Server Migration Service

Getting Started

Issue 14

Date 2025-01-24

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.

Huawei Technologies Co., Ltd.

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

Website: https://www.huawei.com

Email: support@huawei.com

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 Before You Start

Before using SMS, you must:

- **Confirm that you have the required permissions.**

  Your target account must have the **permissions** required to use SMS and its dependent cloud services.
- **Confirm that your source server OS is supported by SMS.**

  You can learn more about supported OSs from the following links:
  - **Supported Windows OSs**
  - **Supported Linux OSs**
- **Determine which region you want to migrate to.**

  You need to know which region you want to migrate to. When you create a migration task, you need to confirm that the preset region is the one you want to migrate to.
- **Read the SMS precautions.**

  SMS Precautions
- **Back up data on the target server disks, and ensure that the disks can be formatted.**

  Disks on the target server will be formatted and re-partitioned based on the source disk settings during the migration. If you choose to use an existing server on the cloud as the target server, make sure that any data on the target server has been backed up and that the disks can be formatted.
- **(Recommended) Disable any software in conflict with SMS on the source server.**

  Any antivirus or conflicting software on the source server may prevent the SMS-Agent from start. It is recommended that you disable the software. If you are not sure whether there is a software conflict with the SMS-Agent, back up your data before the migration.
- **Confirm that your account balance is enough.**
  - SMS is a free service, but you will still be billed for any other resources used during the migration. For details, see **Billing**.
- **Know when the target server can be operated.**

  Do not operate the target server before the migration is complete, such as renewing the target server or changing its billing mode.

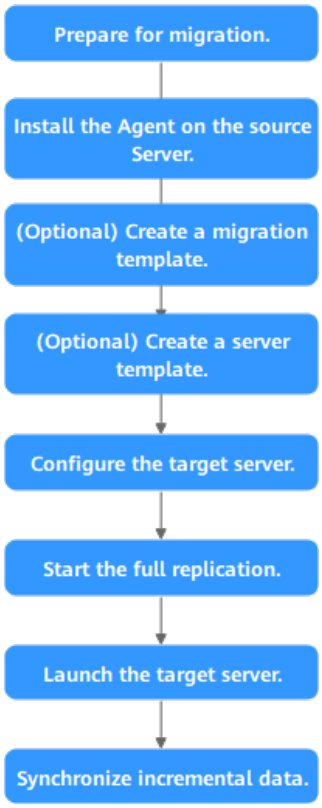
- **Learn where to find the solutions to common migration issues.**

  If you encounter any problem during the migration, try to solve the problem by referring to **FAQs**.

2 Migration Process

The following figure shows the process of using SMS to migrate a server.

Figure 2-1 Migration process



3 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 a Huawei Cloud 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.

4 Installing the Agent on the Source Server

4.1 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?**

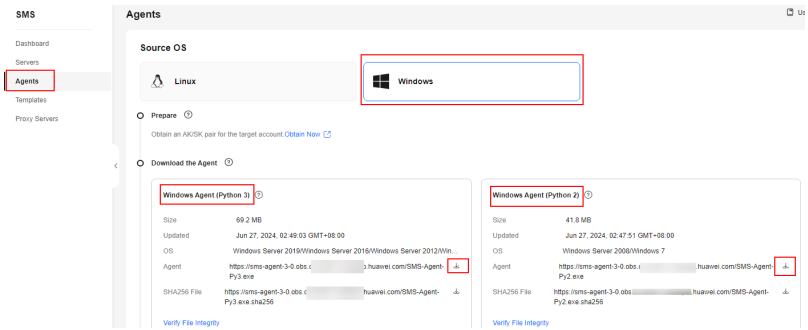
Downloading the Agent Installation File

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

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

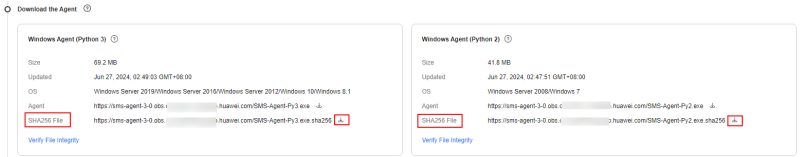
Step 3 Select the **Windows** card, locate the Agent that matches the source server OS, and click the icon next to **Agent**.

- 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 4-2**.

- 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 4-1 Starting the Agent

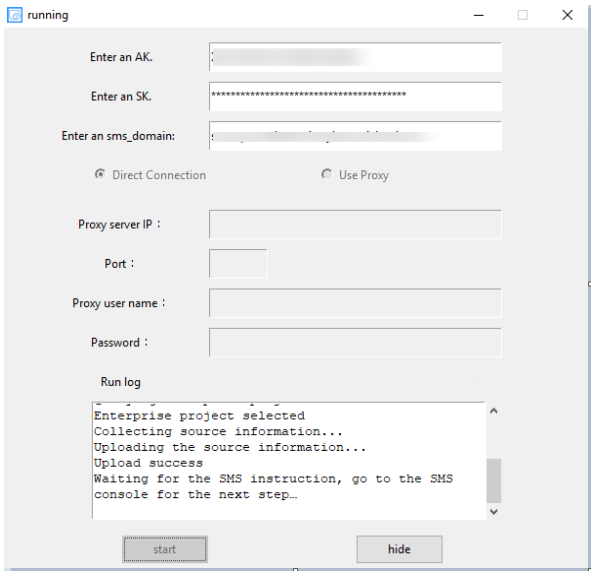
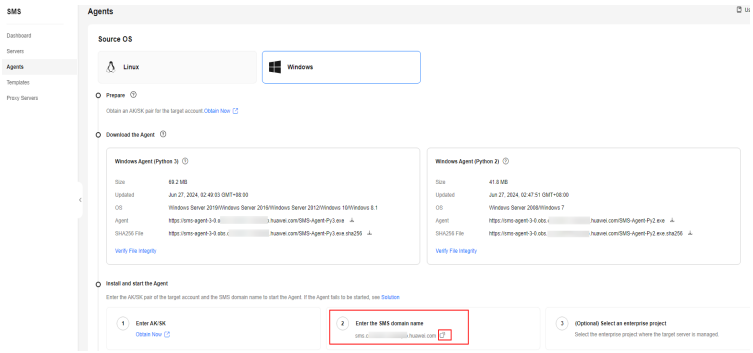


Figure 4-2 Obtaining the SMS domain name



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
```

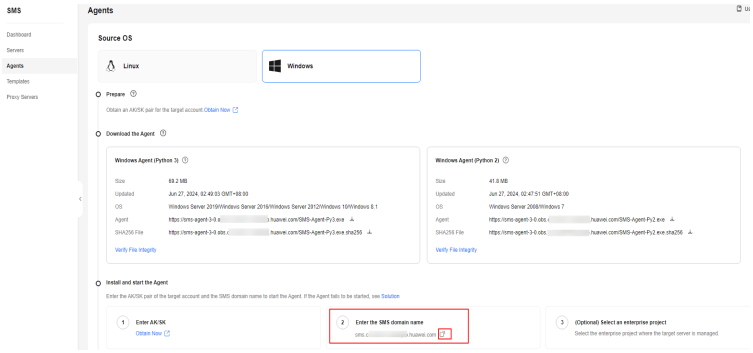
NOTE

- **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 4-3**.

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 4-3 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?**

4.2 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

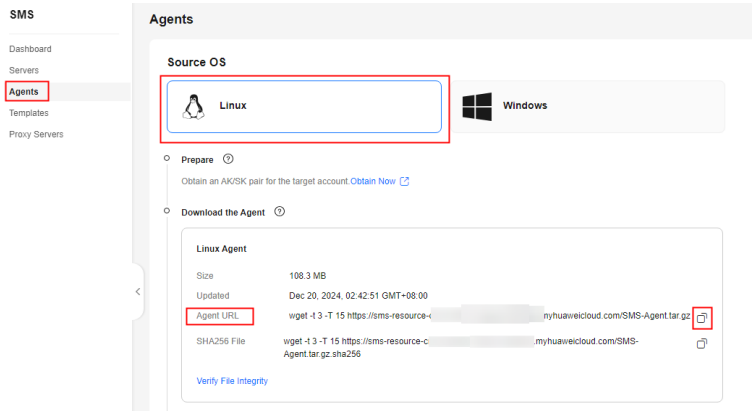
- You have obtained an AK/SK pair for your Huawei Cloud account.
  - If you use an IAM user for migration, obtain an AK/SK pair by referring to **How Do I Create an AK/SK Pair for an IAM User?**
  - If you use an account for migration, obtain an AK/SK pair by referring to **How Do I Create an AK/SK Pair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

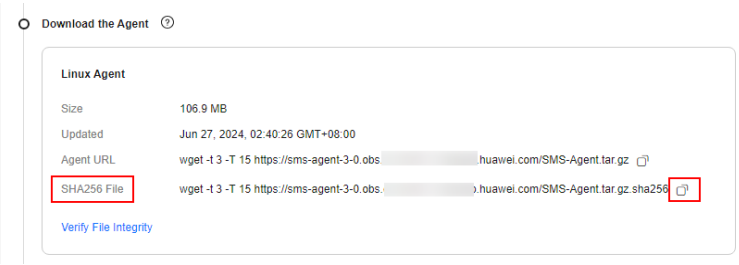
Step 2 In the navigation pane on the left, choose **Agents**.

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.

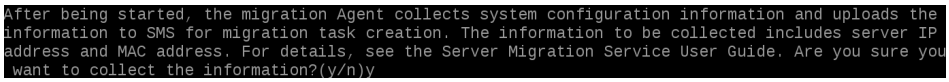
1. Go to the **config** directory.
   ```
   cd SMS-Agent/agent/config
   ```
2. Open and edit the **auth.cfg** file. Do not edit the **auth.cfg** file unless you need to use an HTTP/HTTPS proxy.
   ```
   vi auth.cfg
   ```
   The values shown here are for reference only.
   ```
   [proxy-config]
   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 4-4 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 4-6**.

Figure 4-5 Entering the AK/SK pair

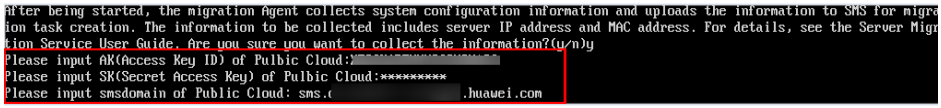
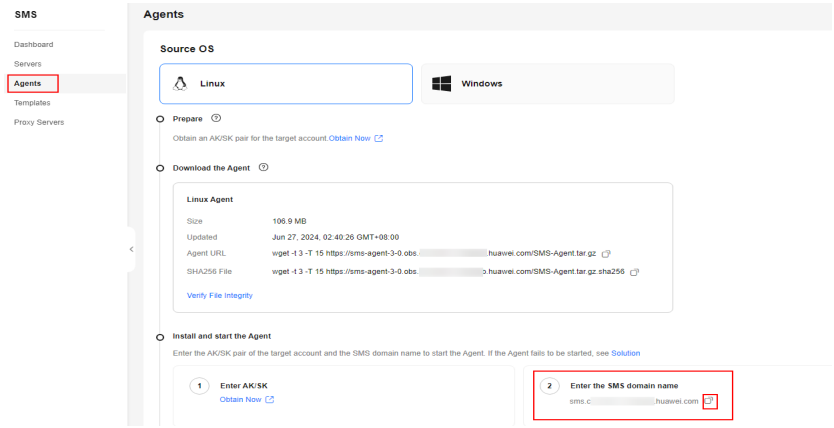


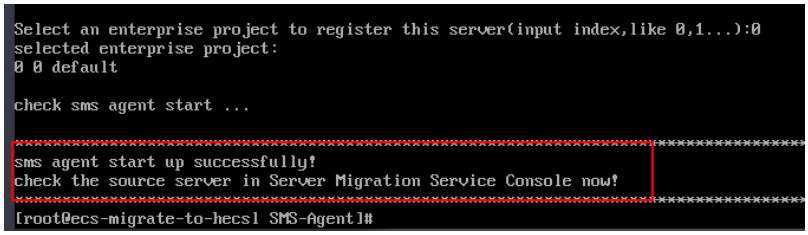
Figure 4-6 Obtaining the SMS domain name



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 4-7 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?**

5 (Optional) Creating a Migration Template

You can create a migration template to quickly define migration settings. In a migration template, you can define several parameters, such as **Network**, **Migration Rate Limit**, **Continuous Synchronization**, and **Region/Project**. For details, see **Creating a Migration Template**.

6 (Optional) Creating a Server Template

You can create a server template to quickly define target server settings. In a server template, you can define several parameters, such as **VPC**, **Subnet**, and **Security Group**. For details, see **Creating a Server Template**.

7 Configuring the 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:

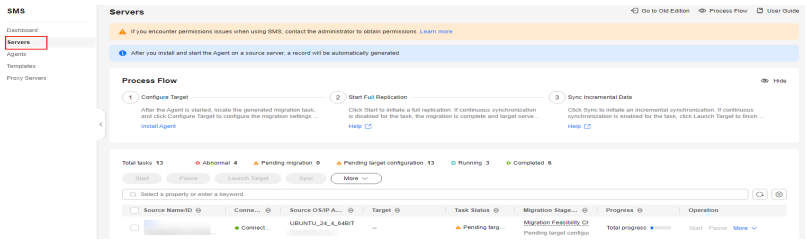
- The source server is **Connected** to SMS.
- The migration task is in the **Migration Feasibility Check** stage.
- The migration task is in the **Pending target configuration** status.

Procedure

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

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

Figure 7-1 Server list

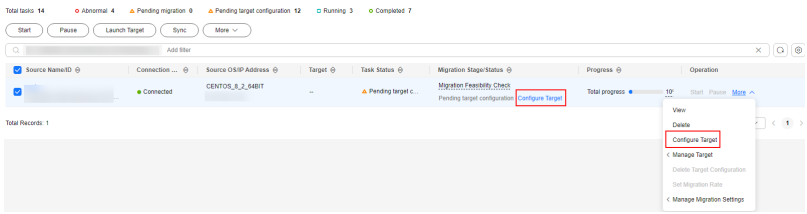


Step 3 In the server list, locate the source server and click **Configure Target** in the **Migration Stage/Status** column.

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 7-1**.

Table 7-1 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.

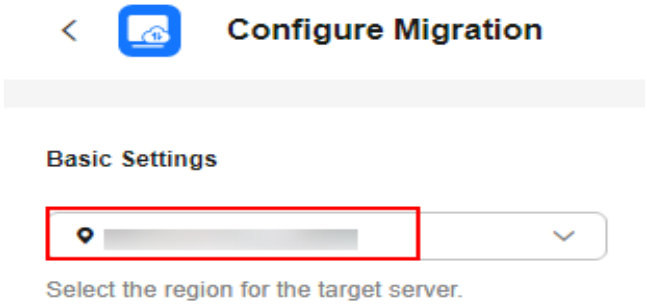
Area	Parameter	Option	Description
	Enable Continuous Synchronization	No	After the full replication is complete, SMS will automatically launch the target server without synchronizing incremental data. To synchronize incremental data, you will need to click **Sync** in the **Operation** column.
		Yes	After 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.



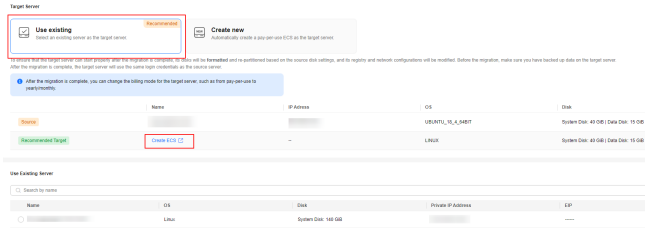
Step 7 In the **Target Server** area, choose whether to use an existing cloud server or create a new one as the target server. For details about the requirements on target servers, see **Target Server Requirements**.

- **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**.

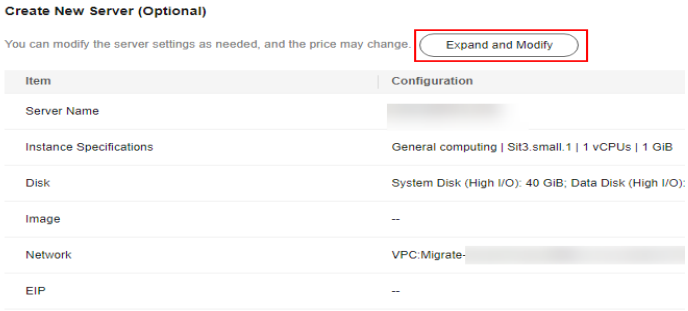
  NOTE

  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

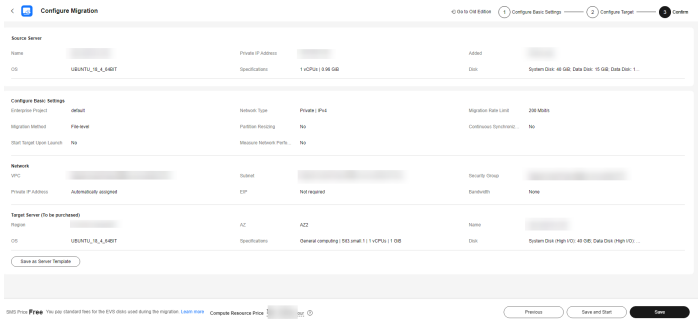
    Enter the ID of a key shared from another user. Ensure that the key is in the target region. For details, see **Creating a Grant**.

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 7-2 The configuration confirmation page

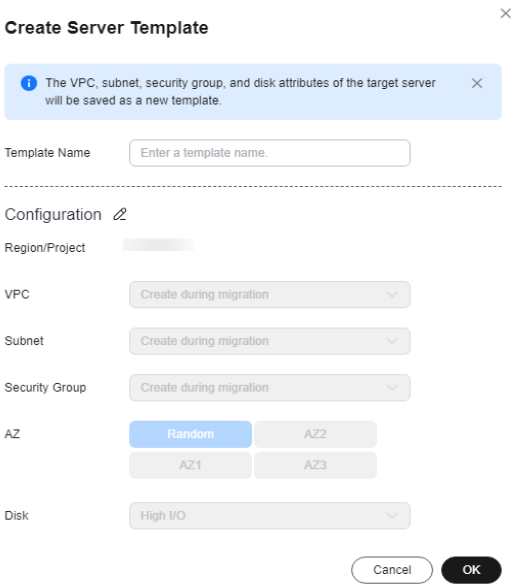


Step 9 (Optional) Click **Save as Server Template**. In the displayed **Create Server Template** dialog box, enter a template name and click **OK** to save the target server settings as a template.

NOTE

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

Figure 7-3 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 7-4 Saving the configuration

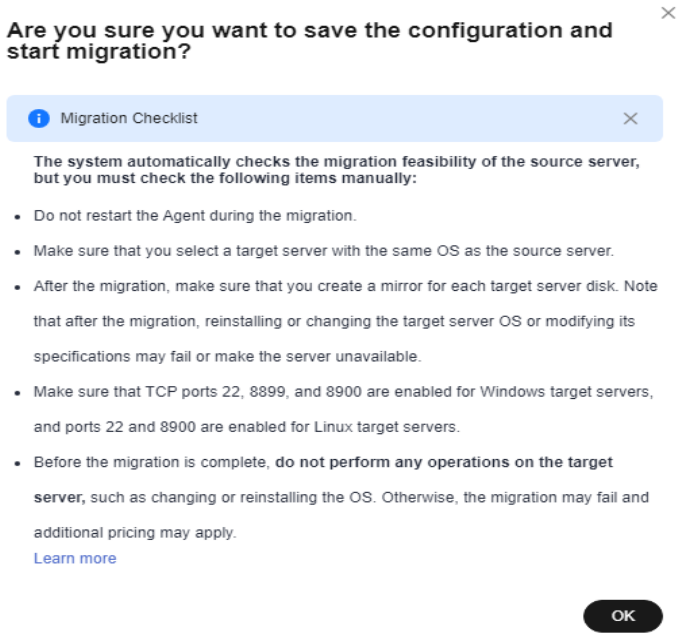
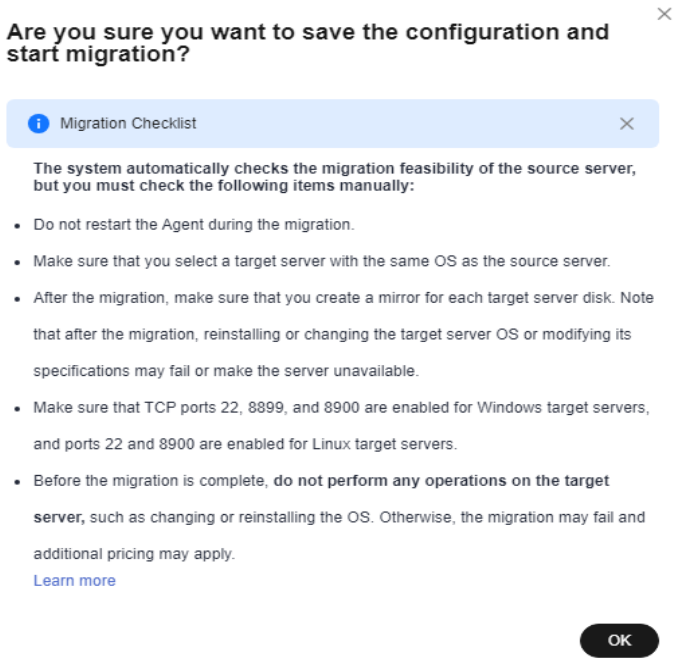


Figure 7-5 Saving the configuration and starting the migration



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 7-6 Resizing disks and partitions (Windows)

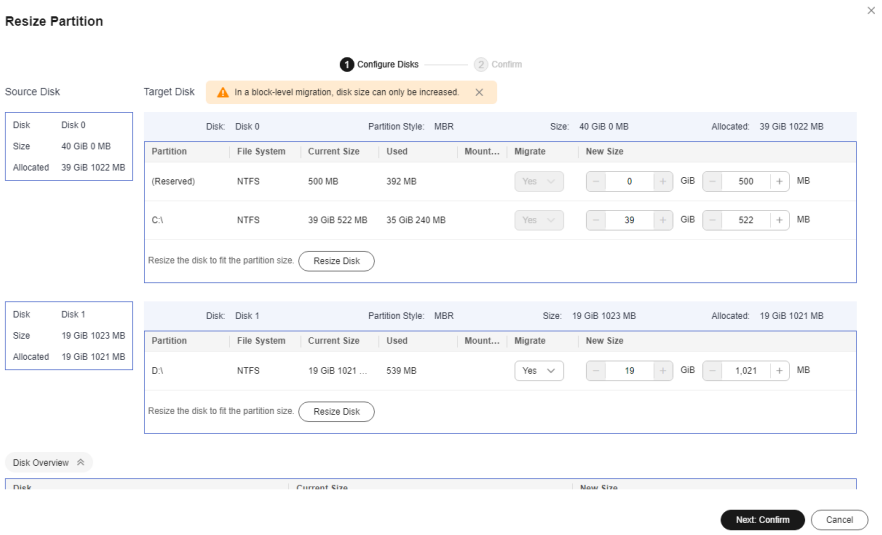
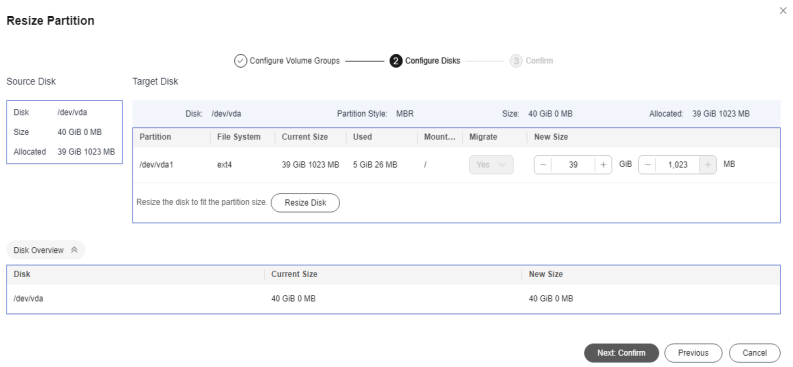


Figure 7-7 Resizing disks and partitions (Linux)



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

8 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 the Target Server**.
- The migration task is in the **Full Replication** stage and the status is **Ready**.

Procedure

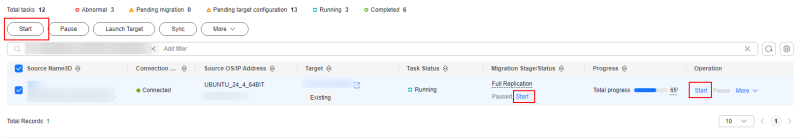
Step 1 Sign in to the **SMS console**.

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 8-1 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 **Enable Continuous Synchronization** to **No** when you defined the migration settings, after the full replication is complete, the migration will go to the **Target Launch** stage, and the target server will be launched to complete the migration automatically.
- If you set **Enable Continuous Synchronization** to **Yes** when you defined the migration settings, after the full replication is complete, the migration will enter a **Continuous sync** status, and any new or modified data will be automatically synchronized from the source server to the target server. You will need to manually launch the target server to complete the migration. For details, see **Launching the 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

9 Launching the Target Server

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

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 the target server when the migration is in the **Continuous sync** status, and continuous synchronization will be interrupted. After the target server is launched, you can start an incremental synchronization by clicking **Sync** in the operation column.

Before launching the 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.

Procedure

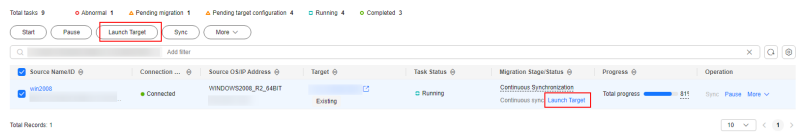
Step 1 Sign in to the **SMS console**.

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.

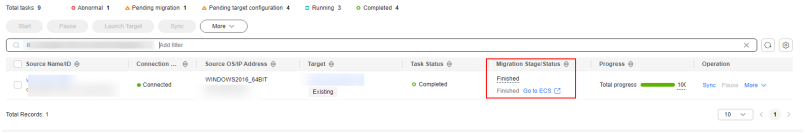
Figure 9-1 Launch Target



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 9-2 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

10 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 from the source server to the target server.

The data changes on the target server will be overwritten by the data synchronized from the source server. For details, see **Will an Incremental Synchronization Overwrite the Existing Data on a Launched Target Server?**

NOTE

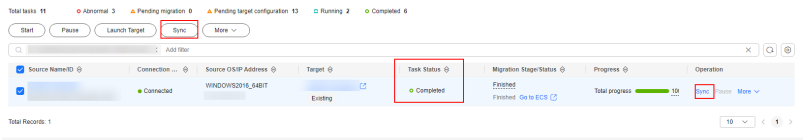
Only tasks in the **Finished** status can be synchronized.

Procedure

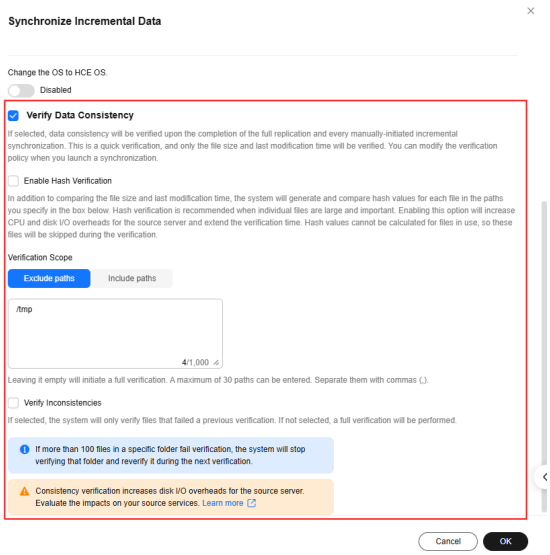
Step 1 Sign in to the **SMS console**.

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

