Server Migration Service

User Guide

Issue 23

Date 2025-01-24

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

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 Permissions Management

1.1 Creating a User and Assigning Permissions

This section describes how to use **IAM** for fine-grained permissions control on your SMS resources. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user is assigned their own distinct security credentials for SMS.
- Assign only the minimum permissions required for users to perform a given task.
- Entrust a Huawei Cloud account or cloud service to perform professional and efficient O&M on your SMS resources.

NOTE

A Huawei Cloud account has all the permissions required for using SMS by default. If you use your Huawei Cloud account to perform migration, skip this chapter.

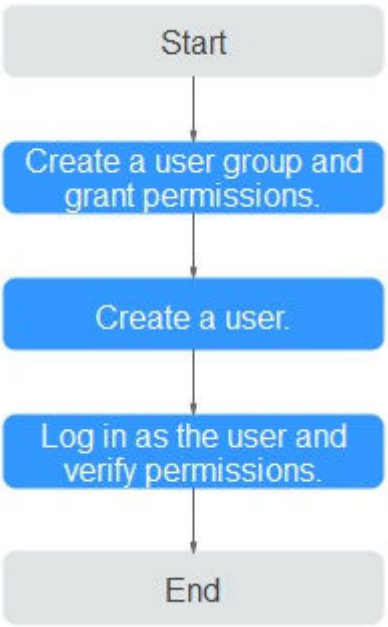
Figure 1-1 shows the process for assigning permissions.

Prerequisites

Before assigning permissions to user groups, you should learn about system policies supported by SMS and choose policies or roles based on service requirements. For more information about system policies supported by SMS, see **SMS Permissions**. For the permissions supported by other services, see **System-defined Permissions**.

Process Flow

Figure 1-1 Process for assigning SMS permissions



Procedure

Step 1 **Create a user group and assign permissions** to it.

- If the IAM users who will be added to this group need all SMS permissions, attach system-defined policies **SMS FullAccess**, **OBS OperateAccess**, **ECS FullAccess**, **VPC FullAccess**, and **EVS FullAccess** to the group. EVS KMSAccess must be attached if disk encryption is required.
- If the IAM users only need specific SMS permissions, create custom policies and attach these policies to the user group. For details, see **SMS Custom Policies**.

  NOTE

  Compared with system-defined policies, custom policies provide more fine-grained and secure permissions control.

Step 2 **Create a user and add it to a user group**.

Create a user on the IAM console and add the user to the group created in **Step 1**.

Step 3 **Sign in** as the created user and verify permissions.

In the authorized region, perform the following operations:

- Choose **Service List** > **Server Migration Service**. In the navigation pane on the left, choose **Servers**. In the server list, locate the server to be migrated, and click **Configure** in the **Target** column to configure the target server. If the target server can be configured, the permissions have taken effect.

- Choose a service other than SMS and its dependents services in the **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the permissions have taken effect.

----End

1.2 SMS Custom Policies

You can create custom policies using the visual editor, or with a JSON file.

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. If you need to migrate source servers to a specific enterprise project, create a custom policy by referring to **Assigning Permissions to a User Group by Enterprise Project**.

The following are example SMS custom policies:

- Example SMS policy that contains permissions for project-level services

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "vpc:securityGroups:create",
                "vpc:securityGroupRules:create",
                "vpc:vpcs:create",
                "vpc:publicIps:create",
                "vpc:subnets:create",
                "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: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",
                "ecs:servers:reboot",
                "evs:volumes:use",
                "evs:volumes:create",
                "evs:volumes:update",
                "evs:volumes:delete",
                "evs:volumes:attach",
                "evs:volumes:detach",
                "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"
    }
  ]
}
```

- Example SMS policy that contains permissions for global services

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

For details about policies supported by SMS, see **Table 1-1**.

Table 1-1 Policy description

Policy	Permission Description
sms:server:queryServer	Read-only permission for viewing source servers
sms:server:registerServer	Read/write permissions for registering source servers
sms:server:migrationServer	Read/write permissions for migrating source servers

2 Installing the Agent on the Source Server

2.1 Installing the Agent on Windows

Scenarios

You need to install the Agent on the source server to be migrated. During the installation, you need to enter the AK/SK pair of the Huawei Cloud account you are migrating to. After the Agent is started, it automatically reports source server information to SMS. The information is used for migration only. For details, see **What Information Does SMS Collect About Source Servers?**

NOTE

Before using SMS to migrate servers, you need to manually install and register the Agent on each server to be migrated. If there are more than 50 servers to migrate, you can **create a server migration workflow** on MgC to automate batch installation and registration of the Agent.

There are two options for Windows:

- GUI-based Windows Agent (Python 3): Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows 10, and Windows 8.1
- CLI-based Windows Agent (Python 2): Windows Server 2008 and Windows 7

CAUTION

You must log in to the source server as user **Administrator**.

Prerequisites

- You have obtained an AK/SK pair for your Huawei Cloud account.
  - If you use an IAM user for migration, obtain an AK/SK pair by referring to **How Do I Create an AK/SK Pair for an IAM User?**

  - If you use an account for migration, obtain an AK/SK pair by referring to **How Do I Create an AK/SK Pair for an Account?**
- You have obtained the administrator permissions for the source server.
- You have confirmed that the source server OS is supported by SMS. Learn more about **supported Windows OSs**.
- There is no antivirus software on the source server. Antivirus software may prevent the Agent from starting up.

  If you encounter Agent startup failures due to antivirus software, refer to the instructions in **How Do I Fix Error "Failed to start the I/O monitoring module" When I Start the Agent?**

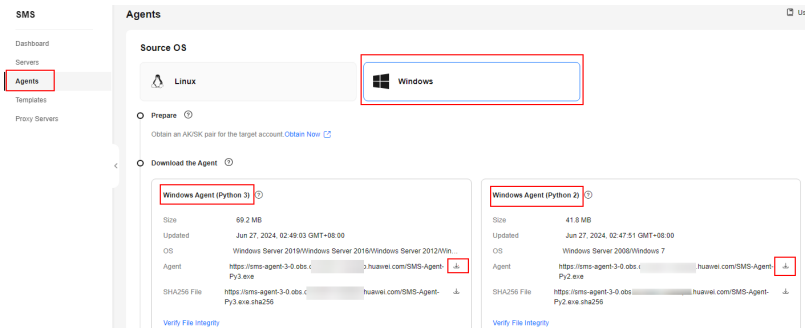
Downloading the Agent Installation File

Step 1 Sign in to the **SMS console**.

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

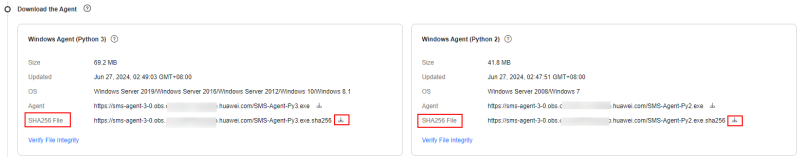
Step 3 Select the **Windows** card, locate the Agent that matches the source server OS, and click the icon next to **Agent**.

- GUI-based Windows Agent (Python 3): Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows 10, and Windows 8.1
- CLI-based Windows Agent (Python 2): Windows Server 2008 and Windows 7



Step 4 Read and agree to the service disclaimer, and click **Yes** to download the Agent installation file.

Step 5 Click the icon next to **SHA256 File** to download the file that contains a hash value to a local directory. Verify the integrity of the Agent installation file. For details, see **How Do I Verify the Integrity of the Agent Installation File?**



----End

Installing the Windows Agent (Python 3)

Step 1 Transmit the **SMS-Agent-Py3.exe** file to the source server.

Step 2 Log in to the source server as user **Administrator** and double-click the **SMS-Agent-Py3.exe** file.

Step 3 Click **Install** and wait for the installation to complete.

Step 4 Click **Finish**. The SMS-Agent GUI is displayed.

Step 5 Enter the AK/SK pair for the Huawei Cloud account and the SMS domain name for the region you are migrating to. You can obtain the SMS domain name on the **Agents** page of the SMS console, as shown in **Figure 2-2**.

- If you do not need to use an HTTP/HTTPS proxy, select **Direct Connection**.
- If you need to use an HTTP/HTTPS proxy, select **Use Proxy** and enter the IP address, port number, username, and password of the proxy server.

  NOTE

  - **Proxy Server IP**: Follow the format **https://***your-proxy-addr***.com**. Use the protocol configured for your proxy server. HTTPS is recommended. Replace *your-proxy-addr* with the IP address of your proxy server, not that of the target server.
  - **Port**: Enter the port used by the proxy server.
  - **Proxy user name**: Enter the username required for using the proxy software. If no username is required, leave this parameter blank.
  - **Password**: Enter the password corresponding to the proxy username. If no password is required, leave this parameter blank.

Figure 2-1 Starting the Agent

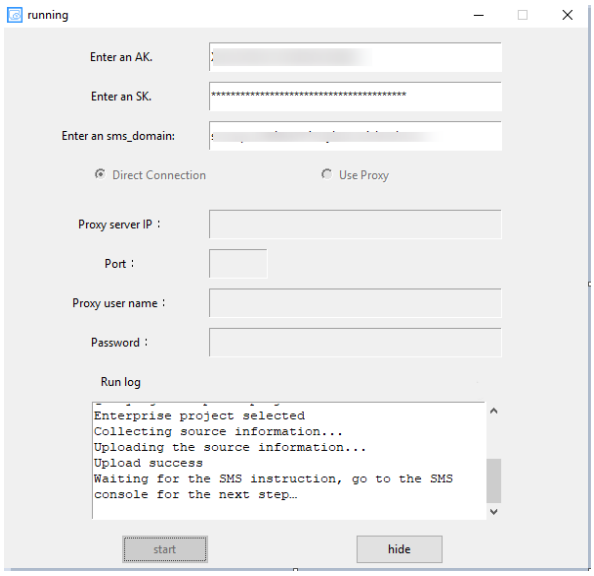
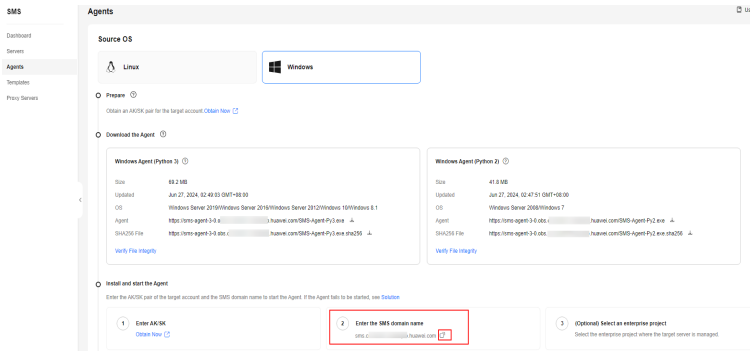


Figure 2-2 Obtaining the SMS domain name



Step 6 If the EPS service has been enabled for the Huawei Cloud account, after you entered the AK/SK pair, the Agent will list all enterprise projects the account is allowed to access. You can select the enterprise project you would like to migrate the source server to. This enables you to isolate permissions, resources, and finance during the migration. For details, see **Migrating Servers into an Enterprise Project**.

Step 7 Click **start**.

Step 8 Carefully review the **Privacy Statement** and click **Yes** if you want to continue.

When the message "Upload success. Waiting for the SMS instruction" is displayed, the Agent has been started. You can sign in to the SMS console and perform subsequent operations.

----End

Installing the Windows Agent (Python 2)

Step 1 Transmit the **SMS-Agent-Py2.exe** file to the source server.

Step 2 Log in to the source server as user **Administrator** and double-click the **SMS-Agent-Py2.exe** file.

Step 3 Click **Install** and wait for the installation to complete.

Step 4 Click **Finish**. The SMS-Agent CLI is displayed.

NOTE

If you need to rerun the Agent, double-click **agent-start.exe** in the **C:\SMS-Agent-Py2** directory where the Agent was installed.

Step 5 If you need to use an HTTP/HTTPS proxy, go to **6**.

If you do not need to use an HTTP/HTTPS proxy, go to **7**.

NOTE

- If your source server cannot access Huawei Cloud over the Internet, you can use a proxy server. You will need to configure the proxy server yourself.
- In a migration over a private line or VPN, a proxy server is used for registering the source server with SMS. It is not used for data migration.

Step 6 (Optional) Configure the HTTP/HTTPS proxy for the Agent.

Go to the directory where the Agent was installed (typically **C:\SMS-Agent-Py2\config**) and edit the **auth.cfg** file. Do not edit the **auth.cfg** file unless you need to use an HTTP/HTTPS proxy.

```
[proxy-config]
enable = true
proxy_addr = https://your-proxy-addr.com
proxy_port = proxyport
proxy_user =
use_password = false
```

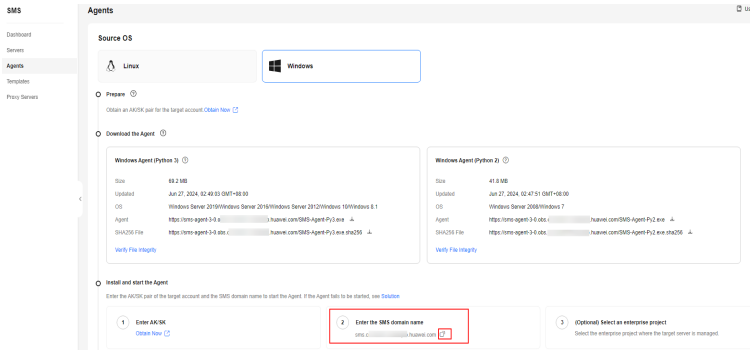
NOTE

- **enable**: To use a proxy, set this parameter to **true**.
- **proxy_addr**: Replace *your-proxy-addr* with the IP address of the proxy server, not that of the target server. Use the protocol configured for the proxy. HTTPS is recommended.
- **proxy_user**: Enter the username required for the proxy. If no username is required, leave it blank.
- **use_password**: If a password is required for the proxy, set it to **true**. If no password is required, set it to **false**.

Step 7 When prompted, enter the AK/SK pair for the Huawei Cloud account and the SMS domain name for the region you are migrating to. You can obtain the SMS domain name on the **Agents** page of the SMS console, as shown in **Figure 2-3**.

If the EPS service has been enabled for the Huawei Cloud account, after you entered the AK/SK pair, the Agent will list all enterprise projects the account is allowed to access. You can select the enterprise project you would like to migrate the source server to. This enables you to isolate permissions, resources, and finance during the migration. For details, see **Migrating Servers into an Enterprise Project**.

Figure 2-3 Obtaining the SMS domain name



After the authentication succeeds, the Agent starts to report source server information to SMS, and the window is closed. You can go to the **Servers** page on the SMS console to view the record of the source server.

----End

Troubleshooting

- **SMS.0202 AK/SK Authentication Failed**
- **Why Wasn't My Source Server Added to the SMS Console After I Configured the Agent?**

2.2 Installing the Agent on Linux

Scenarios

You need to install the Agent on the source server to be migrated. During the installation, you need to enter the AK/SK pair of the Huawei Cloud account you are migrating to. After the Agent is started, it automatically reports source server information to SMS. The information is used for migration only. For details, see **What Information Does SMS Collect About Source Servers?**

NOTE

Before using SMS to migrate servers, you need to manually install and register the Agent on each server to be migrated. If there are more than 50 servers to migrate, you can **create a server migration workflow** on MgC to automate batch installation and registration of the Agent.

Prerequisites

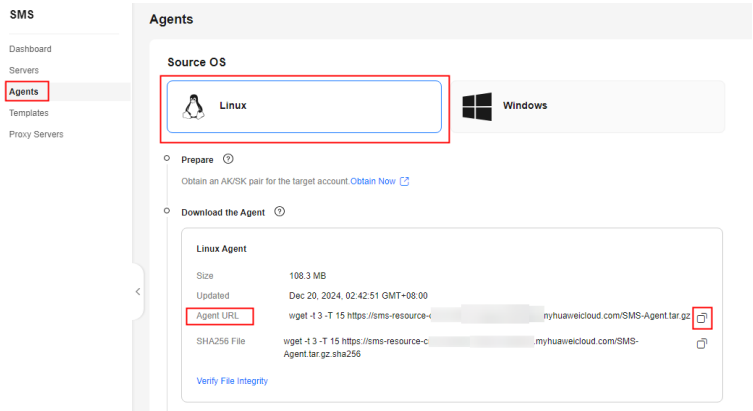
- You have obtained an AK/SK pair for your Huawei Cloud account.
  - If you use an IAM user for migration, obtain an AK/SK pair by referring to **How Do I Create an AK/SK Pair for an IAM User?**
  - If you use an account for migration, obtain an AK/SK pair by referring to **How Do I Create an AK/SK Pair for an Account?**
- You have confirmed that the source server OS is supported by SMS. Learn more about **supported Linux OSs**.

Procedure

Step 1 Sign in to the **SMS console**.

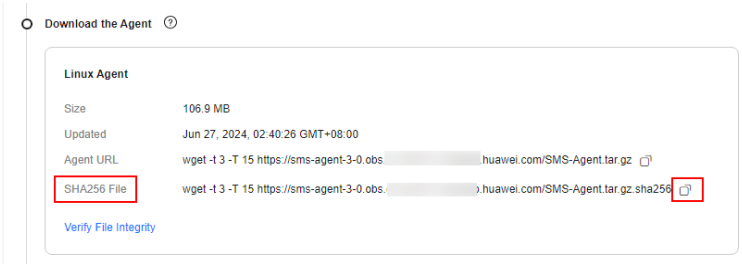
Step 2 In the navigation pane on the left, choose **Agents**.

Step 3 Select the **Linux** card, and in the **Linux Agent** area, click the icon next to **Agent** to copy the Agent download command. Run the command on the source server to download the Agent installation package.



Step 4 Copy the command next to **SHA256 File** and run the command on the source server. Use the hash value contained in the SHA256 file to verify the integrity of

the Agent installation package. For details, see **How Do I Verify the Integrity of the Agent Installation File?**



Step 5 Decompress the Agent software package.

```
tar -zxvf SMS-Agent.tar.gz
```

Step 6 Switch to the **SMS-Agent** directory on the source server.

```
cd SMS-Agent
```

Step 7 If you need to use an HTTP/HTTPS proxy, go to **8**.

If you do not need to use an HTTP/HTTPS proxy, go to **9**.

CAUTION

- If your source server cannot access Huawei Cloud over the Internet, you can use a proxy server. You will need to configure the proxy server yourself.
- In a migration over a private line or VPN, a proxy server is used for registering the source server with SMS. It is not used for data migration.

Step 8 (Optional) Configure the HTTP/HTTPS proxy for the Agent.

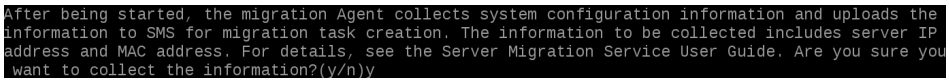
1. Go to the **config** directory.
   ```
   cd SMS-Agent/agent/config
   ```
2. Open and edit the **auth.cfg** file. Do not edit the **auth.cfg** file unless you need to use an HTTP/HTTPS proxy.
   ```
   vi auth.cfg
   ```
   The values shown here are for reference only.
   ```
   [proxy-config]
   enable = true
   proxy_addr = https://your-proxy-addr.com
   proxy_port = 3128
   proxy_user = root
   use_password = true
   ```
   NOTE
   - **enable**: To use a proxy, set it to **true**.
   - **proxy_addr**: Replace *your-proxy-addr* with the IP address of the proxy server, not that of the target server. Use the protocol configured for the proxy. HTTPS is recommended.
   - **proxy_user**: Enter the username required for the proxy. If no username is required, leave it blank.
   - **use_password**: If a password is required for the proxy, set it to **true**. If no password is required, set it to **false**.
3. Save the **auth.cfg** file and exit.
   ```
   :wq
   ```


Step 9 Start the Agent.

```
./startup.sh
```

Step 10 Carefully review what information will be collected by the Agent, enter **y**, and press **Enter**.

Figure 2-4 Entering y



Step 11 Enter the AK/SK pair for the Huawei Cloud account and the SMS domain name for the region you are migrating to. You can obtain the SMS domain name on the **Agents** page of the SMS console, as shown in **Figure 2-6**.

Figure 2-5 Entering the AK/SK pair

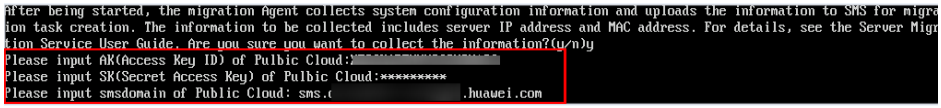
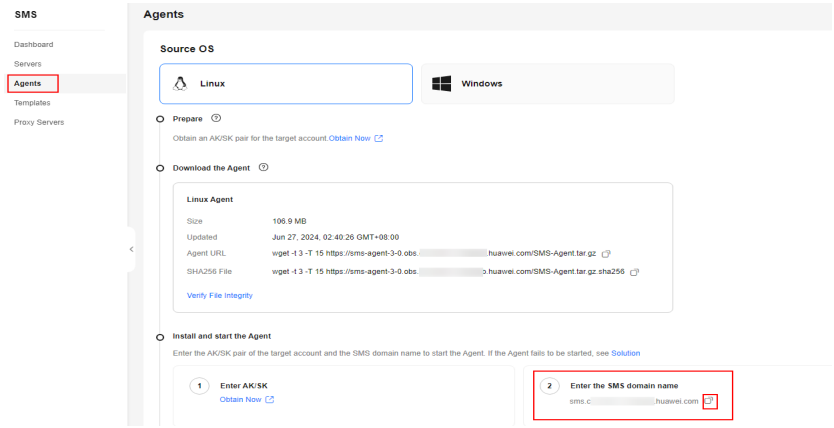


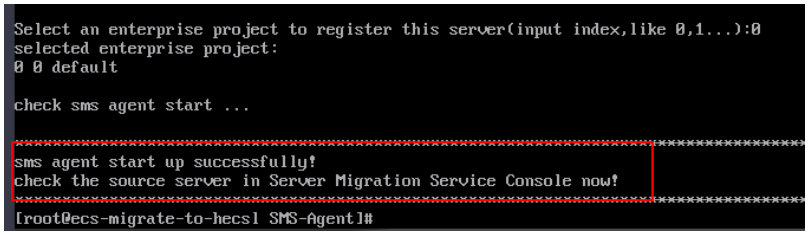
Figure 2-6 Obtaining the SMS domain name



If the EPS service has been enabled for the Huawei Cloud account, after you entered the AK/SK pair, the Agent will list all enterprise projects the account is allowed to access. You can select the enterprise project you would like to migrate the source server to. This enables you to isolate permissions, resources, and finance during the migration. For details, see **Migrating Servers into an Enterprise Project**.

When the following information is displayed, the Agent has been started up and will automatically start reporting source server information to SMS. You can go to the **Servers** page on the SMS console to view the record of the source server.

Figure 2-7 Agent running



----End

Troubleshooting

- **How Do I Resolve Error "No such file or directory: 'rsync':'rsync" When I Start the Linux Agent?**
- **SMS.0202 AK/SK Authentication Failed**
- **Why Wasn't My Source Server Added to the SMS Console After I Configured the Agent?**

3 Migration Management

3.1 Configuring a Target Server

Scenarios

Before starting the migration, you need to configure the target server, which will receive data from the source server. You can clone the target server for service testing and launch it once you've confirmed that your services can run properly.

Prerequisites

You can configure the target server when:

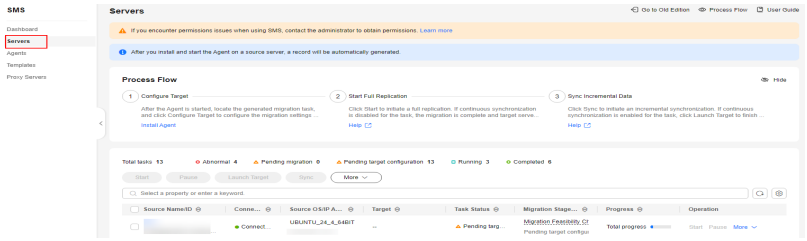
- The source server is **Connected** to SMS.
- The migration task is in the **Migration Feasibility Check** stage.
- The migration task is in the **Pending target configuration** status.

Procedure

Step 1 Sign in to the **SMS console**.

Step 2 In the navigation pane on the left, choose **Servers**.

Figure 3-1 Server list

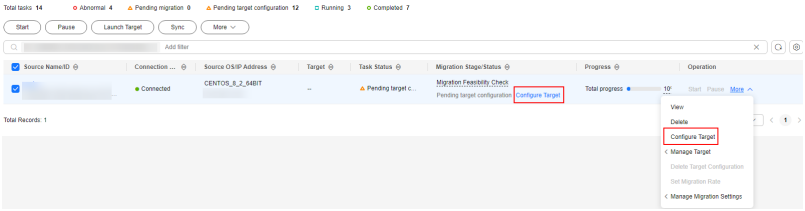


Step 3 In the server list, locate the source server and click **Configure Target** in the **Migration Stage/Status** column.

You can also choose **More** > **Configure Target** in the **Operation** column.

NOTICE

If you do not find the record for your source server, check that the account you are currently using is the migration account.



Step 4 On the **Configure Basic Settings** page, configure parameters by referring to **Table 3-1**.

Table 3-1 Basic parameter settings

Area	Parameter	Option	Description
Migration Template	Migration Template	-	You can use the default migration template provided by the system. You can also **create a migration template** . After you choose a migration template, the system will populate the settings for **Network Type**, **Migration Rate Limit**, **Migration Method**, **Enable Continuous Synchronization**, **Resize Disks and Partitions**, **Region**, and **Project** based on the template.
Network Settings	Network Type	Public	An EIP must be bound to the target server. **Public** is the default value of **Network Type**.
		Private	A Direct Connect connection, VPN connection, VPC peering connection, VPC subnet, or Cloud Connect connection must be provisioned. The private IP address of the target server will be used for migration.
	IP Version	IPv4	IPv4 can be used for data migration.
		IPv6	On a dual-stack network, IPv6 can be used for migration. For details about the preparations and precautions for migration over IPv6, see **Migrating Servers over an IPv6 Network**.

Area	Parameter	Option	Description
	Migration Rate Limit	-	You can limit the migration rate based on the source bandwidth and service requirements. If you do not want to limit the migration rate, set this parameter to **0**. Traffic limiting is unavailable if: ● The migration uses an IPv6 network. ● Traffic Control (TC) is missing from the source server.
	Overrate Threshold (%)	-	You can regulate how much the migration rate can exceed the configured limit. If the migration rate exceeds the threshold for multiple consecutive times, the migration task is automatically paused. For example, if the migration rate limit is set to 10 Mbit/s and the overrate threshold is set to 10%, the task is automatically paused when the migration rate exceeds 11 Mbit/s (110% of the limit) multiple times consecutively. **CAUTION** This option is only available for Linux migration. It will not be available or applied if: ● The migration uses an IPv6 network. ● Traffic Control (TC) is missing from the source server. ● The installed SMS-Agent version is earlier than 24.9.0.
Migration Settings (Optional)	Migration Method	Linux block-level	Migration and synchronization are performed by block. This method is efficient, but the compatibility is poor.
		Linux file-level	Migration and synchronization are performed by file. This method is inefficient, but the compatibility is excellent.
		Windows block-level	Migration and synchronization are performed by block. This method is very efficient and is the only migration method for Windows servers.

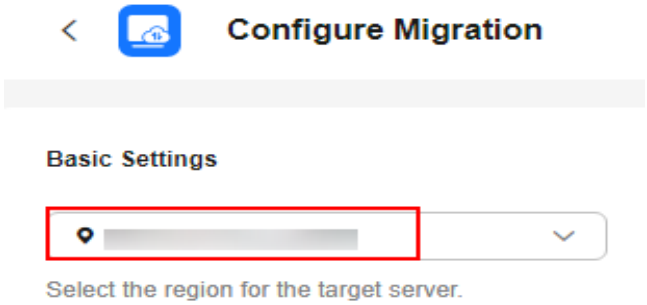
Area	Parameter	Option	Description
	Enable Continuous Synchronization	No	After the full replication is complete, SMS will automatically launch the target server without synchronizing incremental data. To synchronize incremental data, you will need to click **Sync** in the **Operation** column.
		Yes	After the full replication is complete, the migration will enter the continuous synchronization stage. During this stage, incremental data will be periodically synchronized from the source server to the target server, and you will be unable to use the target server since it has not been launched yet. To finish this stage, you will need to click **Launch Target** in the **Operation** column.
	Resize Disks and Partitions	No	The disk and partition settings from the source server will be retained on the target server.
		Yes	You can resize the disks and partitions for the target server. For details, see **Resizing disks and partitions**.
	Start Target Upon Launch	No	The target server will be stopped after the migration is complete.
		Yes	The target server will be started after the migration is complete.
	Measure Network Performance	No	Network performance will not be measured.
		Yes	Before the full migration starts, the system will measure the packet loss rate, network jitter, network latency, bandwidth, memory usage, and CPU usage for the source server. For details, see **How Do I Measure the Network Performance Before the Migration?**
	Enable Concurrency	No	By default, one process is used for migration and synchronization.

Area	Parameter	Option	Description
		Yes	You can specify the maximum number of processes the Agent can start concurrently for migration and synchronization tasks, respectively. Enabling concurrency is only available for Linux file-level migrations. For more information, see **How Do I Set the Number of Concurrent Processes for Linux File-Level Migrations?**
	Transit IP Address	-	For a migration over a private line, you can configure the transit IP address.
Resource Limits (Optional)	CPU Limit	-	These options are only available for Linux migrations. For details, see **How Do I Limit Resource Allocation for the Agent in a Linux Migration?**
	Memory Limit		
	Disk Throughput Limit		

Area	Parameter	Option	Description
Verify Data Consistency	If this option is enabled, the system will automatically verify data consistency after the full replication is complete. This is a quick verification, and only the file size and last modification time will be verified. You can modify the verification policy when you launch an incremental synchronization. • **Enable Hash Verification**: If this option is enabled, the system will generate and compare hash values for each file to be verified. Hash verification is recommended when individual files are large and important. Enabling this option will increase CPU and disk I/O overheads for the source server and extend the verification time. **CAUTION** – Hash values cannot be calculated for files in use, so these files will be skipped during the verification. – Enabling this option requires you to specify the verification scope, and only files in the specified scope will be verified. • Verification Scope – Under **Exclude paths**, enter the paths you want to exclude from the verification. A maximum of 30 paths can be entered. Use commas (,) to separate the paths. For example, **/root/data,/var**. Leaving it empty will initiate a full verification. – Under **Include paths**, enter the paths you want to verify. **NOTICE** • If the entered paths are incorrect or empty, 0 will be displayed for them in the verification results. • The more data you need to verify, the longer the consistency check will take. It is wise to focus on verifying only key paths. • The following paths will be excluded from consistency verification by default: – Linux: **/bin**, **/boot**, **/dev**, **/home**, **/etc**, **/lib**, **/media**, **/proc**, **/sbin**, **/selinux**, **/sys**, **/usr**, **/var**, **/run**, and **/tmp** – Windows: top-level directories of partitions, for example, **C:** and **D:** If you need to include any of the preceding excluded paths in the verification, refer to **Modifying the Default Excluded Paths**.		

Step 5 Click **Next: Configure Target** in the lower right corner.

Step 6 In the **Basic Settings** area, select the region you are migrating to.



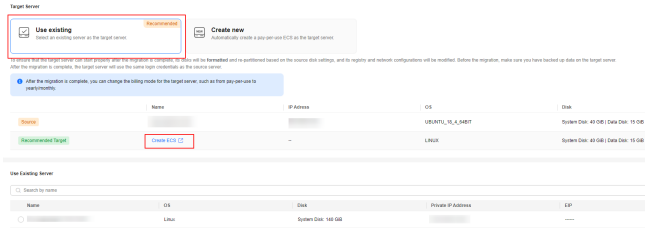
Step 7 In the **Target Server** area, choose whether to use an existing cloud server or create a new one as the target server. For details about the requirements on target servers, see **Target Server Requirements**.

- **Use existing**

  In the list of existing servers, select one that meets the specifications requirements displayed in the **Recommended Target** row. If no existing server meets the requirements, click **Create ECS** and purchase an ECS with the required specifications. For details, see **Purchasing an ECS**.

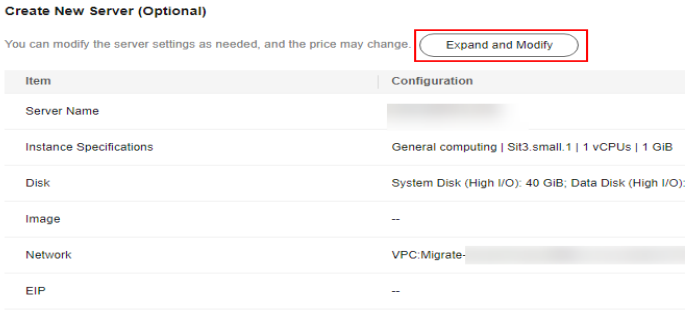
  NOTE

  You can select a pay-per-use or yearly/monthly ECS.



- **Create new**

  The system automatically presets the name, AZ, specifications, disk specifications, EIP, VPC, subnet, and security group for the target server. You can also click **Expand and Modify** to manually modify the server settings.



  – If you select **Recommended** for **Server Template**, the system will automatically create a VPC, subnet, and security group and select an AZ and disk type for the target server. You can also manually adjust the settings recommended by the system.

NOTE

- If **Create during migration** is selected for **VPC**, SMS automatically creates a VPC for the target server based on the following rules:

  If the source server's IP address is 192.168.*X.X*, SMS creates a VPC and a subnet that both belong to network range 192.168.0.0/16.

  If the source IP address is 172.16.*X.X*, SMS creates a VPC and a subnet that both belong to network range 172.16.0.0/12.

  If the source server's IP address is 10.*X.X*, SMS creates a VPC and a subnet that both belong to network range 10.0.0.0/8.

- If **Create during migration** is selected for **Security Group**, the system automatically creates a security group for the target server and allows traffic to the target server over certain ports:

  Windows: ports 8899, 8900, and 22

  Linux (file-level migration): port 22

  Linux (block-level migration): ports 8900 and 22

– If you prefer, you can choose your own server template, and the VPC, subnet, security group, AZ, and disk settings will be preconfigured based on that template. You have the flexibility to adjust these preset settings as needed. To learn how to create a server template, see **Creating a Server Template**.

– Configure advanced disk settings.

- Data disks must be either VBD or SCSI. VBD is the default device type for data disks. For details about disk device types, see **Device Types and Usage Instructions**.
- Data disks can be created as shared disks. For details about shared disks, see **Shared EVS Disks and Usage Instructions**.
- For target servers newly created by the system, system and data disks can be encrypted. For details about shared disks, see **Shared EVS Disks and Usage Instructions**. To enable disk encryption, you need to create an agency to authorize EVS to access KMS. After the authorization is successful, configure the following parameters:
  - Select an existing key

    Select a key from the drop-down list. You can select one of the following keys:

    Default keys: After the KMS access permissions have been granted to EVS, the system automatically creates a default key and names it **evs/default**.

    Custom keys: You can choose an existing key or create a new one. For details about how to create a key, see **Creating a Key**.
  - Enter a key ID

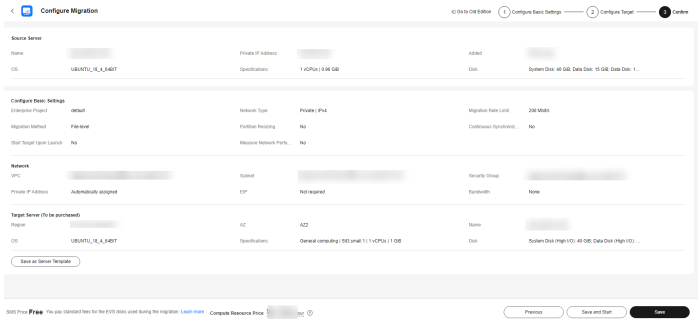
    Enter the ID of a key shared from another user. Ensure that the key is in the target region. For details, see **Creating a Grant**.

NOTICE

- Before the migration is complete, do not disable or delete the key used, or the migration will fail.
- The encryption attribute of a disk cannot be modified after the disk is created.
- Keys can be shared with accounts, not users.
- If KMS encryption is used, you will be billed for what you use beyond the free quota given by KMS. For details, see **DEW Billing**.

Step 8 Click **Next: Confirm** in the lower right corner.

Figure 3-2 The configuration confirmation page

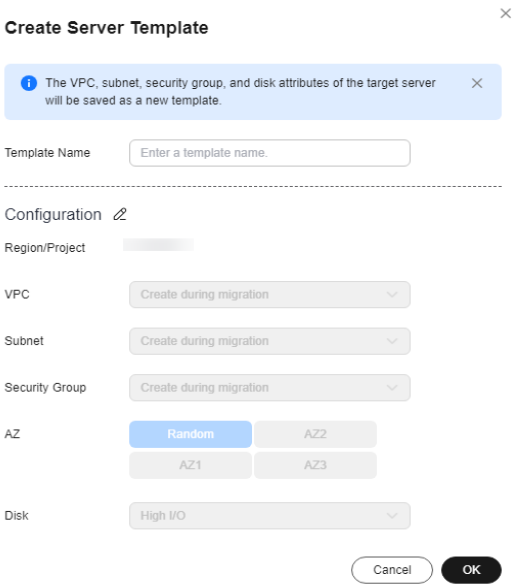


Step 9 (Optional) Click **Save as Server Template**. In the displayed **Create Server Template** dialog box, enter a template name and click **OK** to save the target server settings as a template.

NOTE

Save as Server Template is available only when you select **Create new** for **Server**.

Figure 3-3 Create Server Template



Step 10 Confirm the configuration and click **Save**. In the displayed dialog box, read the migration conditions and click **OK**.

If you want to start the migration immediately, click **Save and Start**. In the displayed dialog box, read the migration conditions and click **OK**.

Figure 3-4 Saving the configuration

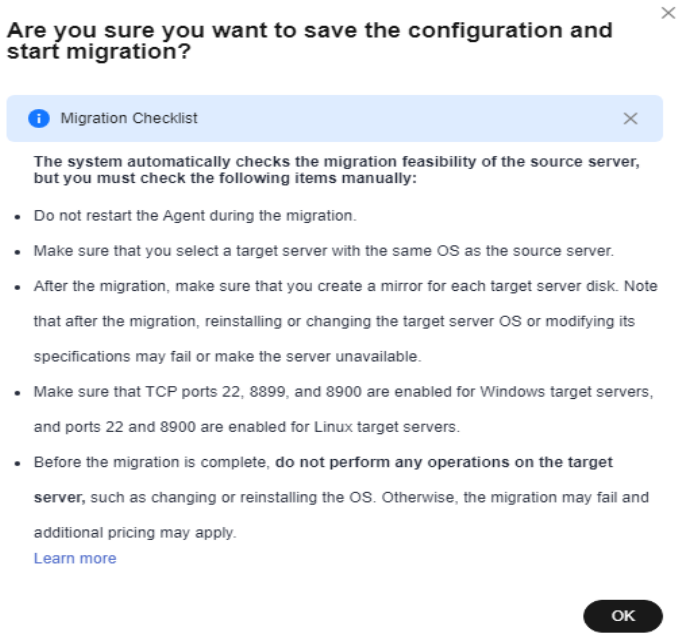
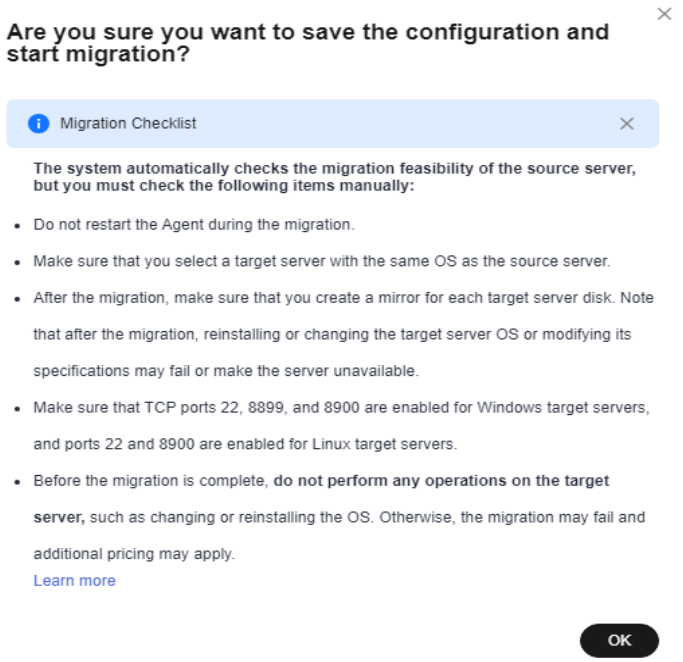


Figure 3-5 Saving the configuration and starting the migration



NOTE

If **Target Configuration** and **Ready** show up in the **Migration Stage/Status** column, the target server has been configured.

----End

Resizing Disks and Partitions

Step 1 When you create a migration task, on the **Configuring Basic Settings** tab page, expand **Migration Settings (Optional)**, enable **Resize Disks and Partitions**, and click **Resize Disks and Partitions**. In the **Resize Disks and Partitions** dialog box, configure disks and partitions as needed.

Figure 3-6 Resizing disks and partitions (Windows)

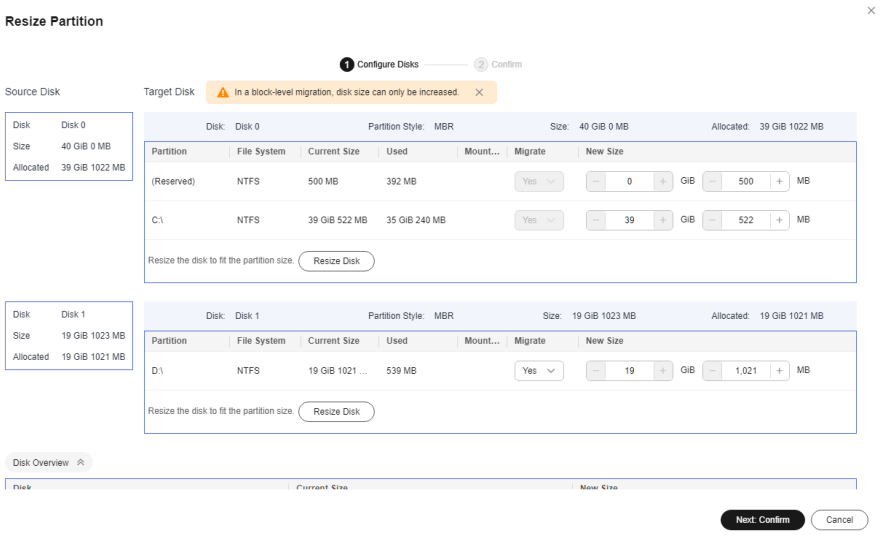
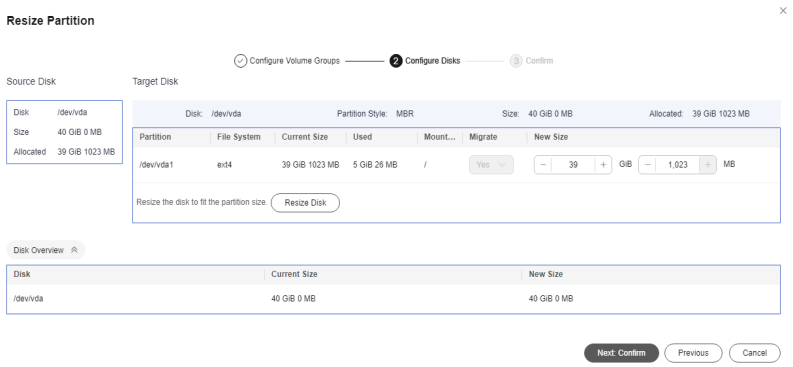


Figure 3-7 Resizing disks and partitions (Linux)



NOTE

- You can choose whether to migrate source partitions and then resize the paired target partitions.
- For a Linux server using LVM, you can choose whether to migrate physical or logical volumes and resize the paired target volumes.

CAUTION

- In a Windows migration, the system and boot partitions are migrated by default.
- In a Windows migration, you can upsize partitions, but you cannot downsize them.
- Partition resizing is not available for Btrfs partitions on Linux.
- In a Linux migration, the system and swap partitions are migrated by default.
- You can choose to migrate all or none volume groups by using the **Migrate All Volume Groups** option.
- If you choose to migrate none of the logical volumes in a volume group, their physical volumes will not be migrated by default.
- In a Linux block-level migration, you can upsize partitions, but you cannot downsize them.
- In a Linux file-level migration, you can upsize or downsize partitions. When downsizing a partition, the new partition size must be at least 1 GB larger than the used partition space. If the current size does not meet this condition, downsizing is not possible. If the current size does not meet this condition, downsizing is not possible. For details, see **What Are the Rules for Resizing Volume Groups, Disks, and Partitions?**
- If the total partition size after resizing is larger than the disk size, you need to expand the disk capacity to fit the partition size.
- If the total partition size after resizing is much smaller than the disk size, you can downsize the disk.

Step 2 Click **Next: Configure Disks**. Resize the disks as needed. Then confirm the configurations and click **OK**.

CAUTION

After you click **OK**, disk and partition resizing cannot be disabled in this task. If you want to restore the original disk and partition settings, locate the source server and choose **More** > **Delete** in the **Operation** column. Then restart the Agent on the source server, and configure the target server again.

----End

3.2 Starting a Full Replication

Scenarios

A full replication replicates all data from the source server to the target server. The replication speed depends on the outbound bandwidth of the source server or the inbound bandwidth of the target server, whichever is smaller.

Constraints

After a full replication starts, do not restart the source server or Agent, or the migration will fail.

Prerequisites

- The target server has been configured. For details, see **Configuring a Target Server**.
- The migration task is in the **Full Replication** stage and the status is **Ready**.

Procedure

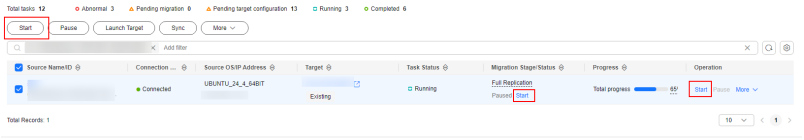
Step 1 Sign in to the **SMS console**.

Step 2 In the navigation pane on the left, choose **Servers**.

Step 3 Locate the source server and click **Start** in the **Migration Stage/Status** or **Operation** column. In the displayed **Start Migration** window, click **OK** to start a full replication.

You can also select the source server and click **Start** above the server list. In the displayed **Start Migration** window, click **OK**.

Figure 3-8 Starting a full replication



NOTE

During the full replication, the target server is locked by default, and you are not allowed to perform any operations on it. After the migration is complete, the target server will be automatically unlocked. If you need to perform operations on the target server during the replication, **unlock the target server**.

Step 4 In the server list, click the name of the source server to view the migration progress.

Step 5 Wait for the full replication to complete.

- If you set **Continuous Synchronization** to **No** when you configure the migration settings, after the full replication is complete, the system puts the migration to a **Target Launch** stage and launches the target server to complete the migration automatically.
- If you set **Continuous Synchronization** to **Yes** when you configure the migration settings, after the full replication is complete, the system puts the migration to a **Continuous sync** status. You will need to manually launch the target server to complete the migration. For details, see **Launching a Target Server**.

After the migration and service cutover are complete, you need to adjust the configurations of the target server based on service requirements. For details, see

What Configuration Items Need to Be Manually Modified After a Server Is Migrated?

----End

3.3 Synchronizing Incremental Data

Scenarios

After the target server is launched, if there are data changes on your source server, you can synchronize the incremental data to the target server.

NOTE

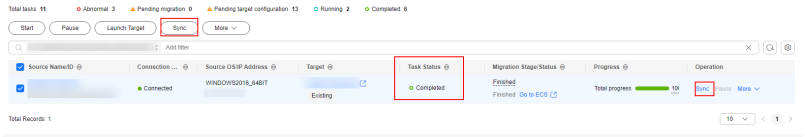
You can synchronize data from a source server only when its migration status is **Finished**.

Procedure

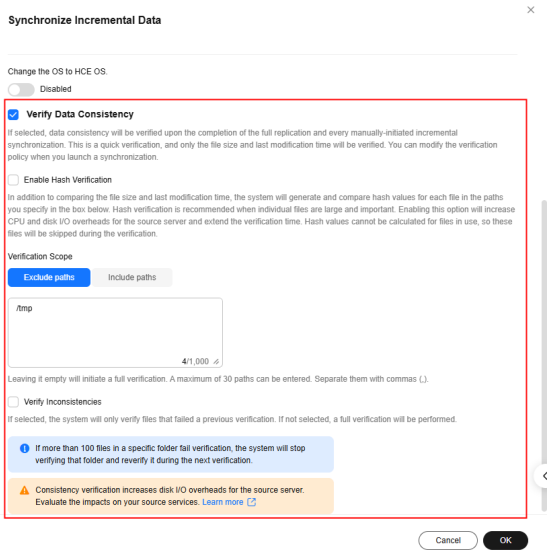
Step 1 Sign in to the **SMS console**.

Step 2 In the navigation pane on the left, choose **Servers**.

Step 3 In the server list, locate the source server you want to synchronize and click **Sync** in the **Operation** column.



Step 4 In the **Sync Incremental Data** dialog box, carefully read the tips, enable **Verify Consistency** if needed, and click **OK**. For details about this option, see **How Do I Verify Data Consistency Between the Source and Target Servers?**



----End

3.4 Setting a Migration Rate

Scenarios

During a migration, a large amount of traffic is generated and bandwidth consumed. To reduce the impact of the migration on services, you can limit the migration rate.

Procedure

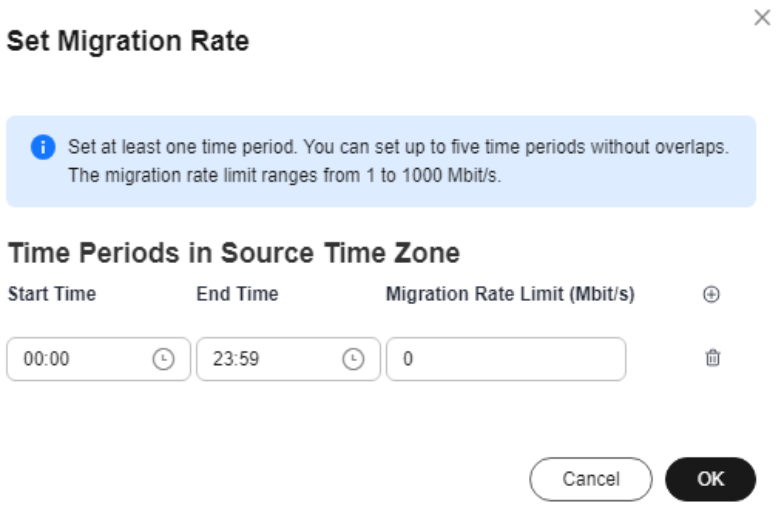
Step 1 Sign in to the **SMS console**.

Step 2 In the navigation pane on the left, choose **Servers**.

Step 3 Locate the server for which you want to set the migration rate, and choose **More** > **Set Migration Rate** in the **Operation** column.

Step 4 In the displayed **Set Migration Rate** dialog box, set migration rate limits for different periods of time and click **OK**.

Figure 3-9 Setting migration rate limits



NOTE

A migration rate limit must be an integer from 0 to 1,000.

- You can enter **0** or leave this field blank to remove migration rate limits. Then data will be migrated at the speed of the network between the source and target servers.
- The migration rate is bottlenecked by the migration rate limit you configure or the actual network speed, whichever is smaller.

----End

3.5 Deleting a Migration Task

Scenarios

You can delete a server migration task or record if it is no longer needed.

CAUTION

- After deleting a server migration record, if you want to register the source server again with SMS, restart the Agent on the source server.
- Deleting a migration record will not delete the involved source or target server.

Procedure

Step 1 Sign in to the **SMS console**.

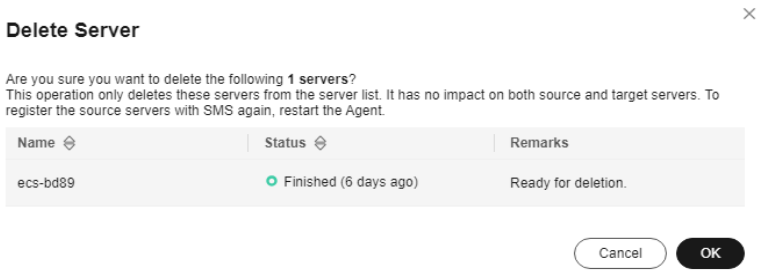
Step 2 In the navigation pane on the left, choose **Servers**.

Step 3 Locate the migration record you want to delete, and choose **More** > **Delete** in the **Operation** column.

You can also select the record and choose **More** > **Delete** in the upper left corner of the server list.

Step 4 In the displayed **Delete Server** dialog box, click **OK**.

Figure 3-10 Confirmation



----End

4 Target Server Management

4.1 (Optional) Cloning a Target Server

Scenarios

Before launching a target server, you can clone the target server for service testing, and only launch the target server after tests confirm there are no issues.

NOTE

The cloned server must be in the same AZ as the target server but can be in a different VPC.

Prerequisites

The migration task is in the **Continuous sync** stage.

Procedure

Step 1 Sign in to the **SMS console**.

Step 2 In the navigation pane on the left, choose **Servers**.

Step 3 Locate the target server you want to clone, choose **More** > **Manage Target** > **Clone Target** in the **Operation** column.

Step 4 Set the parameters and click **Clone Target**.

- If you select **Recommended** for **Server Template**, the system automatically sets **VPC**, **Subnet**, **Security Group**, and parameters in **Advanced Settings** based on the current target server configuration. You can modify these parameters.
- If you select an existing template for **Server Template**, parameters **VPC**, **Subnet**, **Security Group**, and those in **Advanced Settings** are determined by the template. You can modify these parameters.

----End

4.2 Launching a Target Server

If you set **Continuous Synchronization** to **Yes** when configuring the migration settings, you need to manually launch the target server after the full replication is complete

NOTE

If you set **Continuous Synchronization** to **No**, skip this section as the system will automatically launch the target server after the full replication is complete.

Scenarios

You can launch a target server for a migration in the **Continuous sync** status, and the continuous synchronization will be interrupted. If you want to perform a continuous synchronization after you launch the target server, click **Sync** to synchronize the incremental data.

Before launching a target server, you can clone the target server for service testing, and only launch the target server after tests confirm there are no issues.

NOTE

The cloned server must be in the same AZ as the target server, but it can be in a different VPC.

Procedure

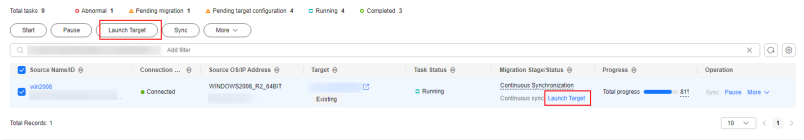
Step 1 Sign in to the **SMS console**.

Step 2 In the navigation pane on the left, choose **Servers**.

Step 3 Locate the target server you want to launch, and click **Launch Target** in the **Migration Stage/Status** column.

Alternatively, select the server you want to launch, and click **Launch Target** above the server list.

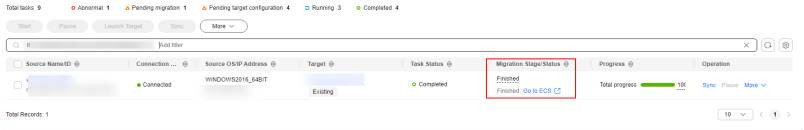
Figure 4-1 Launch Target



Step 4 In the displayed **Launch Target** window, click **OK**.

If **Finished** appears in the **Migration Stage/Status** column, the target server has been launched and the migration is complete.

Figure 4-2 Completed migration



After the migration and service cutover are complete, you need to adjust the configurations of the target server based on service requirements. For details, see **What Configuration Items Need to Be Manually Modified After a Server Is Migrated?**

----End

4.3 Viewing the Details of a Server

Scenarios

After the Agent is installed and started on a source server, it automatically reports the source server information to SMS. All collected data is used for migration only. For details, see **What Information Does SMS Collect About Source Servers?** You can sign in to the SMS console to view the server information at any time. You can see source server details, target server configurations, migration status, and error messages if any.

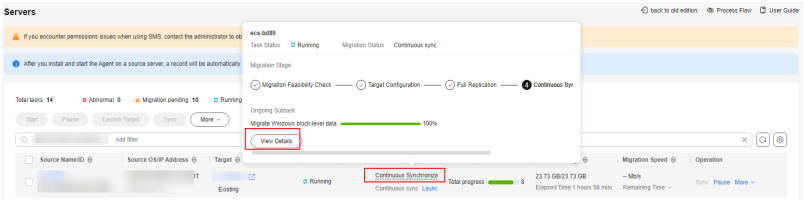
Procedure

Step 1 Sign in to the **SMS console**.

Step 2 In the navigation pane on the left, choose **Servers**.

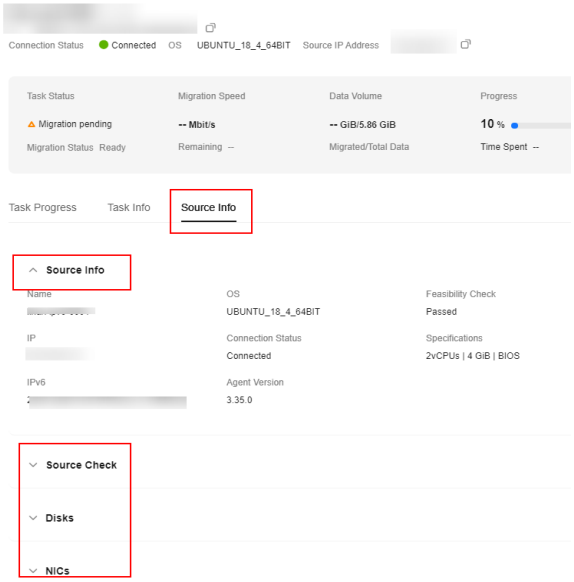
Step 3 In the server list, click the server name. The task details show up on the right.

You can also move the cursor to the migration stage and click **View Details** in the displayed window. The task details show up on the right.



Step 4 Click the **Source Info** tab, and you can view the source server details, including the basic information, migration check results, disk and partition information, and NIC information.

Figure 4-3 Viewing server details



----End

4.4 Deleting a Target Server Configuration

Scenarios

If a target server is incorrectly configured or its configuration need to be modified, you can delete the configuration and reconfigure the target server.

CAUTION

After the target server configuration is deleted, the migration task is still in the list but cannot be performed. You can configure a new target server to perform the migration again.

Procedure

Step 1 Sign in to the **SMS console**.

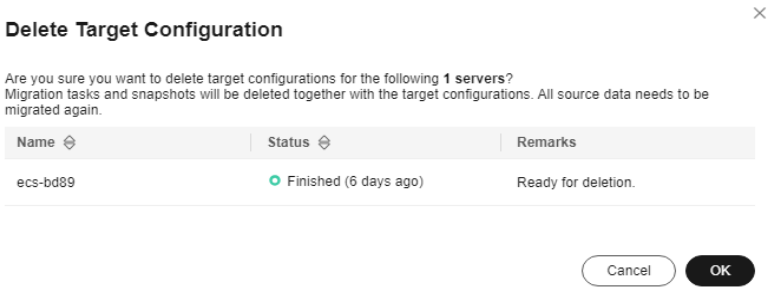
Step 2 In the navigation pane on the left, choose **Servers**.

Step 3 Locate the server for which you want to delete the target server configuration, and choose **More** > **Delete Target Configuration** in the **Operation** column.

You can also choose **More** > **Delete Target Configuration** in the upper left corner of the server list.

Step 4 In the displayed **Delete Target Configuration** dialog box, click **OK**.

Figure 4-4 Confirmation



----End

4.5 (Optional) Deleting a Server Clone

Scenarios

You can delete a server clone when it is no longer needed or the service tests are complete.

NOTE

You can switch to the ECS console to check whether the deletion is successful.

Procedure

Step 1 Sign in to the **SMS console**.

Step 2 In the navigation pane on the left, choose **Servers**.

Step 3 Locate the server for which you want to delete the clone, and choose **More** > **Manage Target** > **Delete Clone** in the **Operation** column.

Step 4 In the **Delete Clone** dialog box, click **OK**.

----End

4.6 Unlocking a Target Server

Scenarios

During a migration, the target server is locked by default and you are not allowed to perform any operations on it. After the migration is complete, the system automatically unlocks the target server. If you need to perform operations on the target server during the migration, unlock the target server first.

Procedure

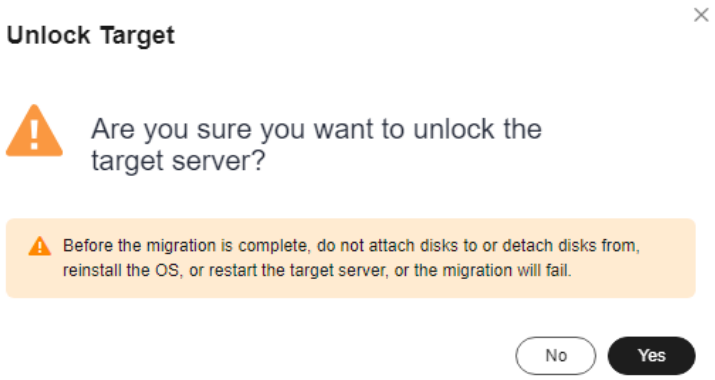
Step 1 Sign in to the **SMS console**.

Step 2 In the navigation pane on the left, choose **Servers**.

Step 3 Locate the server for which you want to unlock the target server, and choose **More** > **Manage Target** > **Unlock Target** in the **Operation** column.

Step 4 In the displayed **Unlock Target** dialog box, click **Yes**.

Figure 4-5 Confirmation



----End

4.7 Deleting an EVS Snapshot

Scenarios

SMS creates snapshots for EVS disks on each target server during the full replication, incremental synchronization, and target cloning. For EVS disks in DSS storage pools, snapshots take up the same amount of space in the pool as the disks. You can delete these snapshots as needed.

NOTE

If a migration task is deleted, the disk snapshots are also deleted.

Although snapshots themselves do not differ in a technical sense, SMS distinguishes between three types of snapshots, based on the events that trigger them:

- **Cutover snapshots**: After a migration is complete, SMS creates a snapshot for each target server disk. These snapshots are used for rollback if any service faults happen.

  NOTE

  You are advised to delete these snapshots after the service cutover is complete and your services run stably on the target server.

- **Synchronization snapshots**: For a Windows migration or Linux block-level migration, after the source data is migrated and synchronized and before the target server is launched, SMS creates a snapshot for each target server disk to ensure data consistency between the source and target.

> **CAUTION**
>
> After the snapshots are deleted, no further synchronization can be performed.

- **Clone snapshots**: When you clone a target server, SMS creates a snapshot for each target server disk. These snapshots are used to clone the target server and put the migration status back to continuous synchronization after the clone is complete.

Procedure

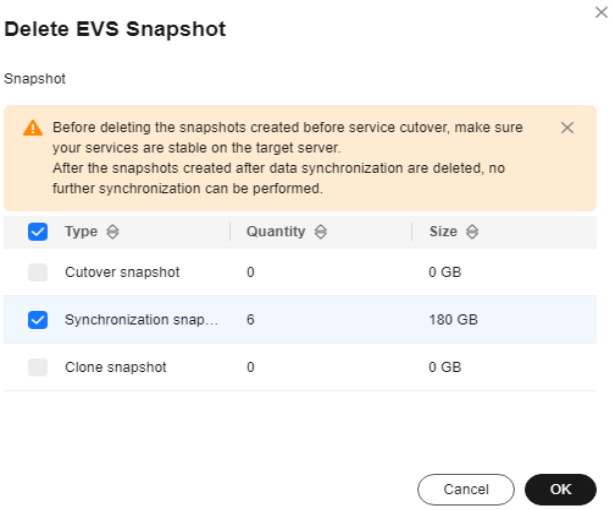
Step 1 Sign in to the **SMS console**.

Step 2 In the navigation pane on the left, choose **Servers**.

Step 3 In the server list, locate the server and choose **More** > **Manage Target** > **Delete EVS Snapshot** in the **Operation** column.

Step 4 In the displayed **Delete EVS Snapshot** dialog box, select the snapshots to be deleted and click **OK**.

Figure 4-6 Confirming the deletion



----End

5 Template Management

5.1 Managing a Migration Template

What Is a Migration Template?

A migration template defines the settings for **Network**, **Migration Rate Limit**, **Enable Continuous Synchronization**, **Region/Project**, and other migration parameters.

You can modify your migration template at any time.

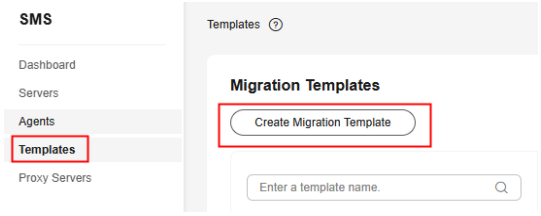
Creating a Migration Template

Step 1 Sign in to the **SMS console**.

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

Step 3 In the upper left corner of the **Migration Templates** area, click **Create Migration Template**.

Figure 5-1 Creating a migration template



Step 4 Set **Name** and **Description** and click **OK**.

Step 5 In the template list on the left of the **Migration Templates** area, click the created template and click **Parameter Settings** to configure the template.

Figure 5-2 Parameter settings

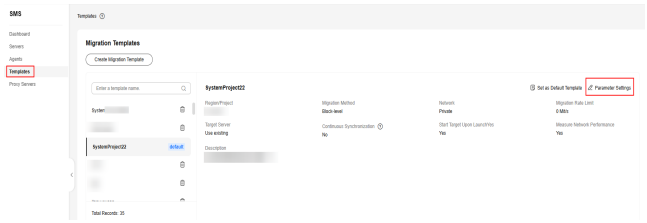


Table 5-1 describes the parameters.

Table 5-1 Parameters

Parameter	Option	Description
Name	-	User-defined
Description	-	User-defined
Region/Project	-	Select the target region and project you want to migrate to.
Migration Method	Block-level	• Migration and synchronization are performed by block. • For Windows servers, SMS only supports block-level migration.
	File-level	Migration and synchronization are performed by file. This method is inefficient, but the compatibility is excellent.
Network	Public	An EIP must be bound to the target server. **Public** is the default value.
	Private	You need to create a Direct Connect or VPN connection between the source and the VPC subnet you are migrating to. If the source and target servers are in the same VPC, select **Private**.

Parameter	Option	Description
Migration Rate Limit	-	You can configure the rate limits based on the source bandwidth and service requirements. If you do not want to limit the migration rate, set this parameter to **0**.
Target Server	Use existing	When you apply this template to a source server migration, you can select an existing server as the target server. The chosen server must meet at least the system-recommended specifications.
	Create new	When you apply this template to a source server migration, you need to configure environment settings for the target server, such as VPC, subnet, and security group.

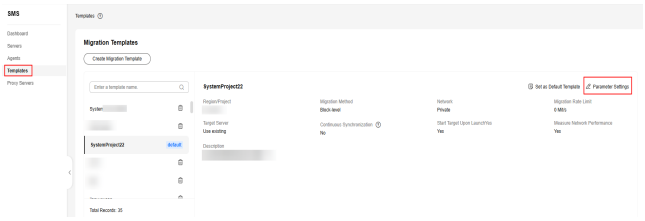
Parameter	Option	Description
Enable Continuous Synchronization	-	• If you do not enable this option, after the full replication is complete, SMS will automatically launch the target server without synchronizing incremental data. To synchronize incremental data, you will need to click **Sync** in the **Operation** column. • If you enable this option, after the full replication is complete, the migration will enter the continuous synchronization stage. During this stage, incremental data will be periodically synchronized from the source server to the target server, and you will be unable to use the target server since it has not been launched yet. To finish this stage, you will need to click **Launch Target** in the **Operation** column.
Start Target Upon Launch	-	• If you enable this option, the target server will be started after the migration is complete. • If you do not enable this option, the target server will be stopped after the migration is complete.

Parameter	Option	Description
Measure Network Performance	-	If you enable this option, before the full migration starts, the system will measure the packet loss rate, network jitter, network latency, bandwidth, memory usage, and CPU usage for the source server. For details, see **How Do I Measure the Network Performance Before the Migration?** If you do not enable this option, network performance will not be measured.

Step 6 Click **OK**.

Step 7 (Optional) Click the name of the created template, and click **Set as Default Template** to set it as the default template.

Figure 5-3 Set as Default Template



----End

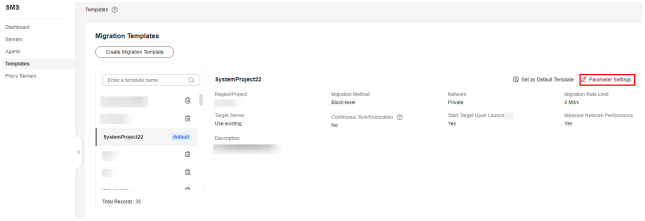
Modifying a Migration Template

Step 1 Sign in to the **SMS console**.

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

Step 3 In the template list on the left of the **Migration Templates** area, click the name of the template to be modified and click **Parameter Settings**.

Figure 5-4 Modifying template parameters



Step 4 Modify the template settings and click **OK**.

----End

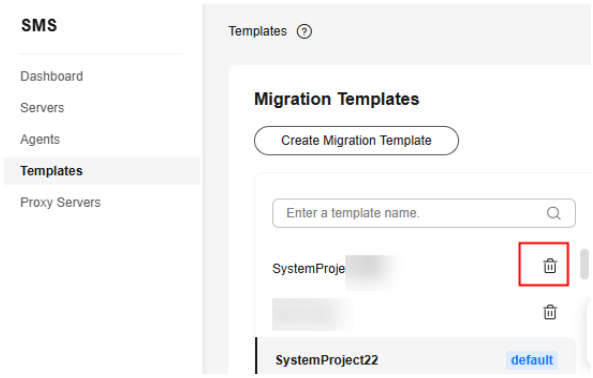
Deleting a Migration Template

Step 1 Sign in to the **SMS console**.

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

Step 3 In the **Migration Templates** area, on the left, click next to the name of the template you want to delete.

Figure 5-5 Deleting a migration template



Step 4 In the displayed **Delete Migration Template** dialog box, click **OK**.

----End

5.2 Managing a Server Template

What Is a Server Template?

A server template defines the environment settings for servers, such as VPC, subnet, and security group settings.

You can modify your server templates at any time.

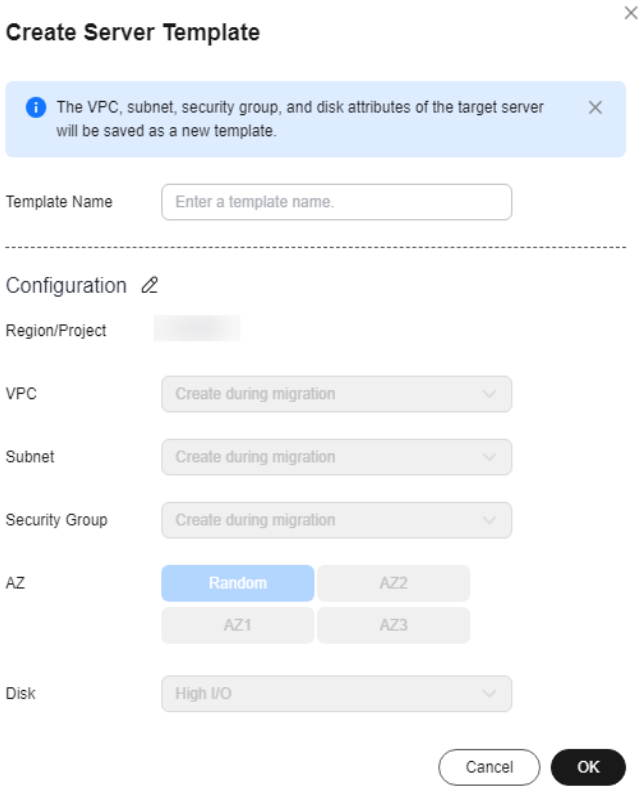
Procedure

Step 1 Sign in to the **SMS console**.

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

Step 3 In the upper right corner of the **Server Templates** area, click **Create Server Template**.

Figure 5-6 Create Server Template



Step 4 Enter a template name, click next to **Configuration**, and set parameters listed in **Table 5-2**.

Table 5-2 Parameters

Parameter	Description
Region	• Select a region where you want to provision a target server. • By default, the region is the one set in the default migration template, but you can change it as needed.
Project	• Select a project in the region from the drop-down list. • You can select a project only after a region is selected.

Parameter	Description
VPC	If you select **Create during migration**, SMS will create a VPC when you use this template to configure a target server. • If the source IP address is 192.168.*X.X*, SMS will create a VPC and a subnet that both belong to network range 192.168.0.0/16. • If the source IP address is 172.16.*X.X*, SMS will create a VPC and a subnet that both belong to network range 172.16.0.0/12. • If the source IP address is 10.*X.X*, SMS will create a VPC and a subnet that both belong to network range 10.0.0.0/8.
Subnet	• If you select **Create during migration**, SMS will recommend a subnet when you use this template to configure a target server. • The subnet is in the same network segment as the VPC.
Security Group	• If you select **Create during migration**, SMS will create a security group and enable the required ports when you use this template to configure a target server. • Windows: ports 8899, 8900, and 22 • Linux: 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.
AZ	The parameter is set to **Random** by default. You can also select another AZ.
Disk Type	The value can be **Common I/O**, **High I/O**, or **Ultra-high I/O**.

Step 5 Click **OK**.

----End

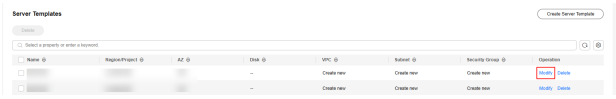
Modifying a Server Template

Step 1 Sign in to the **SMS console**.

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

Step 3 Locate the server template to be modified and click **Modify** in the **Operation** column.

Figure 5-7 Modifying a server template



Step 4 Modify the template settings and click **OK**.

----End

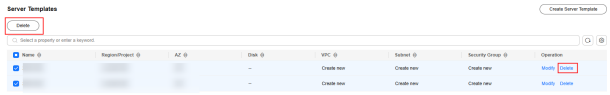
Deleting a Server Template

Step 1 Sign in to the **SMS console**.

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

Step 3 Locate the server template to be deleted and click **Delete** in the **Operation** column. If multiple templates need to be deleted, select them and click **Delete** above the list.

Figure 5-8 Deleting server templates



Step 4 Click **OK**.

----End

6 Viewing CTS Traces

6.1 SMS Operations Supported by CTS

Table 6-1 SMS operations recorded by CTS

Operation	Resource Type	Trace Name
Adding a source	sourceServer	addSource
Deleting a source	sourceServer	removeSource
Updating a source name	sourceServer	updateSourceName
Creating a task	addTask	addTask
Deleting a task	deleteTask	deleteTask
Starting a task	updateTask	task-start
Stopping a task	updateTask	task-stop
Synchronizing a task	updateTask	task-sync
Updating the task progress	updateTaskProgress	updateTaskProgress
Saving a template	addTemplate	addTemplate
Modifying a template	updateTemplate	update
Deleting a template	deleteTemplate	deleteTemplate
Deleting templates in batches	deleteTemplates	deleteTemplates
Response results of operations	TaskCommand	processCommandResult

6.2 Viewing CTS Traces in the Trace List

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in Object Storage Service (OBS) buckets. Cloud Trace Service (CTS) stores operation records (traces) generated in the last seven days.

NOTE

These operation records are retained for seven days on the CTS console and are automatically deleted upon expiration. Manual deletion is not supported.

This section describes how to query or export operation records of the last seven days on the CTS console.

- **Viewing Real-Time Traces in the Trace List of the New Edition**
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for longer than seven days, you must configure transfer to OBS or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.
- After performing operations on the cloud, you can query management traces on the CTS console one minute later and query data traces five minutes later.
- Data traces are not displayed in the trace list of the new version. To view them, you need to go to the old version.

Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & GovernanceManagement & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
   - **Trace Name**: Enter a trace name.
   - **Trace ID**: Enter a trace ID.
   - **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API

operation does not involve the resource name parameter, leave this field empty.

- **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
- **Trace Source**: Select a cloud service name from the drop-down list.
- **Resource Type**: Select a resource type from the drop-down list.
- **Operator**: Select one or more operators from the drop-down list.
- **Trace Status**: Select **normal**, **warning**, or **incident**.
  - **normal**: The operation succeeded.
  - **warning**: The operation failed.
  - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
- **Enterprise Project ID**: Enter an enterprise project ID.
- **Access Key**: Enter a temporary or permanent access key ID.
- Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.

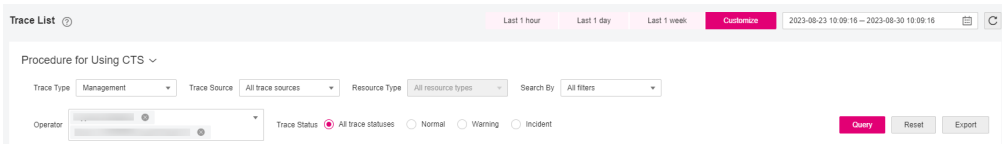
5. On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.
   - Enter any keyword in the search box and press **Enter** to filter desired traces.
   - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
   - Click  to view the latest information about traces.
   - Click  to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled (), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see **Trace Structure**section "Trace References" > "Trace Structure" and **Example Traces**section "Trace References" > "Example Traces".
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

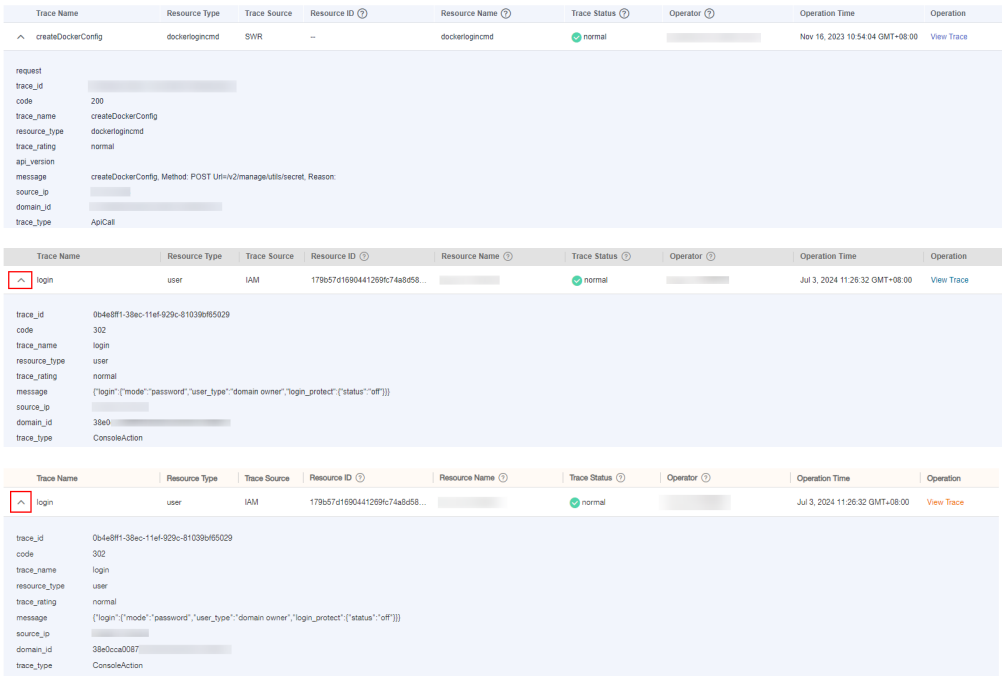
1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & GovernanceManagement & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.

5. Set filters to search for your desired traces, as shown in **Figure 6-1**. The following filters are available.

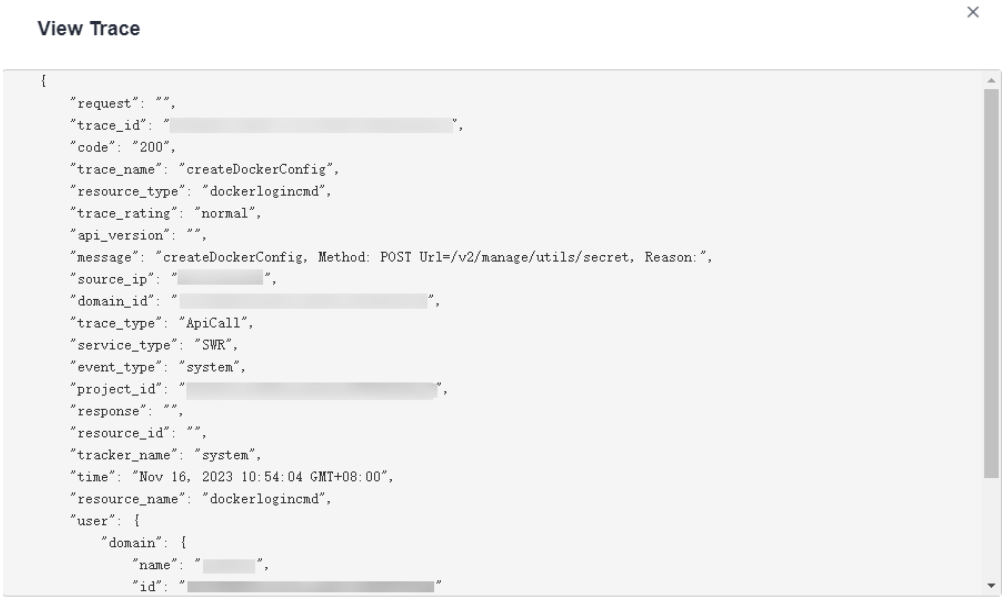
Figure 6-1 Filters



   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
     - If you select **Resource ID** for **Search By**, specify a resource ID.
     - If you select **Trace name** for **Search By**, specify a trace name.
     - If you select **Resource name** for **Search By**, specify a resource name.
   - **Operator**: Select a user.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.
   - Click to view the latest information about traces.
8. Click on the left of a trace to expand its details.



9. Click **View Trace** in the **Operation** column. The trace details are displayed.



10. For details about key fields in the trace structure, see **Trace Structure**section "Trace References" > "Trace Structure" and **Example Traces**section "Trace References" > "Example Traces" in the *CTS User Guide*.
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

6.3 Viewing Traces

Scenarios

After you enable CTS, it records key operations performed on SMS. You can view the operation records of the last seven days on the CTS console.

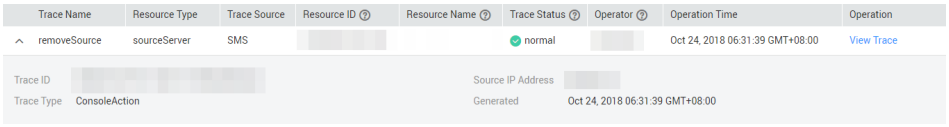
Procedure

1. Sign in to the console.
2. Choose **Service List** > **Management & Governance** > **Cloud Trace Service**.
3. In the navigation pane on the left, choose **Trace List**
4. In the upper right corner of the trace list, click **Filter** to set the search criteria. The following filters are available:
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.

     When you select **Resource ID** for **Search By**, you also need to select or enter a resource ID.
   - **Operator**: Select a specific operator from the drop-down list.
   - **Trace Status**: Available options include **All trace statuses**, **Normal**, **Warning**, and **Incident**.
   - Time range: In the upper right corner of the page, you can query traces in the last one hour, last one day, last one week, or within a customized period.

5. Click **Query**.
6. On the right of the filter box, click **Export**. CTS exports a CSV file which lists query results.
7. Click on the left of the required trace to expand its details. **Figure 6-2** shows an example.

   Figure 6-2 Expanding trace details



8. Click **View Trace** in the **Operation** column. The trace structure details are displayed.

