Server Migration Service

Best Practices

Issue 11

Date 2024-12-16

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Moving Huawei Cloud ECSs from Multiple Accounts to a Single Account

Overview

Server Migration Service (SMS) can help you easily move Elastic Cloud Servers (ECSs) from multiple Huawei Cloud accounts to a single Huawei Cloud account, regardless of whether these ECSs are in the same region or in different regions.

Procedure

1. Obtain an AK/SK pair for the account you are migrating to. For details, see **How Do I Create an AK/SK Pair for an Account?**

   If you are migrating to the account of an IAM user, you need to obtain the required permissions and an AK/SK pair for the IAM user. For details, see **How Do I Create an AK/SK Pair for an IAM User?**

2. Install the SMS Agent on each ECS to be migrated. For details, see **How Do I Install the Agent on Source Servers?**

3. Run the SMS Agent and enter the AK/SK pair obtained in **1**.

   📖 **NOTE**

   > After the Agent is started, it reports details about the ECSs to SMS, so SMS can check whether the ECSs can be migrated.

4. Log in to the SMS console using the account you are migrating to. Choose **Servers** from the navigation pane and view the ECSs in the server list.

5. Create and run migration tasks for migrating these ECSs. For details, see **Configuring the Target Server**, **Starting a Full Replication**, and **Launching the Target Server**.

   If the source and target ECSs are in the same VPC on Huawei Cloud, you can set **Network Type** to **Private**. Private connections will be established to the private IP addresses of the target ECSs, and data will be transmitted over these private connections. After the migration is complete, the target ECSs use the same login credentials as their paired source ECSs.

📖 **NOTE**

- If the source and target ECSs are in the same account and the same region, but are in different VPCs, you need to create a peering connection between the VPCs so that you can migrate over a private network. For more information, see **Creating a VPC Peering Connection with Another VPC in Your Account**.

- If the source and target ECSs are in the same region, but are in different accounts and different VPCs, you need to create a peering connection between the VPCs so that you can migrate over a private network. For more information, see **Creating a VPC Peering Connection with a VPC in Another Account**.

6. (Optional) Synchronize incremental data from the source ECSs to the target ECSs by using the **Sync** option on the SMS console.

2 Migrating Physical or Virtual Servers On-Premises or in Other Clouds to Huawei Cloud

Overview

SMS helps you quickly migrate physical or virtual servers on-premises or in another cloud to Huawei Cloud.

Procedure

1. Obtain an AK/SK pair for the account you are migrating to. For details, see **How Do I Create an AK/SK Pair for an Account?**

   If you are migrating to the account of an IAM user, you need to obtain the required permissions and an AK/SK pair for the IAM user. For details, see **How Do I Create an AK/SK Pair for an IAM User?**

2. Install the SMS Agent on each source server to be migrated. For details, see **How Do I Install the Agent on Source Servers?**

3. Run the SMS Agent and enter the AK/SK pair obtained in **1**.

   📖 NOTE

   > After the Agent has started, it reports details about the source servers to SMS, so SMS can check whether the servers can be migrated.

4. Log in to the SMS console using the account you are migrating to. Choose **Servers** from the navigation pane and view the source servers in the server list.

5. Create and run migration tasks for migration the source servers. For details, see **Configuring the Target Server**, **Starting a Full Replication** and **Launching the Target Server**.

   📖 NOTE

   > After the migration is complete, the target servers use the same login credentials as the source servers.

6. (Optional) Synchronize incremental data from the source servers to the target servers by using the **Sync** option on the SMS console.

Server Migration Service
Best Practices

3 Migrating the System and Data Partitions of a
Windows Server to the Separate Disks of a Huawei
Cloud ECS

3 Migrating the System and Data Partitions of a Windows Server to the Separate Disks of a Huawei Cloud ECS

Overview

A Huawei Cloud ECS consists of one system disk and several data disks, as shown in **Figure 3-1**. An on-premises server may have the system partition and other partitions located on the same disk, as shown in **Figure 3-2**.

You can use SMS to easily migrate the system partition (volume C) of the on-premises server to the system disk of the ECS, and other partitions (volumes D and E) to the data disks of the ECS.

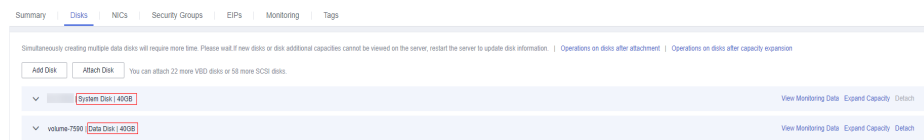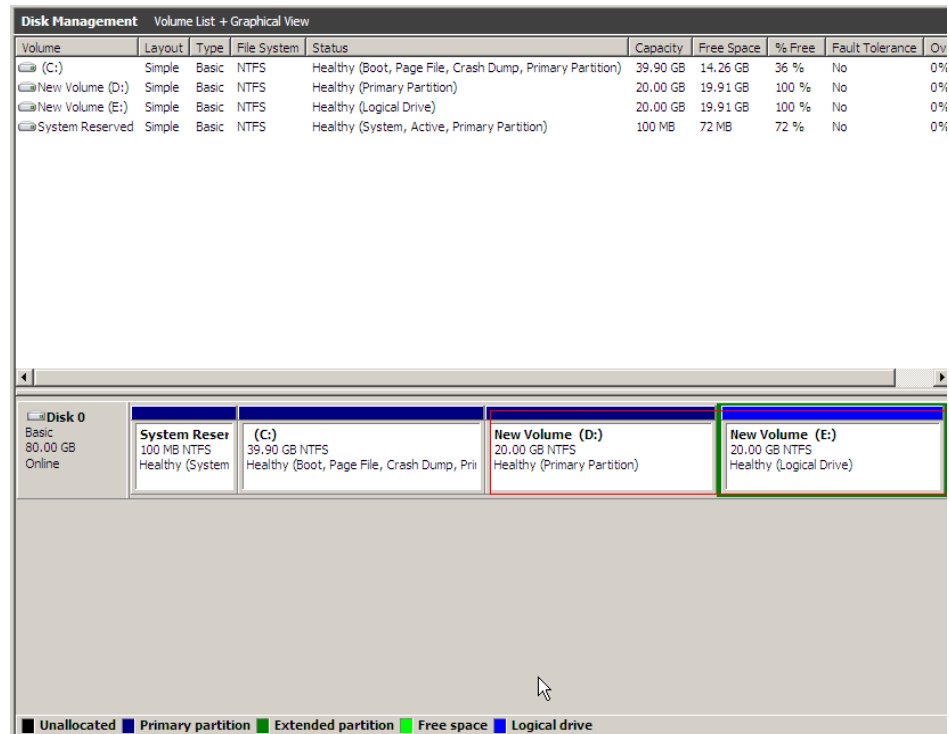**Figure 3-1** Disks on a Huawei Cloud ECS

Server Migration Service
Best Practices

3 Migrating the System and Data Partitions of a
Windows Server to the Separate Disks of a Huawei
Cloud ECS

Figure 3-2 Disks on an on-premises server

Procedure

1. Obtain an AK/SK pair for the account you are migrating to. For details, see **How Do I Create an AK/SK Pair for an Account?**

   If you are migrating to the account of an IAM user, you need to obtain the required permissions and an AK/SK pair for the IAM user. For details, see **How Do I Create an AK/SK Pair for an IAM User?**

2. Install the SMS Agent on the source server to be migrated. For details, see **How Do I Install the Agent on Source Servers?**

3. Go to the Agent installation directory, for example, **C:\SMS-Agent-Py**X**\config**, and modify the configuration file **disk.cfg** as follows:
   ```
   [vol_mount_modify]
   D=2
   E=2
   ```

   > 📖 **NOTE**
   >
   > **D=2** and **E=2** indicate that volumes D and E will be migrated to the second disk, a data disk on the ECS.

4. Run the SMS Agent and enter the AK/SK pair obtained in **1**.

   > 📖 **NOTE**
   >
   > After the Agent has started, it reports source server details to SMS, so SMS can check whether the server can be migrated.

5. Log in to the SMS console using the account you are migrating to. Choose **Servers** from the navigation pane and view the source server in the server list.

6. Create and run a migration task for migrating the source server. For details, see **Configuring the Target Server**, **Starting a Full Replication** and **Launching the Target Server**.

Server Migration Service
Best Practices

3 Migrating the System and Data Partitions of a
Windows Server to the Separate Disks of a Huawei
Cloud ECS

After the migration is complete, the target server has a system disk and a data disk which are separated from each other.

📖 NOTE

After the migration is complete, the target server uses the same login credentials as the source server.

7. (Optional) Synchronize incremental data from the source ECSs to the target ECSs by using the **Sync** option on the SMS console.

4 Migrating a Server into an Enterprise Project

4.1 Background

SMS allows you to migrate a server into a specific enterprise project. You can learn about the Enterprise Project Management Service (EPS) from **What Is Enterprise Project Management Service?**

You must enable the EPS service for the Huawei Cloud account you will migrate to. When you start the SMS Agent on a source server, the Agent lists all enterprise projects the account is allowed to access. You can select the enterprise you would like to migrate the source server to. This enables you to isolate permissions, resources, and finance during the migration.

4.2 Enabling EPS and Creating an Enterprise Project

Enabling EPS

For details, see **Enabling the Enterprise Project Function**.

Creating an Enterprise Project

Create user group **Test_EPS** and IAM user **Test_EPS_User**, and add the IAM user to the user group. Then create enterprise project **Test_EPS_Project**. For details, see **Getting Started with Enterprise Management**.

📖 NOTE

Test_EPS, **Test_EPS_User**, and **Test_EPS_Project** are examples only. You need to change the names as required.

4.3 Authorizing the User Group to Manage the Enterprise Project

You can assign user group **Test_EPS** the permissions required to manage enterprise project **Test_EPS_Project**. Only the IAM users in the user group then are allowed to manage the resources in the enterprise project. This can prevent unauthorized users from accessing the resources in the enterprise project.

> ⚠ **CAUTION**
>
> You need to create two separate custom policies by enterprise project and IAM project and attach them to the user group.

Assigning Permissions to the User Group by Enterprise Project

Step 1 Create custom policy **SMS Custom Policy For EPS**. For details, see section "Creating a Custom Policy in JSON View" in **Creating a Custom Policy**.

Copy the following information to the policy content:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "vpc:securityGroups:create",
                "vpc:securityGroups:delete",
                "vpc:vpcs:create",
                "vpc:vpcs:delete",
                "vpc:publicIps:create",
                "vpc:publicIps:delete",
                "vpc:subnets:create",
                "vpc:subnets:delete",
                "ecs:cloudServers:create",
                "ecs:cloudServers:attach",
                "ecs:cloudServers:detachVolume",
                "ecs:cloudServers:start",
                "ecs:cloudServers:stop",
                "ecs:cloudServers:delete",
                "ecs:cloudServers:reboot",
                "ecs:cloudServers:updateMetadata",
                "ecs:cloudServers:vnc",
                "ecs:serverPasswords:manage",
                "ecs:serverKeypairs:delete",
                "ecs:diskConfigs:use",
                "ecs:CloudServers:create",
                "ecs:servers:setMetadata",
                "ecs:serverVolumes:use",
                "ecs:serverKeypairs:create",
                "ecs:serverInterfaces:use",
                "ecs:serverGroups:manage",
                "ecs:securityGroups:use",
                "ecs:servers:unlock",
                "ecs:servers:rebuild",
                "ecs:servers:lock",
                "evs:volumes:use",
                "evs:volumes:create",
                "evs:volumes:update",
                "evs:volumes:delete",
                "evs:snapshots:create",
```

```
            "evs:snapshots:delete",
            "evs:snapshots:rollback",
            "kms:cmk:list",
            "kms:cmk:get",
            "kms:dek:create",
            "kms:dek:decrypt",
            "ecs:*:get*",
            "ecs:*:list*",
            "evs:*:get*",
            "evs:*:list*",
            "vpc:*:list*",
            "vpc:*:get*",
            "ims:*:get*",
            "ims:*:list*"
        ],
        "Effect": "Allow"
      }
   ]
}
```

Step 2 On the IAM console, choose **User Groups** in the navigation pane.

Step 3 Click user group **Test_EPS**.

Step 4 Click **Authorize**, select the **SMS FullAccess** role and the **SMS Custom Policy For EPS** policy, and click **Next**.

Step 5 Select **Enterprise projects** for **Scope**, select the enterprise project created in **Enabling EPS and Creating an Enterprise Project**, and click **OK**.

----End

Assigning Permissions to the User Group by IAM Project

Step 1 Create custom policy **SMS Custom Policy For EPS At IAM**. For details, see section "Creating a Custom Policy in JSON View" in **Creating a Custom Policy**.

Copy the following information to the policy content:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "ecs:availabilityZones:list",
        "ecs:servers:list",
        "ecs:servers:unlock",
        "ecs:servers:lock",
        "ecs:servers:reboot",
        "ecs:serverPasswords:manage",
        "ecs:diskConfigs:use",
        "ecs:servers:setMetadata",
        "ecs:serverVolumes:use",
        "ecs:serverKeypairs:create",
        "ecs:serverKeypairs:get",
        "ecs:serverKeypairs:delete",
        "ecs:serverInterfaces:use",
        "ecs:serverGroups:manage",
        "ecs:securityGroups:use",
        "vpc:securityGroupRules:create",
        "vpc:securityGroupRules:delete",
        "vpc:securityGroupRules:get",
        "vpc:securityGroupRules:update",
        "vpc:networks:get",
        "vpc:ports:get",
        "vpc:vpcTags:get",
        "vpc:subnetTags:get",
        "vpc:routers:get",
```

```
                "vpc:securityGroups:get",
                "evs:volumes:list",
                "evs:types:get"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Step 2 On the IAM console, choose **User Groups** in the navigation pane.

Step 3 Click user group **Test_EPS**.

Step 4 Click **Authorize**, select the **SMS Custom Policy For EPS At IAM** policy, and click **Next**.

Step 5 Select **All resources** for **Scope** and click **OK**.

----End

Assigning Global Permissions to the User Group

Step 1 Create a custom policy by referring to section "Creating a Custom Policy in JSON View" in **Creating a Custom Policy**.

Copy the following information to the policy content:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sms:server:registerServer",
                "sms:server:migrationServer",
                "sms:server:queryServer"
            ]
        }
    ]
}
```

Step 2 On the IAM console, choose **User Groups** in the navigation pane.

Step 3 Click user group **Test_EPS**.

Step 4 Click **Authorize**, select the created SMS custom policy with global permissions, and click **Next**.

Step 5 Select **All resources** for **Scope** and click **OK**.

----End

4.4 Migrating the Source Server

You need to install the SMS Agent that matches the OS of the source server.

- **Linux Agent**
- **CLI-based Windows Agent (Python 2)**: Windows Server 2008 and Windows 7

- **GUI-based Windows Agent (Python 3)**: Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows 10, and Windows 8.1

Linux Agent

Step 1 **Install the Linux Agent**.

Step 2 Start the Agent. After the Agent lists the enterprise projects your target account is authorized to access, select your desired enterprise project. In this example, select enterprise project **Test_EPS_Project** created in **Creating an Enterprise Project**.

Step 3 Log in to the SMS console. In the navigation pane on the left, choose **Servers**. In the server list, click the server name. The enterprise project **Test_EPS_Project** is displayed in the task details.

Step 4 Perform the procedures described in **Configuring the Target Server**, **Starting a Full Replication**, and **Launching the Target Server**.

📖 **NOTE**

To avoid permission errors, you are advised to create an ECS (that will be used as the target server), VPC, subnet, security group, and EIP in the enterprise project **Test_EPS_Project** before performing the migration.

----End

CLI-based Windows Agent (Python 2)

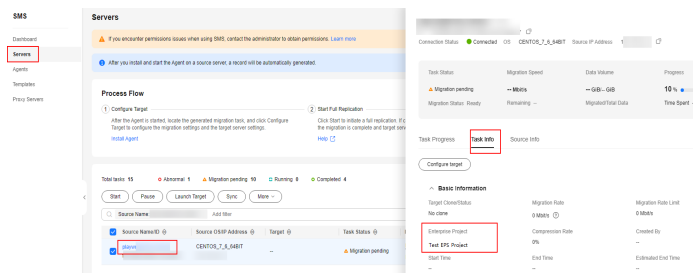**Step 1** **Install the Windows Agent**.

Step 2 Start the Agent. After the Agent lists the enterprise projects your target account is authorized to access, select your desired enterprise project. In this example, select enterprise project **Test_EPS_Project** created in **Creating an Enterprise Project**.

Step 3 Log in to the SMS console. In the navigation pane on the left, choose **Servers**. In the server list, click the server name. The enterprise project **Test_EPS_Project** is displayed in the task details.

Step 4 Perform the procedures described in **Configuring the Target Server**, **Starting a Full Replication**, and **Launching the Target Server**.

📖 **NOTE**

> To avoid permission errors, you are advised to create an ECS (that will be used as the target server), VPC, subnet, security group, and EIP in the enterprise project **Test_EPS_Project** before performing the migration.

----End

GUI-based Windows Agent (Python 3)

Step 1 **Install the Windows Agent**.

Step 2 Start the Agent. After the Agent lists the enterprise projects your target account is authorized to access, select your desired enterprise project. In this example, select enterprise project **Test_EPS_Project** created in **Creating an Enterprise Project**.

Step 3 Log in to the SMS console. In the navigation pane on the left, choose **Servers**. In the server list, click the server name. The enterprise project **Test_EPS_Project** is displayed in the task details.

Step 4 Perform the procedures described in **Configuring the Target Server**, **Starting a Full Replication**, and **Launching the Target Server**.

📖 NOTE

To avoid permission errors, you are advised to create an ECS (that will be used as the target server), VPC, subnet, security group, and EIP in the enterprise project **Test_EPS_Project** before performing the migration.
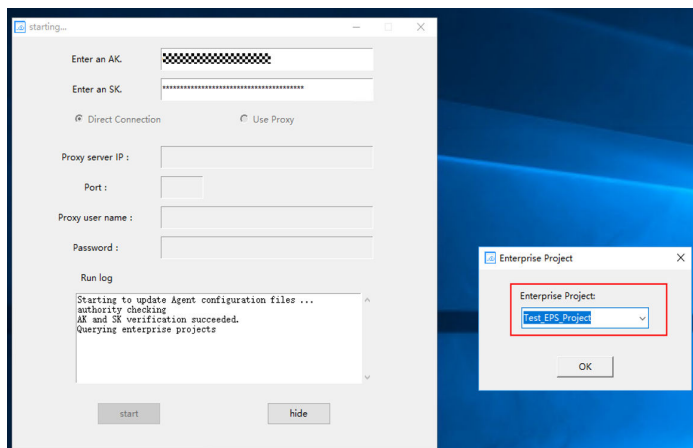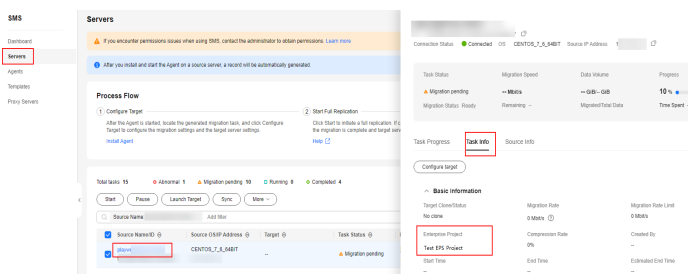
----End

4.5 FAQ

4.5.1 How Do I Fix Error "SMS.0204 Insufficient permissions" When the Migration Fails?

Symptom

During the migration, the system tells you that you have insufficient permission to complete the migration.

Procedure

Obtain the required permissions by referring to **Authorizing the User Group to Manage the Enterprise Project**.

4.5.2 How Do I Fix Error "Enterprise project not enabled" When I Start the Agent?

Symptom

When you started the Agent, the error message "Enterprise project not enabled" was reported.

📖 **NOTE**

If you do not need to migrate the server to a specified enterprise project, ignore this message.

Possible Causes and Solutions

- The enterprise project function may not have been enabled.

  Check whether the enterprise project function has been enabled. If it has not, enable it by referring to **Enabling Enterprise Project**.

- The account you are migrating to may not have the **SMS FullAccess** permissions on the enterprise project you are migrating to.

  Check whether the account has the **SMS FullAccess** permissions on the target enterprise project. If it does not, assign the permissions to it by referring to **Assigning Permissions to the User Group by Enterprise Project**.

- The enterprise project function may not be available in the target region.

  Check whether the enterprise project function is available in the region that you are migrating to. If it is not, you cannot migrate servers to enterprise projects in that region.

5 Migrating Servers Whose OSs Are Not Supported by SMS

5.1 Background

SMS can migrate the OSs listed in **Supported OSs**. The unsupported OSs are still widely used, such as CentOS, Oracle, and Red Hat Linux distributions earlier than 6.0, and Windows releases earlier than Windows Server 2008. We can use a third-party tool to help you migrate servers running these unsupported OSs.

Disclaimer

SMS is not involved in this solution, and we are not responsible for any problems that occur during the migration, including but is not limited to data loss on target servers, startup failures of target servers, and third-party tool errors.

5.2 Migrating Servers Running Unsupported Linux OSs

This practice walks you through how to migrate servers running unsupported Linux OSs. You can check whether your source OSs are supported by SMS in **Supported Linux OSs**.

Procedure

Step 1 Check the format of the system partition on the source server to be migrated.

```
sudo parted -l /dev/vda | grep 'Partition Table'
```

- If **msdos** is displayed, the partition uses MBR, and you can continue to the next step.
- If **gpt** is displayed, the partition uses GPT. This solution does not work, and you need to find another way.

Step 2 Run **df -TH** to view the disk information. As shown in the following figure, **/dev/vda1** is the system partition.

```
[root@ecs-fb30 ~]# df -TH
Filesystem      Type      Size  Used Avail Use% Mounted on
devtmpfs        devtmpfs  4.1G     0  4.1G   0% /dev
tmpfs           tmpfs     4.2G     0  4.2G   0% /dev/shm
tmpfs           tmpfs     4.2G  9.0M  4.1G   1% /run
tmpfs           tmpfs     4.2G     0  4.2G   0% /sys/fs/cgroup
/dev/vda1       ext4      106G  2.4G   99G   3% /
tmpfs           tmpfs     821M     0  821M   0% /run/user/0
```

Step 3   Obtain the UUID of the system partition.

sudo blkid /dev/vda1

Step 4   Use **vi** to open **/etc/fstab**. Press **i** to enter editing mode and add the UUID obtained in **Step 3** to the end of the file.

vi /etc/fstab

Step 5   Save the file and exit.

:wq

Step 6   Install the qemu-img tool.

CentOS is used as an example.

yum -y install qemu-img

Step 7   Export **/dev/vda** to **/mnt/vdb/test.qcow2**.

sudo qemu-img convert -f raw -O qcow2 /dev/vda /mnt/vdb/test.qcow2

In this command, **/mnt/vdb** is the data disk or other storage where the image will be created. To export the partition to another format, you can change the value of the **-O** option.
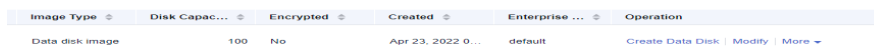
Example Value	Description
qcow2	QCOW2 format
vhd	VHD format
vmdk	VMDK format
raw	Raw image format

Step 8   Use OBS Browser+ to upload the image file to an OBS bucket on Huawei Cloud and register the image file as a private image. For details, see **Registering the Image File as a Private Image**.

Step 9   Create an ECS from the registered private image. For details, see **Creating an ECS from an Image**.

Step 10   Create images for data disks on the source server by repeating **Step 2** to **Step 8**.

Step 11   On the IMS console, create data disks using the data disk images.

Image Type	Disk Capac...	Encrypted	Created	Enterprise ...	Operation
Data disk image	100	No	Apr 23, 2022 0...	default	Create Data Disk | Modify | More

Step 12   Attach the created data disks to the ECS by referring to **Attaching an EVS Disk to an ECS**.

----End

5.3 Migrating Servers Running Unsupported Windows OSs

This section walks you through how to migrate servers running unsupported Windows OSs. You can check whether the source server OSs are supported by SMS in **Supported Windows OSs**.

Procedure

Step 1 **Installing UVP VMTools** on the source server. Then the target server will support KVM virtualization after the migration is complete.

Step 2 **Install and configure Cloudbase-Init** on the source server.

Step 3 Use the Disk2vhd tool to create an image for the system volume of the source server.

1. Download **Disk2vhd** and select the desired version.

2. Select the system volume you want to create an image for and specify where to create the image. Ensure that the destination folder has enough space for the image.
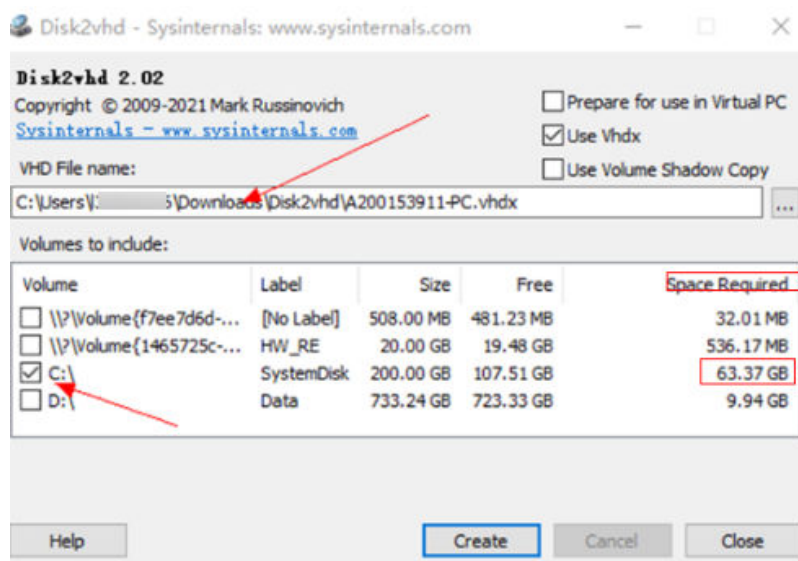
Step 4 Use OBS Browser+ to upload the image file to an OBS bucket on Huawei Cloud and register the image file as a private image. For details, see **Registering the Image File as a Private Image**.

Step 5 Create an ECS from the registered private image. For details, see **Creating an ECS from an Image**.

Step 6 Create images for data disks by repeating **Step 3** and **Step 4**.

Step 7 On the IMS console, create data disks using the data disk images.

Step 8 Attach the created data disks to the ECS by referring to **Attaching an EVS Disk to an ECS**.

----End

6 Customizing Agent Images

6.1 Using Custom Agent Images

You can customize agent images by referring to **Creating a Windows Agent Image** and **Creating a Linux Agent Image**. Then you can use these custom agent images for migration by modifying the SMS Agent configuration file.

Precautions

SMS only provides standard, security-hardened agent images for testing use. You need to use your custom agent images for migration.

- You are advised to use your custom agent images for migration of sensitive data. Before the migration, you need to scan and evaluate security risks in your agent images. Huawei Cloud can provide help for you. You are responsible for possible migration failures and data losses caused by the security risks identified in your agent images.

- The agent images provided by SMS are only for migration testing. You are not advised to use them for other purposes.

- In your custom agent images created using SMS agent images, do not change the IP address 169.254.*XX.XX* contained in the scripts. The IP address is used by ECS to access the metadata service.

Using a Windows Agent Image (Python 3)

Step 1 Log in to the SMS console. In the navigation pane on the left, choose **Agents**.

Step 2 Download Windows Agent (Python 3), upload it to the source server, and double-click **SMS-Agent-Py3.exe** to install the SMS-Agent. Click **Finish** to complete the installation.

Step 3 Enter the AK/SK pair and SMS domain name to start the SMS-Agent.

Step 4 Go to the directory where the SMS-Agent was installed (typically **C:\SMS-Agent-Py3\config**).

Step 5 In the **cloud-region.json** file, search for **"windows_ssh_image_id"** and replace the content as indicated by the arrow in the picture below with the ID of your custom image.

----**End**

Using a Windows Agent Image (Python 2)

Step 1 Log in to the SMS console. In the navigation pane on the left, choose **Agents**.

Step 2 Download Windows Agent (Python 2), upload it to the source server, and double-click **SMS-Agent-Py2.exe** to install the SMS-Agent. Click **Finish** to complete the installation.

Step 3 Enter the AK/SK pair and SMS domain name to start the SMS-Agent.

Step 4 Go to the directory where the SMS-Agent was installed (typically **C:\SMS-Agent-Py2\config**).

Step 5 In the **cloud-region.json** file, search for **"windows_ssh_image_id"** and replace the content as indicated by the arrow in the picture below with the ID of your custom image.

----**End**

Using a Linux Agent Image

Step 1 Log in to the SMS console. In the navigation pane on the left, choose **Agents**.

Step 2 Download the Linux Agent installation package to the source server to be migrated.

Step 3 On the source server, decompress the installation package.

tar -zxvf SMS-Agent.tar.gz

Step 4 Start the Agent.

./startup.sh

Step 5 Enter the AK/SK pair and SMS domain name to start the SMS-Agent.

Step 6 Go to the directory where the SMS-Agent was installed (typically **~\SMS-Agent \agent\config\cloud-region.json**).

Step 7 In the **cloud-region.json** file, search for **"linux_image_id"** and replace the content as indicated by the arrow in the picture below with the ID of your custom image.

----End

6.2 Creating Scripts in Agent Images

Precautions

- You need to prepare scripts based on the OS of the servers to be migrated.
- You need to prepare required scripts on your own. If you need help, contact the Huawei Cloud migration team.
- The script examples below are only for reference.
- You can **download test scripts** from the Huawei Support website for reference.

Windows

Step 1 In the **C:** directory, create a folder and name it **smsWindowesAgent**. In this folder, create three folders and name them **bin**, **Python**, and **smsAgent** respectively.
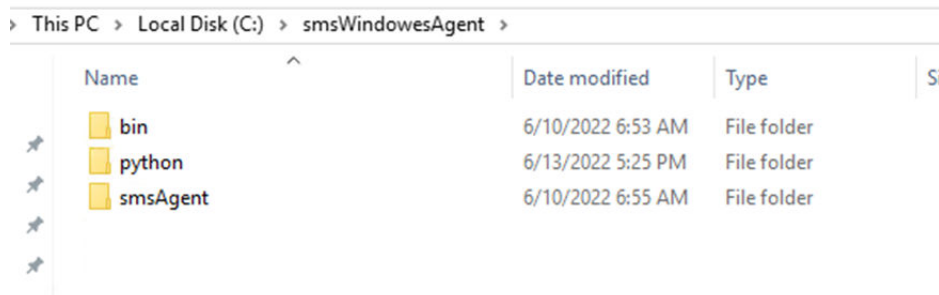
Folder	Function	Location
bin	Stores the startup scripts and the **peagent** folder.	C:\smsWiondowesAgent\bin
python	Installs Python.	C:\smsWiondowesAgent\python
smsAgent	Stores Python scripts for obtaining metadata.	C:\smsWiondowesAgent\smsAgent
peagent	Stores migration components transferred from source servers.	C:\smsWiondowesAgent\bin\peagnet

Step 2 In the **smsAgent** folder, store the scripts used for obtaining certificates and keys.

SMS-Agent uploads SSH public and private keys to metadata of target servers. The scripts you prepared here will be used to obtain the keys from the metadata. The table below shows the three types of metadata.

Script	Function	Destination File
sms_rsa_part (to be deprecated)	Obtains SSH public keys (for server and identity authentication).	C:\Users\Administrator\.ssh \authorized_keys,C:\ProgramData\ssh \ssh_host_rsa_key.pub
sms_rsa_pri_ part (to be deprecated)	Obtains SSH private keys (for server and identity authentication).	C:\ProgramData\ssh\ssh_host_rsa_key
sms_rsa_host _old	Obtains new SSH public keys (for server authentication).	C:\ProgramData\ssh\ssh_host_rsa_key.pub
sms_rsa_host _old_pri	Obtains new SSH private keys (for server authentication).	C:\ProgramData\ssh\ssh_host_rsa_key
sms_rsa_iden tity	Obtains SSH public key certificates (for identity authentication).	C:\Users\Administrator.ssh\authorized_keys
cert_part (to be deprecated)	Obtains TSL 1.2 authentication public keys.	C:\smsWindowesAgent\bin\peAgent\config \cert.pem
prikey_part (to be deprecated)	Obtains TSL 1.2 authentication private keys.	C:\smsWindowesAgent\bin\peAgent\config \prikey.pem

sms_rsa_part and **sms_rsa_pri_part** obtain the SSH public keys and private keys from metadata and write them to the destination files listed in the table above.

Step 3 In the **bin** directory, add a script to check whether **peagent.exe** is running.

'tasklist /nh /fi "imagename eq peAgent.exe'

- If it is not running, add the following command to start it.

  start cmd /k "C:\smsWindowesAgent\bin\peAgent\peAgent.exe"

- If it is running, end the script.

This script should be executed after the scripts in the **smsAgent** folder are executed.

----End

Linux

Step 1 In the **~** directory, create a folder and name it **smsMetadataAgent**. In this folder, create three folders and name them **bin**, **Python**, and **smsAgent** respectively.

Folder	Function	Location
bin	Stores the startup scripts and the **peagent** folder.	~\smsMetadataAgent\bin
smsAgent	Stores Python scripts for obtaining metadata.	~\smsMetadataAgent\smsAgent

Step 2 Prepare scripts for obtaining public and private keys from metadata by referring to the Windows section.

Script	Function	Destination File
sms_rsa_part (to be deprecated)	Obtains SSH public keys (for server and identity authentication).	root/.ssh/authorized_keys, /etc/ssh/ssh_host_rsa_key.pub
sms_rsa_pri_part (to be deprecated)	Obtains SSH private keys (for server and identity authentication).	/etc/ssh/ssh_host_rsa_key
sms_rsa_host_old	Obtains new SSH public keys (for server authentication).	/etc/ssh/ssh_host_rsa_key.pub
sms_rsa_host_old_pri	Obtains new SSH private keys (for server authentication).	/etc/ssh/ssh_host_rsa_key
sms_rsa_identity	Obtains SSH public key certificates (for identity authentication).	/root/.ssh/authorized_keys
cert_part (to be deprecated)	Obtains TSL 1.2 authentication public keys.	/home/config/cert.pem
prikey_part (to be deprecated)	Obtains TSL 1.2 authentication private keys.	/home/config/prikey.pem

Prepare startup scripts by referring to the Windows section.

----End

6.3 Creating a Windows Agent Image

Preparing an ECS

Prepare an ECS that runs Windows Server 2019 Standard 64bit English and has a 40 GB system disk. Windows Server 2019 is used as an example, and you can select another version. Specify a valid password when creating the ECS and name the ECS **SMS**. The official Microsoft image is recommended.

Ensure that the ECS can access the Internet, so that the required tools can be downloaded.

Installing the Required Software

Step 1 Transfer the **smsWindowesAgent** folder created in **Creating Scripts in Agent Images** to the **C:**directory of the ECS. The folder stores the agent image scripts you prepared.

Step 2 Install **Python 3.7.6** to **C:\smsWindowsAgent\Python**. You can select another version as required.
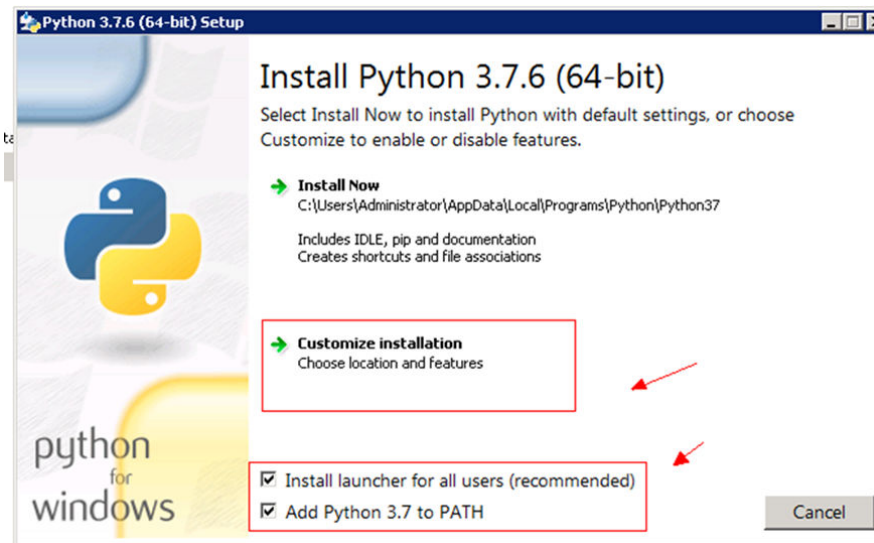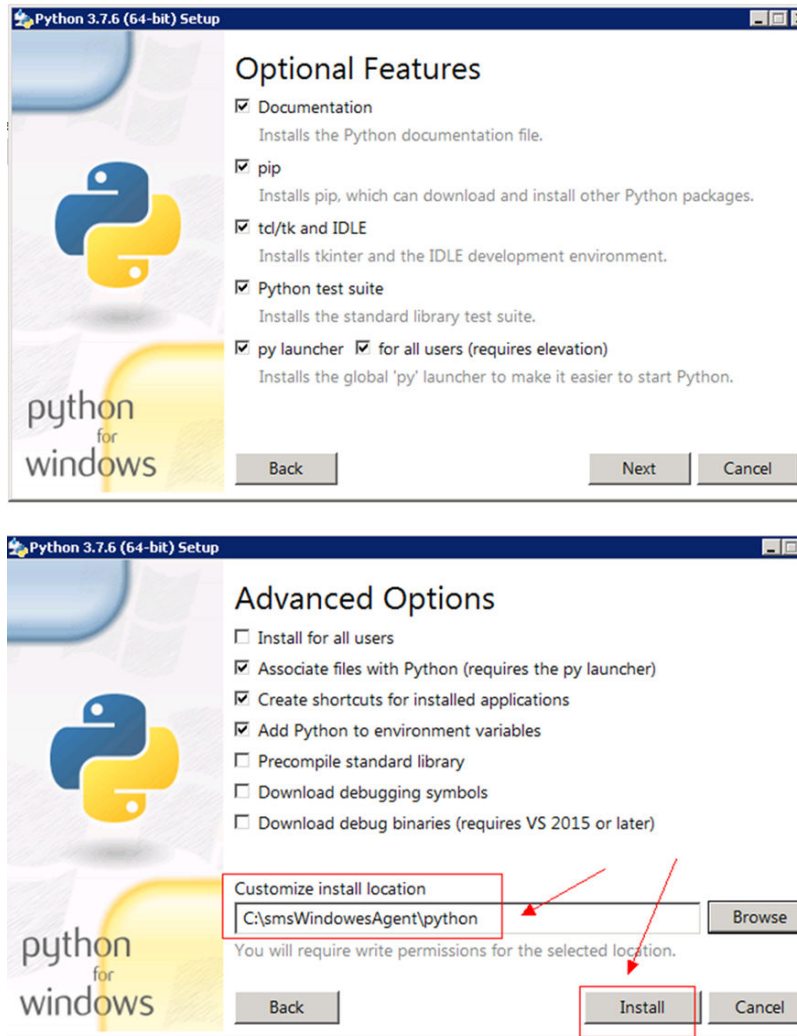
Step 3 Run **where python** to check whether Python has been installed in the specified directory.

----**End**

Installing requests and ConfigParser

Run the following commands on the ECS to install requests and ConfigParser.

pip install requests
pip install configparser

Modifying the ECS

Step 1 Enable scripts to automatically run upon ECS startup.

1. Open the cmd and run **gpedit**. In the displayed window, choose **Computer Configuration** > **Windows Settings** > **Scripts (Startup/Shutdown)** > **Startup**.
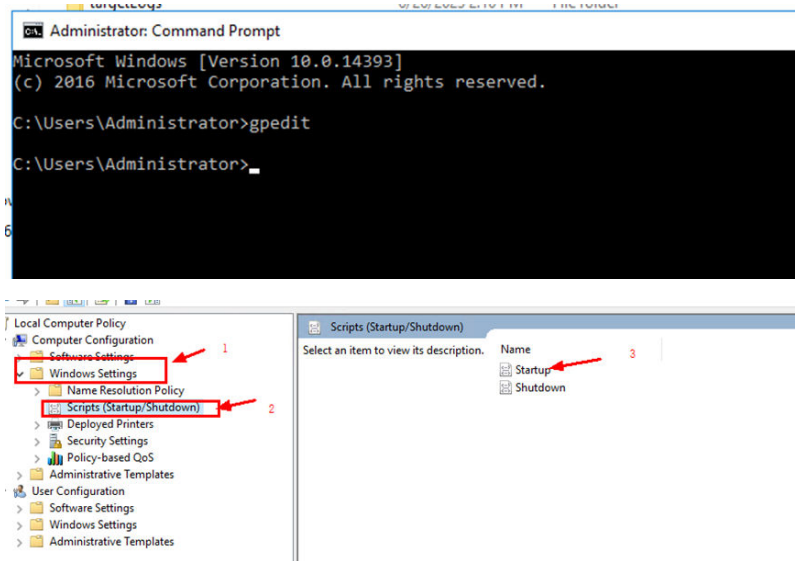
2. Click **Add** and specify **C:\smsWindowesAgent\bin**_Name of script for running Python_**.bat** for **Script Name**.
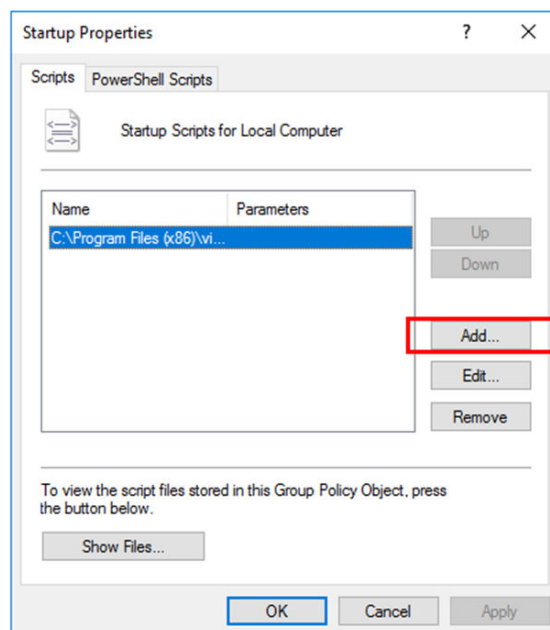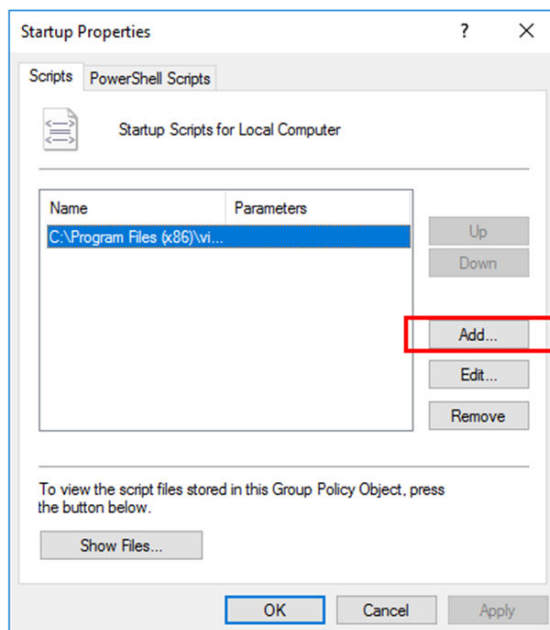
Step 2 Install OpenSSH.

1. Right-click the **Start** icon or press **Win** and **X** keys. In the displayed menu, choose **Windows PowerShell (Administrator)**. In the displayed window, run the following command:
   Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0

2. After the installation is complete, restart the OS for the installation to take effect. Start the sshd and ssh-agent services and set them to automatically run at startup.

   Start sshd.

   Start-Service sshd

   Enable sshd to automatically run at startup.

   Set-Service sshd Automatic

   Start ssh-agent.

   Start-Service ssh-agent

   Enable ssh-agent to automatically run at startup.

   Set-Service ssh-agent -StartupType Automatic

3. Go to the **C:\ProgramData directory** and add the following content to the **sshd_config** file:

   PasswordAuthentication no

Step 3 Install OpenStack.

Download the **VMTools drivers** required by SMS.

Decompress the downloaded package, double-click the extracted file, and find the required drivers in **./vmtools-windows/upgrade/windows** *XX***/drivers**.

Copy all driver files to the specified directory.

Windows Server 2016_64bit is used here as an example.

Copy all files in **upgrade\windows 2016_64\drivers\viostor** to **C:\smsWindowsAgent\bin\peAgent\OpenStack\windows_device_driver \windows2016_64**.

Copy files in the rest of folders under **upgrade\windows 2016_64\drivers** to **C:\smsWindowsAgent\bin\peAgent\OpenStack\windows_device_driver \windows2016_64**.

The picture below shows the files copied to the **C:\smsWindowsAgent\bin \peAgent\OpenStack\windows_device_driver\windows2016_64** directory.

Copy files required by other Windows versions to the corresponding directories.
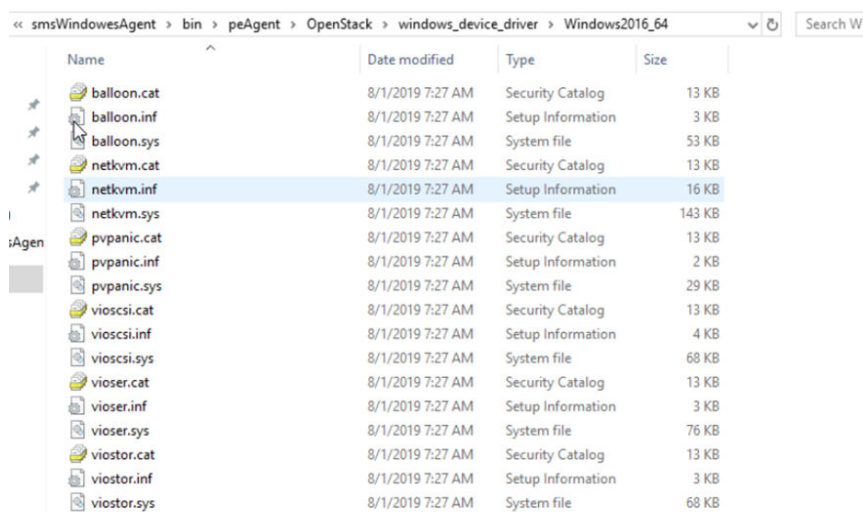
Step 4 Open ports 8899 and 8900 on the ECS.

```
netsh advfirewall firewall add rule name=peagent dir=in action=allow protocol=TCP localport=8899
netsh advfirewall firewall add rule name=ntcldst dir=in action=allow protocol=TCP localport=8900
```

Step 5 (Optional) Install the password reset plug-in if you did no use a public image to create this ECS.

1. Download the plug-in at **https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/windows/reset_pwd_agent/ CloudResetPwdAgent.zip**.

2. Double-click **setup.bat** in the **CloudResetPwdAgent.Windows** or **CloudResetPwdUpdateAgent.Windows** directory.

3. In the Task Manager, search for **cloudResetPwdAgent** and **cloudResetPwdUpdateAgent**.

   – If they are there, the installation is successful.

   – If they are not there, the installation fails.

----End

(Optional) Hardening Security

Step 1 Disable remote login.

Open the Control Panel, choose **System and Security** > **System** > **Allow remote access**, and select **Don't allow remote connections to this computer**.
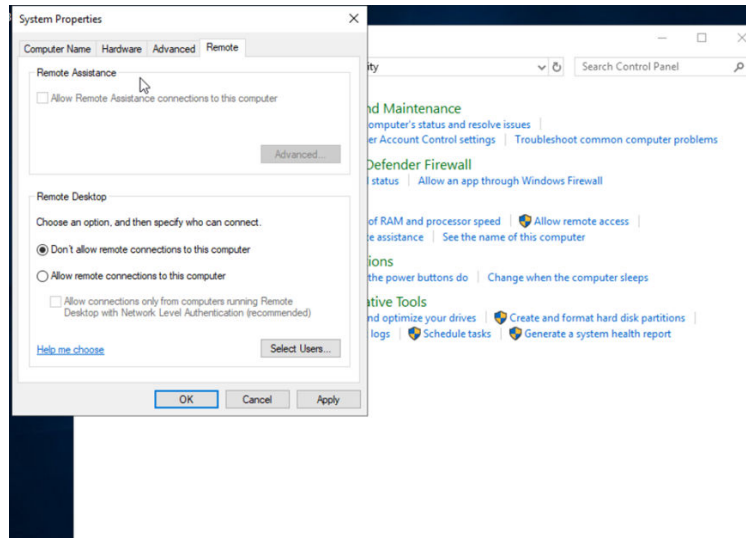
Step 2 Disable the WinRM service.

1. Open the cmd or PowerShell as an administrator.

2. Stop the WinRM service.

   net stop winrm

3. Disable the WinRM service.

   sc config winrm start= disabled

Step 3 Set a password login policy to block brute-force attacks.

1. Open the cmd or PowerShell as an administrator.

2. Run the **gpedit.msc** command to start **Local Group Policy Editor**.

3. In the displayed window, choose **Computer Configuration** > **Windows settings** > **Security Settings** > **Account Policy** > **Account Lockout Policy**. Set the account locking policy shown in the following figure. This policy indicates that if there are 6 consecutive unsuccessful login attempts, the account will be blocked for 3 minutes.

Step 4 Close listening ports in the Windows firewall.

1. Open the cmd and run the **netstat -ano** command to check all listening ports.

```
C:\Users\Administrator>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:22             0.0.0.0:0              LISTENING       2720
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       852
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       456
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1236
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1464
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1988
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2548
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       592
  TCP    0.0.0.0:49675          0.0.0.0:0              LISTENING       600
  TCP    192.168.192.154:139    0.0.0.0:0              LISTENING       4
  TCP    [::]:22                [::]:0                 LISTENING       2720
  TCP    [::]:135               [::]:0                 LISTENING       852
  TCP    [::]:49664             [::]:0                 LISTENING       456
  TCP    [::]:49665             [::]:0                 LISTENING       1236
  TCP    [::]:49666             [::]:0                 LISTENING       1464
  TCP    [::]:49667             [::]:0                 LISTENING       1988
  TCP    [::]:49668             [::]:0                 LISTENING       2548
  TCP    [::]:49669             [::]:0                 LISTENING       592
  TCP    [::]:49675             [::]:0                 LISTENING       600
  UDP    0.0.0.0:123            *:*                                    1420
  UDP    0.0.0.0:500            *:*                                    2676
  UDP    0.0.0.0:4500           *:*                                    2676
  UDP    0.0.0.0:5353           *:*                                    1696
  UDP    0.0.0.0:5355           *:*                                    1696
  UDP    127.0.0.1:62263        *:*                                    2992
  UDP    192.168.192.154:137    *:*                                    4
  UDP    192.168.192.154:138    *:*                                    4
  UDP    [::]:123               *:*                                    1420
  UDP    [::]:500               *:*                                    2676
  UDP    [::]:4500              *:*                                    2676
  UDP    [::]:5353              *:*                                    1696
  UDP    [::]:5355              *:*                                    1696
```

2. Close all dynamic ports (49152-65535) and port 135 used for listening.
   netsh advfirewall firewall add rule name=Tcp_disable dir=in action=block protocol=TCP localport=135,3389,5985,5986,49152-65535

3. Close all UDP ports.
   netsh advfirewall firewall add rule name=Tcp_disable dir=in action=block protocol=UDP localport=any

----End

Creating an Image

Step 1 Log in the IMS console.

Step 2 Click **Create Image**.

Step 3 Create a system disk image for the ECS as prompted.

Step 4 View the ID of the created image.

----End

6.4 Creating a Linux Agent Image

Preparing an ECS

Prepare a Linux ECS using a public image.

Set a password for the ECS. Install Python 3 on the ECS if it is not included in the public image.

Preparing Scripts

For details, see **Creating Scripts in Agent Images**.

Modifying the ECS

Step 1 Install necessary components.

Install Python dependencies. Below is just an example. Install the latest version of Python.

```
yum install python36
ln -s /usr/bin/python36 /usr/bin/python3
yum install python36-setuptools
wget https://files.pythonhosted.org/
packages/ae/e8/2340d46ecadb1692a1e455f13f75e596d4eab3d11a57446f08259dee8f02/pip-10.0.1.tar.gz
tar xvf pip-10.0.1.tar.gz
cd pip-10.0.1
python3 setup.py install
pip3 install requests
```

Step 2 Modify the **/etc/rc.local** file.

```
ln -s /etc/rc.d/rc.local /etc/rc.local     #If files /etc/rc.d/rc.local and /etc/rc.local are not linked t each other
in the public image, the scripts may not be executed at startup.
chmod 766 /etc/rc.d/rc.local
```

Step 3 Install basic system components.

```
yum install expect
yum install lvm2
yum install dosfstools       #mkfs.vfat is supported.
rpm -ivh grub-0.97-99.el6.x86_64.rpm     #This component is only needed when the servers to be migrated
use GRUB 1. Download this component at the grub official website.
```

Step 4 Modify **/etc/mke2fs.conf**.

Delete **64bit** from the **ext4** item. Otherwise, GRUB 1 may fail to be installed in the Ext4 file system.

```
[root@luojiandong-s ~]# vim /etc/mke2fs.conf

  1 [defaults]
  2     base_features = sparse_super,filetype,resize_inode,dir_index,ext_attr
  3     default_mntopts = acl,user_xattr
  4     enable_periodic_fsck = 0
  5     blocksize = 4096
  6     inode_size = 256
  7     inode_ratio = 16384
  8
  9 [fs_types]
 10     ext3 = {
 11         features = has_journal
 12     }
 13     ext4 = {
 14         features = has_journal,extent,huge_file,flex_bg,uninit_bg,dir_nlink,extra_isize,64bit
 15         inode_size = 256
 16     }
 17     ext4dev = {
 18         features = has_journal,extent,huge_file,flex_bg,uninit_bg,dir_nlink,extra_isize
 19         inode_size = 256
 20         options = test_fs=1
 21     }
```

Step 5 Change partition UUIDs.

1. Detach the system disk from the ECS and attach it to a temporary ECS as a data disk.

2. On the temporary ECS, use **uuidgen** to generate new UUIDs and use **tune2fs –U** to assign new UUIDs to partitions.

   a. Run the **blkid** command on the temporary ECS to query the UUID of each partition.

```
[root@host-59-218-96-71 Desktop]# blkid
/dev/xvda1: UUID="012b7e35-22c9-4f4c-ad68-d42fe74f3b8e" TYPE="xfs"
/dev/xvda2: UUID="98e96267-50ce-4dad-b257-a1ff9f60ff72" TYPE="swap"
/dev/xvda3: UUID="bb09db62-4217-46a8-88d0-158005057492" TYPE="xfs"
/dev/xvde1: UUID="012b7e35-22c9-4f4c-ad68-d42fe74f3b8e" TYPE="xfs"
/dev/xvde2: UUID="98e96267-50ce-4dad-b257-a1ff9f60ff72" TYPE="swap"
/dev/xvde3: UUID="bb09db62-4217-46a8-88d0-158005057492" TYPE="xfs"
[root@host-59-218-96-71 Desktop]#
[root@host-59-218-96-71 Desktop]# xfs_admin -u /dev/xvde3
UUID = bb09db62-4217-46a8-88d0-158005057492
[root@host-59-218-96-71 Desktop]#
```

b. Run the **uuidgen** command to generate a new UUID.

```
/dev/xvde3: UUID="bb09db62-4217-46a8-88d0-158005057492" TYPE="xfs"
[root@host-59-218-96-71 Desktop]#
[root@host-59-218-96-71 Desktop]# xfs_admin -u /dev/xvde3
UUID = bb09db62-4217-46a8-88d0-158005057492
[root@host-59-218-96-71 Desktop]# uuidgen
bf1d10f6-daef-45e5-94a0-166ff6df77f7
[root@host-59-218-96-71 Desktop]# xfs_admin -U bf1d10f6-daef-45e5-94a0-166ff6df7
7f7
```

c. Run the **tune2fs -U** <New_UUID> <Device> or **xfs_admin -U** <New_UUID> <Device> command to assign the new UUID to the partition on the data disk.

```
[root@host-59-218-96-71 Desktop]#
[root@host-59-218-96-71 Desktop]# xfs_admin -u /dev/xvde3
UUID = bb09db62-4217-46a8-88d0-158005057492
[root@host-59-218-96-71 Desktop]# uuidgen
bf1d10f6-daef-45e5-94a0-166ff6df77f7
[root@host-59-218-96-71 Desktop]# xfs_admin -U bf1d10f6-daef-45e5-94a0-166ff6df7
7f7 /dev/xvde3
Clearing log and setting UUID
writing all SBs
new UUID = bf1d10f6-daef-45e5-94a0-166ff6df77f7
[root@host-59-218-96-71 Desktop]# blk
```

d. Change the UUID of the partition in **/etc/fstab** and **/boot/grub2/grub.cfg** to the newly assigned UUID.

This is to ensure that OS in the agent image disk can be started.

e. Attach the disk back to the original ECS as the system disk and test whether the OS can start up.

Step 6 Transfer the **smsMetadataAgent** folder where stores the necessary scripts to the ECS and enable these scripts to automatically run at startup. For details, see **Creating Scripts in Agent Images**.

Step 7 Modify the sshd configuration file to disable password login.

Step 8 Delete residual settings. Ensure that there is no **/data** directory, there are no SMS log files in the **/root** directory, and there are no residual certificates in the **/etc/ssh** directory.

----End

(Optional) Hardening Security

Step 1 Add the following content to the **sshd_config** file.

```
MaxAuthTries 6
LoginGraceTime 60
PasswordAuthentication no
```

Step 2 Disable history.

1. Start the Shell and run the following command:
   ```
   sudo nano ~/.bashrc
   ```

2. Add the following content to the end of the file:
   ```
   unset HISTFILE
   ```

3. Save the file and exit. Run the following command for the modification to take effect:
   ```
   source ~/.bashrc
   ```

Step 3 Prevent brute-force attacks.

Add the content below to the **/etc/pam.d/password-auth** file. The content is contained in Huawei Cloud EulerOS by default.

```
auth sufficient pam_faillock.so authsucc audit deny=3 even_deny_root unlock_time=60
```

This can prevent any user from login for 30 seconds after 3 failed login attempts.

Step 4 Set the password complexity requirements.

In the **/etc/pam.d/system-auth** file, append **enforce_for_root minlen=8 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1** to the end of the row that starts with **password requisite pam_pwquality.so try_first_pass**.

```
password requisite pam_pwquality.so try_first_pass local_users_only enforce_for_root minlen=8 ucredit=-1
lcredit=-1 dcredit=-1 ocredit=-1
```

Step 5 Change the umask value. Change the value of umask to **027**. The **umask** command is used to set the default permissions on files and directories.

1. Open the Shell and run the following command to open the **.bashrc** file:
   ```
   nano ~/.bashrc
   ```

2. Add the following content to the end of the file:
   ```
   umask 027
   ```

3. Save and close the file. Run the following command to make the change take effect:
   ```
   source ~/.bashrc
   ```

Step 6 Delete residual system tools because keeping them only increases the attack surface of the system and mislead security software.

Delete the following residual tools:

- tcpdump, sniffer, Wireshark, Netcat, and other WinPcap-based sniffing tools
- gdb, strace, readelf, cpp, gcc, dexdump, mirror, JDK, and other self-developed tools or scripts used only in the development and debugging phase
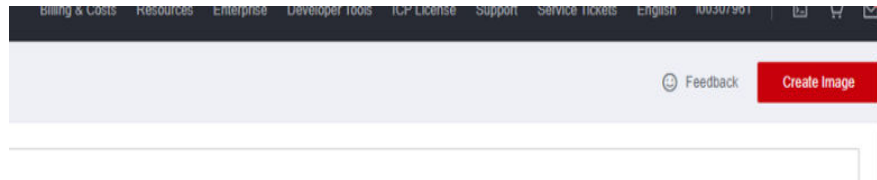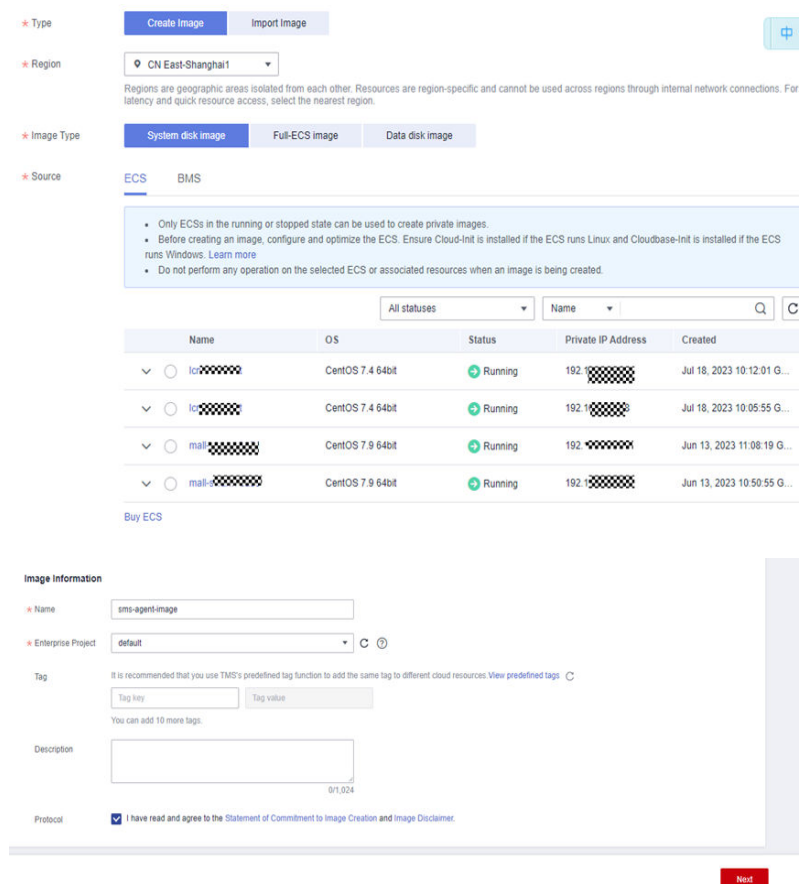
----End

Creating an Image

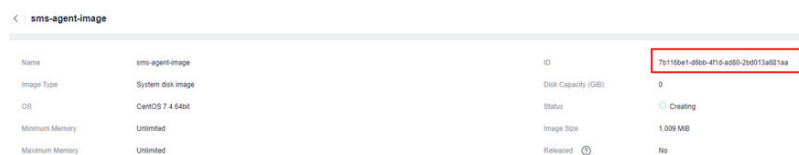**Step 1** Log in the IMS console.

Step 2 Click **Create Image**.

Step 3 Create a system disk image for the ECS as prompted.

Step 4 View the ID of the created image.

----End

7 Migrating Servers over an IPv6 Network

7.1 Preparing for Migration

Before using SMS, make the following preparations:

1. **Register a HUAWEI ID and enable Huawei Cloud services**.

   📖 NOTE

   Real-name authentication is required for migrating servers to regions within the Chinese mainland.

2. Obtain the required permissions.

   If you use an account for migration, you have the required permissions by default. If you use an IAM user for migration, you need to obtain the required permissions. For more information, see **Creating a User Group and Assigning Permissions**.

3. Obtain an AK/SK pair for your target account.

   The AK/SK pair is used for authentication during the migration. To learn how to obtain an AK/SK pair, see **How Do I Create an AK/SK Pair for an Account?** or **How Do I Create an AK/SK Pair for an IAM User?**

   ⚠️ **CAUTION**

   SMS does not support AK/SK-based authentication for federated users (virtual users).

   ---

4. Ensure that the source server OS is supported by SMS.

   See **Supported Windows OSs** or **Supported Linux OSs**.

5. Ensure that the following network requirements are met:

   a. The source server can connect to the Huawei Cloud API Gateway over TCP port 443. For more information, see **Connecting Source Servers to Huawei Cloud API Gateway**.

      📖 NOTE

      It is recommended that all outbound ports on the source server be opened.

b. If you want to migrate over an IPv6 network, the source environment must support IPv4/IPv6 dual-stack networks.

c. The source server can connect to the target server. For more information, see **Connecting Source Servers to Target Servers**.

- For a migration over the Internet, purchase EIPs in the region you are migrating to.

- For a migration over a private network, request a Direct Connect or VPN connection.

d. The following ports are enabled in the security group associated with the target server to allow traffic to these ports:

- Windows: TCP ports 8899, 8900, and 22

- Linux: TCP port 22 for file-level migration, and ports 8900 and 22 for block-level migration

---

⚠ **CAUTION**

- For security purposes, you are advised to only allow traffic from the source server to the ECS over these ports.
- The firewall of the target server must allow traffic to these ports.

To learn how to open the ports, see **How Do I Configure Security Group Rules for Target Servers?**

6. Ensure that the following source server requirements are met:

Available Space

– Windows

- At least 320 MB of available space on a partition not smaller than 600 MB

- At least 40 MB of available space on a partition smaller than 600 MB

– Linux

At least 200 MB of available space on the root partition

Source Environment

– The system time of the source server must be consistent with the local standard time to avoid Agent registration failures.

– If the source server runs Linux, **rsync** must be installed on it. You can run the **rsync -v** command to check whether **rsync** is installed.

If it is not, install it by running the following command:

- CentOS: **yum -y install rsync**

- Ubuntu: **apt-get -y install rsync**

- Debian: **apt-get -y install rsync**

- SUSE: **zypper install rsync**

■ For other distributions, refer to the official website documentation.

📖 **NOTE**

rsync comes preinstalled on most distributions by default.

7.2 Setting Up an IPv6 Network and Creating a Target Server

Before migrating a server over an IPv6 network, you need to set up an IPv6 VPC and create an ECS as the target server in it. For details, see **Setting Up an IPv6 Network**.

Precautions

- The source server must be able to access the IPv6 network. If your source server is an ECS on Huawei Cloud, DHCPv6 must be enabled for it. For details, see **Dynamically Assigning IPv6 Addresses**.

- When configuring a subnet, you need to select **Enable** for **IPv6 CIDR Block** so that the system will automatically allocate an IPv6 CIDR block to the subnet.

- Only some ECS specifications support IPv6 networks. To use an IPv4/IPv6 dual-stack network, you need to create an ECS that supports IPv6 in a supported region. For details about the supported ECS specifications, see **ECS Specifications List**.

- When configuring the network, you must select **Self-assigned IPv6 address**. **Allocate Shared Bandwidth** is optional.

- The security group of the ECS must allow traffic from IPv6 addresses over the following required ports:
  - Windows: TCP ports 8899, 8900, and 22

– Linux: TCP port 22 for file-level migration, and ports 8900 and 22 for block-level migration

---

⚠ **CAUTION**

For security purposes, you are advised to only allow traffic from the source server to the ECS over these ports.
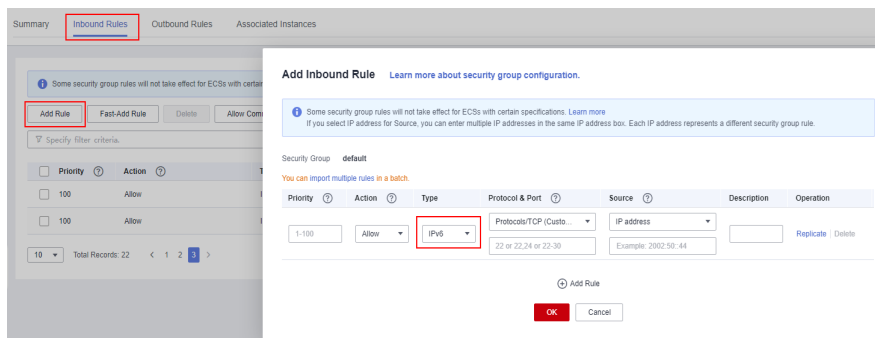
7.3 Creating a Migration Task

SMS supports data migration over an IPv4/IPv6 dual-stack network.

Prerequisites

- You have completed operations in **Preparing for Migration**.
- You have completed operations in **Setting Up an IPv6 Network and Creating a Target Server**.

Constraints

- The account used for migration must have sufficient balance.
- For a migration over an IPv6 network, **Migration Rate Limit**, **Continuous Synchronization**, **Measure Network Performance**, and **Proxy Servers** are unavailable.

Procedure

Step 1 Install the Agent that matches the source server OS.

- **Install the Linux Agent**.
- **Install the Windows Agent**.

Step 2 **Configure the target server**.

On the **Configure Basic Settings** page, in the **Network Settings** area, set **IP Version** to **IPv6**.

On the **Configure Target** page, select **Use existing** for **Target Server** and select the server created in **Setting Up an IPv6 Network and Creating a Target Server**.
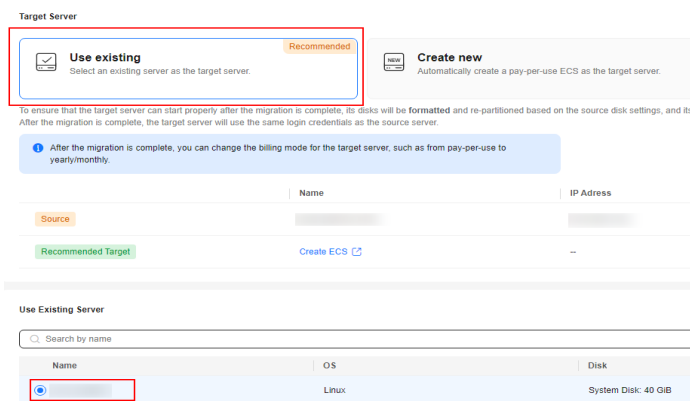
Step 3 **Start the full replication**, and **launch the target server**.

Step 4 (Optional) Synchronize incremental data from the source server to the target server by using the **Sync** option on the SMS console.

----End

8 Network Configurations for Different Migration Scenarios

Background

For a server migration, there are two important aspects to consider: data flow directions and network requirements. A migration using SMS involves two types of traffic: control flow and data flow.

- **Control flow** refers to the communications between the source server and cloud service management planes. To ensure a smooth migration, verify if there are any restrictions on the outbound traffic from the source server. Additionally, confirm that the source server can access the following cloud services via their domain names: SMS, IAM, ECS, EVS, VPC, and IMS.

- **Data flow** refers to data transmission from the source server to the target server. To ensure smooth data transmission, confirm that the security group of the target server allows traffic from the source server's IP address over the specified migration ports. If the source server cannot directly access the Internet or cannot communicate with the target server, a proxy server must be configured. The proxy server must meet the following requirements:

  – The proxy server can correctly forward traffic from the source server.

  – The proxy server's security group is configured to allow traffic from the source server's IP address over the proxy port.

For a Scenario Where the Source Server Has Internet Access and Can Communicate with the Target Server over the Internet

1. **Download and start the SMS-Agent** on the source server.

2. **Configure the target server**. Remember to set **Network Type** to **Public**.

   Ensure that the security group of the target server allows access from the source server's public IP address over the specified migration ports. For details about how to configure security group rules, see **How Do I Configure Security Group Rules for Target Servers?**

For a Scenario Where the Source Server Has Internet Access and Can Communicate with the Target Server over an Intranet

1. Confirm the source and target servers can communicate with each other over the intranet.

2. **Download and start the SMS-Agent** on the source server.

3. **Configure the target server**. Set **Network Type** to **Private** during the configuration.

   Ensure that the security group of the target server allows access from the source server's private IP address over the specified migration ports. For details about how to configure security group rules, see **How Do I Configure Security Group Rules for Target Servers?**

For a Scenario Where the Source Server Has No Internet Access and Can Communicate with the Target Server over an Intranet

1. Prepare a proxy server that can access the Internet and can communicate with the source server over an intranet. Configure the security group of the proxy server to allow access from the source server's private IP address over the proxy port.

2. Install proxy software on the proxy server. Squid is recommended for Linux, and WProxy is recommended for Windows.

3. Download and install the SMS-Agent on the source server, modify the proxy settings in the SMS-Agent configuration file, and start the SMS-Agent. For details, see **How Do I Configure a Source Server to Access Huawei Cloud Through a Proxy?**

4. **Configure the target server**. Set **Network Type** to **Private** during the configuration.

   Ensure that the security group of the target server allows access from the source server's private IP address over the specified migration ports. For details about how to configure security group rules, see **How Do I Configure Security Group Rules for Target Servers?**

For a Scenario Where the Source Server Has No Internet Access and Cannot Communicate with the Target Server

Prepare proxy servers for forwarding control traffic and data traffic. The proxy servers must be able to communicate with the source server and the target server on Huawei Cloud.

1. Configure a proxy server to forward control traffic to cloud services. For details, see step 1 in **How Do I Configure a Source Server to Access Huawei Cloud Through a Proxy?**

2. Create at least one Nginx proxy server to forward data traffic based on the number of servers and the volume of data to be migrated. Run the following command to install the tool:
   ```
   yum install nginx -y
   ```

3. Configure Nginx to forward data traffic. The following uses CentOS 8 as an example:

a. Open the **/etc/ssh/sshd_config** file, find the line containing **Port 22**, delete the default comment tag (#), and add a line containing **Port 2222** below the line.

b. Run the following command to restart the SSH service to apply the configuration:
```
systemctl restart sshd.service
```

c. Run the following command to add a firewall rule:
```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 2222 -j ACCEPT
```

d. Open the **/etc/ssh/sshd_config** file, find the line containing **Port 22**, add **#** to the line to restore the comment, and run the following command to restart the sshd service:
```
systemctl restart sshd.service
```

e. Modify the **/etc/nginx/nginx.conf** configuration file.

- For a Linux file-level migration, add the following content to the end of the file. The content must be at the same identification level as **http{}** in the file. If multiple servers need to be migrated, add multiple mappings. **default backend1** is mandatory because it is for the proxy server mapping.
```
stream {
  map $remote_addr $backend {
    default backend1;
    <IP-address of source-server-1>  backend2;
    <IP-address of source-server-2>  backend3;
  }

  server {
    listen 22;
    proxy_pass $backend;
  }

  upstream backend1 {  server <IP-address-of-proxy-server>:22; }
  upstream backend2 {  server <IP-address-of-target-server-1>:22; }
  upstream backend3 {  server <IP-address-of-target-server-2>:22; }
}
```

- For a Windows migration, add the following content to the end of the file. The content must be at the same identification level as **http{}** in the file. If multiple servers need to be migrated, add multiple multiple **upstream backend_<x>_<xx>** entries and mappings. The following is a configuration example:
```
stream {
  # Server 1
  upstream backend_1_22 {
    server <IP-address-of-target-server-1>:22;
  }

  upstream backend_1_8899 {
    server <IP-address-of-target-server-1>:8899;
  }

  upstream backend_1_8900 {
    server <IP-address-of-target-server-1>:8900;
```

```
        }

        # Server 2
        upstream backend_2_22 {
            server <IP-address-of-target-server-2>:22;
        }

        upstream backend_2_8899 {
            server <IP-address-of-target-server-2>:8899;
        }

        upstream backend_2_8900 {
            server <IP-address-of-target-server-2>:8900;
        }

        map $remote_addr $backend_22 {
            <IP-address-of-source-server-1>  "backend_1_22";
            <IP-address-of-source-server-2>  "backend_2_22";
            default X:22;
        }

        map $remote_addr $backend_8899 {
            <IP-address-of-source-server-1>  "backend_1_8899";
            <IP-address-of-source-server-2>  "backend_2_8899";
            default X:8899;
        }

        map $remote_addr $backend_8900 {
            <IP-address-of-source-server-1>  "backend_1_8900";
            <IP-address-of-source-server-2>  "backend_2_8900";
            default X:8900;
        }

        server {
            listen 22;
            proxy_pass $backend_22;
        }

        server {
            listen 8899;
            proxy_pass $backend_8899;
        }

        server {
            listen 8900;
            proxy_pass $backend_8900;
        }
    }
```

  f. Run the following command to check whether the Nginx configuration is correct:

```
nginx -t
```

   If the message "successful" is displayed, the configuration is successful.

  g. After verifying that the configuration is correct, start the Nginx service.

```
nginx
```

  h. Run the following command to check whether Nginx is listening on the specified port:

```
netstat -ntpl
```

4. Download and install the SMS-Agent on the source server, modify the proxy settings in the SMS-Agent configuration file, and start the SMS-Agent. For details, see step 2 in **How Do I Configure a Source Server to Access Huawei Cloud Through a Proxy?**

5. **Configure the target server**. Set **Transit IP Address** to the private IP address of the proxy server during the configuration.

> ⚠️ CAUTION
>
> Ensure that the proxy server is configured to allow inbound traffic from the source server's IP address, and the target server is configured to allow inbound traffic to the proxy server.

Figure 8-1 Setting a transit IP address
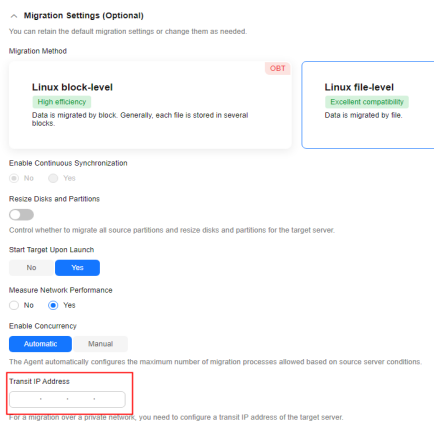
For a Scenario Where MgC Is Used to Batch Migrate Servers

Internet access is required for migration using MgC.

1. Install Edge in the intranet environment. Edge must be able to access the source servers to be migrated. For details, see **Installing Edge for Windows**.

2. Complete steps 2 to 5 described in **Migrating On-premises Servers to Huawei Cloud Using MgC**.

> ⚠️ CAUTION
>
> Ensure that the security group of the target server allows access from the source servers over the specified migration ports. For details about how to configure security group rules, see **How Do I Configure Security Group Rules for Target Servers?**

3. **Create a server migration workflow**.

   – If the source servers can access the Internet, set the migration network to **Public**.

   Figure 8-2 Migration over the Internet
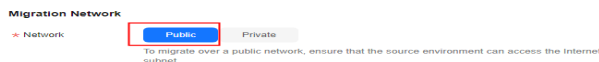
   – If the source servers cannot access the Internet, prepare a proxy server that can access the Internet and install proxy software. For details, see step 1 in **How Do I Configure a Source Server to Access Huawei Cloud Through a Proxy?** The network requirements for the proxy server are as follows:

■ Regardless whether the proxy server is on the source intranet environment or on the cloud, it must be able to access the source servers to be migrated over an intranet.

■ The proxy server must be configured to allow inbound traffic from the source servers over the proxy port.

After the proxy server is configured, set the migration network to **Private**, and enter the private IP address of the proxy server and the port specified for the proxy software.

Figure 8-3 Migration over a private network

9 Using MgC to Migrate Servers Without Internet Access over Private Lines

Overview

This section explains how to use Migration Center (MgC) to migrate servers without Internet access to the LA-Sao Paulo1 region.

> ⚠️ **CAUTION**
>
> This solution only applies to migration to the LA-Sao Paulo1 region.

Step 1: Install Edge, an MgC Tool

Step 1 Log in to the **Huawei Cloud console** and enable MgC in the LA-Sao Paulo1 region.

Step 2 On the MgC console, choose **Tools** in the navigation pane. **Download and install the Edge for Windows**.

Figure 9-1 Downloading Edge
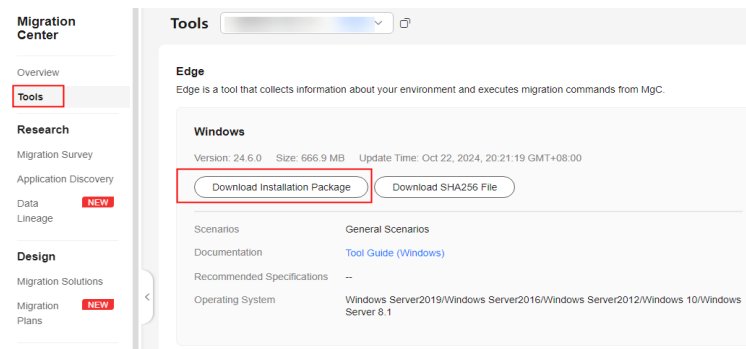
Step 3 After the Edge is installed, register an account and **connect Edge to MgC**.

----End

Step 2: Download the SMS-Agent Installation Packages

Step 1 Log in to the **SMS console** and switch to the LA-Sao Paulo1 region.

Step 2 In the navigation pane, choose **Agents**.

Step 3 Choose the **MgC Migration over Private Lines** card and download the SMS-Agent installation packages and SHA256 verification files for Linux and Windows.
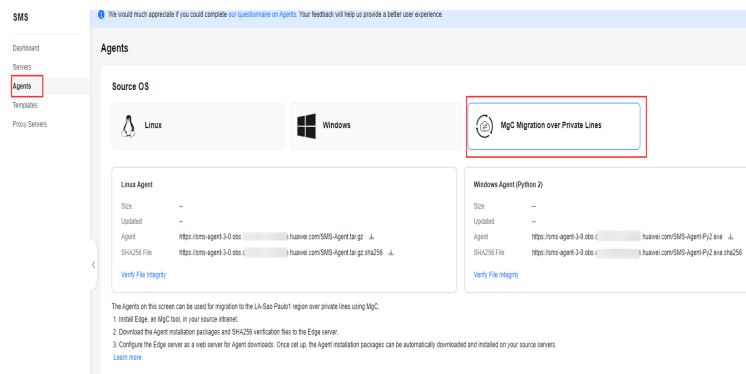
Figure 9-2 Downloading the Agent

Step 4 Save all the downloaded SMS-Agent installation packages and verification files into the same directory on the server where Edge is installed.

----End

Step 3: Configure the Server with Edge Installed as a Web Server

Step 1 On the server with Edge installed, open PowerShell ISE, and copy and paste the following script content. Then modify the script as follows:

- Replace **127.0.0.1** in the first line with the internal IP address of the server with Edge installed.

- Replace the value of **sitePath** in the second line with the directory where the SMS-Agent installation packages are stored from **step 2**.

```
$SMSAgentServerEndpoint = "127.0.0.1:443"
$sitePath = "C:\Users\Administrator\Downloads\SMS-Agent"

# Instal IIS
Install-WindowsFeature -name Web-Server -IncludeManagementTools

# Create Website content
if (-Not (Test-Path $sitePath)) {
    New-Item –Path $sitePath –ItemType Directory
}

# Add IIS website
Import-Module WebAdministration
New-Item "IIS:\Sites\SMSAgentServer" -bindings
@{protocol="http";bindingInformation="$SMSAgentServerEndpoint" + ":"} -physicalPath $sitePath

# Enable content browse
Set-WebConfigurationProperty -filter "system.webServer/directoryBrowse" -name "enabled" -value
"true" -PSPath "IIS:\Sites\SMSAgentServer"

# Set folder permissions
$acl = Get-Acl $sitePath
$acl.SetAccessRule((New-Object
System.Security.AccessControl.FileSystemAccessRule("IUSR","ReadAndExecute","ContainerInherit,Objec
```

```
tInherit","None","Allow")))
$acl.SetAccessRule((New-Object
System.Security.AccessControl.FileSystemAccessRule("IIS_IUSRS","ReadAndExecute","ContainerInherit,O
bjectInherit","None","Allow")))
Add-WebConfigurationProperty -PSPath 'IIS:\Sites\SMSAgentServer' -filter 'system.webServer/
staticContent' -name '.' -value @{fileExtension='.sha256'; mimeType='application/sha256'}

Set-Acl $sitePath $acl

# Restart IIS service
Restart-Service -Name "W3SVC"
$response = Invoke-WebRequest -Uri $SMSAgentServerEndpoint -UseBasicParsing
if ($response.StatusCode -eq 200) {
    Write-Output "Construct SMS agent server successfully!"
}

#Replace Edge SMS download url
$filePath = "C:\Edge\tools\SecAs-1.2.29\webmanagementapps\edge-server-0.0.1\WEB-INF\classes
\application.yml"
$urlPattern = "sms-agent-url:.*"
$newUrl = "sms-agent-url: http://" + $SMSAgentServerEndpoint
$fileContent = Get-Content -Path $filePath -Encoding UTF8
$fileContent = $fileContent -replace $urlPattern, $newUrl
Set-Content -Path $filePath -Value $fileContent -Encoding UTF8

#Restart Edge
Write-Output "Restart Edge server, please wait for a while..."
Restart-Service -Name "Edge_tomcat"
$edgeProcessStatus = Get-Service -Name "Edge_tomcat" | Select-Object Status
if ($edgeProcessStatus.Status -eq "Running") {
    Write-Output "Restart edge successfully"
}
```

Step 2 Run the script and wait until the script execution is complete. If the message
"Restart edge successfully" is displayed, the configuration is successful.

----End

Step 4: Create a Server Migration Workflow on MgC

Go to the MgC console and create a server migration workflow by referring to
Migrating On-premises Servers to Huawei Cloud.

10 Downsizing Disks on Linux

This section introduces how to reduce the disk capacity for a Linux server when you use SMS to migrate it to Huawei Cloud.

Prerequisites

You have performed the operations in **Preparations**.

Procedure

Step 1 **Install and start the SMS-Agent** on the source server. After the Agent is started, view the source server record on the **Servers** page of the SMS console.

Step 2 **Configure a target server**. In the **Configure Basic Settings** > **Migration Settings (Optional)** area, enable **Resize Disks and Partitions** and click **Resize Disks and Partitions**. For details about the resizing rules, see **What Are the Rules for Resizing Volume Groups, Disks, and Partitions?**

⚠️ **CAUTION**

Once set, the settings of disk and partition resizing cannot be modified. To modify the settings, delete the task, restart the SMS-Agent, and configure the the target server again.

Step 3 (Optional) Configure volume groups. If the source server uses LVM, you can resize logical and physical volumes. If the source server does not uses LVM, skip this step.

Step 4 Resize partitions and, if needed, click **Resize Disk** to adjust disk sizes.

Step 5 Click **Next: Confirm** to confirm the disk and partitions settings. Then finish the migration task configuration and start the migration.

----End