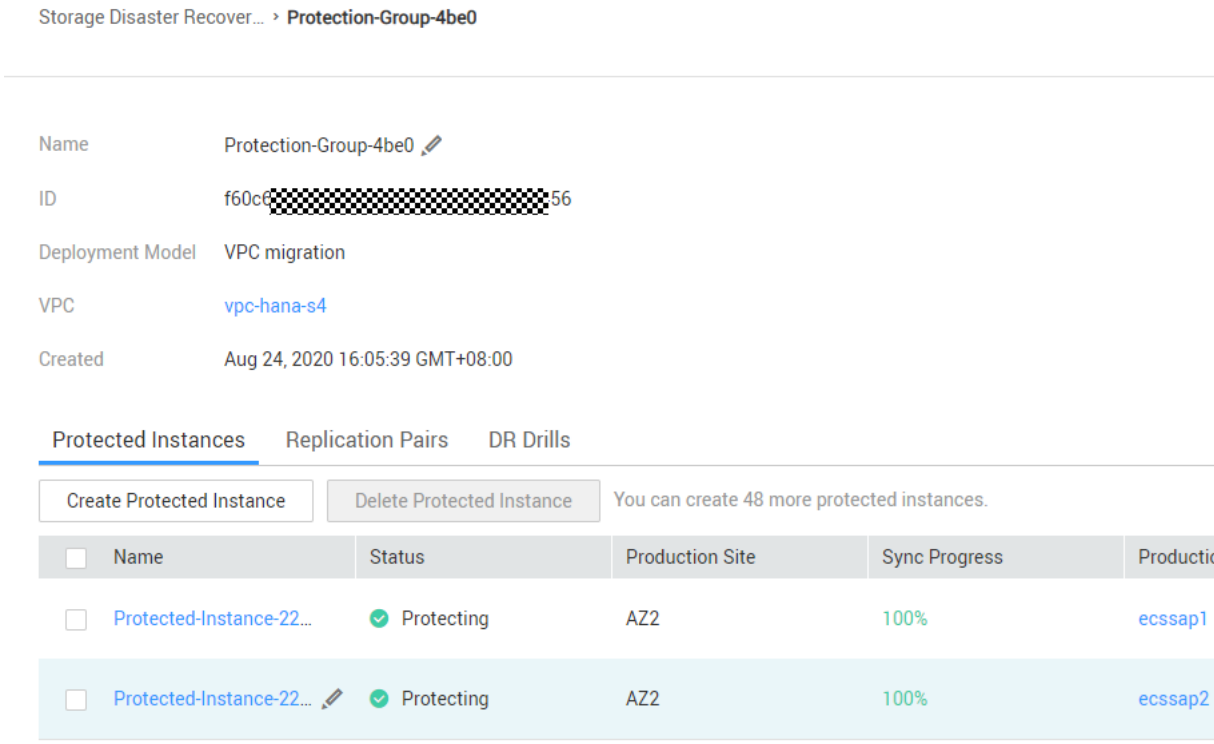
Step 21 After the client copy operation is complete, click **Log Display**.



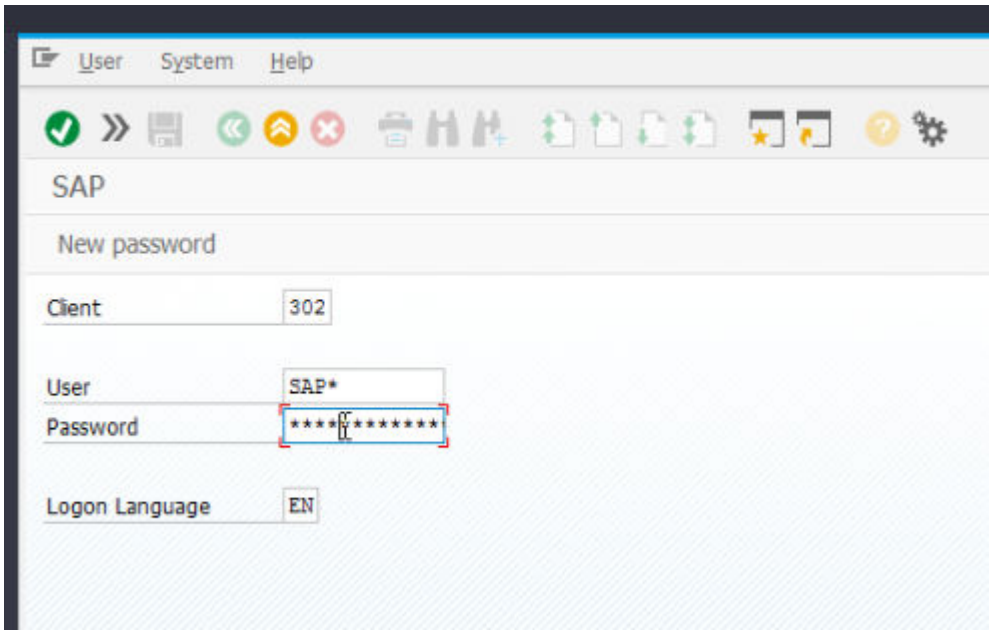
Step 22 Record the operation duration. The duration of **Client Copy** is 1 hour and 13 minutes when SDRS protection is enabled



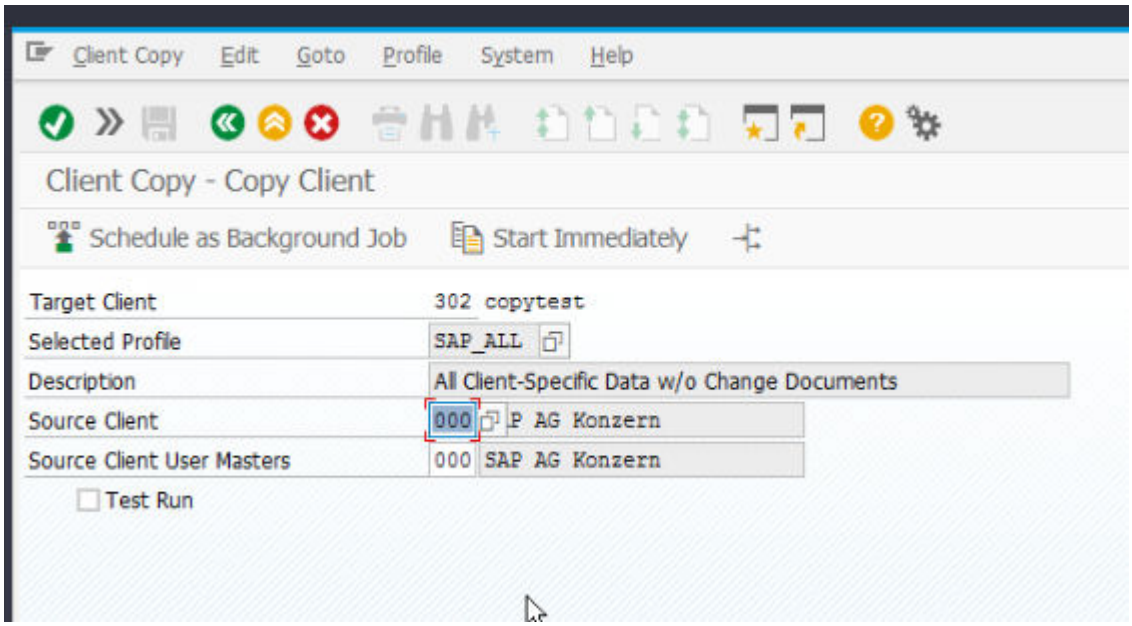
Step 23 Click **Disable Protection** and perform the Client Copy operation again.

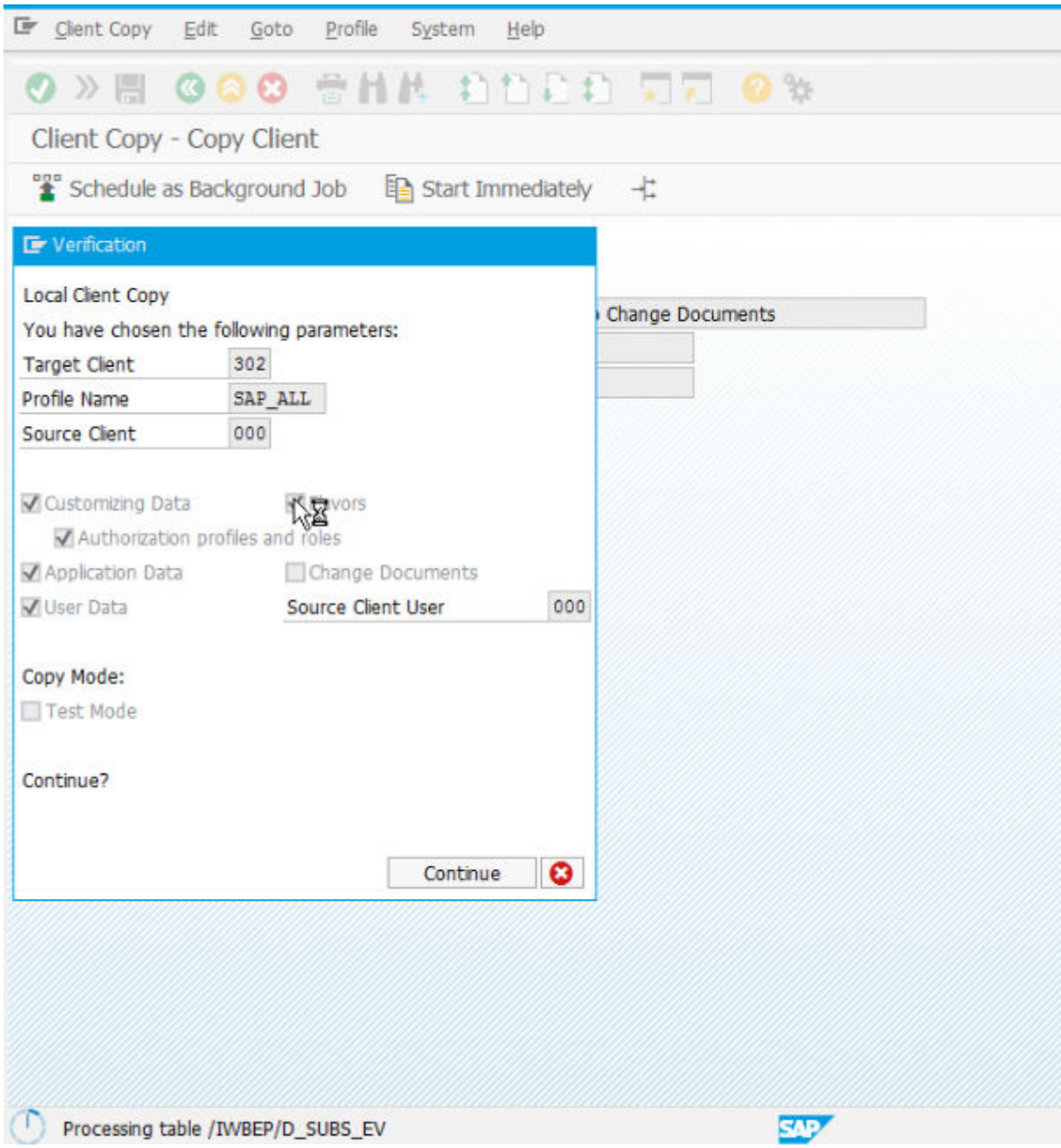


Step 24 Log in to another new client 302.

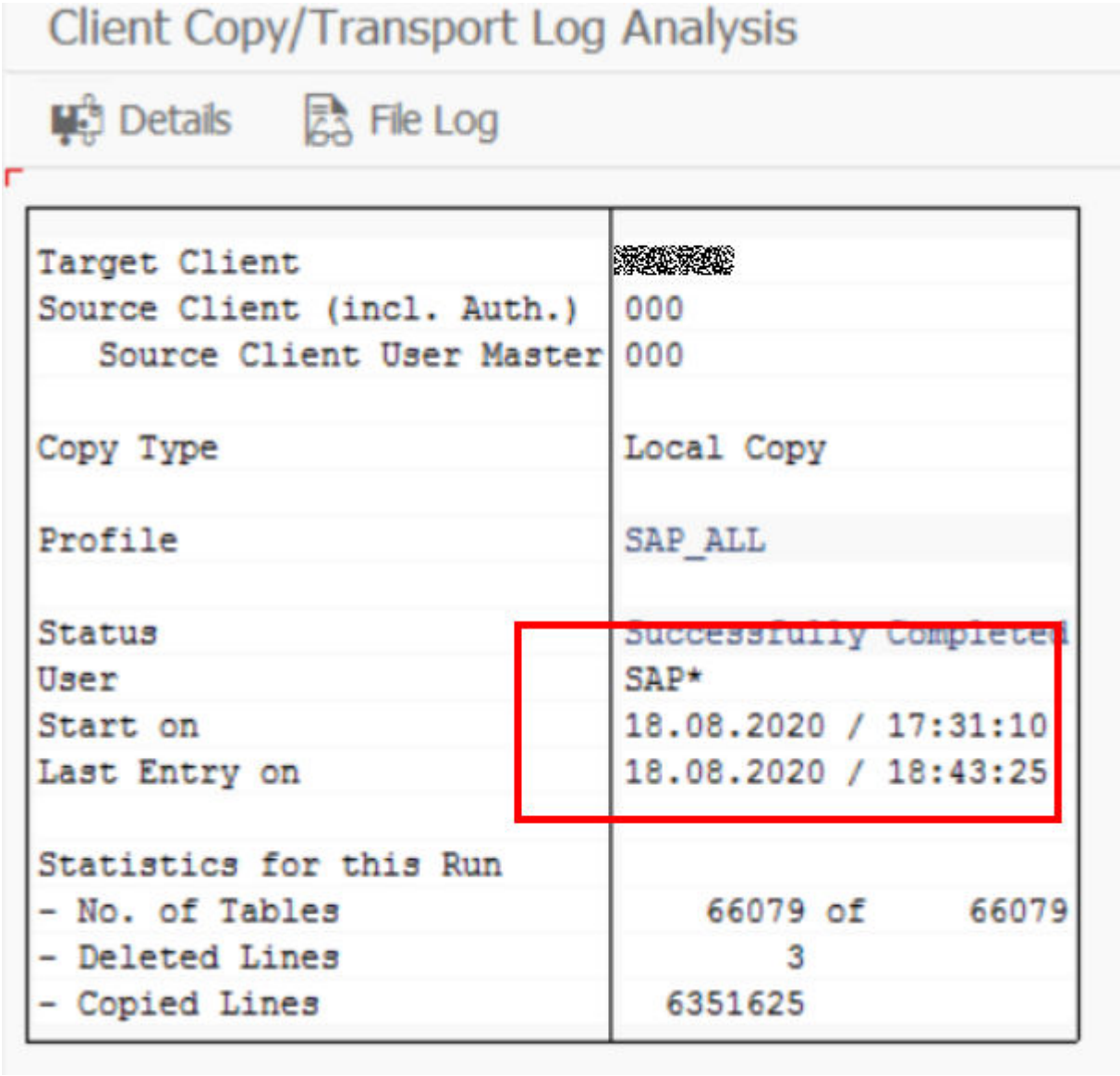


Step 25 Perform the Client Copy operation.





Step 26 Wait until the operation is complete and record the operation duration.



As shown in the preceding figure, when SDRS protection is enabled, the Client Copy operation takes 1 hour and 12 minutes.

----End

Conclusion: By comparing the time required for performing the preceding two Client Copy operations, you can find that the duration of the Client Copy operation does not change before and after SDRS protection is enabled. Therefore, enabling or disabling SDRS protection has no obvious impact on the application performance.

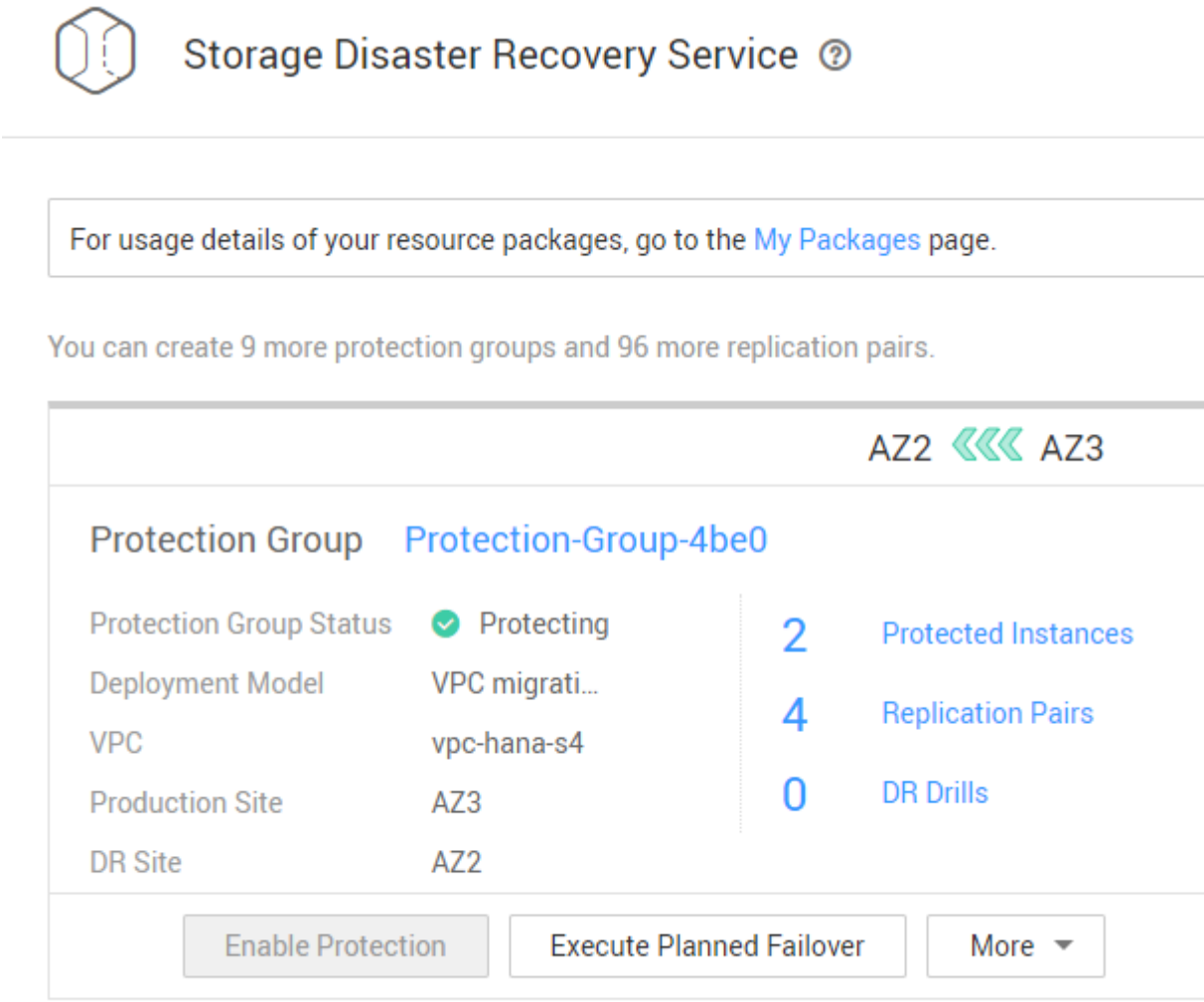
10.4.2 HammerDB Performance Test

HammerDB is a graphical open-source database load testing and benchmarking tool for Linux and Windows to test databases running on any operating system. HammerDB is automated, multithreaded, and extensible with dynamic scripting support. You can use HammerDB to create a test schema, load data, and simulate

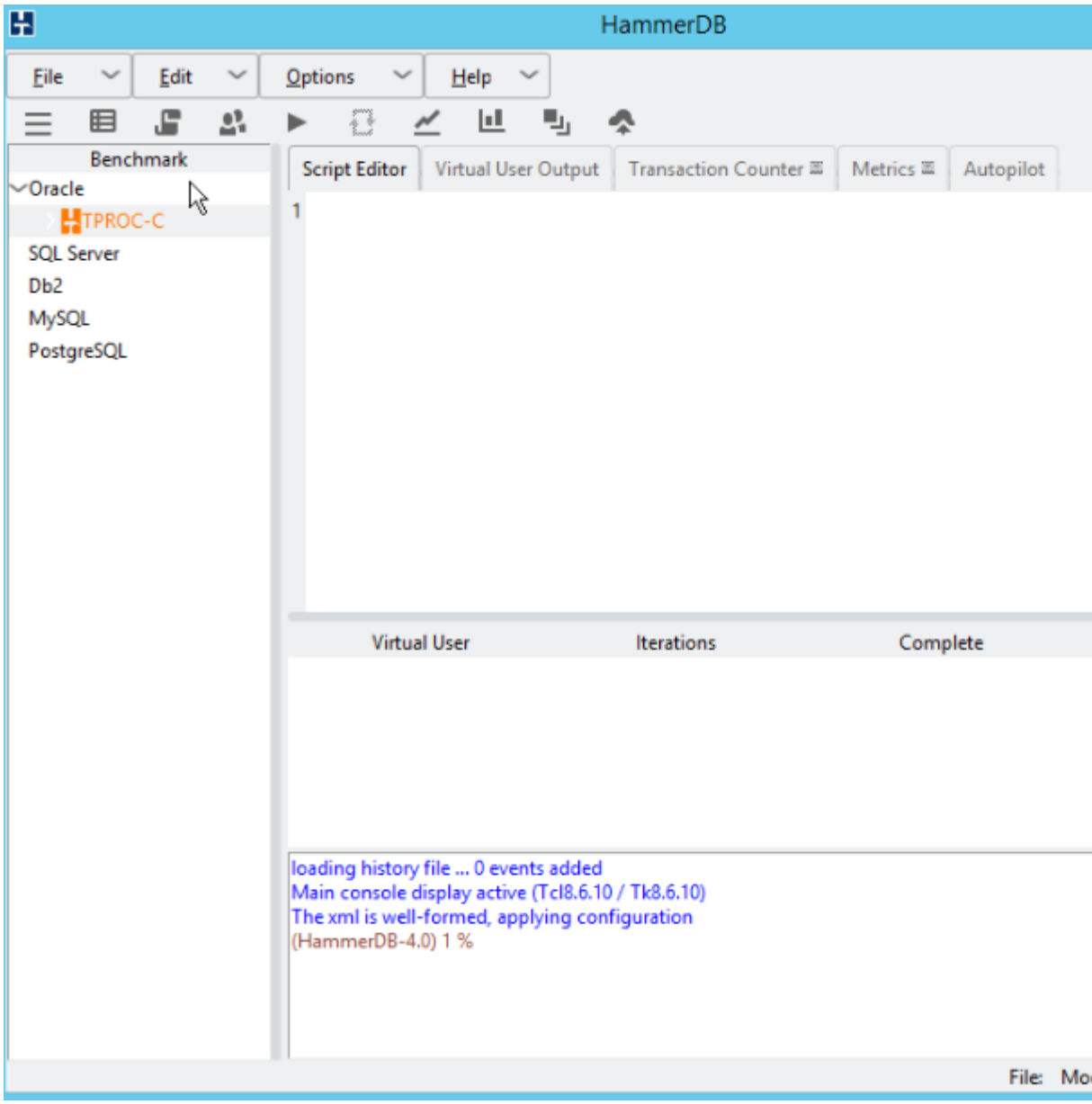
the database workload of multiple virtual users in online transaction processing (OLTP) and online analytical processing (OLAP) scenarios.

HammerDB 3.3 is used in this document. Download **HammerDB of the latest version**.

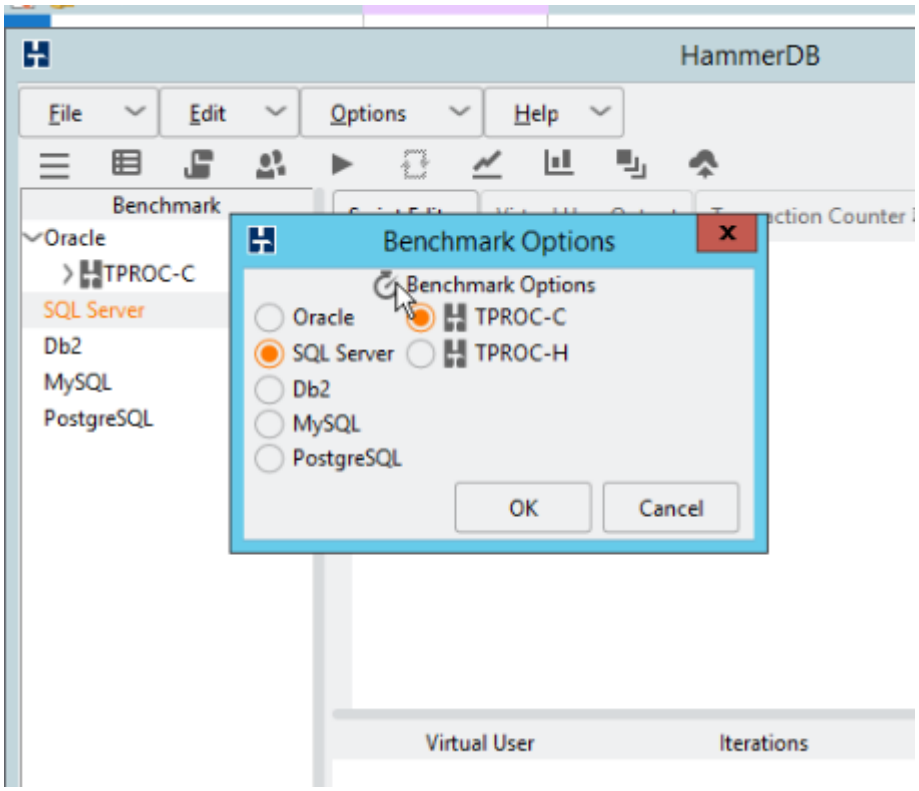
Step 1 Click **Enable Protection** on the **Storage Disaster Recovery Service** page.



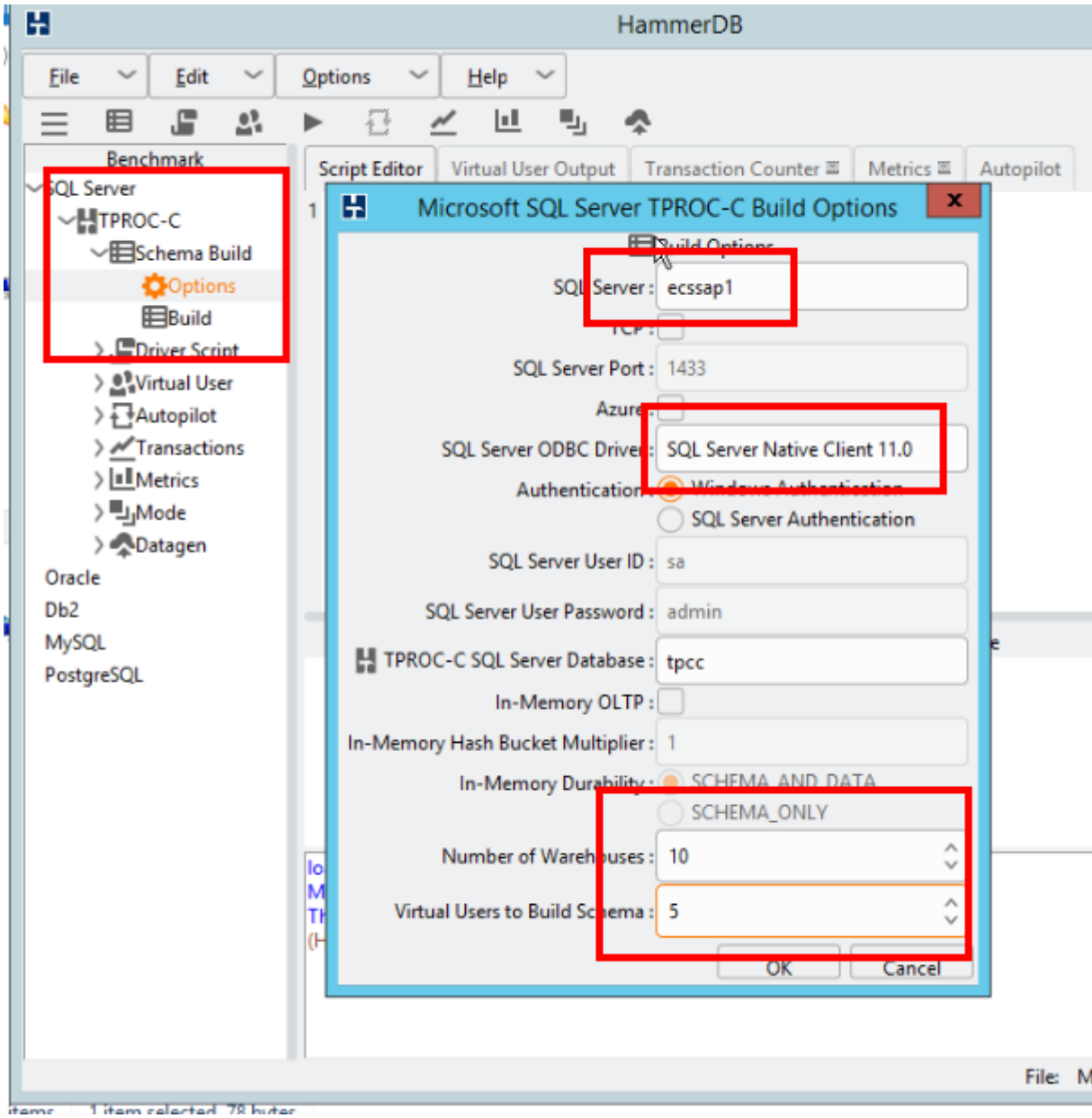
Step 2 Install and run the HammerDB performance test tool. For details, see **Test Method**.



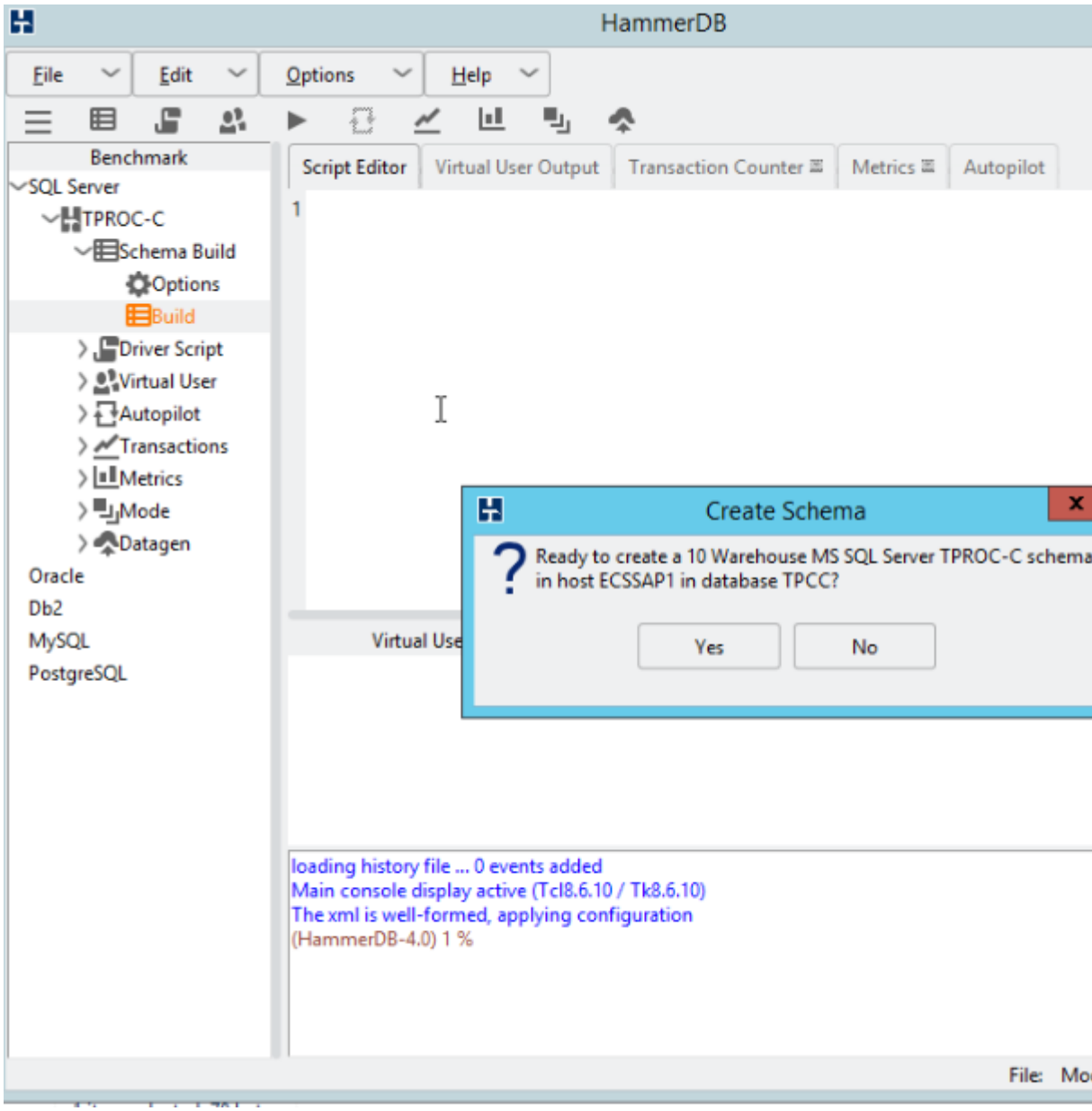
Step 3 Select **SQL Server** and **TORPC-C** and click **OK**.



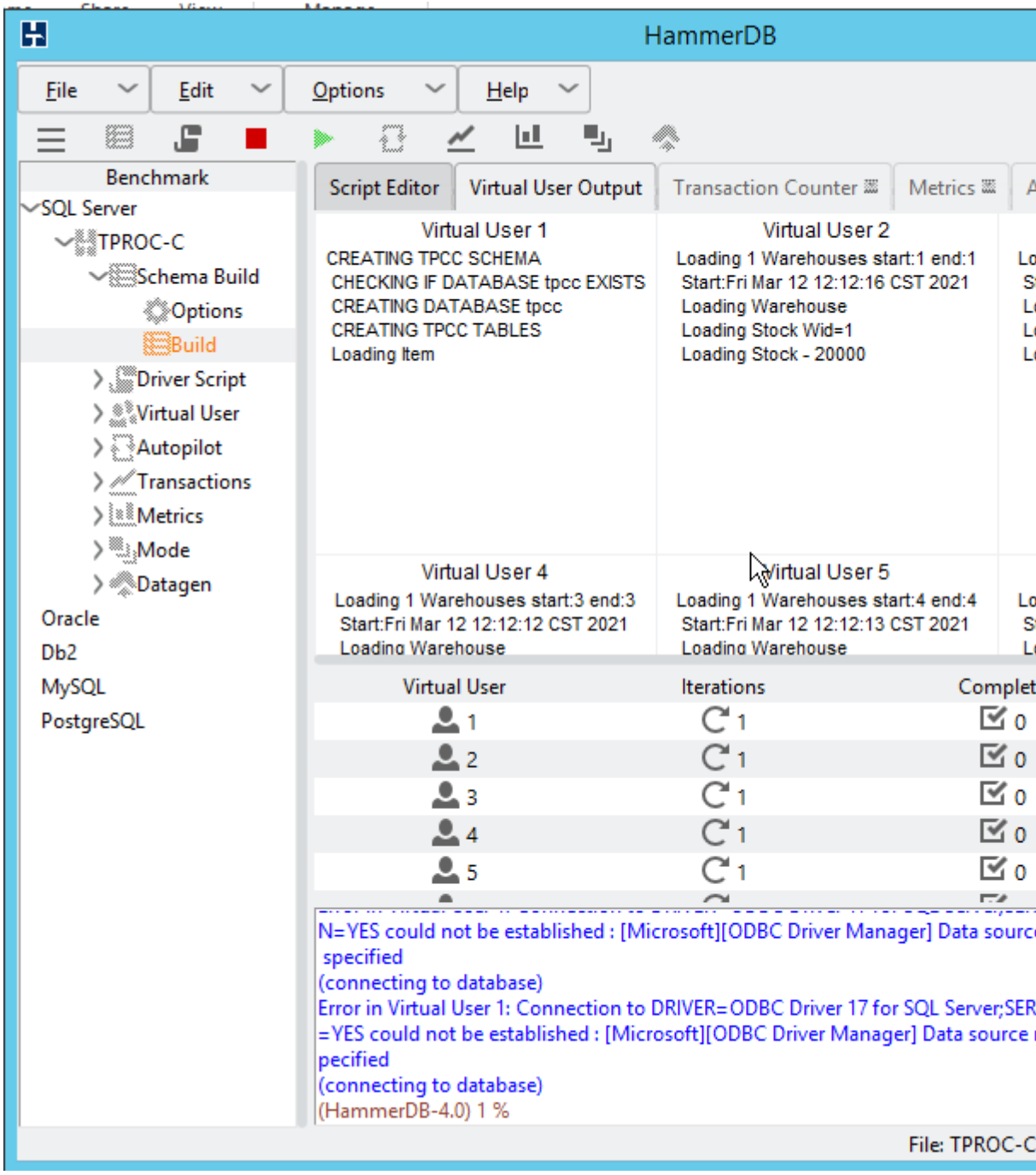
Step 4 Choose **SQL Server** > **TPROC-C** > **Schema Build**, and double-click **Options** to configure parameters. Configure **SQL Server**, **SQL Server ODBC Driver**, **Number of Warehouses**, **Virtual Users to Build Schema**, and click **OK**.

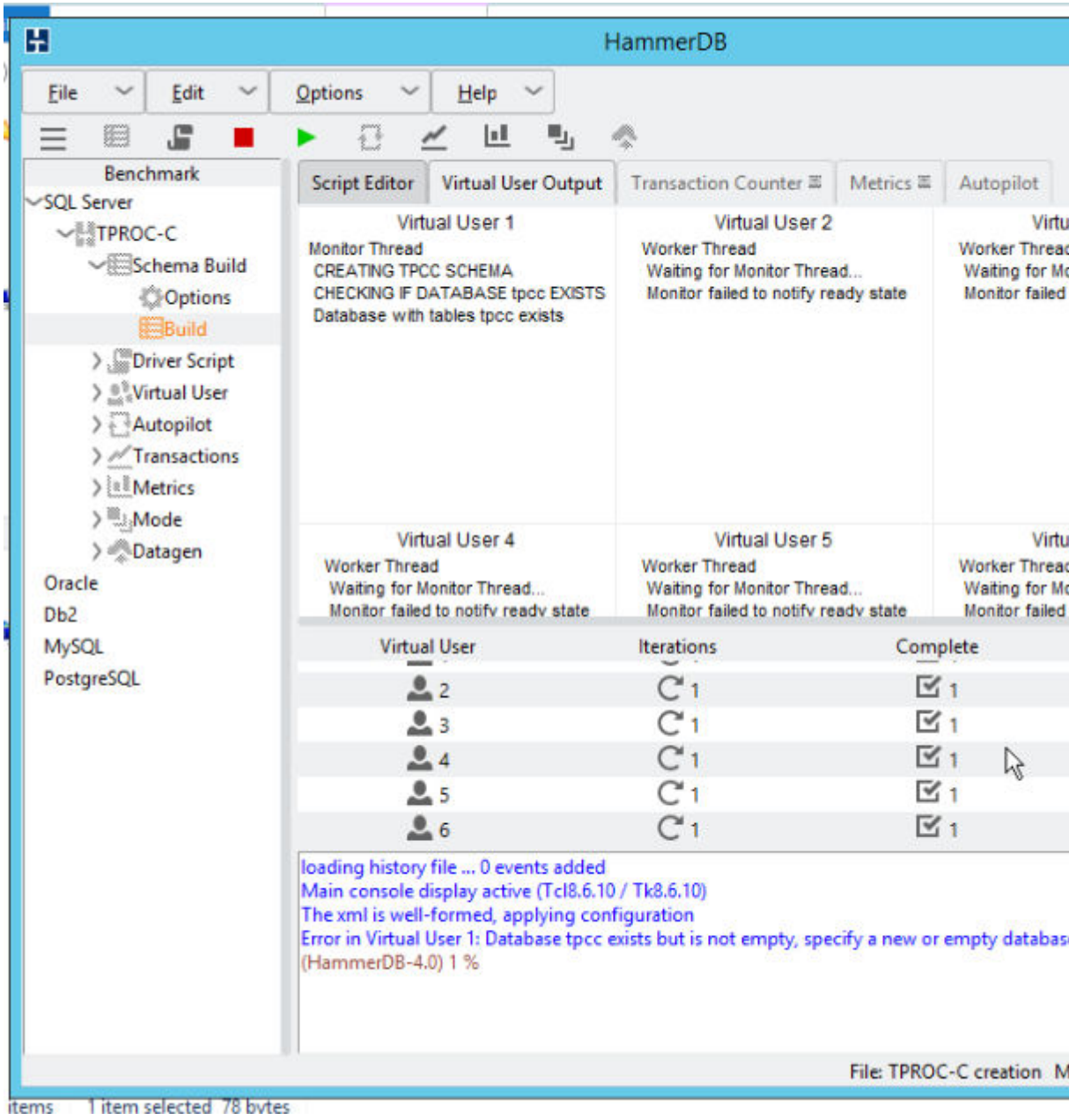


Step 5 Double-click **Build** and click **Yes**.

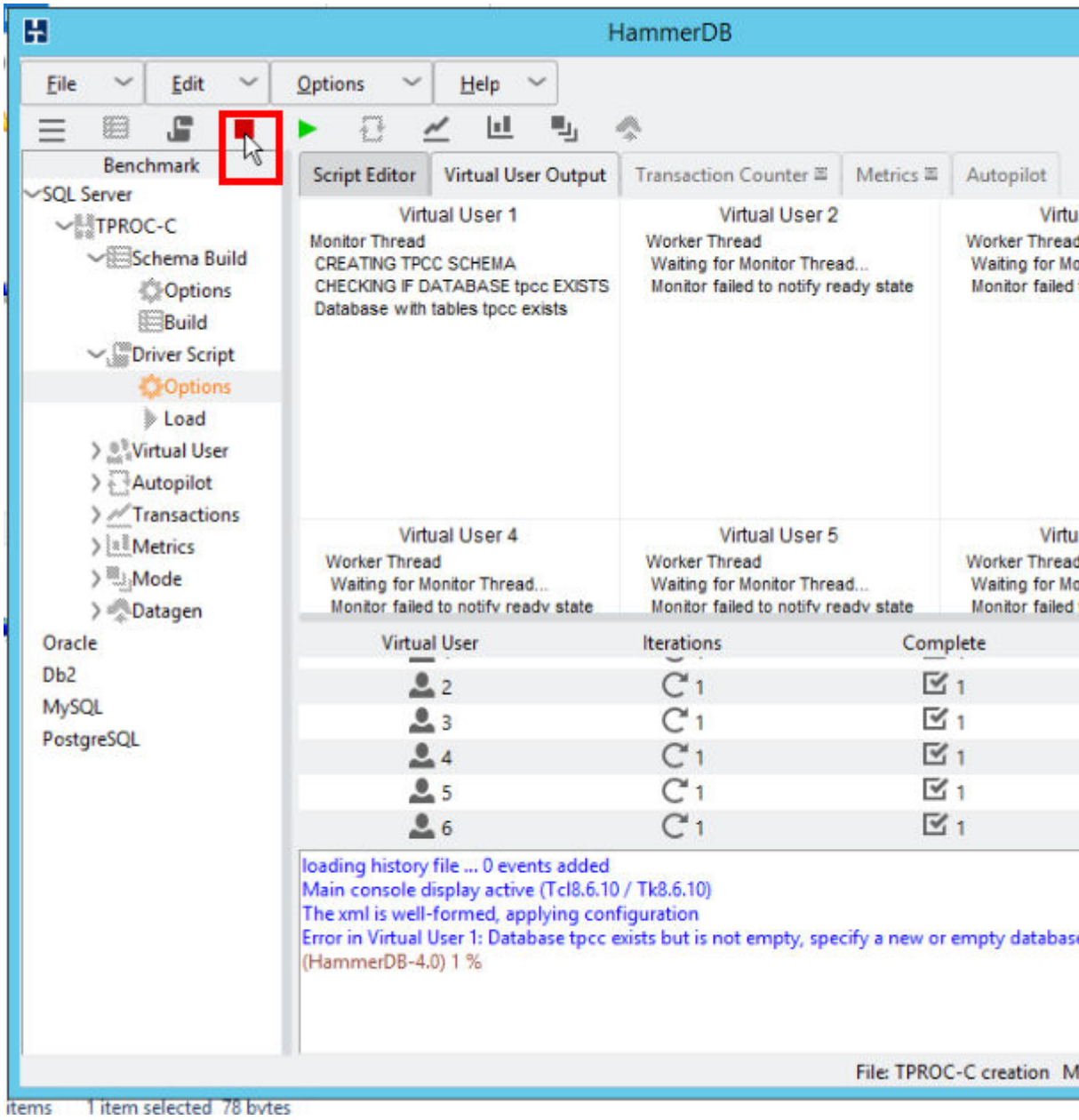


Step 6 Wait until the schema is created. The duration depends on the number of warehouses and schemata.

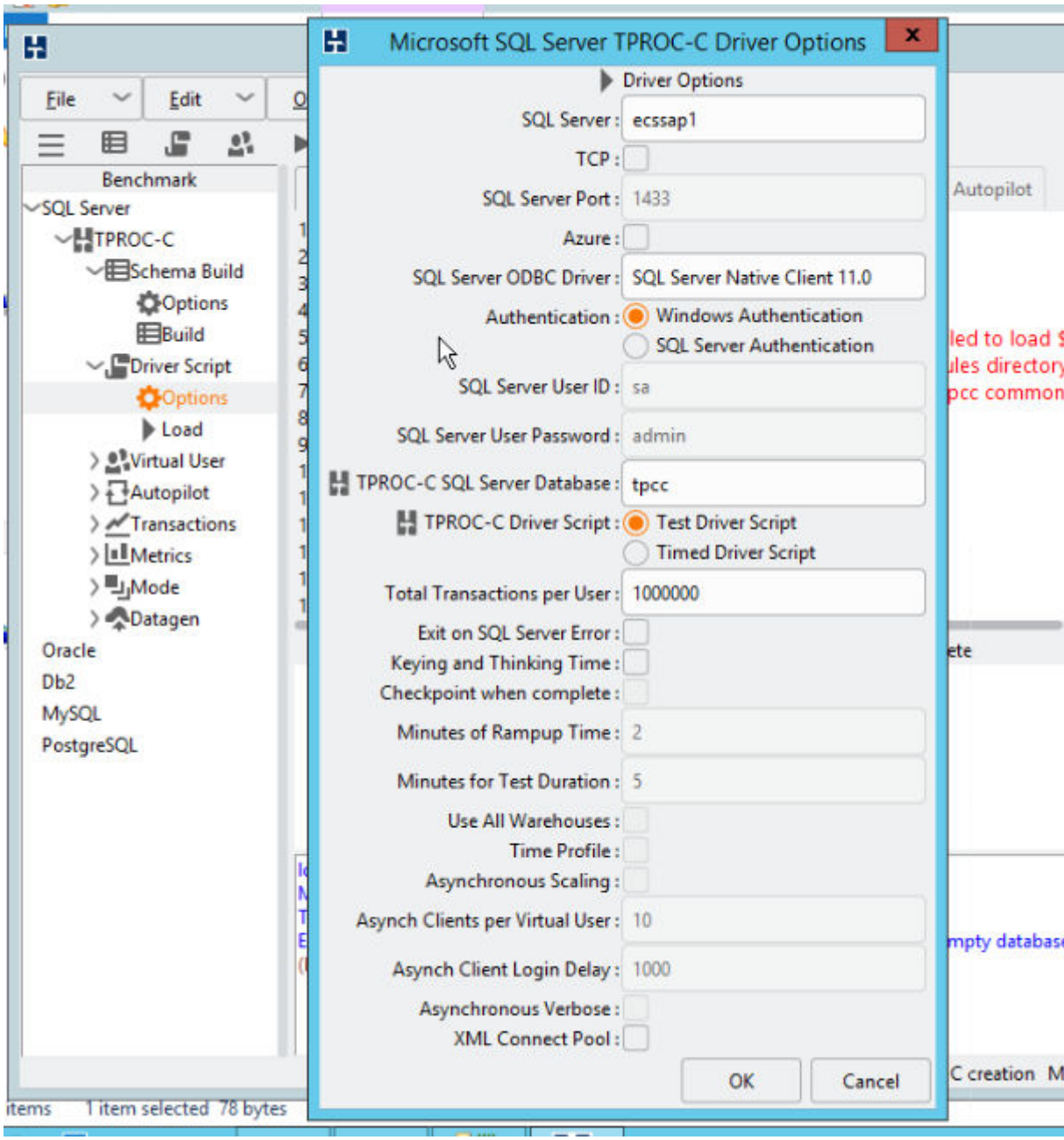

HammerDB
File
Edit
Options
Help
Benchmark
SQL Server
TPROC-C
Schema Build
Options
Build
Driver Script
Virtual User
Autopilot
Transactions
Metrics
Mode
Datagen
Oracle
Db2
MySQL
PostgreSQL
Script Editor
Virtual User Output
Transaction Counter
Metrics
Virtual User 1
CREATING TPCC SCHEMA
CHECKING IF DATABASE tpcc EXISTS
CREATING DATABASE tpcc
CREATING TPCC TABLES
Loading Item
Virtual User 2
Loading 1 Warehouses start:1 end:1
Start:Fri Mar 12 12:12:16 CST 2021
Loading Warehouse
Loading Stock Wid=1
Loading Stock - 20000
Virtual User 4
Loading 1 Warehouses start:3 end:3
Start:Fri Mar 12 12:12:12 CST 2021
Loading Warehouse
Virtual User 5
Loading 1 Warehouses start:4 end:4
Start:Fri Mar 12 12:12:13 CST 2021
Loading Warehouse
Virtual User
Iterations
1 1 0
2 1 0
3 1 0
4 1 0
5 1 0
N=YES could not be established : [Microsoft][ODBC Driver Manager] Data sourc
specified
(connecting to database)
Error in Virtual User 1: Connection to DRIVER=ODBC Driver 17 for SQL Server;SER
=YES could not be established : [Microsoft][ODBC Driver Manager] Data source
pecified
(connecting to database)
(HammerDB-4.0) 1 %
File: TPROC-C



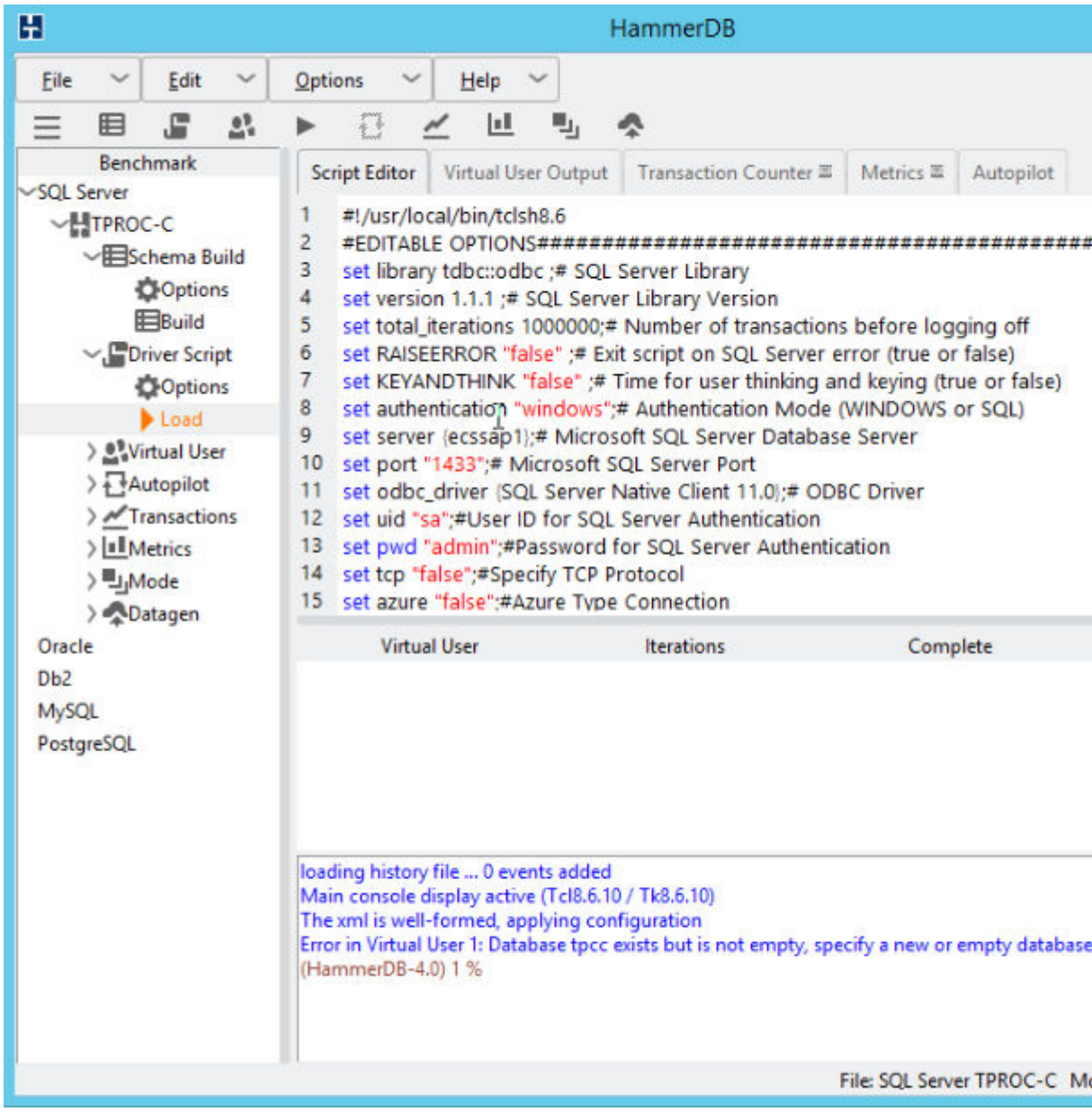
Step 7 Click the stop button.



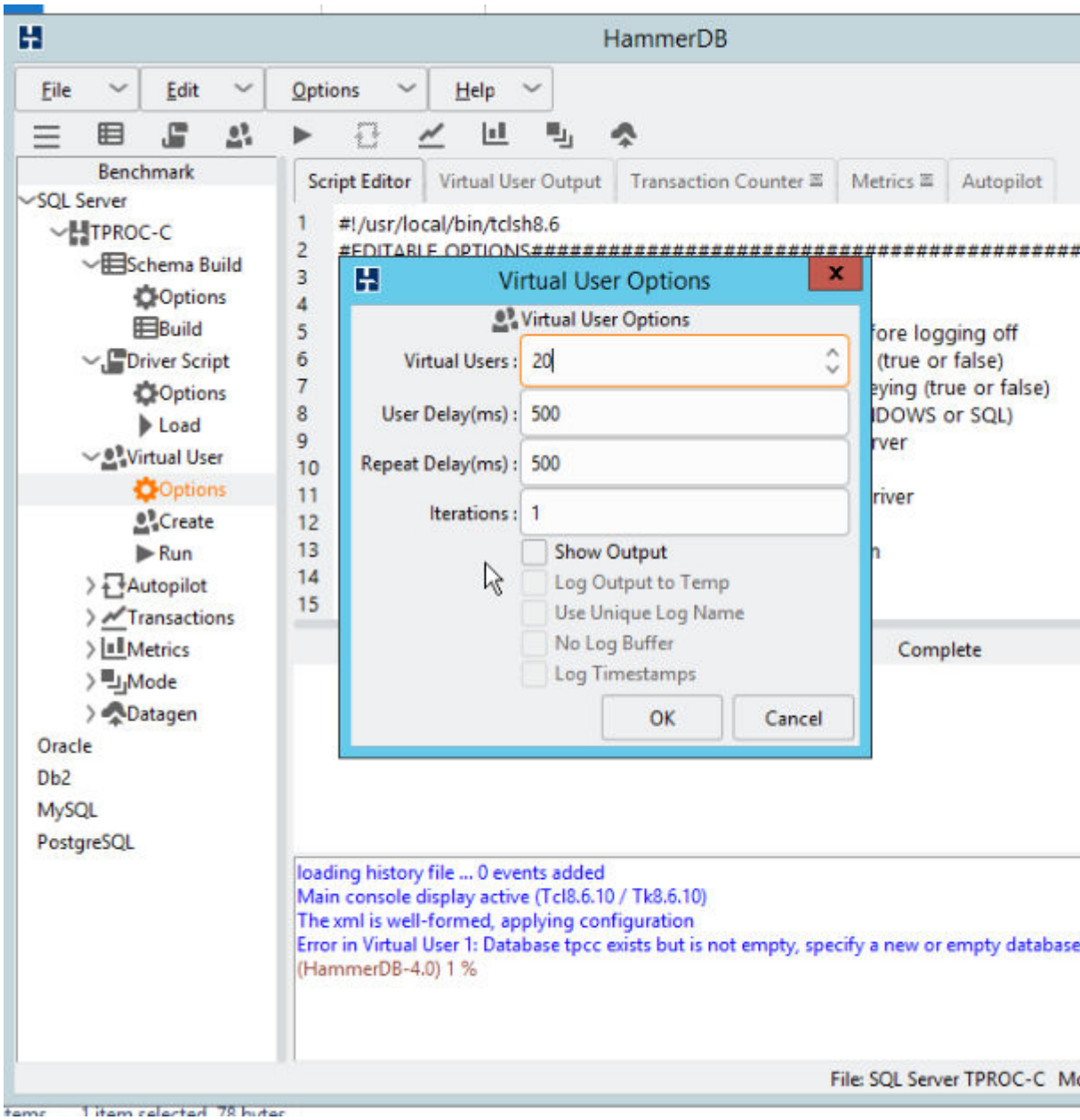
Step 8 Choose **Driver Script**, double-click **Options** to confirm the parameters, and click **OK**.



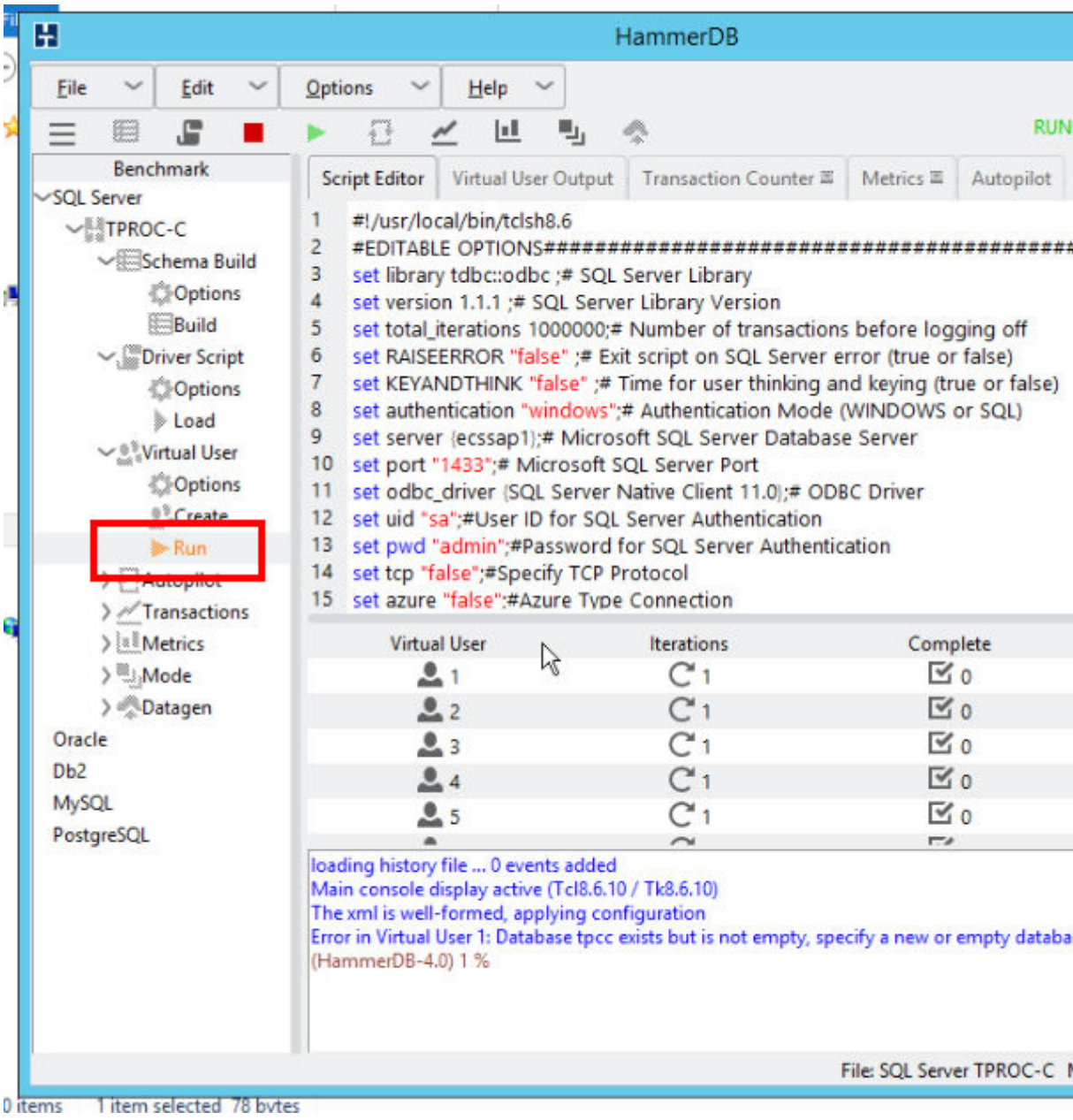
Step 9 Double-click **Load**.



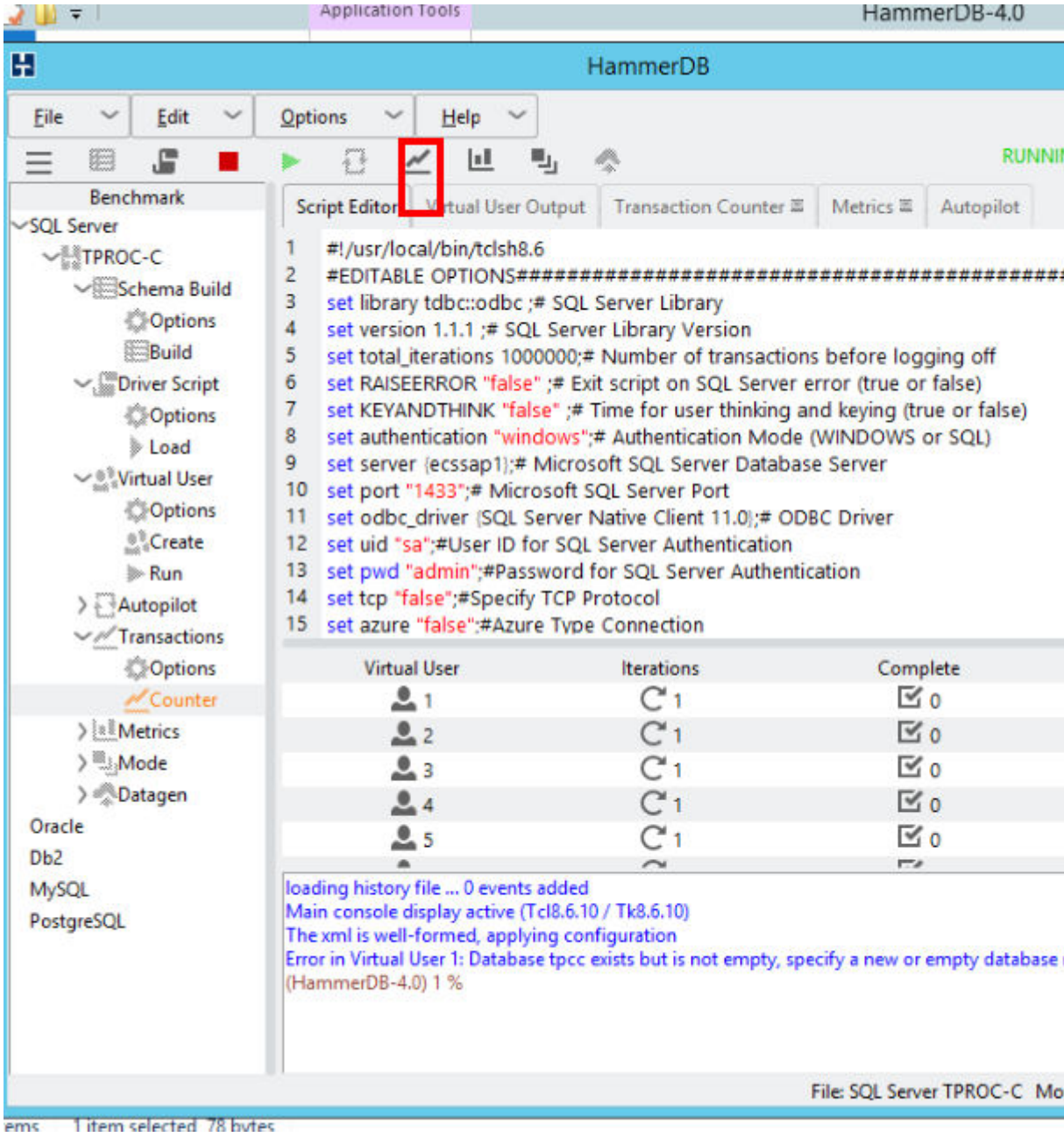
Step 10 Choose **Virtual User** and double-click **Options**. In the **Virtual User Options** dialog box, set **Virtual Users** to the number of virtual users, that is, **20** in this test, deselect **Show Output**, and click **OK**.

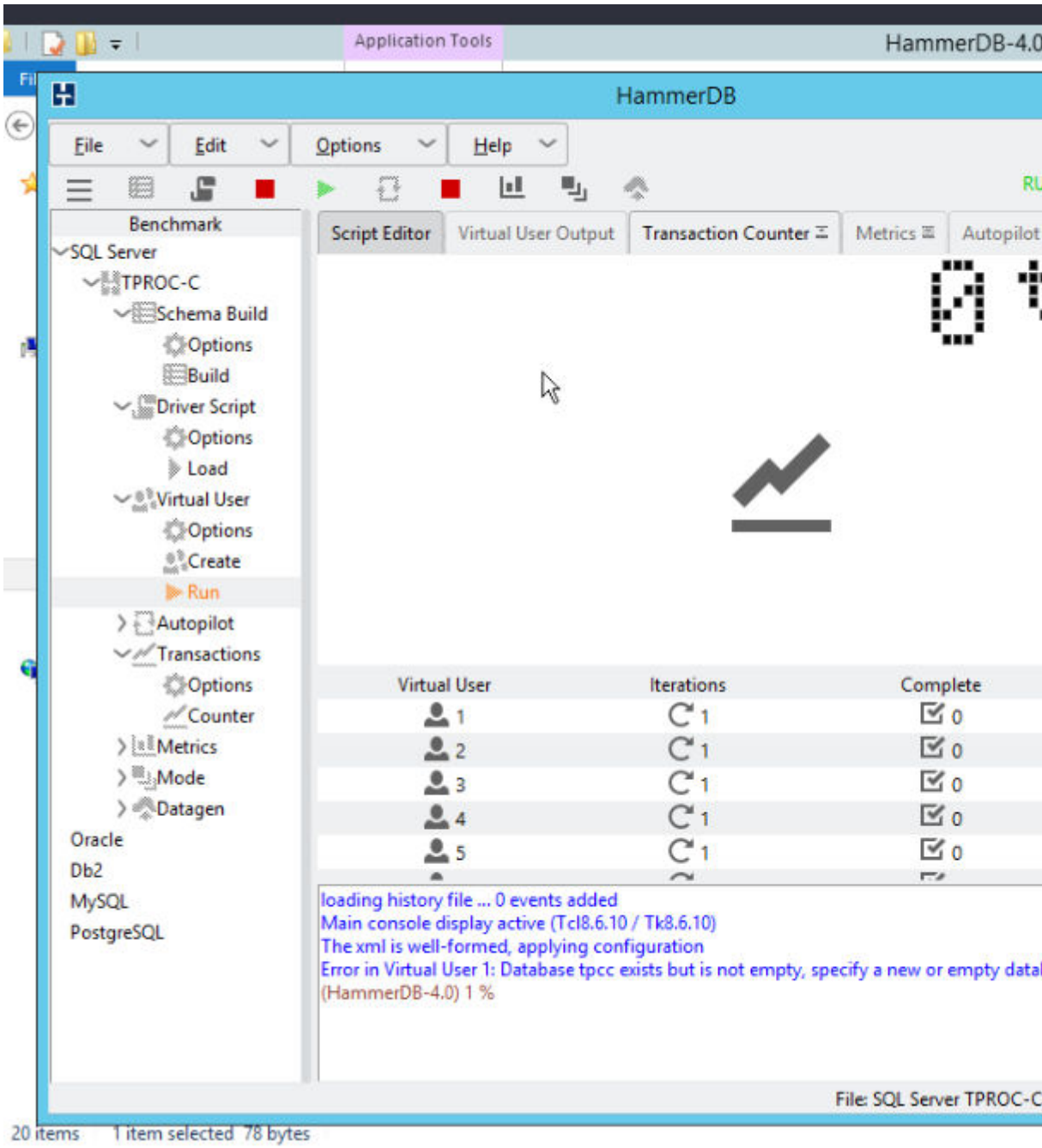


Step 11 Double-click **Run**.

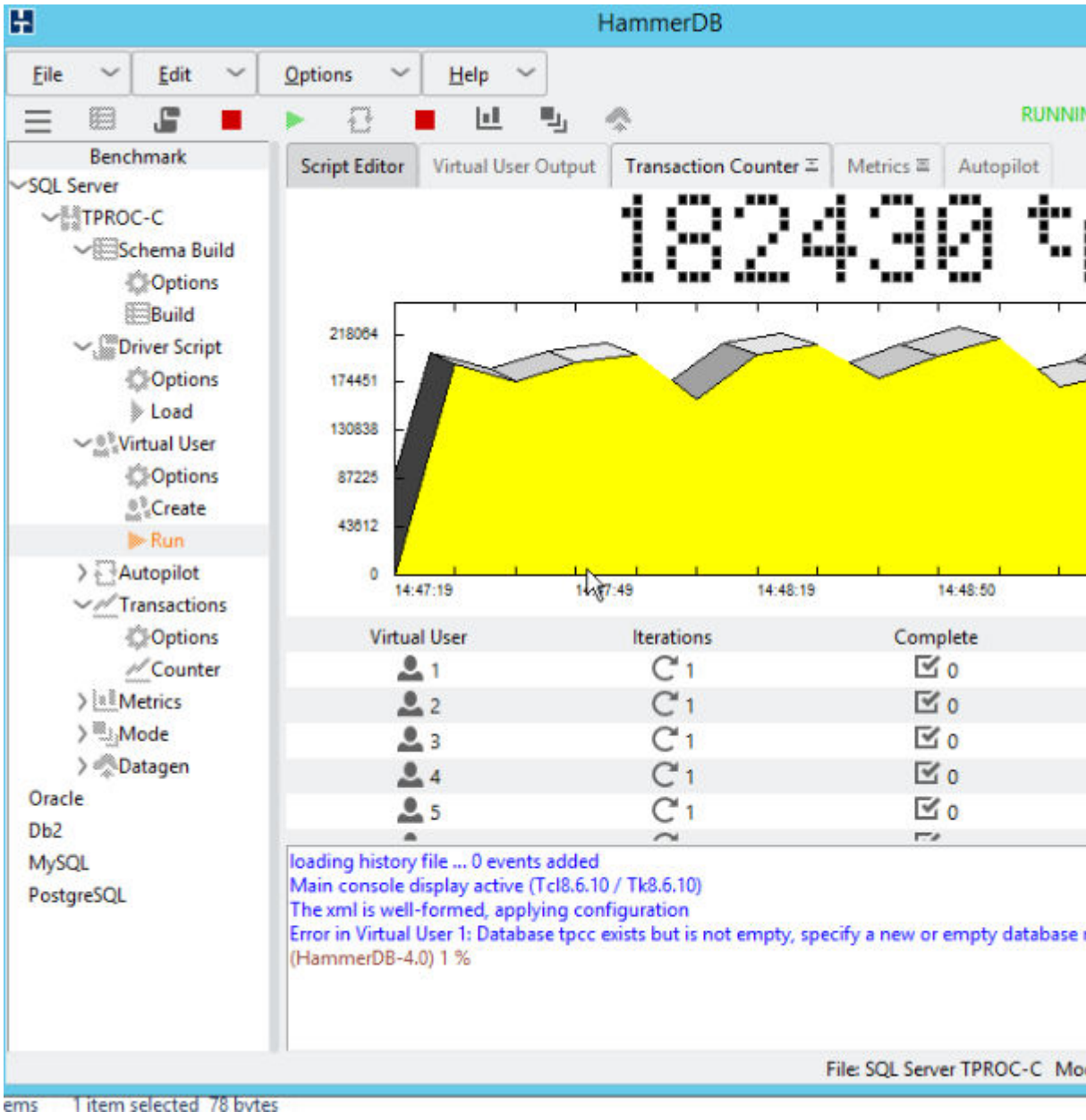


Step 12 Click the icon for starting transactions.

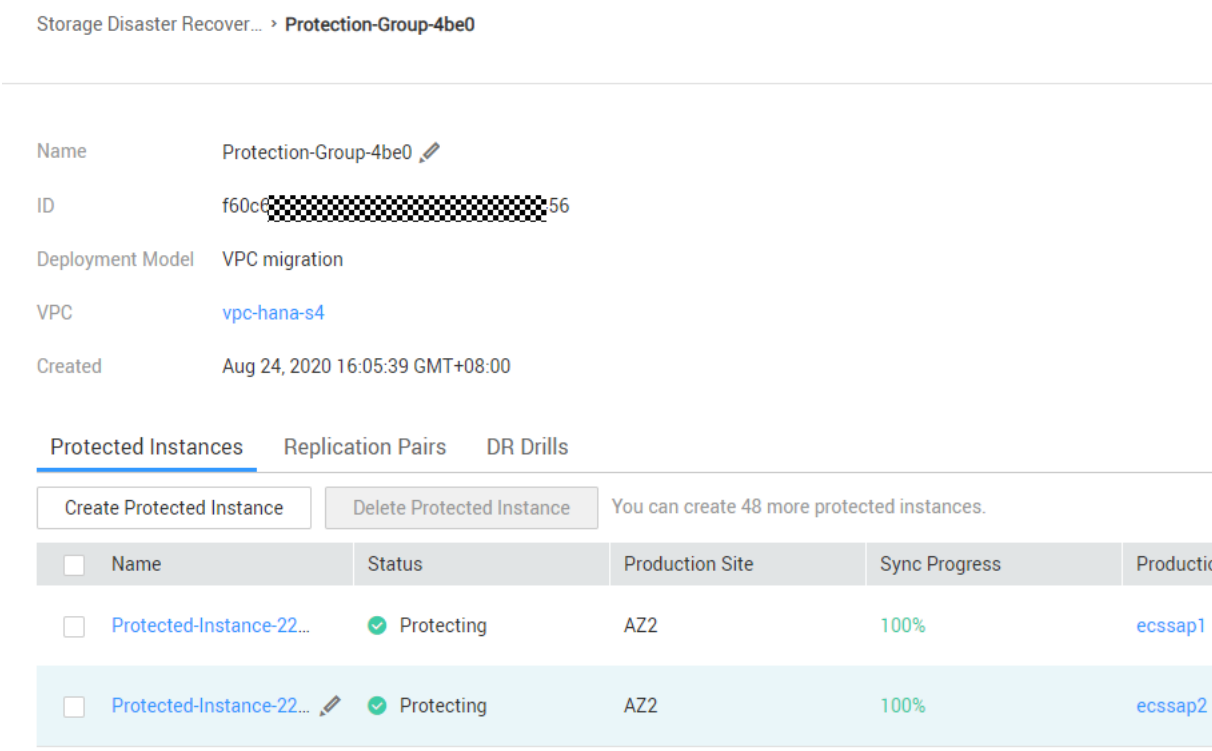

Application Tools
HammerDB-4.0
HammerDB
File
Edit
Options
Help
Benchmark
SQL Server
TPROC-C
Schema Build
Options
Build
Driver Script
Options
Load
Virtual User
Options
Create
Run
Autopilot
Transactions
Options
Counter
Metrics
Mode
Datagen
Oracle
Db2
MySQL
PostgreSQL
Script Editor
Virtual User Output
Transaction Counter
Metrics
Autopilot
#!/usr/local/bin/tclsh8.6
#EDITABLE OPTIONS##
set library tdbc::odbc ;# SQL Server Library
set version 1.1.1 ;# SQL Server Library Version
set total_iterations 1000000;# Number of transactions before logging off
set RAISEERROR "false" ;# Exit script on SQL Server error (true or false)
set KEYANDTHINK "false" ;# Time for user thinking and keying (true or false)
set authentication "windows";# Authentication Mode (WINDOWS or SQL)
set server {ecssap1};# Microsoft SQL Server Database Server
set port "1433";# Microsoft SQL Server Port
set odbc_driver {SQL Server Native Client 11.0};# ODBC Driver
set uid "sa";#User ID for SQL Server Authentication
set pwd "admin";#Password for SQL Server Authentication
set tcp "false";#Specify TCP Protocol
set azure "false";#Azure Type Connection
Virtual User
Iterations
Complete
1 1 0
2 1 0
3 1 0
4 1 0
5 1 0
loading history file ... 0 events added
Main console display active (Tcl8.6.10 / Tk8.6.10)
The xml is well-formed, applying configuration
Error in Virtual User 1: Database tpcc exists but is not empty, specify a new or empty database
(HammerDB-4.0) 1 %
File: SQL Server TPROC-C



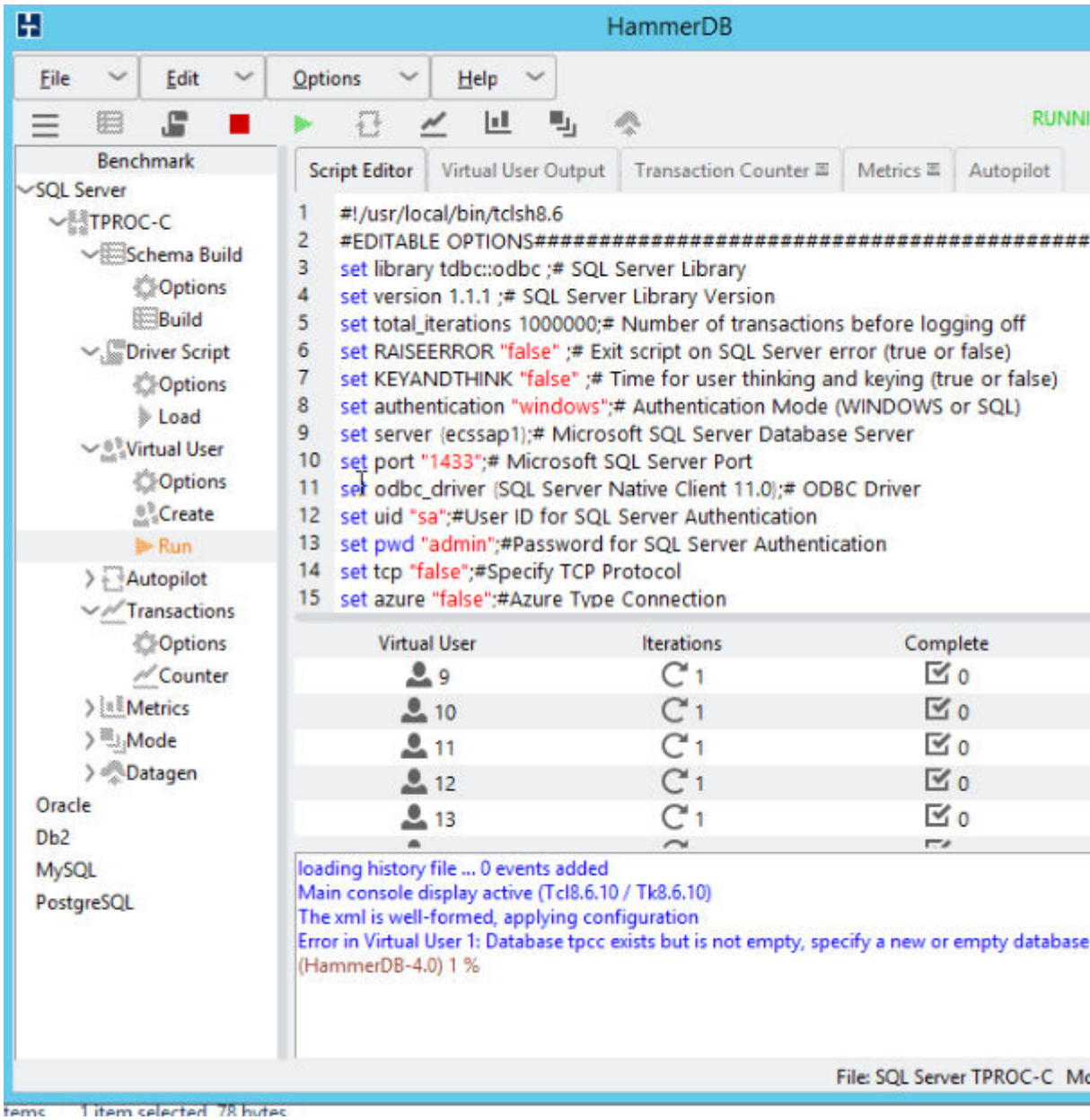
Step 13 Wait until the TPM reaches the peak value.



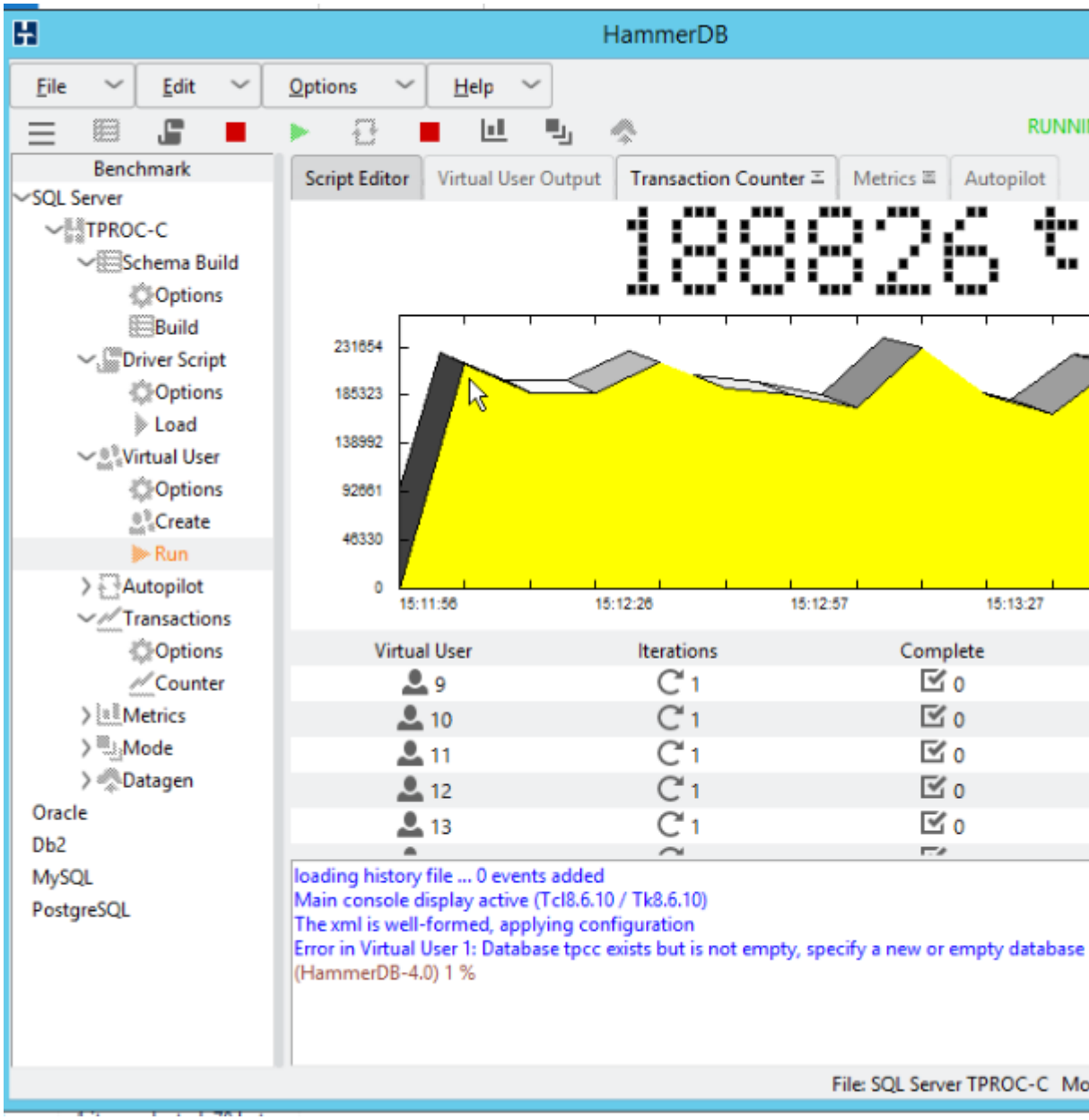
Step 14 Disable SDRS protection.



Step 15 Test the HammerDB performance again.



Step 16 Continue the HammerDB performance test until the TPM peak value is stable.



NOTE

Transactions per minute (TPM): Number of simulated orders processed by the system in the TPCC standard model per minute.

----End

Conclusion: By comparing the TPM values before and after SDRS protection is enabled, performance of the SQL Server database decreases by about 3.39% after SDRS protection is enabled.

10.5 Change History

Table 10-1

Description	Date	Prepared By
Initial version	2020-08-21	Xiong Peng/00508152
Optimized operations.	2021-05-20	Fu Chuandong/00469497

11 Best Practice of Rsync-based SAP Disaster Recovery

11.1 Script Overview

This script is developed using Shell and is executed using Rsync and Inotify. Rsync and Inotify can be used in the Linux OS. This script is used to synchronize folders between two servers in real time.

11.1.1 Introduction to Rsync and Inotify

Remote Synchronize (Rsync) is a remote data synchronization tool. It can quickly synchronize files between multiple servers through LAN/WAN or synchronize different directories in the local disks. This software is pre-installed in the SUSE Linux OS, and can be directly used.

Inotify is a Linux kernel subsystem, which monitors changes to the filesystem, such as file storing, extracting, deleting, moving, and modification. This software is not pre-installed in the SUSE Linux OS. You need to install it if necessary. You can obtain this tool at **https://github.com/rvoicilas/inotify-tools**.

11.1.2 Script File

The script package is **DirSyncScript.zip**, which contains the following files:

- **sync.sh**: Main program
- **sync.conf**: Configuration file, which is used to configure information such as the directories to be synchronized and the address of the destination server
- **start_inotifywait.sh**: Inotify monitoring script, which monitors the changes to the files and reports the changes after being executed

- **inotify-tools-3.14.tar.gz**: Inotify installation package

Rsync synchronization logs are stored in **/var/log/rsyncd.log**.

11.2 Preparations

11.2.1 Preparing the Environment

Prepare two servers for synchronization, and plan the directories to be synchronized and the destination directories for storing the synchronized directories. Note that one-to-one mapping relationships between source directories to be synchronized and destination directories are required, and the source directories must be available.

11.2.2 Configuring the Mutual Trust Relationship

Ensure that two severs can communicate with each other using SSH. Assume that the two servers for synchronization are node 1 and node 2. Perform the following steps to configure the mutual trust relationship.

Procedure

Step 1 Log in to node 1 as **user** root.

Step 2 Generate the public and private keys.

ssh-keygen -t rsa

The following information is displayed:

```
Generating public/private rsa key pair. Enter file in which to save the key (/home/deven/.ssh/
id_rsa): (Press Enter.)
Enter passphrase (empty for no passphrase): (Press Enter.)
Enter same passphrase again: (Press Enter.)
Your identification has been saved in /home/deven/.ssh/id_rsa.
Your public key has been saved in /home/deven/.ssh/id_rsa.pub.
The key fingerprint is:89:56:d6:4a:b2:6c:4a:05:.....
```

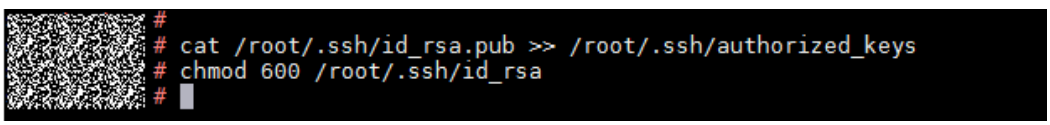
Press **Enter** after you enter the information required each time as prompted. The **id_rsa** and **id_rsa.pub** files are generated in the **/root/.ssh/** directory.

Step 3 Write **id_rsa.pub** to the **authorized-keys** file.

cat /root/.ssh/id_rsa.pub >> /root/.ssh/authorized_keys

Step 4 Modify the permission of **id_rsa**.

chmod 600 /root/.ssh/id_rsa

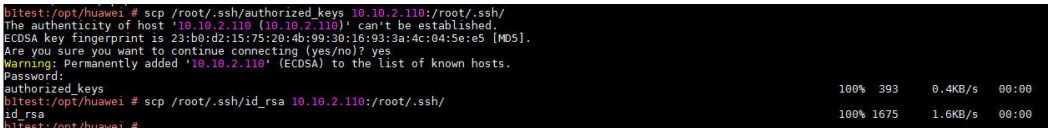


Step 5 Copy **anthorized-keys** and **id_rsa** to node 2.

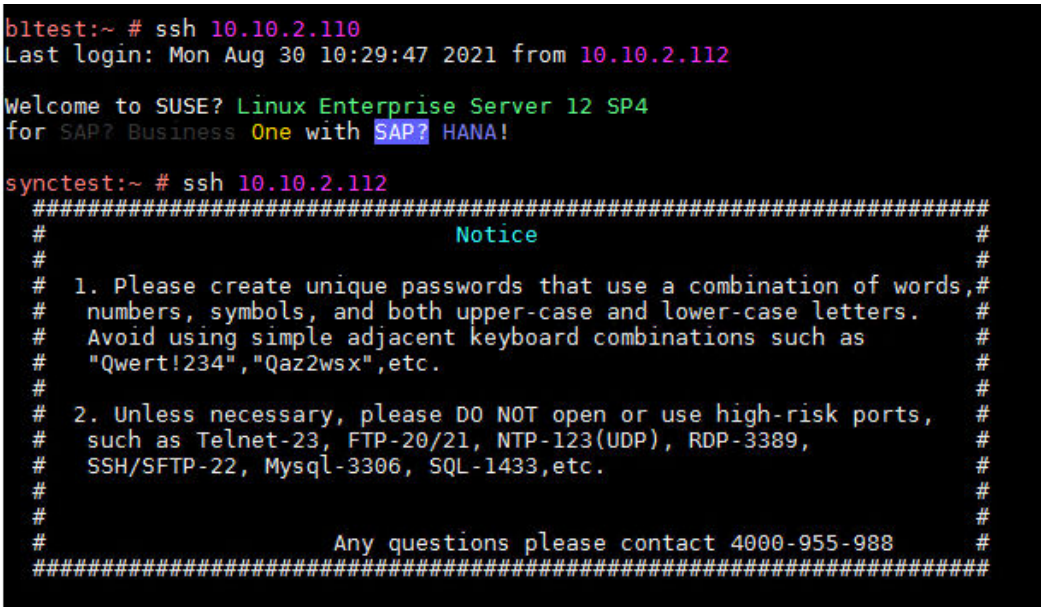
scp /root/.ssh/authorized_keys *IP address of node 2*:**/root/.ssh/**

After the command is executed, a message is displayed, indicating whether to connect to the node. Enter **yes** and then enter the password of node 2. The files are copied to node 2.

scp /root/.ssh/id_rsa*IP address of node 2*:**/root/.ssh/**



Step 6 Check whether the two servers can communicate with each other using using SSH.



----End

11.2.3 Downloading Software

Procedure

Step 1 Log in to the source node 1 as user **root** using a key or password.

Step 2 On the CLI, run the following commands to download the **DirSyncScript.zip** package and decompress it to the **/opt/huawei** directory:

wget https://obs-sap-cn-south-1.obs.cn-south-1.myhuaweicloud.com:443/Rsync/DirSyncScript.zip -P /opt/huawei

cd /opt/huawei

unzip DirSyncScript.zip -d DirSyncScript


```
bltest:/ #
bltest:/ # wget https://obs-sap-cn-south-1.obs.cn-south-1.myhuaweicloud.com:443/Rsync/DirSyncScript.zip  -P /opt/huawei
--2021-08-30 10:22:16--  https://obs-sap-cn-south-1.obs.cn-south-1.myhuaweicloud.com/Rsync/DirSyncScript.zip
Resolving obs-sap-cn-south-1.obs.cn-south-1.myhuaweicloud.com (obs-sap-cn-south-1.obs.cn-south-1.myhuaweicloud.com)... 100.125.24.119, 100.125.24.34, 100.125.24.120, ...
Connecting to obs-sap-cn-south-1.obs.cn-south-1.myhuaweicloud.com (obs-sap-cn-south-1.obs.cn-south-1.myhuaweicloud.com)|100.125.24.119|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 361333 (353K) [application/zip]
Saving to: '/opt/huawei/DirSyncScript.zip.1'

100%[=====================================================================================================>] 361,333     --.-K/s   in 0.06s

2021-08-30 10:22:17 (6.18 MB/s) - '/opt/huawei/DirSyncScript.zip.1' saved [361333/361333]

bltest:/ # cd /opt/huawei
bltest:/opt/huawei # unzip DirSyncScript.zip -d DirSyncScript
```

----End

11.2.4 Modifying Configurations

Procedure

Step 1 Log in to the source node 1 as user **root** using a key or password.

Step 2 Go to the directory where the decompressed file is stored and run the **vi** command to open the **sync.conf** configuration file.

cd /opt/huawei/DirSyncScript

vi sync.conf

```
bltest:~ # cd /opt/huawei/DirSyncScript
bltest:/opt/huawei/DirSyncScript # vi sync.conf
```

Step 3 Modify the configuration parameters by referring to **Table 11-1** and save the modification.

Table 11-1 Configuring parameters

Parameter	Description	Example Value
Source_Directory	Directory to be synchronized on the source server. If there are multiple directories, separate them with slashes (/). **CAUTION** If there is no slash (/) added to the end of the source directory to be synchronized, the directory itself and its content will be synchronized. If there is a slash (/) added to the end of the source directory, all contents in the directory will be synchronized (the directory itself excluded). For example, if the directories to be synchronized on the source host are **/src1,/src2/** and the destination directories are **/dst1,/dst2**, **/dst1** contains the **/src1** file folder itself and the content included after synchronization, while **/dst2** contains all the contents in the **/src2** file folder (excluding the **/src2** folder itself).	/src1/, /src2/, /src3/
Destination_Host	IP address of the destination server	192.168.0.11

Parameter	Description	Example Value
Destination_Directory	Destination directory. Use slashes (/) to separate multiple directories. The number of directories for storing the synchronized directories on the destination host must be the same as those to be synchronized.	/dst1, /dst2, /dst3

The directories in the following figure are used as an example. Configure the directories based on the site requirements.

```
# Use ',' to separate different directories
#Caution: When source path end with '/', will sync the files and directories in it. When not end with '/', will sync the direcotry itself.
Source_Directory = /usr/sap/, /hana/

#One destionation host only.
Destination_Host = 10.10.2.110

# Use ',' to separate different directories.
# Destination directories are one-to-one mapping to source directories.
Destination_Directory = /usr/sap, /hana
```

----End

11.3 Performing Synchronization

Prerequisites

The two servers can communicate with each other using SSH.

Procedure

Step 1 After modifying the configuration file, run the following command on source node 1:

cd /opt/huawei/DirSyncScript

sh sync.sh

```
bltest:/opt/huawei/DirSyncScript # sh sync.sh
Info: Inotify is installed.
Check param done.
Info: Parameters are configured.
Info: Source direcotory ready.
Info: Source dir ready.
Info: Rsync is installed.
Info: Rsync is ready.
Info: Inotify is installed.
Info: inotify is ready.
Info: Test SSH connection success.
Info: SSH to destination success.
Info: Ready to start synchronization.
Sync /usr/sap with /usr/sap/
Sync /hana with /hana/
nohup: appending output to 'nohup.out'
Synchronization started.
nohup: appending output to 'nohup.out'
```


After this command is executed, the environment is initialized. After the environment is ready, the synchronization will be started.

NOTE

In addition to the script execution, the **sh sync.sh** command has the following functions:

- **sh sync.sh init** for environment initialization, checking whether Inotify has been installed. If no, it will be installed.
- **sh sync.sh check** for environment check, checking whether the modification file is correct and whether the required software has been installed to determine whether the synchronization can be started.
- **sh sync.sh start** for starting the synchronization when the environment is ready. A synchronization process will be generated for each directory to be synchronized.
- **sh sync.sh stop** for stopping the synchronization process

Step 2 Verifying the synchronization result.

Log in to node 2 and check whether the synchronized files are the same as those on the source server.

```
synctest:/usr/sap # ll
total 28
drwxr-xr-x  4 1001   79 4096 Jul 31 12:14 HDX
drwxr-xr-x 13 1003 1002 4096 Aug  4 16:49 SAPBusinessOne
drwxr-xr-x  7 root root 4096 Aug  4 15:10 hdbclient
drwxr-x---  4 root   79 4096 Jul 30 19:27 hostctrl
-rwxr-xr-x  1 root   79  208 Jul 31 12:15 sapservices
-rwxr-xr--  1 root   79  182 Jul 30 19:29 sapservices_202107_30_19.29.06
-rwxr-xr-x  1 root   79  208 Jul 30 19:29 sapservices_202107_31_12.10.18
```

----End

12 SAP Backint Installation Guide

12.1 Overview

Backint is a backup and restoration solution provided by SAP HANA. Backint for SAP HANA is an API that enables third-party tool vendors to directly connect their backup agents to the SAP HANA database. Backups are transferred via pipe from the SAP HANA database to the third-party backup agent, which runs on the SAP HANA database server and then sends the backups to the third-party party backup server.

Huawei Backint Agent is provided to back up the data in SAP HANA to OBS. After the SAP HANA database and Huawei Backint Agent are deployed and related parameters of SAP HANA database and OBS are configured, Huawei Backint Agent backs up the SAP HANA database to OBS, restores it, or deletes the backup files using SAP management tools, such as SAP HANA Cockpit, SAP HANA Studio, or SAP HANA HDBSQL. Backint can be applied to the following scenarios:

- Backup: Full backup, incremental backup, and differential backup for system or tenant data
- Restoration: Data restoration from the latest backup file, to a specified time point, or from a specified backup file
- Deletion: Deletion of specified backup file or backup files earlier than the specified one
- Query: Queries for full backups, incremental backups, and differential backups

12.2 Prerequisites

12.2.1 Logging in to Huawei Cloud

Before deploying the SAP system on Huawei Cloud, register a Huawei ID and enable Huawei Cloud services. Through this account, you can use Huawei Cloud services and pay only for the services you use.

For details, see **Registering a HUAWEI ID and Enabling Huawei Cloud Services**

You can log in to Huawei Cloud using any of the methods described in **Logging In to Huawei Cloud**.

The server where the SAP HANA database is located and the OBS bucket must belong to the same Huawei Cloud account and be in the same region.

12.2.2 Purchasing an ECS and Installing SAP HANA

You must install SAP HANA first, and then the Backint Agent. For details about how to install SAP HANA on HUAWEI CLOUD, see **SAP HANA**.

You must install SAP HANA Studio or SAP HANA Cockpit on a Windows ECS to configure Backint. For details about how to install SAP HANA Studio on a HUAWEI CLOUD ECS, see **Installing the SAP HANA Studio on a Windows ECS**.

If you install SAP HANA on different servers, do not use the same system ID (SID). Otherwise, it is difficult to determine which SAP HANA database the data backed up in the OBS bucket belongs to. If you want to use the same system ID, create different OBS buckets for independent backup.

12.3 Installation and Deployment

12.3.1 Installing Backint Agent

12.3.1.1 Downloading Backint Agent

Do not delete the installation script for it is mandatory for installation, upgrade, and uninstallation. If the installation script is deleted by mistake, download the script again.

Run the following command to obtain the installation script. Select the download link based on the region where the server accommodating the SAP HANA database is located.

The following command uses the AP-Bangkok region as an example:

cd /tmp && curl -k -O https://obs-sap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/backint/install.sh

Table 12-1 Commands for obtaining installation scripts

Script	Description	Command
install.sh	Installation script	AP-Bangkok: **cd /tmp && curl -k -O https://obs-sap-ap-southeast-2.obs.ap-southeast-2.myhuaweicloud.com/backint/install.sh** AP-Singapore: **cd /tmp && curl -k -O https://obs-sap-ap-southeast-3.obs.ap-southeast-3.myhuaweicloud.com/backint/install.sh** CN-Hong Kong: **cd /tmp && curl -k -O https://obs-sap-ap-southeast-1.obs.ap-southeast-1.myhuaweicloud.com/backint/install.sh** AF-Johannesburg: **cd /tmp && curl -k -O https://obs-sap-af-south-1.obs.af-south-1.myhuaweicloud.com/backint/install.sh** TR-Istanbul: **cd /tmp && curl -k -O https://obs-sap-tr-west-1.obs.tr-west-1.myhuaweicloud.com/backint/install.sh** LA-Santiago: **cd /tmp && curl -k -O https://obs-sap-la-south-2.obs.la-south-2.myhuaweicloud.com/backint/install.sh** LA-Sao Paulo1: **cd /tmp && curl -k -O https://obs-sap-sa-brazil-11.obs.sa-brazil-1.myhuaweicloud.com/backint/install.sh** LA-Mexico City1: **cd /tmp && curl -k -O https://obs-sap-na-mexico-1.obs.na-mexico-1.myhuaweicloud.com/backint/install.sh** LA-Mexico City2: **cd /tmp && curl -k -O https://obs-sap-la-north-2.obs.la-north-2.myhuaweicloud.com/backint/install.sh**

12.3.1.2 Installing Backint Agent

The downloaded installation script is stored in the **/tmp** directory. You can execute the script in this directory.

Run the following command as user **root** to install Backint Agent. Enter the system ID of the server where Backint Agent is installed for *SID* in the command, for example, **bash install.sh --install S99**.

bash install.sh --install *SID*

The **install.sh** script will:

- Locate the installation package (JAR file) in **/usr/sap/{*SID*}/*SYS/global/hdb/opt/hw-backint-agent/*** and install Backint Agent.
- Download a compatible JRE version.
- Provide the **hdbbackint** script for invoking Backint Agent. The **hdbbackint** script cannot be modified.

- Send a message to notify of updating **/usr/sap/{*SID*}/SYS/global/hdb/opt/hdbconfig/hw-backint-agent.conf** after the installation is finished.

In the high availability (HA) scenario, you need to repeat the preceding operations to install Backint Agent on the standby server.

12.3.2 Configuring Backint Agent

12.3.2.1 Creating an IAM Agency for the ECS Where SAP HANA Is Located

Before configuring Backint Agent, you need to create an agency for the ECS where the SAP HANA database is located to obtain the temporary AK and SK. The procedure is as follows:

1. Log in to the public cloud management console and select a desired region in the upper left corner.

2. In the navigation pane on the left, click  and choose **Management & Governance > Identity and Access Management**.

3. Choose **Agencies** in the pane on the left, and click **Create Agency** in the upper right corner. The **Create Agency** page is displayed.

4. Set agency parameters.

- **Agency Name**: Enter **sap-backint**. The name is only an example.
- **Agency Type**: Select **Cloud service**.
- **Cloud Service**: Select **Elastic Cloud Server (ECS) and Bare Metal Server (BMS)**.
- **Validity Period**: Retain the default setting.
- Click **Next**. Select the policies or roles to be attached to the agency. Enter **OBS** in the search box and select **OBS OperateAccess**.
- Click **Next**, and select the authorization scope. By default, **All resources** is selected. Click **Show More** and select **Global resources**. Click **OK**.

5. Configure the agency created in the previous step for the ECS.

- In the navigation pane on the left, click  and choose **Compute** > **Elastic Cloud Server**.
- Select the ECS for which you want to configure the agency and click its name to switch to the basic information page.
- On the tab page that is displayed by default, click the edit icon next to **Agency** in the **Management Information** area, select the created agency, and save it.

12.3.2.2 Creating an OBS Bucket

Before configuring Backint Agent, you need to create an OBS bucket to store backups. The server where the SAP HANA database is located and the OBS bucket must belong to the same HUAWEI CLOUD account and be in the same region. If you have a qualified OBS bucket, skip this step.

1. Log in to the public cloud management console and select a desired region in the upper left corner.

2. In the navigation pane on the left, click  and choose **Storage** > **Object Storage Service**.

3. Click **Create Bucket** in the upper right corner.

4. Configure the bucket information as required. Note that:

- The server where the SAP HANA database is located and the OBS bucket must be in the same region.
- Select **Private** for **Bucket Policy**.

12.3.2.3 (Optional) Configuring a Lifecycle Rule

You can configure a lifecycle rule to periodically clear the expired files stored in the OBS bucket. For details, see **Configuring a Lifecycle Rule**. As to the file clearing frequency, the files need to be deleted every 30 days according to the SAP official document or you can configure it based on your backup policies.

12.3.2.4 Modifying the Backint Agent Configuration File

You can configure Backint Agent by modifying the parameters in its configuration file.

1. Run the following command to go to the directory where the configuration file is located:

cd /usr/sap/{*SID*}/SYS/global/hdb/opt/hdbconfig

Replace **{*SID*}** in the directory with the actual system ID. Example command:

/usr/sap/S99/SYS/global/hdb/opt/hdbconfig

2. Run the following command to modify the file:

vi hw-backint-agent.conf

You must set **BUCKET**, **LOGLEVEL**, and **SID** in the configuration file.

- **BUCKET**: specifies the name of the OBS bucket where Backint Agent reads and writes data. This OBS bucket will be used to store backups.
- **LOGLEVEL**: specifies to what extent the log details can be. You only need to set it to **INFO**. **DEBUG** is used only for troubleshooting after a fault occurs.
- **SID**: specifies the system ID (SID) used during SAP HANA system installation.
- **THREADNUM**: specifies the number of concurrent backup and restoration tasks. The value ranges from **1** to **20**. The default value is **8**. Set this parameter based on the server specifications.
- **BACKUPSIZE**: indicates the data volume uploaded by each thread during backup and restoration (unit: MB). The data volume can be set to a value ranging from **1** to **2047** (unit: MB). The default value is **200**.

NOTE

When Backint is used for backup or restoration, certain memory is occupied. Peak usage = 2 x THREADNUM x BACKUPSIZE. Configure these parameters properly based on the memory of the server. For oversized backup, the value of **BACKUPSIZE** cannot be too small. Backup size = **BACKUPSIZE** x 10000

The following example shows the valid content of the **hw-backint-agent.conf** file.

BUCKET=xxx

LOGLEVEL=INFO

SID=S01

THREADNUM=8

BACKUPSIZE=200

3. After the file is modified, press **Esc**, and then press **Shift** and **:** at the same time. Enter **wq!** to save and exit.

12.3.2.5 Configuring SAP HANA

You can use the same configuration for the backup of all types of objects (data, log, and catalog), or you can use different configurations for each type of objects. If you want to use different configurations for the backup of different types of objects, set different values for the parameters listed in **Table 12-2**. Otherwise, use the same configuration for the backup of all types of objects.

Use SAP HANA Studio or SAP HANA Cockpit to set the parameters in the **backup** part of the **global.ini** configuration file to the values shown in the following table. To make the changes take effect, you do not need to restart SAP HANA.

Replace **{*SID*}** in the directory with the actual system ID. Example:

/usr/sap/S99/SYS/global/hdb/opt/hdbconfig/hw-backint-agent.conf

Table 12-2 SAP HANA configurations

Parameter	Value	Description
enable_auto_log_backup	yes	Specifies whether to enable the automatic log backup.
catalog_backup_parameter_file (supported only by SAP HANA 2.0)	/usr/sap/{SID}/SYS/global/hdb/opt/hdbconfig/hw-backint-agent.conf	Specifies the configuration file for catalog backup.

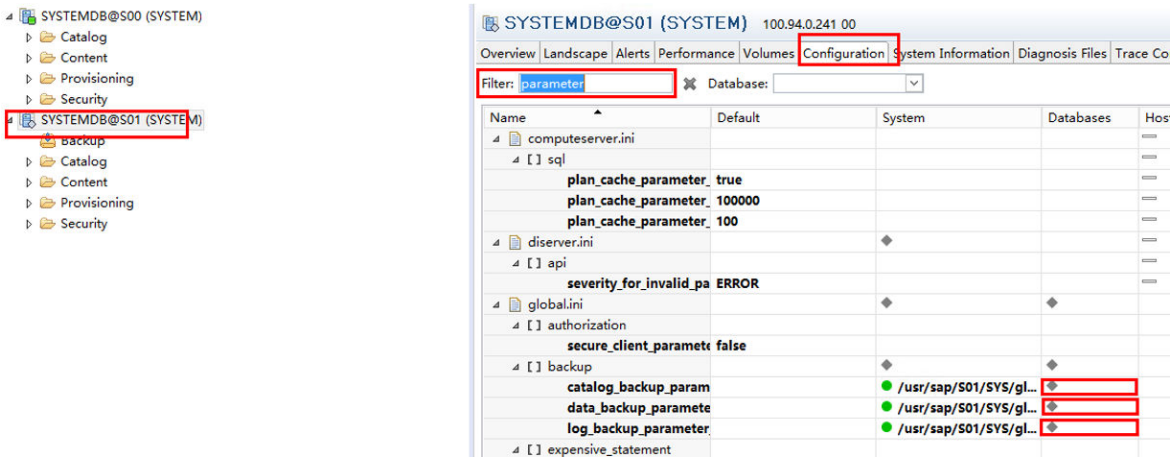
Parameter	Value	Description
catalog_backup_using_backint (supported only by SAP HANA 2.0)	true	Specifies whether to set the catalog backup method to Backint.
data_backup_parameter_file	/usr/sap/{SID}/SYS/global/hdb/opt/hdbconfig/hw-backint-agent.conf	Specifies the configuration file for data backup.
log_backup_parameter_file	/usr/sap/{SID}/SYS/global/hdb/opt/hdbconfig/hw-backint-agent.conf	Specifies the configuration file for log backup.
log_backup_using_backint	true	Specifies whether to set the log backup method to Backint.

The following uses SAP HANA 2.0 and SAP HANA Studio as an example to describe the configuration procedure.

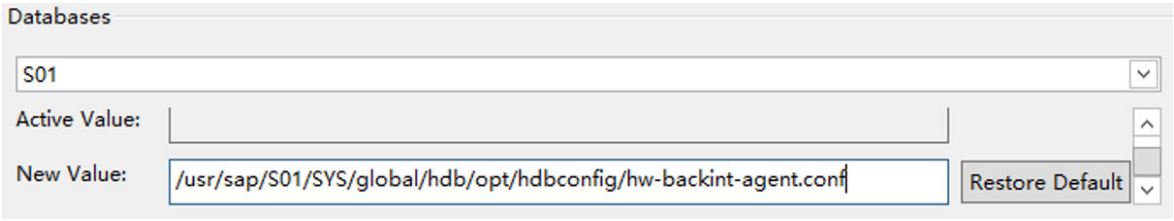
1. Open SAP HANA Studio and select a workspace if necessary. If there is no special requirement, retain the default settings. Right-click the blank area in the navigation pane on the left and select **Add System**.

2. In the displayed dialog box, enter the IP address of the server where SAP HANA is installed and configure required parameters.

3. In the navigation pane on the left, double-click the newly added system. In the **Filter** area on the **Configuration** tab, enter a parameter keyword and configure the system and database.



4. The following uses the tenant database as an example. On the page that is displayed, enter the corresponding value in the table and save the setting.



5. Repeat steps 3 and 4 until all the parameters listed in the table are configured.

For details about how to set other parameters, see the SAP official document.

After the configuration is complete, perform backup and restoration tests by referring to Installation Verification and Common Usage Examples to verify the installation and configuration.

12.3.3 (Optional) Upgrading Backint Agent

The installation script is required for upgrading Backint Agent. If the installation script is deleted by mistake, download the installation script by referring to **Downloading Backint Agent**.

1. Go to the **/tmp** directory.

cd /tmp

2. Run the following command as user **root** to upgrade Backint Agent. Enter the system ID of the server where Backint Agent is installed for *SID* in the command, for example, **bash install.sh --upgrade S99**.

bash install.sh --upgrade *SID*

The **install.sh** will:

- Install the Backint Agent of the latest version in the **/usr/sap/{*SID*}/SYS/global/hdb/opt/hw-backint-agent/**.
- Update the **hdbbackint** script to invoke Backint Agent of the latest version. The **hdbbackint** script cannot be modified.
- Download the latest **VERSION.txt** file.
- Generate the new **hw-backint-agent.conf** configuration file. The original **hw-backint-agent.conf** file is renamed and retained.
- Send a message to notify of **updating /usr/sap/{*SID*}/SYS/global/hdb/opt/hdbconfig/hw-backint-agent.conf** after the upgrade is finished.

After the upgrade, the parameters in the configuration file may be updated. You need to modify the configuration file by referring to **Modifying the Backint Agent Configuration File**.

In the HA scenario, you need to repeat the preceding operations to upgrade Backint Agent on the standby server.

NOTE

Before executing the upgrade command, ensure that no backup (including log backup) or restoration task is being executed. Otherwise, the running tasks may be affected.

12.4 Installation Verification and Common Usage Examples

12.4.1 Important Notes for Naming

Backups are uploaded to OBS buckets after Backint Agent is deployed. You need to follow the rules described in **OBS Naming Rules** when naming, for example, configuring **Backup Prefix**.

12.4.2 Backup

You can use SAP HANA Studio, SAP HANA Cockpit, or SAP HANA HDBSQL to back up the data.

Log backup can be triggered periodically after automatic backup is configured. Catalog can be automatically backed up when Backint Agent is deployed. For details about the configuration methods, see **Configuring SAP HANA**.

The following use a case where SAP HANA Studio is used to back up SAP HANA 2.0 and Backint Agent is deployed to make full backup for data, catalog, and log and store the backups to OBS as an example to describe the backup procedure.

1. Open SAP HANA Studio, right-click the system to be backed up on the left, choose **Backup and Recovery**, and select an option based on the actual requirements:

- Back Up System Database
- Back Up Tenant Database

2. For example, to back up a tenant database, select a tenant database and set **Destination Type** to **Backint**. You can customize **Backup Prefix**.

3. Confirm the backup information and click **Finish**. If the installation and configuration are successful, the backup progress is displayed until the backup is complete.

4. After the backup is complete, you can query the backup in OBS. You can view the backups through **OBS Browser+** or go to the Object Storage Service console to view the backups. The backup directories are as follows:

- System data backup directory: **obs://{BUCKET}/usr/sap/{*SID*}/SYS/global/hdb/backint/SYSTEMDB**
- Tenant data backup directory: **obs://{BUCKET}/usr/sap/{*SID*}/SYS/global/hdb/backint/DB_{*Tenant name*}**

5. After accessing the preceding directories, you can find the corresponding backup files based on *Backup Prefix* you set. Examples of file names for different types of backups are as follows:

- Full data backup: **{***Backup Prefix***}_databackup**_*x_x*.
- Incremental data backup: **{***Backup Prefix***}_databackup_incremental**_*x_xxxxx_xxxxx*

- Differential data backup: **{***Backup Prefix***}_databackup_differential**_*x_xxxxx_xxxxx*
- Catalog backup: **log_backup_0_0_0_0**
- Log backup: **log_backup**_*x*_**0**_*xxxxx_xxxxx*

You can view the backup files in different directories. You can find the corresponding backup files based on the backup time and backup ID. If the corresponding files are found, the backup is successful. The following backup file directory is an example.

obs://xxx/usr/sap/S99/SYS/global/hdb/backint/DB_S30/COMPLETE_DATA_BACKUP_databackup_2_1/1626157625497.bak

12.4.3 Restoration

You can use SAP HANA Studio, SAP HANA Cockpit, or SAP HANA HDBSQL to restore the data for SAP HANA.

The following use a case where SAP HANA Studio is used to restore the data in SAP HANA 2.0 and Backint Agent is deployed to make full backup for data, catalog, and log and store the backups to OBS as an example to describe the restoration procedure.

1. Open SAP HANA Studio, right-click the system which data restoration needs to be performed for on the left, choose **Backup and Recovery**, and select an option based on the actual requirements:

- Recovery System Database
- Recovery Tenant Database

2. For example, to restore the data in the tenant database, select a tenant database and select a restoration type:

- Recover the database to its most recent state
- Recover the database to the following point in time
- Recover the database to a specific data backup

3. For example, to restore the database to its most recent state, select **Search for the backup catalog in Backint only** in **Recover using the backup catalog**.

4. The tenant database needs to be shut down during the restoration. In the dialog box that is displayed, click **OK**.

5. After selecting a backup file, you can click **Check Availability** to check whether the backup file is available. If the icon turns into green, the backup file is available. Click **Next**. Confirm the information and click **Next**.

6. If you want to check the availability of differential backups and log backups during the restoration, select **Third-Party Backup Tool (Backint)** and click **Next**.

7. Confirm the information restored and click **Finish**. If the installation and configuration are successful, the restoration progress is displayed until the restoration is complete.

12.4.4 Restoring Data in New SAP HANA System

Backups in OBS can be used to restore the data (backed up from the production system) to the development or testing system and restore the data for the standby node in the disaster recovery (DR) scenario. You need to manually copy the backup files in OBS to the local path of the new SAP HANA system and then perform the restoration. This restoration method is simple, but it will consume a large storage space and take a long time when the number and size of backup files are large. You can deploy Backint Agent in the new SAP HANA system to enable the new system to connect to the OBS bucket and directly use the backups in the bucket to perform restoration. The specific scenarios are as follows.

12.4.4.1 Unchanged SID and Tenant Name

1. If the new system and the source system are not in the same region, you need to follow the instructions described in **Configuring Cross-Region Replication** to replicate the backups of the source system to the OBS bucket in the region where the new system is located, and perform the subsequent operations.

2. Install and configure Backint in the new system.

Note: If the source system is running and the backups of the source system need to be restored to the new system, do not configure Backint Agent in the new system to back up the logs and catalogs. Otherwise, the backups of the source and new systems will be stored in the same OBS bucket, which will affect the data restoration for the new system.

3. Select a restoration type by referring to **Restoration** based on the actual requirements.

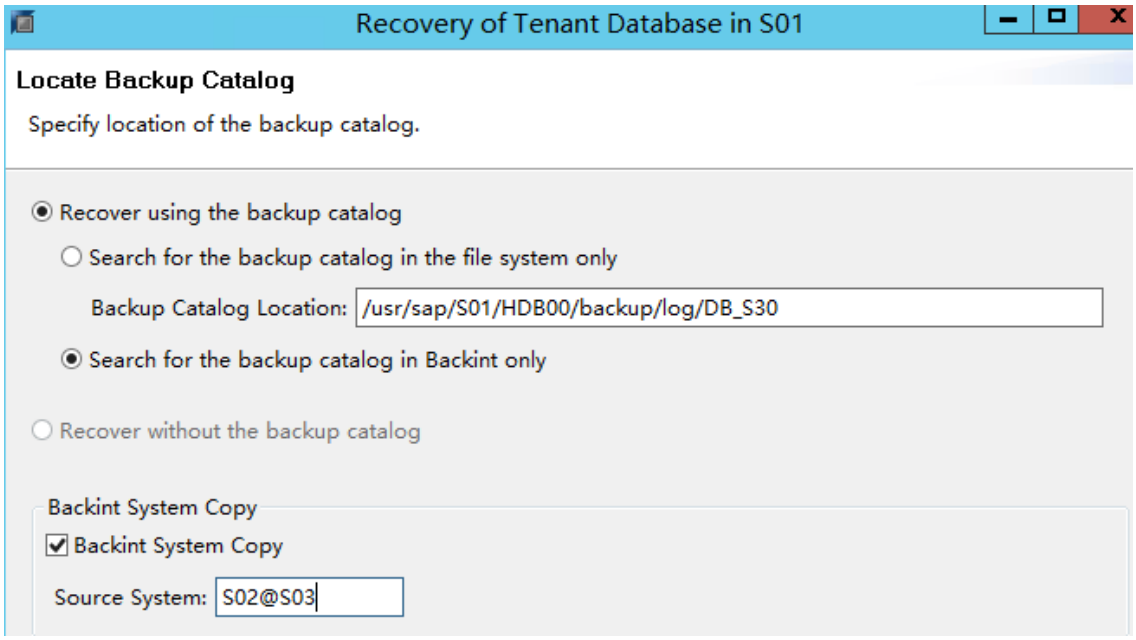
4. If the source system is running and the backups of the source system need to be restored to the new system, configure Backint Agent in the new system to back up the logs and catalogs based on the actual requirements after data restoration is completed and configure a new OBS bucket to store the backups.

12.4.4.2 Changed SID or Tenant Name

1. If the new system and the source system are not in the same region, you need to follow the instructions described in **Configuring Cross-Region Replication** to replicate the backups of the source system to the OBS bucket in the region where the new system is located, and perform the subsequent operations.

2. Install and configure Backint in the new system.

3. Select a restoration type by referring to **Restoration** based on the actual requirements, select **Backint System Copy**, and specify the SID of the source system. Note: If the source system has multiple tenants, you need to specify both the tenant name and SID in the format of **{***Tenant name***}@{***SID***}**. The following figure uses **Recover the database to its most recent state** as an example. Select **Search for the backup catalog in Backint only** and set **Source System** to **S02@S03**.



12.4.5 Deleting Backups

You can use SAP HANA Studio, SAP HANA Cockpit, or SAP HANA HDBSQL to delete a data backup or the backups earlier than the specified one.

The following use a case where SAP HANA Studio is used to delete backups of SAP HANA 2.0 and Backint Agent is deployed to make full backup for data, catalog, and log and store the backups to OBS as an example to describe the backup deletion procedure.

1. Open SAP HANA Studio and double-click **Backup** on the left. On the page that is displayed, select **Backup Catalog** and select the target tenant from **Database**. The corresponding backups are displayed.

2. Right-click a backup to perform the following operations:

- To delete a single data backup, click **Delete Data Backup**.
- To delete the data backups earlier than the specified one, click **Delete Older Backups**. **Third-Party Backup Tool (Backint)** need to be selected in the subsequent step.

3. If you want to delete all backups, select **Catalog and Backup Location**. If you want to delete only the backups from the catalog, select **Catalog**.

4. Click **Next**, confirm the information, and click **Finish**.

12.5 Logs and Troubleshooting

If an error occurs during backup or restoration, the error information will be displayed in SAP HANA Studio or SAP HANA Cockpit. Therefore, you need to check whether the error information exists in the SAP HANA Studio or SAP HANA Cockpit. The error information may be displayed in the **backup.log** and **backint.log** files provided by SAP HANA. When the multi-tenant database is used, you must specify the database name.

If an error occurs, view the following logs:

- SAP HANA backup.log: contains information about operations such as SAP HANA backup and restoration.
- SAP HANA backint.log: contains the information about operations to Backint Agent and other external backup tools.
- Backint Agent log file: contains Backint Agent operation events. Backint Agent log files are stored in **/var/log/huawei/backint/**. The default log level is **INFO**. **DEBUG** is used only for troubleshooting after a fault occurs.

12.6 Uninstalling Backint Agent

The installation script is required for uninstalling Backint Agent. If the installation script is deleted by mistake, download the installation script by referring to **Downloading Backint Agent**.

1. Go to the **/tmp** directory.

cd /tmp

2. Run the following command as user **root** to uninstall Backint Agent. Enter the system ID of the server where Backint Agent is installed for *SID* in the command, for example, **bash install.sh --uninstall S99**.

bash install.sh --uninstall *SID*

The **install.sh** script performs the following operations:

- Delete the **/usr/sap/{*SID*}/SYS/global/hdb/opt/hw-backint-agent** directory and all files in it.
- Delete the **/usr/sap/{*SID*}/SYS/global/hdb/opt/hdbconfig** directory and all files in it.
- Delete the **/usr/sap/{*SID*}/SYS/global/hdb/opt/hdbbackint** file.
- Delete the log files in **/var/log/huawei/backint**.

In the high availability (HA) scenario, you need to repeat the preceding operations to uninstall Backint Agent on the standby server.

13 Best Practices for Uploading SAP Backups to the OBS Bucket

13.1 Overview

13.1.1 Object Storage Service

Object Storage Service (OBS) is a cloud storage service that provides capabilities for massive, secure, reliable, and cost-effective data storage. With OBS, you can easily create, modify, and delete buckets, as well as upload, download, and delete objects.

OBS provides super large storage capacity that can store any type of files and is suitable for websites, enterprises, developers, and common subscribers. As a web service, OBS provides service interfaces over Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS). You can use OBS Console and OBS client to access and manage data stored on OBS from any computer connected to the Internet anytime, anywhere. Besides, OBS supports REST APIs, facilitating data management and development of several types of upper-layer service application. As a cloud service, OBS features flexible expansion and allows the infrastructure to be deployed in multiple regions, while maintaining high reliability. Therefore, you can access OBS in specific regions according to your service needs and experience rapid access speed at cost-effective prices.

For further details about OBS, see **OBS Product Introduction**.

13.1.2 Script

This script is developed using Python and applies to the Linux operating system. This script is used to upload local files to the OBS bucket and save copies locally. This script calls the obsutil to upload files to the OBS bucket.

obsutil is a command line tool for accessing OBS. You can use this tool to perform common configurations in OBS, such as creating buckets, uploading and downloading files/folders, and deleting files/folders. If you are familiar with command line interface (CLI), obsutil is recommended as an optimal tool for batch processing and automated tasks.

For more information about obsutil, see **Introduction to obsutil**.

13.1.3 Dependency

The script runs on the Linux operating system and is compatible with all Linux versions. The script invokes obsutil. **Table 13-1** shows the dependency between the running environment of the obsutil and python.

Table 13-1 Dependency versions and description

Component/Module	Requirement	Remarks	Handling Method
Python	The version of Python must be Python3.	Incompatibility occurs when Python2 is used.	Upgrade the Python version.

13.2 Preparations Before the Upload

13.2.1 Preparing the Environment

Before using obsutil, you need to register a cloud service account, use the OBS service, create an IAM user, and obtain access keys (AKs and SKs). To ensure account and resource security, you are not advised to use the registered account to access OBS. Through the Identity and Access Management (IAM) service, you can create a user who has the permission to access OBS resources and perform operations on the OBS client.

Procedure

Step 1 **Register an account and use OBS.**

Step 2 **Create an IAM user.**

Step 3 **Create Access Keys (AKs and SKs).**

----End

13.2.2 Downloading Software

This section describes how to download and decompress the **obsutil_adapter.zip** software package.

Procedure

Step 1 Log in to a server as user **root** using a key or password.

Step 2 On the CLI, download the **obsutil_adapter.zip** package and decompress it to the **/opt/huawei** directory. The download address of software packages varies by region. For details, see **Table 13-2**. The CN-Hong Kong is used as an example here.

wget https://obs-sap-ap-southeast-1.obs.https://obs-sap.obs.myhuaweicloud.com/obsutil_adapter/obsutil_adapter.zip.com/obsutil_adapter/obsutil_adapter.zip -P /opt/huawei

Table 13-2 Required software package

Name	Description	How to Obtain
obsutil_adapter.zip	Software package	**CN-Hong Kong**: wget https://obs-sap-ap-southeast-1.obs.myhuaweicloud.com/obsutil_adapter/obsutil_adapter.zip -P /opt/huawei
		AP-Bangkok: wget https://obs-sap-ap-southeast-2.obs.myhuaweicloud.com/obsutil_adapter/obsutil_adapter.zip -P /opt/huawei
		SA-Johannesburg: wget https://obs-sap-af-south-1.obs.af-south-1.myhuaweicloud.com/obsutil_adapter/obsutil_adapter.zip -P /opt/huawei

cd /opt/huawei

unzip obsutil_adapter.zip -d obsutil_adapter/

NOTE

- **obsutil_adapter.py**: Script to be uploaded and executed. This script calls obsutil.
- **obsutil_adapter.cfg**: Configuration file of this script
- **obsutil**: the obsutil client
- The log directory is **/var/log/huawei/obsutil_adapter**.

----End

13.2.3 Modifying the Configuration File

Prerequisites

You have prepared the OBS bucket name.

Procedure

Step 1 Log in to a server as user **root** using a key or password.

Step 2 Run the following command to modify the **obsutil_adapter.cfg** configuration file and save it:

vi /opt/huawei/obsutil_adapter/obsutil_adapter.cfg

Step 3 Modify the configuration parameters by referring to **Table 13-3** and save the modification.

Table 13-3 Parameters

Parameter	Description	Example Value
obs_path	Path of the OBS bucket to which the backups will be uploaded. You can enter the OBS bucket name and specify a path after the bucket name. The format is *bucket name*/*bucket path*. Use the OBS bucket path you need.	obs-sap/hana
retry_time	Number of retransmission attempts. For example, if its value is set to **3**, it indicates that if the upload fails, the system retries twice. If the upload still fails, the script exits. **NOTE** The value of **retry_time** must be an integer.	3
modified_interval	Upload interval. The unit is minute. The files that are modified within this period will not be uploaded. For example, if its value is set to 5, files that are modified within the last 5 minutes will not be uploaded. **NOTE** The value of **modified_interval** must be an integer.	5
reserve_time	File reservation period. The unit is minute. For example, if its value is set to 2880, the files in the **backup_archive** can be stored for 2880 minutes at most locally. **NOTE** The value of **reserve_time** must be an integer.	2880

Parameter	Description	Example Value
backup_path	Path that stores file backups. After the backup of a file is complete, the file is moved to **backup_archive**. **NOTE** Multiple paths are supported. Use commas (,) to separate paths. For example: **/hana/backup/data**, **/hana/backup/log**	/hana/backup/data
backup_archive	Files that are successfully uploaded are archived in this directory. When this script is executed, the files in the **backup_archive** directory are queried first. If the difference between the current time and the file creation time exceeds the value of **reserve_time**, the files will be deleted. Otherwise, files will be backed up in the **backup_path** directory. After the backup of files is complete, the files will be archived in **backup_archive**.	/hana/backup/archive

NOTE

- The **backup_path** and **backup_archive** directories must be independent from each other. Each directory cannot be a subdirectory of another one. Ensure that the disk space of the two directories is sufficient for storing backup files.
- To ensure the integrity of uploaded files, you cannot run the multiple scripts that have been uploaded at the same time. Otherwise, the script execution fails.

----End

13.2.4 Initializing obsutil

Before using obsutil, you need to configure the interconnection between obsutil and OBS, including the endpoint and access keys (AK and SK) of OBS. You can use obsutil to perform operations on OBS buckets and objects only after obtaining the OBS authentication.

Prerequisites

- The obsutil has been downloaded. For details, see **Downloading Software**.
- The access keys (AK and SK) have been obtained. For details, see **Step 3** in **Preparing the Environment**.

Procedure

Step 1 Run the following commands to initialize obsutil:

chmod +x obsutil

./obsutil config -i=*ak* **-k=***sk* **-e=***endpoint*

- **ak**: indicates the tenant access key, that is, the AK in **Creating Access Keys (AK and SK)**.

- **sk**: indicates the tenant secret key, that is, the SK in **Creating Access Keys (AK and SK)**.
- **endpoint**: The IP address of an endpoint varies from region to region. **Table 13-4** lists OBS endpoint IP addresses. For more information about OBS endpoints, see **Regions and Endpoints**.

Table 13-4 Endpoints

Region Name	Endpoint Region	Endpoint
CN-Hong Kong	ap-southeast-2	obs.ap-southeast-1.myhuaweicloud.com
AP-Bangkok	ap-southeast-1	obs.ap-southeast-2.myhuaweicloud.com
AF-Johannesburg	af-south-1	obs.af-south-1.myhuaweicloud.com

NOTE

- After running the preceding commands, a configuration file **.obsutilconfig** is automatically generated in the same directory of the user who executes obsutil commands (the ~ directory in Linux). **.obsutilconfig** contains all the configuration information of obsutil. For details about the parameters, see **Parameter Description**.
- The **.obsutilconfig** file contains user AK and SK information. To prevent key leakage, the obsutil file is hidden by default. You can run the **ls -a** command in the directory of the user who executes obsutil commands to view the file.

Step 2 After the configuration is complete, you can run the following command to check the connectivity:

./obsutil ls -s

Check the command output.

- If the command output contains **Bucket number is:**, the configuration is correct.
- If the command output contains **Http status [403]**, the access keys are incorrectly configured.
- If the command output contains **A connection attempt failed**, the OBS service cannot be connected. Check whether the network is normal.

----End

13.3 Uploading Backups to the OBS Bucket

13.3.1 Manually Running the Script

Prerequisites

Before running the script, ensure that the database backup is complete. This script cannot identify whether the backup file is complete.

Procedure

Step 1 After modifying the configuration file, run the following commands to start the upload:

cd /opt/huawei/obsutil_adapter

python3 obsutil_adapter.py

NOTE

After the script is executed, log in to OBS to view the uploaded file. The directory name on OBS is determined by time, and the structure is *Bucket path/Year and month/Day//*, for example, **obs-sap/hana/201808/22/**.

----End

13.3.2 Calling by Other Scripts

If other scripts need to call this script, ensure that its software package has been downloaded and decompressed. Before running the script, ensure that the database backup is complete. This script cannot identify whether the backup file is complete.

Procedure

Step 1 Run the following command to call the script:

cd /opt/huawei/obsutil_adapter && python3 obsutil_adapter.py

NOTE

In the preceding command, **/opt/huawei/obsutil_adapter** indicates the path where the script is decompressed. Change it based on the site requirements.

----End

13.3.3 Configuring Scheduled Tasks

If a backup task needs to be executed periodically, configure scheduled tasks using crontab on Linux to call the script. Before running the script, ensure that the database backup is complete. This script cannot identify whether the backup file is complete.

Procedure

Step 1 Edit the **crontab** file:

crontab -e

Set the scheduled task. Change the time according to the actual situation, save the modification, and exit.

If the following information is displayed, the script will be called at 21:30 o'clock every day:

```
30 21 * * * cd /opt/huawei/obsutil_adapter && python3 obsutil_adapter.py >/dev/null 2>&1
```

NOTE

The scheduled task execution time is defined by the customer. Ensure that the scheduled task execution time is later than the backup time.

Step 2 View scheduled tasks. If you can find the scheduled tasks in **Step 1** by running the following command, it indicates that the setting is successful.

crontab -l

----End

13.4 FAQs

13.4.1 How Do I Download a Backup File of a Day from the OBS Bucket?

This topic describes how to use obsutil to download a backup file of a day from the OBS bucket to the local host.

NOTICE

- Ensure that source objects in the OBS bucket do not change. Otherwise, the download may fail or data may be inconsistent.
- If the objects to be downloaded are in the OBS Archive storage class, you must restore the objects first. Otherwise, the download fails.

Procedure

Step 1 Log in to a server as user **root** using a key or password.

Step 2 Run the following command to recursively download all files and folders (including the folder itself) in the bucket to a local path:

./obsutil cp obs://*obs_path/Year/Month/Day***/***Local path* **-r -***tempFileDir= a specified path* **-f**

In the preceding command:

- **obs_path**: OBS bucket path, for example: **obs-sap/hana**
- *Year/Month/Day*: directory of a folder in the OBS bucket. For example: **201905/28**.
- *Local path*: path where the files are stored on the local host. For example: **src1**.

- *tempFileDir= a specified path*: Directory for storing temporary files during multipart download. The default value is the value of **defaultTempFileDir** in the configuration file. You can also specify a path.

  NOTE

  - Temporary files generated during multipart download are stored in this directory. Ensure that the user who runs obsutil commands has the write permission on the path.
  - The available space of the path must be greater than the size of the objects to be downloaded.

For example, in the **obs-sap** bucket, download the backup files of May 28, 2019 to the local path **src1**. The command is as follows:

./obsutil cp obs://obs-sap/hana/201905/28 /src1 -r -tempFileDir=/hana/backup -f

For more information about obsutil, see **Introduction to obsutil**.

----End

13.4.2 How Can I Periodically Delete Backup Files from a Bucket or Change the Storage Class of Backup Files?

This section applies to the following scenarios:

- Some files uploaded periodically need only to be retained for only one week or one month. You need to delete the files after they expire.
- Files are seldom accessed after a certain period of time. These files need to be transitioned to Infrequent Access or Archive storage or be deleted.

You can create lifecycle rules for objects in the preceding scenarios.

NOTICE

- Use an independent bucket to store backup files to prevent important files from being deleted by mistake during the periodical deletion.
- Apply the lifecycle rules to the entire bucket when configuring the lifecycle management function to manage the lifecycle of all objects in the bucket.

Procedure

Step 1 For details, see **Configuring a Lifecycle Rule**.

----End

14 Best Practices of the SAP ASE Solution

14.1 Purpose

This document describes the HUAWEI CLOUD SAP ASE solution, including information about resource selection, system backup, high availability (HA), disaster recovery (DR), and offline system migration. HUAWEI CLOUD provides various cloud services to ensure stable and secure running of the SAP Adaptive Server Enterprise (ASE) system.

SAP ASE is a high-performance SQL database. It uses a relational model to power transaction-based applications, meeting tenants' advanced requirements on database performance, reliability, and efficiency. With SAP ASE, you can quickly and confidently perform online transaction processing (OLTP). You can build transaction-based modern applications and improve the running speed of applications inside enterprises and on the cloud. The high-performance SQL database server adopts the relational management model to deliver performance, reliability, and efficiency that various industries increasingly require.

The HUAWEI CLOUD SAP ASE solution has the following advantages:

- Rich specifications: Provides Elastic Cloud Servers (ECSs) of various specifications to meet requirements of different application scenarios. You can select appropriate specifications based on user quantity and performance requirements.

- Lower costs: Provides multiple economical ECSs.
- Higher efficiency: The entire SAP system can be deployed on HUAWEI CLOUD, facilitating SAP system O&M and improving the overall running efficiency of the SAP system.

HUAWEI CLOUD uses the built-in license for the SAP ASE database. HUAWEI CLOUD provides a high-performance enterprise-level relational database management system for SAP ASE, which is suitable for mission-critical services and data-intensive environments. For additional information about running SAP ASE on HUAWEI CLOUD, see **SAP Note #2644322**, which requires **SAP Service Marketplace** credentials.

14.2 Resource Planning

14.2.1 Network Planning

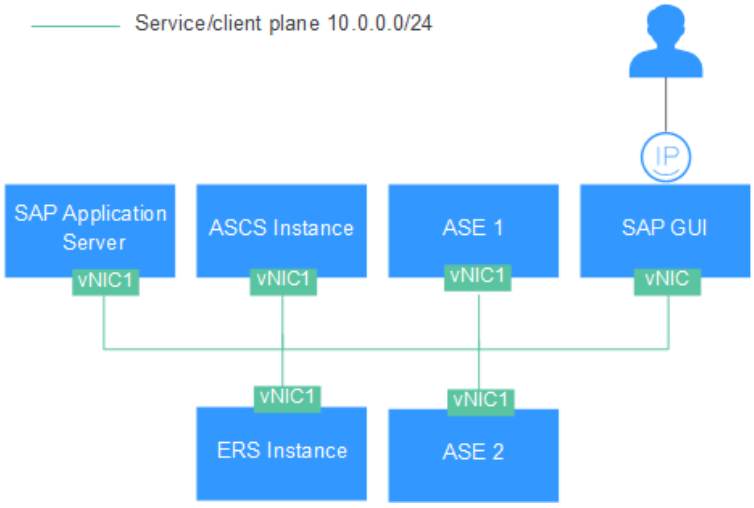
HUAWEI CLOUD Virtual Private Cloud (VPC) service provides an isolated virtual network environment for cloud servers, that can be configured and managed by users. It improves cloud resource security and simplifies network deployment. In a VPC, you can define subnets, IP address ranges, routing tables, and security group rules.

Plan the number of VPCs, number of subnets, IP network segments, and interconnection modes based on your service requirements. For details, see the **Network Planning** section in VPC documentation.

HADR Network Planning

Use only one NIC to build the service/client network communication plane. **Figure 14-1** shows the HADR network plan.

Figure 14-1 HADR network planning



When deploying the SAP ASE system, you need to plan public and private IP addresses. For details, see **Table 14-1**.

NOTE

The following node names, network segments, and IP addresses are provided for reference only. Set them based on the actual network plan.

Table 14-1 Network planning

IP Type	Node Name	NIC	IP Address	Description
Public IP	ase001	eth0	10.0.0.4	Configure the network plane as needed.
	ase002	eth0	10.0.0.5	
Virtual IP	-	-	10.0.0.6	The virtual IP address is optional. The active and standby ECSs where the ASE database resides use the same virtual IP address. You can access the ASE ECSs through the virtual IP address or a private IP address. The virtual IP address must be an unused IP address that is in the same network plane as the public IP address.

Application Server Network Planning

or details about SAP application network planning, see the network planning section in the **Network Plane Planning**.

14.2.2 Server Specifications

This section describes ASE ECS specifications. For details about the ECSs for SAP applications powered on the SAP ASE database, see the **ECS Flavors for SAP NetWeaver**. You can choose from ECSs with the following specifications based on the business scale and application system requirements.

Small-scale

This scheme is applicable to the small enterprise resource planning (ERP) system or other SAP systems, such as PI, SAP Portal product portfolio, CRM, and SRM. M3 ECSs are suitable for development, testing, and production systems. **Table 14-2** lists the specifications.

Table 14-2 Scheme for small ERP

System	vCPUs	Memory (GB)	Flavor
Development	4	32	m3.xlarge.8
Testing	4	32	m3.xlarge.8

System	vCPUs	Memory (GB)	Flavor
Production	8	64	m3.2xlarge.8

Medium-scale

This scheme is applicable to the medium-sized ERP system. M3 ECSs are suitable for development, testing, and production systems. **Table 14-3** lists the specifications.

Table 14-3 Scheme for medium-sized ERP

System	vCPUs	Memory (GB)	Flavor
Development	4	32	m3.xlarge.8
Testing	8	64	m3.2xlarge.8
Production	16	128	m3.4xlarge.8

Large-scale

This scheme is applicable to the large ERP system. M3 ECSs are suitable for development, testing, and production systems. **Table 14-4** lists the specifications.

Table 14-4 Scheme for large ERP

System	vCPUs	Memory (GB)	Flavor
Development	8	64	m3.2xlarge.8
Testing	16	128	m3.4xlarge.8
Production	32	256	m3.8xlarge.8

14.2.3 File Systems

This section describes the file system planning of the SAP ASE database. For details, see **Table 14-5**. For SAP applications powered on the ASE database, the file system planning is the same as that of the applications using the HANA database. For details about the file system planning for SAP applications, see the **SAP NetWeaver User Guide**.

For the single-node ASE system, each file system needs an EVS disk.

Table 14-5 ASE database file system planning

File System	I/O	Space	Description
/sybase/<DBSID>	High I/O	20 GB	ASE software directory (shared or local)
/sybase/<DBSID>/sybsystem	Ultra-high I/O	10 GB	System directory
/sybase/<DBSID>/sybtemp	Ultra-high I/O	10 GB	Temporary directory of the SAP ASE database
/sybase/<DBSID>/saptemp	Ultra-high I/O	20 GB	SAP software temporary directory
/sybase/<DBSID>/sapdiag	Ultra-high I/O	10 GB	SAP tools directory
/sybase/<DBSID>/sapdata_<n>	Ultra-high I/O	> 80 GB for ABAP, or > 40 GB for Java	Data file directory
/sybase/<DBSID>/saplog_<n>	Ultra-high I/O	> 40 GB for ABAP, or > 20 GB for Java	Log file directory
/sybase/<DBSID>/sybsecurity	Ultra-high I/O	10 GB	ASE audit log

14.3 Deployment

14.3.1 Preparing Resources

Before deploying an SAP ASE system on HUAWEI CLOUD, you need to prepare the installation media, licenses, and operating system (OS).

Installation Media

Table 14-6 lists the required installation media.

Table 14-6 Installation media

Installation Media	How to Obtain
Software Provisioning Manager 1.0	Visit the SAP Software Downloads website.
UC Kernel (folder K_<Version>_<N or U>_<OS>)	
ASE Database Software (database patches)	

Installation Media	How to Obtain
Installation Export (folders EXP*)	

Licenses

Bring-Your-Own-License (BYOL) is used for authorization. You can log in to the SAP help portal to apply for the license as required.

You also need to purchase some HUAWEI CLOUD resources.

OSs

The OS is SUSE Linux Enterprise Server For SAP Applications 12 SP3. SAP ASE database is mainly used for SAP NetWeaver 7.4 and 7.5. The Kernel version is 740 or later, and the ASE version is 16.0 or later.

For details about the version mapping, see the **OS Support List** on the SAP website.

14.3.2 Creating and Configuring Networks

Create a VPC and configure IP address segments, subnets, and security groups based on actual requirements. For details, see **Creating and Configuring a VPC**.

14.3.3 Creating an ECS

Purchase an ECS. For details, see **Purchasing an ECS with Customized Configurations**.

14.3.4 (Optional) Other Configuration

Perform the following operations as needed:

- If you need a virtual IP address, see **Virtual IP Address Overview**.
- You can share an EVS disk with multiple servers. For details, see **Attaching a Shared Disk and Binding a Floating IP Address**.
- If you want to connect the network of Huawei Cloud to your local network, see **Connecting the VPC to the IDC**.

14.3.5 Installing SAP ASE

Use **Software Provisioning Manager (SWPM)** to install the SAP ASE software. The installation procedure varies according to the system. For details, see **helpful documents** on the SAP website.

14.4 HA Solution

14.4.1 Database HA

The typical HA solutions commonly used by the ASE database are available on HUAWEI CLOUD. For example, both High-availability and disaster recovery (HADR) and SUSE® Linux Enterprise High Availability Extension (HAE) can be used to achieve ASE system HA. HUAWEI CLOUD also provides HA solutions for both the databases and applications to ensure stable and reliable running of the SAP ASE system.

NOTE

The databases and applications of the SAP ASE production system is installed in distributed mode.

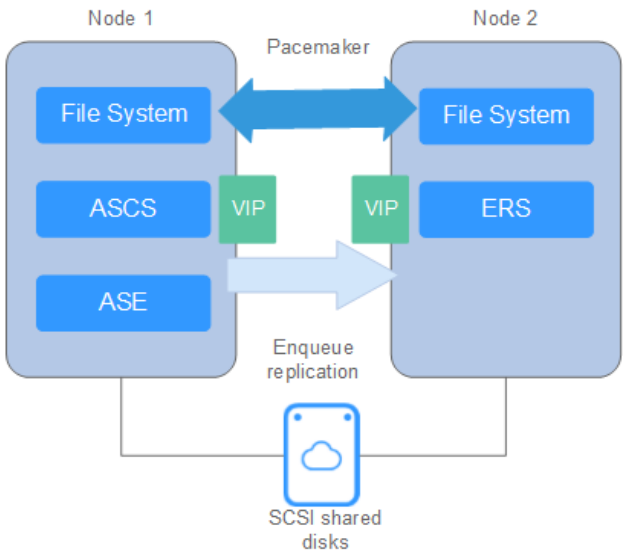
Solution 1: HADR (recommended)

HADR is an SAP solution designed for the ASE database. The HADR solution consists of two database nodes (active and standby) and one management node (Fault Manager). If the active database node is faulty, the standby node automatically takes over the workloads, ensuring high service availability. Generally, HA solutions use shared storage. However, in the HADR solution, resources of all nodes are isolated, which effectively reduces the risk of single points of failure. For details, see the **HADR User Guide** on the SAP website.

Solution 2: SUSE HAE

SUSE HAE is an integrated suite of open source clustering technologies that enables you to implement highly available physical and virtual Linux clusters and eliminates single points of failure. It ensures high availability and manageability of critical resources, including data, applications, and services. Therefore, it helps you maintain business continuity, protect data integrity, and reduce unplanned downtime for your mission-critical Linux workloads. **Figure 14-2** shows the architecture of SUSE HAE for the SAP ASE system. For details, see the **SUSE official document**.

Figure 14-2 SUSE HAE scheme

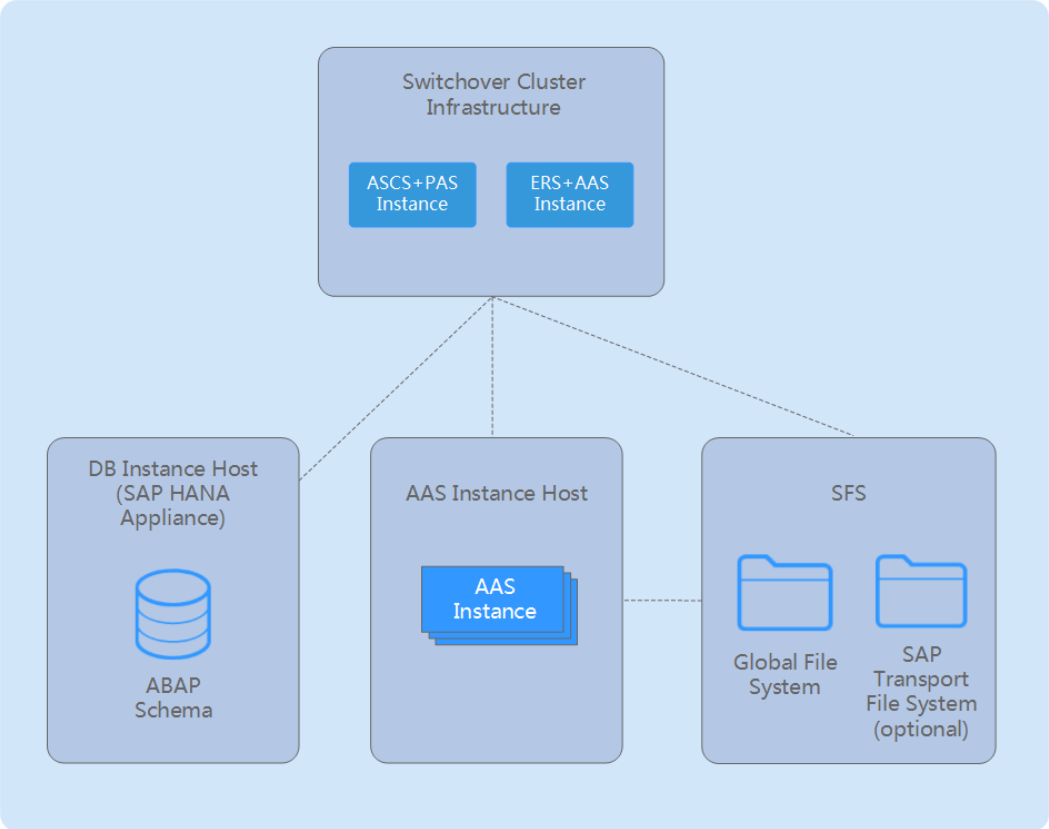


14.4.2 Application HA

Applications and databases in the SAP ASE production system are installed in distributed mode, so that the application layer and HA scheme are the same as those of the SAP HANA system.

The HA solution of SAP ASE system applications is provided in the **SAP NetWeaver User Guide**. For details, see **Distributed HA Deployment Mode**.

Figure 14-3 SAP Application HA Deployment



14.5 Backup

14.5.1 Backing Up the Database

HUAWEI CLOUD provides Scalable File System (SFS), Object Storage Service (OBS), Volume Backup Service (VBS), and Cloud Server Backup Service (CSBS) for backing up the SAP ASE system. As the SAP application servers and the ASE database servers are different, use different service combinations to back up the servers. You can use the tool provided by the ASE database or a third-party tool to back up and restore the database. The backup files can be stored in and restored from SFS file systems or OBS buckets.

SFS and OBS are suitable storage media for the database backup. SFS is a network attached storage (NAS) service that provides scalable high-performance file storage. Use SFS as the storage medium of ASE database backup files. OBS is a

stable, secure, efficient, and easy-to-use cloud storage service. It provides highly reliable storage capabilities at relatively low costs. Use OBS as the archive storage. You can upload SFS data to OBS.

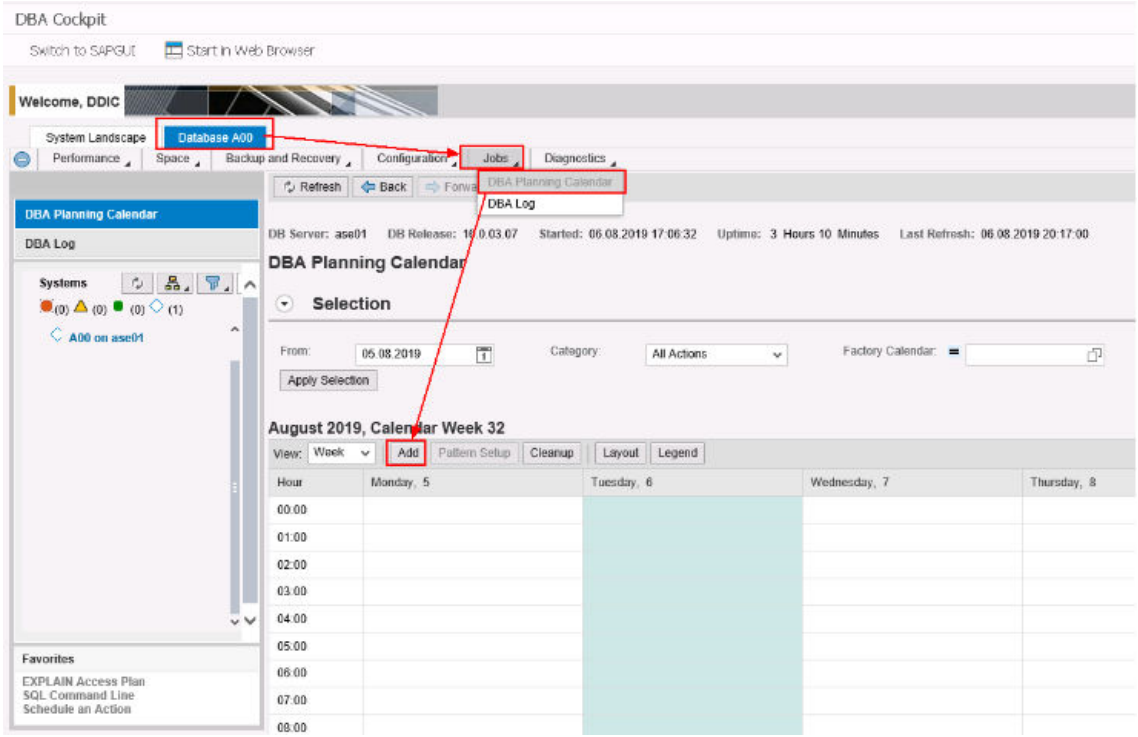
HUAWEI CLOUD provides a free backup uploading script to periodically archive backup files in SFS file systems to OBS buckets, and clear the files in the SFS file systems based on user-defined rules. For details, see **Best Practices for Uploading SAP Backups to the OBS Bucket**.

Solution 1: Using DBA Cockpit

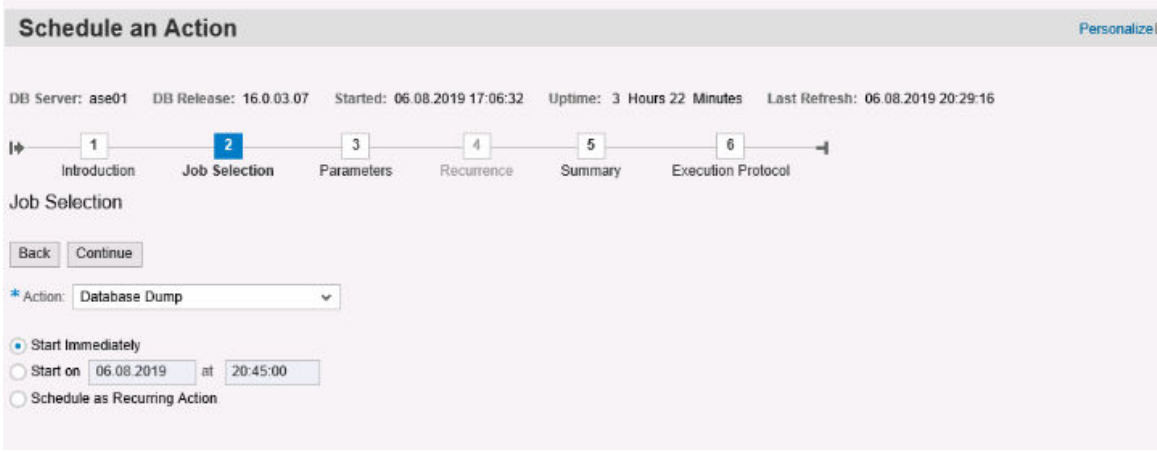
DBA Cockpit is dedicated to monitoring and managing databases of SAP systems. It simplifies the database administration. DBA Cockpit is integrated in SAP NetWeaver by default.

The procedure is as follows:

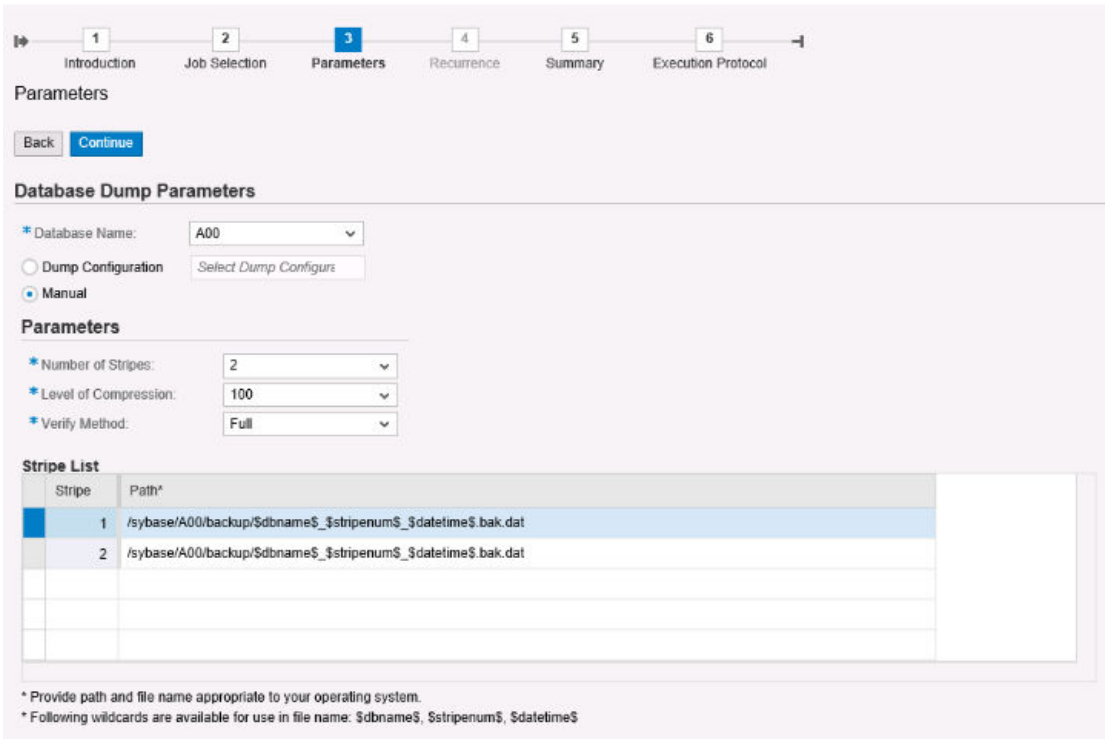
1. Log in to the SAP GUI.
2. Run the **TCODE dbacockpit** command.
3. Choose **Database** > **Jobs** > **DBA Planning Calendar** > **Add**.



4. Choose **Job Selection** > **Database Dump** > **Start Immediately**. You can also choose **Schedule as Recurring Action** as needed.



5. Configure backup parameters.



6. On the **Summary** page, review the parameter configuration and click **Execute**.
7. After the backup is complete, check the backup directory and backup logs.

For details about how to back up the ASE database and logs, see the following notes:

- Note 1588316 - SYB: Configure automatic database and log backups
- Note 1558958 - SYB - DBA Cockpit Correction Collection SAP Basis 7.02 - 7.30

For more details about DBA Cockpit, see **The DBA Cockpit** on the SAP website.

Solution 2: Running the DUMP DATABASE Commands

The procedure is as follows:

1. Run the following dump command to back up my_database:

   DUMP DATABASE my_database TO '/local_dump_dir/my_database.dump'
2. Run the following command to back up transaction logs of my_database:

   DUMP TRANSACTION my_database TO '/local_dump_dir/ my_database.$timestamp.dumptran'
3. Back up the local files to SFS or OBS.
4. Restore the database.
   a. Run the following command to stop the database before the restoration:

      dbcc dbreboot(shutdown_load, my_database)
   b. Run the following commands to restore the database:

      LOAD DATABASE my_database FROM "my_database.dump"

      LOAD TRAN my_database FROM "my_database.$timestamp.dumptran"
   c. Run the following command to start the restored database:

      online database my_database

   NOTE

   For incremental backup, set **trunc log on chkpt** to **false**. The command is as follows:

   sp_dboption my_database, "trunc log on chkpt", false

For details about how to run the DUMP DATABASE commands to back up the database, see the "Backing Up Databases" section in **Backup and Recovery** on the SAP website.

Solution 3: Using a Third-party Backup Tool

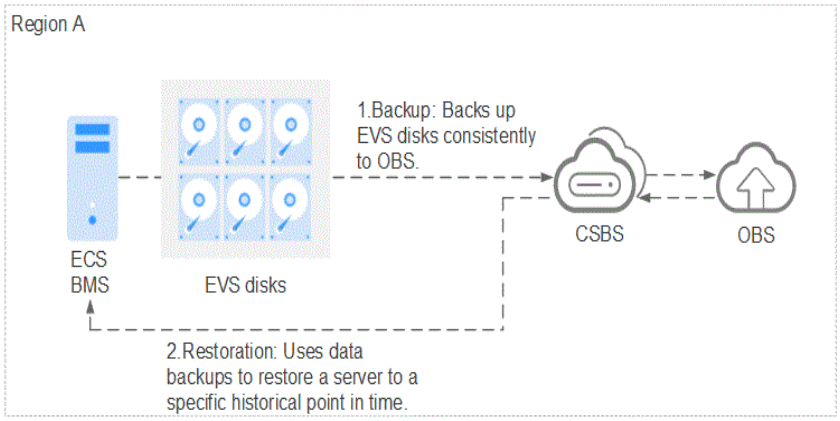
Use a third-party backup tool, such as AnyBackup. For details, see the **EISOO website**.

14.5.2 Backing Up Application Servers

The application servers are stateless. Use CSBS to back up SAP application servers on HUAWEI CLOUD.

CSBS offers the backup protection service for ECSs and Bare Metal Servers (BMSs). It works based on the consistent snapshot technology for disks. With CSBS, you can use backup data to restore server data, enhancing data integrity and service continuity.

For details, see **Cloud Server Backup Service User Guide**.



14.6 DR

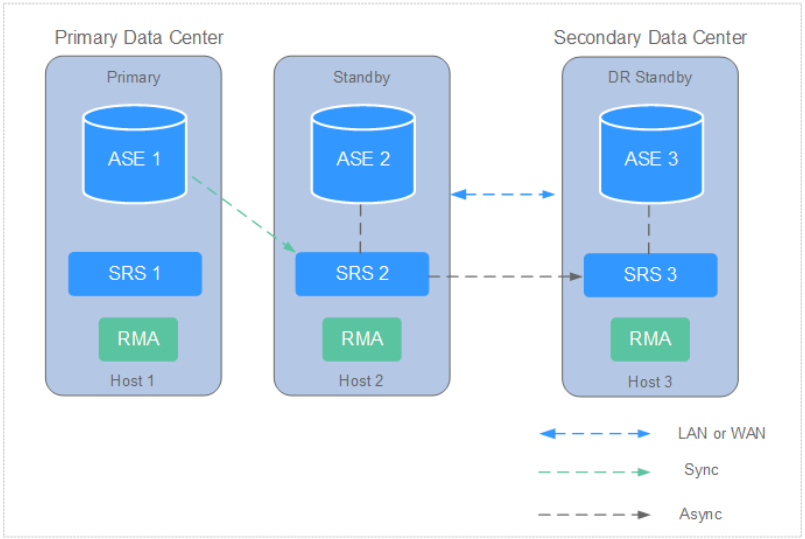
14.6.1 Database DR

In the SAP ASE system, the DR strategies for applications and databases are different.

- On HUAWEI CLOUD, use SDRS for the DR of SAP application servers.
- For the ASE database, use the HADR scheme or HUAWEI CLOUD SDRS. For details about the SDRS, see the **Storage Disaster Recovery Service User Guide**.

Figure 14-4 shows the HADR scheme of the ASE database.

Figure 14-4 Database DR scheme



Description

The SAP ASE production system is deployed in HA mode. The HADR scheme facilitates synchronous replication between the primary and standby nodes to ensure data consistency. The asynchronous replication is implemented between the standby node and the standby DR node.

The DR system is deployed in a different area from the production system. The two areas are connected through private lines. For more details about HADR, see **HADR with SAP ASE** on the SAP website.

NOTE

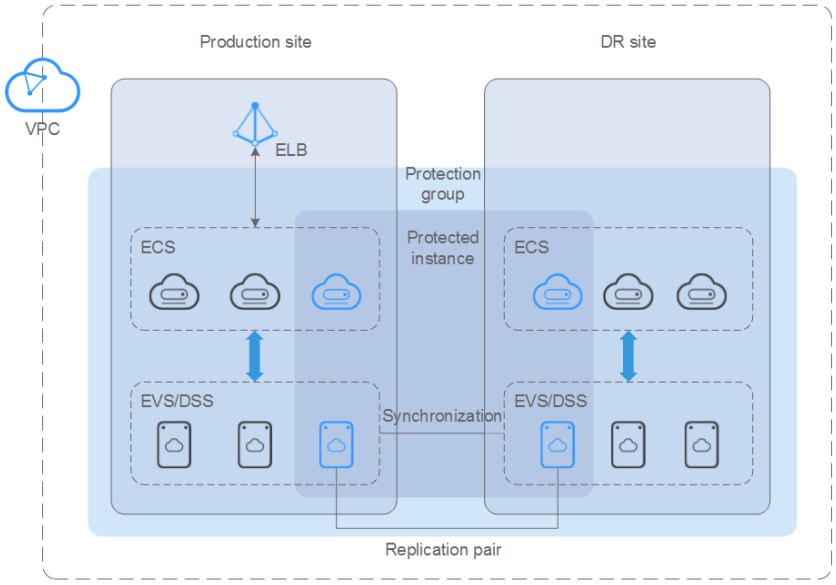
The primary, standby, and standby DR nodes must have the following in common:

- OS and patch level
- SAP ASE version
- ASE database parameter configuration

14.6.2 Application Server DR

Use SDRS for application server DR on HUAWEI CLOUD. SDRS supports ECS, Elastic Volume Service (EVS), and Dedicated Distributed Storage Service (DSS). SDRS uses multiple technologies, such as storage replication, data redundancy, and cache acceleration, to ensure high data reliability and service continuity.

SDRS facilitates and accelerates DR of SAP ASE application servers. For more information, see the **Storage Disaster Recovery Service User Guide**.



NOTE

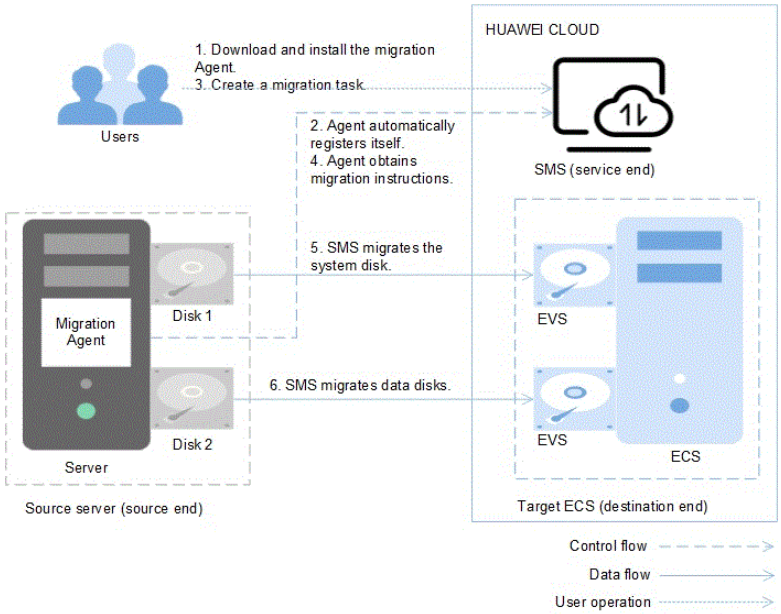
This service applies only to the systems running on HUAWEI CLOUD. To backup and recover on-premises servers to HUAWEI CLOUD, deploy the application servers on HUAWEI CLOUD.

14.7 Cloud Migration

14.7.1 Migrating Application Servers to HUAWEI CLOUD

You can migrate an existing SAP ASE system to HUAWEI CLOUD. There are migration solutions for different systems.

Use HUAWEI CLOUD Server Migration Service to migrate application servers. For details, see the **Server Migration Service User Guide**.



NOTE

This solution applies only to the scenario where the source and target application servers are the same. If you need to change the application server software version or perform heterogeneous database migration, you need to reinstall the application servers.

14.7.2 Migrating the Database to HUAWEI CLOUD

14.7.2.1 Homogeneous Migration

HUAWEI CLOUD ECSs and BMSs can run the ASE database. You have many optional methods to migrate the offline database to HUAWEI CLOUD.

Homogeneous migration refers to the migration where the source server OS is same as the target OS (versions can be different), and the ASE database version and patch do not change.

You can select a homogeneous migration solution as needed. **Table 14-7** describes the optional schemes.

Table 14-7 Migration solutions

Solution	Description
Database backup and restoration	The operation is simple, but the service downtime is long. **NOTE** The downtime includes the time for offline backup, backup uploading, and restoration.
Using HADR for migration	The service downtime is minimized, but the configuration is complex. The administrator must be familiar with the ASE database.

Solution	Description
HUAWEI CLOUD Server Migration Service	SMS supports batch migration and does not require ASE database administrators. However, the downtime of this scheme is long, which is mainly for incremental data synchronization.

Solution 1: Database backup and restoration

The procedure for backing up and restoring the database is as follows:

Step 1 On HUAWEI CLOUD, plan the subnet for the target end, configure security group policies, and build a target system that has the same OS, database, and application servers as the source system.

Step 2 Stop the services on the source system and back up the ASE database offline.

Step 3 Copy the database backup files from the source system to the file system in the target system. You can use OBS to transfer the files. Upload the files to Huawei Cloud OBS using **obsutil** and then download the file to the target server.

Step 4 Import the uploaded backup file to the target database.

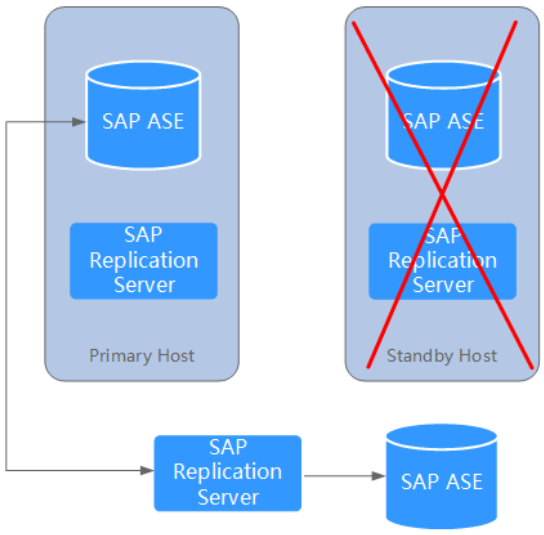
Step 5 Verify data integrity and switch the database services to the target system.

----End

Solution 2: Using HADR for migration

Figure 14-5 shows the HADR migration scheme.

Figure 14-5 Using HADR for migration



The procedure is as follows:

Step 1 On HUAWEI CLOUD, create the a subnet, configure security group policies, and build a target system that has the same OS, database, and application servers as the source system.

Step 2 Configure the data replication from the source system to the target system. For details, see **SAP HADR Users Guide**.

Step 3 After the synchronization is complete, stop services in the source system and switch them to the target system.

----End

Solution 3: HUAWEI CLOUD Server Migration Service

Perform the following steps to use HUAWEI CLOUD Server Migration Service:

Step 1 On HUAWEI CLOUD, plan the subnet for the target end, configure security group policies, and build a target system that has the same OS, database, and application servers as the source system.

Step 2 Prepare for the migration. Install the migration Agent on the source server, enable the ports required for migration, and provide user information used for migration.

Step 3 Migrate the database server. Use the Server Migration Tool to migrate the ECSs. You do not need to stop the services on the source server.

Step 4 Synchronize incremental data and switch the services. Synchronize incremental data to the target ECS and switch services to the target system after the synchronization.

Step 5 Monitor the target system for about one week to check if the target system is running properly. After the verification, release source system resources.

For details, see **Server Migration Service User Guide**.

----End

14.7.2.2 Heterogeneous Migration

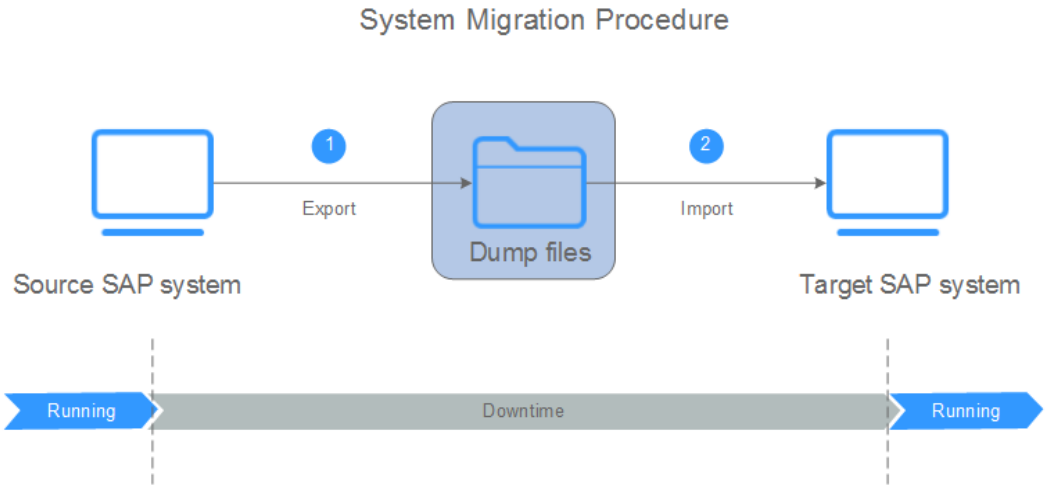
Heterogeneous migration refers to a migration where the source and target OSs, ASE databases, and SAP software versions are different. Use SAP R3load to import and export systems for heterogeneous migration.

Solution: SAP System Copy procedures (R3load)

Services must be stopped when R3load exports data. The service interruption duration depends on the database size. If the data to be imported and exported is more than 1 TB, the interruption time is long, causing great impacts on services. This solution is provided by SAP. If you encounter any problem during the migration, contact SAP technical support for solutions.

Figure 14-6 shows the procedure.

Figure 14-6 System migration



The procedure is described as follows:

Step 1 On HUAWEI CLOUD, create the a subnet, configure security group policies, and build the target system, including the database and application servers.

Step 2 Stop the source system services. Run the SWPM tool on the source server and use System Copy to export data. For details, see **SAP System Copy**.

Step 3 Upload the exported data to the file system of the target system.

Step 4 Run the SWPM tool in the target system and use System Copy to import data.

Step 5 Verify data integrity and switch the database services to the target system.

----End

15 Best Practices of SAP System Capacity Expansion

15.1 Overview

If the ECSs or EVS disks you purchased cannot meet your surging SAP business requirements, you can expand the resources on HUAWEI CLOUD.

This document describes how to expand ECSs and EVS disks on HUAWEI CLOUD.

15.2 Before You Start

15.2.1 Expansion Scenario

This section describes the capacity expansion of ECSs and EVS disks.

ECS Expansion

- **Modifying ECS Specifications**

  If the ECS specifications do not meet service requirements, you can modify the ECS specifications, including vCPUs and memory. **Table 15-1** describes an example where an SAP HANA ECS is upgraded from e1.4xlarge to e1.8xlarge.

Table 15-1 ECS specification modification

ECS Name	Before	After
hana01	e1.4xlarge	e1.8xlarge

- **Modifying Specifications and AZ/Region**

  If you need to migrate an ECS to another AZ or region when upgrading the ECS configuration, you can create a full-ECS image on HUAWEI CLOUD for the migration.
- **Modifying Specifications and AZ/Region with Low RTO**

  If you need to migrate an ECS to another AZ or region when upgrading the ECS configuration, use full-ECS image and backup recovery or system replication for the migration to reduce RTO.

EVS Disk Capacity Expansion

EVS disk capacity expansion is to expand the system disk or data disk to meet data storage requirements. For details about the pricing of a changed specification, see **Pricing of a Changed Specification**.

- For details about **Expanding EVS Disk Capacity (Without LVM)**, see **Table 15-2**.

  Table 15-2 EVS disk capacity expansion (without LVM)

EVS Disk Name	Capacity Before Expansion (GB)	Capacity After Expansion (GB)	Mount Point	Partition	File System	Mounting Directory
hana01-volume-sys	100	200	xvda	xvda1	ext4	N/A
hana01-volume-data	470	940	xvdb	None	xfs	/hana/data

  Description:

  A system disk of 100 GB and a data disk of 470 GB are attached to an ECS. The system disk and data disk are expanded to 200 GB and 940 GB, respectively.
- For details about the **Expanding EVS Disk Capacity (with LVM)**, see **Table 15-3**.

Table 15-3 EVS disk capacity expansion (with LVM)

EVS Disk Name	Capacity Before Expansion (GB)	Capacity After Expansion (GB)	Mount Point	File System	Mounting Directory	Directory Size Before Capacity Expansion	Directory Size After Capacity Expansion
hana-data01	400	800	vdb	xfs	/hana/data	696 GB	1.4 TB
hana-data02	400	800	vdc				

Description:

There are two data disks of 400 GB each attached to an ECS. A logical volume of 696 GB is divided from the LVM volume that is formed by the two data disks and mounted to the **/hana/data** directory. You can expand the **/hana/data** directory to 1.4 TB by expanding the capacity of EVS disks and the file system.

The following documents describe how to expand the capacity of an EVS disk.

- **Expansion Overview**
- **Post-Expansion Operations for a Windows EVS Disk**

15.2.2 Expansion Restrictions

This section describes the restrictions on capacity expansion. You need to learn these restrictions before capacity expansion.

ECS Expansion Restrictions

- SAP HANA ECSs: You can change ECS types E1 to E2, E2 to E1, and ET2 to E3. Other ECS type changes are not supported.
- SAP application ECSs: You cannot change ECS types H1 and M3.

Table 15-4 Supported ECS specification change

ECS Application Scenario	ECS Type Before Change	ECS Type After Change
SAP HANA	E1/E2	E1/E2
	ET2	ET2
	ET2	E3

ECS Application Scenario	ECS Type Before Change	ECS Type After Change
	e3	e3
SAP applications	H1	H1
	M3	M3
	c6	c6

EVS Disk Capacity Expansion Restrictions

Table 15-5 describes the restrictions to the EVS disk capacity expansion.

Table 15-5 EVS disk capacity expansion restrictions

Type	Restriction
Capacity expansion of EVS disks	Disk capacities can be expanded only, but cannot be reduced.
Capacity expansion of non-shared disks	Only certain ECS OSs support capacity expansion of non-shared disks in the **In-use** status. For details, see **Expanding an In-use EVS Disk**. If an EVS disk in the **In-use** status is to be expanded, the ECS OS to which the EVS disk is mounted must meet the requirements. If the server OS does not support capacity expansion of **In-use** disks, detach the disk and then expand its capacity. Otherwise, you may need to stop and then start the ECS after the expansion to make the expansion takes effect. You do not need to shut down the ECS if OSs are: SUSE Linux Enterprise Server 12 SP3 64bit SUSE Linux Enterprise Server 12 SP2 64bit SUSE Linux Enterprise Server 12 SP1 64bit
Capacity expansion of shared disks	A shared disk must be detached from the ECS before expansion, and the shared disk status must be **Available**.
Expansion increment	1 GB

NOTICE

When a disk has been put to use, you must check the disk partition style before expanding its capacity as follows:

- If the MBR partition style is used, the maximum disk capacity supported is 2 TB (2048 GB), and the disk space exceeding 2 TB cannot be allocated and used.
- With GPT, you can expand the capacity of a data disk to up to 32 TB. An EVS data disk supports up to 32 TB (32768 GB) so that you can expand the capacity of a data disk to up to 32 TB when the GPT partition style is used.

If the in-use partition style is MBR and the disk capacity needs to be expanded to over 2 TB, change the partition style from MBR to GPT. Ensure that the disk data has been backed up before changing the partition style because services will be interrupted and data on the disk will be cleared during this change.

15.2.3 Impact

This section describes the possible impacts of the capacity expansion.

Impact During Capacity Expansion

The ECS must be stopped when you change ECS specifications, which interrupts services.

To reduce the impact on the system running, you are advised to perform the capacity expansion during off-peak hours.

Impact After Capacity Expansion

None

15.3 Upgrading ECS Configuration

15.3.1 Modifying ECS Specifications

This section describes how to modify ECS specifications. In this section, a HANA database ECS is changed from e1.4xlarge to e1.8xlarge.

For details, see **General Operations of Modifying Specifications**.

NOTICE

- Modifying ECS specifications, such as the number of vCPUs or memory, may affect the ECS performance. The specifications of an ECS can be modified only when the ECS is in the **Stopped** state.
- Do not power on the ECS during the specification modification. Otherwise, the modification will fail. The new specifications take effect immediately after the modification is complete.

Preparations

To prevent NIC IP address flapping after the specification is modified, run the following commands on the ECS to delete the network rules files whose names contain **persistent** and **net** from the directory before modifying the specification:

rm -fr /etc/udev/rules.d/*net*persistent*.rules

rm -fr /etc/udev/rules.d/*persistent*net*.rules

Procedure

Step 1 Log in to HUAWEI CLOUD management console.

Step 2 Choose **Service List** > **Computing** > **Elastic Cloud Server**.

Step 3 In the ECS list, select the ECS whose specifications you want to modify and click **Stop**.

NOTE

Stop the SAP applications running on the ECS before stopping the ECS.

Step 4 In the displayed dialog box, click **Yes**.

Step 5 After the ECS is stopped, locate the row that contains the ECS, click **More** in the **Operation** column, and choose **Modify Specifications**.

Step 6 Select a flavor, for example: e1.8xlarge, and click **Submit**.

Step 7 Confirm the change details, select **I have read and agree to the Huawei Image Disclaimer**, and click **Submit Application**.

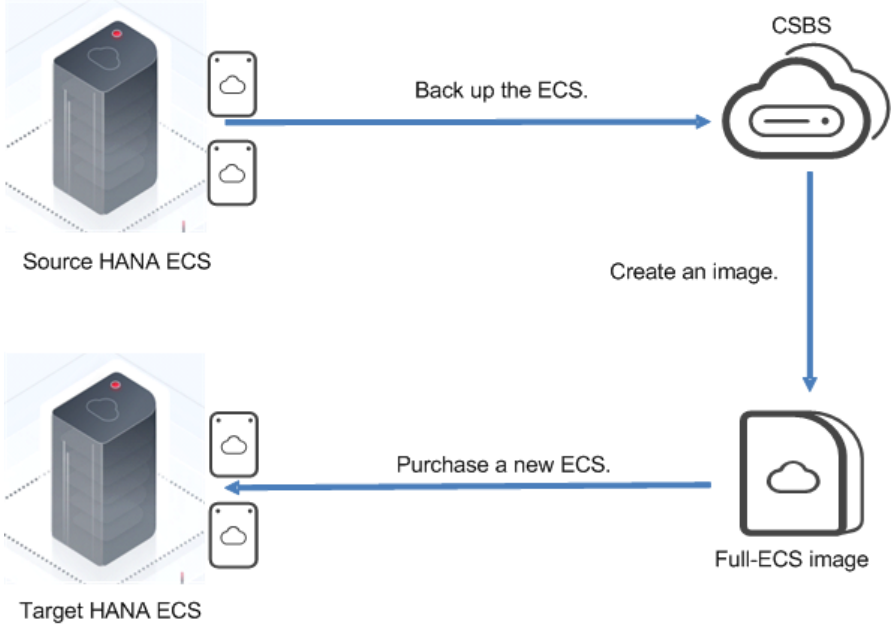
It takes about 2 minutes to change the ECS specification.

----End

15.3.2 Modifying Specifications and AZ/Region

If you need to migrate an ECS to another AZ or region when upgrading the ECS configuration, you can create a full-ECS image on HUAWEI CLOUD for the migration. **Figure 15-1** shows the migration process. This section uses a HANA database ECS as an example.

Figure 15-1 Full-ECS image backup



Procedure

Step 1 Stop the HANA database of the source system or shut down the source ECS.

Step 2 Create a full-ECS image using the ECS. For details, see **Creating a Full-ECS Image Using an ECS**.

Step 3 (Optional) If you need to purchase an ECS in another region, copy the newly created full-ECS image to the target region. For example, the original HANA server is an ECS in a CN East region, and you need to migrate it to a CN South region.

1. Log in to the management console and choose **Service List** > **Computing** > **Image Management Service**.
2. In the **Operation** column of the newly created image, click **More** and choose **Replicate**.
3. Set parameters as prompted. For details, see **Table 15-6**.

Table 15-6 Configuration parameters

Parameter	Description	Example Value
Replication Mode	Set this parameter as you need.	Across Regions
Name	Image name	copy_cn-east-2_hana_002
Destination Region	Select the region where you want to use the image.	CN South-Guangzhou
Destination Project	Select a project in the destination region.	cn-south-1

Parameter	Description	Example Value
IAM Agency	Select a created IMS agency as needed.	ims-rep

4. Click **OK** and wait until the replication is complete.

Step 4 Use the full-ECS image to purchase the target ECS. Select the specifications according to your requirements. You can change the disk size when setting disks to adapt to the new specifications. For details, see **Purchasing an ECS**.

Step 5 The IP address of the newly purchased ECS may be different from that in the source system. If necessary, update all the use of IP addresses in the source system. In addition, you need to log in to the new system and update the **/etc/hosts** file and host name information of the new system.

NOTE

You can modify the private IP address of an ECS. If the source and target systems are in the same VPC, you need to release the source ECS IP address first and then change the target ECS IP address to the released one. For details, see **Modifying a Private IP Address**.

Step 6 (Optional) Adjust the disk capacity after modifying ECS specifications. For details, see **Expanding EVS Disk Capacity**.

Step 7 Start the HANA database for verification.

Step 8 Check the connection between an SAP application and the HANA database and configure SAP HANA HA.

----End

15.3.3 Modifying Specifications and AZ/Region with Low RTO

If you want to reduce the RTO when using a full-ECS image to migrate the HANA database, use the backup recovery or data replication function, such as HANA system replication (HSR). Perform these operations during off-peak hours. The following uses the HANA database as an example to describe how to migrate data with a lower RTO.

Procedure

Step 1 Create a full-ECS image for the ECS. For details, see **Creating a Full-ECS Image Using an ECS**.

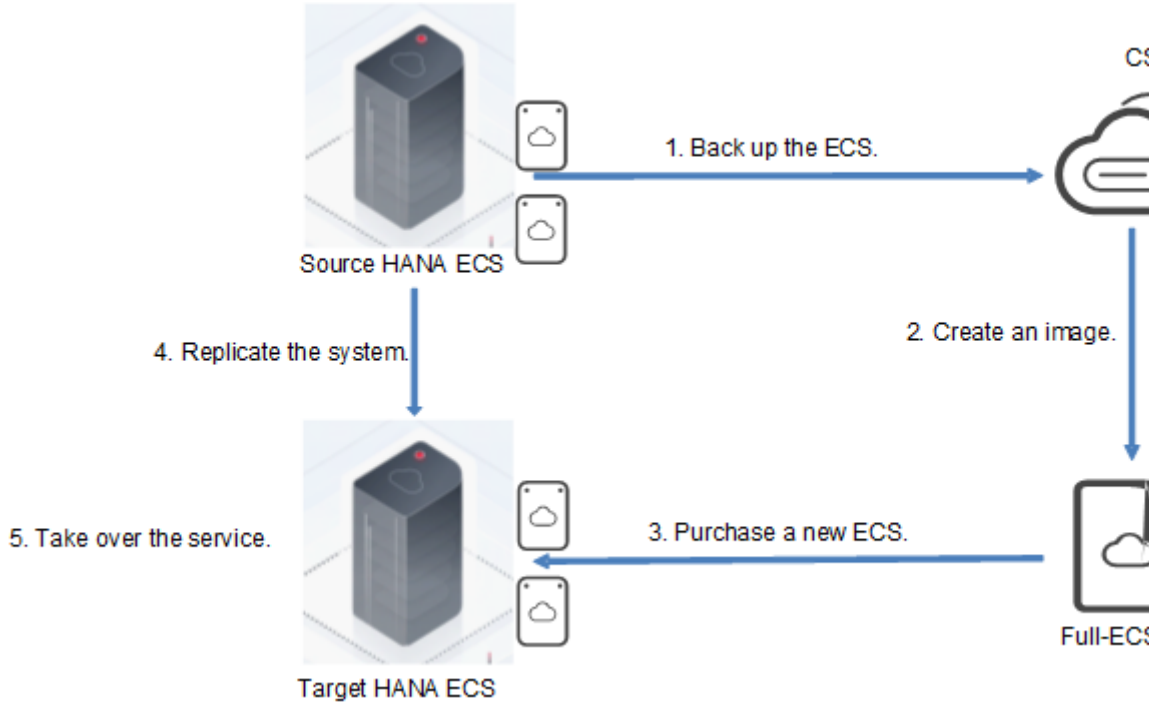
Step 2 Purchase a HANA database ECS using the full-ECS image. For details about how to create the image, see **Step 2** to **Step 7**.

Step 3 Migrate data from the source system to the target system. Use the backup recovery or the HSR function.

- Using HSR for the migration

  After the HANA database ECS is provisioned, use HSR to synchronize data. **Figure 15-2** shows the scheme. For details, see **SAP HANA Administration Guide**. Configure system replication and synchronize the data. Perform database takeover on the target ECS and modify the address mapping between the SAP application server and the database ECS.

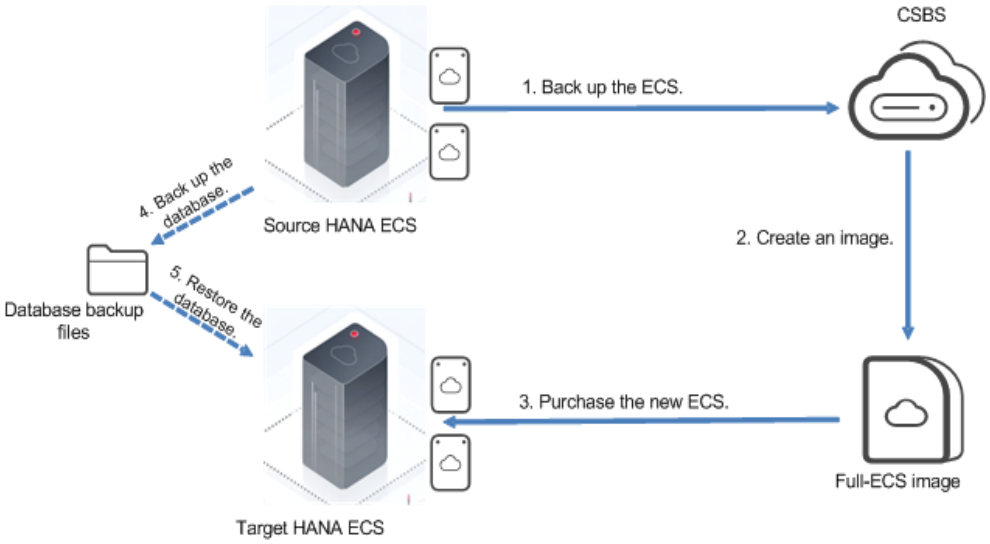
Figure 15-2 Full-ECS backup and system replication



- Using HANA backup recovery for the migration

  After the target ECS is provisioned, stop the source database service to ensure data consistency. Back up the HANA database ECS (including log files) using full-ECS backup, transfer backup data to the target system, and use the HANA database recovery function to import the backup data to the target system. **Figure 15-3** shows the scheme.

Figure 15-3 Full-ECS migration and backup recovery



Step 4 Check connections between SAP applications and the HANA database and perform subsequent operations, such as configuring HANA HA.

----End

15.4 Expanding EVS Disk Capacity

15.4.1 Expanding EVS Disk Capacity (Without LVM)

This section describes how to expand the capacity of an EVS disk that does not have an LVM logical volume. In the following example, a 100-GB system disk and a 470-GB data disk are mounted to an ECS, and the system and data disks are expanded to 200 GB and 940 GB, respectively.

Procedure

Step 1 Expand the EVS disk capacity.

1. Log in to HUAWEI CLOUD management console.
2. Choose **Service List** > **Computing** > **Elastic Cloud Server**.
3. In the ECS list, click the name of an ECS.
4. Under the **Disks** tab, click next to the system disk name.
5. Click the system disk ID to go to the system disk details page.
6. In the upper right corner of the page, click **Expand Capacity**.
7. Enter the capacity to be added based on the site requirements. For example: 100 GB and click **Next**.
8. Confirm the configuration information and click **Submit**.

   The system disk capacity expansion is complete.
9. Expand the data disk capacity by following step **Step 1.1** to **Step 1.8**.

Step 2 Expand partitions.

1. Log in to the ECS as user **root**.
2. Run the following commands to check the disk capacity after the expansion:

   lsblk

   df -Th

   If information similar to the following is displayed, the disk capacity has been expanded to 200 GB and 940 GB, but the mounted directory and **/hana/data** directory are not expanded. Expand partitions and file systems of the expanded EVS disks.

```
hana01:~ # lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0  200G  0 disk
└─xvda1 202:1    0  100G  0 part /
xvdb    202:16   0  940G  0 disk /hana/data
hana01:~ # df -Th
Filesystem     Type      Size  Used Avail Use% Mounted on
devtmpfs       devtmpfs  463G     0  463G   0% /dev
tmpfs          tmpfs     694G   80K  694G   1% /dev/shm
tmpfs          tmpfs     463G   42M  463G   1% /run
tmpfs          tmpfs     463G     0  463G   0% /sys/fs/cgroup
/dev/xvda1     ext4       99G  4.3G   90G   5% /
tmpfs          tmpfs      93G   16K   93G   1% /run/user/0
/dev/xvdb  _   xfs       470G   33M  470G   1% /hana/data
```


3. In this example, system disk **xvda** has a partition **xvda1**. You need to run **growpart** to expand the partition.

   growpart /dev/xvda 1

```
hana01:~ # growpart /dev/xvda 1
CHANGED: partition=1 start=2048 old: size=209713152 end=209715200 new: size=4194
28319,end=419430367
```

4. Run the following command to check whether the **xvda1** partition of the system disk has been expanded to 200 GB. The data disk has no partition. You do not need to run **growpart**. The default size is 940 GB.

   fdisk -l

```
hana01:~ # fdisk -l
Disk /dev/xvda: 200 GiB, 214748364800 bytes, 419430400 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x000ed768

Device     Boot Start       End   Sectors  Size Id Type
/dev/xvda1       2048 419430366 419428319  200G 83 Linux


Disk /dev/xvdb: 940 GiB, 1009317314560 bytes, 1971322880 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

Step 3 Run the following command to expand the capacity of the file system:

- Run the **resize2fs** command to expand the **ext2**, **ext3**, or **ext4** file systems.
- Run the **xfs_growfs** command to expand the **xfs** file system.

In this example, run the following commands:

resize2fs /dev/xvda1

xfs_growfs /hana/data

```
hana01:~ # resize2fs /dev/xvda1
resize2fs 1.42.11 (09-Jul-2014)
Filesystem at /dev/xvda1 is mounted on /; on-line resizing required
old_desc_blocks = 7, new_desc_blocks = 13
The filesystem on /dev/xvda1 is now 52428539 blocks long.

hana01:~ # xfs_growfs /hana/data
meta-data=/dev/xvdb              isize=256    agcount=4, agsize=30801920 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=0        finobt=0 spinodes=0
data     =                       bsize=4096   blocks=123207680, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal               bsize=4096   blocks=60160, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
data blocks changed from 123207680 to 246415360
```

----End

15.4.2 Expanding EVS Disk Capacity (with LVM)

This section describes how to expand the capacity of EVS disks that have an LVM logical volume. In the following example, two 400-GB data disks are mounted to an ECS. The two disks form a 696-GB LVM logical volume through data striping, and the logical volume is mounted to the **/hana/data** directory. This section

describes how to expand the **/hana/data** directory to 1.4 TB by expanding the capacity of the EVS disks and file systems.

Procedure

Step 1 Expand the capacity of the EVS disks by following the instructions provided in **Expanding EVS Disk Capacity (Without LVM)**.

Step 2 Run the following command to check the sizes of the two EVS disks after capacity expansion:

lsblk

If information similar to the following is displayed, the sizes of the two EVS disks are both 800 GB, but the size of the logical volume is still 696 GB.

```
hanaprd-0002:~ # lsblk
NAME                    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
vda                     253:0    0  100G  0 disk
└─vda1                  253:1    0  100G  0 part /
vdb                     253:16   0  800G  0 disk
└─vghanadata-lvhanadata 254:0    0  696G  0 lvm  /hana/data
vdc                     253:32   0  800G  0 disk
└─vghanadata-lvhanadata 254:0    0  696G  0 lvm  /hana/data

Disk /dev/vdb: 800 GiB, 858993459200 bytes, 1677721600 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/vdc: 800 GiB, 858993459200 bytes, 1677721600 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/vghanadata-lvhanadata: 696 GiB, 747324309504 bytes, 1459617792
sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 262144 bytes / 524288 bytes
```

Step 3 Run the following commands to expand the physical volume capacity and check the sizes of the physical volumes after the capacity expansion:

pvresize /dev/vdb

pvresize /dev/vdc

pvs

If information similar to the following is displayed, the sizes of the physical volumes are both 800 GB after the capacity expansion:


```
hanaprd-0002:~ # pvresize /dev/vdb
  Physical volume "/dev/vdb" changed
  1 physical volume(s) resized / 0 physical volume(s) not resized
hanaprd-0002:~ # pvresize /dev/vdc
  Physical volume "/dev/vdc" changed
  1 physical volume(s) resized / 0 physical volume(s) not resized
hanaprd-0002:~ # pvs
  PV         VG         Fmt  Attr PSize   PFree
  /dev/vdb   vghanadata lvm2 a--  800.00g 452.00g
  /dev/vdc   vghanadata lvm2 a--  800.00g 452.00g
```

Step 4 Run the following command to check the size of the LVM volume group:

vgdisplay

If information similar to the following is displayed, the size of the LVM volume group is expanded to 1.56 TB.

```
hanaprd-0002:~ # vgdisplay
  --- Volume group ---
  VG Name               vghanadata
  System ID
  Format                lvm2
  Metadata Areas        2
  Metadata Sequence No  4
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                1
  Open LV               1
  Max PV                0
  Cur PV                2
  Act PV                2
  VG Size               1.56 TiB
  PE Size               4.00 MiB
  Total PE              409598
  Alloc PE / Size       178176 / 696.00 GiB
  Free  PE / Size       231422 / 903.99 GiB
  VG UUID               40I95K-yAw2-ENOV-04rC-Yy5c-fKpU-vXYn3a
```

Step 5 Run the following command to add 696 GB to the logical volume:

lvextend -L +696G /dev/mapper/vghanadata-lvhanadata

If information similar to the following is displayed, the logical volume capacity is expanded by 696 GB.

```
hanaprd-0002:~ # lvextend -L +696G /dev/mapper/vghanadata-lvhanadata
  Using stripesize of last segment 256.00 KiB
  Size of logical volume vghanadata/lvhanadata changed from 696.00 GiB (178176 e
xtents) to 1.36 TiB (356352 extents).
  Logical volume lvhanadata successfully resized
```

Step 6 Run the following command to check the logical volume capacity:

lvdisplay


```
hanaprd-0002:~ # lvdisplay
  --- Logical volume ---
  LV Path                /dev/vghanadata/lvhanadata
  LV Name                lvhanadata
  VG Name                vghanadata
  LV UUID                tt0tqr-wMwv-caGg-eFwk-DXYv-1rtw-1feewu
  LV Write Access        read/write
  LV Creation host, time hanaprd-0002, 2018-10-25 15:38:11 +0800
  LV Status              available
  # open                 1
  LV Size                1.36 TiB
  Current LE             356352
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     8192
  Block device           254:0
```

Step 7 Run the following command to expand the capacity of the file system:

- Run the **resize2fs -d /hana/data** command to expand the **ext2**, **ext3**, or **ext4** file system.
- Run the **xfs_growfs -d /hana/data** command to expand the **xfs** file system.

In this example, run the following command:

xfs_growfs -d /hana/data

```
hanaprd-0002:~ # xfs_growfs -d /hana/data
meta-data=/dev/mapper/vghanadata-lvhanadata isize=256    agcount=32, agsize=5701
568 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=0        finobt=0 spinodes=0
data     =                       bsize=4096   blocks=182450176, imaxpct=25
         =                       sunit=64     swidth=128 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal               bsize=4096   blocks=89088, version=2
         =                       sectsz=512   sunit=64 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
data blocks changed from 182450176 to 364904448
```

----End

15.5 Verifying the Expansion

15.5.1 Verifying the ECS Expansion

After the capacity of an ECS is expanded, you can view the ECS specifications to check whether the capacity expansion is successful.

Procedure

Step 1 View the ECS specification.

1. Log in to HUAWEI CLOUD management console.
2. Choose **Service List** > **Computing** > **Elastic Cloud Server**.
3. In the ECS list, locate the row that contains the target ECS, check whether the ECS specification is successfully changed.
   - If yes, the expansion is successful.
   - If no, handle the problem by referring to **What Can I Do If the ECS Specifications Fail to Be Modified?**.

Step 2 Check disk attachment status.

After the specification is modified, disk attachment may fail. Therefore, check disk attachment after specification modification. If disks are properly attached, the specification modification is successful.

1. Log in to the ECS as user **root**.
2. Run the following command to view the disks attached before specification modification:

   fdisk -l| grep 'Disk /dev/'
3. Run the following command to view disks attached after specification modification:

   df -h| grep '/dev/'
4. Check whether the number of disks in **Step 2.2** and **Step 2.3** is the same.
   - If yes, the disk attachment is successful. No further action is required.
   - If no, the disk attachment failed. In such a case, go to **Step 2.5**.
5. Run the **mount** command to attach the disks.

   Example:

   mount /dev/vbd1 /mnt/vbd1

   In the preceding command, **/dev/vbd1** is the disk to be attached, and **/mnt/vbd1** is the path for disk attachment.

   NOTICE

   Ensure that **/mnt/vbd1** is empty. Otherwise, the attachment will fail.

   Run the following commands to check whether the number of disks in **Step 2.2** and **Step 2.3** are the same:

   fdisk -l| grep 'Disk /dev/'

   df -h| grep '/dev/'
   - If they are the same, no further action is required.
   - If no, contact customer service for technical support.

----End

15.5.2 Verifying the EVS Expansion

After the capacity of an EVS disk is expanded, you can view the EVS specifications and capacity indicators to check whether the capacity expansion is successful.

Procedure

Step 1 Log in to the ECS as user **root**.

Step 2 Run the following command to check the capacity of the **/hana/data** directory after the expansion:

df -Th

- Expanded EVS disk capacity (without the LVM logical volume).

  If information similar to the following is displayed, the capacity of the **/** and **/hana/data** directories have been expanded to 200 GB and 940 GB, respectively.

  ```
  hana01:~ # df -Th
  Filesystem     Type      Size  Used Avail Use% Mounted on
  devtmpfs       devtmpfs  463G     0  463G   0% /dev
  tmpfs          tmpfs     694G   80K  694G   1% /dev/shm
  tmpfs          tmpfs     463G   42M  463G   1% /run
  tmpfs          tmpfs     463G     0  463G   0% /sys/fs/cgroup
  /dev/xvda1     ext4      197G  4.3G  184G   3% /
  tmpfs          tmpfs      93G   16K   93G   1% /run/user/0
  /dev/xvdb      xfs       940G   33M  940G   1% /hana/data
  ```

- Expanded EVS disk capacity (with the LVM logical volume)

  If information similar to the following is displayed, the capacity of the **/hana/data** directory has been expanded to 1.4 TB.

  ```
  hanaprd-0002:~ # df -Th
  Filesystem                          Type      Size  Used Avail Use% Mounted on
  devtmpfs                            devtmpfs  172G  4.0K  172G   1% /dev
  tmpfs                               tmpfs     257G   80K  257G   1% /dev/shm
  tmpfs                               tmpfs     172G   10M  172G   1% /run
  tmpfs                               tmpfs     172G     0  172G   0% /sys/fs/cgroup
  /dev/vda1                           ext4       99G  4.3G   90G   5% /
  tmpfs                               tmpfs      35G   20K   35G   1% /run/user/0
  /dev/mapper/vghanadata-lvhanadata xfs        1.4T   35M  1.4T   1% /hana/data
  ```

----End

15.6 FAQs

15.6.1 What Can I Do If the ECS Specifications Fail to Be Modified?

View the failure cause using the Cloud Trace Service by performing the following operations:

1. Log in to the management console.
2. Under **Management & Governance**, click **Cloud Trace Service**.
3. In the navigation pane on the left, choose **Trace List**.
4. In the **Trace Name** column, locate the **resizeServer** event by resource ID.

   Resource ID is the ID of the target ECS.
5. Click **View Trace** in the **Operation** column to view the failure cause.

   If the fault cannot be rectified based on logs, contact customer service for technical support.

A Change History

Description	Released On
This issue is the fifteenth official release, which incorporates the following changes: Added section "SAP S/4HANA (1809) HA Deployment Best Practice". Removed the best practice of obsfs-enabled SAP HANA backup.	2023-11-06
This issue is the fourteenth official release, which incorporates the following change: Added section "SAP S/4HANA (1809) HA Deployment Best Practice".	2022-12-01
This issue is the thirteenth official release, which incorporates the following change: Updated the SAP Backint Installation Guide and SAP Monitoring Best Practices.	2022-06-24
This issue is the twelfth official release, which incorporates the following change: Added the *SAP Backint Installation Guide*.	2021-12-31
This issue is the eleventh official release, which incorporates the following change: Added the best practice of SAP migration from Xen to KVM.	2021-10-08

Description	Released On
This issue is the tenth official release, which incorporates the following changes: Added the "HUAWEI CLOUD SAP on Oracle Installation Best Practice". Added the "HUAWEI CLOUD SAP Business One on HANA Installation Best Practice". Added the "Best Practice of Using Block-Level Migration of SMS to Migrate SAP Applications and Databases Running on Linux Servers". Added the "Best Practice of Rsync-based SAP Disaster Recovery".	2021-08-31
This issue is the ninth official release, which incorporates the following change: Added the best practice of obsfs-enabled SAP HANA backup on HUAWEI CLOUD.	2021-08-04
This issue is the eighth official release, which incorporates the following change: Added SAP monitoring best practices.	2021-06-30
This issue is the seventh official release, which incorporates the following changes: Added the "SAP S/4HANA (1809) HA Deployment Best Practice". Added the "HUAWEI CLOUD SAP on DB2 Installation Best Practice". Added the "HUAWEI CLOUD SAP on SQL Server Installation Best Practice". Added the "Best Practice of SAP Disaster Recovery with SDRS".	2021-06-07
This issue is the third official release, which incorporates the following change: Added the best practices of migrating the SAP system to HUAWEI CLOUD.	2020-07-06
This issue is the second official release, which incorporates the following change: Added the best practices of uploading SAP backups data to the OBS bucket.	2019-07-12
This issue is the first official release.	2019-05-24

