Migration Center User Guide

Getting Started

Issue 01

Date 2025-08-15

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

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

Contents

1 Overview

This section describes how to get started with MgC. Included are steps to introduce you to the process of using the server migration workflow of MgC.

MgC also supports cross-AZ ECS migration and storage migration. For details, see **Migrating Servers Across AZs on Huawei Cloud**.

Procedure

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 project	Create a project to group and manage your migration resources.
Download and install the MgC Agent	Install the MgC Agent, which is a tool that collects information about your source resources and executes migration commands from MgC.
Discover source servers.	Discover source servers and collect their details through the Internet, an intranet, or manual addition.
(Optional) Group discovered servers as applications	Group the discovered servers as applications. With these applications, you can assess the discovered source servers to get target resource recommendations and create migration workflows to migrate these servers.

Step	Description
Generate target recommendations	Assess the discovered source servers, grouped as applications, to generate recommendations for appropriately sized Huawei Cloud resources. These recommendations are generated based on the specifications, performance, and business purpose of the source servers, while also considering your requirements for cost, availability, and compliance.
Create server migration workflows	Create migration workflows to migrate the source servers in batches.

2 Preparations

Before using MgC, you need to sign up for a HUAWEI ID or create an IAM user. This section describes how to sign up for a HUAWEI ID, enable Huawei Cloud services, complete real-name authentication, and create an IAM user.

Signing up for a HUAWEI ID, Enabling Huawei Cloud Services, and Completing Real-Name Authentication

If you already have a HUAWEI ID, skip this part.

1. Visit **Huawei Cloud** and click **Sign Up**.
2. **Sign up for a HUAWEI ID and enable Huawei Cloud services**.
3. Complete real-name authentication.
   - If your account is an individual account, see **Individual Real-Name Authentication**.
   - If your account is an enterprise account, see **Enterprise Real-Name Authentication**.

Creating an IAM User

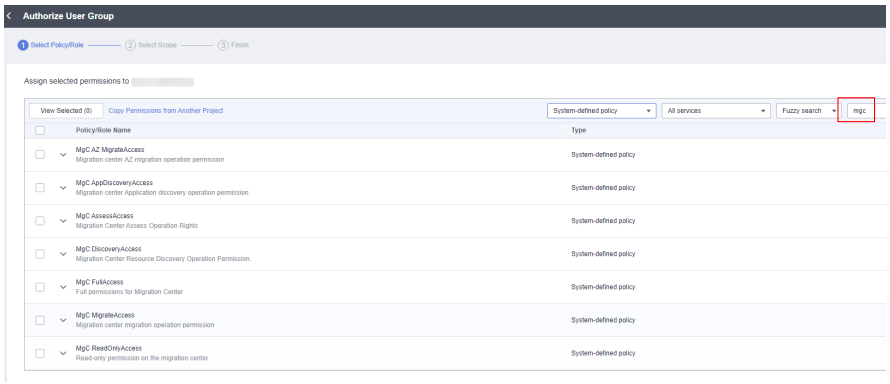
You can use your account to create IAM users to ensure the security of accounts and resources. For more information about IAM users, see **Creating an IAM User**. This section describes how to create an IAM user with permissions to access MgC. If you do not need to use any IAM users, skip this part.

1. Visit **Huawei Cloud**. Click **Console** in the upper right corner. Sign in to the console using the HUAWEI ID you signed up for.
2. Click the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list.
3. **Create a user group and assign permissions** to it.

   Create a user group. In the user group list, locate the user group you created and click **Authorize** in the **Operation** column. On the **Authorize User Group** page, search for **MgC** in the search box. Select the permissions to be assigned to the user group. For details about MgC permissions, see **Permissions Management**.

NOTE

A maximum of 20 user groups can be created.



4. **Create an IAM user and add it to the user group**.

   Create a user and add it to the user group authorized with MgC permissions in **Step 3**.

Obtaining Access Keys (AK/SK)

Access keys are identity credentials used to call APIs. The account administrator and IAM users can only use their own access keys to call APIs. For details about how to obtain an access key, see **Access Keys**.

3 Creating a Project

Using projects, you can easily group and manage migration resources for different initiatives. Two types of projects are available for different migration cases.

- **Application migration**: This type of projects applies to discovery and migration of server and storage resources.
- **Complex migration (for big data)**: This type of projects applies to big data migration and consistency verification.

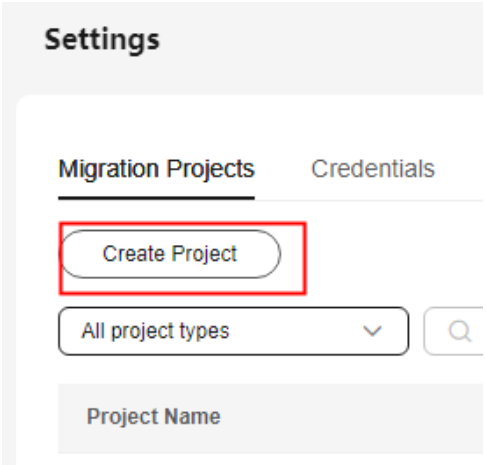
Procedure

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

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

Step 3 Under **Migration Projects**, click **Create Project**.

Figure 3-1 Creating a project

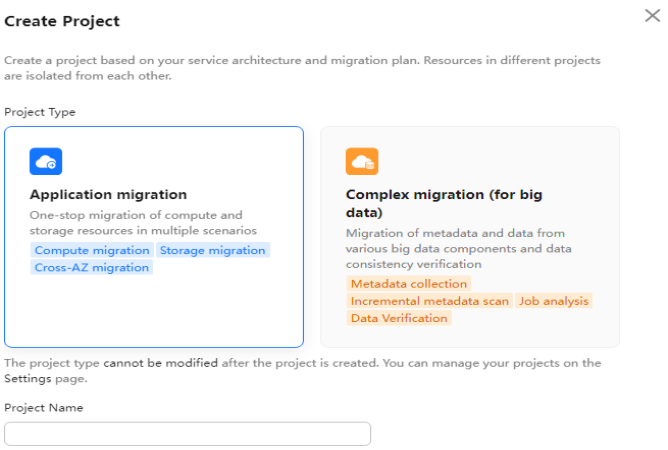


Step 4 In the dialog box that is displayed, view the application scenarios of each project type, and select a project type as required.

NOTICE

The project type cannot be changed after the project is created.

Figure 3-2 Selecting a project type



Step 5 Enter a project name and click **Create**. After the project is created, you can view it in the project list.

----End

4 Installing the MgC Agent

4.1 Installing the MgC Agent on Windows

Preparations

- Prepare a Windows server for installing the MgC Agent 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 port 8883 if the server is in a security group.
  - Not have any antivirus or protection software enabled. This type of software may stop the MgC Agent from executing migration commands, resulting in migration failures.

  CAUTION

  Do not install the MgC Agent on a source server to be migrated.

  - **High resource consumption**: The MgC Agent consumes CPU and memory resources during collection and migration. If a large number of migration tasks are performed by the MgC Agent, services on the source server may be affected.
  - **Port occupation**: The MgC Agent occupies some ports on the server, which may affect services running on it.

- **Sign up for a HUAWEI ID and enable Huawei Cloud services**, and obtain an AK/SK pair for the account.
- **Create a migration project** on the MgC console.

Precautions

- The Windows server where the MgC Agent is installed must be able to access the 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 the MgC Agent is installed. For more information, see **How Do I Configure WinRM and Troubleshoot WinRM Connection Problems?**
- You are advised to change your MgC Agent password every three to six months.

Procedure

Step 1 Sign in to the **MgC console** from the Windows server you prepared.

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

Step 3 In the **Windows** area, click **Download Installation Package** to download the MgC Agent installation package to the Windows server you prepared.

Step 4 Decompress the downloaded the MgC Agent installation package, double-click the installation program, and click **Next**. If the installation program cannot be launched, try to run it in compatibility mode. For details, see **How Do I Run the MgC Agent in Compatibility Mode?**

Step 5 On the **License Agreement** page, read the agreement carefully, select **I accept the terms of the License Agreement**, and click **Next**.

Step 6 Select drive C as the installation directory and click **Install**.

> **CAUTION**
>
> The MgC Agent can only be installed in drive C. If you select another disk for installation, the MgC Agent may fail to start.

Step 7 After the installation is complete, click **Finish**. Open the MgC Agent console, enter the AK/SK pair of your Huawei Cloud account, select a region, and click **Log In**.

----End

5 Discovering Servers

5.1 Online Discovery

This section describes how to discover servers running on clouds, such as Alibaba Cloud, Huawei Cloud, AWS, Tencent Cloud, Azure, Qiniu Cloud, and Kingsoft Cloud.

> **CAUTION**
>
> After the servers are discovered over the Internet, you need to ensure all the servers pass the pre-migration check or perform a deep collection for them, so that you can create a migration workflow to migrate them.

Prerequisites

- You have **installed the MgC Agent** in the source intranet environment and have connected it to MgC.
- You have **added source server credentials** to the MgC Agent. The server credentials must meet the following requirements:
  - Linux: **root** and its password
  - Windows: **administrator** and its password

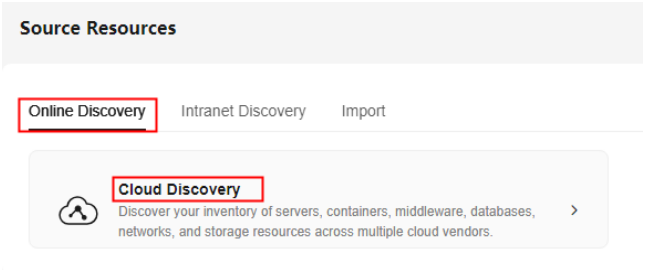
Procedure

Step 1 Sign in to the **MgC console**. In the navigation pane, under **Project**, select your **application migration project** from the drop-down list.

Step 2 In the navigation pane, choose **Discover** > **Source Resources**.

Step 3 Under **Online Discovery**, click **Cloud Discovery**.

Figure 5-1 Cloud discovery



Step 4 Configure the parameters listed in **Table 5-1** to create a discovery task.

Table 5-1 Parameters for creating a cloud discovery task

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. Currently, Alibaba Cloud, Huawei Cloud, AWS, Tencent Cloud, Azure, Qiniu Cloud, and Kingsoft Cloud are supported.	Yes
	Credential	Select the credential for accessing the source cloud platform. If no credential is available, choose **Create** to add one. For details, see **Managing Credentials**. • If the source cloud platform is Alibaba Cloud, Huawei Cloud, AWS, Tencent Cloud, Qiniu Cloud, or Kingsoft Cloud, select **AK/SK** for **Authentication** and enter the AK/SK pair of your source cloud account. • If the source cloud platform is Azure, Select **ID/Secret** for **Authentication**. To learn how to obtain Azure credentials, see **How Do I Obtain Azure Credentials?**	Yes
	Region	Select the region where your source environment is located. Multiple regions can be selected.	Yes

Area	Parameter	Description	Mandatory
	Resource Type	Select **Servers** from the drop-down list.	Yes
	Application	Select the application that you want to group the discovered servers into. If no applications are available, perform the following steps to create one: 1. Click **Create Application**, enter an application name and description, select a business scenario and running environment, and select the region where the application resources will be deployed on the target cloud. 2. Click **OK**.	No

Step 5 Click **Confirm**. The Internet-based discovery task is created, and MgC starts collecting details about source servers.

Step 6 Wait until the task status changes to **Succeeded**. Then perform the following steps to check the migration readiness for the discovered source servers.

1. **Install the MgC Agent** in the source intranet environment and connect the MgC Agent to MgC.
2. Go to the **Source Resources** page, in the server list, select the servers to be migrated and click **Group as Application** above the list. If you have specified an application in the Internet-based discovery task for discovering these source servers, skip this step.
   - If you have created an application, select the application from the drop-down list and click **OK**.
   - If you have not created an application, click **Create Application** in the displayed dialog box. Then enter an application name and description, select a business scenario, environment, and target region, and click **Create**. Then click **OK**.
3. On the top of the server list, choose **Migration Scenario** > **Server migration**.
4. For each source server, click **Configure** in the **Migration Readiness** column.
5. Configure the parameters listed in **Table 5-2**.

Table 5-2 Parameters for configuring migration readiness

Parameter	Configuration
Type	Set this parameter based on the source server OS type.

Parameter	Configuration
MgC Agent	Select the MgC Agent installed in the source environment.
Access 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.
Port	Enter the port on the source server that allows access from the MgC Agent. – By default, port 5985 on Windows source servers must be opened to the MgC Agent. The port cannot be changed. – By default, port 22 on Linux source servers must be opened to the MgC Agent. You can specify a different port if needed.
Credential	Select the server credential. If the credential is not displayed in the list, go to the MgC Agent console, **add the server credential**, and synchronize it to MgC. **NOTICE** The account provided in the credential must have sufficient permissions, so the MgC Agent can collect necessary server details. To perform a deep collection for the server to collect as much as details, the credential you provided must meet the following requirements: – Linux: **root** and its password – Windows: **administrator** and its password

6. Click **Confirm**. The system checks whether the source server can be accessed using the information you provided and whether the server can be migrated. If **Ready** shows up in the **Migration Readiness** column, the source server can be migrated. Then you can **design a migration solution** or **design a migration plan** to migrate the server.

----End

5.2 Intranet Discovery

MgC enables you to discover resources running in on-premises IDCs and vCenters. Before getting started, you need to install the MgC Agent in the source intranet. Then you can discover servers by network range or VMware host.

Precautions

- Only VMs in VMware vSphere 5.0 to 7.0 can be discovered.
- When the system scans for VMware VMs or scans for servers on specific network ranges, it uses the servers' private IP addresses and the ID of the used MgC Agent to identify discovered servers. If a server's private IP address changes after a collection is complete, the server will be identified as a new

one during the next collection, and the total number of discovered servers will increase. To avoid this, do not change private IP addresses for source servers before the migration is complete.

Prerequisites

- You have **installed the MgC Agent** in the source intranet environment and **have connected it to MgC**.
- You have **added source server credentials** to the MgC Agent.

NOTICE

The account provided in the credential must have sufficient permissions, so the MgC Agent can collect necessary server details. To perform a deep collection for the server to collect as much as details, the credential you provided must meet the following requirements:

- Linux: **root** and its password
- Windows: **administrator** and its password

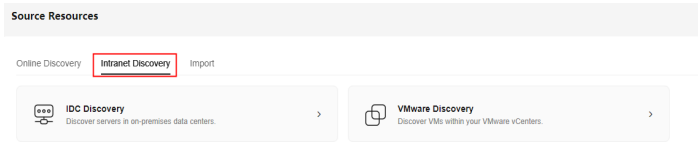
Creating an IDC Discovery Task

Step 1 Sign in to the **MgC console**. In the navigation pane, under **Project**, select your **application migration project** from the drop-down list.

Step 2 In the navigation pane, choose **Discover** > **Source Resources**.

Step 3 Click the **Intranet Discovery** tab and select the environment where your source servers run.

Figure 5-2 Selecting the source environment



Step 4 To configure an IDC discovery task, set the parameters by referring to **Table 5-3**.

Table 5-3 Parameters for configuring an IDC discovery task

Parameter	Description
Task Name	Enter a task name.
Task Description	Describe the task.
MgC Agent	Select the **MgC Agent** installed in the source intranet environment.
Protocol	Only TCP is available.

Parameter	Description
Network Range	Enter an IP address range which must fall within: • 10.0.0.0 – 10.255.255.255 • 172.16.0.0 – 172.31.255.255 • 192.168.0.0 – 192.168.255.255
Linux	Enter the port for scanning for Linux servers. If you do not need to scan for Linux servers, set the port number to **0**.
Windows	Enter the port for scanning for Windows servers. If you do not need to scan for Windows servers, set the port number to **0**.
Application	Select the application that you want to group the discovered servers into. If no applications are available, perform the following steps to create one: 1. Click **Create Application**, enter an application name and description, select a business scenario and running environment, and select the region where the application resources will be deployed on the target cloud. 2. Click **OK**.

Step 5 Click **Confirm**. After the IDC discovery task is created, MgC starts discovering source resources.

Step 6 Wait until the discovery task succeeds, return to the **Source Resources** page and perform a deep collection for the discovered servers.

1. On the **Source Resources** page, in the server list, for each server whose details need to be collected, click **Configure** in the **MgC Agent** column.
2. Configure the parameters listed in **Table 5-4**.

Table 5-4 Parameters for configuring a deep collection

Parameter	Configuration
Type	Set this parameter based on the source server OS type.
MgC Agent	Select the MgC Agent installed in the source environment.
Access 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.

Parameter	Configuration
Port	Enter the port on the source server that allows access from the MgC Agent. – By default, port 5985 on Windows source servers must be opened to the MgC Agent. The port cannot be changed. – By default, port 22 on Linux source servers must be opened to the MgC Agent. You can specify a different port if needed.
Credential	Select the server credential. If the credential is not displayed in the list, go to the MgC Agent console, **add the server credential**, and synchronize it to MgC.

3. Click **Confirm**. Then the system automatically starts executing a deep collection. When **Collected** shows up in the **Deep Collection** column, the collection is complete. You can proceed to **create a migration solution** or **create a migration plan**.

----End

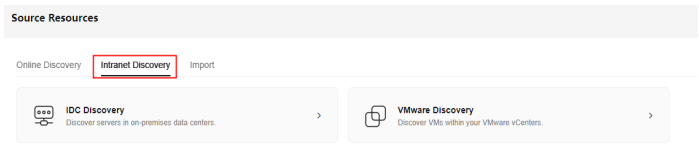
Creating a VMware Discovery Task

Step 1 Sign in to the **MgC console**. In the navigation pane, under **Project**, select your from the drop-down list.

Step 2 In the navigation pane, choose **Discover** > **Source Resources**.

Step 3 Click the **Intranet Discovery** tab and select the environment where your source servers run.

Figure 5-3 Selecting the source environment



Step 4 To configure a VMware discovery task, set the parameters by referring to **Table 5-5**.

Table 5-5 Parameters for configuring a VMware discovery task

Parameter	Description
Task Name	Enter a task name.
Task Description	Describe the task.
MgC Agent	Select the **MgC Agent** installed in the source intranet environment.

Parameter	Description
IP Address	Enter the IP address of the vCenter Server for discovering the managed VMs.
Port	Enter the port for accessing the vCenter Server.
Credential	Select the credential for accessing the vCenter Server. If the drop-down list is empty, go to the MgC Agent console and **add the credential**. When adding the credential, set the resource type to **Private cloud** and enter the username and password for logging in to the vCenter Server.
Application	Select the application that you want to group the discovered servers into. If no applications are available, perform the following steps to create one: 1. Click **Create Application**, enter an application name and description, select a business scenario and running environment, and select the region where the application resources will be deployed on the target cloud. 2. Click **OK**.

Step 5 Click **Confirm**. After the VMware discovery task is created, MgC starts discovering source resources.

Step 6 Wait until the discovery task succeeds, return to the **Source Resources** page and perform a deep collection for the discovered servers.

1. On the **Source Resources** page, in the server list, for each server whose details need to be collected, click **Configure** in the **MgC Agent** column.
2. Configure the parameters listed in **Table 5-6**.

Table 5-6 Parameters for configuring a deep collection

Parameter	Configuration
Type	Set this parameter based on the source server OS type.
MgC Agent	Select the MgC Agent installed in the source environment.
Access 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.

Parameter	Configuration
Port	Enter the port on the source server that allows access from the MgC Agent. – By default, port 5985 on Windows source servers must be opened to the MgC Agent. The port cannot be changed. – By default, port 22 on Linux source servers must be opened to the MgC Agent. You can specify a different port if needed.
Credential	Select the server credential. If the credential is not displayed in the list, go to the MgC Agent console, **add the server credential**, and synchronize it to MgC.

3. Click **Confirm**. Then the system automatically starts executing a deep collection. When **Collected** shows up in the **Deep Collection** column, the collection is complete. You can proceed to **create a migration solution** or **create a migration plan**.

----End

5.3 Manual Addition

This method is for discovering on-premises servers and cloud servers that cannot be discovered over the Internet or an intranet.

Prerequisites

- You have **installed the MgC Agent** in the source intranet environment and have connected it to MgC.
- You have **added source server credentials** to the MgC Agent. The server credentials must meet the following requirements:
  - Linux: **root** and its password
  - Windows: **administrator** and its password

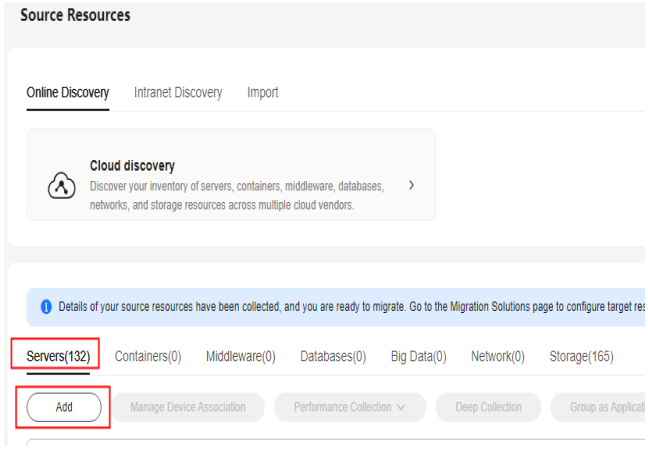
Procedure

Step 1 Sign in to the **MgC console**. In the navigation pane, under **Project**, select your **application migration project** from the drop-down list.

Step 2 In the navigation pane, choose **Discover** > **Source Resources**.

Step 3 On the **Servers** tab, click **Add** above the list.

Figure 5-4 Adding a server



Step 4 In the displayed dialog box, configure parameters listed in **Table 5-7** and click **Confirm**. The system automatically checks the credential status and starts collecting resource details.

Table 5-7 Parameters for adding a server

Parameter	Description
Name	User-defined
MgC Agent	Select the MgC Agent installed in the source environment.
Type	Select the OS type of the source server.
Access IP Address	Enter the IP address of the source server. If the source server is in the same VPC as the MgC Agent, 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 that allows access from the MgC Agent. • By default, port 5985 on Windows source servers must be opened to the MgC Agent. The port cannot be changed. • By default, port 22 on Linux source servers must be opened to the MgC Agent. You can specify a different port if needed.
Credential	Select the server credential. If the credential is not displayed in the list, go to the MgC Agent console, **add the server credential**, and synchronize it to MgC.

Step 5 After the server is added, view it in the list.

----End

6 Grouping Servers as Applications

You can group the discovered servers as applications, so you can assess the discovered source servers to get target resource recommendations and create migration workflows to migrate these servers.

NOTE

If you chose to add the discovered servers to an application when creating the discovery task, skip this section and proceed to **get target recommendations**.

Procedure

Step 1 Sign in to the **MgC console**. In the navigation pane, under **Project**, select your **application migration project** from the drop-down list.

Step 2 In the navigation pane, choose **Source Resources**.

Step 3 In the **Resources** area, choose a resource category to view the resource list.

Step 4 Select the resources to be added to an application and choose **Group as Application** above the list.

Step 5 Select the application from the drop-down list. If no applications are available, click **Create Application** in the displayed dialog box. Then enter an application name and description, select a business scenario, environment, and target region, and click **Create**.

Step 6 Click **OK**. You can view the application name in the **Application** column of the resources.

----End

7 Getting Target Recommendations

Assessing the discovered source servers, grouped as applications, can generate recommendations for appropriately sized Huawei Cloud resources. These recommendations are generated based on the specifications, performance, and business purpose of the source servers, while also considering your requirements for cost, availability, and compliance. You can export these recommendations.

This section describes how to assess an application.

NOTE

You can **associate source servers with existing target servers**. Then you can skip this step and create a workflow to migrate the source servers.

Prerequisites

- You have **discovered servers**.
- You have **grouped the discovered servers as an application**.

Procedure

Step 1 Sign in to the **MgC console**. In the navigation pane, under **Project**, select your **application migration project** from the drop-down list.

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

On the **Migration Solutions** page, you can view how many source resources and applications are managed in the current migration project, as well as whether the source resources have been configured with target resources.

Step 3 Click **Assess** in the **Target Configuration** card.

Step 4 In the **Select Application** drop-down list, select the application that you want to assess.

Step 5 In the **Select Resources** area, select the servers to be assessed in the application.

Step 6 Configure an assessment policy based on **Table 7-1**.

Table 7-1 Settings used for computing target recommendations

Parameter	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 recommends the right Huawei Cloud resources based on source resource specifications. • Match business scenario MgC recommends the right Huawei Cloud resources based on the business scenario of source resources and Huawei Cloud best practices. • Cross-AZ migration This policy only applies to migration of ECSs between AZs on Huawei Cloud, and MgC only assesses servers in the application. You need to select the target AZ you want to migrate to. 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.

Parameter	Description
Preferences	Configure your preferences for target servers. Your preferences will be first attempted to be matched during the assessment. For details about how MgC recommends appropriate target resources for you, see **How Does MgC Generate Target Recommendations?** • 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. • Sizing Criteria Choose the criteria that the system will use to generate server recommendations. – If you select **As-in on source**, the system will recommend target servers with the same or as close CPU and memory capacity as the source servers. – 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 capacity. **NOTICE** The more performance data is collected, the more accurate the assessment is. The collection of server performance data should take no less than seven days.
	For the container assessment, configure parameters such as **Cluster Type**, **Cluster Version**, and **Container Network Model** for getting recommendations for container resources.

Step 7 Click **Create Assessment**. After the assessment is complete, you can **review the target recommendations**. You can also **view the performance data of the source servers**.

Step 8 (Optional) Perform the following operations:

- **Modify target recommendations**. You can modify the recommended specifications for target servers and their disks.

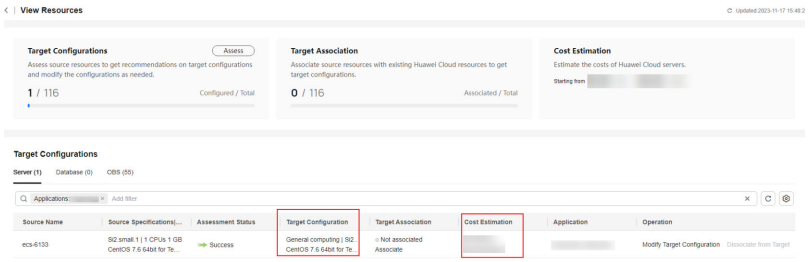
- **Associate source servers with existing target servers**. If you already have servers that match your requirements on Huawei Cloud, you can associate them with source servers to receive migrated workloads and data.

----End

Viewing Target Recommendations

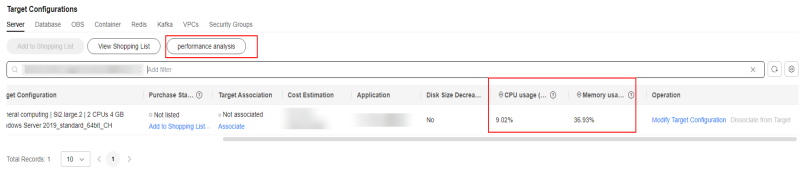
In the application list on the **Migration Solutions** page, click **View Target Configurations** in the **Operation** column.

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

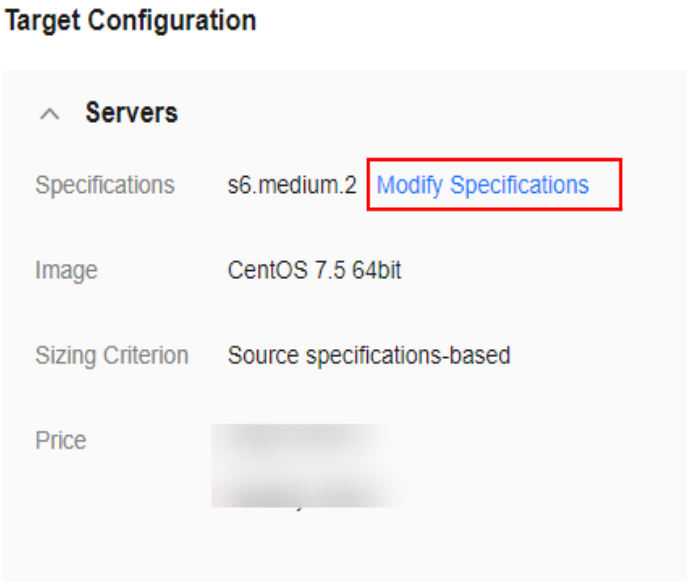
On the **Target Configurations** page, in the server list, you can view the average CPU and memory usage of each server over the last 7 or 30 days. Click **Performance Analysis** to view the performance statistics of all servers.



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.

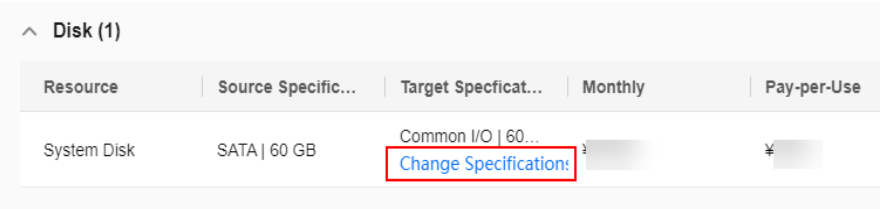
Step 2 Modify the specifications and image for the target server.



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. Only disks on Linux target servers can be downsized if the paired source servers have over-provisioned storage resources. 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

8 Creating a Server Migration Workflow

MgC provides a server migration workflow template crafted from best practices. You can customize workflows from this template by adding tasks and steps as needed. You can run all tasks in just one click and monitor the migration progress in real time.

Prerequisites

- You have **discovered servers**.
- The servers to be migrated have been **grouped as an application**.
- You have got target recommendations for source servers to be migrated by referring to **Getting Target Recommendations**.
- Migrating Windows source servers requires a Windows agent image. Since Huawei Cloud no longer provides public Windows images due to security restrictions, you need to prepare a Windows agent image on your own before the migration. For details, see **Using Custom Agent Images**.

Procedure

Step 1 Sign in to the **MgC console**. In the navigation pane, under **Project**, select your **application migration project** from the drop-down list.

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

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

Step 4 In the **Server Migration** card, click **Preview Steps** to view the steps predefined in the template and the detailed description of each step. **Automated** steps are automatically performed by MgC. **Manual** steps need to be performed by you. Click the **Server Migration** template and click **Configure Workflow** in the lower right corner.

Step 5 Configure the workflow parameters based on **Table 8-1**.

Table 8-1 Parameters for configuring a server migration workflow

Area	Parameter	Description
Workflow Details	Name	User-defined
	Description	User-defined
Application	Application	Select the application which contains the servers to be migrated.
Migration Network	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 connect the source environment to the target environment. ● If the source environment cannot access the Internet, enter the private IP address of the source proxy server and the port used by the proxy software. ● If the source proxy server cannot access the Internet, put the SMS-Agent installation package at a location where the source servers can access directly or over a proxy. You can download the SMS-Agent installation package from the SMS console.
Target Environment	Region	The target region. It defaults to the one you selected when you assessed the application.
	Project	A project in the target region.
	VPC	● If the source IP address is 192.168.*X.X*, you are advised to create a VPC and a subnet that both belong to network range 192.168.0.0/16. ● If the source IP address is 172.16.*X.X*, you are advised to create a VPC and a subnet that both belong to network range 172.16.0.0/12. ● If the source IP address is 10.*X.X.X*, you are advised to create a VPC and a subnet that both belong to network range 10.0.0.0/8.
	Subnet	The subnet must be in the same network segment as the VPC.

Area	Parameter	Description
	Security Group	• Inbound ports 8899, 8900, and 22 are allowed for Windows migrations. • Inbound port 22 is allowed for Linux file-level migrations. **CAUTION** – For security purposes, you are advised to only allow traffic from the source servers on these ports. – The firewall of the target servers must allow traffic to these ports.
	Enable Disk Encryption	If you select **No**, the system and data disks will not be encrypted for target servers newly created in the workflow.

Area	Parameter	Description
		If you select **Yes**, the system and data disks will be encrypted for target servers newly created in the workflow. **NOTICE** • This setting does not apply to the existing target servers associated with the source servers. • This setting applies to all target servers newly created by the workflow. The disks on these new target servers will be encrypted using the same key. • The encryption attribute of a disk cannot be modified after the disk is created. • Keys can be shared with accounts, not users. To enable disk encryption, you need to create an agency to authorize EVS to access KMS. If you have the right to grant the permissions, grant the KMS access permissions to EVS directly. After the authorization is successful, you do not need to perform the authorization again. If you do not have the right to grant the permissions, contact a user with the Security Administrator permissions to grant you the right and then repeat the preceding operations. After the authorization is successful, configure the following parameters: • Select an existing key Select a key from the drop-down list. You can select one of the following keys: Default keys: After the KMS access permissions have been granted to EVS, the system automatically creates a default key and names it **evs/default**. Custom keys: You can choose an existing key or create a new one. For details about how to create a key, see **Creating a Key**. **NOTICE** – The selected key must be enabled. – Only custom keys generated using the AES_256 algorithm are supported. • Enter a key ID Enter the ID of a key shared from another user. Ensure that the key is in the target region. For details, see **Creating a Grant**.

Area	Parameter	Description
Advanced Settings	Start Target After Migration	• If you select **No**, the target servers will be stopped after the migration is complete. • If you select **Yes**, the target servers will be started after the migration is complete.
	Set Bandwidth Limit	• If you select **No**, the migration traffic is not limited. • If you select **Yes**, you can limit the bandwidth that can be used for migration based on the source bandwidth and service requirements.
	Install rsync on Source	• If you select **No**, rsync will not be installed on the source servers. • If you select **Yes**, rsync will be automatically installed on the source servers as long as it is not found on these servers. **CAUTION** Linux migrations depend on rsync. If rsync is not installed on a source server, the server will fail to be migrated.
	Retain IP Address	Enable this option to retain the private IP addresses of the source servers on the target servers. Enabling it may cause risks. You need to evaluate and take responsibility for any potential risks.
	Enable Quick Mode	Enable this option if incremental synchronization is not required. This option is disabled by default. If it is enabled, incremental synchronization is skipped and then subsequent steps are performed after full replication is complete in the workflow. Set this option based on your requirements.
	Enterprise Project	Select the enterprise project you want to migrate to. The enterprise project **default** is selected by default.

Step 6 Click **Next: Confirm**.

Step 7 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 stages** and **add steps** to the workflow, click **Cancel**. The workflow enters a **Waiting** state, and the migration has not started yet. To start the migration, click **Run** in the **Operation** column.

Step 8 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

Adding a Stage

Step 1 On the migration workflow details page, move the cursor to the migration stage before or after which you want to add a stage. In the displayed window, choose **Add Stage Before** or **Add Stage After**.

Step 2 Enter a stage name and description, click **Add Step**, select a step type, enter a step name and description, and click **Confirm**. Multiple steps can be added.

Step 3 Click **Confirm**.

NOTICE

Manually added stages can be modified or deleted, but pre-defined stages cannot.

----End

Adding a Step

Step 1 On the migration workflow details page, move the cursor to the step before or after which you want to add a step. In the displayed window, choose **Add Step Before** or **Add Step After**.

Step 2 Select a step type based on **Table 8-2**, enter a step name and description, and click **Confirm**.

Table 8-2 Step types

Type	Description
Checkpoint	You need to manually confirm this type of steps, so that the workflows can continue.

Step 3 Go back to the migration stage and view the added step.

NOTICE

Manually added steps can be modified or deleted, but pre-defined steps cannot.

----End

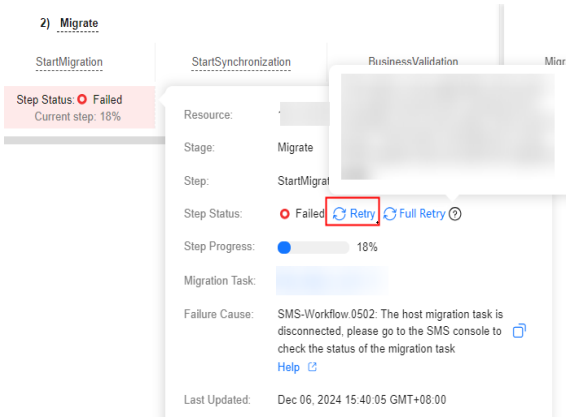
When to Use the Retry and Full Retry Buttons

During the running of the server migration workflow, the MgC Agent launches an SMS-Agent migration process on each source server. After the process is started, it communicates with the SMS console and receives commands to perform migration. During the **StartMigration** and **StartSynchronization** steps in the workflow, if the SMS-Agent process on a source server disconnects from the SMS console, the MgC console will detect the disconnection, causing the migration workflow to fail on that source server. On the migration workflow details page, you will see options **Retry** and **Full Retry**. The appropriate choice depends on the cause of the disconnection. The possible causes for the disconnection include:

- **Possible cause 1**: There is a network exception.

  In this case, the SMS-Agent process still opens on the source server. You only need to restore the network, wait until the connection to the SMS console is restored, and click **Retry** to resume the migration.

Figure 8-1 Retry



Command for checking the SMS-Agent process on Linux:

```
# ps -ef | grep -v grep | grep linuxmain
```

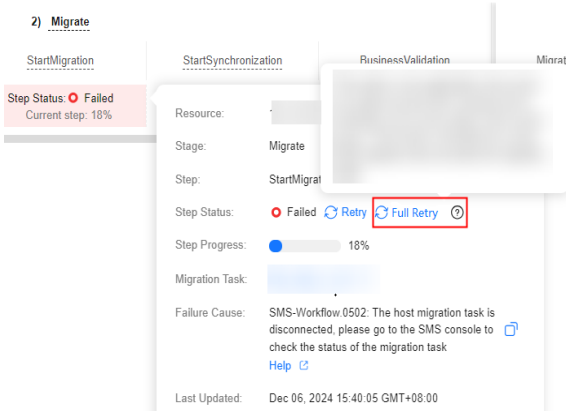
Command for checking the SMS-Agent process on Windows:

```
# Get-Process -Name SMSAgentDeploy -ErrorAction SilentlyContinue
```

- **Possible cause 2**: The SMS-Agent process is stopped due to a restart of the source server.

  In this case, the SMS-Agent process is stopped, and the migration cannot be resumed. You need to create an SMS migration task again by clicking the **Full Retry** button. Then the workflow will directly go to the **MigrationTaskClear** step. After the migration task is cleared, the workflow starts from the **StartUpAgent** step to restart the SMS-Agent process on the source server and create an SMS migration task again.

Figure 8-2 Full Retry



CAUTION

Clicking the **Full Retry** button will delete the original migration task and create a new one. The migrated data will be overwritten.

