Migration Center

Best Practices

Issue 13

Date 2024-12-20

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 Configuring Permissions Required for Server Migration

Overview

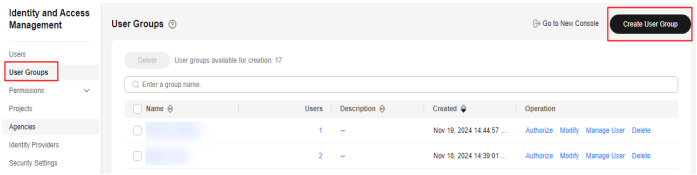
1. Create a user group named **migration_users** and assign the permissions required to use MgC and SMS to the user group. The IAM user to be created will inherit the permissions from the user group.
2. For a user in the local **admin** group, create an IAM user who is named **mgc-user**, belongs to the **migration_users** user group, and has only programmatic access to Huawei Cloud. The IAM user is not allowed to access the Huawei Cloud console using a password.
3. Provide the AK/SK pair downloaded when **mgc-user** to Edge. The AK/SK pair is used to register Edge with MgC and authenticate API calling during the migration.

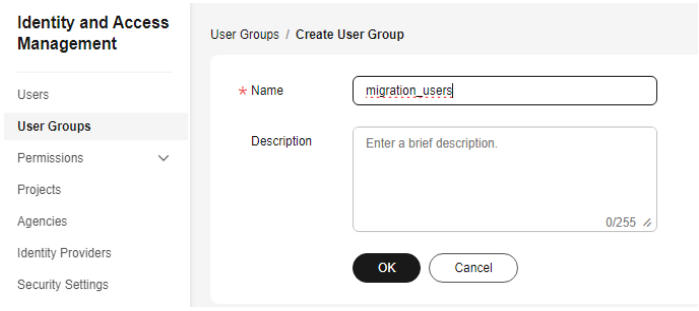
Step 1: Create a User Group

Step 1 Log in to the **IAM console**.

Step 2 On the IAM console, choose **User Groups** from the left navigation pane, and click **Create User Group** in the upper right corner.

Figure 1-1 Creating a user group



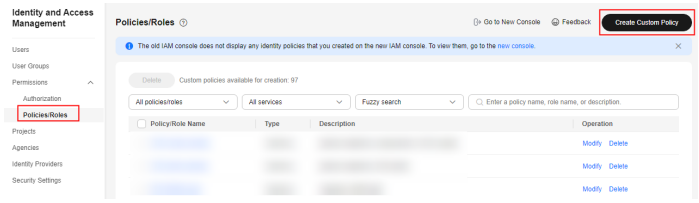


----End

Step 2: Create a Permissions Policy

Step 1 On the IAM console, in the navigation pane, choose **Permissions** > **Policies/Roles** and click **Create Custom Policy** in the upper right corner.

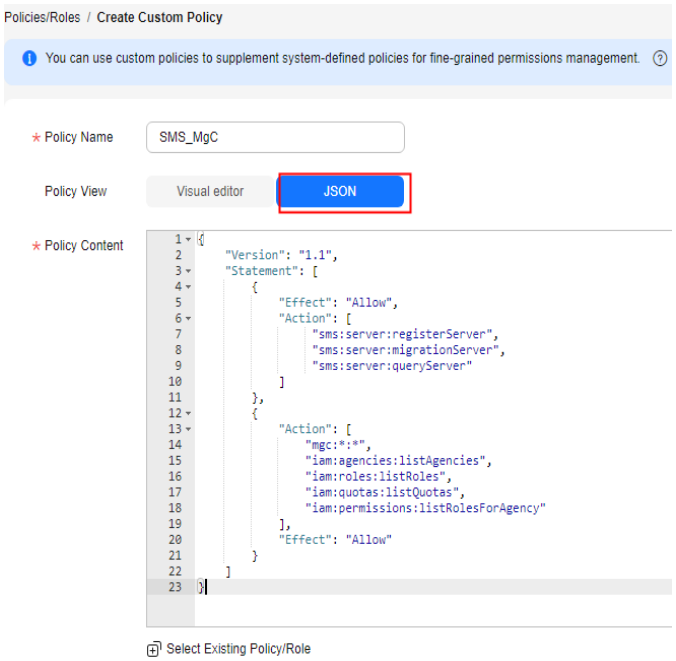
Figure 1-2 Creating a custom policy



Step 2 Create a policy for using SMS, a global cloud service. Enter a policy name, set **Policy View** to **JSON**, and copy the following content to the **Policy Content** box.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
               "sms:server:registerServer",
               "sms:server:migrationServer",
               "sms:server:queryServer"
         ]
      },
      {
         "Action": [
            "mgc:*:*",
            "iam:agencies:listAgencies",
            "iam:roles:listRoles",
            "iam:quotas:listQuotas",
            "iam:permissions:listRolesForAgency"
         ],
         "Effect": "Allow"
      }
   ]
}
```


Figure 1-3 Creating a policy that defines the permissions required for using SMS



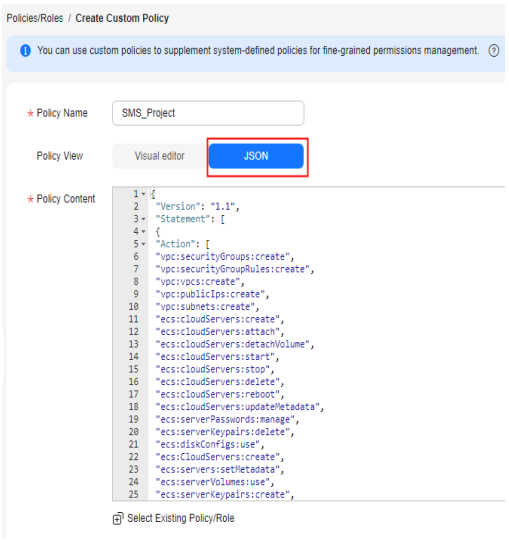
Step 3 Create a policy for using regional cloud services that SMS depends on. Enter a policy name, set **Policy View** to **JSON**, and copy the following content to the **Policy Content** box.

```
{
 "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",
"ecs:*:get*",
"ecs:*:list*",
"evs:*:get*",
"evs:*:list*",
"vpc:*:list*",
"vpc:*:get*",
"ims:*:get*",
"ims:*:list*"
],
"Effect": "Allow"
}
]
}
```

Figure 1-4 Creating a policy for using the regional cloud services that SMS depends on



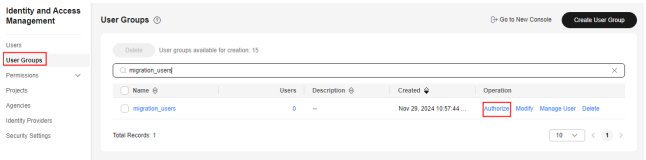
----End

Step 3: Assign Permissions

Step 1 On the IAM console, choose **User Groups** from the navigation pane.

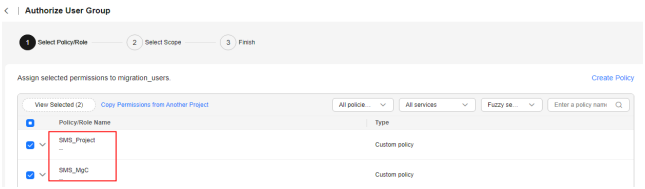
Step 2 In the user group list, locate the user group created in **step 1** and click **Authorize** in the **Operation** column.

Figure 1-5 Assigning permissions to the user group



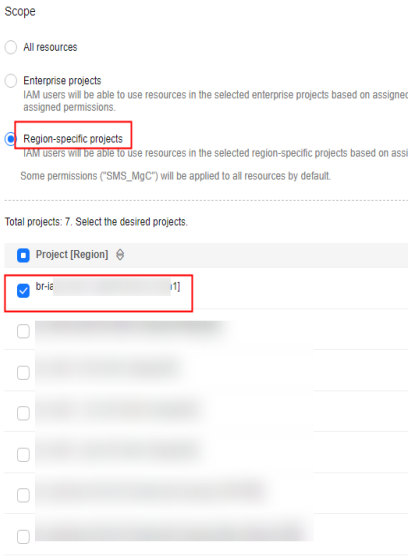
Step 3 Search for and select the two custom policies created in **step 2** and click **Next**.

Figure 1-6 Selecting the created custom policies



Step 4 Select **Region-specific projects** for **Scope** and select a region-specific project. Then the IAM users in the group can use resources in the region-specific project based on their permissions.

Figure 1-7 Selecting a region-specific project



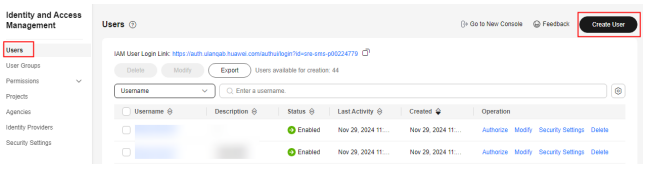
Step 5 Click **OK**.

----End

Step 4: Create a User

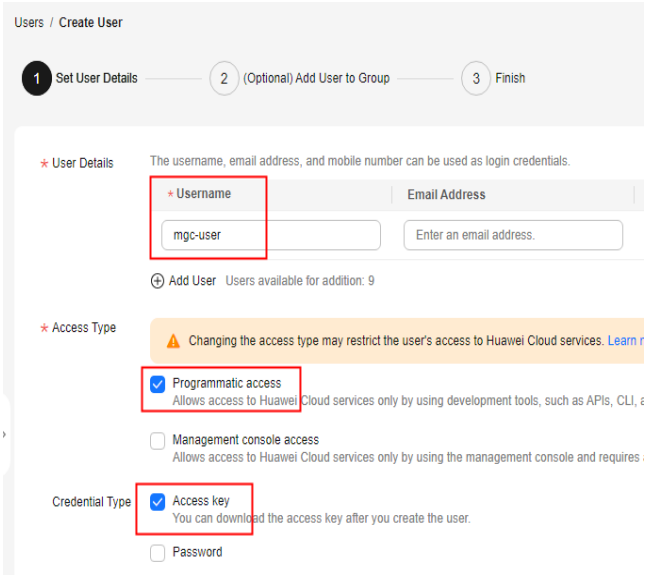
Step 1 On the IAM console, choose **Users** from the left navigation pane, and click **Create User** in the upper right corner.

Figure 1-8 Creating a user



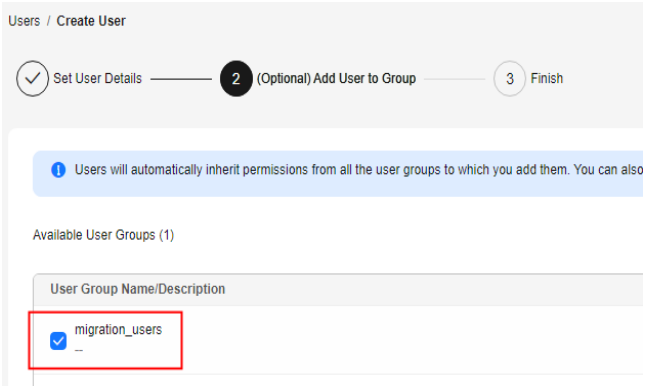
Step 2 Enter a username, deselect **Management console access**, and click **Next**.

Figure 1-9 Configuring basic information



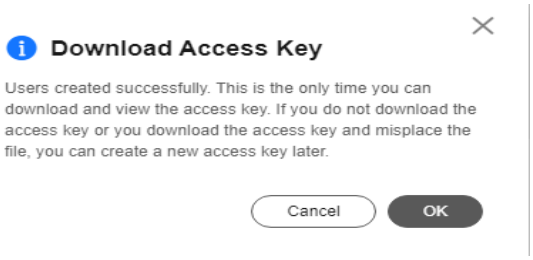
Step 3 Select the user group created in **step 1** and click **Create**.

Figure 1-10 Selecting a user group



Step 4 After the user is created, the **Download Access Key** dialog box is displayed. Click **OK** to download an AK/SK pair for the IAM user.

Figure 1-11 Downloading an access key



----End

2 Server Migration

2.1 Network Requirements for Server Migration

Background

A server migration involves two types of traffic: control flow and data flow.

- **Control flow** refers to the communication between the source server and cloud service management planes. To ensure a smooth migration, verify if there are any restrictions on the outbound traffic from the source server. Additionally, confirm that the source server can access the following cloud services via their domain names: SMS, IAM, ECS, EVS, VPC, and IMS.
- **Data flow** refers to data transmission from the source server to the target server. To ensure smooth data transmission, confirm that the security group of the target server allows traffic from the source server's IP address over the specified migration ports. If the source server cannot directly access the Internet or cannot communicate with the target server, a proxy server must be configured. In this case, consider the following factors:
  - The proxy server can correctly forward traffic from the source server.
  - The proxy server's security group is configured to allow traffic from the source server's IP address over the proxy port.

For General Migration Scenarios

Internet access is required for migration using MgC.

1. Install Edge in the intranet environment. Edge must be able to access the source servers to be migrated. For details, see **Installing Edge for Windows**.
2. Complete steps 2 to 5 described in **Migrating On-premises Servers to Huawei Cloud Using MgC**.

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

3. **Create a server migration workflow**.
   - If the source servers can access the Internet, set the migration network to **Public**.

     Figure 2-1 Migration over the Internet

   - If the source servers cannot access the Internet, prepare a proxy server that can access the Internet and install proxy software. For details, see step 1 in **How Do I Configure a Source Server to Access Huawei Cloud Through a Proxy?** The network requirements for the proxy server are as follows:
     - Regardless whether the proxy server is on the source intranet environment or on the cloud, it must be able to access the source servers to be migrated over an intranet.
     - The proxy server must be configured to allow inbound traffic from the source servers over the proxy port.

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

     Figure 2-2 Migration over a private network

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

SMS is recommended in this migration scenario. You need to prepare a proxy server for forwarding control traffic and data traffic. For details, see **Network Configurations for Different Migration Scenarios**.

2.2 Migrating On-premises Servers to Huawei Cloud

Scenario

This section describes how to use MgC to migrate on-premises servers to Huawei Cloud.

Preparations

- Prepare a Windows server for installing Edge in the source intranet environment. The Windows server must:
  - Be able to access the Internet and the domain names of MgC, IoTDA, and other cloud services. For details about the domain names to be accessed, see **Domain Names**.
  - Use PowerShell **3.0** or later.
  - Have at least 4 CPUs and 8 GB of memory.
  - Allow outbound traffic on 8883 if the server is in a security group.
  - Disable any antivirus and protection software on the server. This type of software may stop Edge from executing migration commands, resulting in migration failures.

  CAUTION

  Do not install Edge on a source server to be migrated.
  - **High resource consumption**: Edge consumes CPU and memory resources during collection and migration. If a large number of migration tasks are performed by Edge, services on the source server may be affected.
  - **Port occupation**: Edge occupies some ports on the source server, which may affect services on the server.
- The Windows server where Edge is installed must be able to access source servers you want to migrate over the following ports:
  - Windows: port 5985
  - Linux: port 22
- WinRM must be enabled on Windows source servers, and these source servers must be able to access the server where Edge is installed. For more information, see **How Do I Configure WinRM on a Windows Source Server and Troubleshoot WinRM Connection Problems?**
- Prepare a Huawei account or an IAM user that can access MgC. For details, see **Preparations**.
- **Create a migration project** on the MgC console.

Notes

Before creating a server migration workflow, read and understand the following precautions.

Item	Precaution
Source download bandwidth	Used to download the migration Agent to source servers. • If each source server uses a dedicated bandwidth, the bandwidth must be at least 30 Mbit/s. • If source servers share a bandwidth, the average bandwidth must be at least 50 Mbit/s.

Item	Precaution
Migration bandwidth	• Used to migrate data. It affects the migration speed and duration. • For details about how to estimate the migration duration, see **How Long Does a Migration Take?**
CPU and memory	• At least 520 MB of available memory • At least 0.3 CPUs available in Linux and at least 1 CPU available in Windows
OS compatibility	For details about what OSs are supported, see **Supported OSs**.
Server migration statements	For details about the important statements you need to understand before the migration, see **What Are the Important Statements of SMS?**
Notes and constraints	For details about the notes and constraints for server migration, see **Notes and Constraints**.
Billing	For details about the fees that may be incurred during the migration, see **Billing**.
Permissions configuration	For details about the permissions the target account must have, see **Permissions Management**.
Migration network and ports	For details about the requirements for the migration network and ports, see **How Do I Set Up a Secure Migration Network for Using SMS?**

Step 1: Download and Install Edge

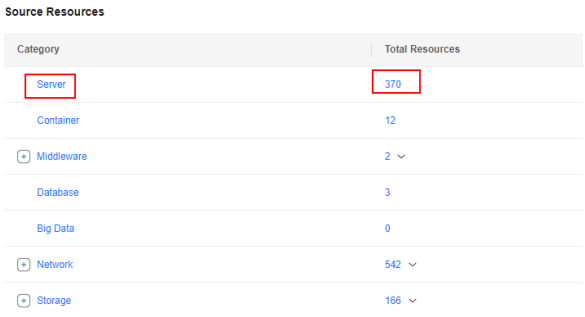
Install Edge and connect it to MgC. For more information, see **Installing Edge**.

Step 2: Add Servers to MgC

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

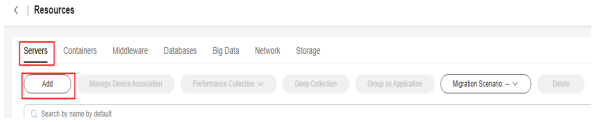
Step 2 In the navigation pane on the left, choose **Research** > **Source Resources**. Select a **migration project** in the upper left corner of the page.

Step 3 In the **Resources** area, click **Server** in the **Category** column or the number in the **Total Resources** column.



Step 4 Click **Add** above the list.

Figure 2-3 Adding a server



Step 5 In the displayed dialog box, configure parameters listed in **Table 2-1** and click **Confirm**. The system automatically checks the credential status and starts collecting resource details.

Table 2-1 Parameters for adding a server

Parameter	Description
Name	Enter a server name.
Edge Device	Select the Edge device installed in the source environment.
Type	Select the OS type of the source server.
IP Address	Enter the IP address of the source server. If the source server is in the same VPC as the Edge device, you can enter the private IP address of the server. Otherwise, you have to enter its public IP address.
Port	Enter the port on the source server opened to the Edge device. • By default, port 5985 on Windows source servers must be opened to the Edge device. The port cannot be changed. • By default, port 22 on Linux source servers must be opened to the Edge device. You can specify a different port if needed.
Credential	Select the server credential. If the credential has not been added to MgC, go to the Edge console, **add the server credential** to Edge, and synchronize it to MgC.

Step 6 View the added server on the **Servers** tab.

----End

Step 3: Group Servers as an Application

You can group the added servers as an application to get sizing recommendations for target resources and execute the migration.

Step 1 On the **Resources** page, in the **Servers** list, select the servers to be grouped as an application and click **Group as Application** above the list.

Step 2 Select an application from the drop-down list. If no applications are available, click **Create Application**. In the displayed dialog box, enter an application name and description; select a business scenario, environment, and target region; and click **Create**. For more information, see **Creating an Application**.

Step 3 Click **OK**. You can view the application name in the **Application** column of these servers.

----End

(Optional) Step 4: Associate Source Servers with Existing Servers on Huawei Cloud

If you have servers on Huawei Cloud, you can associate source servers with these existing Huawei Cloud servers. These Huawei Cloud servers will be used to receive data migrated from their paired source servers. Then you can skip step 5 and go to **Step 6: Create a Migration Workflow**.

If you do not want to migrate data to these existing Huawei Cloud servers, skip the current step and go to **Step 5: Create an Application Assessment**.

CAUTION

Before associating an existing server on Huawei Cloud with a source server, make sure that the existing server meets the following requirements:

- Disks on the existing server can be formatted. During the migration, disks on the existing server will be formatted and re-partitioned based on the source disk settings for receiving data migrated from the source server.
- To migrate over the Internet, the existing server must be able to access the Internet.
- The existing server must be in the same region as the **application** that the source server is added to.

Step 1 In the navigation pane on the left, choose **Design** > **Migration Solutions**.

Step 2 Click **View Resources** in the **Target Configuration** card.

Step 3 On the displayed **Servers** tab, locate a source server and click **Associate** in the **Target Association** column.

Step 4 In the displayed dialog box, select the region of the **application** and select a project. Then, select an existing Huawei Cloud server and click **Confirm**.

After the association is complete, **Associated** is displayed in the **Target Association** column. You can click **Details** to view the specifications of the associated target server.

----End

Step 5: Create an Application Assessment

Assessing an application can get recommendations for most suitable Huawei Cloud resources based on the specifications, performance, and business purpose

data of the source resources added to the application, as well as your selected recommendation references, such as, cost or performance reference and ECS type references.

NOTE

If your source servers have been **associated with existing servers** on Huawei Cloud, you can skip this step and create a migration workflow to migrate them.

Step 1 On the **Migration Solutions** page, click **Assess** in the **Target Configuration** card.

Step 2 In the **Select Application** drop-down list, select the **application** that contains the source servers to be assessed.

Step 3 In the **Select Resources** area, select the servers to be assessed.

Step 4 Configure an assessment policy based on **Table 2-2**.

Table 2-2 Settings used for computing target recommendations

Parameter	Option	Description
Target Region	-	Select the region where you want to purchase resources on Huawei Cloud. You are advised to select a region close to your target users for lower network latency and quick access.
Assessment Policy	Match source configuration	MgC will recommend Huawei Cloud resources in the same or similar size as source resources. For details about how MgC recommends appropriate target resources for you, see **How Does MgC Generate Target Recommendations?**
	Match business scenario	MgC recommends appropriate Huawei Cloud resources based on the business scenario of source resources and Huawei Cloud best practices. For details about how MgC recommends appropriate target resources for you, see **How Does MgC Generate Target Recommendations?**
Priority	High performance	MgC recommends target resources with optimal performance.
	Low cost	MgC recommends the most cost-effective target resources that meet your demands.
Preferences	Server Types (Optional)	Select the server types you prefer.

Parameter	Option	Description
	Server Series (Optional)	Select the server series you prefer. The system will generate recommendations based on your preferred server types and series. **NOTICE** If you select **Display only series allowed on DeHs**, **Server Types** will be dimmed, and the server series allowed on DeHs in the target region will be listed.
	System Disk (Optional)	Select the system disk type you prefer.
	Data Disk (Optional)	Select the data disk type you prefer.
	Sizing Criteria	Select the criteria that the system will follow for generating server recommendations. For details about how MgC recommends appropriate target resources for you, see **How Does MgC Generate Target Recommendations?**

Step 5 Click **OK**.

Step 6 In the application list on the **Migration Solutions** page, locate the applications and click **View Target Configurations** in the **Operation** column.

In the **Target Configurations** area, you can view the specifications of Huawei Cloud resources recommended based on the source resource specifications and your selected preferences. It also gives you the ability to estimate the cost of running on Huawei Cloud. In addition, you can modify the recommended target configurations.

----End

Step 6: Create a Migration Workflow

Create a workflow to migrate the source servers to Huawei Cloud. For details, see **Creating a Server Migration Workflow**.

2.3 Migrating Servers from Alibaba Cloud to Huawei Cloud

2.3.1 Overview

This best practice describes the detailed procedure and precautions for migrating servers from Alibaba Cloud to Huawei Cloud.

The key steps include:

1. **Making Preparations**: Ensure that the migration accounts are available and the accounts have required permissions.
2. **Installing Edge**: Download and install Edge, a tool provided by MgC.
3. **Discovering Resources**: Collect information about the Alibaba Cloud ECSs to be migrated.
4. **Assessing Migration Readiness**: Check the configuration of the Alibaba Cloud ECSs to be migrated, test their network connectivity, and gather them into groups.
5. **Assessing Target Servers**: Get recommendations for Huawei Cloud resources and configure target servers for source servers.
6. **Creating a Workflow**: Create a migration workflow to migrate your source servers.

Notes

Before creating a server migration workflow, read and understand the following precautions.

Item	Precaution
Source download bandwidth	Used to download the migration Agent to source servers. • If each source server uses a dedicated bandwidth, the bandwidth must be at least 30 Mbit/s. • If source servers share a bandwidth, the average bandwidth must be at least 50 Mbit/s.
Migration bandwidth	• Used to migrate data. It affects the migration speed and duration. • For details about how to estimate the migration duration, see **How Long Does a Migration Take?**
CPU and memory	• At least 520 MB of available memory • At least 0.3 CPUs available in Linux and at least 1 CPU available in Windows
OS compatibility	For details about what OSs are supported, see **Supported OSs**.
Server migration statements	For details about the important statements you need to understand before the migration, see **What Are the Important Statements of SMS?**
Notes and constraints	For details about the notes and constraints for server migration, see **Notes and Constraints**.
Billing	For details about the fees that may be incurred during the migration, see **Billing**.
Permissions configuration	For details about the permissions the target account must have, see **Permissions Management**.

Item	Precaution
Migration network and ports	For details about the requirements for the migration network and ports, see **How Do I Set Up a Secure Migration Network for Using SMS?**

2.3.2 Preparations

To ensure a smooth migration, you need to complete the following preparations:

Preparing a Huawei Account

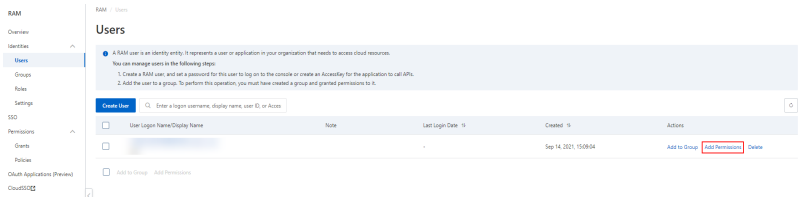
Before using MgC, prepare a Huawei ID or an IAM user that can access MgC and obtain an access key (AK/SK) of the account or IAM user. For more information, see **Preparations**.

Obtaining an Access Key for Your Alibaba Cloud

Check whether your Alibaba Cloud account has an AK/SK pair and has the **AliyunECSReadOnlyAccess** permissions. If it does not have, perform the following steps to generate the AK/SK pair and add the required permissions for it:

1. Sign in to the RAM console using your Alibaba Cloud account.
2. In the navigation pane on the left, choose **Identities** > **Users**.
3. On the **Users** tab, click **Create User**.
4. On the **Create User** page, in the **User Access Key** area, click **Create Access Key**.
5. Assign permissions to the RAM user.

   On the **Users** page, click **Add Permissions** in the **Operation** column and grant the **AliyunECSReadOnlyAccess** permissions to the RAM user.



Creating a Migration Project

Create a migration project on the MgC console. For details, see **Managing Migration Projects**.

2.3.3 Step 1: Download and Install Edge

Edge is a migration tool provided by MgC. It is used to discover source resources and execute migration commands from MgC.

Procedure

Step 1 Prepare a Windows server in the source intranet environment and install Edge on the server. For details about the requirements for the server and how to install Edge, see **Installing Edge for Windows**.

> **CAUTION**
>
> Do not install Edge on a source server to be migrated.
>
> - **High resource consumption**: Edge consumes CPU and memory resources during collection and migration. If a large number of migration tasks are performed by Edge, services on the source server may be affected.
> - **Port occupation**: Edge occupies some ports on the source server, which may affect services on the server.

Step 2 Register an account for logging in to Edge and connect Edge to MgC. For details, see **Connecting the Edge Device to MgC**.

Step 3 After the connection is successful, add the credentials of the source servers to be migrated to Edge. For details, see **Adding Resource Credentials**. Correctly configure **Resource Type** based on the source servers when you add their credentials.

----End

2.3.4 Step 2: Discover Alibaba Cloud ECSs

Prerequisites

- You have completed all **preparations**.
- You have **installed Edge** in the source environment and connected it to MgC.

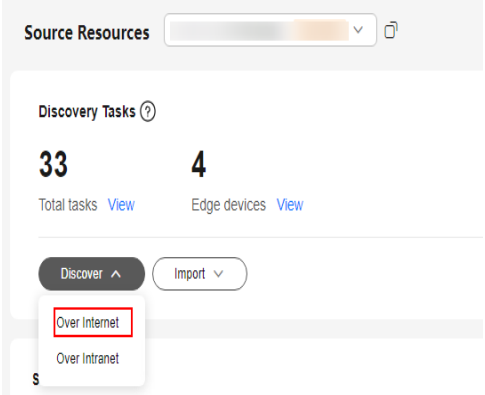
Procedure

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

Step 2 In the navigation pane on the left, choose **Research** > **Source Resources**. In the upper left corner of the page, select the migration project created in **Preparations**.

Step 3 In the **Discovery Tasks** card, choose **Discover** > **Over Internet**.

Figure 2-4 Discovery over Internet



Step 4 Configure the parameters based on **Table 2-3**.

Table 2-3 Parameters for creating an Internet-based discovery task

Region	Parameter	Description	Mandatory
Basic Settings	Task Name	Enter a task name.	Yes
	Task Description	Describe the task.	No
Task Settings	Source Platform	Select **Alibaba Cloud**.	Yes
	Credential	Select the credential for accessing Alibaba Cloud. If the credential has not been added, choose **Create** to add it. For details, see **Managing Credentials**. **NOTICE** Select **AK/SK** for **Authentication** and enter the AK/SK pair of your Alibaba Cloud account. Your account must have the **AliyunECSReadOnlyAccess** permissions.	Yes
	Region	Select the region where the source servers are located. You can select multiple regions.	Yes
Resource Discovery	Cloud Platform Collection	Enable cloud platform collection, select **Servers** from the **Resource Type** drop-down list.	Yes
	Application Association (Optional)	An application is a group of resources that need to be migrated together. You can add resources to or remove resource from an application as needed. You can use the application to get recommendations for target resources and create a workflow to migrate the source resources. • If an application is available, select the application from the **Application** drop-down list. • If no application is available, click **Create Application**. In the displayed dialog box, enter an application name and description, select a business scenario, environment, and region (where you are migrating to), and click **OK**.	No

Step 5 Click **Confirm**. After the task is created, the system automatically starts collecting information about your Alibaba Cloud ECSs.

- On the **Source Resources** page, click **View** next to **Total tasks** to go to the task list. You can view the task status and task details. If the task status is **Failed**, click **View** in the **Operation** column to view the data source that failed to be collected. You can move the cursor to the collection status of the data source to view the failure cause.
- On the **Source Resources** page, in the server list, click **Server** in the **Category** column or the number in the **Total Resources** column. On the **Servers** tab, you can view the discovered source servers and their details.

----End

2.3.5 Step 3: Assess Migration Readiness

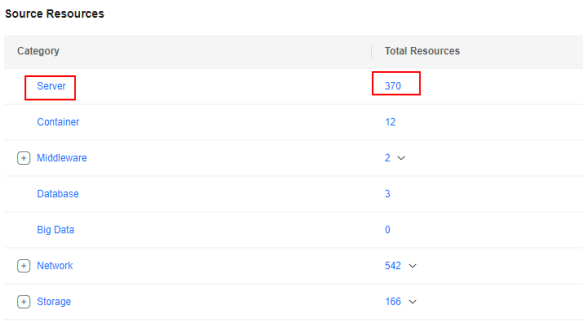
Measure whether the source servers are ready to migrate from the items of basic configuration, network environment, and migration group.

Prerequisites

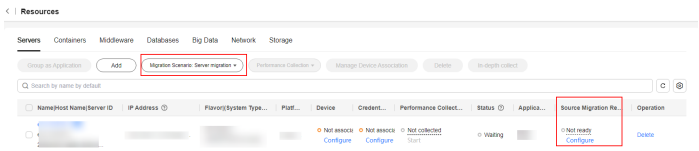
- Your **Alibaba Cloud ECSs have been discovered**.
- You have **added source server credentials** to the Edge device.

Procedure

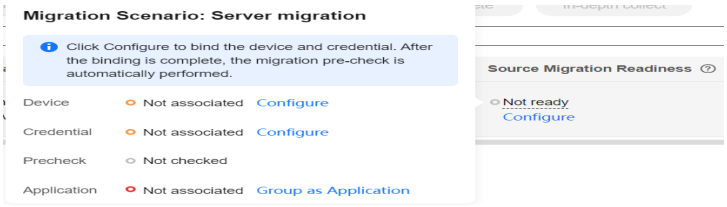
Step 1 On the **Source Resources** page, in the resource list, click **Server** in the **Category** column or the number in the **Total Resources** column.



Step 2 On the top of the server list, choose **Migration Scenario** > **Server migration**.



Step 3 Locate a source server and move the cursor to **Not ready** in the **Migration Readiness** column. You can view the configurations that need to be completed to make the server ready. You need to associate the server with an Edge device and a credential, and add the server to an application, pass the migration pre-check (automatically triggered), and add the server to an application. Click **Configure** in the **Edge Device** or **Credential** column.



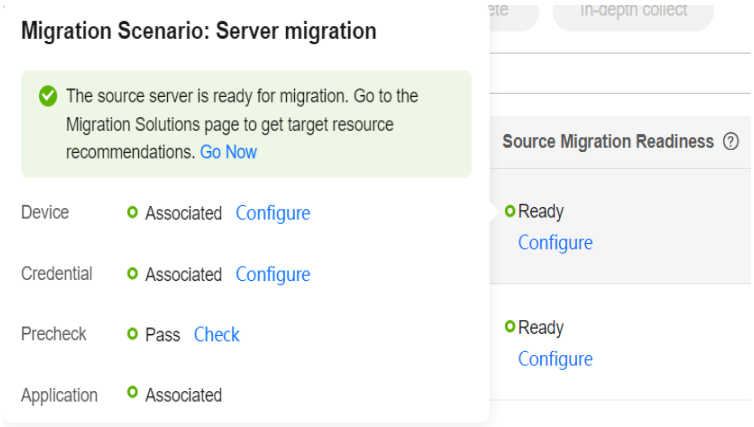
Step 4 Configure the parameters listed in **Table 2-4**.

Table 2-4 Parameters for configuring migration readiness

Parameter	Configuration
Type	Set this parameter based on the source server OS type.
Edge Device	Select the Edge device prepared in **Step 1: Download and Install Edge**. If there are a large number of servers to be associated with this Edge device, you can select these servers and click **Manage Device Association** above the list to associate them in a batch.
IP Address	Select the IP address for accessing the source server. It can be a public or private IP address. After the pre-migration check is passed, the IP address you select here will be used for migration. During the migration, Edge accesses the source server through this IP address.
Port	Select the source server's port that allows traffic from Edge. • By default, port 5985 on Windows source servers must be opened to the Edge device. The port cannot be changed. • By default, port 22 on Linux source servers must be opened to the Edge device. You can specify a different port if needed.
Credential	Select the server credential you added to Edge. If the credential has not been added to MgC, go to the Edge console, **add the server credential** to the Edge device, and synchronize it to MgC.

Step 5 Click **Confirm**. The system performs checks whether the source server can be accessed from the Edge device using the information you provided, and collect resource details again if necessary. The pre-check takes about 10 seconds.

Step 6 Add the source server to an application. For details, see **Grouping Resources as Applications**. Check whether **Ready** is displayed in the **Migration Readiness** column.



CAUTION

To reduce migration risks, you are advised to group no more than 30 servers as an application. If more than 30 servers need to be migrated, group them as multiple applications.

----End

2.3.6 Step 4: Create an Application Assessment

Assessing an application can generate recommendations for rightsized Huawei Cloud resources based on the specifications, performance, and business purpose of the source resources added to the application, as well as your requirements for cost, availability, and compliance.

Prerequisites

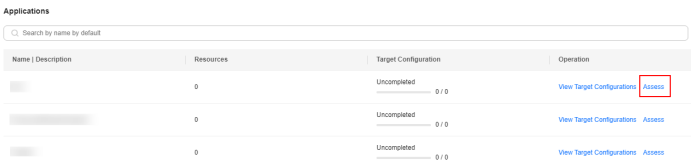
You have **assessed the migration readiness** of source resources and grouped them as applications.

Procedure

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

Step 2 In the navigation pane on the left, choose **Design** > **Migration Solutions**. On the **Migration Solutions** page, you can view the list of applications created in the current project.

Step 3 In the application list, locate the application you want to assess and click **Assess** in the **Operation** column.



Step 4 In the **Select Resources** area, select the servers to be assessed in the application.

Step 5 Configure an assessment policy based on **Table 2-5**.

Table 2-5 Settings used for computing target recommendations

Parameter	Option	Description
Target Region	-	Select the region where you want to purchase resources on Huawei Cloud. You are advised to select a region close to your target users for lower network latency and quick access.
Assessment Policy	Match source configuration	MgC will recommend Huawei Cloud resources in the same or similar size as source resources. For details about how MgC recommends appropriate target resources for you, see **How Does MgC Generate Target Recommendations?**
	Match business scenario	MgC recommends appropriate Huawei Cloud resources based on the business scenario of source resources and Huawei Cloud best practices. For details about how MgC recommends appropriate target resources for you, see **How Does MgC Generate Target Recommendations?**
Priority	High performance	MgC recommends target resources with optimal performance.
	Low cost	MgC recommends the most cost-effective target servers that meet your demands.
Preferences	Server Types (Optional)	Select the server types you prefer.
	Server Series (Optional)	Select the server series you prefer. The system will generate recommendations based on your preferred server types and series. **NOTICE** If you select **Display only series allowed on DeHs**, **Server Types** will be dimmed, and the server series allowed on DeHs in the target region will be listed.
	System Disk (Optional)	Select the system disk type you prefer.
	Data Disk (Optional)	Select the data disk type you prefer.

Parameter	Option	Description
	Sizing Criterion	Select the criteria that the system will follow for generating server recommendations. For details about how MgC recommends appropriate target resources for you, see **How Does MgC Generate Target Recommendations?**

Step 6 Click **Create Assessment**. After the assessment task is complete, you can **view the assessment results** which include the recommended specifications of target resources. You can also **view server performance data**.

Step 7 (Optional) Perform the following operations:

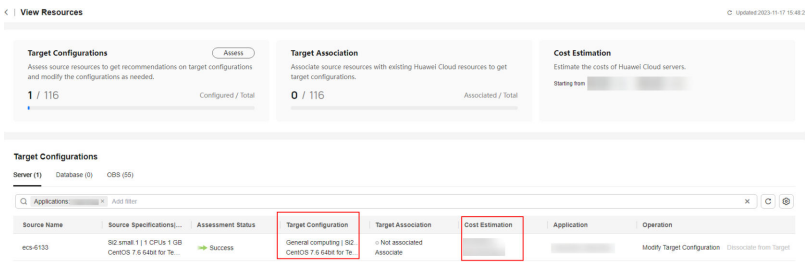
- **Modify the recommended target configurations** as needed. You can change the server and disk specifications. Disk downsizing is supported.
- **Associate source servers with target servers**. If based on the target server recommendations, you find that you already have servers that match your requirements on Huawei Cloud, you can associate them with source servers.

----End

Viewing Target Recommendations

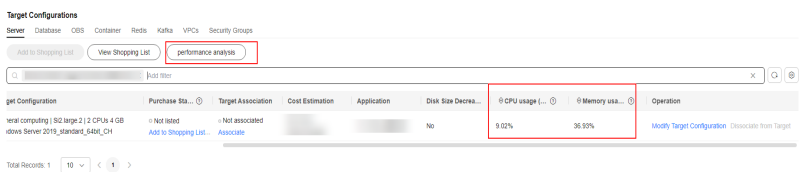
In the application list on the **Migration Solutions** page, click **View Target Configurations** in the **Operation** column.

In the **Target Configurations** area, you can view the specifications of Huawei Cloud resources recommended based on the source resource specifications and your preferences. It also gives you the ability to estimate what it will cost to run your services on Huawei Cloud.



Viewing Server Performance Data

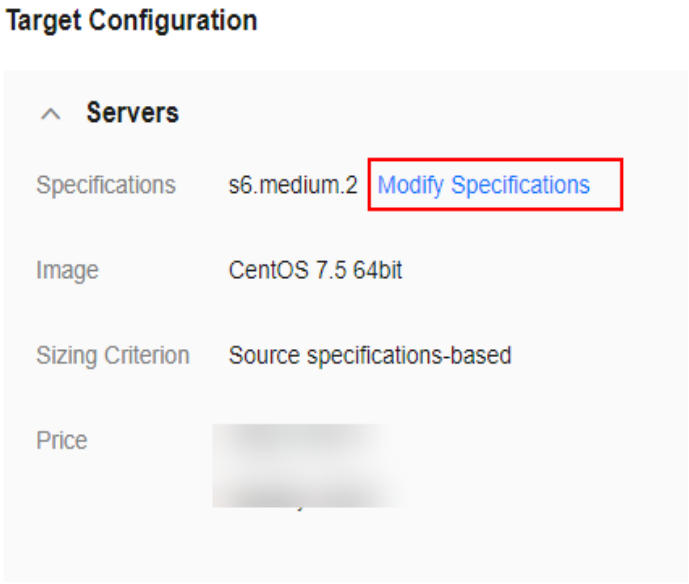
On the **Target Configurations** page, in the server list, you can view the average CPU and memory usage of each server over the last 7 or 30 days. Click **Performance Analysis** to view the performance statistics of all servers.



Modifying Target Recommendations

Step 1 In the **Target Configurations** area, locate the server that you want to modify the recommended target configurations for and click **Modify Target Configuration** in the **Operation** column.

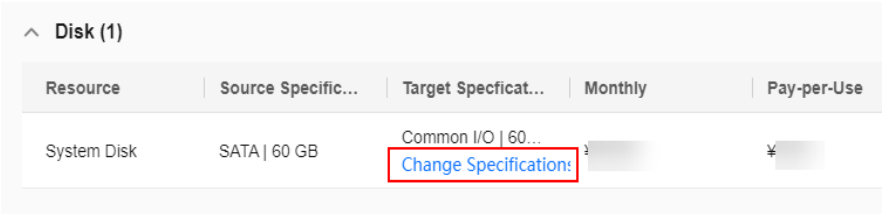
Step 2 Modify the specifications and image for the target server.



Step 3 In the disk area, locate a disk and click **Modify Specifications** in the **Target Specifications** column. You can modify the disk type and capacity. You can downsize disks for Linux target servers based on the disk usage of the source servers. If you downsize a disk for the target server, the system will set **Disk Downsized** to **Yes**. The reverse also applies.

NOTICE

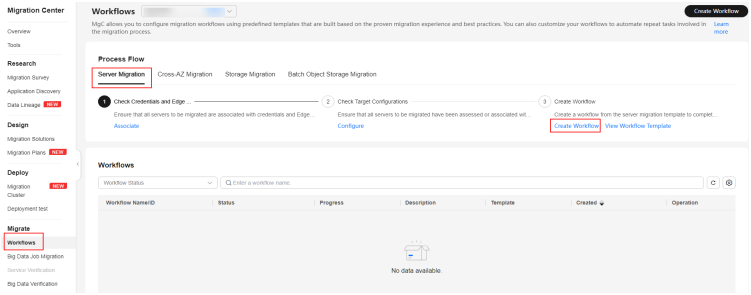
- The system disk capacity ranges from 40 GB to 1,024 GB.
- The data disk capacity ranges from 10 GB to 32,768 GB.
- Disk downsizing is only available for Linux, and the decreased sizes must be larger than the used sizes of the source disks.
- In the cross-AZ migration scenario, only disk upsizing is supported. Even if you choose to downsize disks here, the settings will not be applied, and the system will create target disks as large as source disks.



----End

2.3.7 Step 5: Create a Server Migration Workflow

After all operations in **Making Preparations** and **Step 1** to **Step 4** are complete, you can go to the **Workflows** page to **create a server migration workflow**.



2.4 One-stop Cross-AZ ECS Migration

Scenario

Use MgC to quickly migrate cloud servers from one AZ to another. This practice applies to migration of fewer than 30 ECSs in a single batch across AZs within a region. You only need to specify a resource group name, and MgC takes care of all the rest, from resource discovery, collection, and assessment to migration.

Preparations

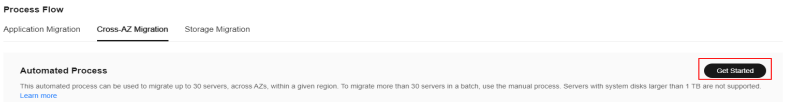
You need to prepare a Huawei account or an IAM user that can access MgC. For details, see **Preparations**.

Procedure

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

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

Step 3 In the **Process Flow** area, click the **Cross-AZ Migration** tab. In the **Automated Process** area, click **Get Started**.



Step 4 In the displayed dialog box, specify an application name and select the target AZ you want to migrate to.

Step 5 Click **Create and Run**. MgC will automatically collect information about servers in the selected source AZ under the current account, creates an application, adds the discovered servers to the application, and starts the assessment process.

Step 6 After the assessment process is complete, click **Close** to configure the workflow.

Step 7 Configure the workflow parameters listed in **Table 2-6**.

Table 2-6 Parameters required for configuring a workflow

Area	Parameter	Description
Workflow Details	Name	Enter a workflow name.
	Description	Enter a workflow name.
Application	Application	Select the application defined in **Step 4**.
Migration Settings	Region	Select the region where the source AZ is located. The region configured in the application is populated by default.
	Target AZ	Select the AZ you want to migrate to. The configuration must be the same as that of the created application.
	Target Network	Only **Retain original** is available.
	Target Server	Create now. MgC creates backups and images for source servers, and uses the images to create target servers immediately after the workflow runs.
	Stop Target Server	• If you select **Yes**, target servers will be stopped after being created. • If you select **No**, target servers will be started after being created.
	Stop Source Server	• If you select **Yes**, source servers will be stopped before incremental backups are created for them. This ensures data consistency as high as possible. • If you select **No**, source servers remain running when incremental backups are created for them.
	Create System Disk Image	• If you select **Yes**, a system disk image will be created for each of the source servers. The images can be used to reinstall the OS for the paired target servers. • If you select **No**, the system will not create system disk images for the source servers.
Advanced Settings	Delete Intermediate Resources	If this function is enabled, intermediate resources generated during the migration, such as backups, snapshots, and images, will be deleted after the service cutover is complete.

Area	Parameter	Description
	Retain Primary NIC IP Addresses	If this function is enabled, the private and public IP addresses of the primary NIC on source servers will be retained on target servers, and random private IP addresses will be allocated to source servers. You need to manually roll back this operation if needed.

Step 8 Configure the workflow and click **Next: Confirm**. After confirming that the configuration is correct, click **Create**. The migration workflow will be created and displayed in the workflow list.

CAUTION

After a migration workflow is created, it switches to the **Waiting** status, and the migration has not started.

Step 9 Click the workflow name to go to the details page. The steps are predefined steps in the template. You can **add stages and steps** to the workflow.

Step 10 Click **Run** in the **Operation** column to start the migration.

- You can view the migration progress on the **Steps** tab. The workflow can continue only after you perform the manual steps contained.
- On the **Servers** tab, you can view the migration status of each server.

----End

2.5 Migrating Servers Across AZs on Huawei Cloud

Scenario

This section describes how to use MgC to migrate a large number of servers between AZs within a region of Huawei Cloud. For a small-scale, single-batch migration of fewer than 30 servers, see **One-stop Cross-AZ ECS Migration**.

Preparations

- Prepare a Huawei account or an IAM user that can access MgC. For details, see **Preparations**.
- **Create a migration project** on the MgC console.

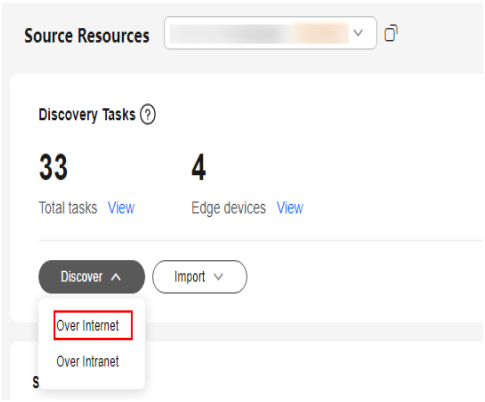
Step 1: Discovers Servers in the Source AZ

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

Step 2 In the navigation pane on the left, choose **Research** > **Source Resources**. Select a **migration project** in the upper left corner of the page.

Step 3 In the **Discovery Tasks** card, choose **Discover** > **Over Internet**.

Figure 2-5 Discovery over Internet



Step 4 Configure the parameters listed in **Table 2-7**.

Table 2-7 Parameters for creating an Internet-based discovery task

Region	Parameter	Description	Mandatory
Task Basics	Task Name	Enter a task name.	Yes
	Task Description	Describe the task.	No
Task Settings	Source Platform	Select **Huawei Cloud**.	Yes
	Credential	Select the credential of the source account. If no credential is available, choose **Create** to create a credential by referring to **Adding a Credential**. **NOTE** The AK/SK pair of the source account must be specified in the new credential.	Yes
	Region	Select the region where the source servers are located. You can select multiple regions.	Yes

Step 5 Enable cloud platform collection, select **Servers** from the **Resource Type** drop-down list.

Step 6 (Optional) Group the servers to be discovered as an application.

- If an application is available, select the **application** from the **Application** drop-down list.

- If no application is available, click **Create Application**. In the displayed dialog box, enter an application name and description, select **Cross-AZ migration** for **Business Scenario**, select the target region and AZ, and click **OK**.

Step 7 Click **OK**. After the discovery task is created, MgC starts to automatically discover servers in the selected regions selected in **Step 4**.

- On the **Source Resources** page, in the resource list, click **Server** in the **Category** column or the number in the **Total Resources** column.
- On the **Source Resources** page, in the **Discovery Tasks** card, click **View** next to **Total tasks**. If the task status is **Failed**, click **View** in the **Operation** column to view the data source that failed to be collected. You can move the cursor to the collection status of the data source to view the failure cause.

----End

Step 2: Group Servers as an Application

If the servers discovered have already been grouped into an application in **step 6**, ski p this section and go to **Step 3: Getting Target Recommendations**.

Step 1 In the **Servers** list of the **Resources** page, select the servers to be added to the same application and choose **Resource Management** > **Manage Application Association** in the upper left corner.

Step 2 Select the application from the drop-down list. If no application is available, click **Create Application**. In the displayed dialog box, enter an application name and description, select **Cross-AZ migration** for **Business Scenario**, select the target region and AZ, and click **OK**. For details, see **Creating an Application**.

Step 3 Click **OK**. You can view the application name in the **Application** column of these servers.

----End

Step 3: Getting Target Recommendations

Step 1 On the **Migration Solutions** page, click **Assess** in the **Target Configuration** card.

Step 2 In the **Select Application** drop-down list, select the **application** into which the source servers have been grouped.

Step 3 In the **Select Resources** area, select the resources to be assessed in the application.

Step 4 Configure the assessment policy based on **Table 2-8**.

Table 2-8 Settings used for computing target recommendations

Parameter	Description
Target Region	Select the region you want to migrate to.
Assessment Policy	Select **Cross-AZ migration** and select the target AZ.

Parameter	Description
Priority	• High performance MgC recommends target resources based on your performance requirements. • Low cost MgC recommends target resources based on your cost requirements.
Preferences	You can select server types, server series, and disk types you prefer. Your preferences have the highest priority during the resource assessment.

Step 5 Click **OK**.

Step 6 In the application list on the **Migration Solutions** page, locate the applications and click **View Target Configurations** in the **Operation** column.

In the **Target Configurations** area, you can view the specifications of Huawei Cloud resources recommended based on the source resource specifications and your selected preferences. It also gives you the ability to estimate the cost of running on Huawei Cloud. In addition, you can modify the recommended target configurations.

----End

Step 4: Creating a Cross-AZ Migration Workflow

After **step 1** to **step 3** are complete, **create a cross-AZ migration workflow**.

2.6 Migrating Servers to FlexusX Instances (Original HECS X Instances)

Overview

Compared with ECSs, **FlexusX instances** provide more refined specifications to accurately match the actual resource requirements of user services. This can help reduce cloud migration costs and avoid resource wastes. To free you from selecting or customizing FlexusX instance specifications, you can use MgC to collect the CPU and memory usage of source servers and then use the collected performance data to get target server recommendations. This can help you improve performance and control costs.

Application Scope

This practice applies to servers from Alibaba Cloud, Huawei Cloud, AWS, Tencent Cloud, and Azure and on-premises servers that you add to MgC manually.

What you need to do differs with the actual scenario. For details, see the following table.

Scenario	What You Need to Do
Getting FlexusX instance recommendations and manually purchasing the recommended FlexusX instances	Preparations, steps 1 to 7, and **manual purchase**
Getting FlexusX instance recommendations, manually purchasing the recommended FlexusX instances, and migrating to FlexusX instances using MgC	Preparations, steps 1 to 8, and **manual purchase**. You need to configure the FlexusX instances you purchase as target servers in step 7.
Getting FlexusX instance recommendations, automatically purchasing the recommended FlexusX instances, and migrating to FlexusX instances using MgC	Preparations and steps 1 to 8

Making Preparations

- Preparing a Huawei Account

  Before using MgC, prepare a HUAWEI ID or an IAM user that can access MgC and obtain an AK/SK pair for the account or IAM user. For details about how to obtain an access key, see **Preparations**.

- Creating a Migration Project

  Create a migration project on the MgC console. For details, see **Managing Migration Projects**.

Procedure

Step 1 Download and install Edge.

Prepare a Windows server in the source intranet environment for installing Edge. If you do not have an idle cloud server, you are advised to purchase a pay-per-use cloud server with 4 vCPUs and 8 GB of memory. For details about the server requirements and Edge installation method, see **Installing Edge for Windows**.

Step 2 Connect Edge to MgC.

Register an account for logging in to Edge and connect Edge to MgC. For details, see **Connecting the Edge Device to MgC**.

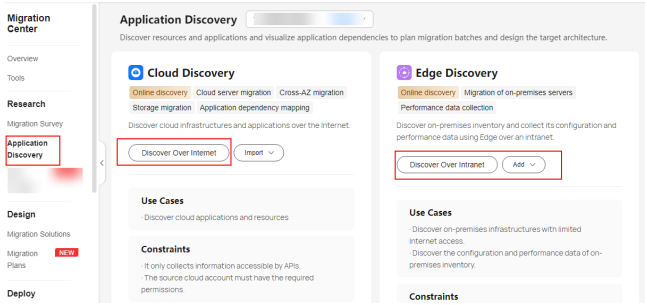
Step 3 Add resource credentials.

After the connection is successful, add the credentials of the source servers to be migrated to Edge. For details, see **Adding Resource Credentials**. Correctly configure **Resource Type** based on the source servers when you add their credentials.

Step 4 Discover servers.

MgC provides three collection methods to meet your requirements in different scenarios. You can choose a method based on your source environment.

Figure 2-6 Collection methods



- If your source servers are on a cloud platform, such as Alibaba Cloud, Huawei Cloud, AWS, Tencent Cloud, Google Cloud, or Azure, you can **collect the data about your servers over the Internet**. You can also **manually add the server data to MgC**.
- If your source servers are in an on-premises IDC, you can **collect the server data over the intranet**. MgC enables you to scan for servers by network range or VMware vCenter Server. You can also **manually add the server data to MgC**.

Step 5 Collect server performance data.

With collected performance data of servers, you can get recommendations for target servers with the right amount of CPU and memory resources to match the needs of your applications. For more information, see **Collecting Server Performance Data**.

NOTICE

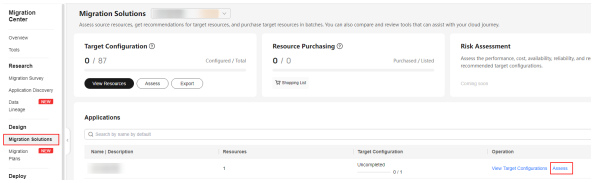
- If the source servers run daily fixed services, it is recommended that the performance collection duration should be no less than one day.
- If the source servers run services that fluctuate periodically, it is recommended that the performance collection duration should cover the entire fluctuation period to accurately evaluate the performance of source servers.

Step 6 Group servers as an application.

Group the discovered servers as an application to get sizing recommendations and execute the migration. For more information, see **Grouping Resources as Applications**.

Step 7 Create an application assessment. Assess the application to get FlexusX instance recommendations.

1. On the MgC console, in the navigation pane on the left, choose **Design** > **Migration Solutions**. On the **Migration Solutions** page, you can view the list of applications created in the current project.
2. In the application list, locate the application you want to assess and click **Assess** in the **Operation** column.



3. In the **Select Resources** area, select the application resources to be assessed.
4. Configure the assessment policy based on **Table 2-9** to get FlexusX instance recommendations.

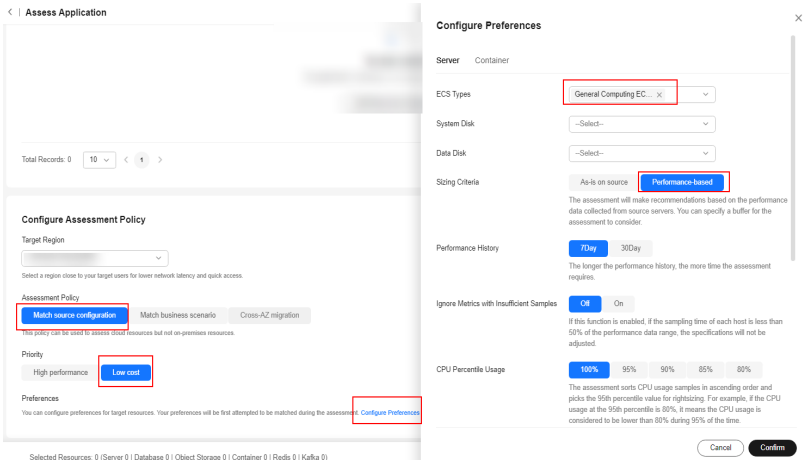


Table 2-9 Parameters for configuring an assessment policy

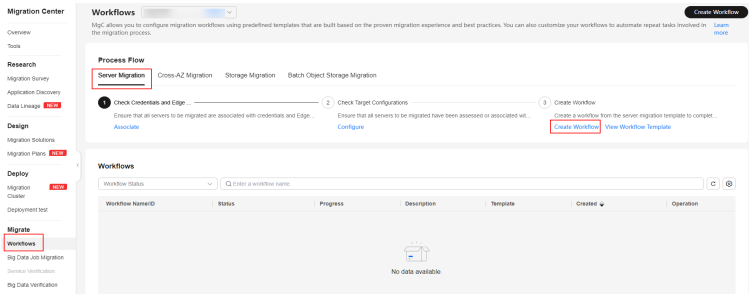
Parameter	Option	Description
Target Region	-	Select the region where you want to purchase resources on Huawei Cloud. You are advised to select a region close to your target users for lower network latency and quick access.
Assessment Policy	Match source configuration	MgC will recommend Huawei Cloud resources in the same or similar size as source resources.
Priority	Low cost	MgC recommends the most cost-effective target servers that meet your demands.

Parameter	Option	Description
(Mandatory) Preferences You are advised to select **Performance-based** for **Sizing Criteria**.	Server Types (Optional)	Select **General Computing**. For details about how MgC recommends appropriate target resources for you, see **How Does MgC Generate Target Recommendations?**
	Server Series (Optional)	Select the server series you prefer.
	System Disk (Optional)	Select the system disk type you prefer.
	Data Disk (Optional)	Select the data disk type you prefer.
	Sizing Criteria	If you select **Performance-based**, you need to perform a **performance collection** for the source servers, and then set assessment parameters. The system will then recommend target servers with your desired CPU and memory specifications. The more performance data is collected, the more accurate the target recommendations are. For details about how MgC recommends appropriate target resources for you, see **How Does MgC Generate Target Recommendations?**

5. Click **Create Assessment**. After the assessment is complete, you can **view the assessment results** and **view server performance data**. The recommended target server sizes are included in the assessment results.
6. (Optional) Perform the following operations:
   - **Modify the recommended target configurations** as needed. You can change the server and disk specifications. Disk downsizing is supported.
   - **Associate source servers with target servers**. If you already have servers that match your requirements on Huawei Cloud, you can associate them with source servers.

Step 8 Create a server migration workflow.

Go to the **Workflows** page and **create a server migration workflow**.



----End

2.7 Keeping Private IP Addresses of Servers Unchanged After the Migration

In MgC server migration workflows, you can choose to retain private IP addresses for source servers on target servers after the migration. This feature can reduce the need to modify service code due to IP address changes.

Disclaimer

- **Service availability risks**

  This feature can ensure that the private IP addresses of source servers are retained on target servers. It does not guarantee your services can run properly on the target servers. You need to evaluate and assume the risks arising from using this feature.

- **Rollback description**

  Migration workflows cannot automatically roll back the IP addresses of target servers to their original ones. If any problems happen when you use this function, you can **perform a rollback manually**.

- **IP address conflicts**

  Since the source and target servers have the same private IP addresses, there may be IP address conflicts. This may result in service unavailability.

- **Unknown risks**

  There may be other unknow issues since the migration does not detect or scan source services.

- **Customer responsibilities**

  You need to fully test and prepare for the migration as well as check and solve possible problems after the migration is complete. You are advised to simulate the migration in a test environment to evaluate potential risks and formulate corresponding countermeasures.

Notes and Constraints

- **Shutting downing target servers**

  To retain source servers' private IP addresses on the paired target servers, the target servers must be stopped. If a target server is not stopped, the system will stop it automatically.

- **Subnet requirements**

When you select a subnet in the target VPC, the subnet must be in the same network range as the source servers.

- **Network interface requirements**

  A target server can only have one network interface. Extended network interfaces are not allowed for target servers.

- **Supported IP version**

  Only IPv4 addresses can be retained.

Preparations

- Preparing a Huawei account

  Before using MgC, prepare a HUAWEI ID or an IAM user that can access MgC and obtain an AK/SK pair for the account or IAM user. For details about how to obtain an access key, see **Preparations**.

- Creating a migration project

  Create a migration project on the MgC console. For details, see **Managing Migration Projects**.

Procedure

Step 1 Download and install Edge.

Prepare a Windows server on the source intranet for installing Edge. For details about the server requirements and Edge installation method, see **Installing Edge for Windows**.

Step 2 Connect Edge to MgC.

Register an account for logging in to Edge and connect Edge to MgC. For details, see **Connecting the Edge Device to MgC**.

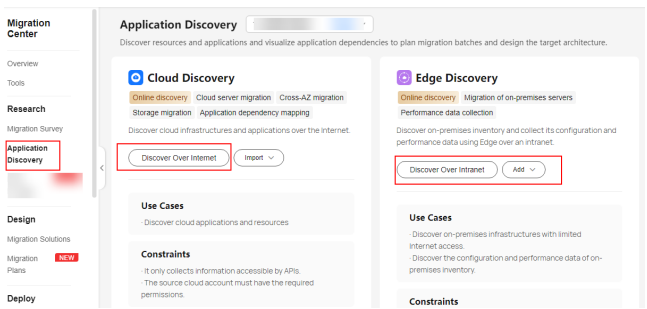
Step 3 Add resource credentials.

After the connection is successful, add the credentials of the source servers to be migrated to Edge. For details, see **Adding Resource Credentials**. Correctly configure **Resource Type** based on the source servers when you add their credentials.

Step 4 Discover source servers.

MgC provides three collection methods to meet your requirements in different scenarios. You can choose a method based on your source environment.

Figure 2-7 Collection methods



- If your source servers are on a cloud platform, such as Alibaba Cloud, Huawei Cloud, AWS, Tencent Cloud, Google Cloud, or Azure, you can **collect the data about your servers over the Internet**. You can also **manually add the server data to MgC**.
- If your source servers are in an on-premises IDC, you can **collect the server data over the intranet**. MgC enables you to scan for servers by network range or VMware vCenter Server. You can also **manually add the server data to MgC**.

Step 5 Group servers as an application.

Group the discovered servers as an application to get sizing recommendations and execute the migration. For more information, see **Grouping Resources as Applications**.

Step 6 Create an application assessment.

The system will generate target server recommendations based on the collected source server details, including specifications, performance data, and workload types. For more information, see **Getting Target Recommendations**.

After the target server recommendations are generated, you can:

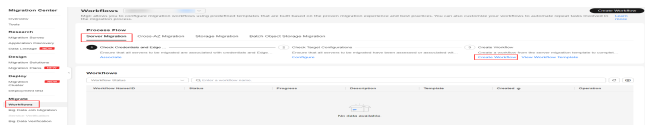
- **Modify the recommended target configurations** as needed. You can change the server and disk specifications. Disk downsizing is supported.
- **Associate source servers with target servers**. If based on the target server recommendations, you find that you already have servers that match your requirements on Huawei Cloud, you can associate them with source servers.

Step 7 Create a server migration workflow. After all the preceding steps are complete, go to the **Workflows** page and create a server migration workflow.

CAUTION

- A workflow can contain a maximum of 100 servers.
- You can migrate a maximum of 1,000 servers concurrently. For any servers beyond this number, the workflows will pause at the first step and put these servers in a pending state until other servers complete their migration. The workflows will then automatically start on these servers in the order the workflows were created.
- If this is your first time to create a server migration workflow, you need to delegate MgC the required permissions. For more information about the required permissions, see **Agency Permissions**.

1. In the navigation pane on the left, choose **Migrate** > **Workflows**. In the upper left corner of the page, select the **migration project you created**.
2. Select the **Server Migration** template and click **Configure Workflow**.



3. In the **Workflow Details** area, customize **Name** and **Description**.

4. In the **Application** area, select the application you created in **Step 5**.

NOTICE

For source servers in the selected applications, you need to **get target server recommendations** or **associate them with target servers**.

5. In the **Migration Network** area, select a network type.
   - If you select **Public**, ensure that all target servers have EIPs bound. These EIPs will be used for the migration.
   - If you select **Private**, configure Direct Connect connections, VPN connections, VPC peering connections, or subnets in the target VPC in advance to ensure that the source environment can access the target environment.
6. In the **Target Environment** area, select the VPC and subnet that have been connected to the source environment. The VPC and subnet will be used as the transit environment.

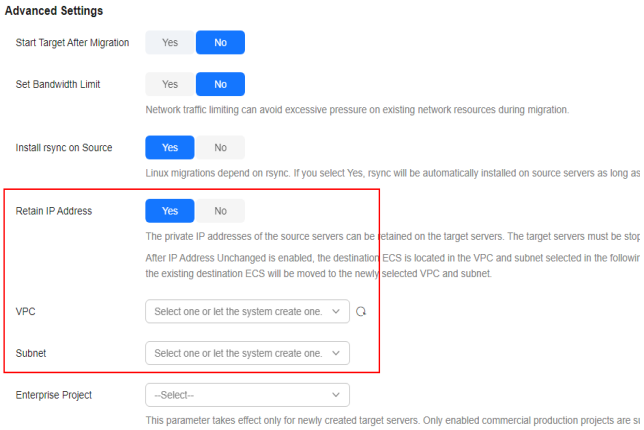
NOTICE

The configured VPC and subnet will not be applied for the target servers associated with source servers. Parameters in **Target Environment** are not required if all source servers in the selected application are associated with target servers.

7. In the **Advanced Settings** area, set **Retain IP Address** to **Yes**, read the on-screen warning and **disclaimer**, and click **Confirm**.

NOTE

Here only describes how to configure the **Retain IP Address** parameter. Set other parameters as required.



8. From the **VPC** drop-down list, select the VPC that contains the private network segment of the source servers. From the **Subnet** drop-down list, select the subnet that contains the private IP addresses of the source servers. After you select a subnet, the system will check whether the selected subnet

contains the source servers' private IP addresses. If it does not, you need to change the subnet.

9. Click **Next: Confirm**.
10. Confirm the workflow settings and click **Confirm**. The **Run Workflow** dialog box is displayed, which indicates that the workflow has been created.
    - If you want to start the migration immediately, click **Confirm** to run the workflow.
    - If you want to **add a stage or step** to the workflow, click **Cancel**. The workflow enters a **Waiting** state, and the migration has not started. To start the migration, click **Run** in the **Operation** column.
11. On the migration workflow details page, view the workflow settings and the migration progress. After the step for starting the migration Agent is completed, a migration task is automatically created on the SMS console. For details about the server information mapping between MgC and SMS, see **What Are the Information Mappings Between MgC and SMS?**
    - Move the cursor to the migration progress bar. In the box that is displayed, view more migration details.
    - When the migration progress bar reaches a step that requires manual confirmation, move the cursor to the progress bar and click **Confirm** next to the step status in the displayed window, so that the subsequent migration steps can be executed.
    - When the workflow reaches the **ResizeDiskPartition** step, the system identifies whether disk capacity reduction has been performed on the target server.
      - If yes, go to **SMS console** and resize disks and partitions for the target server. For details, see the **Partition Resizing** parameter in **Configuring a Target Server**. After the adjustment is complete, go back to the MgC console and click **Confirm** next to the step status so that the workflow can continue.
      - If no, skip this step.
    - The **StartSynchronization** step is repeated before you verify your services on the target server.
    - When the progress bar reaches **Cutover**, the migration is complete. You need check whether your service systems are running properly on the target server. If they are, manually switch services to the target server. After the switchover is complete, click **Confirm** in the workflow. The system automatically performs the following steps **SourceClear** and **MigrationTaskClear**.

----End

Manual Rollback

If you do not want to retain the private IP addresses of the source servers or any problems happen, you can manually switch the VPC for rollback. For details, see **Changing a VPC**.

2.8 Batch Modifying and Restoring the Host Configurations for Linux Source Servers

2.8.1 Overview

Background

When you migrate a Linux source server, you need to ensure that the source server can identify and resolve the interface domain names of related cloud services. This usually involves editing the **hosts** file on the source server. If there are a large number of servers to be migrated, manual editing is time-consuming. To simplify this process, we provide example scripts for batch editing. You can use the scripts to quickly push the mappings between domain names and IP addresses to the **hosts** file on all source servers in batches.

Script Description

The scripts are developed using the Shell language and can run only on Linux. They are used to batch update and restore the **/etc/hosts** file on Linux source servers.

To prevent long script execution, a maximum of 100 servers can be modified at a time.

The following table describes for what and where the scripts are used.

Script	Function	Scenario
update_hosts_linux.sh	Batch update the **/etc/hosts** file on Linux source servers. The script will automatically log operations, alert for any exceptions, and generate a summary of the operations.	Before migrating Linux source servers, run this script to update the **hosts** file for the servers.
rollback_hosts_linux.sh	Batch restore the **/etc/hosts** file on the Linux source servers. The script will automatically log operations, alert for any exceptions, and generate a summary of the operations.	After the Linux source servers are migrated, run this script to restore the **hosts** file on the source servers to the state before the migration.

2.8.2 Preparations

Preparing a CSV File

Create a CSV file and write the source server information in the following format to file. Ensure that the file can be accessed.

```
username,ip,port,password
```

- **username**: indicates the username for logging in to the source server. To ensure that the scripts have sufficient permissions to perform the modification, you need to run them as a user with administrator permissions, such as **root**.
- **ip**: indicates the private IP address of the source server.
- **port**: indicates the listening port of the SSH service. By default, port 22 is used on Linux. If the SSH service of the source server is running on another port, specify the port correctly.
- **password**: indicates the password for logging in to the source server. The scripts use this password to automatically connect to the source server through SSH.

CAUTION

- The first line in the CSV file is the title line and will not be parsed by the scripts.
- Each line in the CSV file contains the information for a single server, with each piece of information separated by a comma.
- Ensure the format is correct and the information is accurate, avoiding any extra spaces, commas, or invalid IP addresses.

For example:

```
username,ip,port,password
root,192.168.1.10,xx,examplePass123
root,192.168.1.11,xx,examplePass456
```

Preparing the Hosts File

Create a text file that contains the content to be added to the **/etc/hosts** file on the source servers. Ensure that the file can be accessed. Write the API domain names mappings for the related cloud services into the file, and start with **#Migration-proxy-start** and end with **#Migration-proxy-end**. The API domain name mappings of related cloud services depend on the actual environment. Contact the environment contact person of the corresponding site to obtain the mappings.

For example:

```
#Migration-proxy-start
xxx.xxx.xxx.xxx  iam.xxx.com
xxx.xxx.xxx.xxx  ecs.xxx.com
xxx.xxx.xxx.xxx  evs.xxx.com
xxx.xxx.xxx.xxx  ims.xxx.com
xxx.xxx.xxx.xxx  obs.xxx.com
xxx.xxx.xxx.xxx  eps.xxx.com
xxx.xxx.xxx.xxx  vpc.xxx.com
#Migration-proxy-end
```


Preparing a Log Directory

- **Configure a log directory**. The scripts use **/var/log/update_hosts** as the default log storage directory. If the directory cannot be found, the scripts automatically create it. To change the log storage directory, change the value of **LOG_DIR** in the script.
- **Check the permissions for the log directory**. Ensure that the current user has the write permission for the log directory. If the permissions are insufficient, modify the directory permissions or use another directory.

Checking the Connectivity of the Source Servers

- **Check the network connection**. Ensure that the server where the scripts are executed can access all source servers over the network.
- **Check whether the SSH port is reachable**. Ensure that the SSH port (22 by default) on the source servers is reachable from the server where the scripts are executed.

Checking the SSH Configuration

- **Configure the SSH service**. Ensure that the SSH service has been enabled and is running properly on all source servers. The SSH service is enabled by default on most Linux distributions.
- **Enable SSH password authentication**. Ensure that the SSH service on all source servers is configured to accept password authentication so that the scripts can use the password provided in the CSV file for automatic login.

Configuring the Script Executor

Ensure that the following tools and commands are installed on the Linux server where the scripts are executed:

- SSH: used to establish secure connections to remote source servers.
- sed: used to edit and modify the **/etc/hosts** file.
- setsid: used to avoid interaction during SSH connections, typically to prevent prompts during password input.
- mktemp: used to create temporary files or directories.

Configuring the Execution and User Permissions

- **Configure user permissions**. Ensure that the user who executes the scripts has the read and write permissions for the log directory, CSV file, and **hosts** file.
- **Assign execute permission to the scripts**. Ensure that the **update_hosts_linux.sh** and **rollback_hosts_linux.sh** scripts are executable. Run the **chmod +x update_hosts_linux.sh** and **chmod +x rollback_hosts_linux.sh** commands to add the execute permission to the scripts.

2.8.3 Configuring the Scripts

2.8.3.1 Configuring the update_hosts_linux.sh Script

Modify the configuration in the example script to meet you specific requirements.

Prerequisites

You have completed all **preparations**.

Procedure

Step 1 Create a file named **update_hosts_linux.sh** on the server where the script is executed, and copy the following script content to the file. If you have connected to the Linux source servers through SSH, you can directly use Vim to create and edit a script file. The procedure is as follows:

1. In the Vim editor, press **I** to enter insert mode.
2. Copy and paste the following script code and press **Esc**.
3. Run **:wq** to save and exit.

```
#!/bin/bash

# Configuration
# Log directory path: Used to store run logs, error logs, and summary logs.
# If the directory doesn't exist, the script will create it automatically.
LOG_DIR="/var/log/update_hosts"

# Run log file path: Records detailed information about the script's execution.
RUN_LOG="$LOG_DIR/run.log"

# Error log file path: Records any errors that occur during the script's execution.
ERROR_LOG="$LOG_DIR/error.log"

# Summary log file path: Records a summary of the script's execution, including the number of successful and failed servers.
SUMMARY_LOG="$LOG_DIR/summary.log"

# CSV file path: Contains information about the target hosts (must be manually created and configured).
CSV_FILE="target_servers.csv"

# Hosts content file path: Contains the content to be appended to each target host's /etc/hosts file (must be manually created and configured).
HOSTS_FILE="hosts_content.txt"
DEFAULT_PORT=22
SSH_TIMEOUT=10

# Initialize log directory and files
initialize_logs() {
    mkdir -p "$LOG_DIR"
    echo "========================================" >> "$RUN_LOG"
    echo "[INFO] $(date '+%Y-%m-%d %H:%M:%S') - Starting new update execution" >> "$RUN_LOG"
    echo "========================================" >> "$RUN_LOG"

    echo "========================================" >> "$ERROR_LOG"
    echo "[INFO] $(date '+%Y-%m-%d %H:%M:%S') - Starting new update execution" >> "$ERROR_LOG"
    echo "========================================" >> "$ERROR_LOG"

    echo "========================================" > "$SUMMARY_LOG"
    echo "[INFO] $(date '+%Y-%m-%d %H:%M:%S') - Starting new update execution" >> "$SUMMARY_LOG"
    echo "========================================" >> "$SUMMARY_LOG"
}

# Log info function
log_info() {
    echo "[INFO] $(date '+%Y-%m-%d %H:%M:%S') - $1" | tee -a "$RUN_LOG"
```

```
}

# Log error function
log_error() {
    echo "[ERROR] $(date '+%Y-%m-%d %H:%M:%S') - $1" | tee -a "$RUN_LOG" "$ERROR_LOG"
}

# Read server information from CSV file
read_servers_from_csv() {
    local csv_file="$1"
    local servers=()
    local header_skipped=false

    if [ ! -f "$csv_file" ]; then
        log_error "CSV file '$csv_file' not found."
        exit 1
    fi

    # Ensure file ends with a newline character
    sed -i -e '$a\' "$csv_file"

    while IFS=, read -r username ip port password; do
        # Skip header row
        if [ "$header_skipped" = false ]; then
            header_skipped=true
            continue
        fi
        # Skip empty and invalid rows
        if [[ -z "$username" || -z "$ip" ]]; then
            continue
        fi
        port=${port:-$DEFAULT_PORT} # Use default port 22
        # Ensure port is numeric
        if ! [[ "$port" =~ ^[0-9]+$ ]]; then
            log_error "Invalid port '$port' for $username@$ip. Skipping this server."
            continue
        fi
        servers+=("$username@$ip:$port:$password")
    done < "$csv_file"

    echo "${servers[@]}"
}

# Read hosts content from TXT file
read_hosts_content_from_txt() {
    local txt_file="$1"
    if [ -f "$txt_file" ]; then
        cat "$txt_file"
    else
        log_error "Hosts content file '$txt_file' not found."
        exit 1
    fi
}

# Initialize log files
initialize_logs

# Read server information from CSV file
servers=($(read_servers_from_csv "$CSV_FILE"))

# Read hosts content from TXT file
hosts_content=$(read_hosts_content_from_txt "$HOSTS_FILE")

# Counters for success and failure
success_count=0
failure_count=0
failed_servers=()

# Iterate over each server and push hosts content
```



```
for server in "${servers[@]}"; do
  # Extract user, IP, port, and password information
  IFS=':' read -r user_host port pass <<< "$server"
  IFS='@' read -r user ip <<< "$user_host"

  log_info "Starting update for $user@$ip:$port"

  # Create temporary script and SSH_ASKPASS script
  tmp_script=$(mktemp)
  askpass_script=$(mktemp)

  cat <<EOF > "$tmp_script"
#!/bin/bash
# Backup hosts file
if [ ! -f /etc/hosts.bak ]; then
  cp /etc/hosts /etc/hosts.bak
fi

# Remove old Migration-proxy section
sed -i '/#Migration-proxy-start/,/#Migration-proxy-end/d' /etc/hosts

# Append new Migration-proxy section
echo "$hosts_content" >> /etc/hosts
EOF

  cat <<EOF > "$askpass_script"
#!/bin/bash
echo "$pass"
EOF

  chmod +x "$tmp_script" "$askpass_script"

  # Set SSH_ASKPASS environment variable and use ssh to connect to the target machine and execute the
temporary script
  export SSH_ASKPASS="$askpass_script"
  export DISPLAY=:0

  ssh_output=$(mktemp)
  setsid ssh -o BatchMode=no -o ConnectTimeout=$SSH_TIMEOUT -o StrictHostKeyChecking=no -p "$port"
"$user@$ip" 'bash -s' < "$tmp_script" 2> "$ssh_output"
  ssh_status=$?

  if [ $ssh_status -eq 0 ]; then
    log_info "Updated hosts on $ip:$port successfully"
    ((success_count++))
  else
    ssh_error=$(cat "$ssh_output")
    case $ssh_status in
      1)
        log_error "General error occurred while updating hosts on $ip:$port: $ssh_error"
        ;;
      2)
        log_error "Misuse of shell builtins while updating hosts on $ip:$port: $ssh_error"
        ;;
      255)
        if [[ "$ssh_error" == *"Permission denied"* ]]; then
          log_error "SSH login failed for $user@$ip:$port: Permission denied (password may be incorrect or
username is wrong)"
        elif [[ "$ssh_error" == *"Connection refused"* ]]; then
          log_error "SSH login failed for $user@$ip:$port: Connection refused (port may be incorrect or SSH
service not running on target)"
        elif [[ "$ssh_error" == *"No route to host"* ]]; then
          log_error "SSH login failed for $user@$ip:$port: No route to host (network unreachable)"
        elif [[ "$ssh_error" == *"Host key verification failed"* ]]; then
          log_error "SSH login failed for $user@$ip:$port: Host key verification failed"
        elif [[ "$ssh_error" == *"Connection timed out"* ]]; then
          log_error "SSH login failed for $user@$ip:$port: Connection timed out"
        else
          log_error "SSH login failed for $user@$ip:$port: $ssh_error"
```



```
        fi
        ;;
      *)
        log_error "An unknown error occurred while updating hosts on $ip:$port: $ssh_error"
        ;;
    esac
    failed_servers+=("$user@$ip:$port")
    ((failure_count++))
  fi

  # Remove temporary scripts and SSH output file
  rm -f "$tmp_script" "$askpass_script" "$ssh_output"
done

# Calculate failure and success percentages
total_count=${#servers[@]}
failure_percentage=$(echo "scale=2; ($failure_count / $total_count) * 100" | bc)
success_percentage=$(echo "scale=2; ($success_count / $total_count) * 100" | bc)

# Output summary result and log to file
summary_content=$(cat <<EOF
========================================
[SUMMARY] $(date '+%Y-%m-%d %H:%M:%S') - Execution Update Summary
========================================
Total number of servers: $total_count
Number of successful updates: $success_count
Number of failed updates: $failure_count
Success rate: $success_percentage%
Failure rate: $failure_percentage%
----------------------------------------
EOF
)

if [ $failure_count -gt 0 ]; then
    summary_content+="Failed servers:\n"
    for server in "${failed_servers[@]}"; do
        summary_content+="  - $server\n"
    done
fi
summary_content+="========================================"

# Output summary result to log file and terminal
echo -e "$summary_content" | tee -a "$SUMMARY_LOG"

log_info "Script execution completed. Check $SUMMARY_LOG for summary."
```

Step 2 Modify the following parameters in the script to meet your needs:

- **LOG_DIR="/var/log/update_hosts"**
  - Description: log directory, which is used to store run, error, and summary logs.
  - Default value: **/var/log/update_hosts**
  - Suggestion: Change the value to a directory for which the current user has the write permission.
  - Example: **LOG_DIR="/home/username/update_hosts_logs"**
- **CSV_FILE="target_servers.csv"**
  - Description: **CSV file** path. The file contains the source server information.
  - Default value: **target_servers.csv**
  - Suggestion: Use an absolute path or a correct relative path.
  - Example: **CSV_FILE="/home/username/configs/servers.csv"**

- **HOSTS_FILE="hosts_content.txt"**
  - Description: **hosts** file path. The file contains the content to be added to the **/etc/hosts** file on the source servers.
  - Default value: **hosts_content.txt**
  - Suggestion: Use an absolute path or a correct relative path.
  - Example: **HOSTS_FILE="/home/username/configs/hosts_content.txt"**

Step 3 After the configuration items are modified and saved, run the script in a terminal window. If a GUI is available, press **Ctrl**+**Alt**+**T** to open the terminal.

```
./update_hosts_linux.sh
```

The script will output log information in the terminal window and generate a result report upon completion. You can view this report in the **summary.log** file in the directory specified by **LOG_DIR**.

----End

2.8.3.2 Configuring the rollback_hosts_linux.sh Script

Modify the configuration in the example script to meet your specific requirements.

Prerequisites

You have completed all **preparations**.

Procedure

Step 1 Create a file named **rollback_hosts_linux.sh** on the server where the script is executed, and copy the following script content to the file. If you have connected to the Linux source servers through SSH, you can directly use Vim to create and edit a script file. The procedure is as follows:

1. In the Vim editor, press **I** to enter insert mode.
2. Copy and paste the following script code and press **Esc**.
3. Run **:wq** to save and exit.

```
#!/bin/bash

# Configuration

# Log directory path: Used to store run logs, error logs, and summary logs.
# If the directory doesn't exist, the script will create it automatically.
LOG_DIR="/var/log/update_hosts"

# Run log file path: Records detailed information about the script's execution.
RUN_LOG="$LOG_DIR/run.log"

# Error log file path: Records any errors that occur during the script's execution.
ERROR_LOG="$LOG_DIR/error.log"

# Summary log file path: Records a summary of the script's execution, including the number of successful and failed servers.
SUMMARY_LOG="$LOG_DIR/summary.log"

# CSV file path: Contains information about the target hosts (must be manually created and configured).
CSV_FILE="target_servers.csv"
DEFAULT_PORT=22
SSH_TIMEOUT=10
```



```
# Initialize log directory and files
initialize_logs() {
    mkdir -p "$LOG_DIR"
    echo "========================================" >> "$RUN_LOG"
    echo "[INFO] $(date '+%Y-%m-%d %H:%M:%S') - Starting new rollback execution" >> "$RUN_LOG"
    echo "========================================" >> "$RUN_LOG"

    echo "========================================" >> "$ERROR_LOG"
    echo "[INFO] $(date '+%Y-%m-%d %H:%M:%S') - Starting new rollback execution" >> "$ERROR_LOG"
    echo "========================================" >> "$ERROR_LOG"

    echo "========================================" > "$SUMMARY_LOG"
    echo "[INFO] $(date '+%Y-%m-%d %H:%M:%S') - Starting new rollback execution" >>
"$SUMMARY_LOG"
    echo "========================================" >> "$SUMMARY_LOG"
}

# Log info function
log_info() {
    echo "[INFO] $(date '+%Y-%m-%d %H:%M:%S') - $1" | tee -a "$RUN_LOG"
}

# Log error function
log_error() {
    echo "[ERROR] $(date '+%Y-%m-%d %H:%M:%S') - $1" | tee -a "$RUN_LOG" "$ERROR_LOG"
}

# Read server information from CSV file
read_servers_from_csv() {
    local csv_file="$1"
    local servers=()
    local header_skipped=false

    if [ ! -f "$csv_file" ]; then
        log_error "CSV file '$csv_file' not found."
        exit 1
    fi

    # Ensure file ends with a newline character
    sed -i -e '$a\' "$csv_file"

    while IFS=, read -r username ip port password; do
        # Skip header row
        if [ "$header_skipped" = false ]; then
            header_skipped=true
            continue
        fi
        # Skip empty and invalid rows
        if [[ -z "$username" || -z "$ip" ]]; then
            continue
        fi
        port=${port:-$DEFAULT_PORT} # Use default port 22
        # Ensure port is numeric
        if ! [[ "$port" =~ ^[0-9]+$ ]]; then
            log_error "Invalid port '$port' for $username@$ip. Skipping this server."
            continue
        fi
        servers+=("$username@$ip:$port:$password")
    done < "$csv_file"

    echo "${servers[@]}"
}

# Initialize log files
initialize_logs

# Read server information from CSV file
servers=($(read_servers_from_csv "$CSV_FILE"))
```



```
# Counters for success and failure
success_count=0
failure_count=0
failed_servers=()

# Iterate over each server and execute rollback
for server in "${servers[@]}"; do
  # Extract user, IP, port, and password information
  IFS=':' read -r user_host port pass <<< "$server"
  IFS='@' read -r user ip <<< "$user_host"

  log_info "Starting rollback for $user@$ip:$port"

  # Create temporary script and SSH_ASKPASS script
  tmp_script=$(mktemp)
  askpass_script=$(mktemp)

  cat <<EOF > "$tmp_script"
#!/bin/bash
# Backup hosts file
if [ ! -f /etc/hosts.bak ]; then
  cp /etc/hosts /etc/hosts.bak
fi

# Remove old Migration-proxy section
sed -i '/#Migration-proxy-start/,/#Migration-proxy-end/d' /etc/hosts
EOF

  cat <<EOF > "$askpass_script"
#!/bin/bash
echo "$pass"
EOF

  chmod +x "$tmp_script" "$askpass_script"

  # Set SSH_ASKPASS environment variable and use ssh to connect to the target machine and execute the
temporary script
  export SSH_ASKPASS="$askpass_script"
  export DISPLAY=:0

  ssh_output=$(mktemp)
  setsid ssh -o BatchMode=no -o ConnectTimeout=$SSH_TIMEOUT -o StrictHostKeyChecking=no -p "$port"
"$user@$ip" 'bash -s' < "$tmp_script" 2> "$ssh_output"
  ssh_status=$?

  if [ $ssh_status -eq 0 ]; then
    log_info "Rolled back hosts on $ip:$port successfully"
    ((success_count++))
  else
    ssh_error=$(cat "$ssh_output")
    case $ssh_status in
      1)
        log_error "General error occurred while rolling back hosts on $ip:$port: $ssh_error"
        ;;
      2)
        log_error "Misuse of shell builtins while rolling back hosts on $ip:$port: $ssh_error"
        ;;
      255)
        if [[ "$ssh_error" == *"Permission denied"* ]]; then
          log_error "SSH login failed for $user@$ip:$port: Permission denied (password may be incorrect or
username is wrong)"
        elif [[ "$ssh_error" == *"Connection refused"* ]]; then
          log_error "SSH login failed for $user@$ip:$port: Connection refused (port may be incorrect or SSH
service not running on target)"
        elif [[ "$ssh_error" == *"No route to host"* ]]; then
          log_error "SSH login failed for $user@$ip:$port: No route to host (network unreachable)"
        elif [[ "$ssh_error" == *"Host key verification failed"* ]]; then
          log_error "SSH login failed for $user@$ip:$port: Host key verification failed"
        elif [[ "$ssh_error" == *"Connection timed out"* ]]; then
```



```
        log_error "SSH login failed for $user@$ip:$port: Connection timed out"
      else
        log_error "SSH login failed for $user@$ip:$port: $ssh_error"
      fi
      ;;
    *)
      log_error "An unknown error occurred while rolling back hosts on $ip:$port: $ssh_error"
      ;;
  esac
  failed_servers+=("$user@$ip:$port")
  ((failure_count++))
 fi

 # Remove temporary scripts and SSH output file
 rm -f "$tmp_script" "$askpass_script" "$ssh_output"
done

# Calculate failure and success percentages
total_count=${#servers[@]}
failure_percentage=$(echo "scale=2; ($failure_count / $total_count) * 100" | bc)
success_percentage=$(echo "scale=2; ($success_count / $total_count) * 100" | bc)

# Output summary result and log to file
summary_content=$(cat <<EOF
========================================
[SUMMARY] $(date '+%Y-%m-%d %H:%M:%S') - Execution Rollback Summary
========================================
Total number of servers: $total_count
Number of successful rollbacks: $success_count
Number of failed rollbacks: $failure_count
Success rate: $success_percentage%
Failure rate: $failure_percentage%
----------------------------------------
EOF
)

if [ $failure_count -gt 0 ]; then
    summary_content+="Failed servers:\n"
    for server in "${failed_servers[@]}"; do
        summary_content+="  - $server\n"
    done
fi
summary_content+="========================================"

# Output summary result to log file and terminal
echo -e "$summary_content" | tee -a "$SUMMARY_LOG"

log_info "Script execution completed. Check $SUMMARY_LOG for summary."
```

Step 2 Modify the following parameters in the script to meet your needs:

- **LOG_DIR="/var/log/rollback_hosts"**
  - Description: log directory
  - Default value: **/var/log/rollback_hosts**
  - **Suggestion**: Change the value to a directory for which the current user has the write permission.
  - Example: **LOG_DIR="/home/username/rollback_hosts_logs"**
- **CSV_FILE="target_servers.csv"**
  - Description: CSV file path. The file contains the source server information.
  - Default value: **target_servers.csv**
  - Suggestion: Use an absolute path or a correct relative path.
  - Example: **CSV_FILE="/home/username/configs/servers.csv"**

Step 3 Saving the changes. Run the script in a terminal window. If a GUI is available, press **Ctrl**+**Alt**+**T** to open the terminal.

```
./rollback_hosts_linux.sh
```

The script will output log information in the terminal window and generate a result report upon completion. You can view this report in the **summary.log** file in the directory specified by **LOG_DIR**.

----End

2.9 Batch Modifying and Restoring the Host Configurations for Windows Source Servers

2.9.1 Overview

Background

When you migrate a Windows source server, you need to ensure that the source server can resolve the interface domain names of related cloud services. This usually involves editing the **hosts** file on the source server. If there are a large number of servers to be migrated, manual editing is time-consuming. To simplify this process, we provide example scripts for batch editing. You can use the scripts to quickly write the mappings between domain names and IP addresses to the **hosts** file on all source servers in batches.

Script Description

The scripts are developed using the PowerShell language and can run only on Windows. They are used to batch update and restore the **/etc/hosts** file on Windows source servers. The path of the **hosts** file is **C:\Windows\System32\drivers\etc\hosts**.

To prevent long script execution, a maximum of 100 servers can be modified at a time.

The following table describes for what and where the scripts are used.

Script	Description	Scenario
update_hosts_win.ps1	Batch update the **hosts** file on Windows source servers. The script will automatically log operations, alert for any exceptions, and generate a summary of the operations.	Before migrating Windows source servers, run this script to update the **hosts** file for the servers.

Script	Description	Scenario
rollback_hosts_win.ps1	Batch restore the **hosts** file on Windows source servers. The script will automatically log operations, alert for any exceptions, and generate a summary of the operations.	After the Windows source servers are migrated, run this script to restore the **hosts** file on these servers to the state before the migration.

PowerShell Version and Dependency Requirements

PowerShell remoting uses WinRM, which provided by the Windows Management Framework (WMF).

To run remote sessions on PowerShell, the local and remote computers must have the following:

- Windows PowerShell 3.0 or later (WMF 5.1 is recommended.)
- Microsoft .NET Framework 4.0 or later
- WinRM 3.0 or later

To run remote sessions on Windows PowerShell 2.0, the local and remote computers must have the following:

- Windows PowerShell 2.0 or later
- Microsoft .NET Framework 2.0 or later
- WinRM 2.0

Features that run only on Windows PowerShell 3.0 or higher, such as the ability to disconnect and reconnect to sessions, are only available when both computers are running Windows PowerShell 3.0 or higher.

Run the following command to check the PowerShell version:

```
$PSVersionTable
```

2.9.2 Preparations

Configuring a PowerShell Execution Policy

Check the execution policy and ensure that PowerShell allows script execution. Open PowerShell and run the following command to check the current execution policy:

```
Get-ExecutionPolicy
```

The PowerShell execution policies are as follows:

- Restricted: No script can be executed.
- AllSigned: Only scripts signed by trusted publishers can be run.
- RemoteSigned: Locally created scripts can be run without signatures, but remotely downloaded scripts must be signed.

- Unrestricted: All scripts can be executed, but a warning is generated when a script downloaded from the Internet is executed.
- Bypass: Nothing is blocked and there are no warnings or prompts.

If the execution policy is **Restricted** or **AllSigned**, run the following command to temporarily change the policy to allow the execution of locally created scripts and signed remote scripts:

```
Set-ExecutionPolicy RemoteSigned -Scope Process
```

This command changes the execution policy only in the current PowerShell session and restores the default policy after the session ends.

Preparing a CSV File

Create a CSV file and write the source server information in the following format to file. Ensure that the file can be accessed.

```
username,ip,port,password
```

- **username**: indicates the username for logging in to the source server. To ensure that the script has sufficient permissions to perform the modification, you need to run it as a user with administrator permissions, such as **Administrator**.
- **ip**: indicates the private IP address of the source server.
- **port**: listening port of the WinRM service. The default port is 5985.
- **password**: indicates the password for logging in to the source server. The scripts use this password to automatically connect to the source server through WinRM.

CAUTION

- The first row in the CSV file is the header row.
- Each line in the CSV file contains the information for a single server, with each piece of information separated by a comma.
- Ensure the format is correct and the information is accurate, avoiding any extra spaces, commas, or invalid IP addresses.

For example:

```
username,ip,port,password
Administrator,192.168.1.10,xx,examplePass123
Administrator,192.168.1.11,xx,examplePass456
```

Preparing the Hosts File

Create a text file that contains the content to be added to the **hosts** file on the source servers. Ensure that the file can be accessed. Write the API domain names mappings for the related cloud services into the file, and start with **#Migration-proxy-start** and end with **#Migration-proxy-end**. The API domain name mappings of related cloud services depend on the actual environment. Contact the environment contact person of the corresponding site to obtain the mappings.

For example:

```
#Migration-proxy-start
xxx.xxx.xxx.xxx  iam.xxx.com
```



```
xxx.xxx.xxx.xxx  ecs.xxx.com
xxx.xxx.xxx.xxx  evs.xxx.com
xxx.xxx.xxx.xxx  ims.xxx.com
xxx.xxx.xxx.xxx  obs.xxx.com
xxx.xxx.xxx.xxx  eps.xxx.com
xxx.xxx.xxx.xxx  vpc.xxx.com
#Migration-proxy-end
```

Preparing a Log Directory

- **Configure the log directory**. The scripts use **C:\Users\Public\Hosts_Script_Logs** as the default log storage directory. If the directory cannot be found, the scripts automatically create it. To change the log storage directory, change the value of **$logDir** in the script.
- **Check the permissions for the log directory**. Ensure that the current user has the write permission for the log directory. If the permissions are insufficient, modify the directory permissions or use another directory.

Checking the Network Connectivity

- **Check the network connection**. Ensure that the server where the scripts are executed can access the IP addresses and ports of all Windows source servers over the network. The script executor must be able to access all Windows source servers over port 5985.
- **Configure the firewalls**. Check and configure the firewalls on the local computer and source servers to ensure that remote PowerShell sessions can be established through WinRM.
- **Enable the WinRM service**. Ensure that the WinRM service has been enabled and is running properly on all Windows source servers. You can run the following command on the source servers to enable WinRM:

  ```
  Enable-PSRemoting -Force
  ```

2.9.3 Example Scripts

2.9.3.1 Configuring the update_hosts_win.ps1 Script

Modify the configuration in the example script to meet you specific requirements.

Prerequisites

You have completed all **preparations**.

Procedure

Step 1 Create a file named **update_hosts_lwin.ps1** on the server where the script is executed, and copy the following script content to the file.

```
# Configuration
# Path to the CSV file with server information. Must exist before running the script.
$csvFile = "C:\Users\Public\target_servers.csv"  # Manually configure

# Path to the hosts content file. Must exist before running the script.
$hostsFile = "C:\Users\Public\hosts_content.txt"  # Manually configure

# Directory for storing log files. Will be created if it doesn't exist.
$logDir = "C:\Users\Public\Hosts_Script_Logs"  # Automatically created
```



```
# Log file for general run information.
$runLog = Join-Path $logDir "run.log"  # Automatically created

# Log file for error messages.
$errorLog = Join-Path $logDir "error.log"  # Automatically created

# Log file for summary information.
$summaryLog = Join-Path $logDir "summary.log"  # Automatically created


# Initialize log directory and files
function Initialize-Logs {
    if (-not (Test-Path $logDir)) {
        New-Item -Path $logDir -ItemType Directory
    }
    Add-Content -Path $runLog -Value "========================================="
    Add-Content -Path $runLog -Value "[INFO] $(Get-Date -Format 'yyyy-MM-dd HH:mm:ss') - Starting new
update execution"
    Add-Content -Path $runLog -Value "========================================="

    Add-Content -Path $errorLog -Value "========================================="
    Add-Content -Path $errorLog -Value "[INFO] $(Get-Date -Format 'yyyy-MM-dd HH:mm:ss') - Starting
new update execution"
    Add-Content -Path $errorLog -Value "========================================="

    Add-Content -Path $summaryLog -Value "========================================="
    Add-Content -Path $summaryLog -Value "[INFO] $(Get-Date -Format 'yyyy-MM-dd HH:mm:ss') -
Starting new update execution"
    Add-Content -Path $summaryLog -Value "========================================="
}

# Log info function
function Log-Info {
    param (
        [string]$message
    )
    $logMessage = "[INFO] $(Get-Date -Format 'yyyy-MM-dd HH:mm:ss') - $message"
    Add-Content -Path $runLog -Value $logMessage
    Write-Output $logMessage
}

# Log error function
function Log-Error {
    param (
        [string]$message
    )
    $logMessage = "[ERROR] $(Get-Date -Format 'yyyy-MM-dd HH:mm:ss') - $message"
    Add-Content -Path $runLog -Value $logMessage
    Add-Content -Path $errorLog -Value $logMessage
    Write-Output $logMessage
}

# Read server information from CSV file
function Read-ServersFromCSV {
    param (
        [string]$csvFile
    )
    if (-not (Test-Path $csvFile)) {
        Log-Error "CSV file '$csvFile' not found."
        exit 1
    }
    return Import-Csv -Path $csvFile
}

# Read hosts content from TXT file
function Read-HostsContentFromTXT {
    param (
        [string]$hostsFile
    )
```



```
    if (-not (Test-Path $hostsFile)) {
        Log-Error "Hosts content file '$hostsFile' not found."
        exit 1
    }
    return Get-Content -Path $hostsFile -Raw
}

# Add to TrustedHosts
function Add-ToTrustedHosts {
    param (
        [string]$ip
    )
    # Check current TrustedHosts list
    $trustedHostsPath = "WSMan:\localhost\Client\TrustedHosts"
    $trustedHosts = (Get-Item $trustedHostsPath).Value

    if ($trustedHosts -eq $null -or $trustedHosts -eq "") {
        # Set the initial trusted host
        Set-Item $trustedHostsPath -Value $ip -Force
        Log-Info "Set initial TrustedHosts value to $ip"
    } elseif ($trustedHosts -notlike "*$ip*") {
        # Add new IP to TrustedHosts if not already present
        $updatedTrustedHosts = if ($trustedHosts -eq "*") { $ip } else { "$trustedHosts,$ip" }
        try {
            Set-Item $trustedHostsPath -Value $updatedTrustedHosts -Force
            Log-Info "Added $ip to TrustedHosts"
        } catch {
            Log-Error "Failed to add $ip to TrustedHosts: $_"
        }
    } else {
        Write-Host "TrustedHosts list already contains IP $ip."
    }
}

# Initialize log files
Initialize-Logs

# Verify CSV file
if (-not (Test-Path $csvFile)) {
    Log-Error "CSV file '$csvFile' not found."
    exit 1
}

# Verify hosts file
if (-not (Test-Path $hostsFile)) {
    Log-Error "Hosts content file '$hostsFile' not found."
    exit 1
}

# Read server information from CSV file
$servers = Read-ServersFromCSV -csvFile $csvFile

# Read hosts content from TXT file
$hostsContent = Read-HostsContentFromTXT -hostsFile $hostsFile

# Counters for success and failure
$successCount = 0
$failureCount = 0
$failedServers = @()

# Remote script block
$remoteScriptBlock = {
    param (
        [string]$hostsContent
    )
    $hostsFilePath = 'C:\Windows\System32\drivers\etc\hosts'

    # Read the file content
    $content = Get-Content -Path $hostsFilePath
```



```
    # Initialize flag
    $inBlock = $false
    $newContent = @()

    # Traverse file content
    foreach ($line in $content) {
        if ($line -match '#Migration-proxy-start') {
            $inBlock = $true
        }
        if (-not $inBlock) {
            $newContent += $line
        }
        if ($line -match '#Migration-proxy-end') {
            $inBlock = $false
            continue
        }
    }

    # Remove trailing empty lines
    while ($newContent[-1] -eq '') {
        $newContent = $newContent[0..($newContent.Count - 2)]
    }

    # Write the new content back to the file
    $newContent | Set-Content -Path $hostsFilePath

    # Append new Migration-proxy section
    Add-Content -Path $hostsFilePath -Value $hostsContent

    Write-Output 'Successfully updated hosts file on remote server.'
}

# Main script logic
Log-Info "Script execution started."

foreach ($server in $servers) {
    $username = $server.username
    $ip = $server.ip
    $password = $server.password

    if (-not $username -or -not ${ip} -or -not $password) {
        Log-Error "Invalid server entry: $username, ${ip}, $password. Skipping."
        continue
    }

    Log-Info "Starting update for $username@${ip}"

    $securePassword = ConvertTo-SecureString $password -AsPlainText -Force
    $credential = New-Object System.Management.Automation.PSCredential ($username, $securePassword)

    Add-ToTrustedHosts -ip $ip

    try {
        $session = New-PSSession -ComputerName ${ip} -Credential $credential -ErrorAction Stop

        Invoke-Command -Session $session -ScriptBlock $remoteScriptBlock -ArgumentList $hostsContent

        Remove-PSSession -Session $session
        Log-Info "Updated hosts on ${ip} successfully"
        $successCount++
    }
    catch {
        Log-Error "Failed to update hosts on ${ip}: $_"
        $failedServers += "$username@${ip}"
        $failureCount++
    }
}
```



```
# Calculate failure and success percentages
$totalCount = $servers.Count
if ($totalCount -gt 0) {
    $failurePercentage = [math]::Round(($failureCount / $totalCount) * 100, 2)
    $successPercentage = [math]::Round(($successCount / $totalCount) * 100, 2)
} else {
    $failurePercentage = 0
    $successPercentage = 100
}

# Output summary result and log to file
$summaryContent = @"
========================================
[SUMMARY] $(Get-Date -Format 'yyyy-MM-dd HH:mm:ss') - Execution Update Summary
========================================
Total number of servers: $totalCount
Number of successful updates: $successCount
Number of failed updates: $failureCount
Success rate: $successPercentage%
Failure rate: $failurePercentage%
----------------------------------------
"@

if ($failedServers.Count -gt 0) {
    $summaryContent += "Failed servers:`n"
    foreach ($server in $failedServers) {
        $summaryContent += "  - $server`n"
    }
}
$summaryContent += "========================================="

# Output summary result to log file and terminal
$summaryContent | Add-Content -Path $summaryLog
Write-Output $summaryContent
Log-Info "Script execution completed. Check $summaryLog for summary."
```

Step 2 Modify the following parameters in the script to meet your needs:

- **$logDir = "C:\Users\Public\Hosts_Script_Logs"**
  - Description: log directory, which is used to store run, error, and summary logs.
  - Default value: **C:\Users\Public\Hosts_Script_Logs**
  - Suggestion: Change the value to a directory for which the current user has the write permission.
  - Example: **$logDir ="C:\Users\username\Documents\Hosts_Script_Logs"**
- **$csvFile = "C:\Users\Public\target_servers.csv"**
  - Description: **CSV file** path. The file contains the source server information.
  - Default value: **C:\Users\Public\target_servers.csv**
  - Suggestion: Use an absolute path or a correct relative path. If the CSV file path changes, you need to update the path here.
  - Example: **$csvFile = "C:\Users\username\Documents\servers.csv"**
- **$hostsFile = "C:\Users\Public\hosts_content.txt"**
  - Description: **hosts** file path. The file contains the content to be added to the **hosts** file on the source servers.
  - Default value: **C:\Users\Public\hosts_content.txt**
  - Suggestion: Use an absolute path or a correct relative path.
  - Example: **$hostsFile = "C:\Users\username\Documents \hosts_content.txt"**

Step 3 After the configuration items are modified and saved, run PowerShell as administrator and execute the script.

```
.\update_hosts_win.ps1
```

The script will output log information in the terminal window and generate a result report upon completion. You can view this report in the **summary.log** file in the directory specified by **$logDir**.

----End

2.9.3.2 Configuring the rollback_hosts_win.ps1 Script

Modify the configuration in the example script to meet you specific requirements.

Prerequisites

You have completed all **preparations**.

Procedure

Step 1 Create a file named **rollback_hosts_win.ps1** on the server where the script is executed, and copy the following script content to the file.

```
# Configuration
# Path to the CSV file with server information. Must exist before running the script.
$csvFile = "C:\Users\Public\target_servers.csv"  # Manually configure

# Directory for storing log files. Will be created if it doesn't exist.
$logDir = "C:\Users\Public\Hosts_Script_Logs"  # Automatically created

# Log file for general run information.
$runLog = Join-Path $logDir "run.log"  # Automatically created

# Log file for error messages.
$errorLog = Join-Path $logDir "error.log"  # Automatically created

# Log file for summary information.
$summaryLog = Join-Path $logDir "summary.log"  # Automatically created


# Initialize log directory and files
function Initialize-Logs {
    if (-not (Test-Path $logDir)) {
        New-Item -Path $logDir -ItemType Directory
    }
    Add-Content -Path $runLog -Value "========================================="
    Add-Content -Path $runLog -Value "[INFO] $(Get-Date -Format 'yyyy-MM-dd HH:mm:ss') - Starting new
restore execution"
    Add-Content -Path $runLog -Value "========================================="

    Add-Content -Path $errorLog -Value "========================================="
    Add-Content -Path $errorLog -Value "[INFO] $(Get-Date -Format 'yyyy-MM-dd HH:mm:ss') - Starting
new restore execution"
    Add-Content -Path $errorLog -Value "========================================="

    Add-Content -Path $summaryLog -Value "========================================="
    Add-Content -Path $summaryLog -Value "[INFO] $(Get-Date -Format 'yyyy-MM-dd HH:mm:ss') -
Starting new restore execution"
    Add-Content -Path $summaryLog -Value "========================================="
}

# Log info function
function Log-Info {
    param (
```



```
        [string]$message
    )
    $logMessage = "[INFO] $(Get-Date -Format 'yyyy-MM-dd HH:mm:ss') - $message"
    Add-Content -Path $runLog -Value $logMessage
    Write-Output $logMessage
}

# Log error function
function Log-Error {
    param (
        [string]$message
    )
    $logMessage = "[ERROR] $(Get-Date -Format 'yyyy-MM-dd HH:mm:ss') - $message"
    Add-Content -Path $runLog -Value $logMessage
    Add-Content -Path $errorLog -Value $logMessage
    Write-Output $logMessage
}

# Read server information from CSV file
function Read-ServersFromCSV {
    param (
        [string]$csvFile
    )
    if (-not (Test-Path $csvFile)) {
        Log-Error "CSV file '$csvFile' not found."
        exit 1
    }
    return Import-Csv -Path $csvFile
}

# Add to TrustedHosts
function Add-ToTrustedHosts {
    param (
        [string]$ip
    )
    # Check current TrustedHosts list
    $trustedHostsPath = "WSMan:\localhost\Client\TrustedHosts"
    $trustedHosts = (Get-Item $trustedHostsPath).Value

    if ($trustedHosts -eq $null -or $trustedHosts -eq "") {
        # Set the initial trusted host
        Set-Item $trustedHostsPath -Value $ip -Force
        Log-Info "Set initial TrustedHosts value to $ip"
    } elseif ($trustedHosts -notlike "*$ip*") {
        # Add new IP to TrustedHosts if not already present
        $updatedTrustedHosts = if ($trustedHosts -eq "*") { $ip } else { "$trustedHosts,$ip" }
        try {
            Set-Item $trustedHostsPath -Value $updatedTrustedHosts -Force
            Log-Info "Added $ip to TrustedHosts"
        } catch {
            Log-Error "Failed to add $ip to TrustedHosts: $_"
        }
    } else {
        Write-Host "TrustedHosts list already contains IP $ip."
    }
}

# Initialize log files
Initialize-Logs

# Verify CSV file
if (-not (Test-Path $csvFile)) {
    Log-Error "CSV file '$csvFile' not found."
    exit 1
}

# Read server information from CSV file
$servers = Read-ServersFromCSV -csvFile $csvFile
```



```
# Counters for success and failure
$successCount = 0
$failureCount = 0
$failedServers = @()

# Remote script block
$remoteScriptBlock = {
    param ()

    $hostsFilePath = 'C:\Windows\System32\drivers\etc\hosts'

    # Read the file content
    $content = Get-Content -Path $hostsFilePath

    # Initialize flag
    $inBlock = $false
    $newContent = @()

    # Traverse file content
    foreach ($line in $content) {
        if ($line -match '#Migration-proxy-start') {
            $inBlock = $true
        }
        if (-not $inBlock) {
            $newContent += $line
        }
        if ($line -match '#Migration-proxy-end') {
            $inBlock = $false
            continue
        }
    }

    # Remove trailing empty lines
    while ($newContent[-1] -eq '') {
        $newContent = $newContent[0..($newContent.Count - 2)]
    }

    # Write the new content back to the file
    $newContent | Set-Content -Path $hostsFilePath

    Write-Output 'Successfully restored hosts file on remote server.'
}

# Main script logic
Log-Info "Script execution started."

foreach ($server in $servers) {
    $username = $server.username
    $ip = $server.ip
    $password = $server.password

    if (-not $username -or -not ${ip} -or -not $password) {
        Log-Error "Invalid server entry: $username, ${ip}, $password. Skipping."
        continue
    }

    Log-Info "Starting restore for $username@${ip}"

    $securePassword = ConvertTo-SecureString $password -AsPlainText -Force
    $credential = New-Object System.Management.Automation.PSCredential ($username, $securePassword)

    Add-ToTrustedHosts -ip $ip

    try {
        $session = New-PSSession -ComputerName ${ip} -Credential $credential -ErrorAction Stop

        Invoke-Command -Session $session -ScriptBlock $remoteScriptBlock

        Remove-PSSession -Session $session
```



```
        Log-Info "Restored hosts on ${ip} successfully"
        $successCount++
    }
    catch {
        Log-Error "Failed to restore hosts on ${ip}: $_"
        $failedServers += "$username@${ip}"
        $failureCount++
    }
}

# Calculate failure and success percentages
$totalCount = $servers.Count
if ($totalCount -gt 0) {
    $failurePercentage = [math]::Round(($failureCount / $totalCount) * 100, 2)
    $successPercentage = [math]::Round(($successCount / $totalCount) * 100, 2)
} else {
    $failurePercentage = 0
    $successPercentage = 100
}

# Output summary result and log to file
$summaryContent = @"
========================================
[SUMMARY] $(Get-Date -Format 'yyyy-MM-dd HH:mm:ss') - Execution Rollback Summary
========================================
Total number of servers: $totalCount
Number of successful restores: $successCount
Number of failed restores: $failureCount
Failure rate: $failurePercentage%
Success rate: $successPercentage%
----------------------------------------
"@

if ($failedServers.Count -gt 0) {
    $summaryContent += "Failed servers:`n"
    foreach ($server in $failedServers) {
        $summaryContent += "  - $server`n"
    }
}
$summaryContent += "========================================"

# Output summary result to log file and terminal
$summaryContent | Add-Content -Path $summaryLog
Write-Output $summaryContent
Log-Info "Script execution completed. Check $summaryLog for summary."
```

Step 2 Modify the following parameters in the script to meet your needs:

- **$logDir = "C:\Users\Public\Hosts_Script_Logs"**
  - Description: log directory, which is used to store run, error, and summary logs.
  - Default value: **C:\Users\Public\Hosts_Script_Logs**
  - Suggestion: Change the value to a directory for which the current user has the write permission.
  - Example: **$logDir ="C:\Users\username\Documents\Hosts_Script_Logs"**
- **$csvFile = "C:\Users\Public\target_servers.csv"**
  - Description: **CSV file** path. The file contains the source server information.
  - Default value: **C:\Users\Public\target_servers.csv**
  - Suggestion: Use an absolute path or a correct relative path. If the CSV file path changes, you need to update the path here.
  - Example: **$csvFile = "C:\Users\username\Documents\servers.csv"**

Step 3 After the configuration items are modified and saved, open the PowerShell window as the administrator and run the following command to execute the script:

```
.\rollback_hosts_win.ps1
```

The script will output log information in the terminal window and generate a result report upon completion. You can view this report in the **summary.log** file in the directory specified by **$logDir**.

----End

2.9.4 FAQs

2.9.4.1 How Do I Enable the PowerShell Remoting?

Generally, PowerShell remoting is enabled by default on Windows Server 2012 and later versions. If the settings are changed, you can perform the following steps to enable PowerShell remoting:

Step 1 Run PowerShell as administrator.

Step 2 Run the following command to enable PowerShell remoting:

```
Enable-PSRemoting
```

Step 3 Verify the configuration. Run the following command in PowerShell:

```
New-PSSession
```

- If the configuration is successful, the command creates a session on the local computer and returns a session object. Example output:

```
Id Name       ComputerName    State    ConfigurationName
-- ----       ------------    -----    -----
1  Session1    localhost       Opened   Microsoft.PowerShell
```

- If the configuration fails, refer to **about_Remote_Troubleshooting** in the PowerShell documentation for solutions.

----End

2.9.4.2 How Do I Enable the WinRM Service?

Step 1 Run PowerShell as administrator.

Step 2 Run the following command to automatically start the WinRM service and configure the remote access settings:

```
Enable-PSRemoting -Force
```

----End

2.9.4.3 What Can I If an Error Is Reported After a Script Is Executed, Indicating that the Remote Server Fails to Be Connected and the Login Credential Information Is Correct?

Symptom

After the script was executed, the error message "[ERROR] Failed to update hosts on xxx.xxx.x.xx: [xxx.xxx.x.xx] Failed to connect to the remote server xxx.xxx.x.xx. For details, see the about_Remote_Troubleshooting topic" was displayed.

Possible Causes

The WinRM service on the remote server is not started or is incorrectly configured.

Solution

Step 1 Check whether the executor can ping the remote server. If the ping operation succeeds, go to step 2.

Step 2 Check whether port 5985 used by the WinRM service on the remote server is open to the executor. If it is, go to step 3.

Step 3 Check whether the login credential of the remote server is correct. After confirming that the credential is correct, perform the following steps.

Step 4 Log in to the remote server that fails to be connected and run PowerShell as administrator.

Step 5 Run the following command to run the script again:

```
Enable-PSRemoting -Force
```

----End

3 Storage Migration

3.1 Migrating Data from Other Cloud Platforms to Huawei Cloud

Scenario

MgC allows you to quickly, easily migrate data to Huawei Cloud, from object storage to file storage, or from file storage to object storage. The choice is yours. This section describes how to use MgC to migrate data in object storage or file storage from other cloud platforms to Huawei Cloud.

The following regions are supported:

- LA-Santiago
- LA-Sao Paulo
- TR-Istanbul
- AP-Bangkok
- AP-Singapore
- AP-Jakarta
- ME-Riyadh
- CN North-Beijing4
- CN East-Shanghai1

Highlights

- Dedicated migration clusters reduce resource contention and improve migration efficiency.
- Supported are object and file storage services on popular cloud platforms and self-built network storage systems. Supported migration sources include:
  - Huawei Cloud OBS
  - Alibaba Cloud OSS
  - Baidu Cloud BOS

- Tencent Cloud COS
- Kingsoft Cloud KS3
- Qiniu Cloud KODO
- UCloud US3
- Amazon S3
- Azure Blob Storage
- NAS_GFS
- NAS_SMB
- NAS_NFS_V3_MOUNT
- NAS_NFS_V3_PROTOCOL
- HTTP/HTTPS data sources

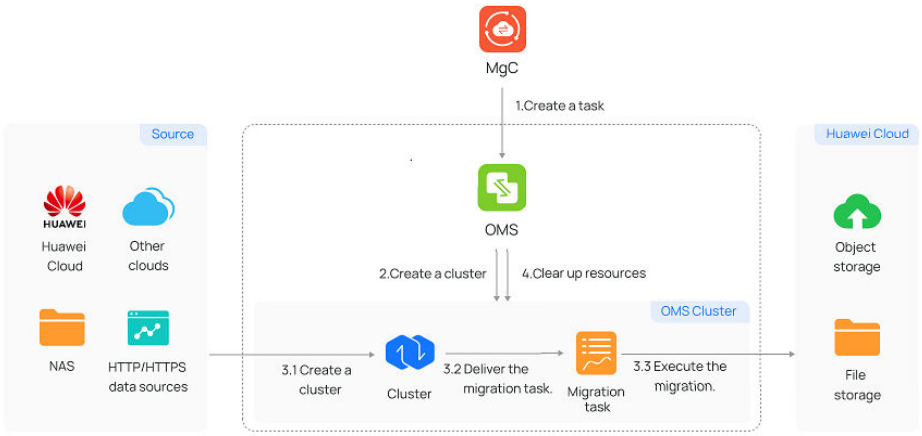
Notes and Constraints

- For more information, see **What Are the Restrictions on Using MgC for Storage Migration?**
- Data in the Deep Cold Archive storage of Alibaba Cloud OSS cannot be restored using the restoration function of MgC. You need to manually restore the data before migration.

Architecture

The figure shows the logical architecture of storage migrations using MgC.

Figure 3-1 Logical architecture of storage migration



Preparations

- Prepare a Huawei account or an IAM user that can access MgC. For details, see **Preparations**.
- **Create a migration project** on the MgC console.
- Ensure that the source and target accounts have the permissions required for the migration. For details, see **How Do I Obtain Required Permissions for the Source and Target Accounts?**

- (Optional) To migrate over a private line, connect the source and target VPCs or ensure the source storage service's private domain name or the source bucket's private domain name can be pinged from an ECS in the target VPC.

Step 1: Create an OBS Bucket or SFS File System

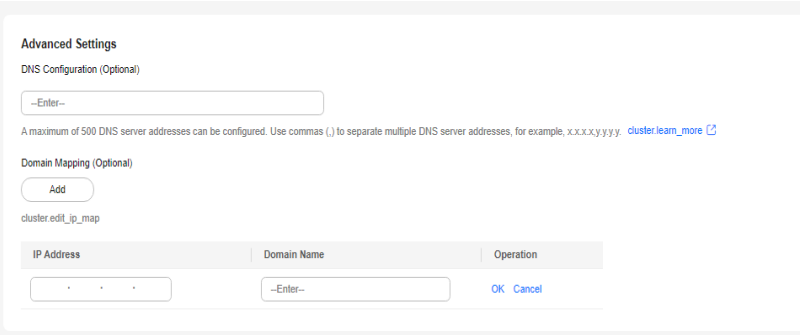
MgC supports migrations from object storage to file storage and from file storage to object storage. **Create an OBS bucket** or **create an SFS file system** on Huawei Cloud as needed.

Step 2: Create a Migration Cluster

You can create dedicated migration clusters to accelerate storage migration. A migration cluster consists of nodes that have the migration plugin installed and are used to execute migration and listing tasks. For details, see **Creating a Migration Cluster**.

To migrate over a private line, map the private IP address used by the private line to the domain names of the target storage service and the target storage resource, such as a bucket, in the advanced settings.

Figure 3-2 Advanced settings



Step 3: Create a Storage Migration Workflow

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

Step 2 In the navigation pane on the left, choose **Migrate** > **Workflows**. Select a **migration project** in the upper left corner of the page.

Step 3 Click **Create Workflow** in the upper right corner of the page.

Step 4 Select **Storage Migration** and click **Configure Workflow**. Click **Preview Steps** to view the migration stages and steps predefined in the template and the description of each stage and step. Steps of the **Automated** type will be automatically performed by MgC.

Step 5 Set workflow basics based on **Table 3-1**.

Figure 3-3 Basic information

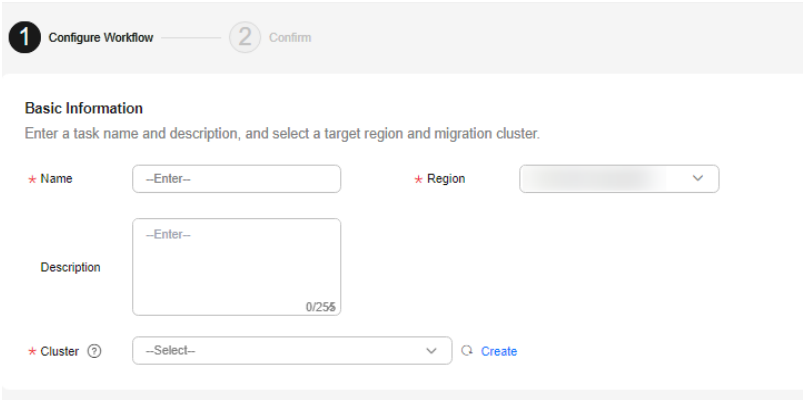


Table 3-1 Basic parameters

Parameter	Description
Name	Enter a workflow name.
Region	Select a region you are migrating to. The migration cluster you want to use must be in this region.
Description	Enter a description.
Cluster	Select the **migration cluster created in step 2**.

Step 6 Configure the migration source and target based on **Table 3-2** and **Table 3-3**.

Figure 3-4 Source and target information

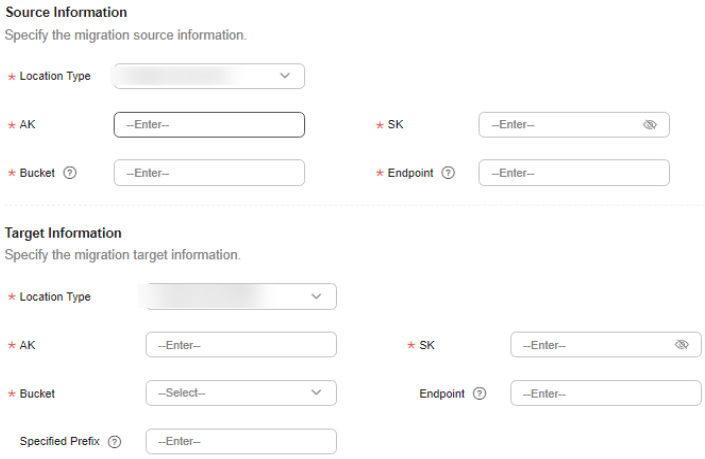


Table 3-2 Parameters for configuring a migration source

Parameter	Description	Remarks
Location Type	The supported migration sources include: • Huawei Cloud OBS • Alibaba Cloud OSS • Baidu Cloud BOS • Tencent Cloud COS • Kingsoft Cloud KS3 • Qiniu Cloud KODO • UCloud US3 • Amazon S3 • Azure Blob Storage • NAS_GFS • NAS_SMB • NAS_NFS_V3_MOUNT • NAS_NFS_V3_PROTOCOL • HTTP/HTTPS data source	-
AK and SK	Enter the AK/SK pair of the source cloud account. Ensure that the entered AK and SK are correct and you have the required permissions for the source bucket.	These parameters are available when cloud storage is selected for **Location Type**.
Bucket	Enter the name of the source bucket to be migrated.	
Endpoint	Enter the endpoint of the region where the source bucket is located.	
Type	Set this parameter based on the source bucket type. You can **view the bucket type in its basic information**.	This parameter is available when **Huawei Cloud OBS** is selected for **Location Type**.
APPID	Enter the APPID of your Tencent Cloud account. **NOTE** You can view the APPID on the account information page of the Tencent Cloud console.	This parameter is available when **Tencent Cloud COS** is selected for **Location Type**.

Parameter	Description	Remarks
Authentication Type	The following authentication types are supported: • Connection string • Storage account name and key For details about how to obtain the credentials, see **How Do I Obtain Credentials for Accessing Microsoft Azure?**	This parameter is available when **Azure Blob Storage** is selected for **Location Type**.
List Path	Enter the path where the lists of files to be migrated are stored. These lists must be stored in the same region as the target bucket. You need to write the URLs of files to be migrated and their new names at the target into the lists. Each line in the list can contain only one URL and one file name. Restrictions on list files are: • The files must be in .txt format, and their metadata **Content-Type** must be **text/plain**. • A single file can contain a maximum of 100,000 rows. • A single file cannot exceed 300 MB. • A maximum of 10,000 list files can be stored in the folder. • The files must be in UTF-8 without BOM. • The length of each line in a file cannot exceed 65,535 characters, or the migration will fail. • The **Content-Encoding** metadata of the files must be left empty, or the migration will fail. • In the files, a tab character (\t) must be used to separate the URL and new file name in each line. The format is [URL][Tab character][New file name]. Only the Chinese and special characters in the names must be URL encoded. • Spaces are not allowed in each line in a file. Spaces may cause migration failures because they may be mistakenly identified as object names.	These parameters are available when **HTTP/HTTPS data source** is selected for **Location Type**.

Parameter	Description	Remarks
File System Address	Enter the mount address of the source file system. The format is *IP address:/xxx*, for example, 192.1.1.1:/0001.	These parameters are available when **Location Type** is set to **NAS_SMB**, **NAS_NFS_V3_MOUNT**, or **NAS_NFS_V3_PROTOCOL**.
Path	Enter the directory where files to be migrated are located. The format is */Folder name*.	
Username	Enter the username of the account that can access all files in the source file system, for example, **administrator**.	These parameters are available when **Location Type** is set to **NAS_SMB**.
Password	Enter the password of the account.	
Domain on Windows	Enter the domain of the target node. **NOTE** You only need to enter the content before .com. For example, if the domain is test.com, enter test.	

Table 3-3 Parameters for configuring a migration target

Parameter	Description	Remarks
Location Type	Select Huawei Cloud storage based on the source storage type.	-
AK	Enter the AK of the Huawei Cloud account you are migrating to.	These parameters are available when **Location Type** is set to **Huawei Cloud OBS**.
SK	Enter the SK of the Huawei Cloud account you are migrating to.	
Bucket	Select the OBS bucket you are migrating your data to.	
Endpoint	Enter the endpoint of the region where the target OBS bucket is located. **NOTE** If the migration source is an OBS bucket, you can view the endpoint in the OBS bucket overview.	

Parameter	Description	Remarks
Specify Prefix	Specify a prefix to rename or relocate objects migrated to the target bucket. For example, if you specify the prefix **/D**, source file **/A/B/C.txt** will be relocated to **/D/A/B/C.txt** after being migrated to the target bucket. For details, see: **Adding a Prefix or Directory Prefix to Migrated Objects**	
File System Address	Enter the mount address of the target file system. The format is *IP address:/xxx*, for example, 192.1.1.1:/0001.	These parameters are available when **Location Type** is set to **NAS_SMB** or **NAS_NFS_V3_MOUNT**.
Path	Enter the directory for storing files migrated. The format is */Folder name*.	
Username	Enter the username of the account that can access all files in the target file system, for example, **administrator**.	These parameters are available when **Location Type** is set to **NAS_SMB**.
Password	Enter the password of the account.	
Domain on Windows	Enter the domain of the target node. **NOTE** You only need to enter the content before .com. For example, if the domain is test.com, enter test.	

Step 7 Configure the migration settings based on **Table 3-4**.

Figure 3-5 Migration settings

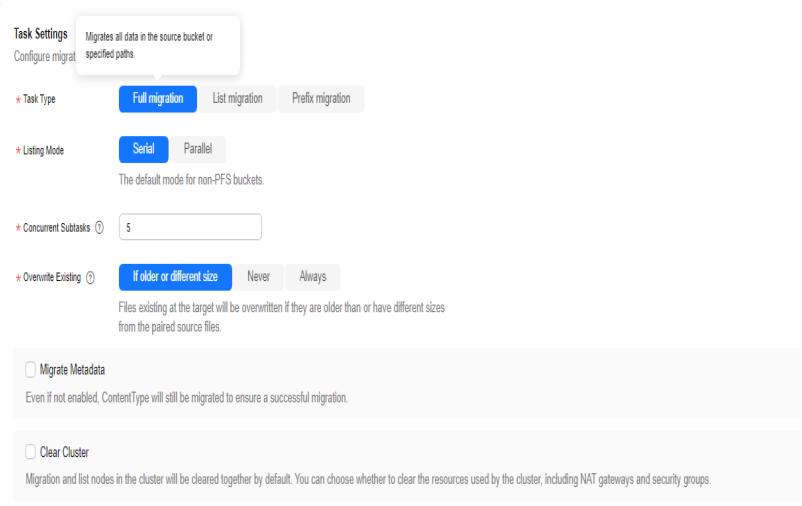


Table 3-4 Parameters for configuring the migration settings

Parameter	Value	Description
Task Type	Full migration	Migrates all data in the source bucket or specified paths.
	Partial migration by list	Migrates files recorded in the list files. In **List Path** box, enter the path of the object lists stored in the target bucket. Restrictions on an object list file vary with the target location. • **Target location: Huawei Cloud OBS** – An object list file cannot exceed 30 MB. – An object list file must be a .txt file, and the Content-Type metadata must be text/plain. – An object list file must be in UTF-8 without BOM. – Each line in an object list file can contain only one object name, and the object name must be URL encoded. – Each line in an object list file cannot exceed 16 KB, or the migration will fail. – The Content-Encoding metadata of an object list file must be left empty, or the migration will fail. – An object list file can contain a maximum of 10,000 lines. • Target location: NAS – An object list file cannot exceed 30 MB. – An object list file must be a .txt file. – An object list file must be in UTF-8 without BOM. – Each line in an object list file can contain only one object name, and the object name must be URL encoded. – Each line in an object list file cannot exceed 16 KB, or the migration will fail. – An object list file can contain a maximum of 10,000 lines.

Parameter	Value	Description
	Partial migration by prefix	This option is only available for migration from cloud storage. If you enter a file name or name prefix in the **Prefix** text box, only the objects that exactly match the specified name or prefix are migrated. **NOTICE** • If the files to be migrated are stored in the root directory of the source bucket, add their prefixes directly. If the files are stored in a non-root directory, add their directories and name prefixes in the format of *Directory*/*Prefix*. • Use commas (,) to separate multiple prefixes.
Concurrent Subtasks	-	Specify the maximum number of concurrent subtasks. There cannot be more than 10 concurrent subtasks for each online migration node. For example, if the number of online migration nodes is 2, the maximum number of subtasks can be 20 or any number below.
Overwrite Existing	Never	Files existing at the migration target are never overwritten. **WARNING** • If you choose **Never** for the initial migration, the attributes of involved parent folders at the source will not be migrated to the target. As a result, the folder attributes may be incomplete at the target. To avoid this issue, use the **Never** option with caution for the initial migration. • If a migration task is paused or interrupted and then restarted or resumed, the **Never** option will cause the system to skip files that were not completely migrated earlier, but the task may still be marked as successful. This affects data integrity. To avoid this issue, use the **Never** option with caution.
	Always	Files existing at the migration target are always overwritten.
	If older or different size	• Files that already exist at the target will be overwritten if they are older than or have different sizes from the paired files at the source. • Verification will be performed for folders after their contents are migrated. Folders that already exist at the target will be overwritten if they have different last modification times, sizes, or permissions from the paired folders at the source. **NOTE** For empty folders, the overwrite policy is the same as that for files.

Parameter	Value	Description
Migrate Metadata	-	Determine whether to migrate metadata. • If you select this option, object metadata will be migrated. • If you do not select this option, only the Content-Type and Content-Encoding metadata will be migrated.
Clear Cluster	-	Determine whether to clear the migration cluster after the migration is complete. • If you select this option, a step for clearing the migration cluster will be created in the workflow. You can also choose whether to clear resources used by the cluster, such as NAT gateways, security groups, and VPCEP resources. • If you do not select this option, a step for clearing the migration cluster will not be created in the workflow.

Step 8 (Optional) Configure advanced options based on **Table 3-5**.

Figure 3-6 Advanced settings

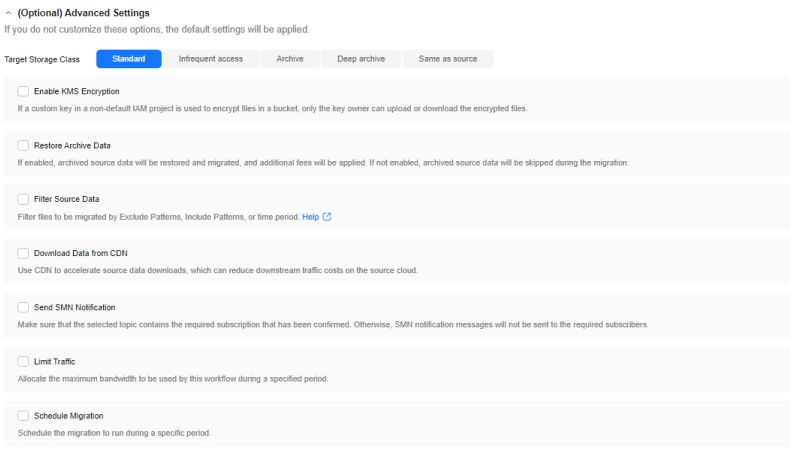


Table 3-5 Advanced options

Parameter	Description	Remarks
Target Storage Class	Choose the storage class that your data will be migrated to in the target bucket. For details about storage classes, see **Introduction to Storage Classes**.	-

Parameter	Description	Remarks
Enable KMS Encryption	• If you do not select this option, whether migrated data will be encrypted in the target bucket depends on the server-side encryption setting of the bucket. • If you select this option, all migrated objects will be encrypted before they are stored in the target bucket. **NOTE** • Using KMS to encrypt migrated data may slow down the migration speed by about 10%. • This option is only available when KMS is supported in the region you are migrating to.	This parameter is only available for migrations to Huawei Cloud OBS.
Restore Archive Data	• If you do not select this option, the system records archive objects in the list of objects that failed to be migrated and continues to migrate other objects in the migration task. • If you select this option, the system automatically restores and migrates archive objects in the migration task. If an archive object fails to be restored, the system skips it and records it in the list of objects that failed to be migrated and continues to migrate other objects in the migration task. **NOTE** The system will restore archive data before migrating it, and you pay the source cloud platform for the API requests and storage space generated accordingly.	-
Filter Source Data	Filter files to be migrated using filters. For details about the filters, see **Source Data Filters**.	
Obtain Data from CDN	If the default domain name cannot meet your migration requirements, then as long as the source cloud service provider supports custom domain names, you can associate a custom domain name to the source bucket, and enable the CDN service on the source platform to reduce data download expenses. Enter a custom domain name in the **Domain Name** text box and select a transmission protocol. HTTPS is more secure than HTTP and is recommended. If the migration source is the Alibaba Cloud OSS or Tencent Cloud COS, you also need to select an authentication type and enter an authentication key.	

Parameter	Description	Remarks
Send SMN Notification	Determine whether to use SMN to get notifications about migration results. ● If you do not select this option, no SMN messages are sent after the migration. ● If you select this option, after the migration, SMN messages are sent to the subscribers of the selected topic. You can select the language and trigger conditions for sending messages.	
Limit Traffic	Allocate the maximum bandwidth to be used by the workflow during a specified period. ● If you do not select this option, migration traffic is not limited. ● If you select this option, limit the migration traffic by setting **Start Time**, **End Time**, and **Bandwidth Limit**. For example, if you set **Start Time** to **08:00**, **End Time** to **12:00**, and **Bandwidth Limit** to **20 MB/s**, the maximum migration speed is limited to 20 MB/s from 08:00 to 12:00. The migration speed is not limited beyond this period. **NOTE** – The rate limit ranges from 0 MB/s to 1,048,576 MB/s. – A maximum of five rules can be added. – The time is the local standard time of the region you are migrating to.	
Schedule Migration	Schedule the migration to automatically run during a period. ● If you do not select this option, you need to manually start or stop the migration. ● If you select this option, the migration runs during the specified period and stops beyond that period. For example: – If you set **Start Time** to **08:00** and **End Time** to **12:00**, the migration task runs from 08:00 to 12:00 every day. The migration stops beyond that period. – If you set **Start Time** to **12:00** and **End Time** to **08:00**, the migration runs from 12:00 of the current day to 08:00 of the next day. The migration stops beyond that period.	

Step 9 Click **Next: Confirm**.

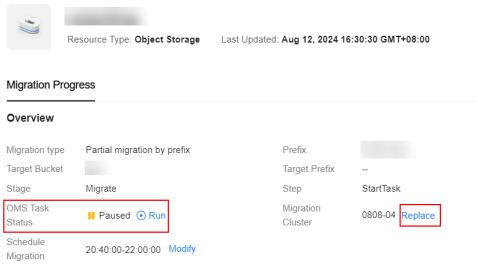
Step 10 Confirm the workflow settings and click **Confirm**. The **Run Workflow** dialog box is displayed, which indicates that the workflow has been created.

- If you want to start the migration immediately, click **Confirm** to run the workflow.
- If you want to **add a stage or step** to the workflow, click **Cancel**. The workflow enters a **Waiting** state, and the migration has not started. To start the migration, click **Run** in the **Operation** column.

Step 11 On the migration workflow details page, view the workflow settings and the migration progress. You can also perform the following operations:

- Move the cursor to the migration progress bar of a resource. In the displayed window, view the migration details about the resource.
- When a migration reaches a step that requires manual confirmation, place the cursor on the progress bar and click **Confirm** next to the step status in the displayed window. The migration can continue only after you confirm.
- In the **Basic Information** area, click **Manage** next to the cluster name. The cluster details page is displayed on the right. On the displayed page, you can:
  - Add, edit, or delete traffic limiting rules to control cluster traffic based on your requirements.
  - Add or delete migration nodes or list nodes, or upgrade plug-ins for existing nodes as required.

Step 12 (Optional) Click the migration progress bar of a resource or click **Migration Progress** in the window displayed when you move course to the progress bar. The migration details page is displayed on the right. You can view the task overview and progress details. You can also perform the following operations:

Operation	Description
Changing the migration cluster	You can change the migration cluster only when the migration task (workflow) is **Paused**.  1. In the **Overview** area, click **Replace** next to the migration cluster name. 2. In the displayed dialog box, select a new cluster from the drop-down list and click **Confirm**. After the cluster is changed, the workflow starts to run automatically.

Operation	Description
Modifying the migration schedule	1. In the **Overview** area, click **Modify** next to **Schedule Migration**. 2. Set **Start Time** and **End Time**, and click **Confirm**.
Modifying the number of concurrent subtasks	1. In the **Progress** area, under **Expected Concurrent Subtasks**, click **Modify** to change the expected number of concurrent subtasks. There cannot be more than 10 concurrent subtasks for each online migration node. For example, if there are 2 online migration nodes, the maximum number of subtasks can be 20 or any number below. 2. Click **Confirm**.
Adding traffic limiting rules	1. In the **Migration Speed** area, click **Add** to add a rule to limit the bandwidth the migration can use in a specified period. **NOTICE** – The bandwidth limit ranges from 1 MB to 1,024 GB. – Time periods in different rules cannot overlap. For example, if there is a rule added for the period from 8:00 to 12:00, you cannot configure rules for any overlapped periods, such as from 7:00 to 13:00, 7:00 to 8:00, and 9:00 to 12:00. – The start time of a rule cannot be later than the end time. For example, the time period from 23:00 to 01:00 is not allowed. 2. Click **Save**.
Obtaining the lists of files that fail to be migrated, skipped, or migrated	In the **File Statistics** area, view the path of the list of files that failed to be migrated, skipped, or migrated. Click a file path, and it will take you to the OBS bucket where the list is stored. You can download the list from the bucket.
Viewing traffic statistics	In the **Traffic Statistics** area, view the migration traffic in the last hour, last 6 hours, last 24 hours, or the entire migration period.

----End

Source Data Filters

The following table describes the rules and restrictions for setting source data filters.

Table 3-6 Filter options

Option	Description	Patten Rule	Constraint
Exclude Patterns	If a file matches any excluded pattern, the file will not be migrated or compared for consistency. Both exact match and fuzzy match are supported.	• Exact match You need to specify absolute paths and use slashes (\) to escape special characters in the paths.	• Except for {}, consecutive characters specified in pattern rules are not allowed, for example, ***, *?, **?, ?*, ?**, *{*, *}*, *}?, ?{*, {*}, {,}, {*,,, *}, and ,*, • Only asterisks (*) can be used as wildcard characters in {}. • {1} cannot be nested in {0}. • Excluded patterns take precedence over included patterns. • Semicolons (;) are used to separate patterns outside {}.
Include Patterns	• If no included patterns are specified, all files in the source will be migrated. • If included patterns are specified, only the files whose absolute paths match the specified patterns will be migrated or compared for consistency.		

Option	Description	Patten Rule	Constraint
		CAUTION Precautions for configuring exclude and include patterns: • If the file system address ends with :/, when you configure the paths to be excluded or included, enter their absolute paths relative to the mount point. For example, if the file system address is **192.1.1.1:/** and the mount point is **/mnt/turbo**, enter absolute paths relative to **/mnt/turbo**. For example: [root@oms-cluster-ecs filter_test]# pwd /mnt/sts_turbo/mgc/filter_test [root@oms-cluster-ecs-filter_test]# ll drwxr-xr-x 2 root root 0 Aug 16 15:27 test2 -rw-r--r-- 1 root root 5 Aug 16 15:27 test2.log To exclude the **test2.log** file from the migration, you can enter its absolute path **/mgc/filter_test/test2.log** in the **Exclude**	

Option	Description	Patten Rule	Constraint
		• Fuzzy match – An asterisk (*) matches zero or more characters except for slashes (/). – A pair of asterisks (**) matches zero or more characters including slashes (/). – A question mark (?) matches exactly one character, but not slashes (/). – Commas (,) are used to separate patterns in {}. Patterns in {} are in an OR relationship. – Wildcard characters asterisk (*) and question mark (?) are escaped by backslashes (\). In other cases, a backslash (\) means itself.	

Option	Description	Patten Rule	Constraint
Time Range	Filters files and directories to be migrated based on when they were last modified. Only files and directories whose last modification times fall in the configured time range will be migrated. The start time and end time can be left empty. If they are left empty, the system will not filter out source files by time. The time can be precise to the minute.		

The following table lists example pattern rules for different scenarios.

NOTICE

Assume that you want to migrate the directory **test** in the source storage system.

- If the source storage system is a NAS device, enter **/test** as an "include" pattern.
- If the source storage system is an object storage system, enter **test** as an "include" pattern.

Scenario	Example Pattern for NAS	Example Pattern for Object Storage	Description
File paths that end with *xx*	/xx /**xx	xx /**xx	*xx* can be an expression containing asterisks (*) and question marks (?).
Files whose names start with *xx* in the root directory	/xx* • **/testssss** matches the pattern. • **/test/xx** does not matches the pattern.	/xx* • **testssss** matches the pattern. • **/test/xx** does not matches the pattern.	
File paths that start with *xx*	/xx** /xx/**	xx** xx/**	
Files whose names contain *xx*	**xx*	**xx*	
File paths that contain *xx*	**xx**	**xx**	

Scenario	Example Pattern for NAS	Example Pattern for Object Storage	Description
File paths that start with *xx* and end with *yy*.	/xx**yy	xx**yy	*xx* and *yy* can be expressions containing asterisks (*) and question marks (?).
File paths that end with *xx* or *yy*	**{xx,yy}	**{xx,yy}	
Files whose names contain *xx* or *yy*	**{xx,yy}*	**{xx,yy}*	
Files paths that contain *xx* or *yy*	**{xx,yy}**	**{xx,yy}**	

3.2 Migrating Data from Multiple Source Buckets by Prefix

This section describes how to filter objects to be migrated in source buckets using prefixes and migrate the objects to Huawei Cloud OBS buckets.

Preparations

- Prepare a Huawei account or an IAM user that can access MgC. For details, see **Preparations**.
- **Create a migration project** on the MgC console.
- Add the AK/SK pair used for accessing the source cloud platform to MgC. The AK/SK pair will be used to collecting details about source buckets. For more information, see **Adding Resource Credentials**.
- Ensure that the source and target accounts have the permissions required for the migration. For details, see **How Do I Obtain Required Permissions for the Source and Target Accounts?**
- On Huawei Cloud, create an OBS bucket for receiving migrated data. For details, see **Creating a Bucket**. You can also use as existing bucket.
- Create a prefix list for each source bucket to be migrated. A prefix list must meet the following requirements:
  - The list must be in .txt format and the file size cannot exceed 2 MB.
  - Each line in the file can only contain one prefix, and a prefix cannot be longer than 1,024 characters.
  - A maximum of 1,000 prefixes can be contained in a file.

Precautions

- Supported regions

  You can object storage data in batches to the following regions. To migrate to other regions, use RDA or other solutions.

  - LA-Santiago
  - LA-Sao Paulo
  - TR-Istanbul
  - AP-Bangkok
  - AP-Singapore
  - AP-Jakarta
  - ME-Riyadh
  - CN North-Beijing4
  - CN East-Shanghai1
- Intranet migration

  Data can be migrated between buckets in the same region over the intranet.
- Soft link processing

  MgC does not support migration through symbolic links. To migrate a path pointed to by a symbolic link, you need to:
  - Enter the actual path to be migrated when creating a migration workflow.
  - After the migration is complete, manually create a symbolic link to the path at the target.

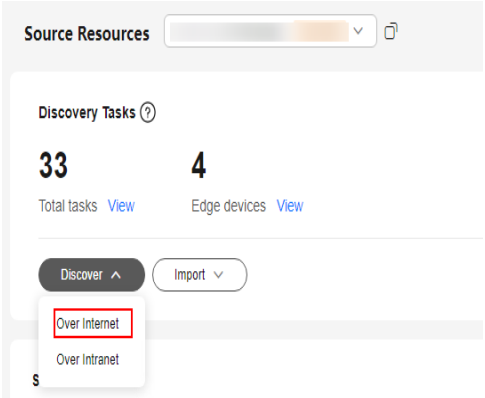
Step 1: Discovering Source Buckets

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

Step 2 In the navigation pane on the left, choose **Research** > **Source Resources**. In the upper left corner of the page, select the migration project created in **Preparations**.

Step 3 In the **Discovery Tasks** card, choose **Discover** > **Over Internet**.

Figure 3-7 Discovery over Internet



Step 4 Set parameters in the **Basic Settings** and **Task Settings** areas based on **Table 3-7**.

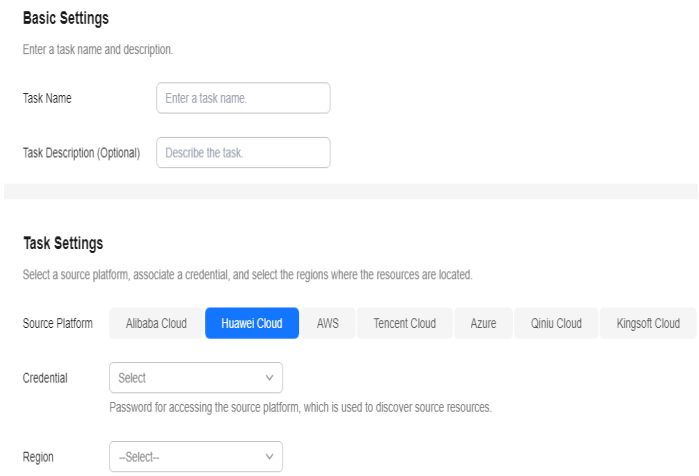
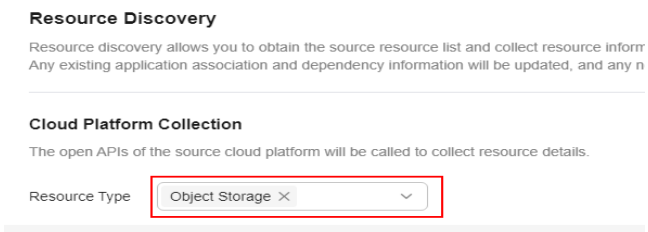


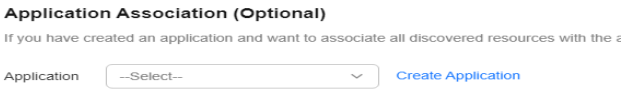
Table 3-7 Parameters in the **Basic Settings** and **Task Settings** areas

Area	Parameter	Description	Mandatory
Basic Settings	Task Name	Enter a task name.	Yes
	Task Description	Describe the task.	No
Task Settings	Source Platform	Select the source cloud platform. In this example, select **Huawei Cloud**.	Yes
	Credential	Select the source credential added in **Preparations**. If you did not **add the credential**, click **Create**. In the displayed area, set **Authentication** to **AK/SK**, enter the AK/SK pair of the source account, and click **Verify and Save**.	Yes
	Region	Select the regions where your source resources are located.	Yes

Step 5 In the **Resource Discovery** area, select **Object Storage** from the **Resource Type** drop-down list. If the source platform is the Alibaba Cloud or Tencent Cloud, you need to enable **Cloud Platform Discovery** before selecting a resource type.



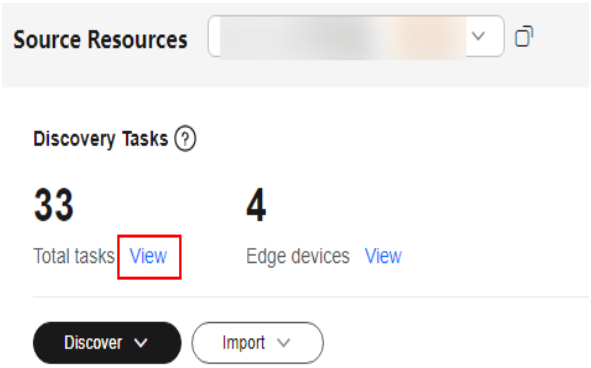
Step 6 Associate the collected object storage resources with an application.



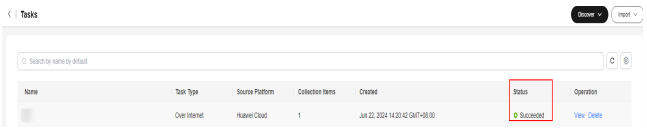
- If an application is available, select the **application** from the **Application** drop-down list.
- If no applications are available, click **Create Application**. In the displayed dialog box, enter an application name and description; select the business scenario, environment, and region; and click **OK**.

Step 7 Click **Confirm**. The task for discovering object storage resources over the Internet is created, and the system automatically starts collecting resource details.

Step 8 On the **Source Resources** page, click **View** next to **Total tasks** to go to the task list.



Wait until the task status changes to **Succeeded** that indicates the collection is complete.



----End

Step 2: Create a Migration Cluster

Additional charges incur for migration clusters. For details, see **Billing**.

NOTICE

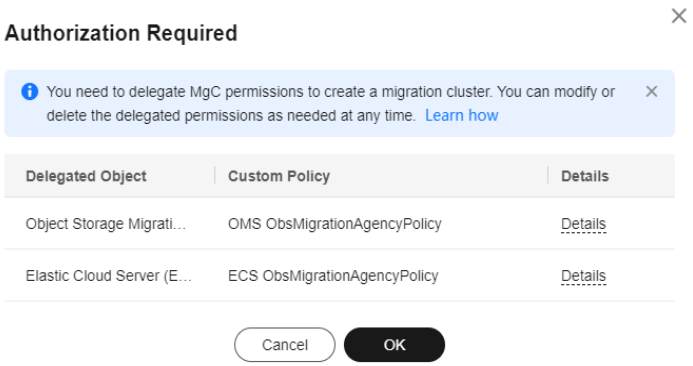
To ensure migration stability and data security, you are not allowed to log in to nodes in migration clusters. If you indeed need to log in to the nodes, contact technical support.

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

Step 2 In the left navigation pane, choose **Deploy** > **Migration Clusters**.

Step 3 Click **Create Cluster** in the upper right corner of the page.

If this is your first time to create a migration cluster, you need to delegate MgC the required permissions. For more information about the required permissions, see **Agency Permissions**.



Step 4 Configure the parameters listed in **Table 3-8**.

Table 3-8 Parameters for creating a cluster

Area	Parameter	Configuration	Constraints
Basic Settings	Cluster Name	Enter a name.	The cluster name must be unique in the same account.
	Region	Select the region to provision the cluster.	The cluster must be provisioned in the target region you are migrating to.
	Cluster Type	Select what the cluster will be used for.	Currently, only storage migration is supported.
Node Settings	Master Node	It is used to manage migration nodes and list nodes.	A cluster can only have one master node.

Area	Parameter	Configuration	Constraints
	Migration Node	Migration nodes are used for executing migration and verification tasks. The recommended specifications are 8 vCPUs and 16 GB of memory.	• The node specifications cannot be modified after the cluster is created. • The number of nodes must meet the following requirements: – Number of migration nodes + Number of list nodes + 1 ≤ 100 – Number of migration nodes + Number of list nodes + 1 ≤ Number of unused IP addresses in the subnet
	List Node	List nodes are used for listing tasks. The recommended specifications are 8 vCPUs and 16 GB of memory.	
Network Settings	VPC	Select a VPC from the drop-down list.	-
	Subnet	Make sure that there are enough unused IP addresses for the migration and list nodes in this cluster.	Number of unused IP addresses in the subnet ≥ Number of migration nodes + Number of list nodes + 1

Area	Parameter	Configuration	Constraints
	Network Type	• **Internet**: You need to select a public NAT gateway. If there is no gateway available, choose **Buy Gateway** from the drop-down list and select the gateway specifications and EIPs you want to associate with the gateway. A maximum of 20 EIPs can be selected at a time. • **Intranet**: This option is suitable for data migration within a region. • **Private line**: Source data is directly accessed through the private line. For details about Direct Connect, see **Direct Connect**.	-
Advanced Settings	DNS Configuration (Optional)	Enter the IP address of the DNS server to update the value of **nameserver** in the **/etc/resolv.conf** file. Use commas (,) to separate multiple DNS server addresses, for example, 192.0.2.1,192.0.2.2.	A maximum of three DNS IP addresses can be specified.
	Domain Mapping (Optional)	Add mappings between domain names and IP addresses to update the **/etc/hosts** file.	A maximum of 500 mappings can be added.

Area	Parameter	Configuration	Constraints
-	Traffic Limiting	Allocate the maximum bandwidth to be used by the workflow during a specified period. • If you do not select this option, migration traffic is not limited. • If you select this option, limit the migration traffic by setting the start time, end time, and bandwidth limit. **NOTICE** For example, if you set **Start Time** to **08:00**, **End Time** to **12:00**, and **Maximum Bandwidth** to **20 MB/s**, the maximum migration speed is limited to 20 MB/s when the migration task is running in the period from 08:00 to 12:00. The migration speed is not limited beyond this period.	• A maximum of five traffic limiting rules can be added. • The time is the local standard time of the region you are migrating to.
	Log Collection	• If this option is enabled, logs generated during the migration are collected for possible troubleshooting later. • If this option is disabled, logs generated during storage migrations are not collected.	-

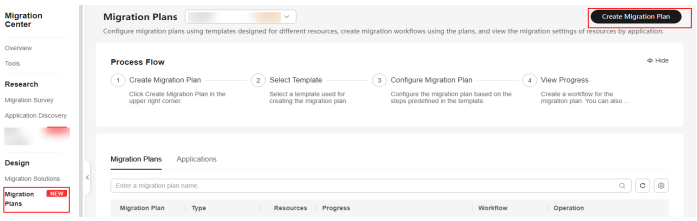
Step 5 Click **Confirm**. Then you can view the cluster in the list. For details about cluster statuses, see **Cluster Statuses**. If the cluster status is **Creation failed**, move the cursor to the status to view the failure cause. After the fault is rectified, choose **More** > **Retry** to try to create the cluster again.

----End

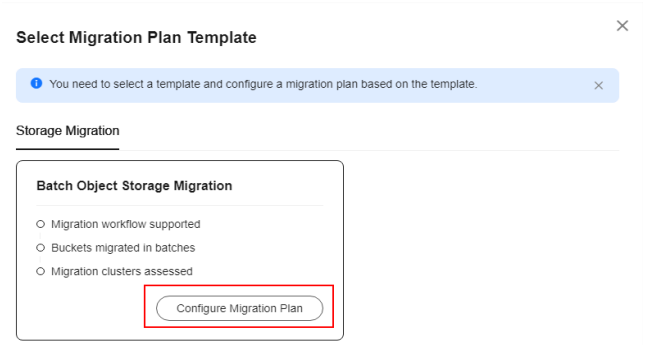
Step 3: Creating a Migration Plan

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

Step 2 In the navigation pane, choose **Design** > **Migration Plans**. Click **Create Migration Plan** in the upper right corner of the page.



Step 3 In the **Batch Object Storage Migration** card, click in the **Configure Migration Plan**.

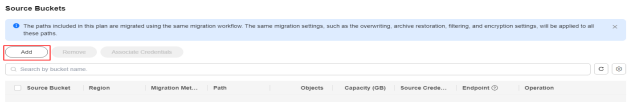


Step 4 In the **Basic Settings** area, set parameters listed in **Table 3-9**.

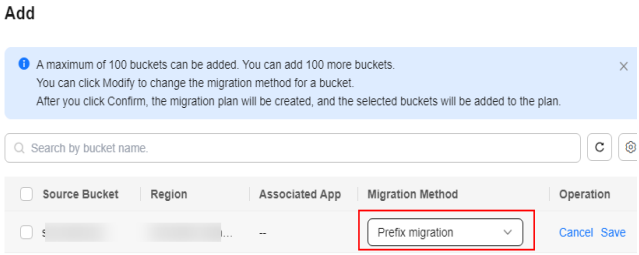
Table 3-9 Basic parameters

Parameter	Configuration
Migration Plan	Enter a name.
Description (Optional)	Enter a description.
Source Platform	Select the source platform you selected in **Step 1**. Select **Huawei Cloud**.
Target Region	Select the region you want to migrate to.

Step 5 Above the source bucket list, click **Add**.



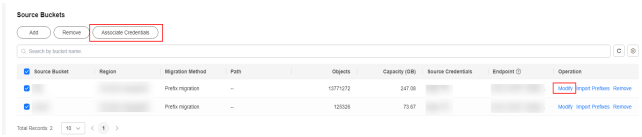
Step 6 Select the buckets to be migrated, click **Modify** in the **Operation** column, set **Migration Method** to **Prefix migration**, and click **Save** and then **Confirm**.



CAUTION

- The selected resources must come from the source platform selected in **Basic Settings**.
- A maximum of 100 buckets can be added.

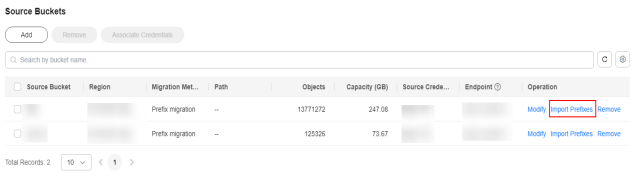
Step 7 Associate source credentials.



- To associate a source bucket with a credential, locate the source bucket in the list and click **Modify** in the **Operation** column. In the **Modify Migration Settings** dialog box that is displayed, select a source credential.
- To associate multiple source buckets with a credential, select these buckets from the list and click **Associate Credentials** above the list.

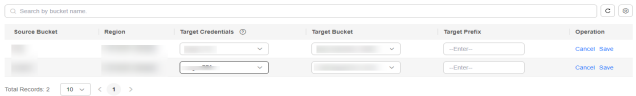
Step 8 Import the prefix lists.

Locate a source bucket in the list, and click **Import Prefixes** in the **Operation** column. Upload the prefix list file prepared for the bucket and click **Confirm**.



Step 9 Confirm that the source buckets have been associated with their credentials and the prefix import is complete for all the buckets, and click **Next** to configure the target buckets.

Step 10 Locate a source bucket, click **Modify** in the **Operation** column, select the credential used for accessing target bucket, enter a prefix to rename migrated objects, and click **Save**.



Step 11 After you configure the migration settings for all buckets to be migrated, click **Next**. Assess how large of a migration cluster is required for the migration and create a migration cluster in the recommended size. Alternatively, you can skip this step and use an existing migration cluster. For details, see **Managing a Migration Cluster**.

Step 12 Click **Next**. On the displayed page, click **Select Cluster** to choose an existing migration cluster.

Step 13 In the displayed cluster list, select the cluster created in **step 2** and click **Confirm**. The source resources in the migration plan will be migrated using the selected cluster.

NOTICE

Only healthy or subhealthy migration clusters can be selected.

Step 14 Click **OK**. After migration plan is created, you can see it in the list.

- If you need to modify the plan settings, click **Design** in the **Operation** column.
- When the design progress of the plan is **Completed**, click **Create Workflow** in the **Operation** column to **create a migration workflow** to migrate all buckets in the plan in a batch.

----End

Step 4: Creating a Batch Object Storage Migration Workflow

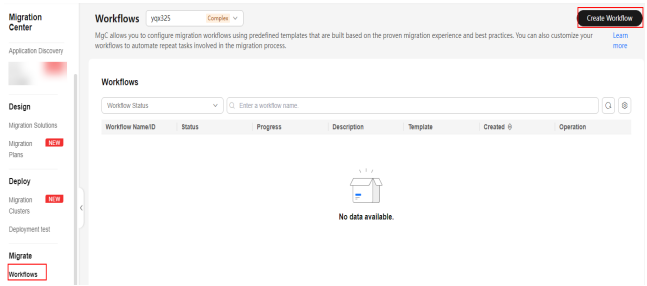
NOTICE

- A single object cannot be larger than 4.76837158203125 TB (500 MB x 10,000). Otherwise, the migration may fail.
- During the migration, the system automatically creates a temporary folder named **oms** in the target bucket. Do not perform any operations on this folder, including but not limited to modifying, deleting, or adding data in the folder. Otherwise, the migration will be interrupted or fail.

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

Step 2 In the navigation pane on the left, choose **Migrate** > **Workflows**.

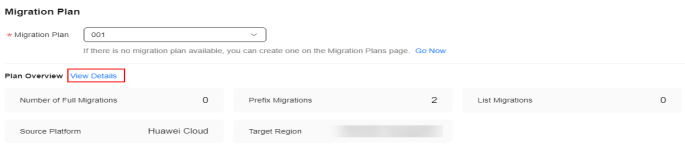
Step 3 Click **Create Workflow** in the upper right corner of the page.



Step 4 Select **Batch Object Storage Migration** and click **Configure Workflow**.

Step 5 In the **Basic Information** area, enter a name and description for the workflow.

Step 6 In the **Migration Plan** area, select the migration plan created in **Step 3**. Then you should view the overview of the migration plan. Click **View Details** to view more information about the plan.



Step 7 In the **Migration Cluster** area, select the cluster used for the migration. The cluster specified in the migration plan is preselected by default, but you can select another one if needed. The modification is applied to the current workflow but not to the migration plan.

Step 8 Configure the migration settings based on **Table 3-10**.

Table 3-10 Migration settings

Parameter	Option	Description
Concurrent Subtasks	-	This parameter is user-defined. There cannot be more than 10 concurrent subtasks for each online migration node. For example, if the number of online migration nodes is 2, the maximum number of subtasks can be 20 or any number below.
Overwrite Existing	Never	Files existing at the migration target are never overwritten. **WARNING** • If you choose **Never** for the initial migration, the attributes of involved parent folders at the source will not be migrated to the target. As a result, the folder attributes may be incomplete at the target. To avoid this issue, use the **Never** option with caution for the initial migration. • If a migration task is paused or interrupted and then restarted or resumed, the **Never** option will cause the system to skip files that were not completely migrated earlier, but the task may still be marked as successful. This affects data integrity. To avoid this issue, use the **Never** option with caution.
	Always	Files existing at the migration target are always overwritten.

Parameter	Option	Description
	If older or different size	• Files that already exist at the target will be overwritten if they are older than or have different sizes from the paired files at the source. • Verification will be performed for folders after their contents are migrated. Folders that already exist at the target will be overwritten if they have different last modification times, sizes, or permissions from the paired folders at the source. **NOTE** For empty folders, the overwrite policy is the same as that for files.
Migrate Metadata	-	Determine whether to migrate metadata. • If you select this option, object metadata will be migrated. • If you do not select this option, only the Content-Type and Content-Encoding metadata will be migrated.

Step 9 (Optional) Configure advanced options based on **Table 3-11**.

Table 3-11 Advanced settings

Parameter	Description
Target Storage Class	Choose the storage class that your data will be migrated to in the target bucket. For details about storage classes, see **Introduction to Storage Classes**.
Enable KMS Encryption	• If you do not select this option, whether migrated data will be encrypted in the target bucket depends on the server-side encryption setting of the bucket. • If you select this option, all migrated objects will be encrypted before they are stored in the target bucket. **NOTE** • Using KMS to encrypt migrated data may slow down the migration speed by about 10%. • This option is only available when KMS is supported in the region you are migrating to.

Parameter	Description
Restore Archive Data	• If you do not select this option, the system records archived objects in the list of objects that failed to be migrated and continues to migrate other objects in the migration task. • If you select this option, the system automatically restores and migrates archived objects in the migration task. If an archived object fails to be restored, the system skips it and records it in the list of objects that failed to be migrated and continues to migrate other objects in the migration task. **NOTE** The system will restore archived data before migrating it, and you pay the source cloud platform for the API requests and storage space generated accordingly.
Filter Source Data	Filter files to be migrated by applying filters. For details about filters, see **Source Data Filters**.
Download Data from CDN	If the default domain name cannot meet your migration requirements, then as long as the source cloud service provider supports custom domain names, you can associate a custom domain name with the source bucket, and enable the CDN service on the source platform to reduce data download fees. Enter a custom domain name in the **Domain Name** text box and select a transmission protocol. HTTPS is more secure than HTTP and is recommended. If the migration source is the Alibaba Cloud OSS or Tencent Cloud COS, you also need to select an authentication type and enter an authentication key.
Send SMN Notification	Determine whether to use SMN to get notifications about migration results. • If you do not select this option, no SMN messages are sent after the migration is complete. • If you select this option, after the migration is complete, SMN messages are sent to the subscribers of the selected topic. You can select the language and trigger conditions for sending messages.

Parameter	Description
Limit Traffic	Allocate the maximum bandwidth to be used by the workflow during a specified period. • If you do not select this option, migration traffic is not limited. • If you select this option, limit the migration traffic by setting **Start Time**, **End Time**, and **Bandwidth Limit**. For example, if you set **Start Time** to **08:00**, **End Time** to **12:00**, and **Bandwidth Limit** to **20 MB/s**, the maximum migration speed is limited to 20 MB/s from 08:00 to 12:00. The migration speed is not limited beyond this period. **NOTE** – The rate limit ranges from 0 MB/s to 1,048,576 MB/s. – A maximum of five rules can be added. – The time is the local standard time of the region you are migrating to.

Step 10 Click **Next: Confirm**.

Step 11 Confirm the workflow settings and click **Confirm**. The **Run Workflow** dialog box is displayed, which indicates that the workflow has been created.

- If you want to start the migration immediately, click **Confirm** to run the workflow.
- If you want to **add a stage or step** to the workflow, click **Cancel**. The workflow enters a **Waiting** state, and the migration has not started. To start the migration, click **Run** in the **Operation** column.

Step 12 On the migration workflow details page, view the workflow settings and the migration progress. You can also perform the following operations:

- Move the cursor to the migration progress bar of a resource. In the displayed window, view the migration details about the resource.
- When a migration reaches a step that requires manual confirmation, place the cursor on the progress bar and click **Confirm** next to the step status in the displayed window. The migration can continue only after you confirm.
- In the **Basic Information** area, click **Manage** next to the migration cluster name. The cluster details page is displayed on the right. On the displayed page, you can:
  - Add, edit, or delete traffic limiting rules to control cluster traffic based on your requirements.
  - Add or delete migration nodes or list nodes, or upgrade plug-ins for existing nodes as required.

----End

(Optional) Step 5: Clearing the Migration Cluster

If the migration cluster is no longer needed after your data migration is complete, you can delete the cluster and the associated resources. For details, see **Deleting a Migration Cluster**.

3.3 Migrating Archive (Cold) Data

Background

Cold storage is a long-term backup solution for infrequently accessed data. For example, data accessed annually can be stored in archive storage, while data accessed every few years can be stored in deep archive storage. This storage mode has advantages such as high security, durability, and low costs.

When migrating cold storage data, you need to consider data access latency because data is usually in a "frozen" state. Data must be restored or unfrozen before it can be accessed. Typically, there are two restoration options: **standard** and **expedited retrieval**. Their differences are as follows:

- **Standard**: Archive objects can be restored within 3 to 5 hours. This option is ideal for scenarios where immediate access is not required.
- **Expedited**: Archive objects can be restored within 1 to 5 minutes, and additional fees may be incurred. This option is ideal for scenarios where immediate access is required.

MgC storage migration workflows enable you to restore archive source data expeditiously.

Supported Regions

The following regions are supported:

- LA-Santiago
- LA-Sao Paulo
- TR-Istanbul
- AP-Bangkok
- AP-Singapore
- AP-Jakarta
- ME-Riyadh
- CN North-Beijing4
- CN East-Shanghai1

Notes and Constraints

- For more information, see **What Are the Restrictions on Using MgC for Storage Migration?**
- Data in the Deep Cold Archive storage of Alibaba Cloud OSS cannot be restored using the restoration function of MgC. You need to manually restore the data before migration.

Preparations

- Preparing a Huawei account

  Before using MgC, prepare a HUAWEI ID or an IAM user that can access MgC and obtain an AK/SK pair for the account or IAM user. For details about how to obtain an access key, see **Making Preparations**.

- Creating a migration project

  On the MgC console, create a migration project. For details, see **Managing Migration Projects**.

- Creating an OBS bucket

  Create an OBS bucket on Huawei Cloud in the target region for receiving source data. For details, see **Creating a Bucket**.

- Configuring permissions

  Ensure that the source and target accounts have the permissions required for the migration. For details, see **How Do I Obtain Required Permissions for the Source and Target Accounts?**

- Creating a migration cluster

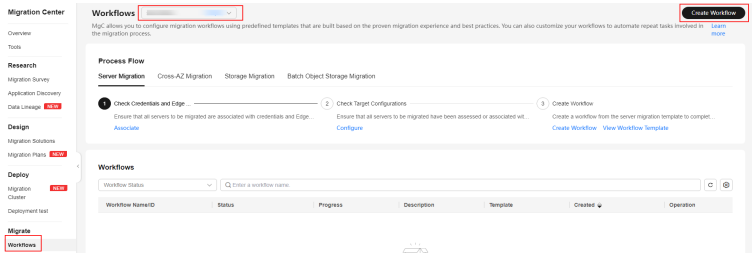
  Create a dedicated migration cluster for this migration. A cluster consists of a master node and several list and migration nodes. For details about how to create a cluster, see **Creating a Migration Cluster**.

Creating a Migration Workflow

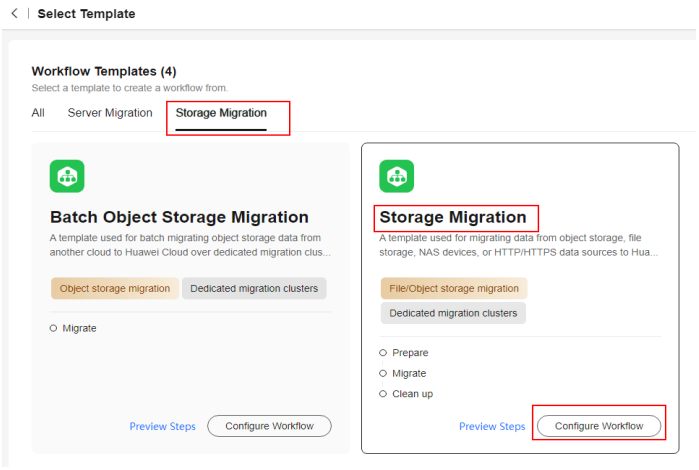
Step 1 Sign in to the **MgC console**.

Step 2 In the navigation pane on the left, choose **Migrate** > **Workflows**. In the upper left corner of the page, select the **migration project you created**.

Step 3 Click **Create Workflow** in the upper right corner of the page.



Step 4 Select **Storage Migration** and click **Configure Workflow**.



Step 5 Set workflow basics based on **Table 3-12**.

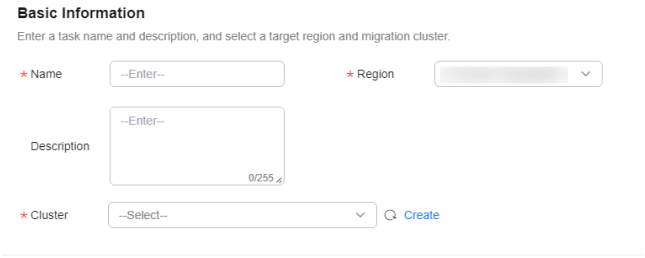


Table 3-12 Basic parameters

Parameter	Description
Name	User-defined
Region	Select the region where the **target bucket** is located from the drop-down list.
Description	User-defined
Cluster	Select the **cluster you created**.

Step 6 Configure the migration source and target based on **Table 3-13** and **Table 3-14**.

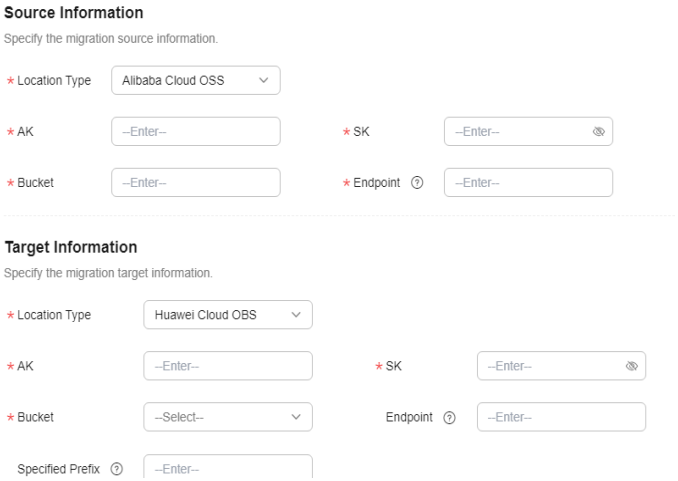


Table 3-13 Parameters for configuring a migration source

Parameter	Description
Location Type	Select the source cloud platform and data source.
AK	Enter the AK of the source cloud account.
SK	Enter the SK of the source cloud account.
Bucket	Enter the name of the source bucket to be migrated.
Endpoint	Enter the endpoint of the region where the source bucket is located. For example, if **Location Type** is set to **Alibaba Cloud OSS** and the source bucket is located in **CN East 1 (Hangzhou)**, enter **oss-cn-hangzhou.aliyuncs.com**.
Type	This parameter is available when **Huawei Cloud OBS** is selected for **Location Type**. Set this parameter based on the source bucket type. You can **view the bucket type in the basic information**.
AppID	This parameter is available when **Tencent Cloud COS** is selected for **Location Type**. Enter the AppID of your Tencent Cloud account. **NOTE** You can view the AppID on the account information page of the Tencent Cloud console.

Table 3-14 Parameters for configuring a migration target

Parameter	Description
Location Type	Select **Huawei Cloud OBS**.

Parameter	Description
AK	Enter the AK/SK pair of the target Huawei Cloud account.
SK	
Bucket	Select the **created OBS bucket**.
Endpoint	Enter the endpoint of the region where the target bucket is located. For example, if the target bucket is located in the **CN North-Beijing4** region of Huawei Cloud, enter **obs.cn-north-4.myhuaweicloud.com**. **NOTE** You can view the endpoint in the **basic information about the bucket**.
Specify Prefix	This parameter is optional. Specify a prefix to rename or relocate objects migrated to the target bucket. For example, if you specify the prefix **/D**, source file **/A/B/C.txt** will be relocated to **/D/A/B/C.txt** after being migrated to the target bucket. For details, see: **Adding a Name Prefix or Path Prefix to Migrated Objects**

Step 7 Configure the migration settings based on **Table 3-15**.

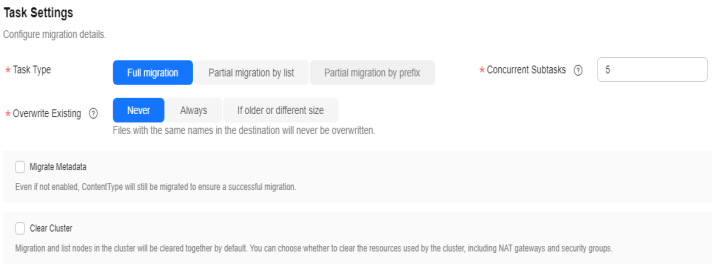


Table 3-15 Migration settings

Parameter	Option	Description
Task Type	List migration	Migrates objects recorded in the list files.
Concurrent Subtasks	-	Specify the maximum number of concurrent subtasks. There cannot be more than 10 concurrent subtasks for each online migration node. For example, if there are 2 online migration nodes, the maximum number of subtasks can be 20 or any number below.

Parameter	Option	Description
Overwrite Existing	Never	Files existing at the migration target will never be overwritten. **WARNING** • If you choose **Never** for the initial migration, the attributes of involved parent folders at the source will not be migrated to the target. As a result, the folder attributes may be incomplete at the target. To avoid this issue, use the **Never** option with caution for the initial migration. • If a migration task is paused or interrupted and then restarted or resumed, the **Never** option will cause the system to skip files that were not completely migrated earlier, but the task may still be marked as successful. This affects data integrity. To avoid this issue, use the **Never** option with caution.
	Always	Files existing at the migration target will always be overwritten.
	If older or different size	• Files that already exist at the target will be overwritten if they are older than or have different sizes from the paired files at the source. • Verification will be performed for folders after their contents are migrated. Folders that already exist at the target will be overwritten if they have different last modification times, sizes, or permissions from the paired folders at the source. **NOTE** For empty folders, the overwrite policy is the same as that for files.
Clear Cluster	-	Determine whether to clear the migration cluster after the migration is complete. • If you select this option, a step for clearing the migration cluster will be created in the workflow. You can also choose whether to clear resources used by the cluster, such as NAT gateways, security groups, and VPCEP resources. • If you do not select this option, a step for clearing the migration cluster will not be created in the workflow.

Step 8 Click before **(Optional) Advanced Settings** to expand advanced options and select **Restore Archive Data**. Configure the other advanced options as needed. For details, see **Table 3-16**.

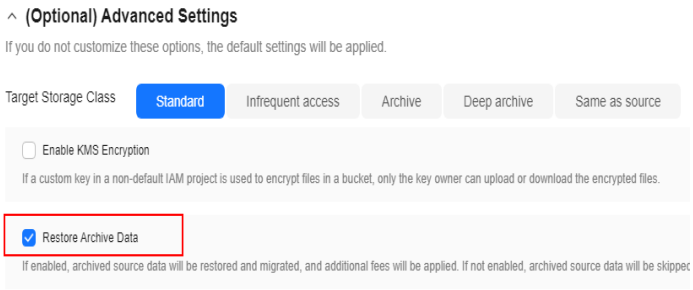


Table 3-16 Advanced options

Function	Description
Target Storage Class	Choose the storage class that your data will be migrated to in the target bucket. For details about storage classes, see **Introduction to Storage Classes**.
Enable KMS Encryption	• If you do not select this option, whether migrated data will be encrypted in the target bucket depends on the server-side encryption setting of the bucket. • If you select this option, all migrated objects will be encrypted before they are stored in the target bucket. **NOTE** • Using KMS to encrypt migrated data may slow down the migration speed by about 10%. • This option is only available when KMS is supported in the region you are migrating to.
Restore Archive Data	• If you do not select this option, the system records archived objects in the list of objects that failed to be migrated and continues to migrate other objects in the migration task. • If you select this option, the system automatically restores and migrates archived objects in the migration task. If an archive object fails to be restored, the system skips it and records it in the list of objects that failed to be migrated and continues to migrate other objects in the migration task. **NOTE** The system will restore archive data before migrating it, and you pay the source cloud platform for the API requests and storage space generated accordingly.
Filter Source Data	Filter files to be migrated by applying filters. For details about filters, see **Source Data Filters**.

Function	Description
Send SMN Notification	Determine whether to use SMN to get notifications about migration results. ● If you do not select this option, no SMN messages are sent after the migration is complete. ● If you select this option, after the migration is complete, SMN messages are sent to the subscribers of the selected topic. You can select the language and trigger conditions for sending messages.
Limit Traffic	Allocate the maximum bandwidth to be used by the workflow during a specified period. ● If you do not select this option, migration traffic is not limited. ● If you select this option, limit the migration traffic by setting **Start Time**, **End Time**, and **Bandwidth Limit**. For example, if you set **Start Time** to **08:00**, **End Time** to **12:00**, and **Bandwidth Limit** to **20 MB/s**, the maximum migration speed is limited to 20 MB/s from 08:00 to 12:00. The migration speed is not limited beyond this period. **NOTE** – The rate limit ranges from 0 MB/s to 1,048,576 MB/s. – A maximum of five rules can be added. – The time is the local standard time of the region you are migrating to.
Schedule Migration	Schedule the migration to run during a period. ● If you do not select this option, you need to manually start or stop the migration. ● If you select this option, the migration runs during the specified period and stops beyond that period. For example: – If you set **Start Time** to **08:00** and **End Time** to **12:00**, the migration task runs from 08:00 to 12:00 every day. The migration stops beyond that period. – If you set **Start Time** to **12:00** and **End Time** to **08:00**, the migration runs from 12:00 of the current day to 08:00 of the next day. The migration stops beyond that period.

Step 9 Click **Next: Confirm**.

Step 10 Confirm the workflow settings and click **Confirm**. The **Run Workflow** dialog box is displayed, which indicates that the workflow has been created.

- If you want to start the migration immediately, click **Confirm** to run the workflow.

- If you want to **add a stage or step** to the workflow, click **Cancel**. The workflow enters a **Waiting** state, and the migration has not started. To start the migration, click **Run** in the **Operation** column.

Step 11 On the migration workflow details page, view the workflow settings and the migration progress. You can also perform the following operations:

- Move the cursor to the migration progress bar of a resource. In the displayed window, view the migration details about the resource.
- When a migration reaches a step that requires manual confirmation, place the cursor on the progress bar and click **Confirm** next to the step status in the displayed window. The migration can continue only after you confirm.
- In the **Basic Information** area, click **Manage** next to the migration cluster name. The cluster details page is displayed on the right. On the displayed page, you can:
  - Add, edit, or delete traffic limiting rules to control cluster traffic based on your requirements.
  - Add or delete migration nodes or list nodes, or upgrade plug-ins for existing nodes as required.

----End

3.4 Migrating Data from SFS 1.0 to SFS 3.0

3.4.1 Precautions

- Supported regions

  You can use MgC to migrate data between SFS file systems in the following regions. To migrate to other regions, use RDA or other solutions.
  - LA-Santiago
  - LA-Sao Paulo
  - TR-Istanbul
  - AP-Bangkok
  - AP-Singapore
  - AP-Jakarta
  - ME-Riyadh
  - CN North-Beijing4
  - CN East-Shanghai1
- Migration over intranets

  Data can be migrated between file systems in the same region over the intranet.
- Soft link processing

  MgC does not support migration through symbolic links. To migrate a path pointed to by a symbolic link, you need to:
  - Enter the actual path to be migrated when creating a migration workflow.

- After the migration is complete, manually create a symbolic link to the path at the target.

3.4.2 Preparations

Preparing a Huawei Account

Before using MgC, prepare a HUAWEI ID or an IAM user that can access MgC and obtain an AK/SK pair for the account or IAM user. For details about how to obtain an access key, see **Preparations**.

Creating a Migration Project

Create a migration project on the MgC console. For details, see **Managing Migration Projects**.

Creating a Target File System

Create a file system for storing migrated data. For details, see **Creating a File System**.

3.4.3 Creating a Migration Cluster

You can create a dedicated migration cluster for fast migration. You can define and manage migration and list nodes in the cluster, such as installing or upgrading the migration plug-in on the nodes.

You need to pay for the resources used in the clusters. For details, see **Billing**.

NOTICE

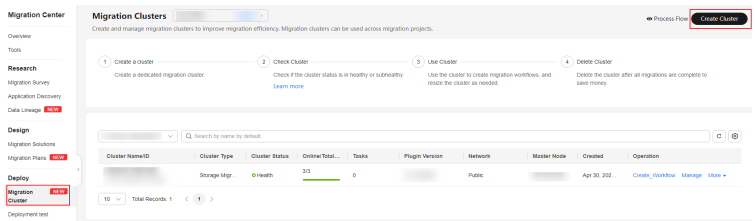
You cannot log in to nodes in a migration cluster. If you need to log in to them, contact technical support.

Procedure

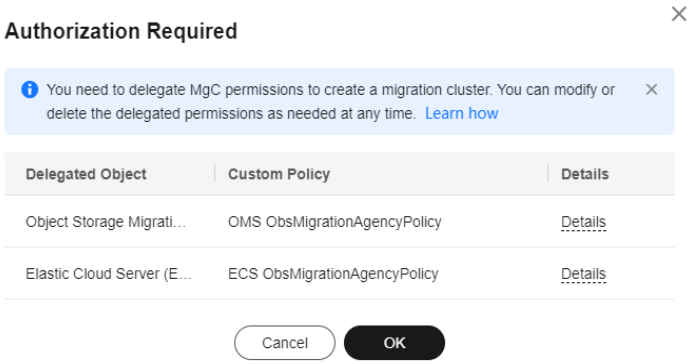
Step 1 Sign in to the **MgC** console.

Step 2 In the left navigation pane, choose **Deploy** > **Migration Clusters**. In the upper left corner of the page, select the migration project created in **Preparations**.

Step 3 Click **Create Cluster** in the upper right corner of the page.



If this is your first time to create a migration cluster, you need to delegate MgC the required permissions. For more information about the required permissions, see **Agency Permissions**.



Step 4 Configure the parameters listed in **Table 3-17**.

Table 3-17 Parameters for creating a cluster

Region	Parameter	Configuration	Constraints
Basic Settings	Cluster Name	Enter a custom name.	Cluster names must be unique in the same account.
	Region	Select the region to provision the cluster.	The cluster must be provisioned in the target region you are migrating to.
	Cluster Type	Select what the cluster will be used for.	Currently, only storage migration is supported.
Node Settings	Master Node	Select the specifications of the master node. The master node is used to manage migration nodes and list nodes in the cluster. The master node is created by default. You do not need to configure it.	The master node has the same specifications as migration nodes.

Region	Parameter	Configuration	Constraints
	Migration Node	Migration nodes are used for migration and verification. It is recommended that you use C-series ECSs with 8 vCPUs and 16 GB of memory.	• The node specifications cannot be modified after the cluster is created. • The number of nodes must meet the following requirements: – Number of migration nodes + Number of list nodes + 1 ≤ 100 – Number of migration nodes + Number of list nodes + 1 ≤ Number of unused IP addresses in the subnet
	List Node	List nodes are used for listing files to be migrated. It is recommended that you use C-series ECSs with 8 vCPUs and 16 GB of memory.	
Network Settings	VPC	Select a VPC from the drop-down list.	-
	Subnet	Make sure that there are enough IP addresses for the migration and list nodes in this cluster.	Number of unused IP addresses in the subnet ≥ Number of migration nodes + Number of list nodes + 1
	Network Type	Select **Intranet**.	Migrating data within a region is over the intranet. No EIP is required.

Region	Parameter	Configuration	Constraints
-	Limit Traffic	Allocate the maximum bandwidth to be used by the workflow during a specified period. • If you do not select this option, migration traffic is not limited. • If you select this option, limit the migration traffic by setting the start time, end time, and bandwidth limit. **NOTICE** For example, if you set **Start Time** to **08:00**, **End Time** to **12:00**, and **Maximum Bandwidth** to **20 MB/s**, the maximum migration speed is limited to 20 MB/s when the migration task is running in the period from 08:00 to 12:00. The migration speed is not limited beyond this period.	• A maximum of five traffic limiting rules can be added. • The time is the local standard time of the region you selected.
	Log Collection	• If this option is enabled, logs generated during the migration are collected for possible troubleshooting later. • If this option is disabled, logs generated during the migration are not collected.	-

Step 5 Click **Confirm**. View the cluster status in the migration cluster list. For descriptions of cluster statuses, see **Cluster Statuses**.

Step 6 Perform the following operations:

- If the cluster status is **Healthy** or **Subhealthy**, click **Create Workflow** in the **Operation** column to **create a storage migration workflow**.
- **Manage the cluster**. You can add or delete nodes and traffic limiting rules for the cluster.

----End

3.4.4 (Optional) Setting Up Network Connections

If your migration cluster is in a VPC different from the source SFS 1.0 file system and the target SFS 3.0 file system, you need enable communications between them.

Connecting the Migration Cluster to the Source SFS 1.0 File System

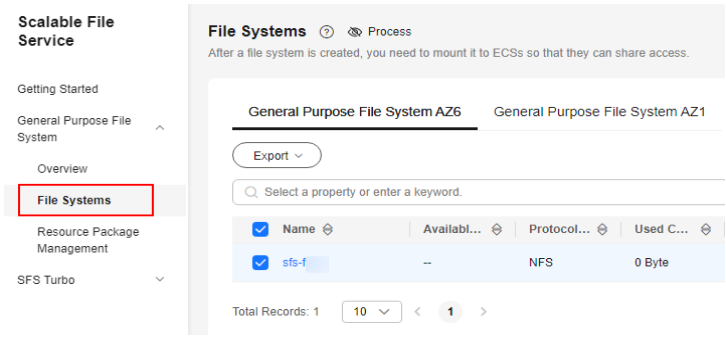
Create a VPC peering connection between the SFS 1.0 file system and the migration cluster. For details, see **Creating a VPC Peering Connection with Another VPC in the Same Account**.

Connecting the Migration Cluster to the Target SFS 3.0 File System

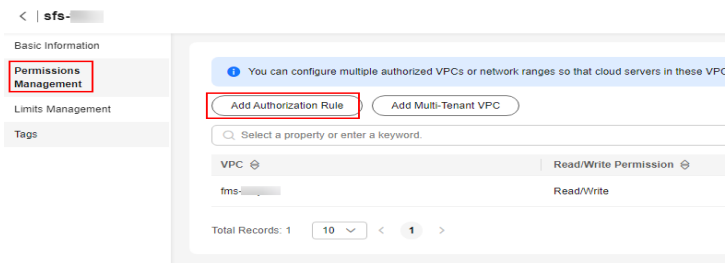
To connect to the target SFS 3.0 file system, you need to configure a VPC endpoint for the VPC where the migration cluster runs.

Step 1 Buy a VPC endpoint by referring to **Configuring a VPC Endpoint**. During the purchase, select the VPC where the **migration cluster** runs.

Step 2 Sign in to the SFS console. In the navigation pane on the left, choose **General Purpose File System** > **File Systems**.



Step 3 Click the name of your file system to go to its details page. In the navigation pane on the left, choose **Permissions Management**. Then click **Add Authorization Rule**.



Step 4 Configure authorization parameters based on the **Table 3-18** and click **OK**.

Table 3-18 Parameters required for creating an authorization rule

Parameter	Configuration
VPC	Select the VPC where the **migration cluster** runs.
Read/Write Permission	Select **Read/Write**.
User Permission	Select **no_root_squash** from the drop-down list.
Authorized Addresses	Select **All IP addresses**.

----End

3.4.5 Creating a Migration Workflow

This section describes how to create a storage migration workflow using the predefined template.

Prerequisites

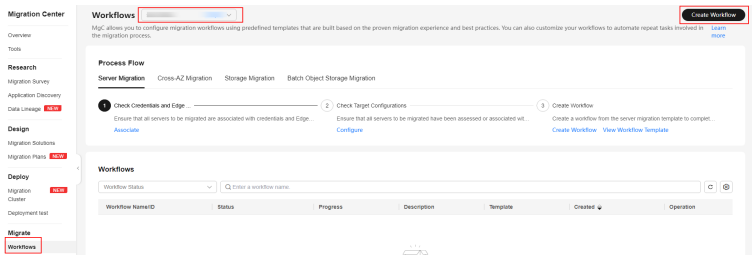
- You have completed operations in **Preparations**.
- You have **created a migration cluster**.
- (Optional) The network among SFS 1.0, SFS 3.0, and the migration cluster has been connected. For details, see **(Optional) Setting Up Network Connections**.

Procedure

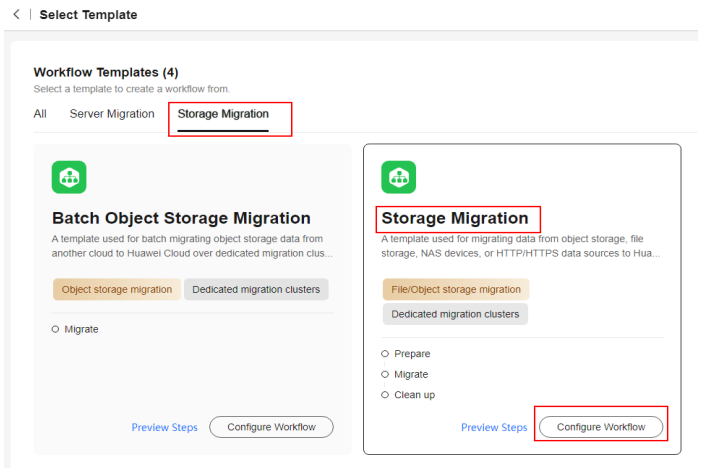
Step 1 Sign in to the **MgC** console.

Step 2 In the navigation pane on the left, choose **Migrate** > **Workflows**. In the upper left corner of the page, select the migration project created in **Preparations**.

Step 3 Click **Create Workflow** in the upper right corner of the page.



Step 4 Select **Storage Migration** and click **Configure Workflow**.



Step 5 Set workflow basics based on **Table 3-19**.

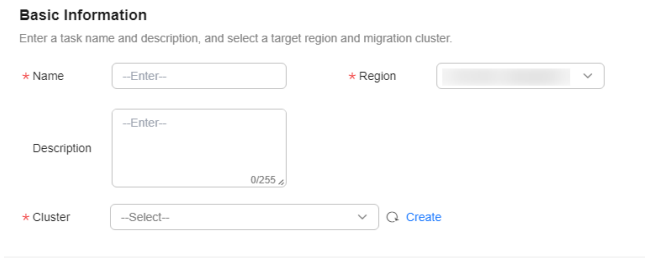


Table 3-19 Basic parameters required for creating a storage migration workflow

Parameter	Description
Name	Enter a workflow name.
Region	Select a region you are migrating to.
Description	Describe the workflow.
Cluster	Select the migration cluster created in **Creating a Migration Cluster**.

Step 6 Configure the migration source and target based on **Table 3-20** and **Table 3-21**.

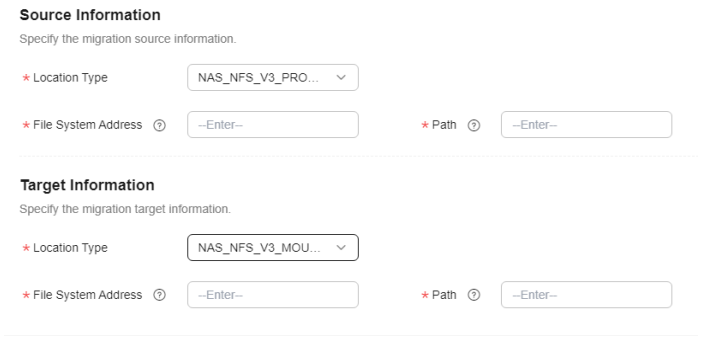
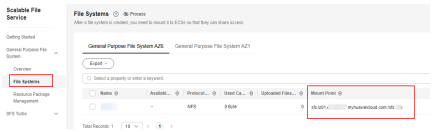


Table 3-20 Parameters for configuring a migration source

Parameter	Description	Remarks
Location Type	Select **NAS_NFS_V3_PROTOCOL**.	-
File System Address	Enter the mount address of the source file system. The format is *IP address*:/ or *IP address*:/*xxx*, for example, 192.1.1.1:/0001.	-
Path	Enter the directory where files to be migrated are located. The format is /*Folder name*.	If you enter /, the entire source file system will be migrated.

Table 3-21 Parameters for configuring a migration target

Parameter	Description	Remarks
Location Type	Select **NAS_NFS_V3_MOUNT**.	-
File System Address	Enter the mount address of the target file system. To obtain the mount address, go to the SFS file system list and click the  icon next to the address in the **Mount Point** column. 	-
Path	Enter the directory for storing files migrated. The format is */Folder name*.	If you enter /, source files will be migrated to the root directory of the target file system.

Step 7 Configure the migration settings based on **Table 3-22**.

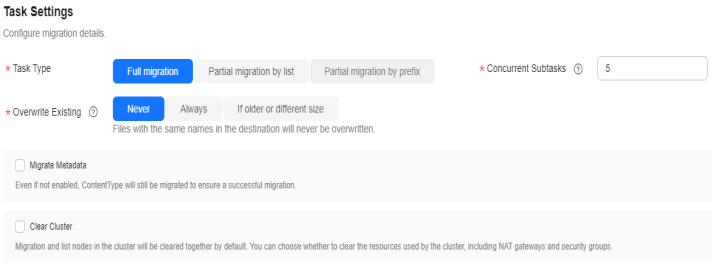


Table 3-22 Parameters for configuring migration settings

Parameter	Option	Description
Task Type	Full migration	Migrates all data in the source bucket or paths specified in **Table 3-20**.
	List migration	Migrates objects recorded in the list files. In **List Path** box, enter the path of the object lists stored in the target bucket. Restrictions on an object list file vary with the target location. • An object list file cannot exceed 30 MB. • An object list file must be a .txt file. • An object list file must be in UTF-8 without BOM. • Each line in an object list file can contain only one object name, and the object name must be URL encoded. • Each line in an object list file cannot exceed 16 KB, or the migration will fail. • An object list file can contain a maximum of 10,000 lines.
Concurrent Subtasks	-	This parameter is user-defined. There cannot be more than 10 concurrent subtasks for each online migration node. For example, if there are 2 online migration nodes, the maximum number of subtasks can be 20 or any number below.

Parameter	Option	Description
Overwrite Existing	Never	Files existing at the migration target are never overwritten. **WARNING** • If you choose **Never** for the initial migration, the attributes of involved parent folders at the source will not be migrated to the target. As a result, the folder attributes may be incomplete at the target. To avoid this issue, use the **Never** option with caution for the initial migration. • If a migration task is paused or interrupted and then restarted or resumed, the **Never** option will cause the system to skip files that were not completely migrated earlier, but the task may still be marked as successful. This affects data integrity. To avoid this issue, use the **Never** option with caution.
	Always	Files existing at the migration target are always overwritten.
	If older or different size	• Files that already exist at the target will be overwritten if they are older than or have different sizes from the paired files at the source. • Verification will be performed for folders after their contents are migrated. Folders that already exist at the target will be overwritten if they have different last modification times, sizes, or permissions from the paired folders at the source. **NOTE** For empty folders, the overwrite policy is the same as that for files.
Migrate Metadata	-	Determine whether to migrate metadata. • If you select this option, object metadata will be migrated. • If you do not select this option, only the Content-Type and Content-Encoding metadata will be migrated.
Clear Cluster	-	Determine whether to clear the migration cluster after the migration is complete. • If you select this option, a step for clearing the migration cluster will be created in the workflow. You can also choose whether to clear resources used by the cluster, such as NAT gateways, security groups, and VPCEP resources. • If you do not select this option, a step for clearing the migration cluster will not be created in the workflow.

Step 8 (Optional) Configure advanced options based on **Table 3-23**.

Table 3-23 Advanced settings

Parameter	Description
Filter Source Data	Filter files to be migrated by applying filters. For details about filters, see **Source Data Filters**.
Send SMN Notification	Determine whether to use SMN to get notifications about migration results. • If you do not select this option, no SMN messages are sent after the migration. • If you select this option, after the migration, SMN messages are sent to the subscribers of the selected topic. You can select the language and trigger conditions for sending messages.
Limit Traffic	Allocate the maximum bandwidth to be used by the workflow during a specified period. • If you do not select this option, migration traffic is not limited. • If you select this option, limit the migration traffic by setting **Start Time**, **End Time**, and **Bandwidth Limit**. For example, if you set **Start Time** to **08:00**, **End Time** to **12:00**, and **Bandwidth Limit** to **20 MB/s**, the maximum migration speed is limited to 20 MB/s from 08:00 to 12:00. The migration speed is not limited beyond this period. **NOTE** – The rate limit ranges from 0 MB/s to 1,048,576 MB/s. – A maximum of five rules can be added. – The time is the local standard time of the region you are migrating to.
Schedule Migration	Schedule the migration to run during a period. • If you do not select this option, you need to manually start or stop the migration. • If you select this option, the migration runs during the specified period and stops beyond that period. Assume that: – If you set **Start Time** to **08:00** and **End Time** to **12:00**, the migration task runs from 08:00 to 12:00 every day. The migration stops beyond that period. – If you set **Start Time** to **12:00** and **End Time** to **08:00**, the migration runs from 12:00 of the current day to 08:00 of the next day. The migration stops beyond that period.

Step 9 Click **Next: Confirm**.

Step 10 Confirm the workflow settings and click **Confirm**. In the displayed dialog box, click **Confirm** to run the workflow immediately.

Step 11 In the workflow list, click the workflow name to go to its details page. You can view the configuration information and migration progress of the workflow.

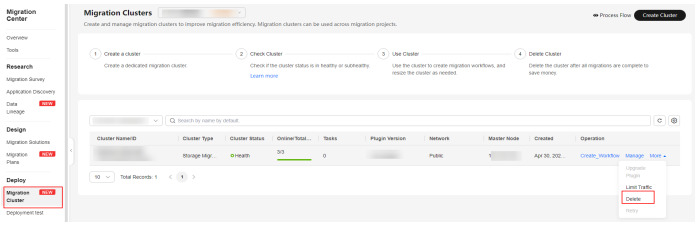
----End

3.4.6 (Optional) Clearing the Migration Cluster

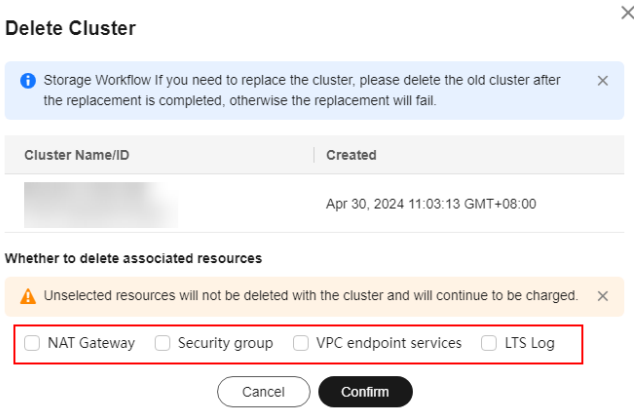
If the migration cluster is no longer needed after your data migration is complete, you can delete the cluster and associated resources.

Step 1 In the left navigation pane, choose **Deploy** > **Migration Clusters**.

Step 2 In the cluster list, locate the cluster to be deleted and choose **More** > **Delete** in the **Operation** column.



Step 3 Select whether to delete associated resources and click **Confirm**.



----End

3.5 Performing a NAS-to-NAS Migration and Service Cutover

Overview

- This solution is applicable to scenarios where source services must keep running during a NAS-to-NAS migration.
- It involves multiple incremental migrations to ensure data accuracy, data consistency, and service continuity.
- The supported source storage types include NAS_SMB, NAS_NFS_V3_MOUNT, NAS_NFS_V3_PROTOCOL, and NAS_GFS.
- The supported target storage types include NAS_SMB and NAS_NFS_V3_MOUNT.

Notes

During the migration, the APIs of the source cloud platform will be called. These API calls might incur fees on the source platform, and you will be responsible for those fees according to the source billing structure.

Process

Step	Description
Preparations	• Sign up for a HUAWEI ID, enable Huawei Cloud services, and top up your account. • Obtain the required permissions for the source and target accounts. • Obtain an AK/SK pair for the target account. • Create a migration project on the MgC console. • Create a migration cluster on the MgC console. • Prepare a file system in the target region.
Step 1: Create a Full Migration Workflow	Create a migration workflow on the MgC console to fully migrate source data.
Step 2: Create an Incremental Migration Workflow	Create a migration workflow and execute it multiple times to migrate incremental data.
Step 3: (Optional) Switch Gray Traffic	If possible, switch gray traffic to the target to verify service continuity and data consistency.
Step 4: Perform a Service Cutover	After multiple incremental migrations are complete, identify an optimal time window for the final incremental migration and the final service cutover.

Preparations

- Preparing a Huawei account

  Before using MgC, prepare a HUAWEI ID or an IAM user that can access MgC and obtain an AK/SK pair for the account or IAM user. For details, see **Making Preparations**.

- Creating a migration project

  Create a migration project on the MgC console. For details, see **Managing Migration Projects**.

- Creating a migration cluster

  Create a dedicated migration cluster for this migration. For details, see **Creating a Cluster**.

- Creating an SFS file system

  Create a file system for storing migrated data. For details, see **Creating a File System**.

Step 1: Create a Full Migration Workflow

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

Step 2 In the navigation pane on the left, choose **Migrate** > **Workflows**. In the upper left corner of the page, select the migration project created in **Preparations**.

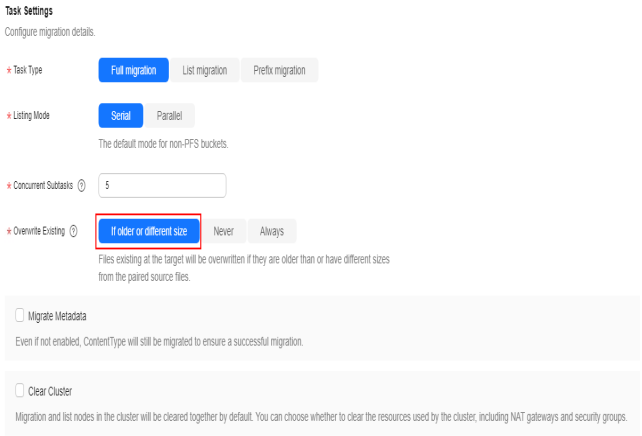
Step 3 **Create a workflow** to perform a full migration.

----End

Step 2: Create an Incremental Migration Workflow

After the full migration is complete, **create a workflow** to perform incremental migrations. For this workflow, set **Overwrite Existing** to **If older or different size** and retain all other parameters as they were in the workflow created in **step 1**. After the configuration is complete, run this workflow to start an incremental migration.

Figure 3-8 Choosing how to overwrite existing files



Step 3: (Optional) Switch Gray Traffic

After the first incremental migration is complete, if possible, switch gray traffic to the target to verify services.

Step 4: Perform a Service Cutover

After completing multiple incremental migrations, schedule a window for the final service cutover. Stop services at the source, complete the last incremental migration, and transition service traffic to the target.

3.6 Migrating File Systems in Batches

This section describes how to use MgC to efficiently migrate file systems in batches.

- The supported source storage types include NAS_NFS_V3_MOUNT, NAS_NFS_V3_PROTOCOL, and NAS_GFS.

- The supported target storage type includes NAS_NFS_V3_MOUNT.

Notes and Constraints

For details, see **What Are the Restrictions on Using MgC for Storage Migration?**

Preparations

- Preparing a Huawei account

  Before using MgC, prepare a HUAWEI ID or an IAM user that can access MgC. For details, see **Making Preparations**.
- Creating a migration project

  Create a migration project on the MgC console. For details, see **Managing Migration Projects**.
- Preparing file systems in the target region.

  Create target file systems for receiving migrated source data. For details, see **Creating a General Purpose File System** or **Creating an SFS Turbo File System**.

Step 1: Create a Migration Cluster

You can create dedicated migration clusters to accelerate storage migration. A migration cluster consists of nodes that have the migration plugin installed and are used to execute migration and listing tasks. Create a dedicated migration cluster for this migration. For details, see **Creating a Cluster**.

Step 2: Create a File Storage Migration Plan

Create a migration plan to include all the source file systems that need to be migrated the same target region. In the plan, configure a target file system for each source file system and specify the migration cluster to be used. For details, see **Creating a Batch File Storage Migration Plan**.

Step 3: Create a Migration Workflow

When you create a migration workflow, select the migration plan you created and define the migration settings. For details, see **Creating a Batch File Storage Migration Workflow**.

3.7 Migrating Data from MinIO to Huawei Cloud OBS over HTTP

Use MgC storage migration workflows to migrate data from MinIO to Huawei Cloud OBS over HTTP.

Supported Regions

The following regions are supported:

- LA-Santiago
- LA-Sao Paulo
- TR-Istanbul
- AP-Bangkok
- AP-Singapore
- AP-Jakarta
- ME-Riyadh
- CN North-Beijing4
- CN East-Shanghai1

CAUTION

A single object cannot be larger than 4.76837158203125 TB (500 MB x 10,000). Otherwise, the migration may fail.

Preparations

- Preparing a Huawei account

  Before using MgC, prepare a HUAWEI ID or an IAM user that can access MgC and obtain an AK/SK pair for the account or IAM user. For details about how to obtain an access key, see **Making Preparations**.

- Creating a migration project

  On the MgC console, create a migration project. For details, see **Managing Migration Projects**.

- Creating an OBS Bucket

  On Huawei Cloud OBS, create a Standard bucket in the target region for storing URL list files and receiving source data. For details, see **Creating a Bucket**.

  If an IAM user is used for migration, the IAM user must have the read and write permissions for the target bucket. For details, see **Granting an IAM User the Read/Write Permissions for a Bucket**.

- Creating a migration cluster

  You can create a dedicated migration cluster for this task. A cluster consists of a master node and several list and migration nodes. For details about how to create a cluster, see **Creating a Migration Cluster**.

Step 1: Generate URLs for Sharing and Downloading MinIO Files

Replace **minioLink**, **bucket-public01**, and **http://100.85.xxx.xx:xxxx** in the following steps with the actual MinIO alias, bucket name, and access address.

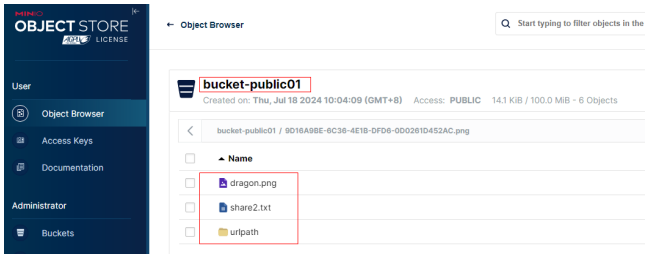
Step 1 Open the CLI on the server where MinIO is deployed.

Step 2 Run the mc command to share file and generate URLs for downloading the file. The command format is as follows:

```
mc share download --recursive --expire=<EXPIRE-IN-HOURS> <MINIO-ALIAS>/<BUCKET-NAME>/
```


- **--recursive**: recursively shares files in all subdirectories.
- **--expire=**<EXPIRE-IN-HOURS>: The expiration time of the share URLs, in hours. The maximum duration is 7 days (168 hours).
- <MINIO-ALIAS>: user-defined alias of the MinIO service deployment.
- **<BUCKET-NAME>**: bucket name

For example, you have a bucket named **bucket-public01**. The bucket contains two files (**dragon.png** and **share2.txt**) and one subfolder (**urlpath**). The subfolder contains one file (**share2.txt**).



Assume that you want to generate URLs for sharing and downloading all files in the bucket, set the URLs to expire after 12 hours, and save the URLs in the **test2.txt** file. You can run the following command:

```
mc share download --recursive --expire=12h minioLink/bucket-public01/ >> test2.txt
```

After the command is executed, the share URLs of the three files are generated and saved in the **test2.txt** file.

```
[root@oms-cluster-ecs-1797559186613161988-d32e ~]# mc share download --recursive --expire=12h minioLink/bucket-public01/
URL: http://1          000/bucket-public01/dragon.png
Expire: 12 hours 0 minutes 0 seconds
Share: http://100.85.118.88:9000/bucket-public01/dragon.png?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=admin%2F20240724
24T090221Z&X-Amz-Expires=43200&X-Amz-SignedHeaders=host&X-Amz-Signature=80df3a76c21afb74ebb9cfd151cd84934c9c7e4a1c47c901a10a86

URL: http://1          00/bucket-public01/share2.txt
Expire: 12 hours 0 minutes 0 seconds
Share: http://100.85.118.88:9000/bucket-public01/share2.txt?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=admin%2F20240724
24T090221Z&X-Amz-Expires=43200&X-Amz-SignedHeaders=host&X-Amz-Signature=7c183cedc0b4a8455b7bf2753c86c3938b7b7b5ffe22f020f29b1f

URL: http://           00/bucket-public01/urlpath/share2.txt
Expire: 12 hours 0 minutes 0 seconds
Share: http://100.85.118.88:9000/bucket-public01/urlpath/share2.txt?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=admin%2F
e=20240724T090221Z&X-Amz-Expires=43200&X-Amz-SignedHeaders=host&X-Amz-Signature=63c322ca1594fe7abe2f500fd3e42d208a7581921cd728
```

Step 3 Open the generated URL list file (**test2.txt** in this example) and you will see the share URL for each file. Try to access these URLs using a browser to check whether the URLs are valid.

If any URLs cannot be accessed, check whether the corresponding files are readable. If they are, generate URLs for them again.

Step 4 Based on the MgC requirements, edit the URL list file to include the shared URLs and file names in the following format:

```
<SHARED-URL> <FILE-NAME>
```

A shared URL and file name are separated by a tab character. The name of a file in a subfolder must contain the subfolder name.. For more requirements

and restrictions on the URL list file, see **What Are the Restrictions on Using MgC for Storage Migration?**

For example:

```
http://100.85.xxx.xx:xxxx/bucket-public01/dragon.png dragon.png
http://100.85.xxx.xx:xxxx/bucket-public01/share2.txt share2.txt
http://100.85..xxx.xx:xxxx/bucket-public01/urlpath/share2.txt urlpath/share2.txt
```

Step 5 After editing all URLs as required and verifying that the URLs are correct, save the URL list file.

----End

Step 2: Upload the URL List File to the OBS Bucket

Step 1 Sign in to the **OBS console**. In the navigation pane, choose **Buckets**.

Step 2 In the bucket list, click **the created OBS bucket** to go to the **Objects** page.

Step 3 Click **Create Folder**, enter a folder name (for example, **minioUrl**), and click **OK**.

Step 4 Click the name of the folder created in the previous step. Click **Upload Object**.

Step 5 Upload the **URL list file** (**test2.txt** in this example) to the folder in either of the following ways:

- Drag the URL list file to the **Upload Object** box and click **Upload**.
- In the **Upload Object** box, click **add files**, select the URL list file, and click **Upload**.

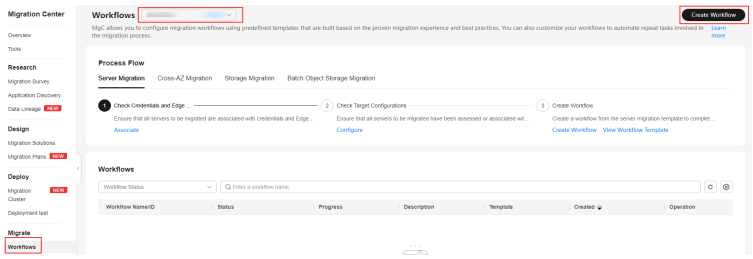
----End

Step 3: Create a Storage Migration Workflow

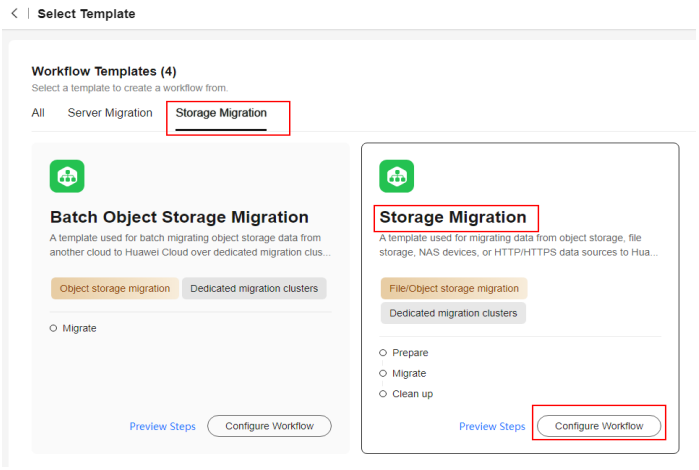
Step 1 Sign in to the **MgC console**.

Step 2 In the navigation pane on the left, choose **Migrate** > **Workflows**. In the upper left corner of the page, select the **migration project you created**.

Step 3 Click **Create Workflow** in the upper right corner of the page.



Step 4 Select **Storage Migration** and click **Configure Workflow**.



Step 5 Set workflow basics based on **Table 3-24**.

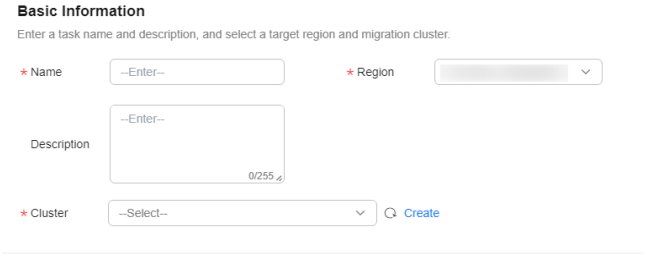


Table 3-24 Basic parameters

Parameter	Description
Name	User-defined
Region	Select the region where the **target bucket** is located from the drop-down list.
Description	User-defined
Cluster	Select the **created cluster**.

Step 6 Configure the migration source and target based on **Table 3-25** and **Table 3-26**.

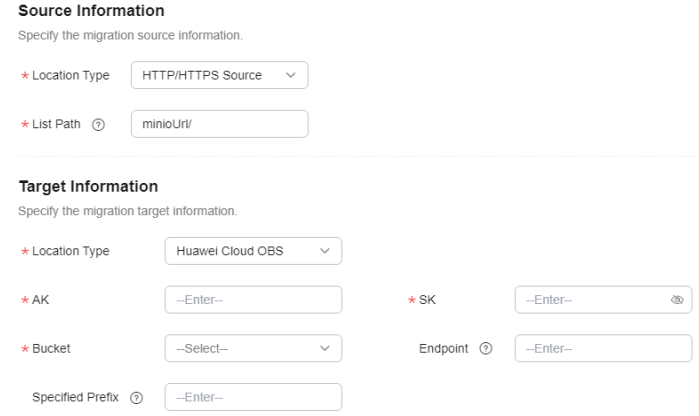


Table 3-25 Parameters for configuring a migration source

Parameter	Description
Location Type	Select **HTTP/HTTPS Source**.
List Path	Enter the name of the folder (**minioUrl/** in this example) where the **URL list file** is stored. Note that the folder name must be suffixed with a slash (/).

Table 3-26 Parameters for configuring a migration target

Parameter	Description
Location Type	Select **Huawei Cloud OBS**.
AK	Enter the AK/SK pair of the target Huawei Cloud account. The account must have the read and write permissions for the target bucket.
SK	
Bucket	Select the **created OBS bucket**.
Endpoint	Enter the endpoint of the region where the target bucket is located. For example, if the target bucket is located in the **CN North-Beijing4** region of Huawei Cloud, enter **obs.cn-north-4.myhuaweicloud.com**. **NOTE** You can view the endpoint in the OBS bucket overview.
Specify Prefix	This parameter is optional. Specify a prefix to rename or relocate objects migrated to the target bucket. For example, if you specify the prefix **/D**, source file **/A/B/C.txt** will be relocated to **/D/A/B/C.txt** after being migrated to the target bucket. For details, see: **Adding a Name Prefix or Path Prefix to Migrated Objects**

Step 7 Configure the migration settings based on **Table 3-27**.

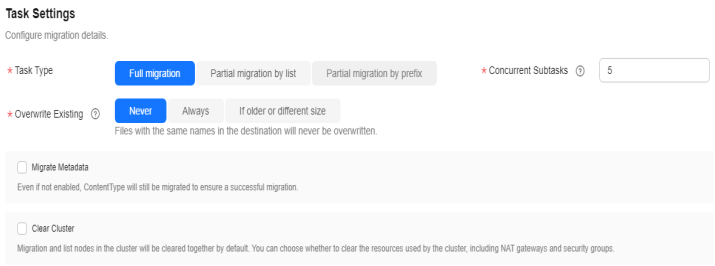


Table 3-27 Migration settings

Parameter	Option	Description
Task Type	List migration	Migrates objects recorded in the list files.
Concurrent Subtasks	-	Specify the maximum number of concurrent subtasks. There cannot be more than 10 concurrent subtasks for each online migration node. For example, if there are 2 online migration nodes, the maximum number of subtasks can be 20 or any number below.
Overwrite Existing	Never	Files existing at the migration target will never be overwritten. **WARNING** • If you choose **Never** for the initial migration, the attributes of involved parent folders at the source will not be migrated to the target. As a result, the folder attributes may be incomplete at the target. To avoid this issue, use the **Never** option with caution for the initial migration. • If a migration task is paused or interrupted and then restarted or resumed, the **Never** option will cause the system to skip files that were not completely migrated earlier, but the task may still be marked as successful. This affects data integrity. To avoid this issue, use the **Never** option with caution.
	Always	Files existing at the migration target will always be overwritten.
	If older or different size	• Files that already exist at the target will be overwritten if they are older than or have different sizes from the paired files at the source. • Verification will be performed for folders after their contents are migrated. Folders that already exist at the target will be overwritten if they have different last modification times, sizes, or permissions from the paired folders at the source. **NOTE** For empty folders, the overwrite policy is the same as that for files.
Clear Cluster	-	Determine whether to clear the migration cluster after the migration is complete. • If you select this option, a step for clearing the migration cluster will be created in the workflow. You can also choose whether to clear resources used by the cluster, such as NAT gateways, security groups, and VPCEP resources. • If you do not select this option, a step for clearing the migration cluster will not be created in the workflow.

Step 8 (Optional) Configure advanced options based on **Table 3-28**.

Table 3-28 Advanced options

Parameter	Description
Target Storage Class	Choose the storage class that your data will be migrated to in the target bucket. For details about storage classes, see **Introduction to Storage Classes**.
Enable KMS Encryption	• If you do not select this option, whether migrated data will be encrypted in the target bucket depends on the server-side encryption setting of the bucket. • If you select this option, all migrated objects will be encrypted before they are stored in the target bucket. **NOTE** • Using KMS to encrypt migrated data may slow down the migration speed by about 10%. • This option is only available when KMS is supported in the region you are migrating to.
Filter Source Data	Filter files to be migrated by applying filters. For details about filters, see **Source Data Filters**.
Send SMN Notification	Determine whether to use SMN to get notifications about migration results. • If you do not select this option, no SMN messages are sent after the migration is complete. • If you select this option, after the migration is complete, SMN messages are sent to the subscribers of the selected topic. You can select the language and trigger conditions for sending messages.
Limit Traffic	Allocate the maximum bandwidth to be used by the workflow during a specified period. • If you do not select this option, migration traffic is not limited. • If you select this option, limit the migration traffic by setting **Start Time**, **End Time**, and **Bandwidth Limit**. For example, if you set **Start Time** to **08:00**, **End Time** to **12:00**, and **Bandwidth Limit** to **20 MB/s**, the maximum migration speed is limited to 20 MB/s from 08:00 to 12:00. The migration speed is not limited beyond this period. **NOTE** – The rate limit ranges from 0 MB/s to 1,048,576 MB/s. – A maximum of five rules can be added. – The time is the local standard time of the region you are migrating to.

Parameter	Description
Schedule Migration	Schedule the migration to run during a period. • If you do not select this option, you need to manually start or stop the migration. • If you select this option, the migration runs during the specified period and stops beyond that period. For example: – If you set **Start Time** to **08:00** and **End Time** to **12:00**, the migration task runs from 08:00 to 12:00 every day. The migration stops beyond that period. – If you set **Start Time** to **12:00** and **End Time** to **08:00**, the migration runs from 12:00 of the current day to 08:00 of the next day. The migration stops beyond that period.

Step 9 Click **Next: Confirm**.

Step 10 Confirm the workflow settings and click **Confirm**. In the displayed dialog box, click **Confirm** to run the workflow immediately.

Step 11 In the workflow list, click the workflow name to go to its details page. You can view the configuration information and migration progress of the workflow.

----End

3.8 Migrating Data from Ceph to Huawei Cloud OBS over HTTP

Use MgC storage migration workflows to migrate data from Ceph to Huawei Cloud OBS over HTTP.

Supported Regions

The following regions are supported:

- LA-Santiago
- LA-Sao Paulo
- TR-Istanbul
- AP-Bangkok
- AP-Singapore
- AP-Jakarta
- ME-Riyadh
- CN North-Beijing4
- CN East-Shanghai1

> **CAUTION**
>
> A single object cannot be larger than 4.76837158203125 TB (500 MB x 10,000). Otherwise, the migration may fail.

Preparations

- Preparing a Huawei account

  Before using MgC, prepare a HUAWEI ID or an IAM user that can access MgC and obtain an AK/SK pair for the account or IAM user. For details about how to obtain an access key, see **Making Preparations**.

- Creating a migration project

  On the MgC console, create a migration project. For details, see **Managing Migration Projects**.

- Creating an OBS bucket

  On Huawei Cloud OBS, create a Standard bucket in the target region for storing URL list files and receiving source data. For details, see **Creating a Bucket**.

  If an IAM user is used for migration, the IAM user must have the read and write permissions for the target bucket. For details, see **Granting an IAM User the Read/Write Permissions for a Bucket**.

- Creating a migration cluster

  You can create a dedicated migration cluster for this task. A cluster consists of a master node and several list and migration nodes. For details about how to create a cluster, see **Creating a Migration Cluster**.

Step 1: Generate URLs for Sharing and Downloading Ceph Files

Replace **bucket01** and **http://100.93.xxx.xx:7480** in the following steps with the actual Ceph S3 bucket name and Ceph RGW web access address and port.

Replace the following parameters in the example with the actual values:

- <BUCKET-NAME>: bucket name
- < FILE-NAME >: name of the JSON file to be created
- <DOMAIN>: actual domain name or IP address of the Ceph RGW (RADOS Gateway) service.
- <PORT>: actual access port of the Ceph RGW service.

If data in the bucket to be migrated can be accessed using a browser, skip step 1 and go to **step 2**.

Step 1 Run the following command to check whether an access policy has been configured for the source bucket:

```
s3cmd info s3://<BUCKET-NAME>
```

- If the value of **Policy** is **none** in the command output, no access policy is configured for the bucket. Go to step **2**.


```
s3://bucket01/ (bucket):
   Location:  default
   Payer:     BucketOwner
   Expiration Rule: none
   Policy:    none
   CORS:      none
   ACL:       admin: FULL_CONTROL
```

- If the value of **Policy** is not **none** in the command output, copy and save the policy information for restoring the policy after data migration.

```
s3://bucket01/ (bucket):
   Location:  default
   Payer:     BucketOwner
   Expiration Rule: none
   Policy:    {
        "Statement": [{
                "Effect":
                "Principal
                "Action":
                "Resource"
        }]
}

   CORS:      none
   ACL:       admin: FULL_CONTROL
```

Step 2 On the server where the s3cmd tool is installed, open the text editor and create a JSON file (with a user-defined name). The file contains the S3 bucket policy, which allows objects to be obtained from the specified S3 bucket. Copy the following content to the editor, replace <BUCKET-NAME> with the actual S3 bucket name, save the JSON file, and exit the editor.

```
{
    "Statement": [{
        "Effect": "Allow" ,
        "Principal": "*",
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3::: <BUCKET-NAME>/*"
    }]
}
```

For more parameter settings, see **Example Amazon S3 Bucket Policies**.

Step 3 Use the s3cmd command line tool to set a bucket policy that allows public access to the files in the bucket. The command is in the following format:

```
s3cmd setpolicy <FILE-NAME>.json s3://<BUCKET-NAME>
```

Replace <FILE-NAME> with the name of the JSON file created in **step 2** and <BUCKET-NAME> with the actual S3 bucket name.

Step 4 Run the following command to list all files in the bucket and export the result to a text file:

```
s3cmd ls -r s3://<BUCKET-NAME> >> <FILE-URL>.txt
```

Replace <BUCKET-NAME> with the actual S3 bucket name and <FILE-URL> with the name of the local file that you want to save the result to, for example, **s3url.txt**.

Step 5 Open the generated list file (**s3url.txt** in this example) to view the list of shared S3 addresses of all files in the bucket. Replace **s3://** and all parameters before it with **http://**<DOMAIN>:<PORT>/ to generate URLs that can be accessed using a browser. Enter a URL in the address box of the browser. If the file can be accessed,

the setting is correct. If the access is denied and AccessDenied is returned, repeat **step 1** to **step 4** to set the access policy.

For example, the actual domain name or IP address of the Ceph RGW service is 100.93.xxx.xx, the port number is 7480, the bucket name is **bucket01**, there are two files (**dragon.png** and **index.html**) in the bucket, and the generated shared S3 address list is as follows:

```
2024-07-26 03:09      3987  s3://bucket01/dragon.png
2024-07-26 02:01      1701  s3://bucket01/index.html
```

Replace **s3://** and all parameters before it with **http://**<DOMAIN>:<PORT>/, that is, replace the content from *Date* to **s3://** with **http://100.93.xxx.xxx:7480**. Then the generated URL list is as follows:

```
http://100.93.xxx.xxx:7480/bucket01/dragon.png
http://100.93.xxx.xxx:7480/bucket01/index.html
```

Step 6 According to the method and requirements in the previous step, replace all shared S3 addresses in the list file with URLs. If there are a large number of S3 addresses in the list file, you can use a text editor (such as NotePad++) to replace them in batches.

Step 7 Based on the MgC requirements, edit the URL list file to include the shared URLs and file names in the following format:

```
<SHARED-URL> <FILE-NAME>
```

A shared URL and file name are separated by a tab character. The name of a file in a subfolder must contain the subfolder name.. For more requirements and restrictions on the URL list file, see **What Are the Restrictions on Using MgC for Storage Migration?**

For example:

```
http://100.93.xxx.xxx:7480/bucket01/dragon.png dragon.png
http://100.93.xxx.xxx:7480/bucket01/index.html index.html
```

Step 8 After editing all URLs as required and verifying that the URLs are correct, save the URL list file.

----End

Step 2: Upload the URL List File to the OBS Bucket

Step 1 Sign in to the **OBS console**. In the navigation pane, choose **Buckets**.

Step 2 In the bucket list, click **the created OBS bucket** to go to the **Objects** page.

Step 3 Click **Create Folder**, enter a folder name (for example, **cephUrl**), and click **OK**.

Step 4 Click the name of the folder created in the previous step. Click **Upload Object**.

Step 5 Upload the **URL list file** (**s3url.txt** in this example) to the folder in either of the following ways:

- Drag the URL list file to the **Upload Object** box and click **Upload**.
- In the **Upload Object** box, click **add files**, select the URL list file, and click **Upload**.

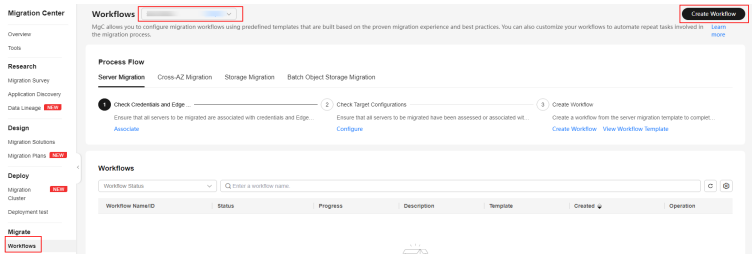
----End

Step 3: Create a Storage Migration Workflow

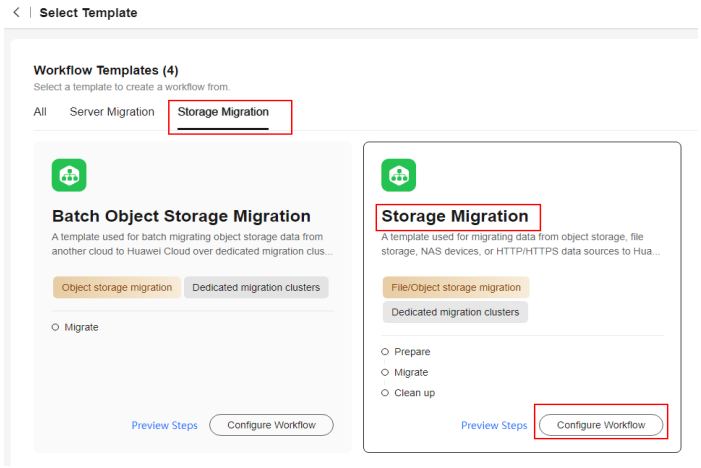
Step 1 Sign in to the **MgC console**.

Step 2 In the navigation pane on the left, choose **Migrate** > **Workflows**. In the upper left corner of the page, select the **migration project you created**.

Step 3 Click **Create Workflow** in the upper right corner of the page.



Step 4 Select **Storage Migration** and click **Configure Workflow**.



Step 5 Set workflow basics based on **Table 3-29**.

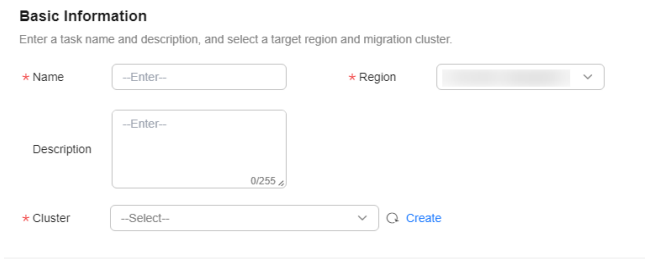


Table 3-29 Basic parameters

Parameter	Description
Name	User-defined
Region	Select the region where the **target bucket** is located from the drop-down list.
Description	User-defined

Parameter	Description
Cluster	Select the **created cluster**.

Step 6 Configure the migration source and target based on **Table 3-30** and **Table 3-31**.

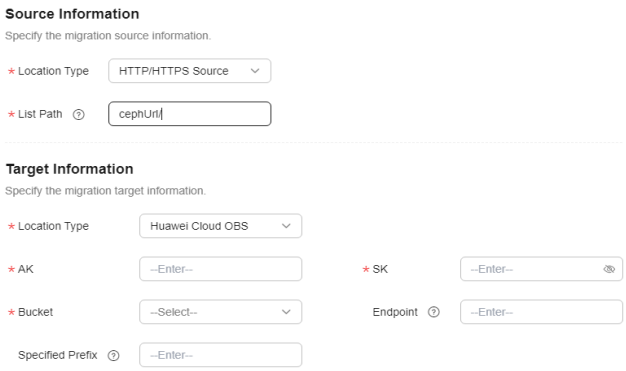


Table 3-30 Parameters for configuring a migration source

Parameter	Description
Location Type	Select **HTTP/HTTPS Source**.
List Path	Enter the name of the folder (**cephUrl/** in this example) where the **URL list file** is stored. Note that the folder name must be suffixed with a slash (/).

Table 3-31 Parameters for configuring a migration target

Parameter	Description
Location Type	Select **Huawei Cloud OBS**.
AK	Enter the AK/SK pair of the target Huawei Cloud account. The account must have the read and write permissions for the target bucket.
SK	
Bucket	Select the **created OBS bucket**.
Endpoint	Enter the endpoint of the region where the target bucket is located. For example, if the target bucket is located in the **CN North-Beijing4** region of Huawei Cloud, enter **obs.cn-north-4.myhuaweicloud.com**. **NOTE** You can view the endpoint in the OBS bucket overview.

Parameter	Description
Specify Prefix	This parameter is optional. Specify a prefix to rename or relocate objects migrated to the target bucket. For example, if you specify the prefix **/D**, source file **/A/B/C.txt** will be relocated to **/D/A/B/C.txt** after being migrated to the target bucket. For details, see: **Adding a Name Prefix or Path Prefix to Migrated Objects**

Step 7 Configure the migration settings based on **Table 3-32**.

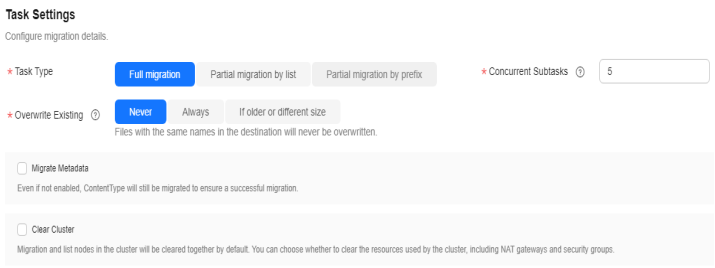


Table 3-32 Migration settings

Parameter	Option	Description
Task Type	List migration	Migrates objects recorded in the list files.
Concurrent Subtasks	-	Specify the maximum number of concurrent subtasks. There cannot be more than 10 concurrent subtasks for each online migration node. For example, if there are 2 online migration nodes, the maximum number of subtasks can be 20 or any number below.
Overwrite Existing	Never	Files existing at the migration target will never be overwritten. **WARNING** • If you choose **Never** for the initial migration, the attributes of involved parent folders at the source will not be migrated to the target. As a result, the folder attributes may be incomplete at the target. To avoid this issue, use the **Never** option with caution for the initial migration. • If a migration task is paused or interrupted and then restarted or resumed, the **Never** option will cause the system to skip files that were not completely migrated earlier, but the task may still be marked as successful. This affects data integrity. To avoid this issue, use the **Never** option with caution.

Parameter	Option	Description
	Always	Files existing at the migration target will always be overwritten.
	If older or different size	• Files that already exist at the target will be overwritten if they are older than or have different sizes from the paired files at the source. • Verification will be performed for folders after their contents are migrated. Folders that already exist at the target will be overwritten if they have different last modification times, sizes, or permissions from the paired folders at the source. **NOTE** For empty folders, the overwrite policy is the same as that for files.
Clear Cluster	-	Determine whether to clear the migration cluster after the migration is complete. • If you select this option, a step for clearing the migration cluster will be created in the workflow. You can also choose whether to clear resources used by the cluster, such as NAT gateways, security groups, and VPCEP resources. • If you do not select this option, a step for clearing the migration cluster will not be created in the workflow.

Step 8 (Optional) Configure advanced options based on **Table 3-33**.

Table 3-33 Advanced options

Parameter	Description
Target Storage Class	Choose the storage class that your data will be migrated to in the target bucket. For details about storage classes, see **Introduction to Storage Classes**.
Enable KMS Encryption	• If you do not select this option, whether migrated data will be encrypted in the target bucket depends on the server-side encryption setting of the bucket. • If you select this option, all migrated objects will be encrypted before they are stored in the target bucket. **NOTE** • Using KMS to encrypt migrated data may slow down the migration speed by about 10%. • This option is only available when KMS is supported in the region you are migrating to.
Filter Source Data	Filter files to be migrated by applying filters. For details about filters, see **Source Data Filters**.

Parameter	Description
Send SMN Notification	Determine whether to use SMN to get notifications about migration results. ● If you do not select this option, no SMN messages are sent after the migration is complete. ● If you select this option, after the migration is complete, SMN messages are sent to the subscribers of the selected topic. You can select the language and trigger conditions for sending messages.
Limit Traffic	Allocate the maximum bandwidth to be used by the workflow during a specified period. ● If you do not select this option, migration traffic is not limited. ● If you select this option, limit the migration traffic by setting **Start Time**, **End Time**, and **Bandwidth Limit**. For example, if you set **Start Time** to **08:00**, **End Time** to **12:00**, and **Bandwidth Limit** to **20 MB/s**, the maximum migration speed is limited to 20 MB/s from 08:00 to 12:00. The migration speed is not limited beyond this period. **NOTE** – The rate limit ranges from 0 MB/s to 1,048,576 MB/s. – A maximum of five rules can be added. – The time is the local standard time of the region you are migrating to.
Schedule Migration	Schedule the migration to run during a period. ● If you do not select this option, you need to manually start or stop the migration. ● If you select this option, the migration runs during the specified period and stops beyond that period. For example: – If you set **Start Time** to **08:00** and **End Time** to **12:00**, the migration task runs from 08:00 to 12:00 every day. The migration stops beyond that period. – If you set **Start Time** to **12:00** and **End Time** to **08:00**, the migration runs from 12:00 of the current day to 08:00 of the next day. The migration stops beyond that period.

Step 9 Click **Next: Confirm**.

Step 10 Confirm the workflow settings and click **Confirm**. In the displayed dialog box, click **Confirm** to run the workflow immediately.

Step 11 In the workflow list, click the workflow name to go to its details page. You can view the configuration information and migration progress of the workflow.

----End

Step 4: Restore the Bucket Access Policy

After the migration is complete, restore the access policy of the source bucket.

- If the command output in **step 1** is **Policy: none**, run the following command to delete the added public access policy:
  ```
  s3cmd delpolicy s3://<BUCKET-NAME>
  ```
- If the command output in **step 1** contains an access policy, perform the following steps:
  a. Run the following command to delete the added public access policy:
     ```
     s3cmd delpolicy s3://<BUCKET-NAME>
     ```
  b. Run the following command to restore the access policy to the original one:
     ```
     s3cmd setpolicy <Saved original policy>.json s3://<BUCKET-NAME>
     ```


4 Reducing Disk Capacity for Target Servers

MgC enables you to reduce disk capacity and quantity for target servers based on the disk usage of source servers. This helps you reduce storage costs.

Precautions

- The system disk capacity ranges from 40 GB to 1,024 GB.
- The data disk capacity ranges from 10 GB to 32,768 GB.
- Only Linux disk sizes can be decreased, and decreased sizes must be larger than the used sizes of source disks.
- In the cross-AZ migration scenario, disk sizes can only be increased. Even if you decrease disk sizes here, the settings will not be applied, and the system will create target disks as large as source disks.

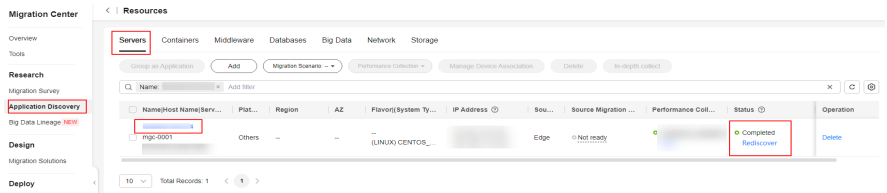
Collecting Disk Information of Source Servers

You need to collect the disk information of source servers and then, against the collected information, reduce disk capacity for target servers.

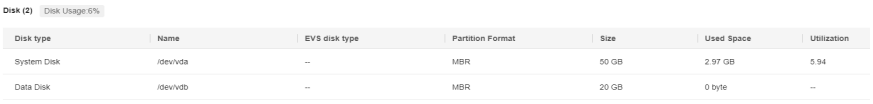
Step 1 Select a collection method based on your requirements.

- **Discovering Resources over the Internet**
- **Discovering Resources over an Intranet**
- **Manually Adding Resources to MgC**

Step 2 Wait for the resource discovery and deep collection to complete. View the server list on the **Resources** page and click a source server.



Step 3 In the disk information area, view the number and usage of disks on the source server. Based on the information, you can adjust disk settings for paired target servers.



----End

Associating Source Servers with Target Servers and Reducing Disk Capacity for Target Servers

Step 1 In the navigation pane on the left, choose **Design** > **Migration Solutions**.

Step 2 Click **View Resources** in the **Target Configuration** card.

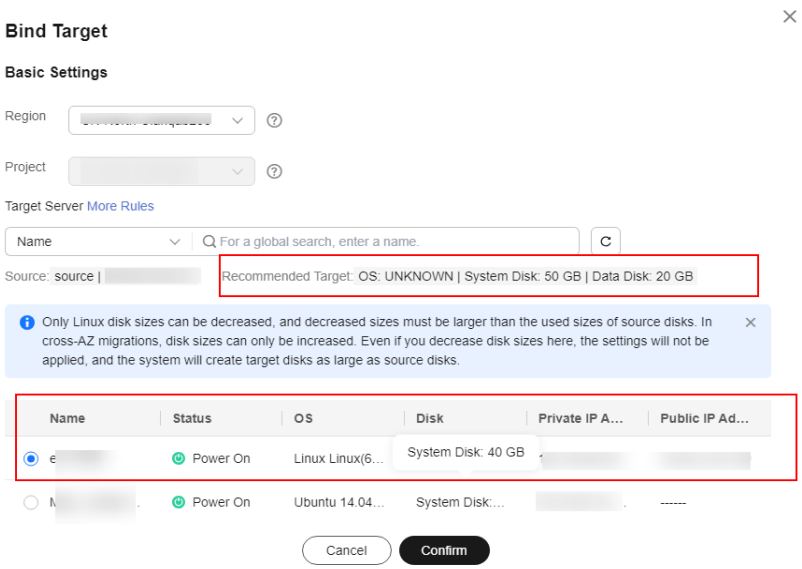
Step 3 On the displayed **Servers** tab, locate a source server and click **Associate** in the **Target Association** column.

Step 4 Select the region of the **application** that the source server was added to, and select a project in that region. In the project, select a target server based on the **collected disk information of the source server** and your requirements.

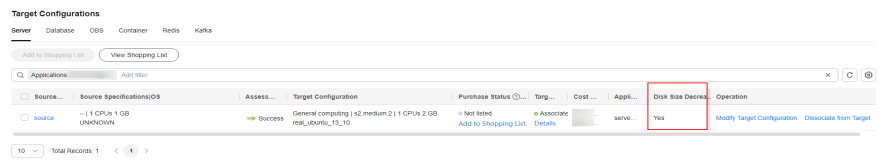
CAUTION

Ensure that the disk capacity of the selected target server is greater than the used disk capacity of the source server.

Assume the source server has a 50 GB system disk with a little space used and a 20 GB data disk that is unused at all. You can associate a target server containing only a 40 GB system disk with the source server.

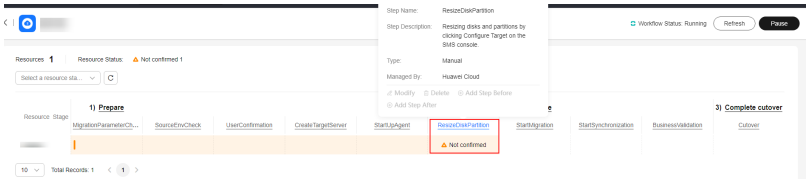


Step 5 Click **Confirm**. The system will automatically check whether the associated target server has downsized disks compared with the source server. If it does, **Yes** will be displayed in the **Disk Downsized** column. If it does not, **No** will be displayed.



Step 6 **Create a server migration workflow**. When the workflow reaches the **ResizeDiskPartition** step, the system identifies whether disk capacity reduction has been performed on the target server.

- If yes, this step is paused. You need to go to **SMS console** and resize disks and partitions for the target server. For details, see **Resizing Disks and Partitions for Target Servers**. After the adjustment is complete, go back to the MgC console and click **Confirm** next to the step status so that the workflow can continue.



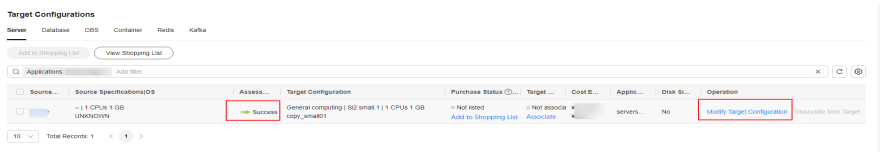
- If no, skip this step and proceed with the subsequent migration steps.

----End

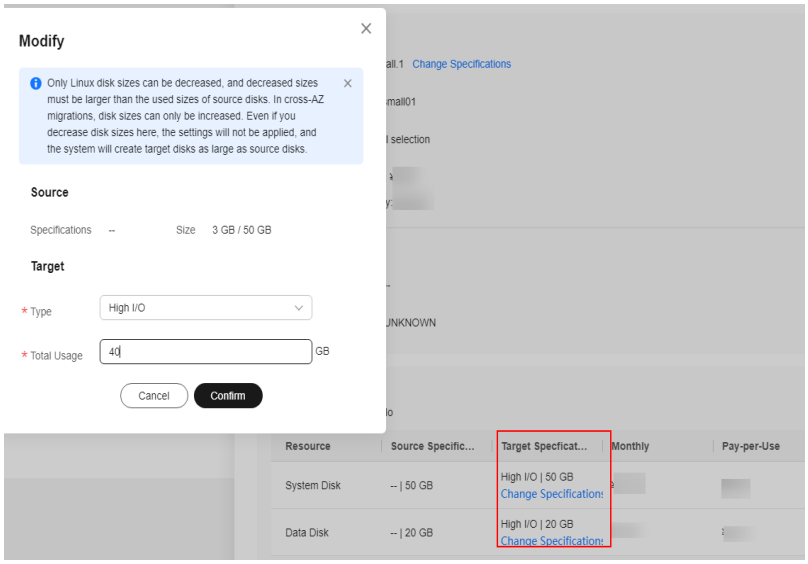
Getting Target Server Recommendations and Reducing Disk Capacity for Target Servers

Step 1 Get recommendations for target servers. For details, see **Getting Target Recommendations**.

Step 2 In the **Target Configurations** area, locate the server that you want to modify the recommended target configurations for and click **Modify Target Configuration** in the **Operation** column.



Step 3 Locate the desired disk and click **Modify** in the **Target Specifications** column.



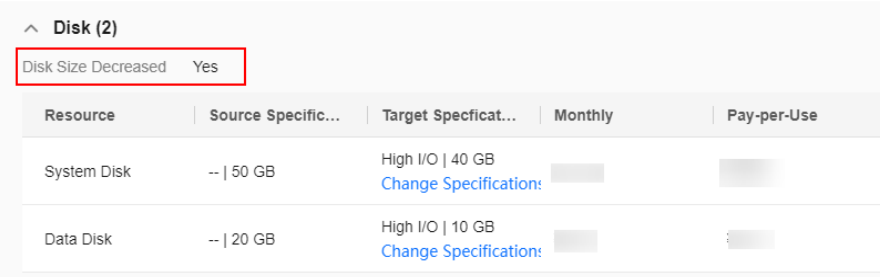
Step 4 Modify the disk capacity based on the **collected disk information of the source server** and your service requirements.

Assume the source server has a 50 GB system disk and a 20 GB data disk, and the usage of both disks is very low. You can reduce the system disk to 40 GB and the data disk to 10 GB for the target server.

CAUTION

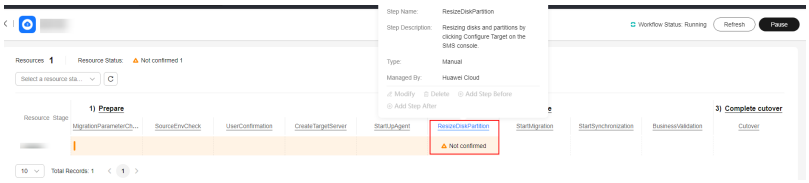
Ensure that the disk capacity of the selected target server is greater than the used disk capacity of the source server.

Step 5 Click **Confirm**. You can see **Yes** is displayed after **Disk Downsized**, which means that the disks are downsized for the target server. If you do not change the disk specifications of the target server, **No** will be displayed after **Disk Downsized**.



Step 6 **Create a server migration workflow**. When the workflow reaches the **ResizeDiskPartition** step, the system identifies whether disk capacity reduction has been performed on the target server.

- If yes, this step is paused. You need to go to **SMS console** and resize disks and partitions for the target server. For details, see **Resizing Disks and Partitions for Target Servers**. After the adjustment is complete, go back to the MgC console and click **Confirm** next to the step status so that the workflow can continue.



- If no, skip this step and proceed with the subsequent migration steps.

----End

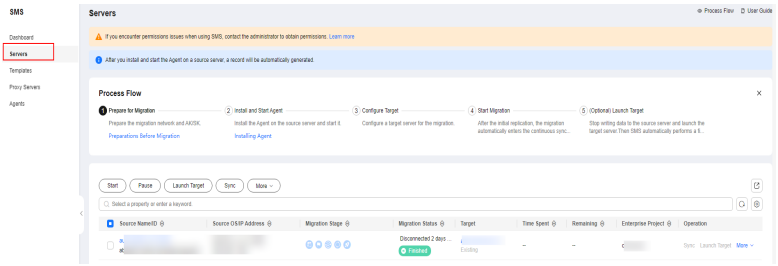
5 Resizing Disks and Partitions for Target Servers

In a server migration workflow, if the system detects that the disk capacity reduction has been performed on a target server, the workflow will be paused, and you need to go to the SMS console to resize disks and partitions for the target server.

Procedure

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

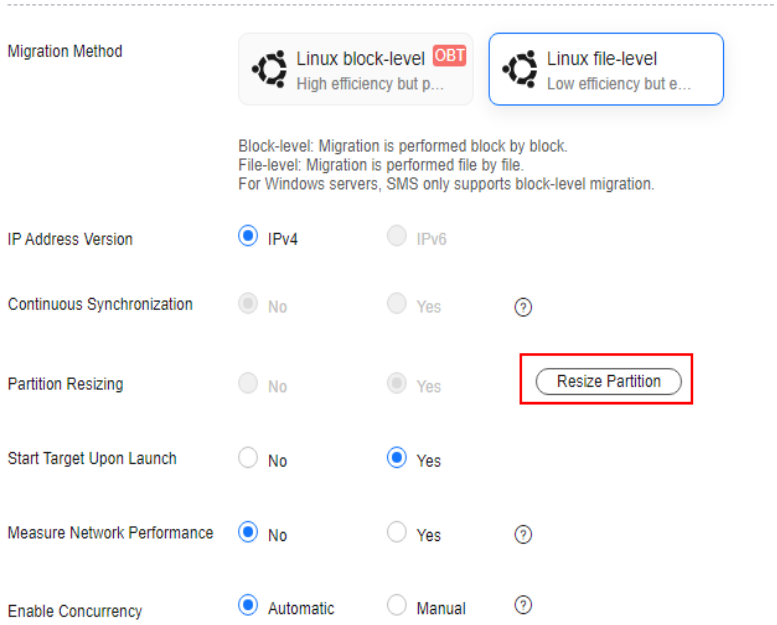
Step 2 In the navigation pane on the left, choose **Servers**.



Step 3 Locate the desired server in the server list based on the resource name in the MgC migration workflow, and click **Configure** in the **Target** column.

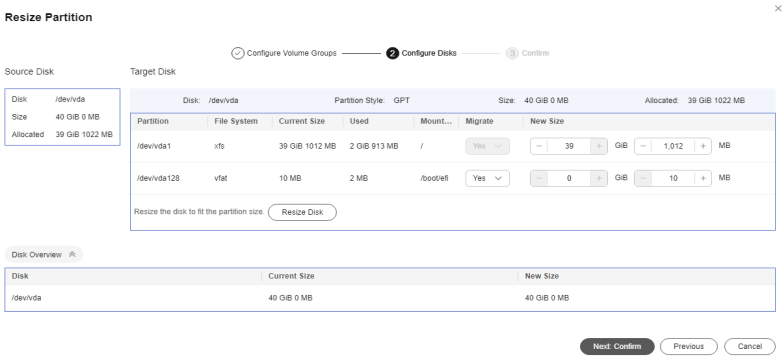
Step 4 Select **Configure now** next to **Advanced Settings**.

Step 5 Click **Resize Partition** next to **Partition Resizing**.



Step 6 Adjust the disk size, disk quantity, and partition size based on the target server specifications configured in the workflow.

Figure 5-1 Resizing disks and partitions on Linux



NOTE

- For a Linux server using LVM, you can choose whether to migrate physical or logical volumes and resize the paired target volumes.
- 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 configuring **Migrate All Volume Groups**.
- If you choose to migrate none of the logical volumes in a volume group, their physical volumes will not be migrated by default.

Step 7 After the configuration is completed, click **Next: Confirm**. After confirming that the configuration is correct, click **OK**.

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

Step 9 In the server list, select the target server paired with the source server and click **Next: Confirm**. You can view the name of the target server by clicking the **CreateTargetServer** step in the MgC migration workflow.

Step 10 After confirming that the configuration is correct, click **Save**. Read the migration checklist carefully and click **OK**.

Step 11 Return to the MgC migration workflow. Locate the **ResizeDiskPartition** step, and click **Confirm** next to the step status to continue the subsequent migration steps.

----End

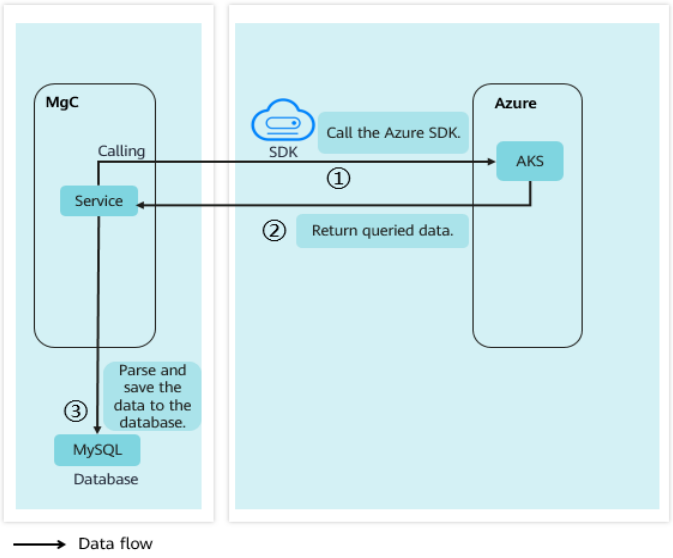
6 Collecting Details of Azure Kubernetes Service (AKS) Resources

Before migrating Azure Kubernetes Service (AKS) resources, use MgC to collect resource details, which are necessary for subsequent migration. This section describes the basic principles, preparations, account permission requirements, and specific operations for using MgC to collect AKS resource details efficiently and accurately.

Collection Principles

Figure 6-1 illustrates how to use MgC to collect AKS resource details.

Figure 6-1 Principle for collecting AKS resource details



1. MgC invokes AKS APIs through the Azure SDK to obtain information about resources such as containers and VMs.
2. MgC receives API call responses, which typically contain extensive resource data.

3. MgC parses the returned data and extracts key information, such as the number of nodes and number of VM cores. Then, the key information is saved to the database for subsequent analysis and migration.

Preparations

- Preparing a Huawei account

  Before using MgC, you need to prepare a HUAWEI ID or an IAM user that can access MgC. For details about how to register a HUAWEI ID and create an IAM user, see **Preparations**.

- Creating a migration project

  Create a migration project (a simple project is recommended) on the MgC console. For details, see **Managing Migration Projects**.

- **Preparing Azure credentials**

  Obtain the password of the application client that owns the AKS resources, subscription ID used to purchase the AKS resources, tenant ID of the application, and client (application) ID. To learn how to obtain Azure credentials, see **How Do I Obtain Azure Credentials?**

- Providing the source credentials

  Add the Azure authentication information to the MgC console as the collection credential. For details, see **Managing Credentials**.

Required Permissions

Ensure that the application to which the added Azure credentials belong has the following permissions in the resource group and subscription for purchasing the AKS resources:

- Microsoft.ClassicCompute/virtualMachines/read
- Microsoft.Insights/MetricDefinitions/Read
- Microsoft.Management/getEntities/action

For details, see **How Do I Configure the Permissions Required for Collecting Details of Azure Containers?**

Procedure

Create a discovery task on the MgC console. For details, see **Discovering Resources over the Internet**.

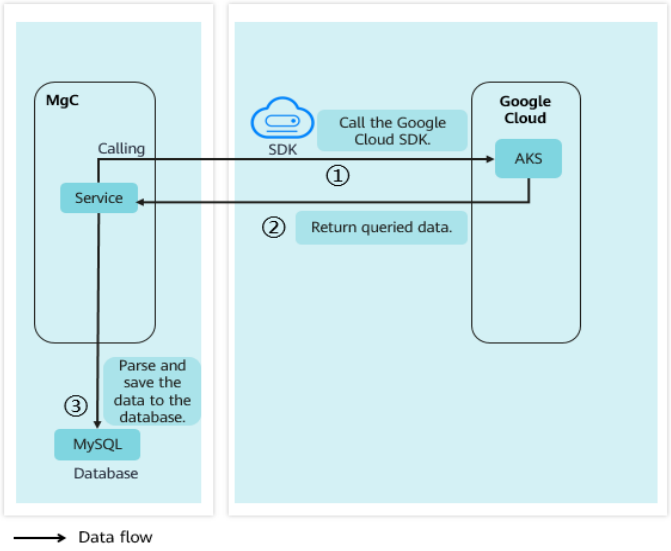
7 Collecting Details of Google Cloud GKE Resources

Before migrating Google Kubernetes Engine (GKS) resources, use MgC to collect resource details, which are necessary for subsequent migration. This section describes the basic principles, preparations, account permission requirements, and specific operations for using MgC to collect GKE resource details efficiently and accurately.

Collection Principles

Figure 7-1 illustrates how to use MgC to collect GKE resource details.

Figure 7-1 Principle for collecting GKE resource details



1. Through the SDK provided by GCP, MgC calls GKE APIs to obtain information about resources such as container instances, regions, networks, and subnets.
2. MgC receives API call responses, which typically contain extensive resource data.

3. MgC parses the returned data and extracts key information, such as the number of nodes and subnet segments. Then, the key information is saved to the database for subsequent analysis and migration.

Preparations

- Preparing a Huawei account

  Before using MgC, prepare a HUAWEI ID or an IAM user that can access MgC. For details about how to register a HUAWEI ID and create an IAM user, see **Preparations**.

- Creating a migration project

  Create a migration project (a simple project is recommended) on the MgC console. For details, see **Managing Migration Projects**.

- Preparing Google Cloud account credentials

  Obtain the credentials (key file) of the Google Cloud account to which the GKE resources belong.

- Providing the source credentials

  Add the key file of the Google Cloud account as the collection credential on the MgC console. For details, see **Managing Credentials**. Select **Configuration File** and upload the key file of the Google Cloud account. The file must be in JSON format and the file size cannot exceed 4 KB.

Account Permission Requirements

Before collecting details of GKE resources, ensure that the Google Cloud account has the following permissions:

- container.clusters.list
- compute.regions.get
- compute.networks.list
- compute.subnetworks.list

Procedure

Create a discovery task on the MgC console. For details, see **Discovering Resources over the Internet**.

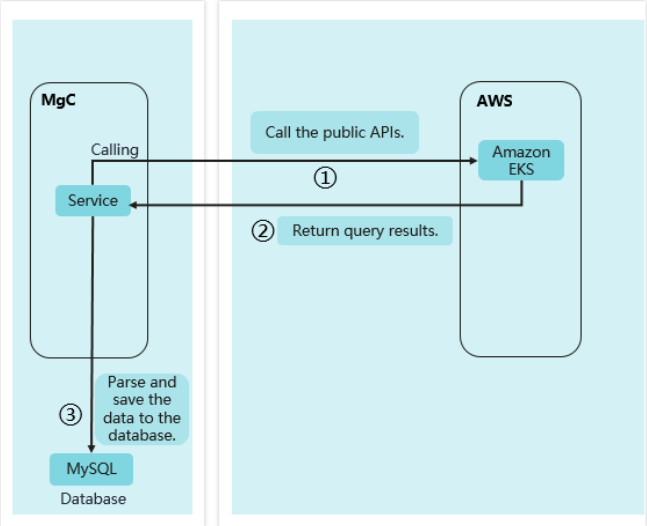
8 Collecting Details of AWS Container Resources

This section describes the basic principles, preparations, account permission requirements, and specific operations for using MgC to collect AWS container resource details efficiently and accurately.

Principle of Collection over the Internet

Figure 8-1 illustrates how to use MgC to collect details about AWS container resources over the Internet.

Figure 8-1 Principle of collecting AWS container resource details

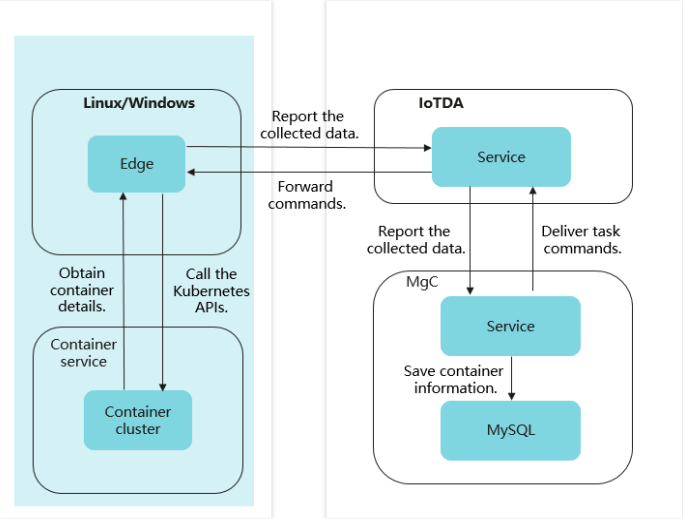


1. MgC invokes Amazon EKS APIs to obtain information about resources such as containers and VMs.
2. MgC receives API call responses, which typically contain extensive resource data.
3. MgC parses the returned data and extracts key information, such as the number of nodes and number of VM cores. Then, the key information is saved to the database for subsequent analysis and migration.

Principle of Deep Collection

Figure 8-2 shows the principle of a deep collection for AWS container resources by MgC.

Figure 8-2 Principle of deep collection for AWS containers



The process is as follows:

1. MgC sends commands to Edge to collect container resource information.
2. Edge access the container cluster using the credentials you provide.
3. Edge interacts with the container clusters through Kubernetes APIs to collect cluster details, including container specifications, node configurations, persistent volume configurations, and network policies.
4. Edge reports the collected information to MgC.
5. After receiving the reported information, MgC parses the information, extracts useful information, and saves the information to the database.

Preparations

- Preparing a Huawei account

  Before using MgC, you need to prepare a HUAWEI ID or an IAM user that can access MgC. For details about how to register a HUAWEI ID and create an IAM user, see **Preparations**.

- Creating a migration project

  Create a migration project (a simple project is recommended) on the MgC console. For details, see **Managing Migration Projects**.

- Preparing AWS account credentials

  Obtain an AK/SK pair for the AWS account that owns the resources to be collected. For details, see **Obtaining AWS Access Keys**.

- Providing the source credentials

  Add the AWS authentication information to the MgC console as the collection credential. For details, see **Managing Credentials**.

- Obtaining the login configuration files of the AWS container clusters

  The configuration files are used for deep collection. Edge uses them to access the AWS container clusters and invoke the Kubernetes APIs to collect details about the container clusters.

Required Permissions

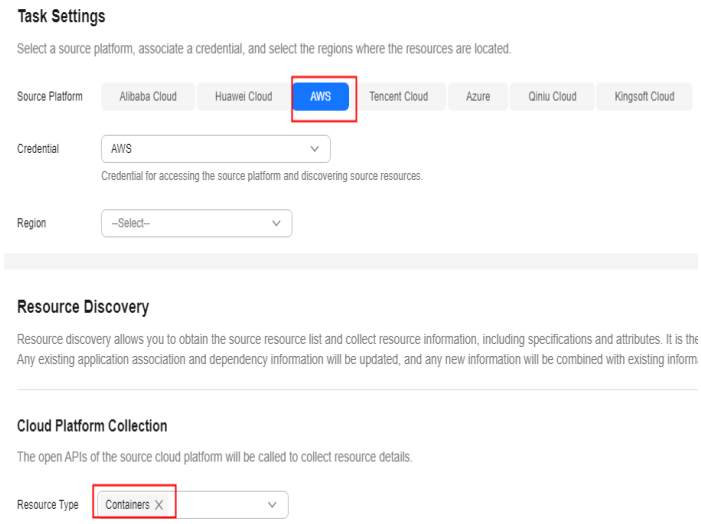
Before collecting details of Amazon EKS resources, ensure that the AWS account has the following permissions:

- eks:DescribeCluster
- eks:ListClusters
- ec2:DescribeInstances
- ec2:DescribeSubnets
- cloudwatch:GetMetricStatistics

Creating an Internet-based Discovery Task

Create a discovery task on the MgC console. For details, see **Discovering Resources over the Internet**. During the task creation, set **Source Platform** to **AWS**, **Credential** to the credential provided in preparations, **Region** as required, and **Resource Type** to **Container**.

Figure 8-3 Creating an Internet-based discovery task

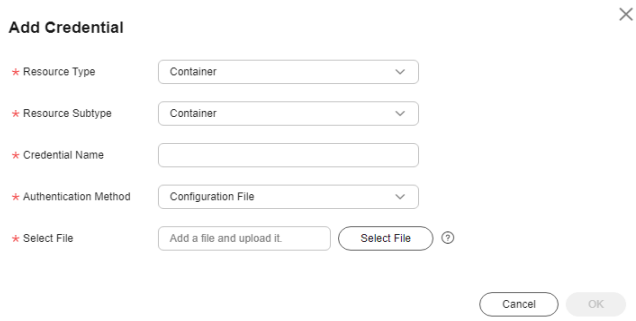


Performing a Deep Collection

After obtaining the list of AWS containers through the **Internet-based discovery task**, you can perform a deep collection for container resources to obtain their details, including container specifications, node configurations, persistent volume configurations, and network policies. For details, see **Performing a Deep Collection for Containers**.

Before that, you need to provide Edge with the login configuration files for accessing the AWS container clusters.

Figure 8-4 Adding credentials required for deep collection to Edge



9 Verifying Big Data Consistency After Migration

9.1 Verifying the Consistency of Data Migrated from MaxCompute to DLI

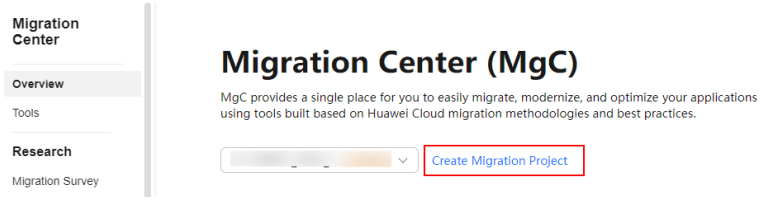
This section describes how to use MgC to verify the consistency of data migrated from Alibaba Cloud MaxCompute to Huawei Cloud Data Lake Insight (DLI).

Preparations

Install Edge, an MgC tool used for data verification, in the source intranet environment and register an account for using Edge. For details, see **Installing Edge for Linux**.

Procedure

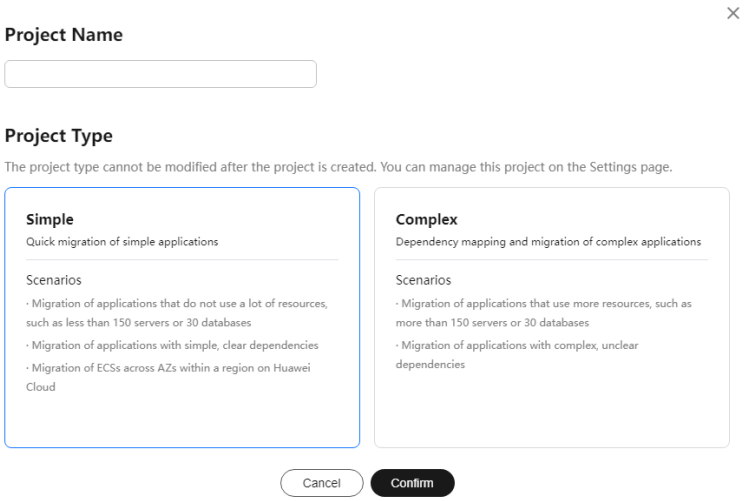
Step 1 Sign in to the **MgC** console. On the **Overview** page, click **Create Migration Project**.



Step 2 In the displayed dialog box, enter a project name, select a project type, and click **Confirm**.

NOTICE

To review this migration project, choose **Settings** > **Migration Projects** in the navigation pane.

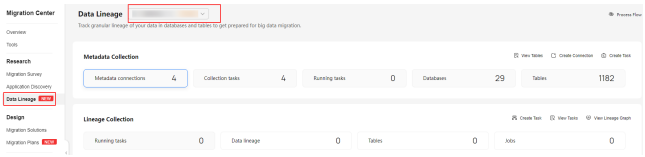


Step 3 Connect Edge to MgC. For more information, see **Connecting the Edge Device to MgC**.

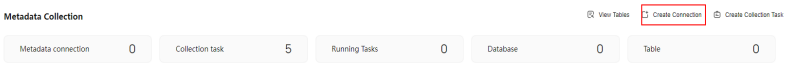
Step 4 On the Edge console, add your AK/SK pairs required for accessing MaxCompute and DLI. For more information, see **Adding Resource Credentials**.

- For details about how to obtain an AK/SK pair for accessing DLI, see **How Do I Obtain the AK/SK Pair?**
- For details about how to obtain an AK/SK pair for accessing MaxCompute, see **Viewing the Information About AccessKey Pairs of a RAM User**.

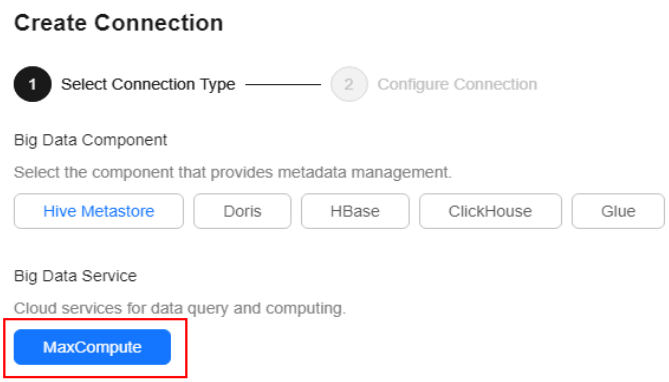
Step 5 On the MgC console, in the navigation pane on the left, choose **Research** > **Data Lineage**. In the upper left corner of the page, choose the migration project created in **step 2**.



Step 6 In the **Metadata Collection** area, click **Create Connection**.



Step 7 On the **Select Connection Type** page, select **MaxCompute** and click **Next**.

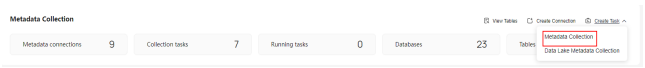


Step 8 Configure the **parameters for creating a MaxCompute connection**, and click **Test**. If the test is successful, the connection is set up.

Table 9-1 Parameters for creating a MaxCompute connection

Parameter	Configuration
Connection To	Select **Source**.
Connection Name	The default name is **MaxCompute-***4 random characters* (including letters and numbers). You can also customize a name.
Edge Device	Select the Edge device connected to MgC in **step 3**.
Alibaba Cloud Credential	Select the MaxCompute credential added to Edge in **step 4**.
MaxCompute Project	Enter the name of your MaxCompute project. You can obtain the project name from the MaxCompute console.
Endpoint	Enter the endpoint of the region where the MaxCompute project is located. For details about the MaxCompute endpoints in different regions, see **MaxCompute Endpoints**.

Step 9 In the **Metadata Collection** area, choose **Create Task** > **Metadata Collection**.



Step 10 Configure the **parameters for creating a metadata collection task** and click **Confirm**.

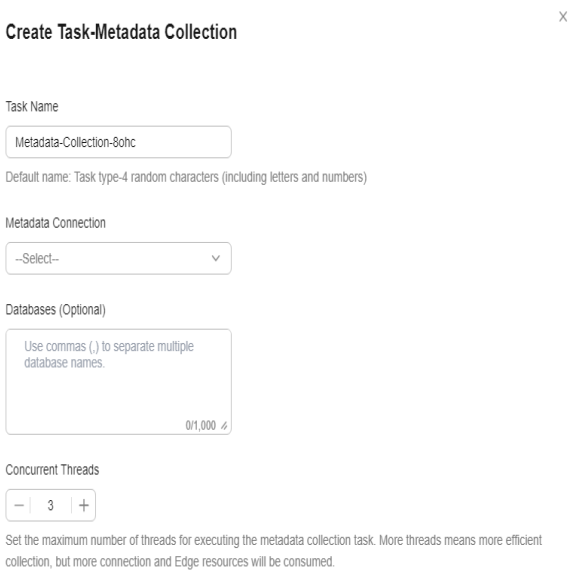
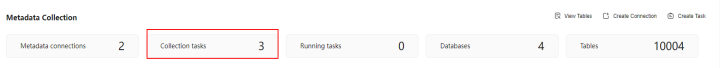


Table 9-2 Parameters for configuring a metadata collection task

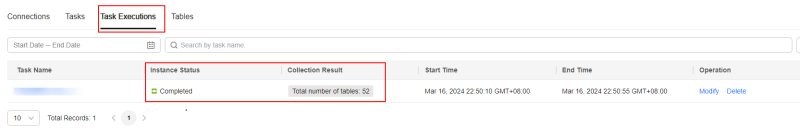
Parameter	Configuration
Task Name	The default name is **Metadata-Collection-***4 random characters* (including letters and numbers). You can also customize a name.
Metadata Connection	Select the connection created in **step 8**.
Databases	Enter the names of the databases whose metadata needs to be collected. Use commas (,) to separate the database names. **NOTICE** This parameter is mandatory only if a MaxCompute metadata connection is selected.
Concurrent Threads	Set the maximum number of threads for executing the collection. The default value is **3**. The value ranges from **1** to **10**. Configuring more concurrent threads means more efficient collection, but more connection and Edge device resources will be consumed.

Step 11 In the **Metadata Collection** area, click **Collection tasks**.

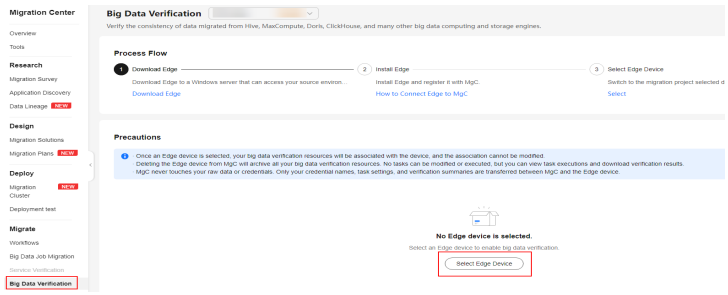


Step 12 Under **Tasks**, you can review the created metadata collection task and its settings. Click **Execute Task** in the **Operation** column to run the task. Each time the task is executed, a task execution is generated.

Step 13 Click **View Executions** in the **Operation** column. Under **Task Executions**, you can view the execution records of the task and the status and collection results of each task execution. When a task execution enters a **Completed** status and the collection results are displayed, you can view the list of databases and tables extracted from collected metadata on the **Tables** tab.



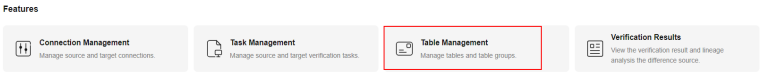
Step 14 In the navigation pane on the left, choose **Migrate** > **Big Data Verification**. If this is your first time to visit this page, select an Edge device to enable the verification feature. Click **Select Edge Device**. In the displayed dialog box, select the Edge device connected to MgC in **step 3**.



CAUTION

Ensure that the selected Edge device is always **Online** and **Enabled** before your verification is complete.

Step 15 In the **Features** area, click **Table Management**.



Step 16 Under **Table Groups**, click **Create**. Configure the **parameters for creating a table group** and click **Confirm**.

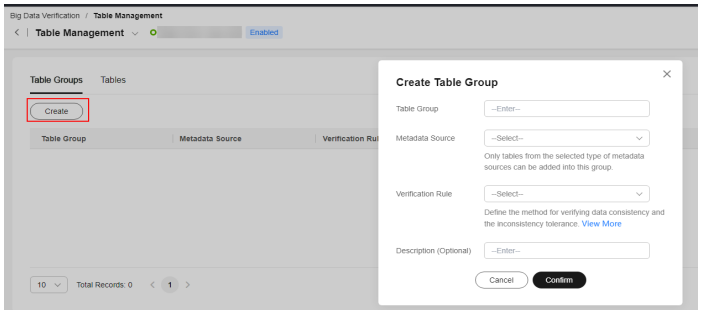
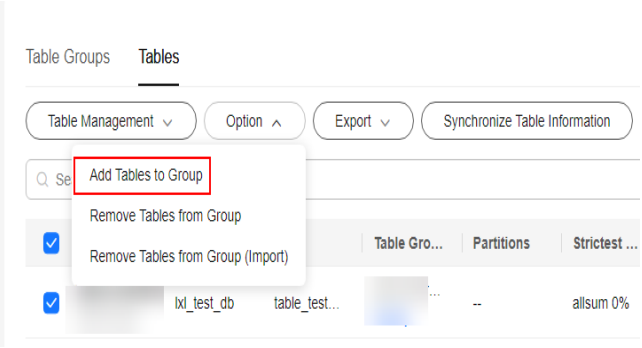


Table 9-3 Parameters for creating a table group

Parameter	Configuration
Table Group	Enter a name.
Metadata Connection	Select the connection created in **step 8**. **CAUTION** A table group can only contain tables coming from the same metadata source.
Verification Rule	Select a rule that defines the method for verifying data consistency and the inconsistency tolerance. You can **View More** to see more information about the verification rules provided by MgC.
Description (Optional)	Enter a description to identify the table group.

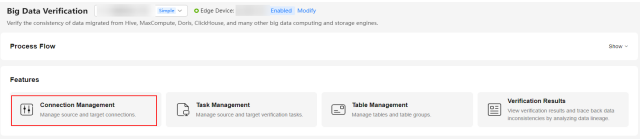
Step 17 On the **Table Management** page, click the **Tables** tab, select the data tables to be added to the same table group, and choose **Option** > **Add Tables to Group** above the list. In the displayed dialog box, select the desired table group and click **Confirm**.



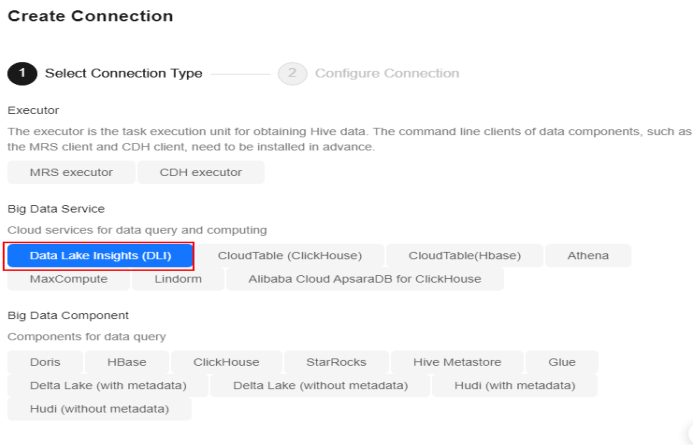
NOTICE

You can manually import information of incremental data tables to MgC. For details, see **Creating a Table Group and Adding Tables to the Group**.

Step 18 On the **Big Data Verification** page, in the **Features** area, click **Connection Management**.



Step 19 Click **Create Connection** in the upper right corner of the page. On the **Select Connection Type** page, select **Data Lake Insight (DLI)** and click **Next**.



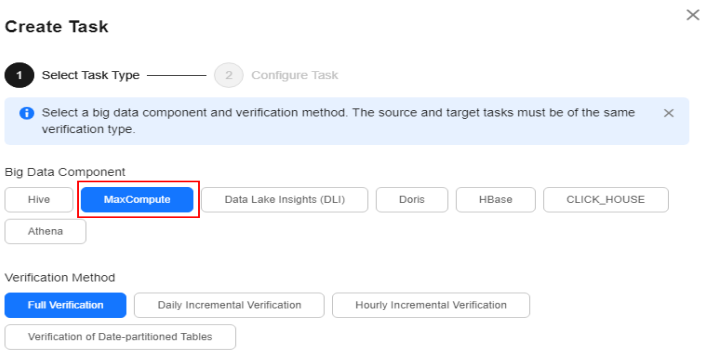
Step 20 Configure the parameters listed in **Table 9-4**, and click **Test**. If the test is successful, the connection is set up.

Table 9-4 Parameters for creating a DLI connection

Parameter	Configuration
Connection To	Select **Target**.
Connection Name	The default name is **DLI-***4 random characters* (including letters and numbers). You can also customize a name.
DLI Credential	Select the DL credential added to Edge in **step 4**. If the selected credential is the one you currently use to access MgC, you can select **This is my MgC credential**, and the projects in the region you choose will be listed.
Region	Enter the code of the target region where the data to be verified is located, for example, ap-southeast-1. For details about region codes, see **Endpoints**.
Project	Enter the ID of the project where the data to be verified is stored. For details about how to obtain the project ID, see **Obtaining Project Information**.
Queue	Enter the name of the DLI queue used to execute verification. The queue must be a SQL queue.

Step 21 On the MgC console, create a verification task for MaxCompute and execute the task. For details, see **Creating and Executing Verification Tasks**. During the task creation, select the table group created in **step 16**.

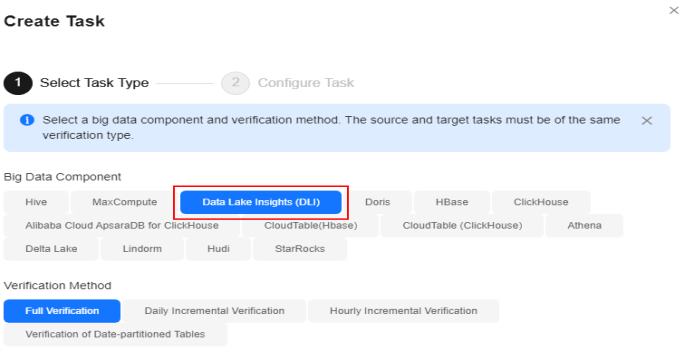
- On the **Select Task Type** page, select **MaxCompute** for **Big Data Component**.



- Select a verification method. For details about each verification method, see **Verification Methods**.

Step 22 On the MgC console, create a verification task for DLI and execute the task. For details, see **Creating and Executing Verification Tasks**. During the task creation, select the table group created in **step 16**.

- On the **Select Task Type** page, choose **Data Lake Insight (DLI)**.



- Select a verification method. For details about each verification method, see **Verification Methods**.

Step 23 Wait until the task executions enter a **Completed** status. On the **Verification Results** page, you can view and export the task execution results. For details, see **Viewing and Exporting Verification Results**.

----End

9.2 Verifying the Consistency of Data Migrated Between MRS ClickHouse Clusters

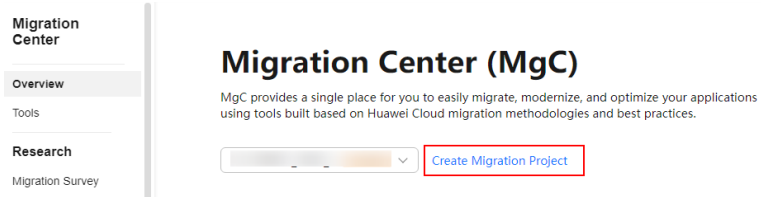
This section describes how to use MgC to verify the consistency of data migrated between MRS ClickHouse clusters of different versions.

Preparations

Install Edge, an MgC tool used for data verification, in the source intranet environment and register an account for using Edge. For details, see **Installing Edge for Linux**.

Procedure

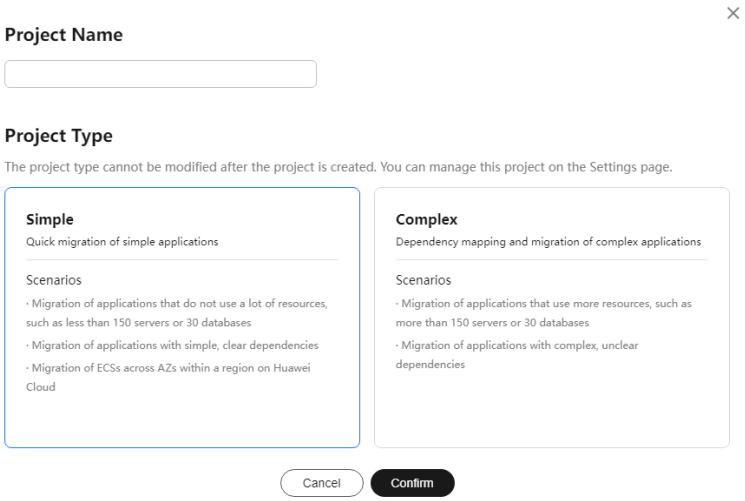
Step 1 Sign in to the **MgC** console. On the **Overview** page, click **Create Migration Project**.



Step 2 In the displayed dialog box, enter a project name, select a project type, and click **Confirm**.

NOTICE

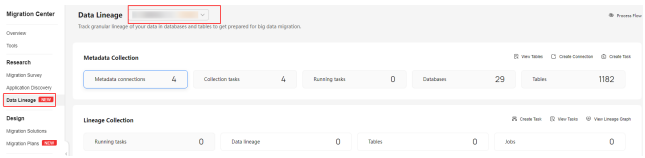
To review this migration project, choose **Settings** > **Migration Projects** in the navigation pane.



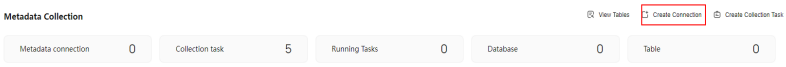
Step 3 Connect Edge to MgC. For more information, see **Connecting the Edge Device to MgC**.

Step 4 After the connection is successful, add the username/password pairs for accessing the source and target MRS ClickHouse clusters to Edge. For more information, see **Adding Resource Credentials**.

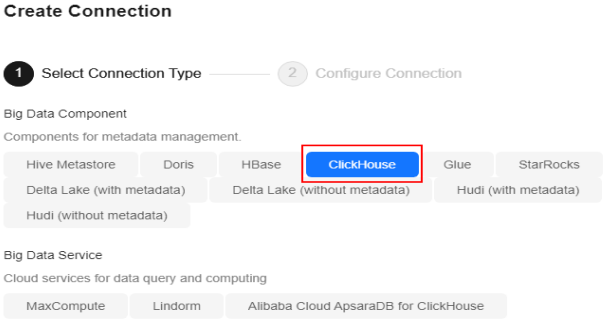
Step 5 On the MgC console, in the navigation pane on the left, choose **Research** > **Data Lineage**. In the upper left corner of the page, choose the migration project created in **step 2**.



Step 6 In the **Metadata Collection** area, click **Create Connection**.



Step 7 On the **Select Connection Type** page, select **ClickHouse** and click **Next**.

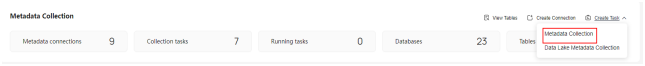


Step 8 Configure the **parameters for creating a ClickHouse connection**, and click **Test**. If the test is successful, the connection is set up.

Table 9-5 Parameters for creating a ClickHouse connection

Parameter	Configuration
Connection To	Select **Source**.
Connection Name	The default name is **ClickHouse-***4 random characters* (including letters and numbers). You can also customize a name.
Edge Device	Select the Edge device connected to MgC in **step 3**.
ClickHouse Credential (Optional)	Select the credential used for accessing the source MRS ClickHouse cluster you added to Edge in **step 4**.
Secured Cluster	Choose whether the cluster is secured.
ClickHouse Server IP Address	Enter the IP address for accessing the source ClickHouse server. Generally, the IP address refers to that of the server where ClickHouse is hosted.
HTTP Port	If the ClickHouse cluster is unsecured, enter the HTTP port for communicating with the ClickHouse servers. To obtain the value, log in to the **FusionInsight Manager** of the source cluster, choose **Cluster** > **Services** > **ClickHouse** > **Configurations** > **All Configurations**, and search for the **http_port** parameter.
HTTP SSL/TLS Port	If the ClickHouse cluster is secured, enter the HTTPS port for communicating with the ClickHouse server. To obtain the value, log in to the **FusionInsight Manager**, choose **Cluster** > **Services** > **ClickHouse** > **Configurations** > **All Configurations**, and search for the **https_port** parameter.

Step 9 In the **Metadata Collection** area, choose **Create Task** > **Metadata Collection**.



Step 10 Configure the **parameters for creating a metadata collection task** and click **Confirm**.

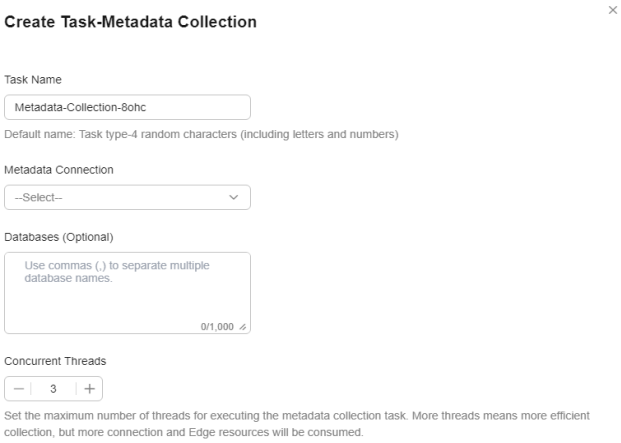
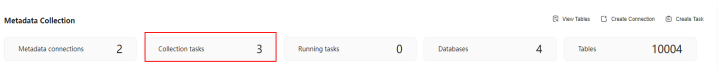


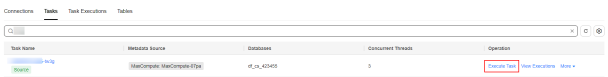
Table 9-6 Parameters for configuring a metadata collection task

Parameter	Configuration
Task Name	The default name is **Metadata-Collection-***4 random characters* (including letters and numbers). You can also customize a name.
Metadata Connection	Select the connection created in **step 8**.
Databases (Optional)	Enter the names of the databases whose metadata needs to be collected. Use commas (,) to separate the database names. If no database name is specified, the metadata of all databases is collected.
Concurrent Threads	Set the maximum number of threads for executing the collection. The default value is **3**. The value ranges from **1** to **10**. Configuring more concurrent threads means more efficient collection, but more connection and Edge device resources will be consumed.

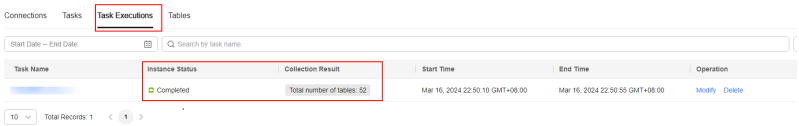
Step 11 In the **Metadata Collection** area, click **Collection tasks**.



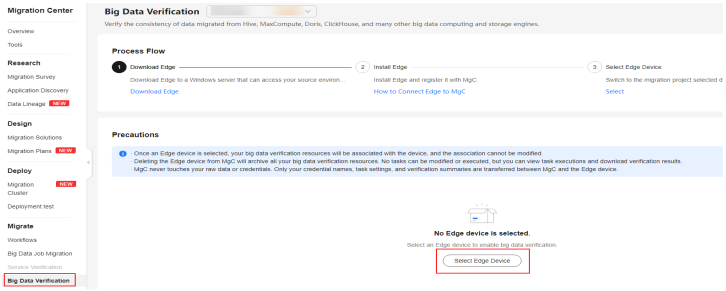
Step 12 Under **Tasks**, you can review the created metadata collection task and its settings. Click **Execute Task** in the **Operation** column to run the task. Each time the task is executed, a task execution is generated.



Step 13 Click **View Executions** in the **Operation** column. Under **Task Executions**, you can view the execution records of the task and the status and collection results of each task execution. When a task execution enters a **Completed** status and the collection results are displayed, you can view the list of databases and tables extracted from collected metadata on the **Tables** tab.



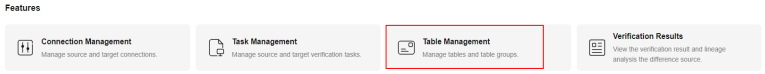
Step 14 In the navigation pane on the left, choose **Migrate** > **Big Data Verification**. If this is your first time to visit this page, select an Edge device to enable the verification feature. Click **Select Edge Device**. In the displayed dialog box, select the Edge device connected to MgC in **step 3**.



CAUTION

Ensure that the selected Edge device is always **Online** and **Enabled** before your verification is complete.

Step 15 In the **Features** area, click **Table Management**.



Step 16 Under **Table Groups**, click **Create**. Configure the **parameters for creating a table group** and click **Confirm**.

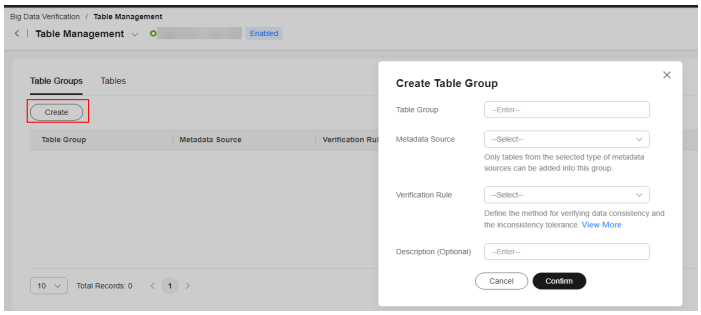
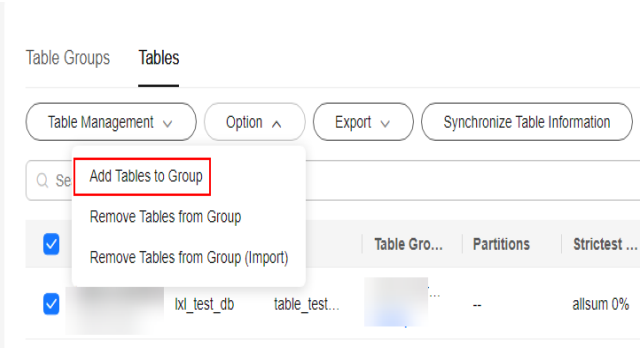


Table 9-7 Parameters for creating a table group

Parameter	Description
Table Group	Enter a name.
Metadata Connection	Select the connection created in **step 8**. **CAUTION** A table group can only contain tables coming from the same metadata source.

Parameter	Description
Verification Rule	Select a rule that defines the method for verifying data consistency and the inconsistency tolerance. You can **View More** to see more information about the verification rules provided by MgC.
Description (Optional)	Enter a description to identify the table group.

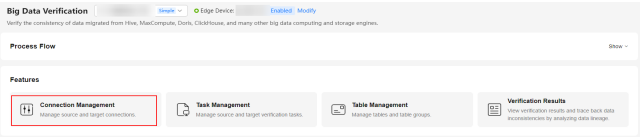
Step 17 On the **Table Management** page, click the **Tables** tab, select the data tables to be added to the same table group, and choose **Option** > **Add Tables to Group** above the list. In the displayed dialog box, select the desired table group and click **Confirm**.



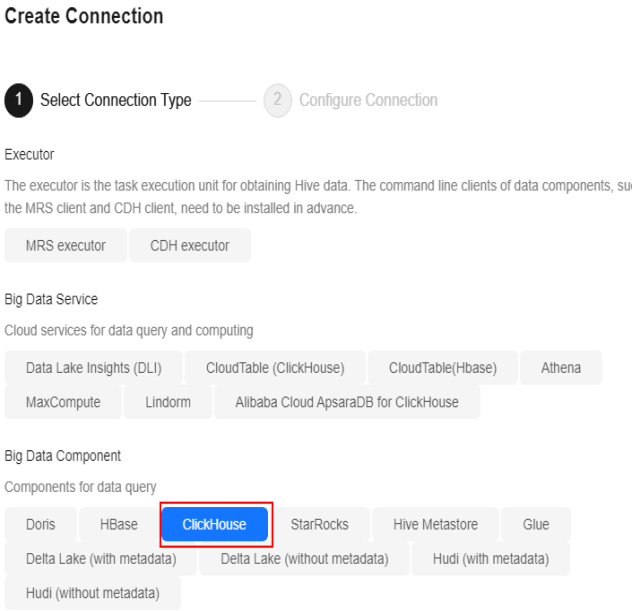
NOTICE

You can manually import information of incremental data tables to MgC. For details, see **Creating a Table Group and Adding Tables to the Group**.

Step 18 On the **Big Data Verification** page, in the **Features** area, click **Connection Management**.



Step 19 Click **Create Connection** in the upper right corner of the page. On the **Select Connection Type** page, select **ClickHouse** and click **Next**.



Step 20 Configure the **parameters for creating a ClickHouse connection**, and click **Test**. If the test is successful, the connection is set up.

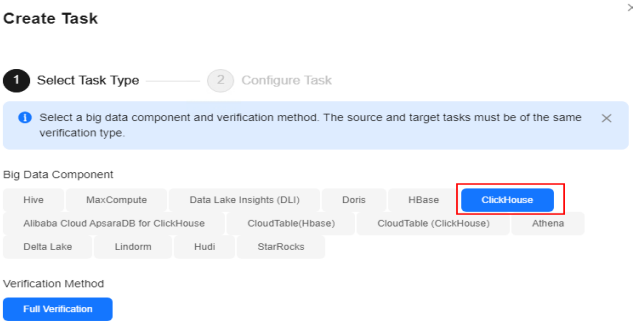
Table 9-8 Parameters for creating a ClickHouse connection

Parameter	Configuration
Connection To	Select **Target**.
Connection Name	The default name is **ClickHouse-***4 random characters* (including letters and numbers). You can also customize a name.
ClickHouse Credential (Optional)	Select the credential used for accessing the target MRS ClickHouse cluster you added to Edge in **step 4**.
Secured Cluster	Choose whether the cluster is secured.
ClickHouse Server IP Address	Enter the IP address of the MRS ClickHouse server. Generally, the IP address refers to that of the server where ClickHouse is hosted.
HTTP Port	If the MRS ClickHouse cluster is unsecured, enter the HTTP port for communicating with the ClickHouse server. To obtain the value, log in to the **FusionInsight Manager** of the target cluster, choose **Cluster** > **Services** > **ClickHouse** > **Configurations** > **All Configurations**, and search for the **http_port** parameter.

Parameter	Configuration
HTTP SSL/TLS Port	If the MRS ClickHouse cluster is secured, enter the HTTPS port for communicating with the MRS ClickHouse server. To obtain the value, log in to the **FusionInsight Manager** of the target cluster, choose **Cluster** > **Services** > **ClickHouse** > **Configurations** > **All Configurations**, and search for the **https_port** parameter.

Step 21 Create a data verification task for the source and target MRS ClickHouse clusters, respectively, and execute the tasks. For more information, see **Creating and Executing Verification Tasks**. During the task creation, select the table group created in **step 16**.

- On the **Select Task Type** page, select **ClickHouse** for **Big Data Component**.



- Select **Full Verification** for **Verification Method**.

Step 22 Wait until the task executions enter a **Completed** status. On the **Verification Results** page, you can view and export the task execution results. For details, see **Viewing and Exporting Verification Results**.

----End

9.3 Verifying the Consistency of Data Migrated from Alibaba Cloud EMR ClickHouse to Huawei Cloud MRS ClickHouse

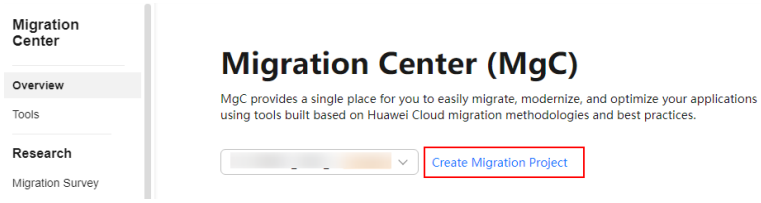
This section describes how to use MgC to verify the consistency of data migrated from Alibaba Cloud EMR ClickHouse to Huawei Cloud MRS ClickHouse.

Preparations

Install Edge, an MgC tool used for data verification, in the source intranet environment and register an account for using Edge. For details, see **Installing Edge for Linux**.

Procedure

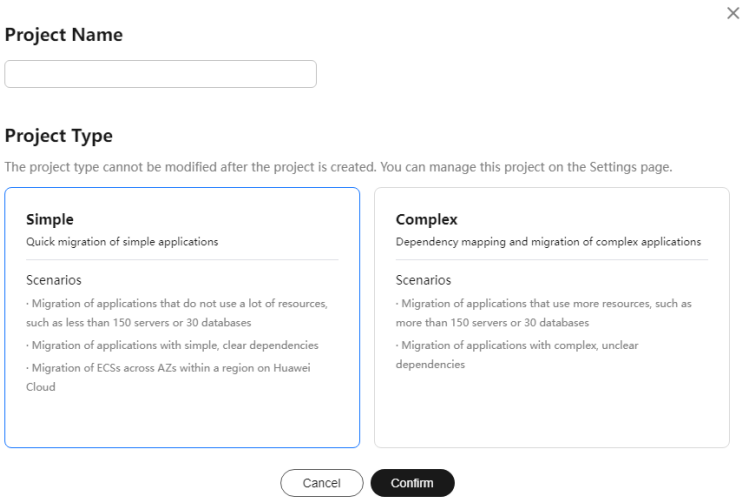
Step 1 Sign in to the MgC console. On the **Overview** page, click **Create Migration Project**.



Step 2 In the displayed dialog box, enter a project name, select a project type, and click **Confirm**.

NOTICE

To review this migration project, choose **Settings** > **Migration Projects** in the navigation pane.

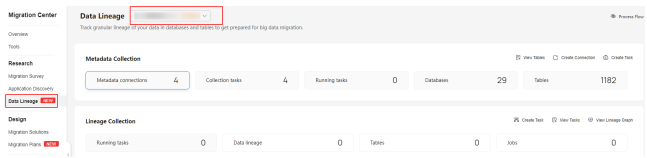


Step 3 Connect Edge to MgC. For more information, see **Connecting the Edge Device to MgC**.

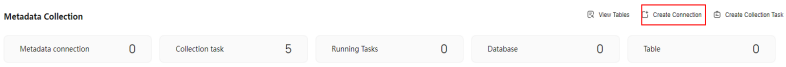
Step 4 After the connection is successful, add the username/password pairs for accessing the source and target ClickHouse servers to Edge. For more information, see **Adding Resource Credentials**.

To obtain the username and password for logging in to the Alibaba Cloud EMR ClickHouse server, go to the EMR console, on the **Configuration** page of ClickHouse, and view the **users.default.password** parameter.

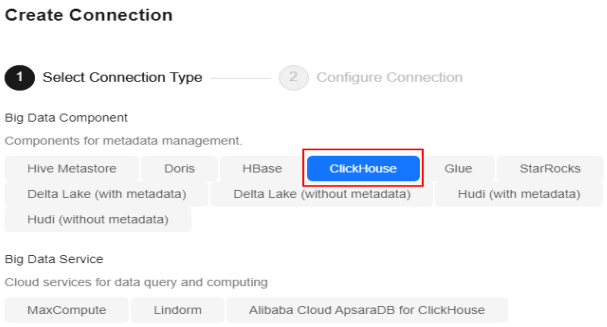
Step 5 On the MgC console, in the navigation pane on the left, choose **Research** > **Data Lineage**. In the upper left corner of the page, choose the migration project created in **step 2**.



Step 6 In the **Metadata Collection** area, click **Create Connection**.



Step 7 On the **Select Connection Type** page, select **ClickHouse** and click **Next**.



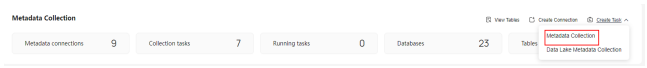
Step 8 Configure the **parameters for creating a ClickHouse connection**, and click **Test**. If the test is successful, the connection is set up.

Table 9-9 Parameters for creating a ClickHouse connection

Parameter	Configuration
Connection To	Select **Source**.
Connection Name	The default name is **ClickHouse-***4 random characters* (including letters and numbers). You can also customize a name.
Edge Device	Select the Edge device connected to MgC in **step 3**.
ClickHouse Credential (Optional)	Select the credential used for accessing the Alibaba Cloud MRS ClickHouse server you added to Edge in **step 4**.
Secured Cluster	Choose whether the cluster is secured.
ClickHouse Server IP Address	Enter the IP address of the Alibaba Cloud EMR ClickHouse server. Generally, the IP address refers to that of the server where ClickHouse is hosted.
HTTP Port	If the Alibaba Cloud MRS ClickHouse cluster is unsecured, enter the HTTP port for communicating with the ClickHouse server. To obtain the value, log in to the EMR console, go to the **Configuration** page of the ClickHouse service, click the **server-config** tab, and view the value of **http_port**.

Parameter	Configuration
HTTP SSL/TLS Port	If the Alibaba Cloud MRS ClickHouse cluster is unsecured, enter the HTTPS port for communicating with the ClickHouse server. To obtain the value, log in to the EMR console, go to the **Configuration** page of the ClickHouse service, click the **server-config** tab, and view the value of **http_port**.

Step 9 In the **Metadata Collection** area, choose **Create Task** > **Metadata Collection**.



Step 10 Configure the **parameters for creating a metadata collection task** and click **Confirm**.

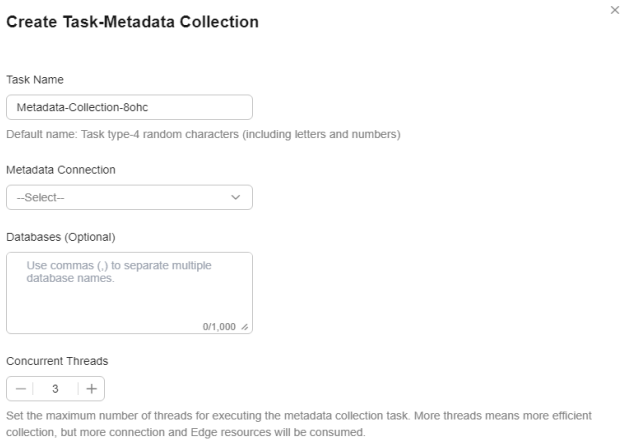
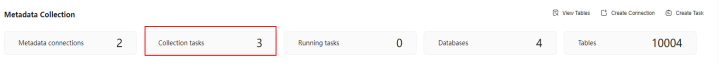


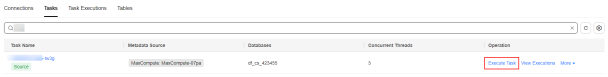
Table 9-10 Parameters for configuring a metadata collection task

Parameter	Configuration
Task Name	The default name is **Metadata-Collection-***4 random characters* (including letters and numbers). You can also customize a name.
Metadata Connection	Select the connection created in **step 8**.
Databases (Optional)	Enter the names of the databases whose metadata needs to be collected. Use commas (,) to separate the database names. If no database name is specified, the metadata of all databases is collected.
Concurrent Threads	Set the maximum number of threads for executing the collection. The default value is **3**. The value ranges from **1** to **10**. Configuring more concurrent threads means more efficient collection, but more connection and Edge device resources will be consumed.

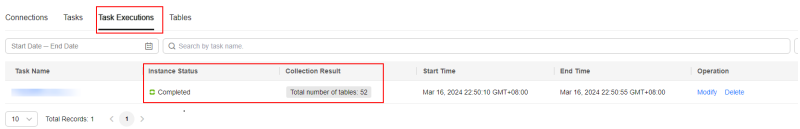
Step 11 In the **Metadata Collection** area, click **Collection tasks**.



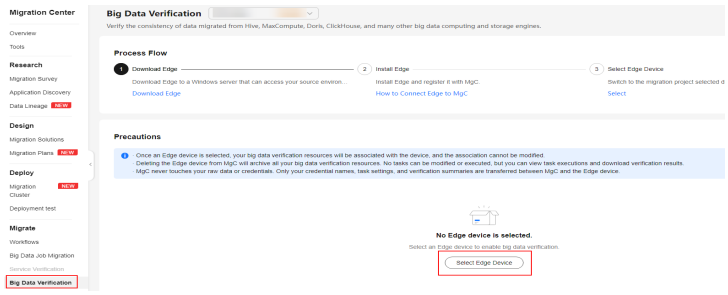
Step 12 Under **Tasks**, you can review the created metadata collection task and its settings. Click **Execute Task** in the **Operation** column to run the task. Each time the task is executed, a task execution is generated.



Step 13 Click **View Executions** in the **Operation** column. Under **Task Executions**, you can view the execution records of the task and the status and collection results of each task execution. When a task execution enters a **Completed** status and the collection results are displayed, you can view the list of databases and tables extracted from collected metadata on the **Tables** tab.



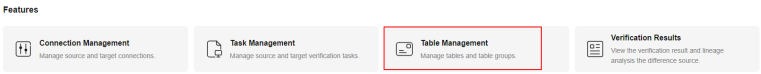
Step 14 In the navigation pane on the left, choose **Migrate** > **Big Data Verification**. If this is your first time to visit this page, select an Edge device to enable the verification feature. Click **Select Edge Device**. In the displayed dialog box, select the Edge device connected to MgC in **step 3**.



CAUTION

Ensure that the selected Edge device is always **Online** and **Enabled** before your verification is complete.

Step 15 In the **Features** area, click **Table Management**.



Step 16 Under **Table Groups**, click **Create**. Configure the **parameters for creating a table group** and click **Confirm**.

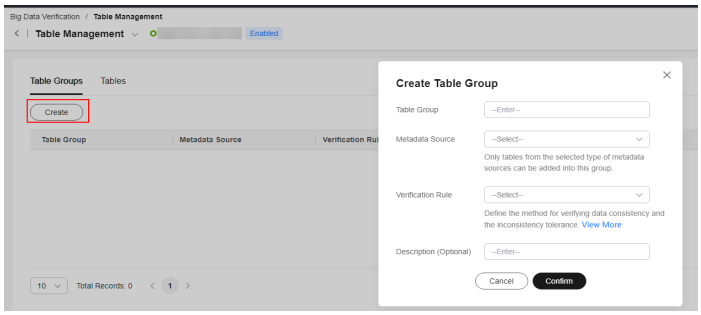
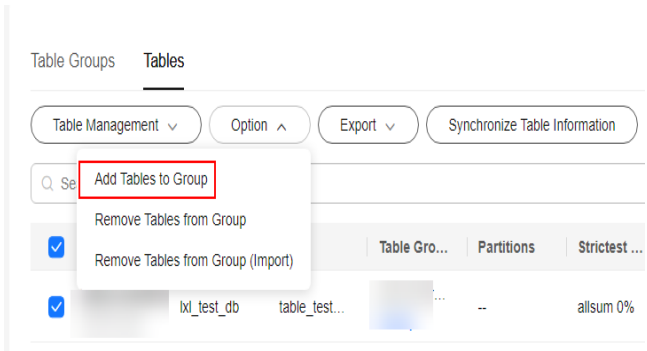


Table 9-11 Parameters for creating a table group

Parameter	Description
Table Group	User-defined
Metadata Connection	Select the connection created in **step 8**. **CAUTION** A table group can only contain tables coming from the same metadata source.
Verification Rule	Select a rule that defines the method for verifying data consistency and the inconsistency tolerance. You can **View More** to see more information about the verification rules provided by MgC.
Description (Optional)	Enter a description to identify the table group.

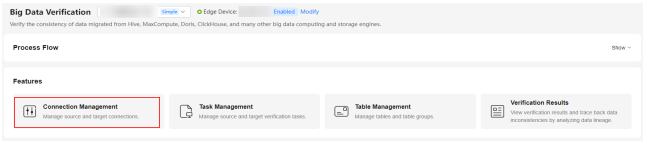
Step 17 On the **Table Management** page, click the **Tables** tab, select the data tables to be added to the same table group, and choose **Option** > **Add Tables to Group** above the list. In the displayed dialog box, select the desired table group and click **Confirm**.



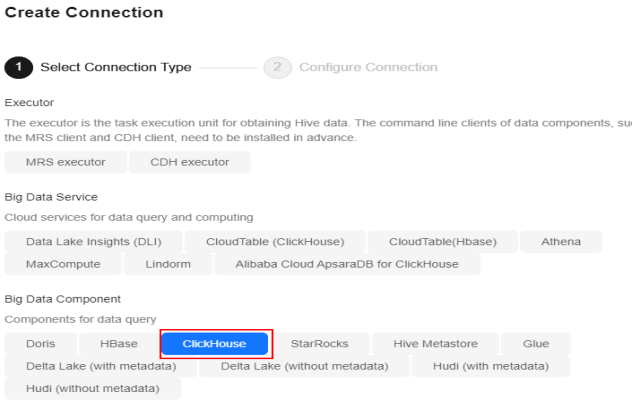
NOTICE

You can manually import information of incremental data tables to MgC. For details, see **Creating a Table Group and Adding Tables to the Group**.

Step 18 On the **Big Data Verification** page, in the **Features** area, click **Connection Management**.



Step 19 Click **Create Connection** in the upper right corner of the page. On the **Select Connection Type** page, select **ClickHouse** and click **Next**.



Step 20 Configure the **parameters for creating a ClickHouse connection**, and click **Test**. If the test is successful, the connection is set up.

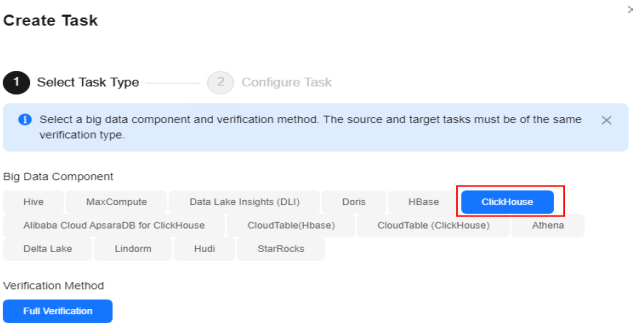
Table 9-12 Parameters for creating a ClickHouse connection

Parameter	Configuration
Connection To	Select **Target**.
Connection Name	The default name is **ClickHouse-***4 random characters* (including letters and numbers). You can also customize a name.
ClickHouse Credential (Optional)	Select the credential used for accessing the target MRS ClickHouse cluster you added to Edge in **step 4**.
Secured Cluster	Choose whether the cluster is secured.
ClickHouse Server IP Address	Enter the IP address of the MRS ClickHouse server. Generally, the IP address refers to that of the server where ClickHouse is hosted.
HTTP Port	If the MRS ClickHouse cluster is unsecured, enter the HTTP port for communicating with the ClickHouse server. To obtain the value, log in to the **FusionInsight Manager** of the target cluster, choose **Cluster** > **Services** > **ClickHouse** > **Configurations** > **All Configurations**, and search for the **http_port** parameter.

Parameter	Configuration
HTTP SSL/TLS Port	If the MRS ClickHouse cluster is secured, enter the HTTPS port for communicating with the ClickHouse server. To obtain the value, log in to the **FusionInsight Manager** of the target cluster, choose **Cluster** > **Services** > **ClickHouse** > **Configurations** > **All Configurations**, and search for the **https_port** parameter.

Step 21 Create a data verification task for the source EMR ClickHouse cluster and the target MRS ClickHouse cluster, respectively, and execute the tasks. For more information, see **Creating and Executing Verification Tasks**. During the task creation, select the table group created in **step 16**.

- On the **Select Task Type** page, choose **ClickHouse**.



- Select **Full Verification** for **Verification Method**.

Step 22 Wait until the task executions enter a **Completed** status. On the **Verification Results** page, you can view and export the task execution results. For details, see **Viewing and Exporting Verification Results**.

----End

9.4 Verifying the Consistency of Data Migrated from Alibaba Cloud ApsaraDB for ClickHouse to Huawei Cloud MRS ClickHouse

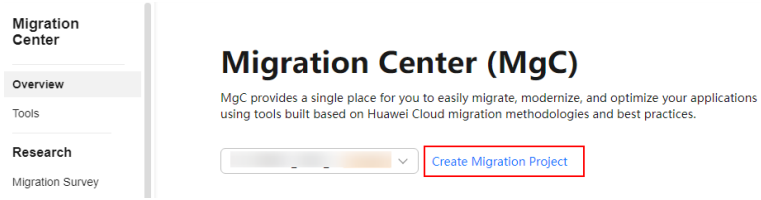
This section describes how to use MgC to verify the consistency of data migrated from Alibaba Cloud ApsaraDB for ClickHouse to Huawei Cloud MRS ClickHouse.

Preparations

Install Edge, an MgC tool used for data verification, in the source intranet environment and register an account for using Edge. For details, see **Installing Edge for Linux**.

Procedure

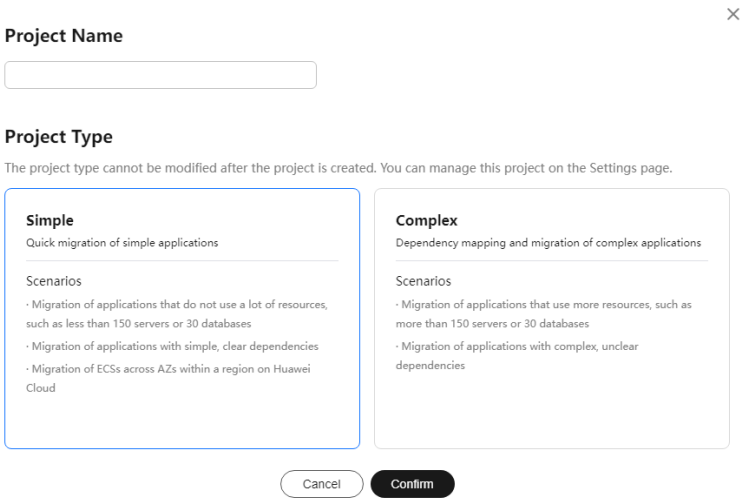
Step 1 Sign in to the MgC console. On the **Overview** page, click **Create Migration Project**.



Step 2 In the displayed dialog box, enter a project name, select a project type, and click **Confirm**.

NOTICE

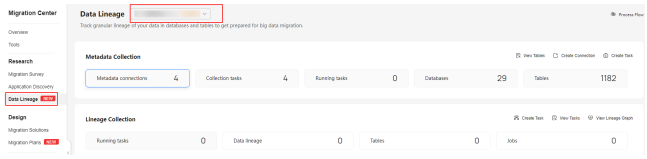
To review this migration project, choose **Settings** > **Migration Projects** in the navigation pane.



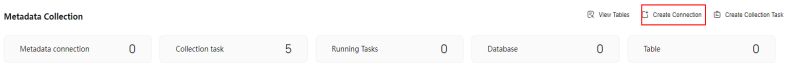
Step 3 Connect Edge to MgC. For more information, see **Connecting the Edge Device to MgC**.

Step 4 After the connection is successful, add the username/password pairs for accessing the source and target ClickHouse servers to Edge. For more information, see **Adding Resource Credentials**.

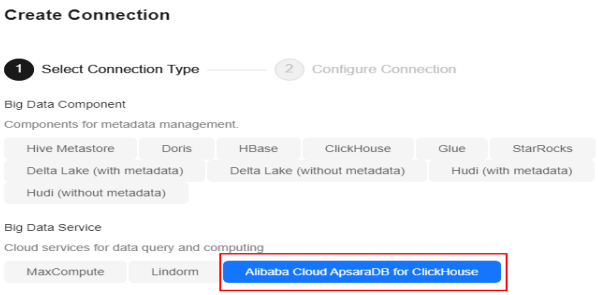
Step 5 On the MgC console, in the navigation pane on the left, choose **Research** > **Data Lineage**. In the upper left corner of the page, choose the migration project created in **step 2** from the drop-down list.



Step 6 In the **Metadata Collection** area, click **Create Connection**.



Step 7 On the **Select Connection Type** page, select **ApsaraDB for ClickHouse** and click **Next**.

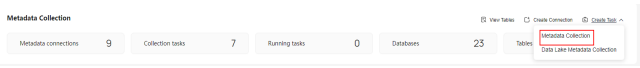


Step 8 Configure the **parameters for creating a ClickHouse connection**, and click **Test**. If the test is successful, the connection is set up.

Table 9-13 Parameters for creating a ClickHouse connection

Parameter	Configuration
Connection To	Select **Source**.
Connection Name	The default name is **ApsaraDB for ClickHouse-***4 random characters* (including letters and numbers). You can also customize a name.
Edge Device	Select the Edge device connected to MgC in **step 3**.
ClickHouse Credential (Optional)	Select the credential used for accessing Alibaba Cloud ApsaraDB for ClickHouse you added to Edge in **step 4**.
Database URL	Enter the public address of the source ClickHouse cluster. You can view the IP address in the cluster details.

Step 9 In the **Metadata Collection** area, choose **Create Task** > **Metadata Collection**.



Step 10 Configure the **parameters for creating a metadata collection task** and click **Confirm**.

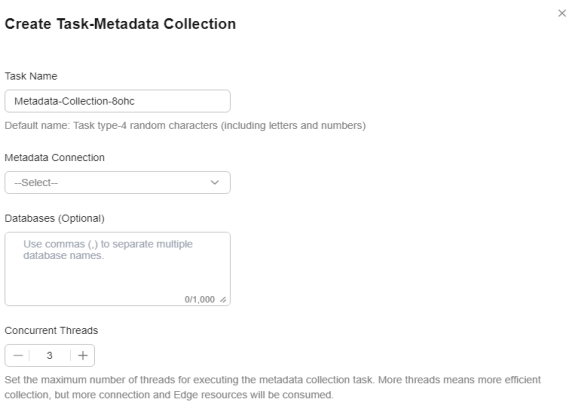
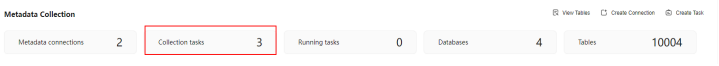


Table 9-14 Parameters for configuring a metadata collection task

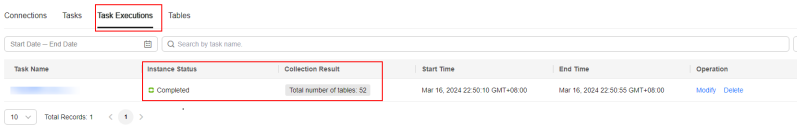
Parameter	Configuration
Task Name	The default name is **Metadata-Collection-***4 random characters* (including letters and numbers). You can also customize a name.
Metadata Connection	Select the connection created in **step 8**.
Databases (Optional)	Enter the names of the databases whose metadata needs to be collected. Use commas (,) to separate the database names. If no database name is specified, the metadata of all databases is collected.
Concurrent Threads	Set the maximum number of threads for executing the collection. The default value is **3**. The value ranges from **1** to **10**. Configuring more concurrent threads means more efficient collection, but more connection and Edge device resources will be consumed.

Step 11 In the **Metadata Collection** area, click **Collection tasks**.

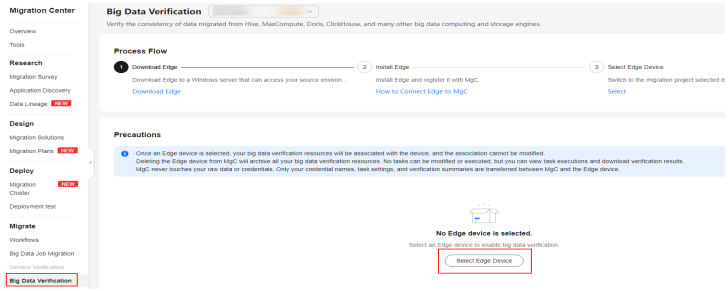


Step 12 Under **Tasks**, you can review the created metadata collection task and its settings. Click **Execute Task** in the **Operation** column to run the task. Each time the task is executed, a task execution is generated.

Step 13 Click **View Executions** in the **Operation** column. Under **Task Executions**, you can view the execution records of the task and the status and collection results of each task execution. When a task execution enters a **Completed** status and the collection results are displayed, you can view the list of databases and tables extracted from collected metadata on the **Tables** tab.



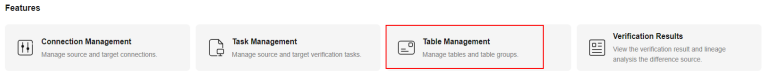
Step 14 In the navigation pane on the left, choose **Migrate** > **Big Data Verification**. If this is your first time to visit this page, select an Edge device to enable the verification feature. Click **Select Edge Device**. In the displayed dialog box, select the Edge device connected to MgC in **step 3**.



CAUTION

Ensure that the selected Edge device is always **Online** and **Enabled** before your verification is complete.

Step 15 In the **Features** area, click **Table Management**.



Step 16 Under **Table Groups**, click **Create**. Configure the **parameters for creating a table group** and click **Confirm**.

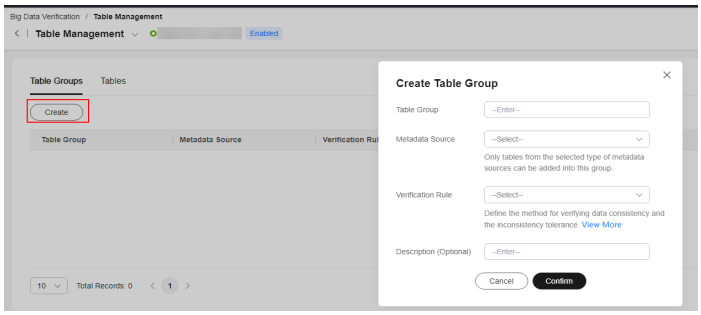
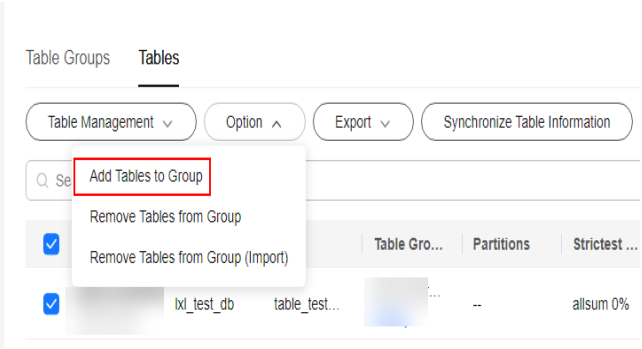


Table 9-15 Parameters for creating a table group

Parameter	Description
Table Group	User-defined
Metadata Connection	Select the connection created in **step 8**. **CAUTION** A table group can only contain tables coming from the same metadata source.

Parameter	Description
Verification Rule	Select a rule that defines the method for verifying data consistency and the inconsistency tolerance. You can **View More** to see more information about the verification rules provided by MgC.
Description (Optional)	Enter a description to identify the table group.

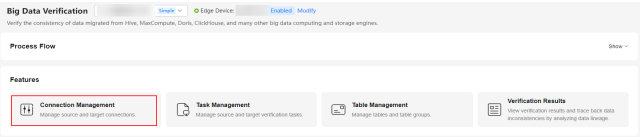
Step 17 On the **Table Management** page, click the **Tables** tab, select the data tables to be added to the same table group, and choose **Option** > **Add Tables to Group** above the list. In the displayed dialog box, select the desired table group and click **Confirm**.



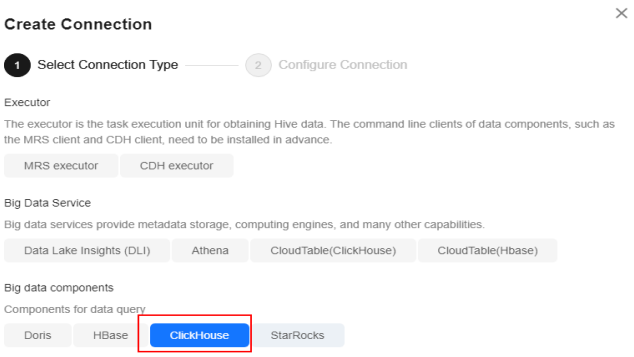
NOTICE

You can manually import information of incremental data tables to MgC. For details, see **Creating a Table Group and Adding Tables to the Group**.

Step 18 On the **Big Data Verification** page, in the **Features** area, click **Connection Management**.



Step 19 Click **Create Connection** in the upper right corner of the page. On the **Select Connection Type** page, select **ClickHouse** and click **Next**.



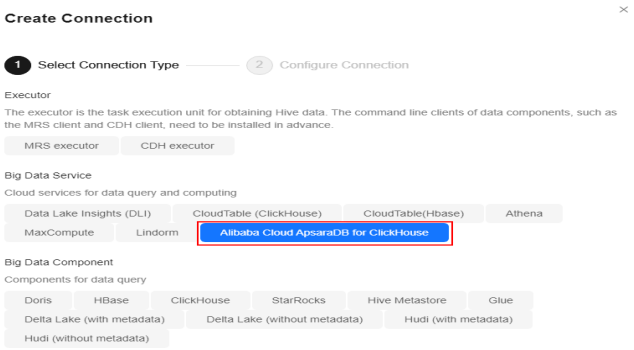
Step 20 Configure the **parameters for creating a ClickHouse connection**, and click **Test**. If the test is successful, the connection is set up.

Table 9-16 Parameters for creating a ClickHouse connection

Parameter	Configuration
Connection To	Select **Target**.
Connection Name	The default name is **ClickHouse-***4 random characters* (including letters and numbers). You can also customize a name.
ClickHouse Credential (Optional)	Select the credential used for accessing the target MRS ClickHouse cluster you added to Edge in **step 4**.
Secured Cluster	Choose whether the cluster is secured.
ClickHouse Server IP Address	Enter the IP address of the MRS ClickHouse server. Generally, the IP address refers to that of the server where ClickHouse is hosted.
HTTP Port	If the MRS ClickHouse cluster is unsecured, enter the HTTP port for communicating with the ClickHouse server. To obtain the value, log in to the **FusionInsight Manager** of the target cluster, choose **Cluster** > **Services** > **ClickHouse** > **Configurations** > **All Configurations**, and search for the **http_port** parameter.
HTTP SSL/TLS Port	If the MRS ClickHouse cluster is secured, enter the HTTPS port for communicating with the ClickHouse server. To obtain the value, log in to the **FusionInsight Manager** of the target cluster, choose **Cluster** > **Services** > **ClickHouse** > **Configurations** > **All Configurations**, and search for the **https_port** parameter.

Step 21 Create a data verification task for the source Alibaba Cloud ApsaraDB for ClickHouse cluster, and execute the task. For more information, see **Creating and Executing Verification Tasks**. During the task creation, select the table group created in **step 16**.

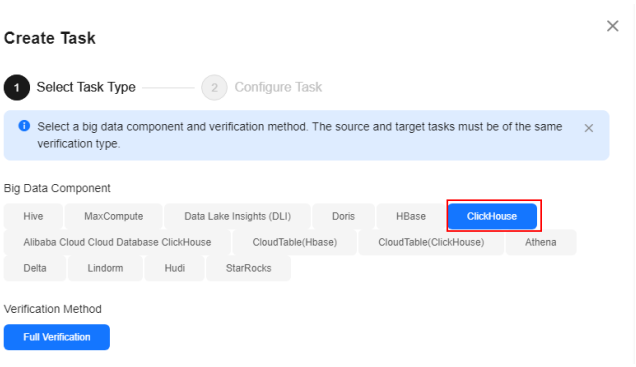
- On the **Select Task Type** page, choose **ApsaraDB for ClickHouse**.



- Select **Full Verification** for **Verification Method**.

Step 22 Create a data verification task for the MRS ClickHouse cluster, and execute the task. For more information, see **Creating and Executing Verification Tasks**. During the task creation, select the table group created in **step 16**.

- On the **Select Task Type** page, choose **ClickHouse**.



- Select **Full Verification** for **Verification Method**.

Step 23 Wait until the task executions enter a **Completed** status. On the **Verification Results** page, you can view and export the task execution results. For details, see **Viewing and Exporting Verification Results**.

----End

9.5 Verifying the Consistency of Data Migrated from Alibaba Cloud ApsaraDB for ClickHouse to Huawei Cloud CloudTable ClickHouse

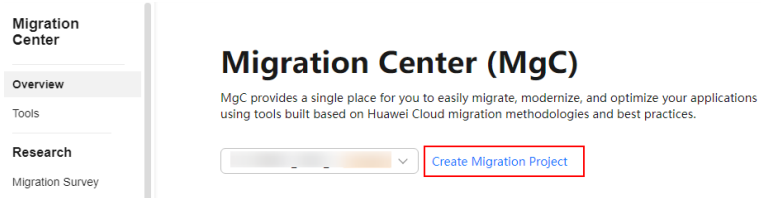
This section describes how to use MgC to verify the consistency of data migrated from Alibaba Cloud ApsaraDB for ClickHouse to Huawei Cloud CloudTable ClickHouse.

Preparations

Install Edge, an MgC tool used for data verification, in the source intranet environment and register an account for using Edge. For details, see **Installing Edge for Linux**.

Procedure

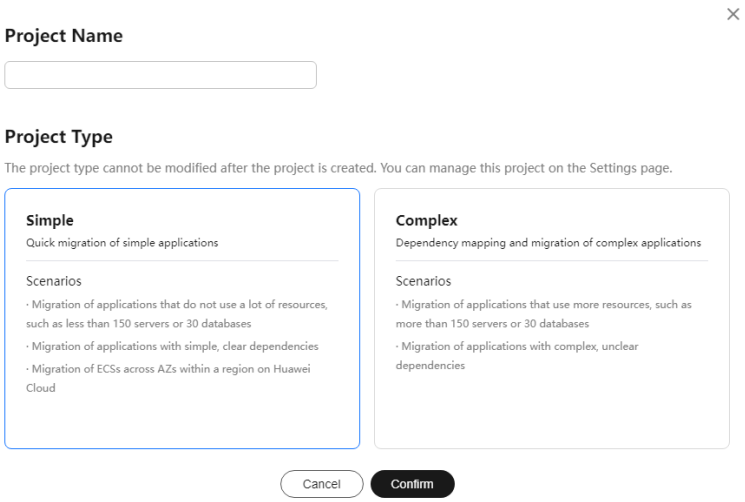
Step 1 Sign in to the MgC console. On the **Overview** page, click **Create Migration Project**.



Step 2 In the displayed dialog box, enter a project name, select a project type, and click **Confirm**.

NOTICE

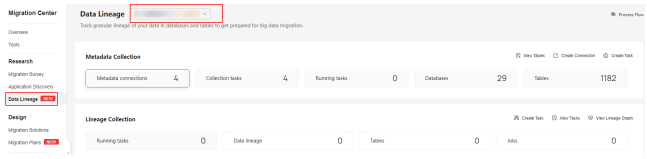
To review this migration project, choose **Settings** > **Migration Projects** in the navigation pane.



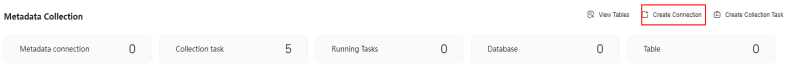
Step 3 Connect Edge to MgC. For more information, see **Connecting the Edge Device to MgC**.

Step 4 After the connection is successful, add the username/password pairs for accessing the source and target ClickHouse servers to Edge. For more information, see **Adding Resource Credentials**.

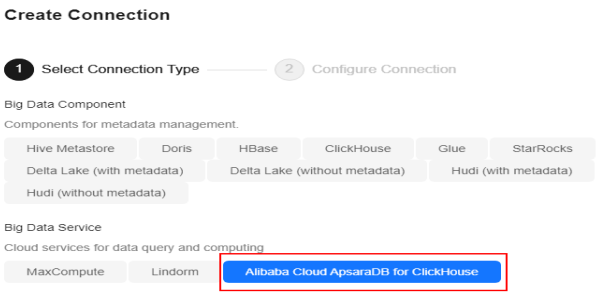
Step 5 On the MgC console, in the navigation pane on the left, choose **Research** > **Data Lineage**. In the upper left corner of the page, choose the migration project created in **step 2** from the drop-down list.



Step 6 In the **Metadata Collection** area, click **Create Connection**.



Step 7 On the **Select Connection Type** page, select **ApsaraDB for ClickHouse** and click **Next**.

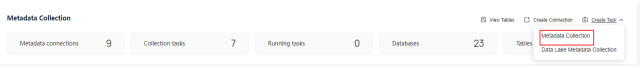


Step 8 Configure the **parameters for creating a ClickHouse connection**, and click **Test**. If the test is successful, the connection is set up.

Table 9-17 Parameters for creating a ClickHouse connection

Parameter	Configuration
Connection To	Select **Source**.
Connection Name	The default name is **ApsaraDB for ClickHouse-***4 random characters* (including letters and numbers). You can also customize a name.
Edge Device	Select the Edge device connected to MgC in **step 3**.
ClickHouse Credential (Optional)	Select the credential used for accessing the source ApsaraDB for ClickHouse cluster you added to Edge in **Step 4**.
Database URL	Enter the public address of the source ClickHouse cluster. You can view the IP address in the cluster details.

Step 9 In the **Metadata Collection** area, choose **Create Task** > **Metadata Collection**.



Step 10 Configure the **parameters for creating a metadata collection task** and click **Confirm**.

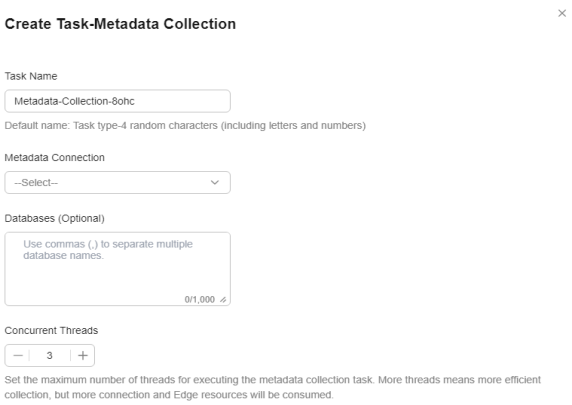
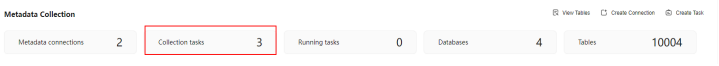


Table 9-18 Parameters for configuring a metadata collection task

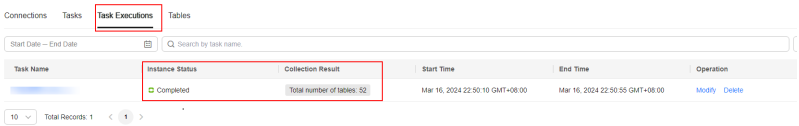
Parameter	Configuration
Task Name	The default name is **Metadata-Collection-***4 random characters* (including letters and numbers). You can also customize a name.
Metadata Connection	Select the connection created in **step 8**.
Databases (Optional)	Enter the names of the databases whose metadata needs to be collected. Use commas (,) to separate the database names. If no database name is specified, the metadata of all databases is collected.
Concurrent Threads	Set the maximum number of threads for executing the collection. The default value is **3**. The value ranges from **1** to **10**. Configuring more concurrent threads means more efficient collection, but more connection and Edge device resources will be consumed.

Step 11 In the **Metadata Collection** area, click **Collection tasks**.

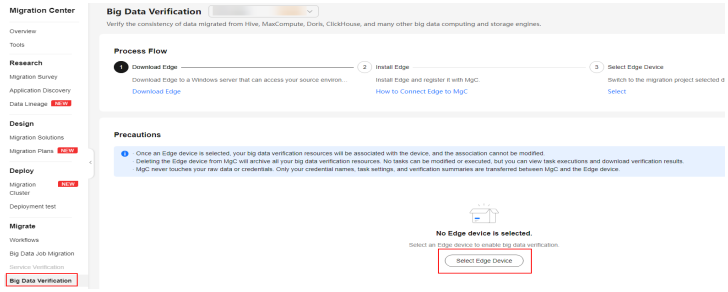


Step 12 Under **Tasks**, you can review the created metadata collection task and its settings. Click **Execute Task** in the **Operation** column to run the task. Each time the task is executed, a task execution is generated.

Step 13 Click **View Executions** in the **Operation** column. Under **Task Executions**, you can view the execution records of the task and the status and collection results of each task execution. When a task execution enters a **Completed** status and the collection results are displayed, you can view the list of databases and tables extracted from collected metadata on the **Tables** tab.



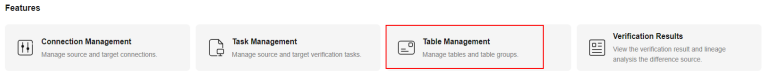
Step 14 In the navigation pane on the left, choose **Migrate** > **Big Data Verification**. If this is your first time to visit this page, select an Edge device to enable the verification feature. Click **Select Edge Device**. In the displayed dialog box, select the Edge device connected to MgC in **step 3**.



CAUTION

Ensure that the selected Edge device is always **Online** and **Enabled** before your verification is complete.

Step 15 In the **Features** area, click **Table Management**.



Step 16 Under **Table Groups**, click **Create**. Configure the **parameters for creating a table group** and click **Confirm**.

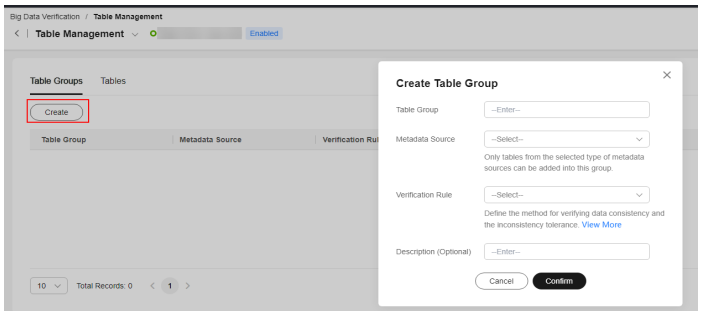
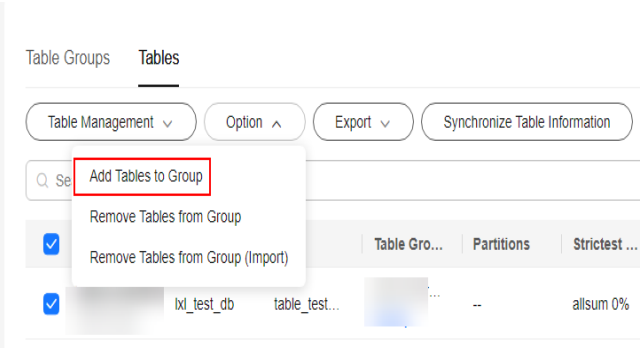


Table 9-19 Parameters for creating a table group

Parameter	Description
Table Group	User-defined
Metadata Connection	Select the connection created in **step 8**. **CAUTION** A table group can only contain tables coming from the same metadata source.

Parameter	Description
Verification Rule	Select a rule that defines the method for verifying data consistency and the inconsistency tolerance. You can **View More** to see more information about the verification rules provided by MgC.
Description (Optional)	Enter a description to identify the table group.

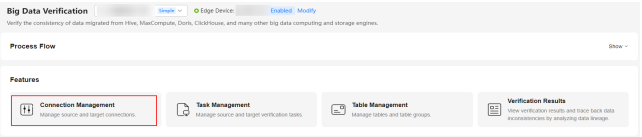
Step 17 On the **Table Management** page, click the **Tables** tab, select the data tables to be added to the same table group, and choose **Option** > **Add Tables to Group** above the list. In the displayed dialog box, select the desired table group and click **Confirm**.



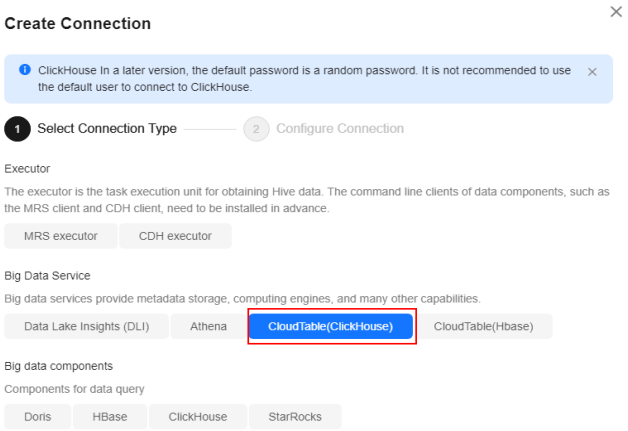
NOTICE

You can manually import information of incremental data tables to MgC. For details, see **Creating a Table Group and Adding Tables to the Group**.

Step 18 On the **Big Data Verification** page, in the **Features** area, click **Connection Management**.



Step 19 Click **Create Connection** in the upper right corner of the page. On the **Select Connection Type** page, select **CloudTable (ClickHouse)** and click **Next**.



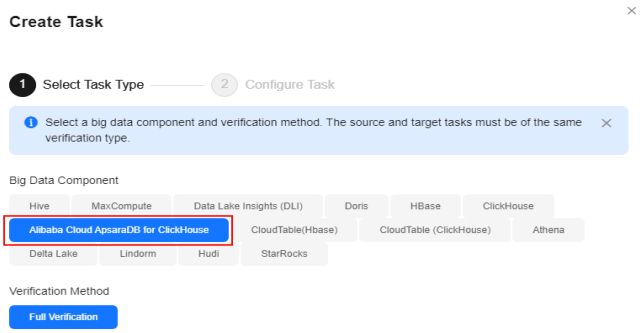
Step 20 Configure the **parameters for creating a ClickHouse connection**, and click **Test**. If the test is successful, the connection is set up.

Table 9-20 Parameters for creating a ClickHouse connection

Parameter	Configuration
Connection To	Select **Target**.
Connection Name	The default name is **CloudTable-ClickHouse***4 random characters* (including letters and numbers). You can also customize a name.
CloudTable (ClickHouse) Credential	Select the credential used for accessing the target CloudTable ClickHouse cluster you added to Edge in **step 4**.
Database URL	Enter the URL to access the CloudTable (ClickHouse) database. You can obtain the access address from the **basic information of the ClickHouse cluster**.

Step 21 Create a data verification task for the source Alibaba Cloud ApsaraDB for ClickHouse cluster, and execute the task. For more information, see **Creating and Executing Verification Tasks**. During the task creation, select the table group created in **step 16**.

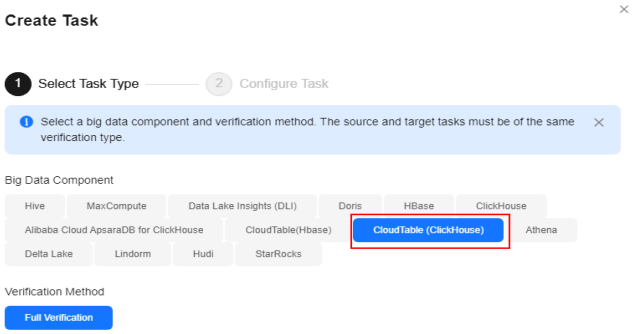
- On the **Select Task Type** page, choose **ApsaraDB for ClickHouse**.



- Select **Full Verification** for **Verification Method**.

Step 22 Create a data verification task for the CloudTable (ClickHouse) cluster, and execute the task. For more information, see **Creating and Executing Verification Tasks**. During the task creation, select the table group created in **step 16**.

- On the **Select Task Type** page, choose **CloudTable (ClickHouse)**.



- Select **Full Verification** for **Verification Method**.

Step 23 Wait until the task executions enter a **Completed** status. On the **Verification Results** page, you can view and export the task execution results. For details, see **Viewing and Exporting Verification Results**.

----End

9.6 Verifying the Consistency of Data Migrated Between MRS Doris Clusters

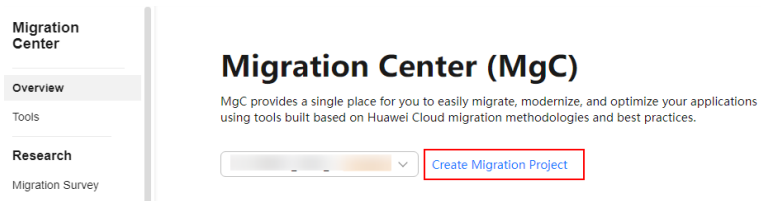
This section describes how to use MgC to verify the consistency of data migrated between different versions of Huawei Cloud MRS Doris clusters.

Preparations

Install Edge, an MgC tool used for data verification, in the source intranet environment and register an account for using Edge. For details, see **Installing Edge for Linux**.

Procedure

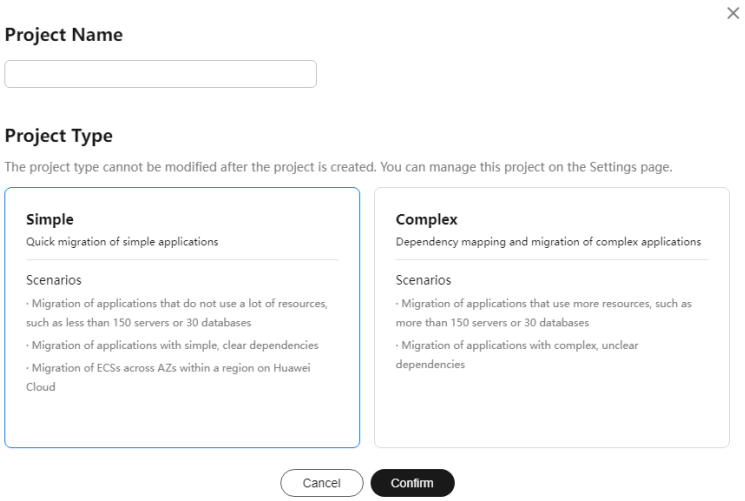
Step 1 Sign in to the **MgC** console. On the **Overview** page, click **Create Migration Project**.



Step 2 In the displayed dialog box, enter a project name, select a project type, and click **Confirm**.

NOTICE

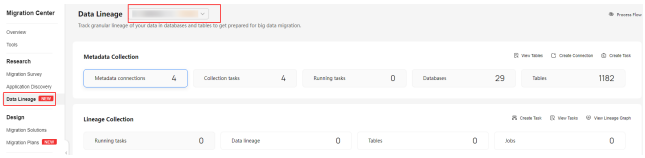
To review this migration project, choose **Settings** > **Migration Projects** in the navigation pane.



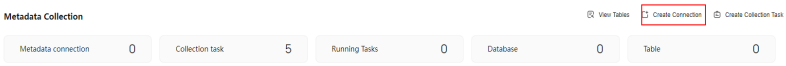
Step 3 Connect Edge to MgC. For more information, see **Connecting the Edge Device to MgC**.

Step 4 After the connection is successful, add the username/password pairs for accessing the source and target MRS Doris clusters to Edge. For more information, see **Adding Resource Credentials**.

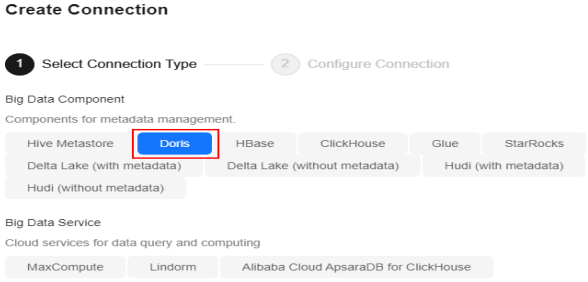
Step 5 On the MgC console, in the navigation pane on the left, choose **Research** > **Data Lineage**. In the upper left corner of the page, choose the migration project created in **step 2** from the drop-down list.



Step 6 In the **Metadata Collection** area, click **Create Connection**.



Step 7 On the **Select Connection Type** page, select **Doris** and click **Next**.

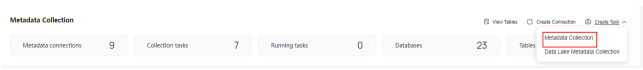


Step 8 Configure the **parameters for creating a Doris connection**, and click **Test**. If the test is successful, the connection is set up.

Table 9-21 Parameters for creating a Doris connection

Parameter	Configuration
Connection To	Select **Source**.
Connection Name	The default name is **Doris-***4 random characters* (including letters and numbers). You can also customize a name.
Edge Device	Select the Edge device connected to MgC in **step 3**.
Doris Credential	Select the credential used for accessing the source MRS Doris cluster you added to Edge in **Step 4**.
Database IP Address	Enter the IP address of the Doris FE instance that is connected to the source Doris database. To obtain the IP address of a Doris FE instance, log in to the **MRS Manager** of the cluster and choose **Cluster** > **Services** > **Doris** > **Instances** to view the IP address of any FE instance.
Database Port	Enter the port for connecting to the source Doris database. The database connection port is the query connection port of the Doris FE. To obtain the port, you can log in to the MRS Manager, choose **Cluster** > **Services** > **Doris** > **Configurations**, and query the value of **query_port** of the Doris service.
Database Name	Enter the name of the source Doris database.

Step 9 In the **Metadata Collection** area, choose **Create Task** > **Metadata Collection**.



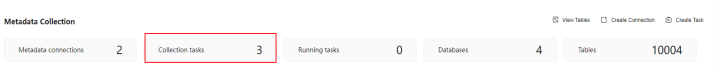
Step 10 Configure the **parameters for creating a metadata collection task** and click **Confirm**.

Table 9-22 Parameters for configuring a metadata collection task

Parameter	Configuration
Task Name	The default name is **Metadata-Collection-***4 random characters* (including letters and numbers). You can also specify a name.
Metadata Connection	Select the connection created in **step 8**.

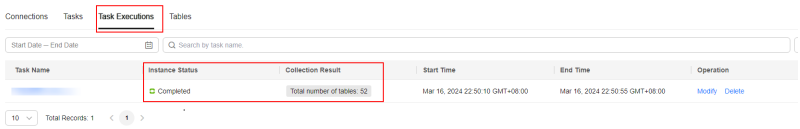
Parameter	Configuration
Databases	Enter the names of the databases whose metadata needs to be collected. Use commas (,) to separate the database names. If no database name is specified, the metadata of all databases is collected.
Concurrent Threads	Set the maximum number of threads for executing the collection. The default value is **3**. The value ranges from **1** to **10**. Configuring more concurrent threads means more efficient collection, but more connection and Edge device resources will be consumed.

Step 11 In the **Metadata Collection** area, click **Collection tasks**.

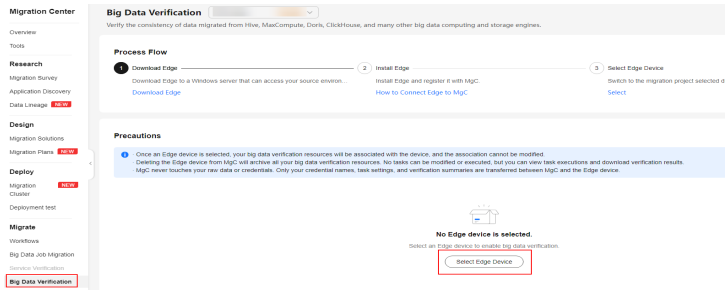


Step 12 Under **Tasks**, you can review the created metadata collection task and its settings. Click **Execute Task** column to run the task. Each time the task is executed, a task execution is generated.

Step 13 Click **View Executions** in the **Operation** column. Under **Task Executions**, you can view the execution records of the task and the status and collection results of each task execution. When a task execution enters a **Completed** status and the collection results are displayed, you can view the list of databases and tables extracted from collected metadata on the **Tables** tab.



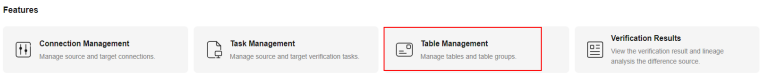
Step 14 In the navigation pane on the left, choose **Migrate** > **Big Data Verification**. If this is your first time to visit this page, select an Edge device to enable the verification feature. Click **Select Edge Device**. In the displayed dialog box, select the Edge device connected to MgC in **step 3**.



CAUTION

Ensure that the selected Edge device is always **Online** and **Enabled** before your verification is complete.

Step 15 In the **Features** area, click **Table Management**.



Step 16 Under **Table Groups**, click **Create**. Configure the **parameters for creating a table group** and click **Confirm**.

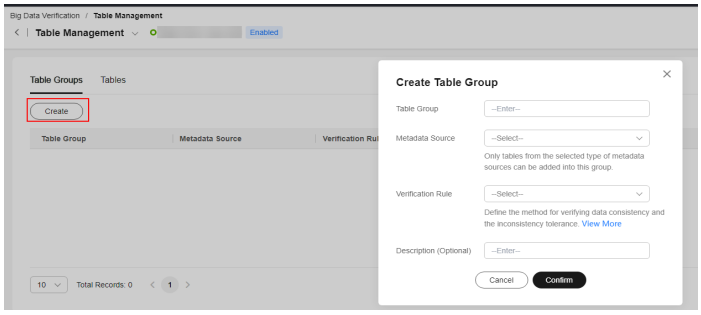
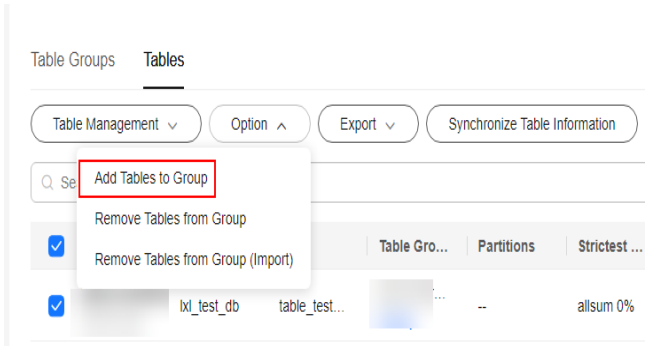


Table 9-23 Parameters for creating a table group

Parameter	Description
Table Group	Enter a name.
Metadata Connection	Select the connection created in **step 8**. **CAUTION** A table group can only contain tables coming from the same metadata source.
Verification Rule	Select a rule that defines the method for verifying data consistency and the inconsistency tolerance. You can **View More** to see the details about the verification rules provided by MgC.
Description (Optional)	Enter a description to identify the table group.

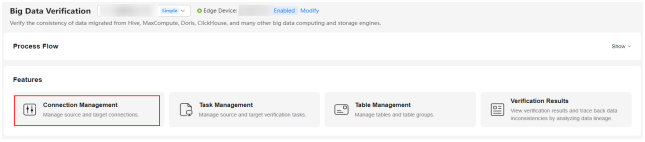
Step 17 On the **Table Management** page, click the **Tables** tab, select the data tables to be added to the same table group, and choose **Option** > **Add Tables to Group** above the list. In the displayed dialog box, select the desired table group and click **Confirm**.



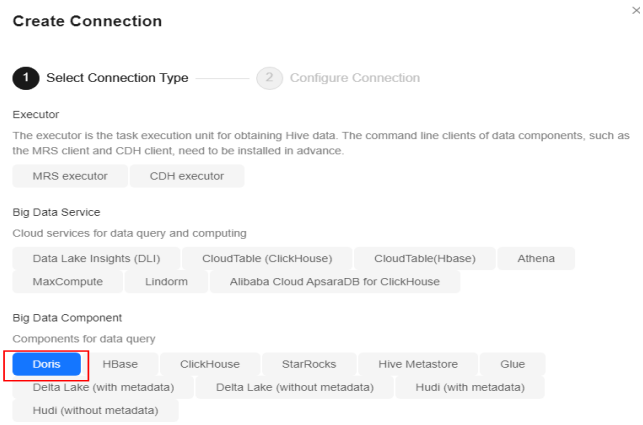
NOTICE

You can manually import information of incremental data tables to MgC. For details, see **Creating a Table Group and Adding Tables to the Group**.

Step 18 On the **Big Data Verification** page, in the **Features** area, click **Connection Management**.



Step 19 Click **Create Connection** in the upper right corner of the page. On the **Select Connection Type** page, select **Doris** and click **Next**.



Step 20 Set connection parameters based on **Table 9-24** and click **Test**. If the test is successful, the connection is set up.

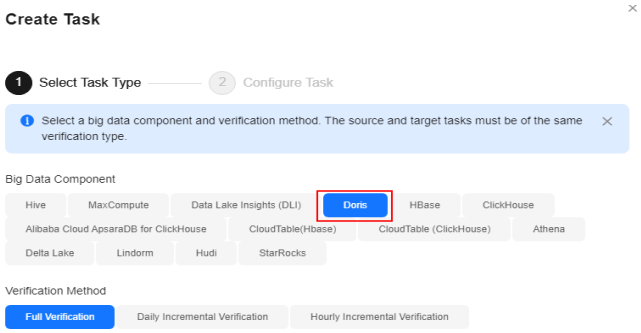
Table 9-24 Parameters for creating a Doris connection

Parameter	Configuration
Connection To	Select **Target**.
Connection Name	The default name is **Doris-***4 random characters* (including letters and numbers). You can also customize a name.
Doris Credential	Select the credential used for accessing the target MRS HBase cluster you added to Edge in **step 4**.
Database IP Address	Enter the IP address of the Doris FE instance that is connected to the target Doris database. To obtain the IP address of a Doris FE instance, log in to the **MRS Manager** of the cluster and choose **Cluster** > **Services** > **Doris** > **Instances** to view the IP address of any FE instance.

Parameter	Configuration
Database Port	Enter the port for connecting to the target Doris database. The database connection port is the query connection port of the Doris FE. To obtain the port, you can log in to MRS Manager, choose **Cluster** > **Services** > **Doris** > **Configurations**, and query the value of **query_port** of the Doris service.
Database Name	Enter the name of the MRS Doris database where the data to be verified is located.

Step 21 On the MgC console, create a verification task for the source and target Doris clusters, respectively, and execute the tasks. For details, see **Creating and Executing Verification Tasks**. During the task creation, select the table group created in **step 16**.

- On the **Select Task Type** page, choose **Doris**.



- Select a verification method. For details about each verification method, see **Verification Methods**.

Step 22 Wait until the task executions enter a **Completed** status. You can view and export the task execution results on the **Verification Results** page. For details, see **Viewing and Exporting Verification Results**.

----End

9.7 Verifying the Consistency of Data Migrated Between MRS Doris Clusters or from CDH or EMR to MRS Doris

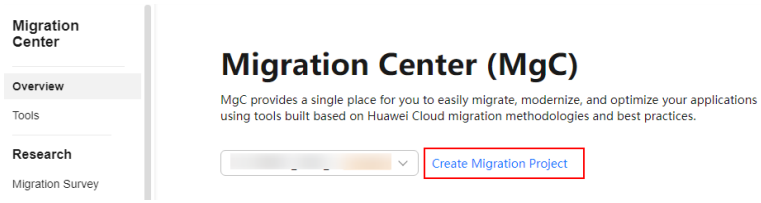
This section describes how to use MgC to verify the consistency of data migrated between Huawei Cloud MRS Doris clusters or migrated from self-built CDH or EMR clusters to Huawei Cloud MRS Doris clusters.

Preparations

Install Edge, an MgC tool used for data verification, in the source intranet environment and register an account for using Edge. For details, see **Installing Edge for Linux**.

Procedure

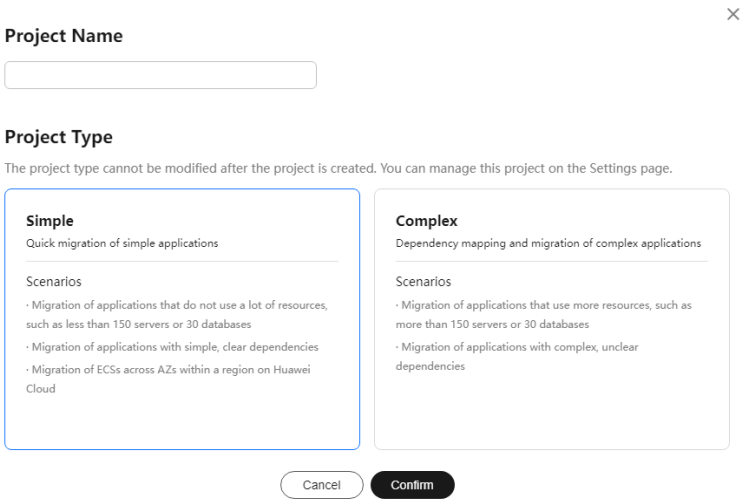
Step 1 Sign in to the **MgC** console. On the **Overview** page, click **Create Migration Project**.



Step 2 In the displayed dialog box, enter a project name, select a project type, and click **Confirm**.

NOTICE

To review this migration project, choose **Settings** > **Migration Projects** in the navigation pane.



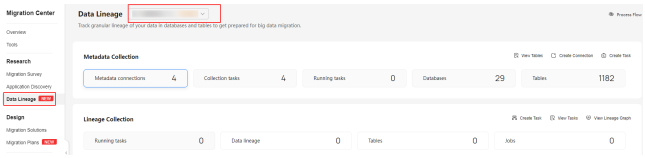
Step 3 Connect Edge to MgC. For more information, see **Connecting the Edge Device to MgC**.

Step 4 After the connection is successful, add the username/password pairs for accessing the source and target executors to Edge. For more information, see **Adding Resource Credentials**.

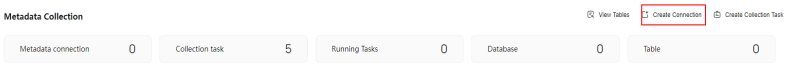
NOTICE

If the source MRS Hive cluster is secured (with Kerberos authentication enabled), add the Hive Metastore credential. You need to set **Type** to **Big Data - Hive Metastore** and **Authentication** to **Username/Key**. Upload the **core-site.xml**, **hivemetastore-site.xml**, **hive-site.xml**, **krb5.conf**, and **user.keytab** files. For details about how to obtain the certificate file, see **How Do I Obtain the Hive Metastore Credential Files?**

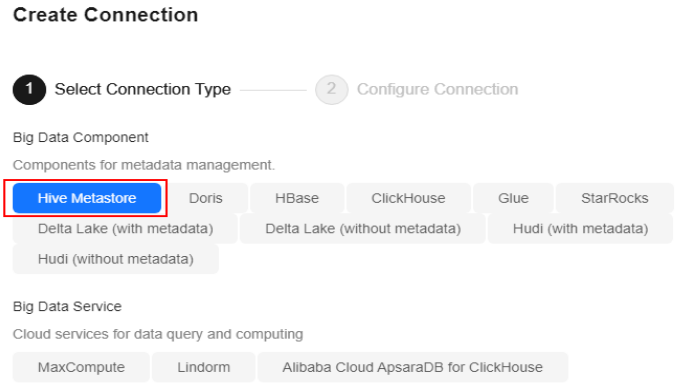
Step 5 On the MgC console, in the navigation pane on the left, choose **Research** > **Data Lineage**. In the upper left corner of the page, choose the migration project created in **step 2**.



Step 6 In the **Metadata Collection** area, click **Create Connection**.



Step 7 On the **Select Connection Type** page, select **Hive Metastore** and click **Next**.



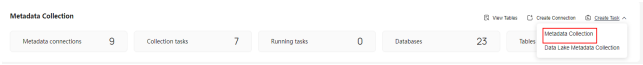
Step 8 Configure the **parameters for creating a Hive Metastore connection**, and click **Test**. If the test is successful, the connection is set up.

Table 9-25 Parameters for creating a Hive Metastore connection

Parameter	Configuration
Connection To	Select **Source**.
Connection Name	The default name is **Hive-Metastore-***4 random characters* (including letters and numbers). You can also customize a name.
Edge Device	Select the Edge device connected to MgC in **step 3**.

Parameter	Configuration
Secure Connection	Decide whether to enable secure connection. • If Hive Metastore is deployed in an unsecured cluster, do not enable secure connection. • If Hive Metastore is deployed in a secured cluster, enable secure connection and provide access credentials. Select the source Hive Metastore credential added to Edge in **step 4**.
Hive Version	Select the Hive version at the source.
Hive Metastore IP Address	Enter the IP address for connecting to the Hive Metastore node.
Hive Metastore Thrift Port	Enter the port for connecting to the Hive Metastore Thrift service. The default port is **9083**.

Step 9 In the **Metadata Collection** area, choose **Create Task** > **Metadata Collection**.



Step 10 Configure the **parameters for creating a metadata collection task** and click **Confirm**.

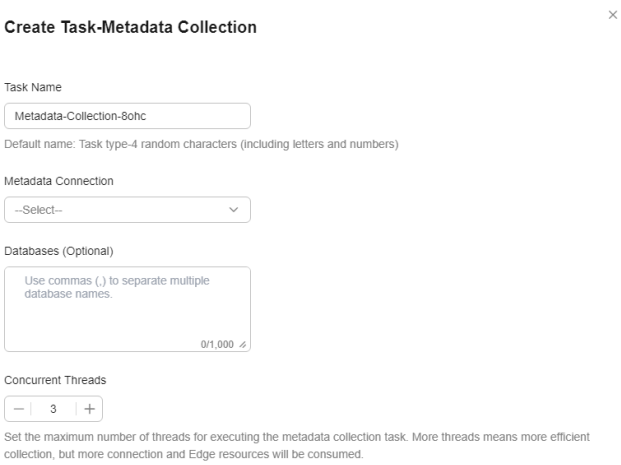
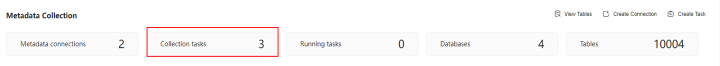


Table 9-26 Parameters for configuring a metadata collection task

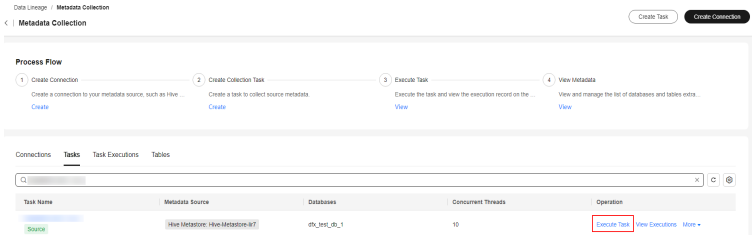
Parameter	Configuration
Task Name	The default name is **Metadata-Collection-***4 random characters* (including letters and numbers). You can also specify a name.
Metadata Connection	Select the connection created in **step 8**.

Parameter	Configuration
Databases (Optional)	Enter the names of the databases whose metadata needs to be collected. If no database name is specified, the metadata of all databases is collected.
Concurrent Threads	Set the maximum number of threads for executing the collection. The default value is **3**. The value ranges from **1** to **10**. Configuring more concurrent threads means more efficient collection, but more connection and Edge device resources will be consumed.

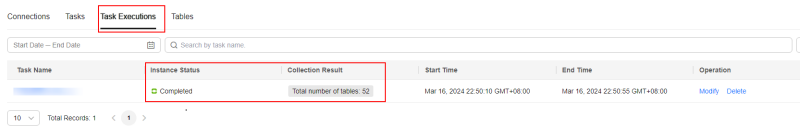
Step 11 In the **Metadata Collection** area, click **Collection tasks**.



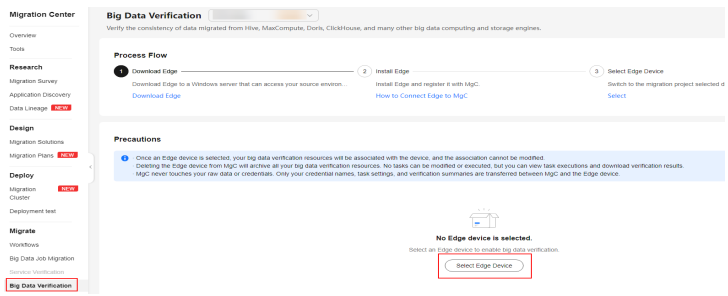
Step 12 Under **Tasks**, you can review the created metadata collection task and its settings. Click **Execute Task** in the **Operation** column to run the task. Each time the task is executed, a task execution is generated.



Step 13 Click **View Executions** in the **Operation** column. Under **Task Executions**, you can view the execution records of the task and the status and collection results of each task execution. When a task execution enters a **Completed** status and the collection results are displayed, you can view the list of databases and tables extracted from collected metadata on the **Tables** tab.



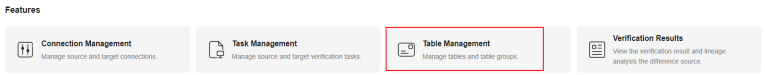
Step 14 In the navigation pane on the left, choose **Migrate** > **Big Data Verification**. If this is your first time to visit this page, select an Edge device to enable the verification feature. Click **Select Edge Device**. In the displayed dialog box, select the Edge device connected to MgC in **step 3**.



CAUTION

Ensure that the selected Edge device is always **Online** and **Enabled** before your verification is complete.

Step 15 In the **Features** area, click **Table Management**.



Step 16 Under **Table Groups**, click **Create**. Configure the **parameters for creating a table group** and click **Confirm**.

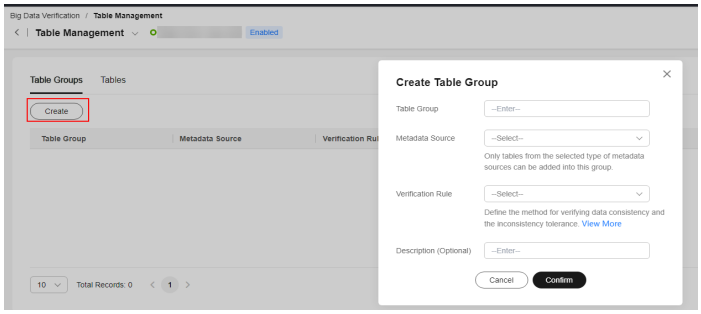
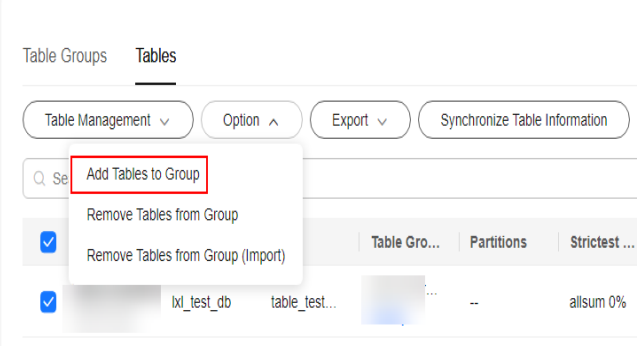


Table 9-27 Parameters for creating a table group

Parameter	Description
Table Group	Enter a name.
Metadata Connection	Select the connection created in **step 8**. **CAUTION** A table group can only contain tables coming from the same metadata source.
Verification Rule	Select a rule that defines the method for verifying data consistency and the inconsistency tolerance. You can **View More** to see the details about the verification rules provided by MgC.
Description (Optional)	Enter a description to identify the table group.

Step 17 On the **Table Management** page, click the **Tables** tab, select the data tables to be added to the same table group, and choose **Option** > **Add Tables to Group** above the list. In the displayed dialog box, select the desired table group and click **Confirm**.



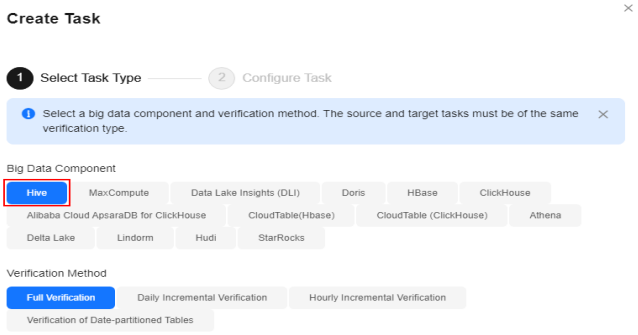
NOTICE

You can manually import information of incremental data tables to MgC. For details, see **Creating a Table Group and Adding Tables to the Group**.

Step 18 Create a connection to the source and target executors separately. For details, see **Creating an Executor Connection**. Select the source and target executor credentials added to Edge in **step 4**.

Step 19 Create a data verification task for the source and target Hive clusters, respectively, and execute the tasks. For more information, see **Creating and Executing Verification Tasks**. During the task creation, select the table group created in **step 16**.

- On the **Select Task Type** page, choose **Hive**.



- Select a verification method. For details about each verification method, see **Verification Methods**.

Step 20 Wait until the task executions enter a **Completed** status. You can view and export the task execution results on the **Verification Results** page. For details, see **Viewing and Exporting Verification Results**.

----End

9.8 Verifying the Consistency of Data Migrated from Alibaba Cloud MaxCompute to Huawei Cloud DLI

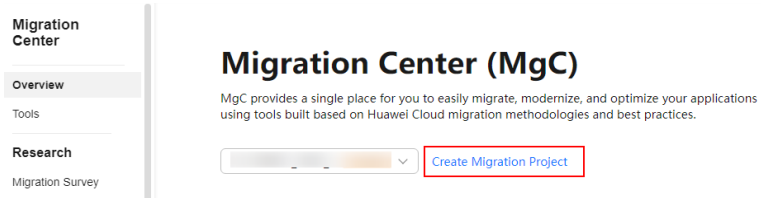
This section describes how to use MgC to verify the consistency of data migrated from Alibaba Cloud MaxCompute to Huawei Cloud MRS Hive.

Preparations

Install Edge, an MgC tool used for data verification, in the source intranet environment and register an account for using Edge. For details, see **Installing Edge for Linux**.

Procedure

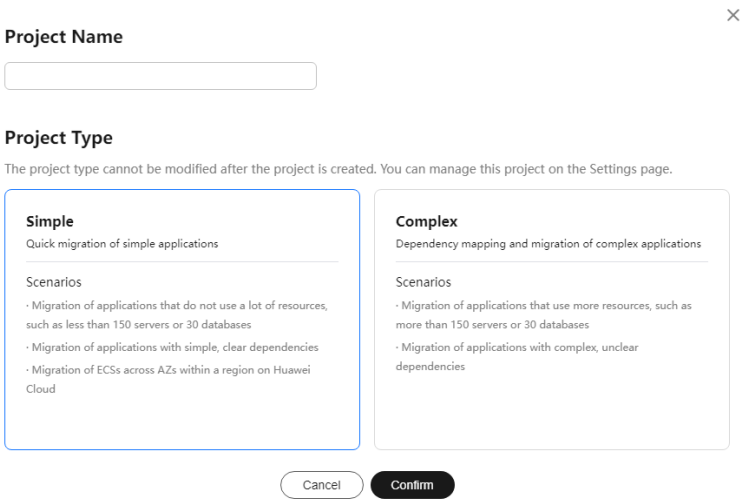
Step 1 Sign in to the **MgC** console. On the **Overview** page, click **Create Migration Project**.



Step 2 In the displayed dialog box, enter a project name, select a project type, and click **Confirm**.

NOTICE

To review this migration project, choose **Settings** > **Migration Projects** in the navigation pane.

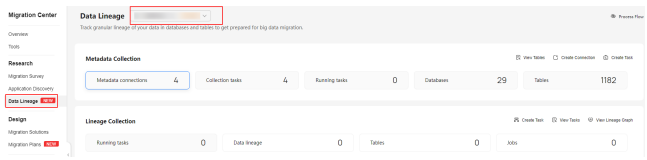


Step 3 Connect Edge to MgC. For more information, see **Connecting the Edge Device to MgC**.

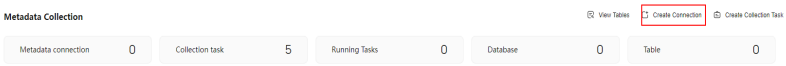
Step 4 After the connection is successful, add the AK/SK pair for accessing MaxCompute and the username/passwords pairs for accessing Hive Metastore and MRS executor to Edge. For more information, see **Adding Resource Credentials**.

- For details about how to obtain an AK/SK pair for accessing MaxCompute, see **Viewing the Information About AccessKey Pairs of a RAM User**.
- For details about how to obtain the Hive Metastore credential files, see **How Do I Obtain the Hive Metastore Credential Files?**

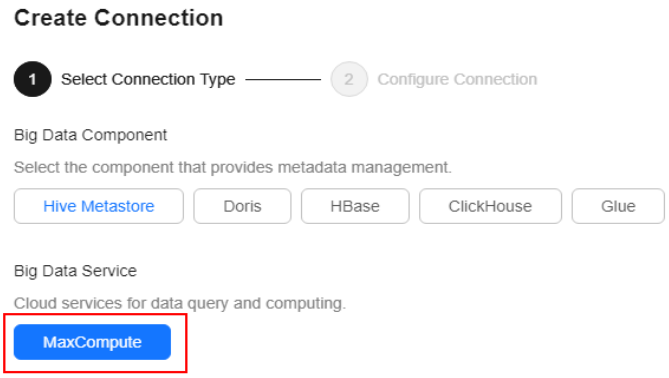
Step 5 On the MgC console, in the navigation pane on the left, choose **Research** > **Data Lineage**. In the upper left corner of the page, choose the migration project created in **step 2**.



Step 6 In the **Metadata Collection** area, click **Create Connection**.



Step 7 On the **Select Connection Type** page, select **MaxCompute** and click **Next**.



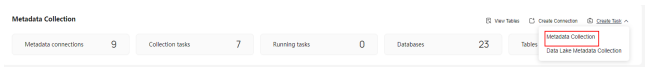
Step 8 Configure the **parameters for creating a MaxCompute connection**, and click **Test**. If the test is successful, the connection is set up.

Table 9-28 Parameters for creating a MaxCompute connection

Parameter	Configuration
Connection To	Select **Source**.
Connection Name	The default name is **MaxCompute-***4 random characters* (including letters and numbers). You can also customize a name.
Edge Device	Select the Edge device connected to MgC in **step 3**.
Alibaba Cloud Credential	Select the MaxCompute credential added to Edge in **step 4**.
MaxCompute Project	Enter the name of your MaxCompute project. You can obtain the project name from the MaxCompute console.

Parameter	Configuration
Endpoint	Enter the endpoint of the region where the MaxCompute project is located. For details about the MaxCompute endpoints in different regions, see **MaxCompute Endpoints**.

Step 9 In the **Metadata Collection** area, choose **Create Task** > **Metadata Collection**.



Step 10 Configure the **parameters for creating a metadata collection task** and click **Confirm**.

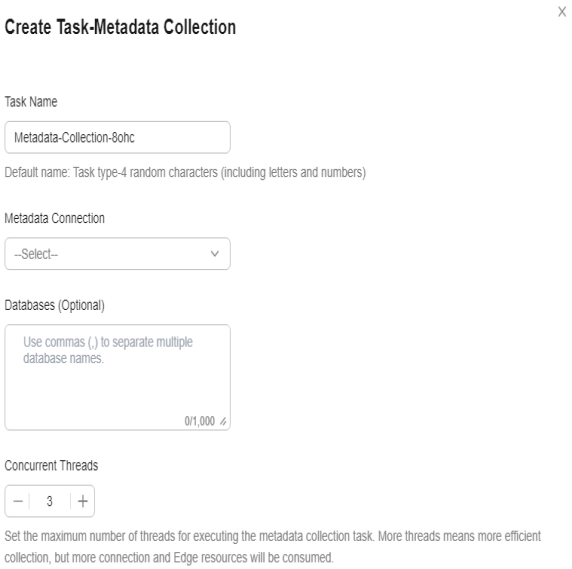
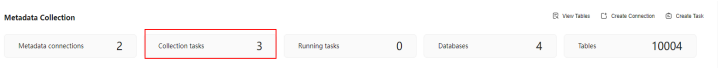


Table 9-29 Parameters for configuring a metadata collection task

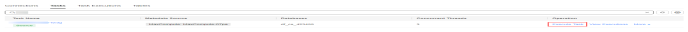
Parameter	Configuration
Task Name	The default name is **Metadata-Collection-***4 random characters* (including letters and numbers). You can also specify a name.
Metadata Connection	Select the connection created in **step 8**.
Databases	Enter the names of the databases whose metadata needs to be collected. Use commas (,) to separate the database names. **NOTICE** This parameter is mandatory only if a MaxCompute metadata connection is selected.

Parameter	Configuration
Concurrent Threads	Set the maximum number of threads for executing the collection. The default value is **3**. The value ranges from **1** to **10**. Configuring more concurrent threads means more efficient collection, but more connection and Edge device resources will be consumed.

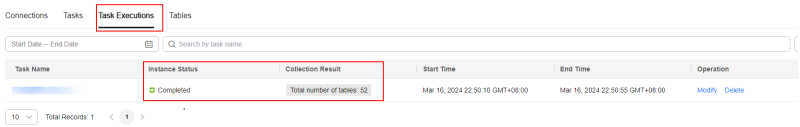
Step 11 In the **Metadata Collection** area, click **Collection tasks**.



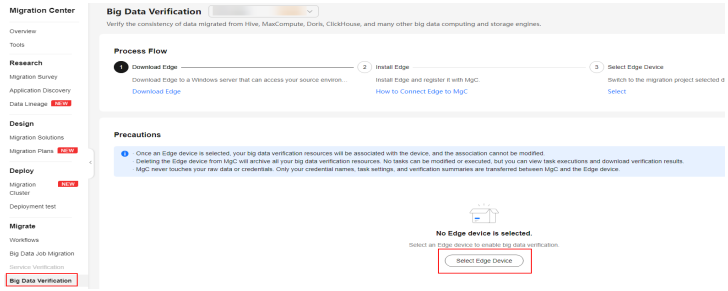
Step 12 Under **Tasks**, you can review the created metadata collection task and its settings. Click **Execute Task** in the **Operation** column to run the task. Each time the task is executed, a task execution is generated.



Step 13 Click **View Executions** in the **Operation** column. Under **Task Executions**, you can view the execution records of the task and the status and collection results of each task execution. When a task execution enters a **Completed** status and the collection results are displayed, you can view the list of databases and tables extracted from collected metadata on the **Tables** tab.



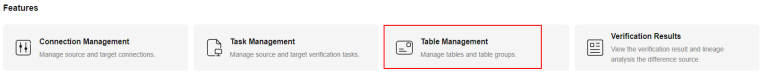
Step 14 In the navigation pane on the left, choose **Migrate** > **Big Data Verification**. If this is your first time to visit this page, select an Edge device to enable the verification feature. Click **Select Edge Device**. In the displayed dialog box, select the Edge device connected to MgC in **step 3**.



CAUTION

Ensure that the selected Edge device is always **Online** and **Enabled** before your verification is complete.

Step 15 In the **Features** area, click **Table Management**.



Step 16 Under **Table Groups**, click **Create**. Configure the **parameters for creating a table group** and click **Confirm**.

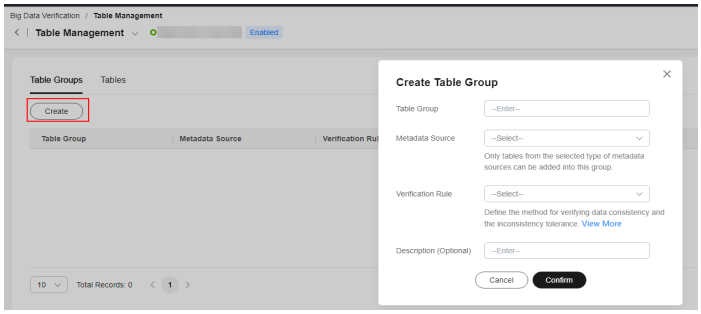
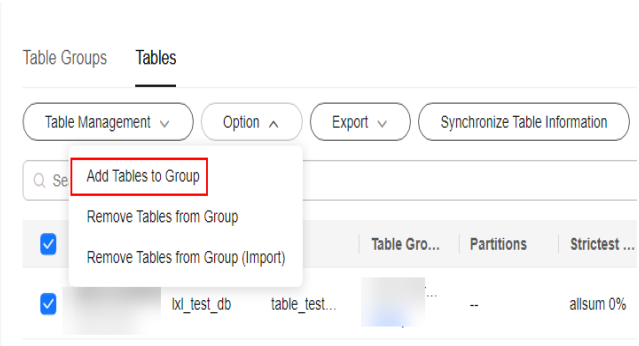


Table 9-30 Parameters for creating a table group

Parameter	Description
Table Group	Enter a name.
Metadata Connection	Select the connection created in **step 8**. **CAUTION** A table group can only contain tables coming from the same metadata source.
Verification Rule	Select a rule that defines the method for verifying data consistency and the inconsistency tolerance. You can **View More** to see the details about the verification rules provided by MgC.
Description (Optional)	Enter a description to identify the table group.

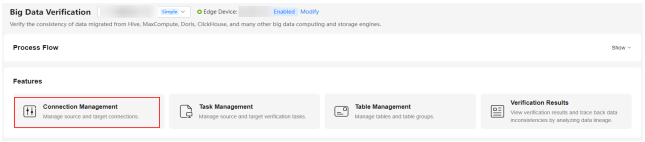
Step 17 On the **Table Management** page, click the **Tables** tab, select the data tables to be added to the same table group, and choose **Option** > **Add Tables to Group** above the list. In the displayed dialog box, select the desired table group and click **Confirm**.



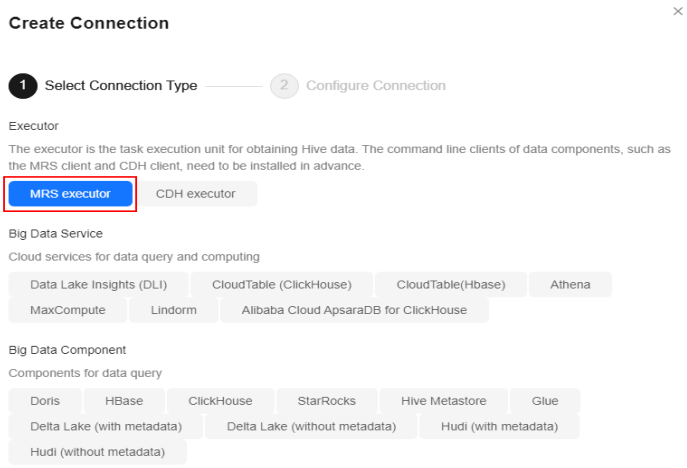
NOTICE

You can manually import information of incremental data tables to MgC. For details, see **Creating a Table Group and Adding Tables to the Group**.

Step 18 On the **Big Data Verification** page, in the **Features** area, click **Connection Management**.



Step 19 Click **Create Connection** in the upper right corner of the page. On the **Select Connection Type** page, select **MRS executor** and click **Next**.



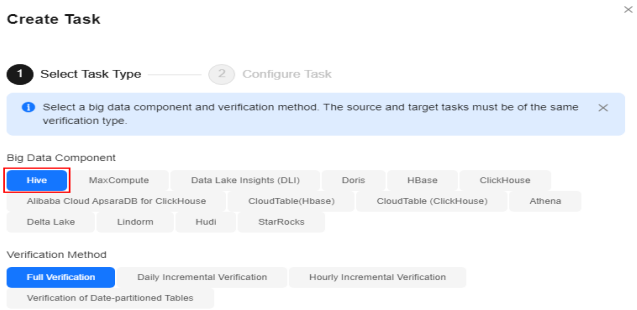
Step 20 Set connection parameters based on **Table 9-31** and click **Test**. If the test is successful, the connection is set up.

Table 9-31 Parameters for creating an executor connection

Parameter	Configuration
Connection To	Select **Target**.
Connection Name	The default name is *Executor type*-4 random characters (including letters and numbers). You can also customize a name.
Executor Credential	Select the MRS executor credential added to Edge in **step 4**.
Executor IP Address	Enter the IP address for connecting to the executor.
Executor Port	Enter the port for connecting to the executor. The default port is **22**.
Installation Directory	Enter the installation directory of the MRS client. That is, the directory where **./install.sh** is installed.
SQL File Location	Enter a directory for storing the SQL files generated for consistency verification. You must have the read and write permissions for the directory. **NOTICE** After the migration is complete, you need to manually clear the folders generated at this location to release storage space.

Step 21 On the MgC console, create a verification task for the source and target Hive clusters, respectively, and execute the tasks. For details, see **Creating and Executing Verification Tasks**. Select the table group created in **step 16** and the MRS executor connection created in **step 20**.

- On the **Select Task Type** page, choose **Hive**.



- Select a verification method. For details about each verification method, see **Verification Methods**.

Step 22 Wait until the task executions enter a **Completed** status. You can view and export the task execution results on the **Verification Results** page. For details, see **Viewing and Exporting Verification Results**.

----End

9.9 Verifying the Consistency of Data Migrated Between MRS HBase Clusters

This section describes how to use MgC to verify the consistency of data migrated between different versions of Huawei Cloud MRS HBase clusters.

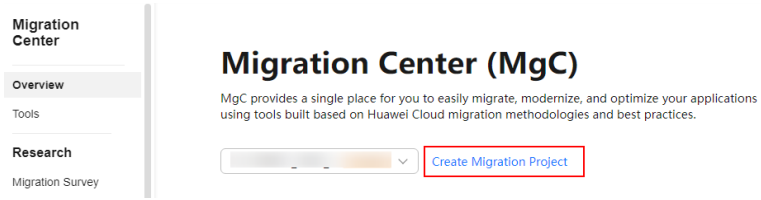
Preparations

- Install Edge, an MgC tool used for data verification, in the source intranet environment and register an account for using Edge. For details, see **Installing Edge for Linux**.
- Add the mappings between the hostnames and IP addresses of all nodes in the source and target clusters to the **/etc/hosts** file on the server where Edge is installed.
  a. On the server where Edge is installed, open the **/etc/hosts** file.
  b. In the **/etc/hosts** file, add a line for each node in the source and target clusters in the following format:
  ```
  IP address Hostname
  ```
  For example, if a node uses the IP address **192.168.1.1** and has the hostname **source-node-01**, add the following information:
  ```
  192.168.1.1 source-node-01
  ```
  c. After all mappings are added, save and close the **/etc/hosts** file.
  d. Ping a hostname to check whether it can be resolved successfully. For example:


```
ping source-node-01
```

Procedure

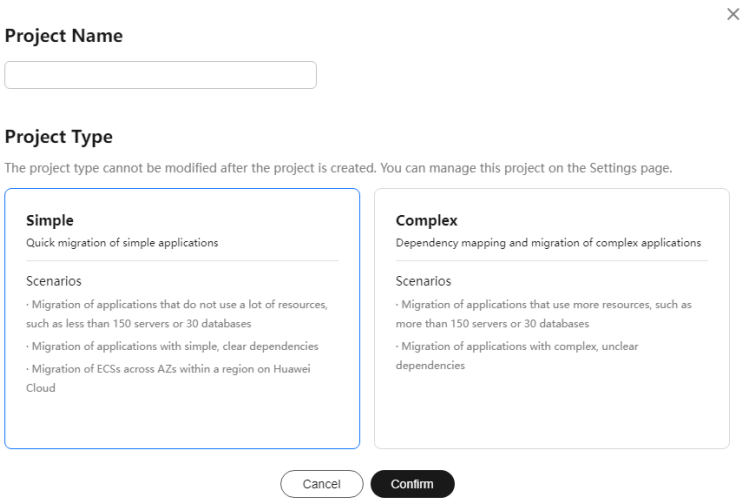
Step 1 Sign in to the MgC console. On the **Overview** page, click **Create Migration Project**.



Step 2 In the displayed dialog box, enter a project name, select a project type, and click **Confirm**.

NOTICE

To review this migration project, choose **Settings** > **Migration Projects** in the navigation pane.



Step 3 Connect Edge to MgC. For more information, see **Connecting the Edge Device to MgC**.

Step 4 After the connection is successful, add the username/key pairs for accessing the source and target MRS HBase clusters to Edge. For more information, see **Adding Resource Credentials**. Enter the username for logging in to the HBase client in the **Username** box and upload the configuration files for **Key**:

- For an unsecured cluster (with Kerberos authentication disabled), you need to upload five configuration files: **core-site.xml**, **hdfs-site.xml**, **yarn-site.xml**, **mapred-site.xml**, and **hbase-site.xml**. For details about how to obtain the configuration files, see **Preparing the Configuration Files of the Running Environment**. Review whether Kerberos authentication is enabled for the cluster in the **basic cluster information**.
- For a secured cluster (with Kerberos authentication enabled), upload seven files: **core-site.xml**, **hdfs-site.xml**, **yarn-site.xml**, **krb5.conf**, **user.keytab**,

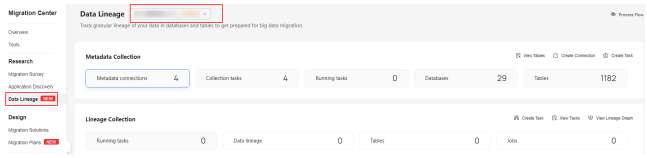
mapred-site.xml, and **hbase-site.xml**. The **krb5.conf** and **user.keytab** files contain the credentials of the cluster users. You can perform the following steps to obtain the two files. For details about how to obtain the other five configuration files, see **Preparing the Configuration Files of the Running Environment**.

a. Log in to **FusionInsight Manager**, and choose **System** > **Permission** > **User**.

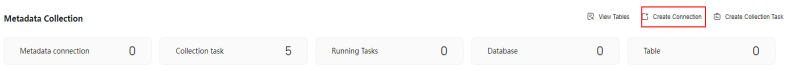
b. Select **developuser** and choose **More** > **Download Authentication Credential** to download the authentication credential files.

c. Decompress the downloaded file to obtain the **user.keytab** and **krb5.conf** files.

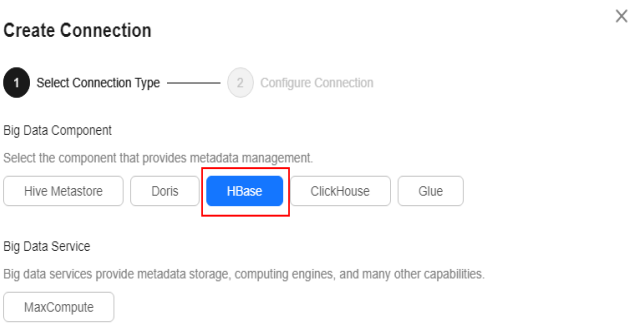
Step 5 On the MgC console, in the navigation pane on the left, choose **Research** > **Data Lineage**. In the upper left corner of the page, choose the migration project created in **step 2**.



Step 6 In the **Metadata Collection** area, click **Create Connection**.



Step 7 On the **Select Connection Type** page, select **HBase** and click **Next**.



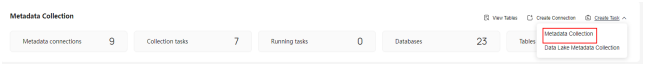
Step 8 Set connection parameters based on **Table 9-32** and click **Test**. If the test is successful, the connection is set up.

Table 9-32 Parameters for creating an HBase connection

Parameter	Configuration
Connection To	Select **Source**.
Connection Name	The default name is **HBase-***4 random characters* (including letters and numbers). You can also customize a name.
Edge Device	Select the Edge device connected to MgC in **step 3**.

Parameter	Configuration
HBase Credential	Select the credential used for accessing the source MRS HBase cluster you added to Edge in **step 4**.
Secured Cluster	Choose whether the cluster is secured.
ZooKeeper IP Address	Enter the IP address for connecting to the ZooKeeper node. You can enter the public or private IP address of the ZooKeeper node.
ZooKeeper Port	Enter the port for connecting to the ZooKeeper node.
HBase Version	Select the HBase version.

Step 9 In the **Metadata Collection** area, choose **Create Task** > **Metadata Collection**.

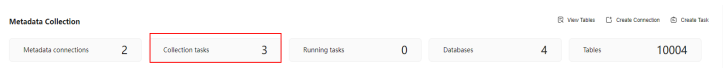


Step 10 Configure the **parameters for creating a metadata collection task** and click **Confirm**.

Table 9-33 Parameters for configuring a metadata collection task

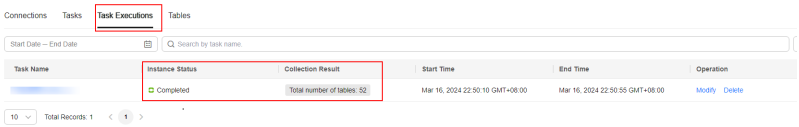
Parameter	Configuration
Task Name	The default name is **Metadata-Collection-***4 random characters* (including letters and numbers). You can also specify a name.
Metadata Connection	Select the connection created in **step 8**.
Databases (Optional)	Enter the names of the databases whose metadata needs to be collected. Use commas (,) to separate the database names. If no database name is specified, the metadata of all databases is collected.
Concurrent Threads	Set the maximum number of threads for executing the collection. The default value is **3**. The value ranges from **1** to **10**. Configuring more concurrent threads means more efficient collection, but more connection and Edge device resources will be consumed.

Step 11 In the **Metadata Collection** area, click **Collection tasks**.

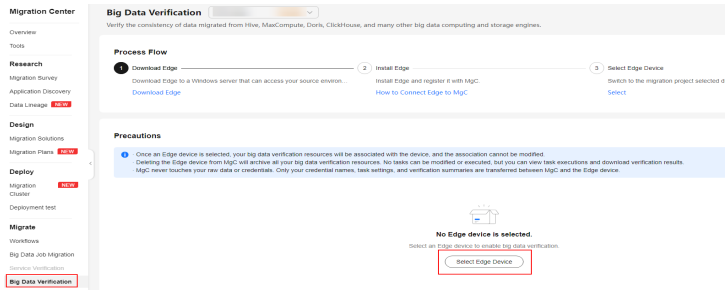


Step 12 Under **Tasks**, you can review the created metadata collection task and its settings. Click **Execute Task** in the **Operation** column to run the task. Each time the task is executed, a task execution is generated.

Step 13 Click **View Executions** in the **Operation** column. Under **Task Executions**, you can view the execution records of the task and the status and collection results of each task execution. When a task execution enters a **Completed** status and the collection results are displayed, you can view the list of databases and tables extracted from collected metadata on the **Tables** tab.



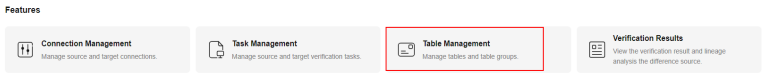
Step 14 In the navigation pane on the left, choose **Migrate** > **Big Data Verification**. If this is your first time to visit this page, select an Edge device to enable the verification feature. Click **Select Edge Device**. In the displayed dialog box, select the Edge device connected to MgC in **step 3**.



CAUTION

Ensure that the selected Edge device is always **Online** and **Enabled** before your verification is complete.

Step 15 In the **Features** area, click **Table Management**.



Step 16 Under **Table Groups**, click **Create**. Configure the **parameters for creating a table group** and click **Confirm**.

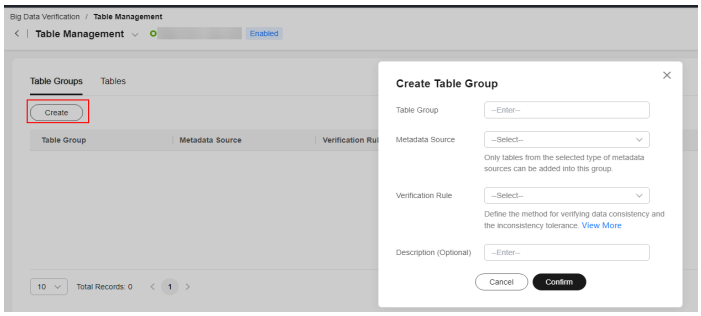
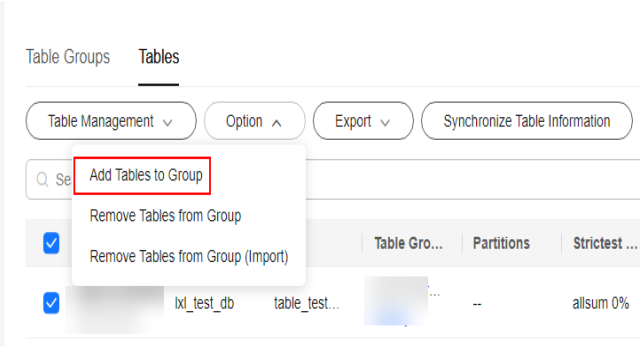


Table 9-34 Parameters for creating a table group

Parameter	Description
Table Group	Enter a name.
Metadata Connection	Select the connection created in **step 8**. **CAUTION** A table group can only contain tables coming from the same metadata source.
Verification Rule	Select a rule that defines the method for verifying data consistency and the inconsistency tolerance. You can **View More** to see the details about the verification rules provided by MgC.
Description (Optional)	Enter a description to identify the table group.

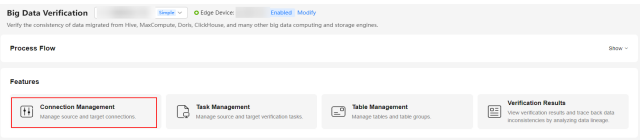
Step 17 On the **Table Management** page, click the **Tables** tab, select the data tables to be added to the same table group, and choose **Option** > **Add Tables to Group** above the list. In the displayed dialog box, select the desired table group and click **Confirm**.



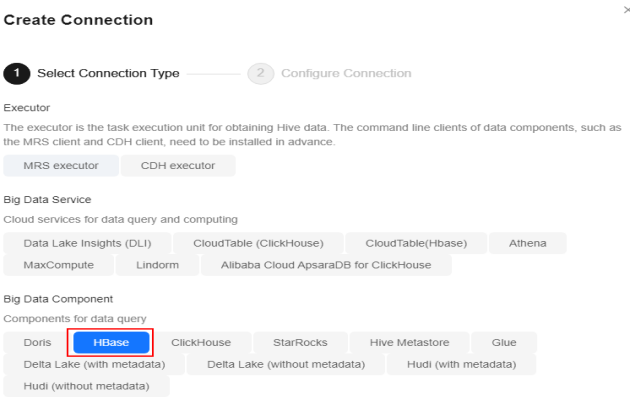
NOTICE

You can manually import information of incremental data tables to MgC. For details, see **Creating a Table Group and Adding Tables to the Group**.

Step 18 On the **Big Data Verification** page, in the **Features** area, click **Connection Management**.



Step 19 Click **Create Connection** in the upper right corner of the page. On the **Select Connection Type** page, select **HBase** and click **Next**.



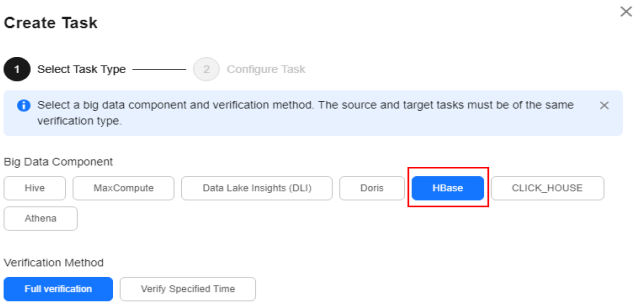
Step 20 Set connection parameters based on **Table 9-35** and click **Test**. If the test is successful, the connection is set up.

Table 9-35 Parameters for creating an HBase connection

Parameter	Configuration
Connection To	Select **Target**.
Connection Name	The default name is **HBase-***4 random characters* (including letters and numbers). You can also customize a name.
HBase Credential	Select the credential used for accessing the target MRS HBase cluster you added to Edge in **step 4**.
Secured Cluster	Choose whether the cluster is secured.
ZooKeeper IP Address	Enter the IP address for connecting to the ZooKeeper node. You can enter the public or private IP address of the ZooKeeper node.
ZooKeeper Port	Enter the port for connecting to the ZooKeeper node. The default value is **2181**.
HBase Version	Select the HBase version.

Step 21 On the MgC console, create a verification task for the source and target HBase clusters, respectively, and execute the tasks. For details, see **Creating and Executing Verification Tasks**. During the task creation, select the table group created in **step 16**.

- On the **Select Task Type** page, choose **HBase**.



- Select a verification method. For details about each verification method, see **Verification Methods**.

Step 22 Wait until the task executions enter a **Completed** status. You can view and export the task execution results on the **Verification Results** page. For details, see **Viewing and Exporting Verification Results**.

----End

9.10 Verifying the Consistency of Data Migrated from Delta Lake (with Metadata) to MRS Delta Lake

This section describes how to use MgC to verify the consistency of data migrated from self-built Delta Lake clusters to Huawei Cloud MRS Delta Lake clusters.

NOTICE

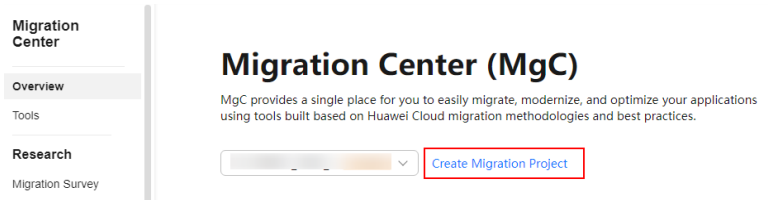
For Delta Lake clusters that have metadata storage, the metadata can be collected through data lake metadata collection tasks.

Preparations

Install Edge, an MgC tool used for data verification, in the source intranet environment and register an account for using Edge. For details, see **Installing Edge for Linux**.

Procedure

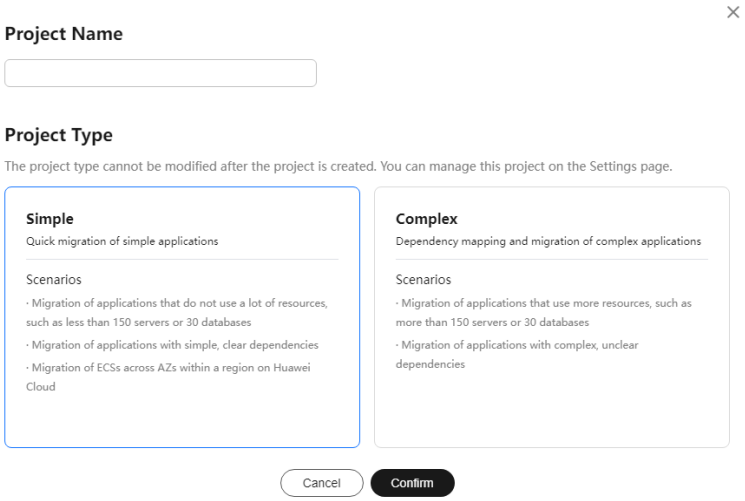
Step 1 Sign in to the **MgC** console. On the **Overview** page, click **Create Migration Project**.



Step 2 In the displayed dialog box, enter a project name, select a project type, and click **Confirm**.

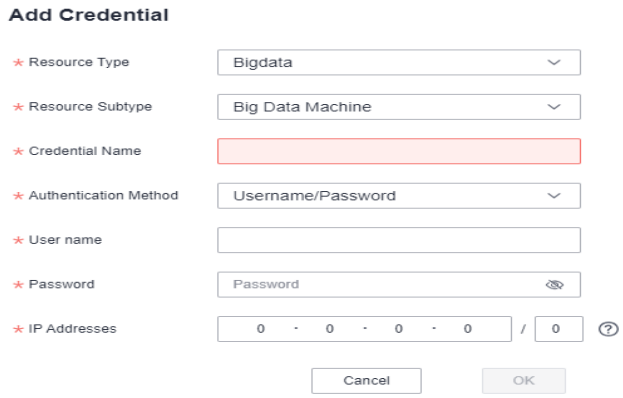
NOTICE

To review this migration project, choose **Settings** > **Migration Projects** in the navigation pane.

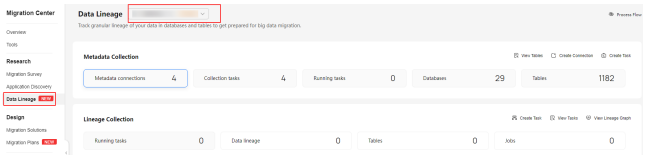


Step 3 Connect Edge to MgC. For more information, see **Connecting the Edge Device to MgC**.

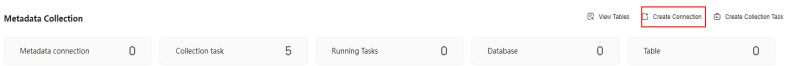
Step 4 After the connection is successful, add the username/password pairs for accessing the source Delta Lake executor and the target MRS Delta Lake executor to Edge. For more information, see **Adding Resource Credentials**.



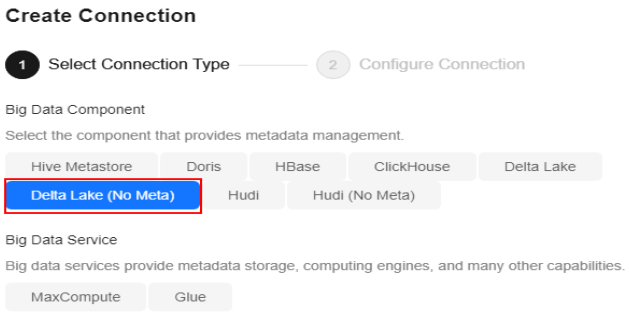
Step 5 On the MgC console, in the navigation pane on the left, choose **Research** > **Data Lineage**. In the upper left corner of the page, choose the migration project created in **step 2**.



Step 6 In the **Metadata Collection** area, click **Create Connection**.



Step 7 Select **Delta Lake (with metadata)** and click **Next**.

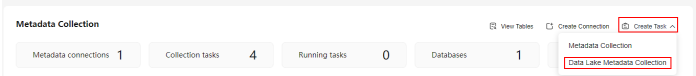


Step 8 Set connection parameters based on **Table 9-36** and click **Test**. If the test is successful, the connection is set up.

Table 9-36 Parameters for creating a connection to Delta Lake (with metadata)

Parameter	Configuration
Connection To	Select **Source**.
Connection Name	The default name is **Delta-Lake-with-metadata-***4 random characters* (including letters and numbers). You can also customize a name.
Edge Device	Select the Edge device connected to MgC in **step 3**.
Executor Credential	Select the source Delta Lake executor credential added to Edge in **step 4**.
Executor IP Address	Enter the IP address for connecting to the executor.
Executor Port	Enter the port for connecting to the executor. The default port is **22**.
Spark Client Directory	Enter the absolute path of the bin directory on the Spark client.
Environment Variable Address	Enter the absolute path of the environment variable file, for example, **/opt/bigdata/client/bigdata_env**. If this field is not left blank, the environment variable file is automatically sourced before commands are executed.
SQL File Location	Enter a directory for storing the SQL files generated for consistency verification. You must have the read and write permissions for the folder. **NOTICE** After the migration is complete, you need to manually clear the folders generated at this location to release storage space.

Step 9 In the **Metadata Collection** area, choose **Create Task** > **Data Lake Metadata Collection**.



Step 10 Set a data lake metadata collection task based on **Table 9-37** and click **Confirm**.

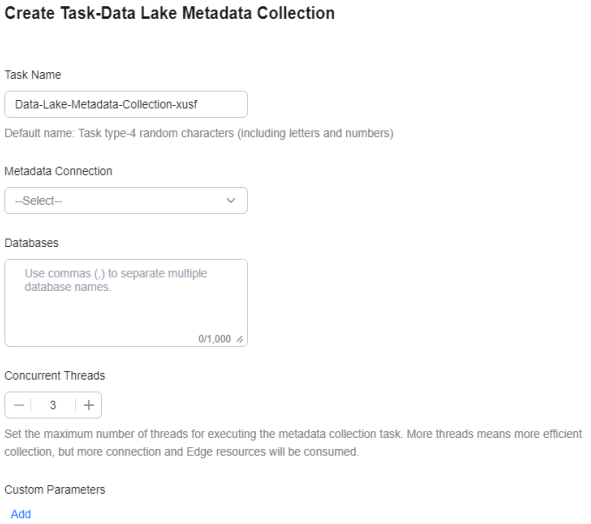
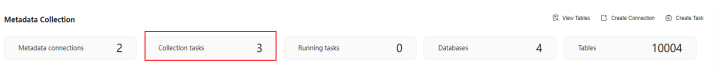


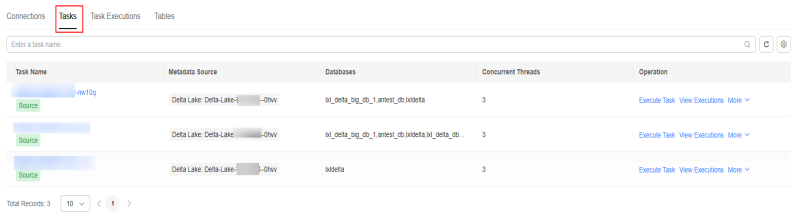
Table 9-37 Parameters for configuring a metadata collection task

Parameter	Configuration
Task Name	The default name is **Data-Lake-Metadata-Collection-Task-*4 random characters*** (including letters and numbers). You can also customize a name.
Metadata Source	Select the connection created in **step 8**.
Databases (Optional)	Enter the names of the databases whose metadata needs to be collected. If no database name is specified, the metadata of all databases is collected.
Concurrent Threads	Set the maximum number of threads for executing the collection. The default value is **3**. The value ranges from **1** to **10**. Configuring more concurrent threads means more efficient collection, but more connection and Edge device resources will be consumed.
Custom Parameters	You can customize parameters to specify the tables and partitions to collect or set criteria to filter tables and partitions. • If you want to collect metadata from Alibaba Cloud EMR, add the following parameter: – Parameter: **conf** – **Value**: **spark.sql.catalogImplementation=hive** • If the source is Alibaba Cloud EMR Delta Lake 2.2 and is accessed through Delta Lake 2.3, add the following parameters: – Parameter: **master** – **Value**: **local**

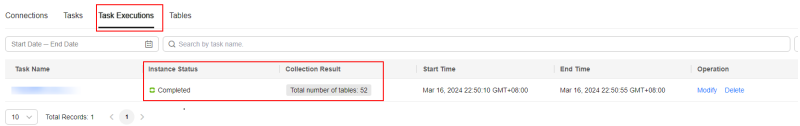
Step 11 In the **Metadata Collection** area, click **Collection tasks**.



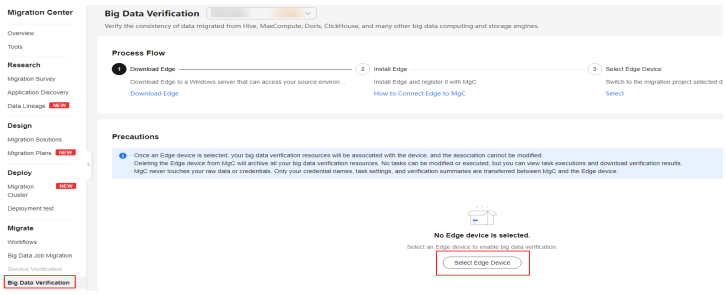
Step 12 Under **Tasks**, you can review the created metadata collection task and its settings. Click **Execute Task** in the **Operation** column to run the task. Each time the task is executed, a task execution is generated.



Step 13 Click **View Executions** in the **Operation** column. Under **Task Executions**, you can view the execution records of the task and the status and collection results of each task execution. When a task execution enters a **Completed** status and the collection results are displayed, you can view the list of databases and tables extracted from collected metadata on the **Tables** tab.



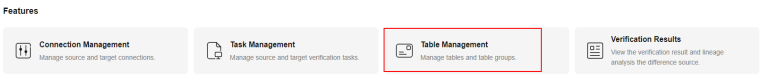
Step 14 In the navigation pane on the left, choose **Migrate** > **Big Data Verification**. If this is your first time to visit this page, select an Edge device to enable the verification feature. Click **Select Edge Device**. In the displayed dialog box, select the Edge device connected to MgC in **step 3**.



CAUTION

Ensure that the selected Edge device is always **Online** and **Enabled** before your verification is complete.

Step 15 In the **Features** area, click **Table Management**.



Step 16 Under **Table Groups**, click **Create**. Configure the **parameters for creating a table group** and click **Confirm**.

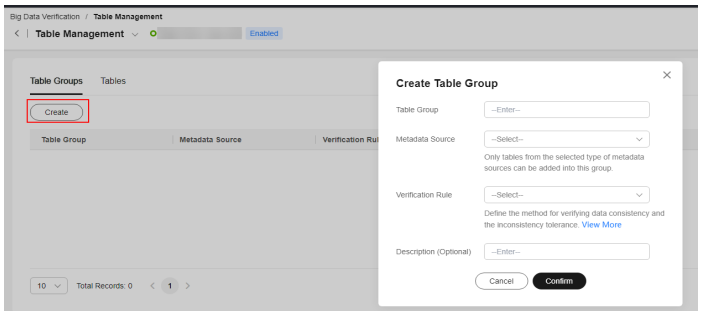
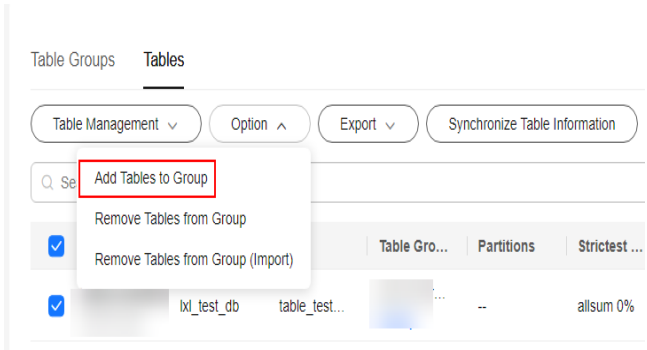


Table 9-38 Parameters for creating a table group

Parameter	Description
Table Group	Enter a name.
Metadata Source	Select the connection created in **step 8**. **CAUTION** A table group can only contain tables coming from the same metadata source.
Verification Rule	Select a rule that defines the method for verifying data consistency and the inconsistency tolerance. MgC provides multiple verification rules for you to choose. For details about these rules, click **View More**.
Description (Optional)	Enter a description to identify the table group.

Step 17 On the **Table Management** page, click the **Tables** tab, select the data tables to be added to the same table group, and choose **Option** > **Add Tables to Group** above the list. In the displayed dialog box, select the desired table group and click **Confirm**.



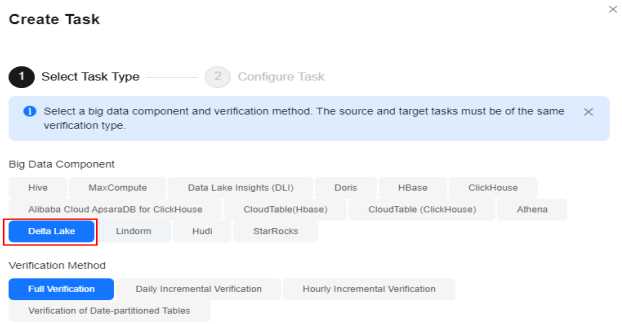
NOTICE

You can manually import information of incremental data tables to MgC. For details, see **Creating a Table Group and Adding Tables to the Group**.

Step 18 Create a connection to the source and target executors separately. For details, see **Creating an Executor Connection**. Select the source and target executor credentials added to Edge in **step 4**.

Step 19 Create a data verification task for the source and target Delta Lake clusters, respectively, and execute the tasks. For more information, see **Creating and Executing Verification Tasks**. During the task creation, select the table group created in **step 16**.

- On the **Select Task Type** page, choose **Delta Lake**.



- Select a verification method. For details about each verification method, see **Verification Methods**.

Step 20 Wait until the task executions enter a **Completed** status. You can view and export the task execution results on the **Verification Results** page. For details, see **Viewing and Exporting Verification Results**.

----End

9.11 Verifying the Consistency of Data Migrated from Delta Lake (without Metadata) to MRS Delta Lake

This section describes how to use MgC to verify the consistency of data migrated from self-built Delta Lake clusters to Huawei Cloud MRS Delta Lake clusters.

NOTICE

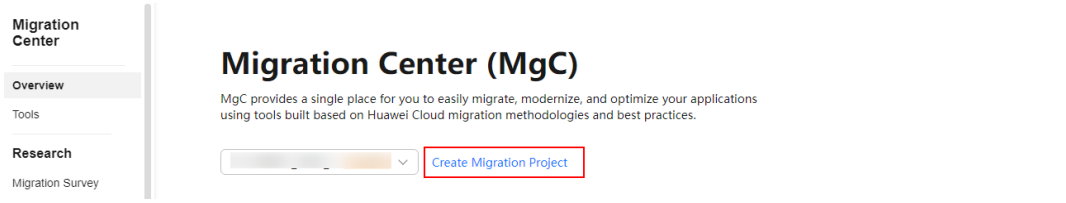
For Delta Lake clusters without metadata storage, you need to import the metadata to MgC.

Preparations

Install Edge, an MgC tool used for data verification, in the source intranet environment and register an account for using Edge. For details, see **Installing Edge for Linux**.

Procedure

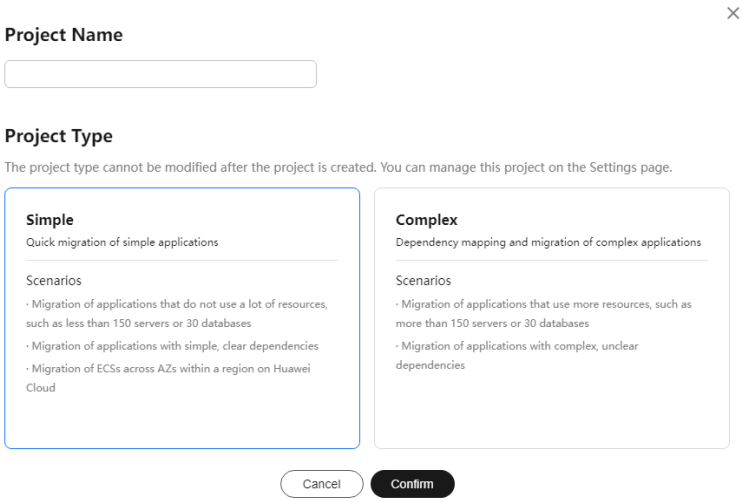
Step 1 Sign in to the **MgC** console. On the **Overview** page, click **Create Migration Project**.



Step 2 In the displayed dialog box, enter a project name, select a project type, and click **Confirm**.

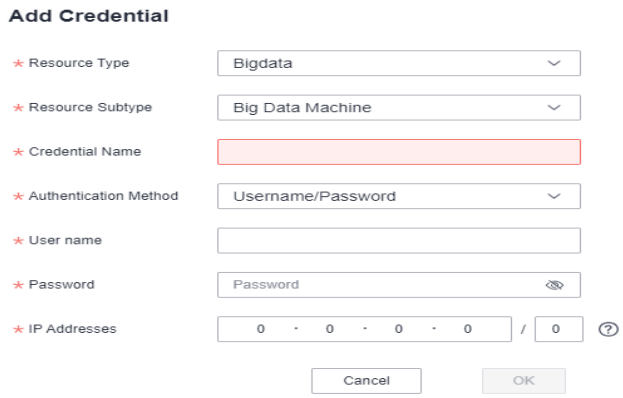
NOTICE

To review this migration project, choose **Settings** > **Migration Projects** in the navigation pane.

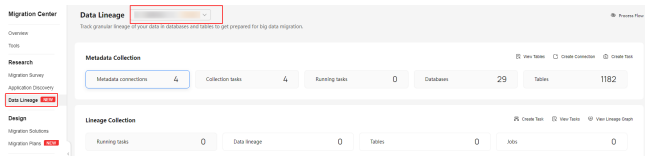


Step 3 Connect Edge to MgC. For more information, see **Connecting the Edge Device to MgC**.

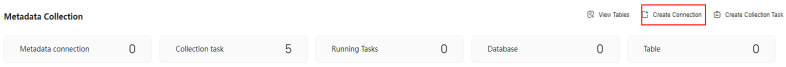
Step 4 After the connection is successful, add the username/password pairs for accessing the source Delta Lake executor and the target MRS Delta Lake executor to Edge. For more information, see **Adding Resource Credentials**.



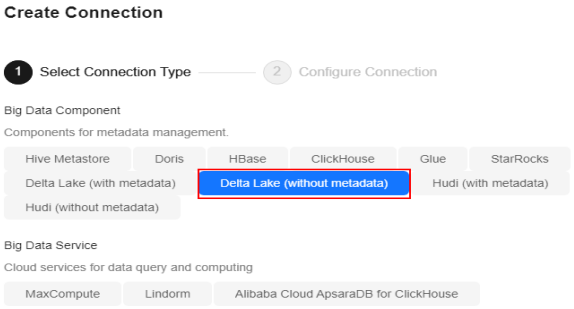
Step 5 On the MgC console, in the navigation pane on the left, choose **Research** > **Data Lineage**. In the upper left corner of the page, choose the migration project created in **step 2**.



Step 6 In the **Metadata Collection** area, click **Create Connection**.



Step 7 Select **Delta Lake (without metadata)** and click **Next**.



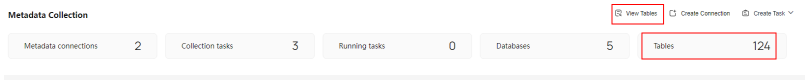
Step 8 Set connection parameters based on **Table 9-39** and click **Test**. If the test is successful, the connection is set up.

Table 9-39 Parameters for creating a connection to Delta Lake (without metadata)

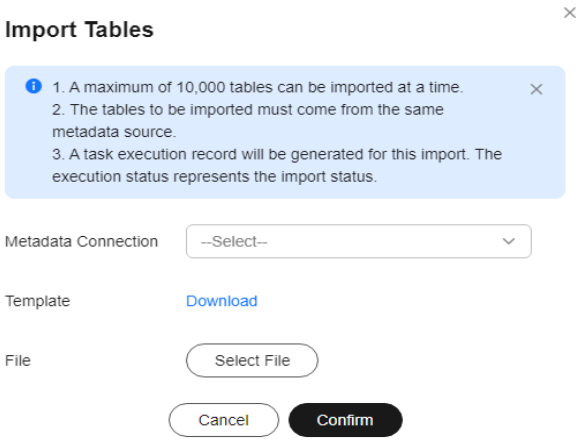
Parameter	Configuration
Connection To	Select **Source**.
Connection Name	The default name is **Delta-Lake-without-metadata-***4 random characters* (including letters and numbers). You can also customize a name.
Edge Device	Select the Edge device connected to MgC in **step 3**.
Executor Credential	Select the source Delta Lake executor credential added to Edge in **step 4**.
Executor IP Address	Enter the IP address for connecting to the executor.
Executor Port	Enter the port for connecting to the executor. The default port is **22**.
Spark Client Directory	Enter the absolute path of the bin directory on the Spark client.
Environment Variable Address	Enter the absolute path of the environment variable file, for example, **/opt/bigdata/client/bigdata_env**. If this field is not left blank, the environment variable file is automatically sourced before commands are executed.

Parameter	Configuration
SQL File Location	Enter a directory for storing the SQL files generated for consistency verification. You must have the read and write permissions for the folder. **NOTICE** After the migration is complete, you need to manually clear the folders generated at this location to release storage space.

Step 9 In the **Metadata Collection** area, click **View Tables** or **Tables**.

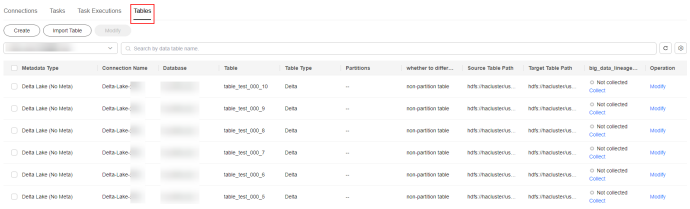


Step 10 On the displayed page, click **Import**.

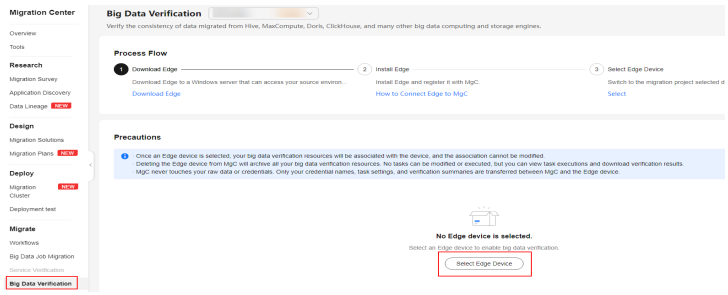


Step 11 Click **Download** to download the import template to the local PC. Open the template, fill in table information, and save the template.

Step 12 In the **Import Tables** dialog box, click **Select File**, choose the filled template file, and click **Confirm**. After the import is complete, you can view the imported tables on **Tables** tab.



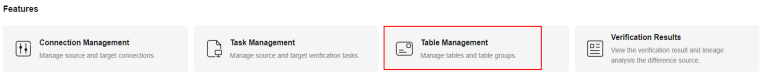
Step 13 In the navigation pane on the left, choose **Migrate** > **Big Data Verification**. If this is your first time to visit this page, select an Edge device to enable the verification feature. Click **Select Edge Device**. In the displayed dialog box, select the Edge device connected to MgC in **step 3**.



CAUTION

Ensure that the selected Edge device is always **Online** and **Enabled** before your verification is complete.

Step 14 In the **Features** area, click **Table Management**.



Step 15 Under **Table Groups**, click **Create**. Configure the **parameters for creating a table group** and click **Confirm**.

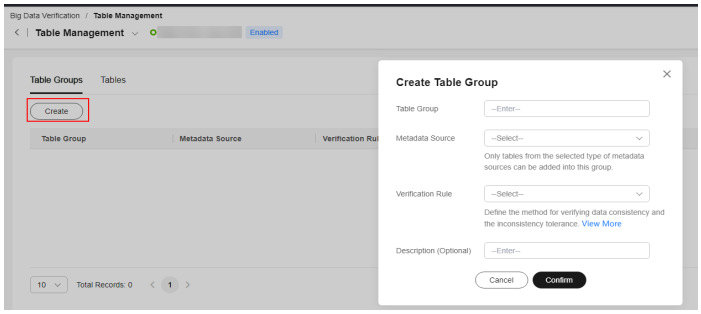
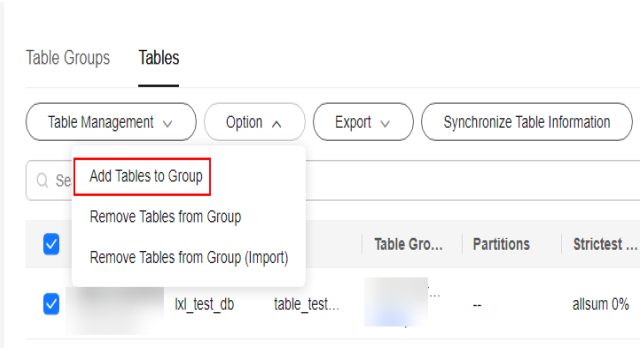


Table 9-40 Parameters for creating a table group

Parameter	Description
Table Group	Enter a name.
Metadata Source	Select the connection created in **step 8**. **CAUTION** A table group can only contain tables coming from the same metadata source.
Verification Rule	Select a rule that defines the method for verifying data consistency and the inconsistency tolerance. MgC provides multiple verification rules for you to choose. For details about these rules, click **View More**.
Description (Optional)	Enter a description to identify the table group.

Step 16 On the **Table Management** page, click the **Tables** tab, select the data tables to be added to the same table group, and choose **Option** > **Add Tables to Group** above the list. In the displayed dialog box, select the desired table group and click **Confirm**.



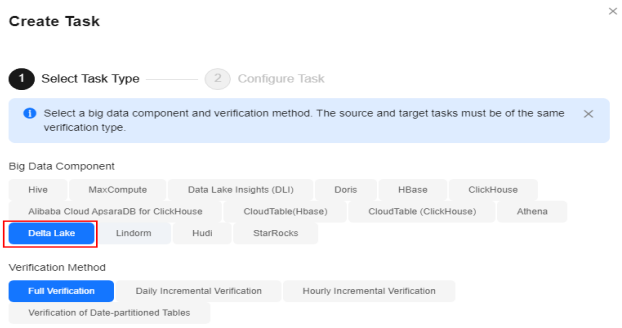
NOTICE

You can manually import information of incremental data tables to MgC. For details, see **Creating a Table Group and Adding Tables to the Group**.

Step 17 Create a connection to the source and target executors separately. For details, see **Creating an Executor Connection**. Select the source and target executor credentials added to Edge in **step 4**.

Step 18 Create a data verification task for the source and target Delta Lake clusters, respectively, and execute the tasks. For more information, see **Creating and Executing Verification Tasks**. During the task creation, select the table group created in **step 16**.

- On the **Select Task Type** page, choose **Delta Lake**.



- Select a verification method. For details about each verification method, see **Verification Methods**.

Step 19 Wait until the task executions enter a **Completed** status. You can view and export the task execution results on the **Verification Results** page. For details, see **Viewing and Exporting Verification Results**.

----End

10 Migrating Big Data Without Using the Internet

This section describes how to use NAT gateways and VPNs to migrate and synchronize big data when Edge has no Internet access. The following assumes that Alibaba Cloud is the source and Edge is installed on the Alibaba Cloud ECS.

Step 1: Configure a Huawei Cloud VPN

Step 1 Log in to the Huawei Cloud console and, in the service list, choose **Networking** > **Virtual Private Network**.

Step 2 Configure a VPN gateway

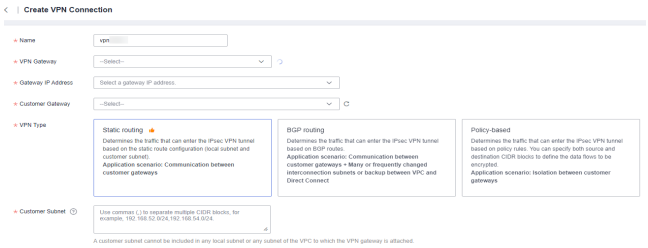
1. In the navigation pane, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
2. Click **Buy S2C VPN Gateway** and set parameters by following the on-screen instructions.
3. Configure all required parameters and click **Buy Now**.

Step 3 Configure customer gateways. You need to create an active and a standby customer gateway.

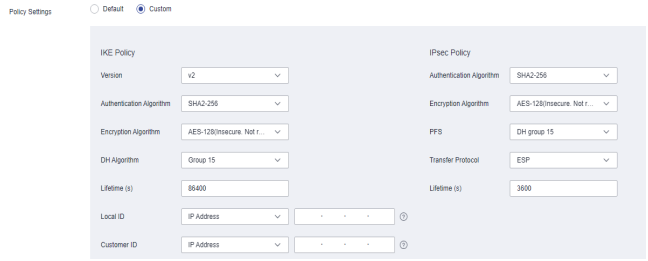
1. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.
2. Click **Create Customer Gateway** and set parameters by following the on-screen instructions. Select **IP Address** for **Identifier** and enter the public IP address of the Alibaba Cloud gateway.
3. Click **Create Now**.

Step 4 Create VPN connections. Create two VPN connections to connect to the Huawei Cloud VPN gateway and Alibaba Cloud customer gateway, respectively.

1. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
2. Click **Create VPN Connection**. On the displayed page, select the created VPN gateway and a customer gateway, and enter the subnet address of the customer gateway. Ensure that the subnet addresses do not overlap.



Select **Custom** for **Policy Settings** and ensure that the settings are the same as those on Alibaba Cloud.



3. Configure all required parameters and click **Buy Now**.

----End

Step 2: Configure an Alibaba Cloud VPN

Step 1 Sign in to the Alibaba Cloud console and choose **Products and Services** > **Networking and CDN** > **Hybrid Cloud Network** > **VPN Gateway**.

Step 2 Configure a VPN gateway

1. Click **Create VPN Gateway** and set parameters by following the on-screen instructions.
2. Configure all required parameters and click **Buy Now**.

Step 3 Configure the customer gateway.

1. In the navigation pane, choose **VPN** > **Customer Gateways**.
2. Click **Create Customer Gateway** and set parameters by following the on-screen instructions.
3. Click **OK**.

Step 4 Create a VPN connection.

1. In the navigation pane, choose **VPN** > **IPsec Connections**.
2. Click **Create IPsec Connection**, select the VPN gateway configured in step 2, and keep the policy settings the same as those on Huawei Cloud.
3. Click **OK**.

Step 5 Configure a route to the Huawei Cloud VPC subnet.

1. In the navigation pane, choose **VPN** > **VPN Gateways**.
2. Click the VPN gateway name. On the **Destination-based Route Table** tab, click **Add Route Entry** and set parameters based on the instructions.

----End

Step 3: Configure an Alibaba Cloud NAT Gateway

Create an Alibaba Cloud NAT gateway and configure SNAT and DNAT entries. For details, see **Creating and Managing an Internet Public NAT Gateway**.

Step 1 Sign in to the Alibaba Cloud console and choose **Products and Services** > **Networking and CDN** > **Hybrid Cloud Network** > **VPN Gateway**.

Step 2 Create an Internet NAT gateway.

1. On the **Internet NAT Gateway** page, click **Create Internet NAT Gateway** and configure parameters based on the instructions.
2. Configure all required parameters and click **Buy Now**.

Step 3 Configure an SNAT entry.

1. On the **Internet NAT Gateway** page, locate the Internet NAT gateway created in step 2 and click **Configure SNAT** in the **Actions** column.
2. On the **SNAT Management** tab, click **Create SNAT Entry** and set parameters based on the instructions.
3. Click **OK**.

Step 4 Configure a DNAT entry.

1. On the **Internet NAT Gateway** page, locate the Internet NAT gateway created in step 2 and click **Configure DNAT** in the **Actions** column.
2. On the **DNAT Management** tab, click **Create DNAT Entry** and set parameters based on the instructions.
3. Click **OK**.

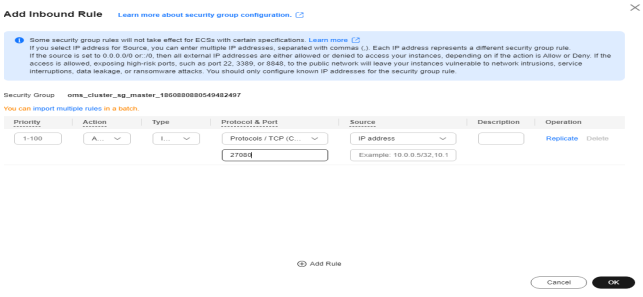
----End

Step 4: Configure Security Groups

You need to configure security groups on Huawei Cloud and Alibaba Cloud.

Step 1 On the Huawei Cloud console, configure the involved security group to allow access from the private IP address of the server where Edge is installed.

1. Sign in to the Huawei Cloud console.
2. In the **Service List**, choose **Networking** > **Virtual Private Cloud**.
3. In the navigation pane, choose **Access Control** > **Security Groups**.
4. In the security group list, locate the security group where the target big data cluster is managed and click **Manage Rules** in the **Operation** column.
5. On the **Inbound Rules** tab, click **Add Rule**.
6. In the displayed dialog box, add a rule that allows TCP traffic to port 27080. Enter the private IP address of the server where Edge is installed in the **Source** text box.



7. Click **OK**.

Step 2 On the Alibaba Cloud console, configure the involved security group to allow access from the private IP address of the server where Edge is installed.

1. Sign in to the Alibaba Cloud ECS console.
2. In the navigation pane, choose **Network & Security** > **Security Groups**.
3. Locate the security group that the server with Edge installed belongs to and click **Manage Rules** in the **Operation** column.
4. On the **Inbound** tab, click **Quick Add**. Set **Action** to **Allow**, **Authorization Object** to the public IP address of the server where Edge is installed, and **Port Range** to **All**.
5. Click **OK**.

----End

Step 5: Set Up a Migration Environment

Set up a migration environment by referring to **Preparations**. Purchase an ECS on Alibaba Cloud. Configure an SNAT rule for the NAT gateway to allow the ECS to access the Internet using its private IP address. Install Edge on the ECS, register an account, and **connect Edge to MgC**.

Step 6: Create a Big Data Migration Task

Review and understand the **notes** about big data verification tasks. Perform the following steps to create a big data migration task:

Step 1 **Create a connection to MaxCompute**.

Step 2 **Create a connection to DLI**.

Step 3 **Create a metadata migration task** or **Create a data migration task** and execute it.

----End

