

Migration Center

User Guide

Issue 09
Date 2024-05-08



Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

1 Permissions Management.....	1
1.1 Creating a User and Granting MgC Permissions.....	1
1.2 MgC Custom Policies.....	6
1.3 Agency Permissions.....	7
2 Configuration Management.....	17
2.1 Managing Migration Projects.....	17
2.2 Managing Credentials.....	19
3 Migration Survey.....	21
3.1 Creating a TCO Analysis Task.....	21
3.2 Assessing Migration Motivations.....	24
3.3 Assessing Migration Readiness.....	25
4 Application Discovery.....	26
4.1 Creating an Application.....	26
4.2 Discovering Resources – Complex Project.....	27
4.2.1 Discovering Resources over the Internet.....	27
4.2.2 Discovering Resources over an Intranet.....	38
4.2.3 Importing Application Associations.....	40
4.2.4 Importing Discovery Results.....	40
4.2.5 Importing Alibaba Cloud Servers.....	41
4.2.6 Importing RVTools Data.....	42
4.2.7 Viewing Application Dependency Analysis Results.....	43
4.3 Discovering Resources – Simple Project.....	45
4.3.1 Discovering Resources over the Internet.....	46
4.3.2 Discovering Resources over an Intranet.....	55
4.4 Manually Adding Resources.....	57
4.5 Collecting Server Performance Data.....	58
4.6 Grouping Resources as Applications.....	60
5 Migration Solution Design.....	62
5.1 Associating Source Servers with Target Servers.....	62
5.2 Getting Target Recommendations.....	63
5.3 Purchasing Resources.....	67
5.4 Creating a Migration Plan.....	68

6 Migration Clusters	72
6.1 Creating a Migration Cluster	72
6.2 Managing a Migration Cluster	75
6.3 Billing	76
6.4 Cluster Statuses	76
7 Migration Workflow	78
7.1 Workflow Quotas	78
7.2 Creating a Server Migration Workflow	78
7.3 Creating a Cross-AZ Migration Workflow	81
7.4 Creating a Storage Migration Workflow	83
7.5 Creating a Batch Object Storage Migration Workflow	95
7.6 Adding a Stage or Step	99
8 Change History	101

1 Permissions Management

1.1 Creating a User and Granting MgC Permissions

This section describes how to use [Identity and Access Management \(IAM\)](#) for fine-grained permissions control on your Migration Center (MgC) resources. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials for accessing MgC resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a Huawei Cloud account or cloud service to perform professional and efficient O&M on your MgC resources.

If your Huawei Cloud account does not need individual IAM users, then you may skip over this section.

This section describes the procedure for granting permissions (see [Process Flow](#)).

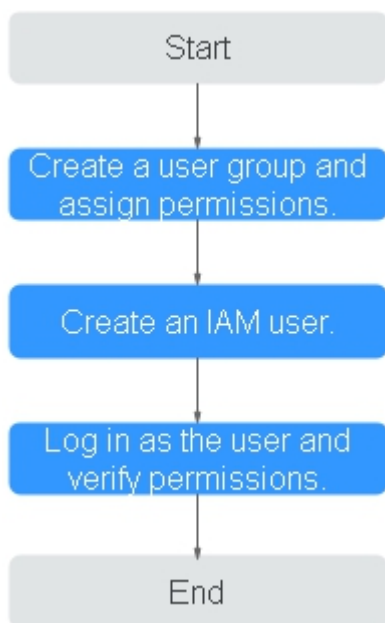
Prerequisites

Before assigning permissions to user groups, you should learn about system-defined policies supported by MgC and select the policies based on service requirements.

For details about the system-defined policies supported by MgC and the comparison between them, see [System-defined Policies](#). For the system-defined policies of other services, see [System-defined Permissions](#).

Process Flow

Figure 1-1 Granting MgC permissions to users



1. **Create a user group and assign permissions** to it.
 - **System-defined policy:** Create a user group on the IAM console, and assign the MgC system-defined policies to the user group based on the [Description of MgC System-defined Policies](#) and actual permissions requirements. Select **All Resources** for **Scope**.

Table 1-1 MgC system-defined policies

Policy Name	Description	Policy Type	Policy Content
MgC FullAccess	Administrator permissions of MgC. Users with these permissions can perform all operations on MgC data.	System-defined policy	MgC FullAccess Policy Content
MgC ReadOnlyAccess	Read-only permissions for MgC. Users with permissions can only view MgC data.	System-defined policy	MgC ReadOnlyAccess Policy Content

Policy Name	Description	Policy Type	Policy Content
MgC DiscoveryAccess	Permissions for resource discovery of MgC. Users with these permissions can use the resource discovery function of MgC and view MgC data.	System-defined policy	MgC DiscoveryAccess Policy Content
MgC AssessAccess	Permissions for application assessment of MgC. Users with these permissions can use the resource discovery and application assessment functions of MgC and view MgC data.	System-defined policy	MgC AssessAccess Policy Content
MgC MigrateAccess	Permissions for application migration of MgC. Users with these permissions can use the resource discovery, application assessment, and application migration functions of MgC and view MgC data.	System-defined policy	MgC MigrateAccess Policy Content
MgC AppDiscoveryAccess	Permissions for application discovery of MgC. Users with these permissions can use the application discovery and resource discovery functions of MgC and view MgC data.	System-defined policy	MgC AppDiscoveryAccess Policy Content
MgC MrrAccess	Permissions for service verification of MgC. Users with these permissions can use the service verification function of MgC and view MgC data.	System-defined policy	MgC MrrAccess Policy Content

- **Custom policy:** If an IAM user only needs specific MgC permissions, create custom policies. For details, see [MgC Custom Policies](#).
2. **Create an IAM user and add it to the user group.**
Create a user on the IAM console and add the user to the group created in 1.

3. **Log in** and verify permissions.
Log in to the IAM console using the created user, and in the authorized region, perform the following operations:
 - Choose **Migration Center > Service List**. On the MgC console, perform operations based on the granted permissions. If you can, the granted permissions have taken effect.
 - Choose another service from **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the granted permissions have taken effect.

MgC FullAccess Policy Content

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "mgc:*",
        "iam:agencies:listAgencies",
        "iam:agencies:createAgency",
        "iam:permissions:grantRoleToAgency"
      ],
      "Effect": "Allow"
    }
  ]
}
```

MgC ReadOnlyAccess Policy Content

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mgc:*:query*"
      ]
    }
  ]
}
```

MgC DiscoveryAccess Policy Content

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mgc:*:query*",
        "mgc:*:discovery"
      ]
    }
  ]
}
```

MgC AssessAccess Policy Content

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "mgc:*:query*",

```

```

        "mgc*:discovery",
        "mgc*:assess",
        "iam:agencies:listAgencies",
        "iam:agencies:createAgency",
        "iam:permissions:grantRoleToAgency"
    ],
    "Effect": "Allow"
  }
]
}

```

MgC MigrateAccess Policy Content

```

{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "mgc*:query*",
        "mgc*:discovery",
        "mgc*:assess",
        "mgc*:migrate",
        "iam:agencies:listAgencies",
        "iam:agencies:createAgency",
        "iam:permissions:grantRoleToAgency"
      ],
      "Effect": "Allow"
    }
  ]
}

```

MgC AppDiscoveryAccess Policy Content

```

{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mgc*:query*",
        "mgc*:discovery",
        "mgc*:appdiscovery"
      ]
    }
  ]
}

```

MgC MrrAccess Policy Content

```

{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "mgc*:query*",
        "mgc:mrr:query",
        "mgc:mrr:update",
        "mgc:mrr:export",
        "mgc:mrr:import",
        "mgc:mrr:upgrade",
        "mgc:mrr:delete",
        "mgc:mrr:check"
      ],
      "Effect": "Allow"
    }
  ]
}

```

1.2 MgC Custom Policies

Custom policies can be created to supplement the system-defined policies of MgC.

You can create custom policies in either of the following ways:

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

For details, see [Creating a Custom Policy](#). The following section contains examples of common MgC custom policies.

Example MgC Custom Policies

- Allowing users to perform platform collection and resource management

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mgc:*:query*",
        "mgc:*:discovery"
      ]
    }
  ]
}
```

- Allowing users to perform TCO analysis and server assessment

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "mgc:*:query*",
        "mgc:*:discovery",
        "mgc:*:assess",
        "iam:agencies:listAgencies",
        "iam:agencies:createAgency",
        "iam:permissions:grantRoleToAgency"
      ],
      "Effect": "Allow"
    }
  ]
}
```

- Allowing users to perform application dependency mapping

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mgc:*:query*",
        "mgc:*:discovery",
        "mgc:*:appdiscovery"
      ]
    }
  ]
}
```

- Allowing users to use migration workflows

```
{
  "Version": "1.1",
```

```
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "mgc:*:query*",
      "mgc:*:discovery",
      "mgc:*:assess",
      "mgc:*:migrate",
      "iam:agencies:listAgencies",
      "iam:agencies:createAgency",
      "iam:permissions:grantRoleToAgency"
    ]
  }
]
```

1.3 Agency Permissions

Overview

To use some functions of MgC, you must delegate MgC required permissions so that we can provide you with complete services. This section describes the scenarios where authorization is required and what custom permission policies will be created.

The system may create a new custom policy or update an existing policy during the authorization.

- If there is no available custom policy, the system automatically creates a new one.
- If there is an available custom policy but it does not contain required permissions, the system automatically updates the policy.

Creating a Cross-AZ Migration Workflow

Scenario	Delegated Object	Custom Policy	Minimum Permission
Creating a cross-AZ migration workflow	MgC	MgC AzMigrationAgencyPolicy	<p>ecs:cloudServers:showServer (Query details about an ECS)</p> <p>ecs:flavors:get (Querying ECS Flavors)</p> <p>ecs:cloudServerFlavors:get (Querying details about flavors and extended flavor information)</p> <p>ecs:cloudServerQuotas:get (Querying quotas of a tenant)</p> <p>ecs:servers:list (Querying ECSs)</p> <p>ecs:cloudServers:list (Querying details about ECSs)</p> <p>ecs:servers:stop (Stopping an ECS)</p> <p>ecs:cloudServers:listServerInterfaces (Querying NICs of an ECS)</p> <p>ecs:cloudServers:createServers (Creating an ECS)</p> <p>ecs:cloudServers:listServerBlockDevices (Querying information about the disks attached to an ECS)</p> <p>ecs:cloudServerNics:update (Configuring a private IP address for a NIC of an ECS)</p> <p>ecs:availabilityZones:list (Listing AZs)</p> <p>vpc:publicIps:create (Creating an EIP)</p> <p>vpc:publicIps:update (Updating an EIP)</p> <p>vpc:subnets:get (Querying subnets)</p> <p>vpc:networks:get (Querying networks)</p> <p>vpc:publicIps:list (Querying EIPs)</p> <p>vpc:publicIps:list (Querying details about an EIP)</p> <p>vpc:ports:get (Querying ports or querying details about a port)</p> <p>vpc:ports:delete (Deleting a port)</p> <p>vpc:ports:update (Updating a port)</p> <p>vpc:ports:create (Creating a port)</p> <p>evs:types:get (Querying EVS disk types)</p> <p>evs:volumes:list (Querying EVS disks)</p>

Scenario	Delegated Object	Custom Policy	Minimum Permission
			cbr:vaults:get (Querying a specified vault) cbr:vaults:list (Querying vaults) cbr:vaults:create (Creating a vault) cbr:vaults:addResources (Associating resources) cbr:vaults:backup (Creating a restore point) cbr:backups:list (Querying backups) cbr:tasks:list (Querying tasks) cbr:tasks:get (Querying details about a task) cbr:backups:delete (Deleting a backup) cbr:backups:get (Querying a backup) cbr:vaults:delete (Deleting a vault) ims:wholeImages:create (Creating a full-ECS image) ims:images:list (Querying images) ims:images:delete (Deleting an image) ims:images:get (Querying details about an image.) ims:serverImages:create (Creating an image)

Creating a TCO Analysis Task

Scenario	Delegated Object	Custom Policy	Minimum Permission
Creating a TCO analysis task	MgC	MgC TcoAgencyPolicy	ecs:cloudServerFlavors:get (Querying details about flavors and extended flavor information) evs:types:get (Querying EVS disk types) ims:*.get* (Querying details about an image) ims:*.list* (Querying images)

Getting Target Recommendations

Scenario	Delegated Object	Custom Policy	Minimum Permission
Getting target recommendations	MgC	MgC ServerAssessAgencyPolicy	ecs:cloudServerFlavors:get (Querying details about flavors and extended flavor information) ims:images:list (Querying images) evs:types:get (Querying EVS disk types)

Binding a Source Server to an Existing Target Server

Scenario	Delegated Object	Custom Policy	Minimum Permission
Binding a source server to an existing target server	MgC	MgC ServerBindTargetAgencyPolicy	ecs:cloudServers:showServer (Query details about an ECS) evs:volumes:list (Querying EVS disks) ecs:cloudServerFlavors:get (Querying details about flavors and extended flavor information)

Creating a Server Migration Workflow

Scenario	Delegated Object	Custom Policy	Minimum Permission
Creating a Server Migration Workflow	MgC	MgC ServerMigrationAgencyPolicy	ecs:cloudServers:showServer (Query details about an ECS) ecs:cloudServers:createServers (Creating an ECS) sms:server:migrationServer (Migrating a source server) sms:server:queryServer (Querying source servers) ecs:cloudServers:list (Querying ECSs) ecs:cloudServers:listServerBlockDevices (Querying information about the disks attached to an ECS) ecs:cloudServerQuotas:get (Querying quotas of a tenant) vpc:publicIps:create (Creating an EIP)

Purchasing Resources

Scenario	Delegated Object	Custom Policy	Minimum Permission
Purchasing resources	MgC	MgC PurchaseAgencyPolicy	eps:resources:add (Adding resources to an enterprise project) ecs:cloudServers:createServers (Creating an ECS) evs:volumes:list (Querying EVS disks) ecs:cloudServerFlavors:get (Querying details about flavors and extended flavor information) ecs:cloudServers:list (Querying details about ECSs) ecs:cloudServers:createServers (Creating an ECS) vpc:publicIps:update (Updating an EIP) vpc:publicIps:create (Creating an EIP)

Configuring a Server Purchase Template

Scenario	Delegated Object	Custom Policy	Minimum Permission
Configuring a server purchase template	MgC	MgC PurchaseTemplateAgencyPolicy	iam:projects:listProjects (Querying projects) eps:enterpriseProjects:list (Querying enterprise projects) vpc:subnets:get (Querying subnets or querying details about a subnet) vpc:securityGroups:get (Querying security groups or querying details about a security group)

Creating a Migration Cluster

Scenario	Delegated Object	Custom Policy	Minimum Permission
Creating a migration cluster	OMS	OMS ObsMigrationAgencyPolicy	ecs:cloudServers:createServers (Creating an ECS) ecs:cloudServers:listServerInterfaces (Querying NICs of an ECS) ecs:cloudServers:showServer (Query details about an ECS) ecs:cloudServers:deleteServers (Deleting ECSs) ecs:cloudServers:list (Querying details about ECSs) nat:natGateways:create (Creating a NAT Gateway) nat:natGateways:get (Querying details about a NAT gateway) nat:natGateways:delete (Deleting a NAT gateway) nat:snatRules:create (Creating an SNAT rule) nat:snatRules:get (Querying details about an SNAT rule) nat:dnatRules:list (Querying DNAT rules) nat:dnatRules:list (Querying DNAT rules) nat:snatRules:delete (Deleting an SNAT rule) nat:natGateways:list (Querying NAT gateways) vpc:securityGroups:create (Creating a security group) vpc:securityGroups:delete (Deleting a security group) vpc:securityGroups:get (Querying security groups) vpc:securityGroupRules:create (Creating a security group rule) vpc:securityGroups:get (Querying security group rules or querying details about a security group rule)

Scenario	Delegated Object	Custom Policy	Minimum Permission
			vpc:securityGroupRules:delete (Deleting a security group rule) vpc:securityGroups:get (Querying security groups or querying details about a security group) vpcep:epservices:create (Creating a VPC endpoint service) vpcep:epservices:get (Querying details about a VPC endpoint service) vpcep:permissions:list (Querying whitelist records of a VPC endpoint service) vpcep:connections:list (Querying connections of a VPC endpoint service) vpcep:epservices:list (Querying VPC endpoint services) vpcep:epservices:delete (Deleting a VPC endpoint service) vpcep:endpoints:create (Creating a VPC endpoint) vpcep:endpoints:list (Querying VPC endpoints) vpcep:endpoints:get (Querying details about a VPC endpoint) vpcep:endpoints:delete (Deleting a VPC endpoint) vpcep:connections:update (Accepting or rejecting a VPC endpoint) vpcep:permissions:update (Batch adding or deleting whitelist records of a VPC endpoint service) lts:topics:get (Querying a log topic) lts:topics:create (Creating a log topic) lts:topics:list (Querying log topics) lts:topics:delete (Deleting a log topic)

Scenario	Delegated Object	Custom Policy	Minimum Permission
			lts:*:* (Performing all operations on host groups) lts:groups:create (Creating a log group) lts:groups:get (Querying details about a log group) lts:groups:delete (Deleting a log group) aom:*:* (Full permissions for AOM) apm:icmgr:* (Full permissions for the APM collection component)
	ECS	ECS ObsMigrationAgencyPolicy	apm:icmgr:* (Full permissions for the APM collection component)

Creating a Storage Migration Workflow

Scenario	Delegated Object	Custom Policy	Minimum Permission
Creating a storage migration workflow	MgC	-	OMS Administrator (system-defined role, the administrator role of the OMS)

Creating a Lineage Collection Task

Scenario	Delegated Object	Custom Policy	Minimum Permission
Creating a lineage collection task	MgC	MgC LineageCollectionAgencyPolicy	obs:object:GetObject (Obtaining object content and metadata) obs:object:PutObject (Uploading objects with PUT or POST, copying objects, appending content to objects, initiating a multipart upload, as well as uploading, copying, and assembling parts)

2 Configuration Management

2.1 Managing Migration Projects

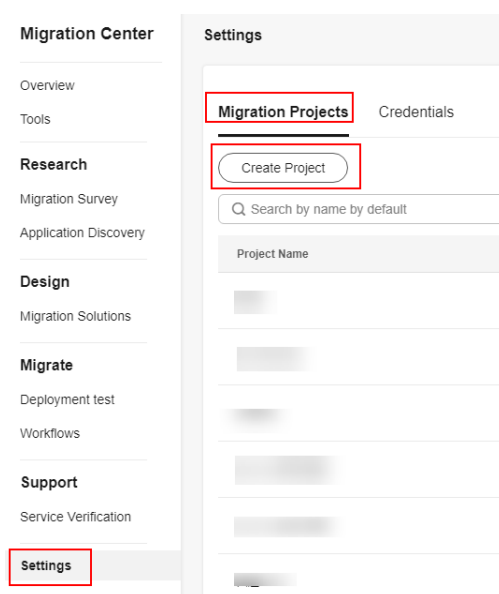
Scenarios

You can create a migration project to group, isolate, and manage resources. For example, you can create a project for migration from Alibaba Cloud to Huawei Cloud. The information about your servers, databases, and components on Alibaba Cloud and the migration progress of these resources will be stored in this project.

Creating a Migration Project

Step 1 Log in to the [MgC](#) console.

Step 2 In the navigation pane on the left, choose **Settings**. On the **Migration Projects** tab page, click **Create Project**.



Step 3 In the displayed dialog box, enter a project name, select a project type, and click **Confirm**. The project is created and you can view it in the migration project list.

Project Name ×

Project Type
The project type cannot be modified after the project is created. You can manage this project on the Settings page.

Simple
Quick migration of simple applications

Scenarios

- Migration of applications that do not use a lot of resources, such as less than 150 servers or 30 databases
- Migration of applications with simple, clear dependencies
- Migration of ECSs across AZs within a region on Huawei Cloud

Complex
Dependency mapping and migration of complex applications

Scenarios

- Migration of applications that use more resources, such as more than 150 servers or 30 databases
- Migration of applications with complex, unclear dependencies

----End

Modifying a Migration Project

Step 1 Locate the project and click **Modify** in the **Operation** column.

Step 2 In the displayed dialog box, modify the project name, project description, start time, and end time, and click **Confirm**.

Modify Project ×

* Project Name

Project Description 0/255

Start Time

End Time

----End

Archiving a Migration Project

Archived projects are not displayed in the **Migration Project** drop-down list on the top of the page. Locate the project and click **Archive** in the **Operation** column to archive the project. If you want to display an archived project in the drop-down list, you need to unarchive it first.



NOTE

The migration project being used cannot be archived.

2.2 Managing Credentials

Credentials are used by MgC to authenticate your identity during resource discovery. This section describes how to add credentials required by MgC to discovering cloud resources. To learn how to add credentials required by Edge to discover on-premises resources or required for manually adding resources to MgC, see [Adding Resource Credentials](#).

Supported Authentication Methods

Currently, only credentials of public cloud resources can be added. For details about the supported authentication modes, see [Table 2-1](#).

Table 2-1 Supported public cloud authentication methods

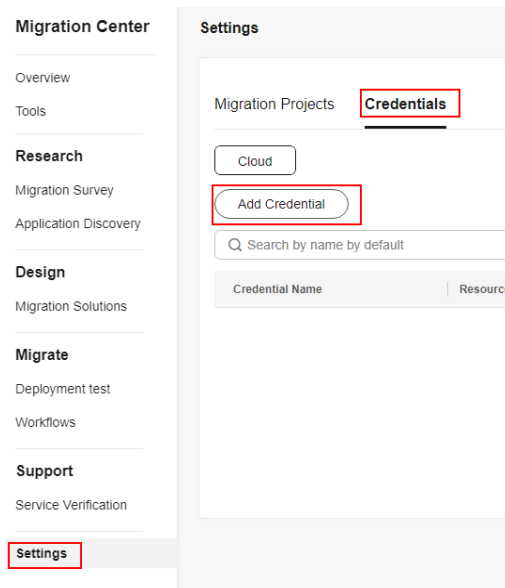
Resource Type	Authentication Method	Description
Public cloud	AK/SK	AK/SK pairs of cloud platforms, such as Huawei Cloud, Alibaba Cloud, AWS, and Tencent Cloud
	Configuration file	Credential configuration files of Google Cloud. A configuration file that contains credentials for Google Cloud service accounts can be uploaded to MgC, and the file must be in .json format and cannot exceed 4 KB.
	ID/Secret	Azure credentials. To learn how to obtain Azure credentials, see How Do I Obtain Azure Credentials?

CAUTION

Your cloud credentials are stored in the MgC database for seven days. After the validity period expires, you need to add the credentials to MgC again if you still want to discover or migrate your cloud resources.

Procedure

- Step 1** Log in to the **MgC** console.
- Step 2** In the navigation pane on the left, choose **Settings**. Select a **migration project** in the upper left corner of the page.
- Step 3** On the **Credentials** tab page, click **Add Credential**.



- Step 4** Select a resource type and authentication method as prompted. Specify a credential name, enter or upload your credential, and click **Confirm**.

After the credential is added, you can choose **Credentials > Cloud** to view the added credential.

X

Add Cloud Platform Credential

- * Resource Type: Platforms
- * Type: Public cloud
- * Credential Name: Enter a credential name.
- * Authentication: AK/SK
- * AK: Please enter AK.
- * SK: Please enter SK.
- * Location: Cloud

----End

3 Migration Survey

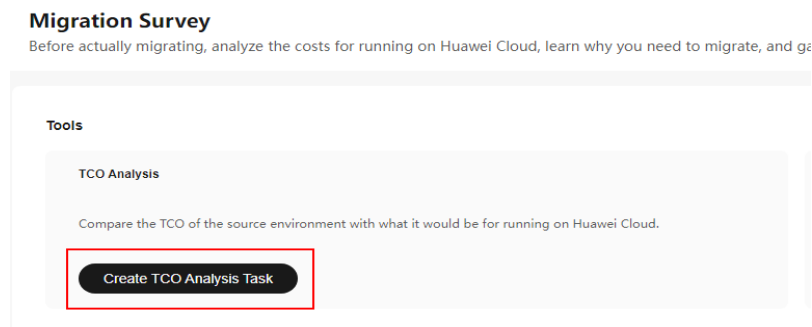
3.1 Creating a TCO Analysis Task

MgC allows you to compare the Total Cost of Ownership (TCO) of your source environment with what it would be for running on Huawei Cloud by automatically analyzing the source bills and the prices of mapped target resources.

Currently, TCO analysis supports AWS Cloud and Alibaba Cloud.

Creating a TCO Analysis Task

- Step 1** Log in to the [MgC](#) console.
- Step 2** In the navigation pane on the left, choose **Research > Migration Survey**. Select a [migration project](#) in the upper left corner of the page.
- Step 3** Click **Create TCO Analysis Task** in the **TCO Analysis** pane.



- Step 4** Configure the parameters listed in [Table 3-1](#).

Create TCO Analysis Task
✕

Task

* Task Name

Source

* Vendor

* Region

* Research Method AK/SK ?

* Credential

* Time Range ?

* Products

Target

* Region

Cancel
Confirm

Table 3-1 Parameters required for creating a TCO analysis task

Area	Parameter	Operation
Task	Task Name	Enter a task name.
Source	Vendor	Select the source cloud vendor. NOTE Currently, AWS and Alibaba Cloud can be chosen.
	Region	Select the regions where your services are running.
	Research Method	<ul style="list-style-type: none"> If you select AK/SK, specify Credential, Time Range, and Products. If no credential is available, add a credential by choosing Create from the credential drop-down list. Configure the parameters for adding a credential and click Verify and Save. <p>NOTE</p> <ul style="list-style-type: none"> Enter the AK/SK of the source platform account in the new credential. The source account only needs read-only permissions. Fees for API requests may be incurred. <ul style="list-style-type: none"> If you select Form upload, download the template, fill it out, and upload the file.

Area	Parameter	Operation
Target	Region	Select the region you want to migrate to.

Step 5 Click **Confirm**.

After the task is submitted, it will be displayed on the **TCO Analysis Tasks** page. You can click the task name to view the task progress. After the task is finished, you can [download bills](#), [view product mappings](#), and [obtain TCO analysis results](#) for further analysis.

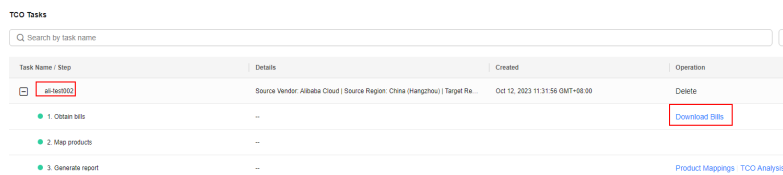
----End

Downloading Bills

MgC analyzes your bills in the specified period by product billing item and obtains the specifications, monthly usage, and monthly consumption of each product. You can download your bills after the TCO analysis is finished.

Step 1 In the TCO analysis task list, click the task name.

Step 2 Click **Download Bills** in the **Operation** column. An Excel file will be downloaded.



----End

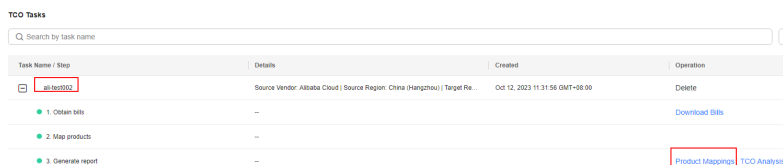
Viewing Product Mappings


MgC automatically recommends right-sized Huawei Cloud resources based on source resource specifications and usage. The least-cost-first principle is followed on the top of performance considerations.

You can view the product mapping details and adjust the mappings as needed.

Step 1 In the TCO analysis task list, click the task name.

Step 2 Click **Product Mappings** in the **Operation** column.



Step 3 Click  on the left of a resource type to view the mapping details.

----End

Viewing TCO Analysis Results

You can view how much you would save if you migrate to Huawei Cloud.

You can also compare the average monthly costs of a certain type of resource between the source cloud vendor and Huawei Cloud. In addition, you can get discounts for each type of resource from your sales manager to save more money on Huawei Cloud.

Step 1 In the TCO analysis task list, click the task name.

Step 2 Click **TCO Analysis** in the **Operation** column.

Task Name / Step	Details	Created	Operation
at-test002	Source Vendor: Alibaba Cloud Source Region: China (Hangzhou) Target Re...	Oct 12, 2023 11:31:56 GMT+08:00	Delete
1. Obtain bills	--		Download Bills
2. Map products	--		
3. Generate report	--		Product Mappings TCO Analysis

Step 3 View **Analysis Details** and **Price Differences**, and adjust the estimated costs of Huawei Cloud resources based on the discounts you got.

Click **Export Report** in the upper right corner. The analysis report will be exported to a PDF file.

----End

3.2 Assessing Migration Motivations

Scenarios

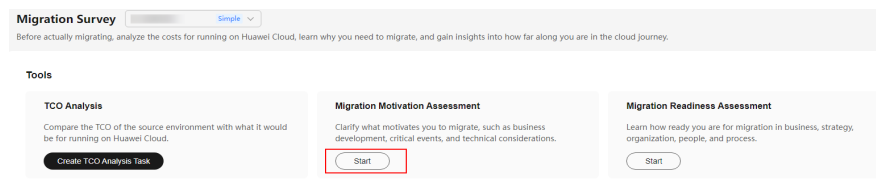
A motivation assessment helps you plan more feasible cloud migration paths and solutions.

Procedure

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

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

Step 3 Click **Start** in the **Migration Motivation Assessment** pane.



Step 4 Answer all questions and click **Submit**.

Then MgC generates and downloads the assessment report on your motivations for cloud migration. You can get Huawei Cloud suggestions on your migration to the cloud in the report.

----End

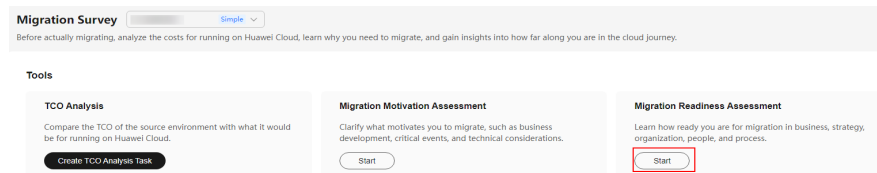
3.3 Assessing Migration Readiness

Scenarios

A cloud readiness assessment helps you learn how you are ready for migration in terms of business, strategy, organization, finance, and security. It helps you design a complete migration path and specific project plans.

Procedure

- Step 1** Log in to the **MgC** console.
- Step 2** In the navigation pane on the left, choose **Research > Migration Survey**. Select a **migration project** in the upper left corner of the page.
- Step 3** Click **Start** in the **Migration Readiness Assessment** pane.



- Step 4** Answer all questions and click **Submit**.

Then MgC generates and downloads the assessment report on your readiness for cloud migration. You can get Huawei Cloud suggestions on your migration to the cloud in the report.

----End

4 Application Discovery

4.1 Creating an Application

You can group resources with a shared business purpose as an application. These applications will be used for getting target resource recommendations and creating migration workflows.

Creating an Application for the First Time

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

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

Step 3 When you access the page for the first time, click **Create Application** in the procedure.

If a discovery task has been created, click **Create Application** in the **Application** box.

Step 4 Enter an application name and description, select a service scenario and environment, select the region you are migrating to, and click **Create Application**. The application is successfully created and the page for adding resources to the application is displayed.

- If resources have been discovered, and you want to add the discovered resources to the created application, select the resources and click **Add Now**.
- If no resources have been discovered, click **Add Later**. You can add resources to the application later.

----End

Creating More Applications

Step 1 On the **Application Discovery** page, click **Create Application** in the **Application** pane.

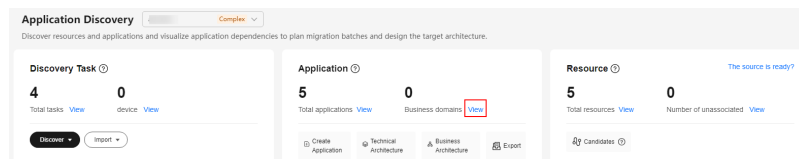
Step 2 Specify an application name and description, select the business scenario and environment, select the region where you want to provision target resources, and click **OK**. After the application is created, it will be displayed in the application list.

----End

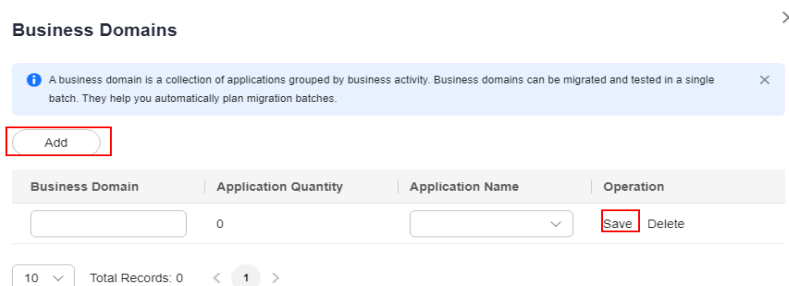
Managing Applications

You can manage applications by business domain.

Step 1 On the **Application Discovery** page, click **View** next to **Business domains**.



Step 2 Click **Add**, enter the business domain name, select the applications you want to add to this domain, and click **Save**.



----End

Modifying an Application

This operation is only supported for simple projects.

Step 1 In the application list, locate the application you want to modify and click **Modify** in the **Operation** column.

Step 2 Modify application parameters and click **OK**.

----End

4.2 Discovering Resources – Complex Project

4.2.1 Discovering Resources over the Internet

Before migrating, you need to discover your resources to be migrated. This section describes how to discover resources provisioned on cloud platforms such as Alibaba Cloud, Huawei Cloud, AWS, Tencent Cloud, Google Cloud, Azure, Qiniu Cloud, and Kingsoft Cloud over the Internet. Then you can sort out the associations between resources and applications. The resource types supported by MgC depend on the source cloud platform.

- Alibaba Cloud and Huawei Cloud: servers, containers, middleware, databases, networks, and storage
- AWS and Tencent Cloud: servers, databases, and storage
- Google Cloud and Azure: servers, containers, middleware, databases, storage, and networks
- Qiniu Cloud and Kingsoft Cloud: object storage resources

Creating a Discovery Task

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

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

Step 3 If you are a first-time user of the application discovery feature, click **Discover Over Internet** in the **Cloud Discovery** area.

If you are not a first-time user, choose **Discover > Over Internet** in the **Discovery Task** card.

Step 4 Configure the parameters listed in **Table 4-1**.

Table 4-1 Parameters for creating an Internet-based discovery task

Area	Parameter	Description	Mandatory
Basic Settings	Task Name	Specify a name for the task.	Yes
	Task Description	Enter a description of the task.	No
Task Settings	Source Platform	Select the source cloud platform. Currently, Alibaba Cloud, Huawei Cloud, AWS, Tencent Cloud, Google Cloud, Azure, Qiniu Cloud, and Kingsoft Cloud are supported.	Yes

Area	Parameter	Description	Mandatory
	Credential	<p>Select the credential for accessing the source cloud platform. If no credential is available, choose Create to add one. For details, see Managing Credentials.</p> <ul style="list-style-type: none"> • 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 Google Cloud, select Configuration File for Authentication and upload the configuration file that contains your Google Cloud service account credentials. The file must be in JSON format and cannot exceed 4 KB. • If your 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

Step 5 Enable **Cloud Platform Collection**, choose the resource types (collection items) to be collected from the **Resource Type** drop-down list. For resource types supported for each cloud platform, see [Table 4-2](#).

Table 4-2 Types of supported resources

Cloud Platform	Resource Type	Subtype
Alibaba Cloud	<ul style="list-style-type: none"> • Servers • Containers • Databases 	-
	Middleware	<ul style="list-style-type: none"> • Redis • Kafka
	Storage	<ul style="list-style-type: none"> • Object storage • File storage
	Network	<ul style="list-style-type: none"> • Cloud connections • Load balancers (ALB and CLB) • Private lines • Public domain names • Private domain names • EIPs • Public NAT gateways • Route tables • Security groups • VPCs • VPN gateways
Huawei Cloud	<ul style="list-style-type: none"> • Servers • Containers • Databases 	-
	Middleware	<ul style="list-style-type: none"> • Redis • Kafka
	Storage	<ul style="list-style-type: none"> • Object storage • File storage
	Network	<ul style="list-style-type: none"> • ELB • Public domain names • Private domain names • EIPs • Public NAT gateways • Route tables • Security groups • VPCs

Cloud Platform	Resource Type	Subtype
AWS	<ul style="list-style-type: none"> • Servers • Containers • Databases 	-
	Middleware	<ul style="list-style-type: none"> • Redis • Kafka
	Networks	<ul style="list-style-type: none"> • ELB • Public domain names • Private domain names • EIPs • Public NAT gateways • Route tables • Security groups • VPCs
	Storage	<ul style="list-style-type: none"> • Object storage • File storage
Tencent Cloud	<ul style="list-style-type: none"> • Servers • Databases 	-
	Storage	<ul style="list-style-type: none"> • Object storage • File storage
Google Cloud	<ul style="list-style-type: none"> • Servers • Containers • Databases 	-
	Middleware	Redis
	Storage	<ul style="list-style-type: none"> • Object storage • File storage
	Networks	<ul style="list-style-type: none"> • EIPs • Route tables • Security groups • VPCs
Azure	<ul style="list-style-type: none"> • Servers • Containers • Databases 	-
	Storage	<ul style="list-style-type: none"> • Object storage • File storage

Cloud Platform	Resource Type	Subtype
	Middleware	<ul style="list-style-type: none"> Redis Kafka
	Networks	<ul style="list-style-type: none"> EIPs Route tables Security groups Public NAT gateways VPCs Load balancers
Qiniu Cloud	Storage	Object storage
Kingsoft Cloud	Storage	Object storage

Step 6 (Optional) In the **Application Discovery** area, select the collection items based on which you want to identify invocation chains between resources and applications and map application dependencies.

NOTICE

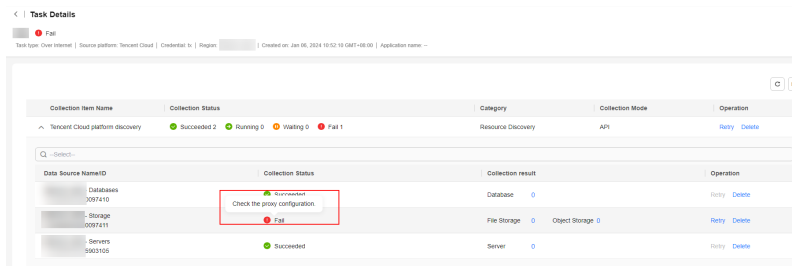
Before selecting a collection item, ensure that the account of the provided credential has the permissions for accessing the collection item.

The following table lists what information each collection item can provides.

Collection Item	Function
Resource Management	Collecting this item can help complete associations between applications and resources.
DNS	Collecting this item can help gain insights into associations between applications by analyzing traffic flows.
WAF	Collecting this item can help gain insights into application traffic flows.
LB	Collecting this item can help gain insights into applications traffic flows.
MSE	Collecting this item helps analyze associations between applications and microservices.

Step 7 Click **Confirm**. After this Internet-based discovery task is created, MgC starts discovering details about resources and applications.

- You can [view the list and details of discovered resources](#) on the **Application Discovery** page.
- You can view the task status and [view the task details](#) on the task list page.
 - 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.



- If the task status is **Succeeded**, you can go to the **Application Discovery** page to [view discovered applications and resources](#), visualized technical and business architectures, resource candidates (that you need to determine whether they belong to applications), and microservices.

Step 8 Wait until the task status changes to **Succeeded**. Then perform subsequent operations based on the resource type.

- Perform a [migration readiness check](#) or [deeper discovery](#) on the discovered servers, and [design migration solutions](#).
- Perform a [deep collection](#) on the discovered containers, and [design migration solutions](#) for them.
- [Design migration solutions](#) for middleware, database, and storage resources. [Deep collection](#) can be performed for AWS RDS for MySQL, MariaDB, and Aurora databases to obtain detailed database information.
- Perform [deep collection](#) and design migration plans for object storage resources. For details, see [Creating a Migration Plan](#).

----End

Performing a Migration Pre-check

Perform the following steps to check whether your source servers meet the migration requirements:

1. Ensure that [Edge](#) has been installed in the source intranet environment and has been registered with MgC.
2. On the **Application Discovery** page, click the **Resources** tab and click the number in the **Server** row.
3. On the top of the server list, choose **Migration Scenario > Server migration** above the list.
4. Then click **Configure** in the **Migration Readiness** column.
5. Configure the parameters listed in [Table 4-3](#).

Table 4-3 Parameters for configuring a migration pre-check

Parameter	Configuration
Type	Set this parameter based on the source server OS type.
Edge Device	Select the Edge device in the source environment.
IP Address	Select the IP address for accessing the source server. It can be a public or private IP address. After the migration pre-check is passed, the IP address you select here will be used for migration.
Port	Enter the port on the source server opened to the Edge device. <ul style="list-style-type: none">• 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 another port if needed.
Credential	Select the server credential. If the credential has not been added to MgC, go to the Edge console and add the server credential to the Edge device and synchronize it to MgC.

6. Click **Confirm**. MgC checks whether the source server can be accessed using the credential you specify. If the status in the **Migration Readiness** column changes to **Ready**, the source server can be migrated. Then you can [design a migration solution](#) to migrate the server.

Performing a Deep Collection for Servers or Containers

Perform the following steps to perform a deep collection for your source servers or containers:

1. Ensure that [Edge](#) has been installed in the source intranet environment and has been registered with MgC.
2. On the **Application Discovery** page, click the **Resources** tab and click the number in the **Server** or **Container** row.
3. Locate the server or container for which a deep collection is to be performed, click **Associate** in the **Device** column.

To associate multiple resources with the same Edge device, select them and choose **Manage Device Association** in the upper right corner of the page.

4. Select your Edge device. For **Access Setting**, if the selected resource is in the same VPC as the Edge device, select **Private access**. Otherwise, select **Public access**. Then click **OK**. Wait until the device association status changes to **Associated**.
5. In the **Credential** column, click **Associate** to associate the credential for accessing the resource.

6. Select the resource credential. If the credential has not been added to MgC, go to the Edge console and [add the credential](#) to the Edge device and synchronize it to MgC.

NOTICE

To perform a deep collection for your source servers to collect as much as details, provide server credentials that meet the following requirements:

- Linux: root account and password
- Windows: Administrator account and password

7. Click **OK**. Then MgC checks the credential association status. When the collection status is **Ready**, click **Discover** in the **Status** column to perform a deeper discovery. You can click **Rediscover** in the **Status** column to perform a second deeper discovery if needed. After the deeper discovery is complete, you can proceed to the next phase: [Designing a Migration Solution](#).

Performing a Deep Collection for Object Storage Resources

Follow the steps below to perform a deep collection for your object storage resources, so the system can use the collected details to recommend appropriate specifications of migration clusters.

1. Ensure that [Edge](#) has been installed in the source intranet environment and has been registered with MgC.
2. On the **Application Discovery** page, click the **Resources** tab and click the number in the **Storage** row.
3. In the object storage resource list, click **Configure** in the **Deep Collection** column.
4. Select the Edge device in the source environment and the credential used for accessing the resource, and click **Confirm**. If the credential has not been added to MgC, go to the Edge console and [add the resource credential](#) to the Edge device and synchronize it to MgC.
5. Click **Add Prefix** in the **Operation** column.
6. Enter a prefix to filter the objects whose details need to be collected. If this parameter is not specified, all objects in the bucket are collected by default. Click **OK** to save the prefix settings.
7. Click **Deep Collection** in the **Operation** column. The system starts collecting path details. You can perform a deep collection on a resource for multiple times. When **Collection Status** changes to **Completed**, click the resource name to view the collected information.

Performing a Deep Collection for Databases

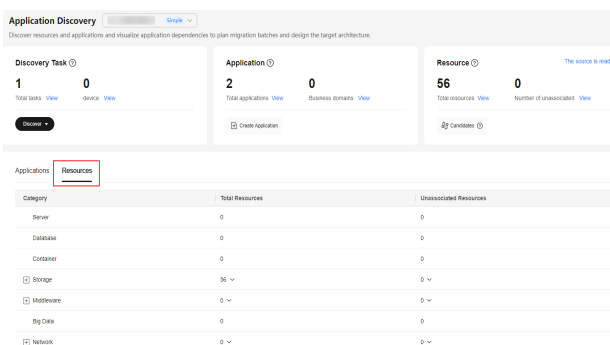
Deep collection is available for AWS RDS for MySQL, MariaDB, and Aurora databases. The data collected includes database version, engine, server character set, average transactions per second (TPS), and queries per second (QPS), and other key performance metrics (KPIs). The collected data depends on the database type.

1. Ensure that **Edge** has been installed in the source intranet environment, can access source databases, and has been registered with MgC.
2. On the **Application Discovery** page, click the **Resources** tab and click the number in **Database** row.
3. In the database list, filter all collected AWS databases by applying the **Vendor** filter. In the **Edge Device** column of each database for which deep collection is supported, click **Associate**.
To associate multiple databases with one Edge device, select them and choose **Manage Device Association** in the upper right corner of the page.
4. Select your Edge device. For **Access Setting**, if the resource to be discovered deeply is in the same VPC as the Edge device, select **Private access**. Otherwise, select **Public access**. Then click **OK**. Wait until the device association status changes to **Associated**.
5. In the **Credential** column, click **Associate** to associate the credential for accessing the database.
6. Select the database credential. If the credential has not been added to MgC, go to the Edge console and **add the credential** to the Edge device and synchronize it to MgC.
7. Click **OK**. Then MgC checks the credential association status. When **Ready** is displayed in the **Deep Collection** column, click **Collect** to start collecting database details. You can click **Collect** in the **Deep Collection** column to perform a deep collection again if needed.
8. Wait for the deep collection to complete. Then click the database name to go to the database details page. In the **Database Information** area, you can view the collected details.

Viewing the List and Details of Discovered Source Resources

A discovery task can obtain only basic information about source resources. To obtain more in-depth details, you need to perform deeper discovery.

1. On the **Application Discovery** page, click the **Resources** tab to view the number of discovered resources of each type and the number of resources that are not associated with applications.



2. Click a resource type or resource quantity to view the details.
3. Click **View** in the **Operation** column of a resource to view the basic information about the resource.

Viewing Task Details


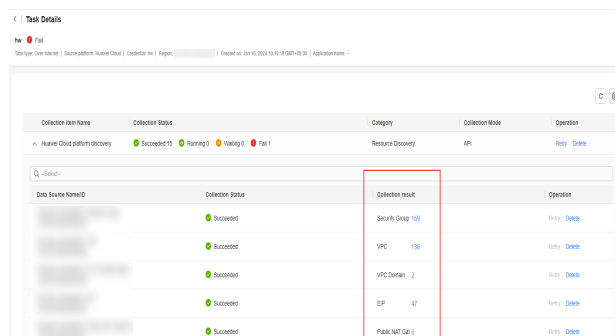
- Step 1** On the **Application Discovery** page, click **View** next to **Total tasks** to go to the task list.
- Step 2** Locate a discovery task, and click **View** in the **Operation** column.
- Step 3** Click  before a collection item to view the data sources contained in the collection item and the collection result of each resource type.

Figure 4-1 Viewing collection results



Collection Item Name	Collection Status	Category	Collection Mode	Operation
Huawei Cloud platform discovery	Succeeded 10 Running 0 Waiting 0 Fail 1	Resource Discovery	API	View Delete
Q Search				
Data Source Name/ID	Collection Status	Collection result	Operation	
	Succeeded	Security Group 100	View Delete	
	Succeeded	VPC 136	View Delete	
	Succeeded	VPC Domain 2	View Delete	
	Succeeded	EIP 47	View Delete	
	Succeeded	Public NAT Gate 1	View Delete	

- Step 4** In the **Collection Result** column, you can click the number next to a resource type to view the corresponding resource list.

----End

Rediscovering Resource Details

Rediscovery can only be executed for collection items whose collection status is **Succeeded** and collection mode is **API** and for data sources whose collection status is **Succeeded**. You need to delete the data sources that fail to be collected and click **Add Data Source** to collect data again.

- Step 1** On the task list page, locate a discovery task, and click **View** in the **Operation** column.
- Step 2** Locate a data source, click **Collect** in the **Operation** column, and click **OK**.

Locate the required collection item, choose **More > Collect** in the **Operation** column, and click **OK**.

----End

Viewing Application Dependency Analysis Results

After the resource discovery is complete, MgC sorts out the associations between these resources and your applications. For details, see [Viewing Application Dependency Analysis Results](#).

Exporting Application Dependencies

On the **Application Discovery** page, click **Export** in the upper right corner to export the access-layer call chains, database dependencies, middleware dependencies, and application dependencies for further analysis.

4.2.2 Discovering Resources over an Intranet

This section describes how to discover on-premises infrastructure with limited Internet access. You need to install Edge in the on-premises environment to discover resources by network range or VMware host.

Precautions

- Only VMs in VMware vSphere 5.0 to 7.0 can be discovered.
- When the system scans VMware VMs or scans servers on specified network ranges, private IP addresses and the ID of the involved Edge device are used to identify discovered servers. If the private IP address of a discovered server, 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, you are advised not to change private IP addresses of source servers before the migration is complete.

Prerequisites

- You have **installed Edge** in the source intranet environment and have connected the Edge device with MgC.
- You have **added source server credentials** to the Edge device.

NOTICE

To perform a deep collection for your source servers to collect as much as details, provide server credentials that meet the following requirements:

- Linux: root account and password
 - Windows: Administrator account and password
-

Creating a Discovery Task

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

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

Step 3 If you are first-time user of MgC, click **Discover Over Intranet** in the **Edge Discovery** area.

If you are not a first-time user of MgC, choose **Discover > Over Intranet** in the **Discovery Task** card.

Step 4 Configure a discovery task based on **Table 4-4**.

Table 4-4 Parameters for creating an intranet-based discovery task

Parameter	Description
Task Name	Enter a task name.

Parameter	Description
Task Description	Describe the task.
Device	Select the device where Edge was installed in the source intranet environment.

Step 5 Enable **Scan Network Range** or **Scan VMware VMs** to discover servers as needed.

- If **Scan Network Range** is enabled, configure parameters listed in [Table 4-5](#).

Table 4-5 Parameters for scanning a network range

Parameter	Description
Protocol	Select the communication protocol TCP or ICMP .
Network Range	There are three supported IP address ranges: <ul style="list-style-type: none"> - 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 Linux servers. This parameter is available only if you choose the TCP protocol. If you need to skip Linux servers during the scan, set this parameter to 0 .
Windows	Enter the port for scanning Windows servers. This parameter is available only if you choose the TCP protocol. If you need to skip Windows servers during the scan, set this parameter to 0 .

- If **Scan VMware VMs** is enabled, enter the IP address of a vCenter Server in the **IP Address** text box, and select the credential for accessing the vCenter Server. All VMs managed by the vCenter Server will be discovered. If the vCenter Server's credential has not been added, click **Create** to add it to MgC by referring to [Adding Resource Credentials](#). When adding the credential, enter the username and password for logging in to the vCenter Server.

Step 6 Click **Confirm**. The intranet-based discovery task is created, and MgC starts collecting details about source servers.

On the **Application Discovery** page, click **View** next to **Total tasks** to go to the task list and view the task status.

Step 7 Wait until the task status changes to **Succeeded**, and perform a deeper discovery. Servers discovered on an intranet have an Edge device associated. You just need to associated credentials with these servers before you can perform a deeper discovery.

1. On the **Application Discovery** page, click the **Resources** tab and click the number in the **Server** row.

2. Locate a server and click **Associate** in the **Credential** column.
3. Select the server credential. If the credential has not been added to MgC, go to the Edge console and [add the server credential](#) to the Edge device and synchronize it to MgC.
4. Click **OK**. Then MgC checks the credential association status. When the collection status is **Ready**, click **Discover** in the **Status** column to perform a deeper discovery. You can click **Rediscover** in the **Status** column to perform a second deeper discovery if needed.

----End

4.2.3 Importing Application Associations

You can import application details obtained from the configuration management database in your source environment to MgC. Then, MgC can use the imported details to analyze application dependencies.

Procedure

- Step 1** Log in to the [MgC](#) console.
- Step 2** In the navigation pane on the left, choose **Research > Application Discovery**. Select a [migration project](#) in the upper left corner of the page.
- Step 3** If you are creating an import task for the first time, choose **Import > Application associations** in the **Tool Discovery** card. If you have created import tasks before, choose **Import > Application associations** in the **Discovery Task** card. In the displayed **Import Application Associations** dialog box, click **Download import template** to download the import template to the local PC.
- Step 4** Populate the template with your application details and save the file. Parameters highlighted in yellow are mandatory. Then click **Select File** to upload the saved file to MgC.
- Step 5** Click **Confirm**.

You can view the task in the task list.

- 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 a data source to view the failure cause. After handling the failure cause, you need to delete the failed task and perform a second import.
- If the task status is **Succeeded**, you can go to the application discovery page to [view application dependency analysis results](#).

----End

4.2.4 Importing Discovery Results

You can use offline collectors to discover your resources and applications, and import the discovery results to MgC for automated application association analysis.

Prerequisites

You have created collection tasks using offline collectors by referring to [Creating a Collection Task](#), and have obtained the discovery results.

Procedure

- Step 1** Log in to the [MgC](#) console.
- Step 2** In the navigation pane on the left, choose **Research > Application Discovery**. Select a [migration project](#) in the upper left corner of the page.
- Step 3** If you create an import task for the first time, choose **Import > Discovery results** in the **Tool Discovery** area. If you have created import tasks before, choose **Import > Discovery results** in the **Discovery Task** pane.
- Step 4** In the **Import Discovery Results** dialog box, click **Select File** to upload the JSON file that stores the discovery results to MgC.
- Step 5** Click **Confirm**.

You can view the task in the task list.

- 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. After handling the failure cause, you need to delete the failed task and perform a second import.
- If the task status is **Succeeded**, you can go to the application discovery page to [view application dependency analysis results](#).

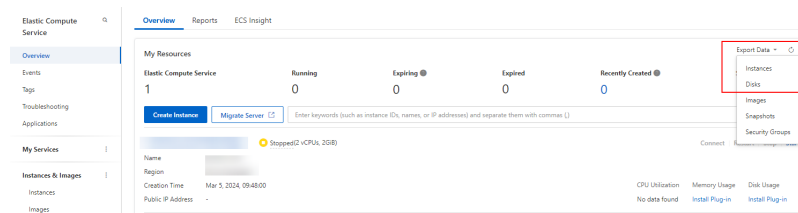
----End

4.2.5 Importing Alibaba Cloud Servers

You can directly import information about cloud servers and disks on Alibaba Cloud to MgC. The resource information must be recorded in CSV files. Using the imported information, MgC can recommend appropriate Huawei Cloud resources for you.

Exporting Alibaba Cloud ECS Instances and Disks

- Step 1** Log in to the Alibaba Cloud ECS console.
- Step 2** On the **Overview** page, choose **Export Data > Instances** to export a list of all ECS instances.



- Step 3** Choose **Export Data > Disks** to export a list of all cloud disks.

- Step 4** Open the instance list and the disk list and adjust the resource information in the list as required. Ensure that the lists contain the following necessary information:

List	Mandatory Fields
Instance list	Instance ID, OS, instance specifications, CPU, and memory
Disk list	Instance ID, disk ID, capacity (GiB), and disk attributes

----End

Importing Alibaba Cloud Resources

- Step 1** Log in to the [MgC](#) console.
- Step 2** In the navigation pane on the left, choose **Research > Application Discovery**. Select a [migration project](#) in the upper left corner of the page.
- Step 3** If you are creating an import task for the first time, in the **Tool Discovery** area, choose **Import > Alibaba Cloud Resources**. If you have created import tasks before, in the **Discovery Task** card, choose **Import > Alibaba Cloud Resources**.

NOTICE

Only CSV files encoded in UTF-8 format with English table headers can be imported. The size of a single file cannot exceed 15 MB. For details about how to convert the encoding format of a CSV file to UTF-8, see [How Do I Convert the Encoding Format of a CSV File to UTF-8?](#)

- Step 4** Click **Select File** next to **Server List** and select the [exported instance list](#).
- Step 5** Click **Select File** next to **Disk List** and select the [exported disk list](#).
- Step 6** Click **Confirm**. After the instance and disk information is imported successfully, click the **Resource** tab and view the server list. You can view the imported Alibaba Cloud servers in the list.
- Step 7** (Optional) Group imported Alibaba Cloud servers as an application. For details, see [Grouping Resources as Applications](#). Then assess the application to obtain recommendations for Huawei Cloud resources. For details, see [Getting Target Recommendations](#).

----End

4.2.6 Importing RVTools Data

Constraints

- **Supported RVTools versions**
The file to be imported must be an Excel (.xlsx) exported from **RVTools 4.5.1**. If you use another RVTools version, adjust the exported file to fit the RVTools 4.5.1 version.

- **File size and compression ratio requirements**
The file to be imported cannot be larger than 50 MB, and the compression ratio cannot be lower than 5%.
- **Data filtering**
In the imported RVTools file, if **CPUs** or **Memory** of a server on the **vInfo** sheet is empty or **0**, the server information will not be parsed by MgC.

Exporting RVTools Data

Step 1 Start the RVTools application.

Step 2 On the login page, enter the following information:

- In the **IP address/Name** text box, enter IP address of the vCenter server.
- In the **User name** text box, enter the username for connecting to the vCenter server.
- In the **Password** text box, enter the password corresponding to the username.

Step 3 Click **Login**. In the top menu bar, choose **File > Export all to Excel**.

Step 4 Select a path for saving the file that contains details about your resource.

----End

Importing RVTools Data

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

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

Step 3 If you are creating a discovery task for the first time, in the **Tool Discovery** card, choose **Import > RVTools data**. If you have created discovery tasks before, in the **Discovery Task** card, choose **Import > RVTools data**.

Step 4 In the displayed **Improt RVTools Data** window, click **Select File** and select the **file exported from RVTools**.

Step 5 Click **Confirm**.

You can view the task in the task list.

- 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. After handling the failure cause, you need to delete the failed task and perform a second import.
- If the task status is **Succeeded**, you can go to the resource list page to view the imported details about your resources.

----End

4.2.7 Viewing Application Dependency Analysis Results

To help you make migration plans and design architectures for the target environment, MgC sorts out the relationships between your resources and

applications and represents application technical architectures and application dependencies into graphs.

Prerequisites

You need to complete one of the following tasks:

- [Discovering Resources over the Internet](#)
- [Discovering Resources over an Intranet](#)
- [Importing Application Associations](#)
- [Importing Discovery Results](#)

Viewing the Technical Architecture

Step 1 On the **Applications** tab page of the **Application Discovery** page, click **Technical Architecture** in the upper right corner to view the matrix of all discovered services, microservices, and resources.

Step 2 Right-click a service and view its technical architecture, dependencies, and microservices.

----End

Viewing the Business Architecture

Step 1 On the **Applications** tab page of the **Application Discovery** page, click **Business Architecture** in the upper right corner to view a matrix of all discovered services, microservices, and resources.

Step 2 Right-click a service and view its technical architecture, dependencies, and microservices.

----End

Viewing Resources

Step 1 On the **Application Discovery** page, click the **Resources** tab to view the number of discovered resources and the number of resources that are not associated with applications.

Step 2 Click a resource type or resource quantity to view the details. Click **View** in the **Operation** column of a resource to view the basic information about the resource.

----End

Viewing Applications

On the **Application** tab page of the **Application Discovery** page, you can view all discovered applications. In the application list, you can view the name, type, business domain, number of microservices, as well as the numbers of downstream and upstream applications of each application.

- To view all microservices contained in an application, click the number in the **Microservices** column.

- To view all applications that an application relies on, click the number in the **Upstream Applications** column.
- To view all applications that an application is relied on, click the number in the **Downstream Applications** column.
- To view what microservices are contained in an application, as well as their layers and associations, locate the service and click **Technical Architecture** in the **Operation** column. In the displayed technical architecture, click a microservice or resource node to view its details.
- To view the associations between an application and its upstream and downstream applications, you can click **Dependency Map** in the **Operation** column. To view the details about this service and its upstream and downstream services, click its box.

Viewing Resource Candidates

Step 1 On the **Application Discovery** page, click **Candidates** in the **Resource** pane.

Step 2 On the **Resources** tab page, view the list of all collected resources and their details.

- To view the associations between a service and its upstream and downstream services, you can click **Service Dependencies** in the **Operation** column.
- To delete a service, click **Delete** in the **Operation** column.

----End

Viewing Microservices

Step 1 On the **Application Discovery** page, click **Candidates** in the **Resource** pane.

Step 2 Click the **Microservices** tab to view the list of all collected microservices.

- To view the layer of a microservice and its associations with other resources, click **Technical Architecture** in the **Operation** column. In the displayed technical architecture, click a microservice or resource node to view its details.
- To view the associations between a microservice and its upstream and downstream services, choose **More > Service Dependencies** in the **Operation** column. To view the details about this microservice and its upstream and downstream services, click its box.
- To delete a microservice, click **More > Delete** in the **Operation** column.

----End

Exporting Application Dependencies

On the **Application Discovery** page, click **Export** in the **Application** card to export the access-layer call chains, database dependencies, middleware dependencies, and application dependencies for further analysis.

4.3 Discovering Resources – Simple Project

4.3.1 Discovering Resources over the Internet

Before migrating, you need to discover your resources. This section describes how to discover resources provisioned on cloud platforms such as Alibaba Cloud, Huawei Cloud, AWS, Tencent Cloud, Google Cloud, Azure, Qiniu Cloud, and Kingsoft Cloud over the Internet. The resource types MgC can discover depends on the cloud platform.

- Alibaba Cloud and Huawei Cloud: servers, containers, middleware, databases, networks, and storage
- AWS: servers, databases, and storage
- Google Cloud and Azure: servers, containers, middleware, databases, storage, and networks
- Qiniu Cloud and Kingsoft Cloud: object storage resource

Creating a Discovery Task

Step 1 Log in to the [MgC](#) console.

Step 2 In the navigation pane on the left, choose **Research > Application Discovery**. Select a [migration project](#) in the upper left corner of the page.

Step 3 If you are a first-time user of MgC, click **Discover Over Internet** in the **Cloud Discovery** area.

If you are not a first-time user of MgC, choose **Discover > Over Internet** in the **Discovery Task** card.

Step 4 Configure a discovery task based on [Table 4-6](#).

Table 4-6 Parameters for creating an Internet-based discovery task

Area	Parameter	Description	Mandatory
Task Basics	Task Name	Specify a name for the task.	Yes
	Task Description	Describe the task.	No
Task Settings	Source Platform	Select the source cloud platform. Currently, Alibaba Cloud, Huawei Cloud, AWS, Tencent Cloud, Google Cloud, Azure, Qiniu Cloud, and Kingsoft Cloud are supported.	Yes

Area	Parameter	Description	Mandatory
	Credential	<p>Select the credential for accessing the source cloud platform. If no credential is available, choose Create to create a credential by referring to Adding a Credential.</p> <ul style="list-style-type: none"> 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 Google Cloud, select Configuration File for Authentication and upload the configuration file that contains your Google Cloud service account credentials. The file must be in JSON format and cannot exceed 4 KB. If your 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 regions where your source services are running.	Yes

Step 5 Choose the resource types (collection items) to be collected from the **Resource Type** drop-down list. For resource types supported for each cloud platform, see [Table 4-7](#).

Table 4-7 Types of supported resources

Cloud Platform	Resource Type	Subtype
Alibaba Cloud	<ul style="list-style-type: none"> Servers Containers Databases 	-

Cloud Platform	Resource Type	Subtype
	Middleware	<ul style="list-style-type: none"> • Redis • Kafka
	Storage	<ul style="list-style-type: none"> • Object storage • File storage
	Networks	<ul style="list-style-type: none"> • Cloud connections • Load balancers (ALB and CLB) • Private lines • Public domain names • Private domain names • EIPs • Public NAT gateways • Route tables • Security groups • VPCs • VPN gateways
Huawei Cloud	<ul style="list-style-type: none"> • Servers • Containers • Databases 	-
	Middleware	<ul style="list-style-type: none"> • Redis • Kafka
	Storage	<ul style="list-style-type: none"> • Object storage • File storage
	Networks	<ul style="list-style-type: none"> • Load balancers (ELB) • Public domain names • Private domain names • EIPs • Public NAT gateways • Route tables • Security groups • VPCs
AWS	<ul style="list-style-type: none"> • Servers • Containers • Databases 	-
	Storage	<ul style="list-style-type: none"> • Object storage • File storage

Cloud Platform	Resource Type	Subtype
	Networks	<ul style="list-style-type: none"> • Load balancers (ELB) • Public domain names • Private domain names • EIPs • Public NAT gateways • Route tables • Security groups • VPCs
	Storage	<ul style="list-style-type: none"> • Object storage • File storage
Tencent Cloud	<ul style="list-style-type: none"> • Servers • Databases 	-
	Storage	<ul style="list-style-type: none"> • Object storage • File storage
Google Cloud	<ul style="list-style-type: none"> • Servers • Containers • Databases 	-
	Middleware	Redis
	Storage	<ul style="list-style-type: none"> • Object storage • File storage
	Networks	<ul style="list-style-type: none"> • EIPs • Route tables • Security groups • VPCs
Azure	<ul style="list-style-type: none"> • Servers • Containers • Databases 	-
	Storage	<ul style="list-style-type: none"> • Object storage • File storage
	Middleware	<ul style="list-style-type: none"> • Redis • Kafka

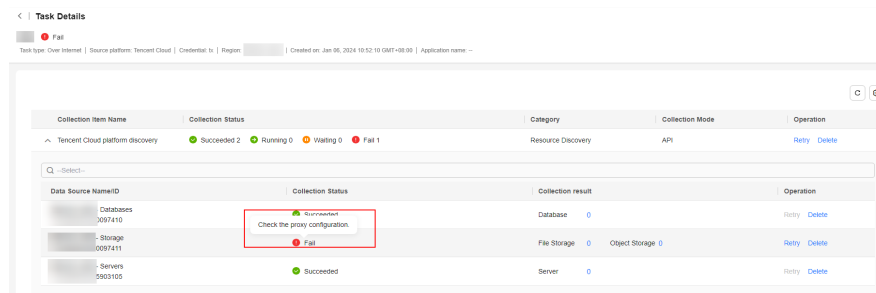
Cloud Platform	Resource Type	Subtype
	Networks	<ul style="list-style-type: none"> EIPs Route tables Security groups Public NAT gateways VPCs Load balancers
Qiniu Cloud	Storage	Object storage
Kingsoft Cloud	Storage	Object storage

Step 6 (Optional) Associate the servers to be discovered 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**. After this Internet-based discovery task is created, MgC starts discovering details about resources and applications.

- You can **view the list and details of discovered resources** on the **Application Discovery** page.
- You can view the task status and **view the task details** on the task list page. 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.



Step 8 Wait until the task status changes to **Succeeded**. Then perform subsequent operations based on the resource type.

- Perform a **migration readiness check** or **deeper discovery** on the discovered servers, and **design migration solutions**.
- Perform a **deeper discovery** on the discovered containers, and **design migration solutions**.

- **Design migration solutions** for middleware, database, and storage resources. **Deep collection** can be performed for AWS RDS for MySQL, MariaDB, and Aurora databases to obtain detailed database information.
- Perform **deep collection** and design migration plans for object storage resources. For details, see **Creating a Migration Plan**.

----End

Performing a Migration Readiness Check

Perform the following steps to check whether your source servers meet the migration requirements:

1. Ensure that **Edge** has been installed in the source intranet environment and has been registered with MgC.
2. On the **Application Discovery** page, click the **Resources** tab and click the number in the **Server** row.
3. On the top of the server list, choose **Migration Scenario > Server migration** above the list.
4. Then click **Configure** displayed in the **Migration Readiness** column.
5. Configure the parameters listed in **Table 4-8**.

Table 4-8 Migration readiness parameters

Parameter	Configuration
Type	Set this parameter based on the source server OS type.
Edge Device	Select the Edge device in the source environment.
IP Address	Select the IP address for accessing the source server. It can be a public or private IP address. After the migration pre-check is passed, the IP address you select here will be used for migration.
Port	Enter the port on the source server opened to the Edge device. <ul style="list-style-type: none"> • 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 another port if needed.
Credential	Select the server credential. If the credential has not been added to MgC, go to the Edge console and add the server credential to the Edge device and synchronize it to MgC.

6. Click **Confirm**. The system verifies the configuration information and starts to check whether the source server is ready for migration. If the status in the **Migration Readiness** column changes to **Ready**, the source server can be migrated. Then you can **design a migration solution** to migrate the server.

Performing a Deep Collection for Servers or Containers

Perform the following steps to perform a deeper discovery on your source servers or containers:

1. Ensure that **Edge** has been installed in the source intranet environment and has been registered with MgC.
2. On the **Application Discovery** page, click the **Resources** tab and click the number in the **Server** or **Container** row.
3. Locate the server or container that a deeper discovery is to be performed for, click **Associate** in the **Device** column.

To perform a deeper discovery for multiple servers, select them and choose **Manage Device Association** in the upper right corner of the page.

4. Select your Edge device. For **Access Setting**, if the resource to be discovered deeply is in the same VPC as the Edge device, select **Private access**. Otherwise, select **Public access**. Then click **OK**. Wait until the device association status changes to **Associated**.
5. In the **Credential** column, click **Associate** to associate the credential for accessing the server or container.
6. Select the resource credential. If the credential has not been added to MgC, go to the Edge console and **add the credential** to the Edge device and synchronize it to MgC.

NOTICE

To perform a deep collection for your source servers to collect as much as details, provide server credentials that meet the following requirements:

- Linux: root account and password
- Windows: Administrator account and password

-
7. Click **OK**. MgC checks the credential association status. When the collection status is **Ready**, click **Discover** in the **Status** column to perform a deeper discovery. You can click **Rediscover** in the **Status** column to perform a second deeper discovery if needed. After the deeper discovery is complete, you can proceed to the next phase: **Designing a Migration Solution**.

Performing a Deep Collection for Object Storage Resources

Follow the steps below to perform a deep collection for your object storage resources, so the system can use the collected details to recommend appropriate specifications of migration clusters.

1. Ensure that **Edge** has been installed in the source intranet environment and has been registered with MgC.
2. On the **Application Discovery** page, click the **Resources** tab and click the number in the **Storage** row.
3. In the object storage resource list, click **Configure** in the **Deep Collection** column.
4. Select the Edge device in the source environment and the credential used for accessing the resource, and click **Confirm**. If the credential has not been

added to MgC, go to the Edge console and [add the resource credential](#) to the Edge device and synchronize it to MgC.

5. Click **Add Prefix** in the **Operation** column.
6. Enter a prefix to filter the objects whose details need to be collected. If this parameter is not specified, all objects in the bucket are collected by default. Click **OK** to save the prefix settings.
7. Click **Deep Collection** in the **Operation** column. The system starts collecting path details. You can perform a deep collection on a resource for multiple times. When **Collection Status** changes to **Completed**, click the resource name to view the collected information.

Performing a Deep Collection for Databases

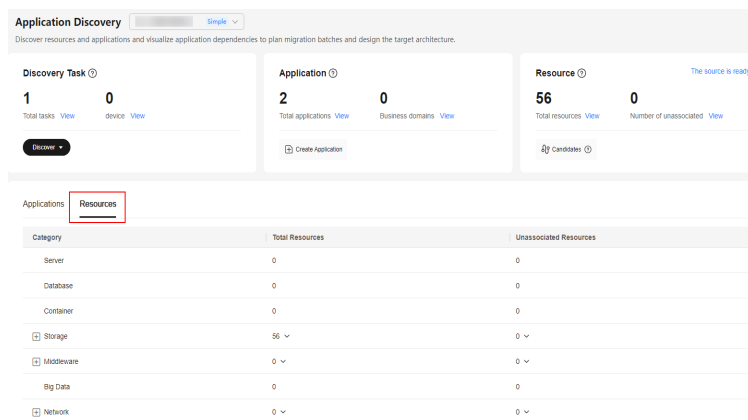
Deep collection is available for AWS RDS for MySQL, MariaDB, and Aurora databases. The data collected includes database version, engine, server character set, average transactions per second (TPS), and queries per second (QPS), and other key performance metrics (KPIs). The collected data depends on the database type.

1. Ensure that [Edge](#) has been installed in the source intranet environment, can access source databases, and has been registered with MgC.
1. On the **Application Discovery** page, click the **Resources** tab and click the number in the **Database** row.
2. In the database list, filter all collected AWS databases by applying the **Vendor** filter. In the **Edge Device** column of each database for which deep collection is supported, click **Associate**.
To associate multiple databases with one Edge device, select them and choose **Manage Device Association** in the upper right corner of the page.
3. Select your Edge device. For **Access Setting**, if the resource to be discovered deeply is in the same VPC as the Edge device, select **Private access**. Otherwise, select **Public access**. Then click **OK**. Wait until the device association status changes to **Associated**.
4. In the **Credential** column, click **Associate** to associate the credential for accessing the resource.
5. Select the database credential. If the credential has not been added to MgC, go to the Edge console and [add the credential](#) to the Edge device and synchronize it to MgC.
6. Click **OK**. Then MgC checks the credential association status. When **Ready** is displayed in the **Deep Collection** column, click **Collect** to start collecting database details. You can click **Collect** in the **Deep Collection** column to perform a deep collection again if needed.
7. Wait for the deep collection to complete. Then click the database name to go to the database details page. In the **Database Information** area, you can view the collected details.

Viewing the List and Details of Discovered Source Resources

A discovery task can obtain only basic information about source resources. More detailed information needs to be obtained through a deeper discovery.

1. On the **Application Discovery** page, click the **Resources** tab to view the number of discovered resources of each type and the number of resources that are not associated with applications.



2. Click a resource type or resource quantity to view the details.
3. Click **View** in the **Operation** column of a resource to view the basic information about the resource.

Viewing Task Details


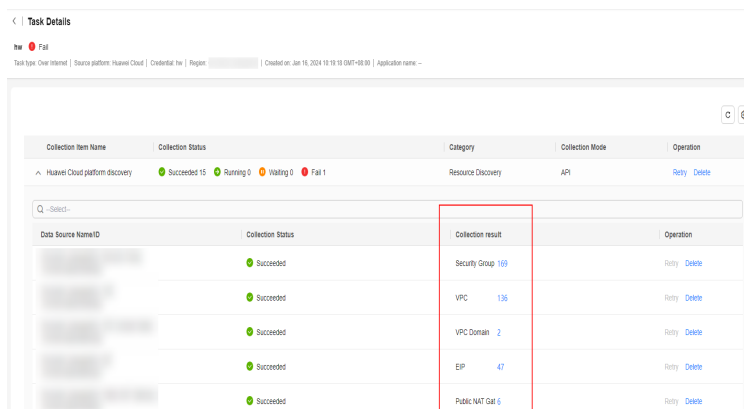
- Step 1** On the **Application Discovery** page, click **View** next to **Total tasks** to go to the task list.
- Step 2** Locate a discovery task, and click **View** in the **Operation** column.
- Step 3** Click  before a collection item to view the data sources contained in the collection item and the collection result of each resource type.

Figure 4-2 Viewing collection results



- Step 4** In the **Collection Result** column, you can click the number next to a resource type to view the corresponding resource list.

----End

Rediscovering Resource Details

Rediscovery can only be executed for collection items whose collection status is **Succeeded** and collection mode is **API** and for data sources whose collection

status is **Succeeded**. You need to delete the data sources that fail to be collected and click **Add Data Source** to collect data again.

Step 1 On the task list page, locate a discovery task, and click **View** in the **Operation** column.

Step 2 Locate the required data source, click **Re-collect** in the **Operation** column, and click **OK**.

Locate the required collection item, choose **More > Re-collect** in the **Operation** column, and click **OK**.

----End

4.3.2 Discovering Resources over an Intranet

This section describes how to discover on-premises infrastructure with limited Internet access. You need to install Edge in the on-premises environment to discover resources by network range or VMware host.

Precautions

- Only VMs in VMware vSphere 5.0 to 7.0 can be discovered.
- When the system scans VMware VMs or scans servers on specified network ranges, private IP addresses and the ID of the involved Edge device are used to identify discovered servers. If the private IP address of a discovered server, 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, you are advised not to change private IP addresses of source servers before the migration is complete.

Prerequisites

- You have **installed Edge** in the source intranet environment and have connected the Edge device with MgC.
- You have **added source server credentials** to the Edge device.

NOTICE

To perform a deep collection for your source servers to collect as much as details, provide server credentials that meet the following requirements:

- Linux: root account and password
 - Windows: Administrator account and password
-

Creating a Discovery Task

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

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

Step 3 If you are first-time user of MgC, click **Discover Over Intranet** in the **Edge Discovery** area.

If you are not a first-time user of MgC, choose **Discover** > **Over Intranet** in the **Discovery Task** card.

Step 4 Configure a discovery task based on [Table 4-9](#).

Table 4-9 Parameters for creating an intranet-based discovery task

Parameter	Description
Task Name	Specify a name for the task.
Task Description	Describe the task.
Device	Select the device where Edge was installed in the source intranet environment.

Step 5 Enable **Scan Network Range** or **Scan VMware VMs** to discover servers as needed.

- If **Scan Network Range** is enabled, configure parameters listed in [Table 4-10](#).

Table 4-10 Parameters for scanning a network range

Parameter	Description
Protocol	Select the communication protocol TCP or ICMP .
Network Range	There are three supported IP address ranges: <ul style="list-style-type: none">- 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 Linux servers. This parameter is available only if you choose the TCP protocol. If you need to skip Linux servers during the scan, set this parameter to 0 .
Windows	Enter the port for scanning Windows servers. This parameter is available only if you choose the TCP protocol. If you need to skip Windows servers during the scan, set this parameter to 0 .

- If **Scan VMware VMs** is enabled, enter the IP address of a vCenter Server in the **IP Address** text box, and select the credential for accessing the vCenter Server. All VMs managed by the vCenter Server will be discovered. If the vCenter Server's credential has not been added, click **Create** to add it to MgC by referring to [Adding Resource Credentials](#). When adding the credential, enter the username and password for logging in to the vCenter Server.

Step 6 Click **Confirm**. An intranet-based discovery task is created, and MgC starts collecting details about source servers.

On the **Application Discovery** page, click **View** next to **Total tasks** to go to the task list and view the task status.

Step 7 Wait until the task status changes to **Succeeded**, and perform a deeper discovery. Servers discovered on an intranet have an Edge device associated. You just need to associated credentials with these servers before you can perform a deeper discovery.

1. On the **Application Discovery** page, click the **Resources** tab and click the number in the **Server** row.
2. Locate a server and click **Associate** in the **Credential** column.
3. Select the server credential. If the credential has not been added to MgC, go to the Edge console and **add the server credential** to the Edge device and synchronize it to MgC.
4. Click **OK**. MgC checks the credential association status. When the collection status is **Ready**, click **Discover** in the **Status** column to perform a deeper discovery. You can click **Rediscover** in the **Status** column to perform a second deeper discovery if needed.

----End

4.4 Manually Adding Resources

You can only add servers to MgC manually. To perform a deeper discovery on these added resources, you need to install Edge in the source environment.

Prerequisites

- You have **installed Edge** in the source intranet environment and have connected the Edge device with MgC.
- You have **added source server credentials** to the Edge device.

Adding a Server

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

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

Step 3 Click the **Resources** tab, click **Server** in the **Category** column or the number in the **Total Resources** column.

Step 4 Click **Add**.

Step 5 In the displayed dialog box, configure parameters listed in **Table 4-11** and click **Confirm**. The system automatically checks the credential status and starts collecting resource details.

Table 4-11 Parameters for adding a server

Parameter	Description
Name	Enter a server name.
Edge Device	Select the Edge device installed in the source environment.

Parameter	Description
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. <ul style="list-style-type: none">• 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 another port if needed.
Credential	Select the server credential. If the credential has not been added to MgC, go to the Edge console and add the server credential to the Edge device and synchronize it to MgC.

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

----End

4.5 Collecting Server Performance Data

MgC can collect server performance data, including the CPU usage, memory usage, disk IOPS, inbound and outbound traffic, inbound and outbound packets, and the number of network connections. The collected performance data will be used by MgC to recommend rightsized servers.

Precautions

- After a collection starts, performance data is collected every 5 minutes by default.
- The collection duration should be at least 1 hour. If the collection duration is too short, the maximum and average values in 7- and 30-day history cannot be calculated.
- A performance collection runs for seven days by default and stops after the period ends. You can stop or restart the collection at any time. After the collection is restarted, the collection period is recalculated.
- Collected performance data will be retained for 180 days and automatically deleted after that.
- It is recommended that Edge be installed on an independent server to ensure collection stability and efficiency.
- Edge can collect performance data from up to 1,000 Linux servers at the same time. If there are 1,000 or more Linux servers to be collected, the server where

Edge is installed must have at least 8 CPUs and 16 GB of memory with at least 8 GB available.

- Edge can collect performance data from up to 500 Windows servers at the same time. If there are 500 or more Windows servers to be collected, the server where Edge is installed must have at least 16 CPUs and 32 GB of memory with at least 8 GB available.

Prerequisites

- You have completed a discovery task over the Internet or intranet, or you have manually added servers to MgC.
- You have **installed Edge** in the source intranet environment and have connected the Edge device with MgC.
- You have **added source server credentials** to Edge.

Procedure

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

Step 2 In the navigation pane on the left, choose **Research > Application Discovery**. Select a **migration project**.

Step 3 Click the **Resources** tab and click the number in the **Server** row.

Step 4 Configure an Edge device and credentials for the server whose performance data needs to be collected. If the **Start** button in the **Performance Collection** column is available, the configuration is complete. In this case, skip this step and go to **Step 7**.

Move the cursor to the **Start** button in the **Performance Collection** column. In the dialog box that is displayed, click **Configure**. The configuration window is displayed.

Step 5 Configure the parameters listed in **Table 4-12**.

Table 4-12 Parameters for configuring a migration pre-check

Parameter	Configuration
Type	Set this parameter based on the source server OS type.
Edge Device	Select the Edge device in the source environment.
IP Address	Select the IP address used for accessing the source server. It can be a public or private IP address. If you need to use a proxy to access the server, enter the proxy IP address. After the migration pre-check passes, the IP address will be used for subsequent migration.

Parameter	Configuration
Port	Enter the port on the source server opened to the Edge device. <ul style="list-style-type: none">• 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 another port if needed.
Credential	Select the server credential. If the credential has not been added to MgC, go to the Edge console and add the server credential to the Edge device and synchronize it to MgC.

Step 6 Click **Confirm**. The system will verify the correctness of the configuration.

Step 7 After the configuration is verified, click **Start** in the **Performance Collection** column to start collecting server performance data. The collection status will change to **Collecting**.

After performance data collection is complete, you can perform the following operations:

- **Viewing Collected Data**
 - a. Click a server name to go to its details page. In the **Performance Info** area, you can view the collected performance data. The maximum values in 7 days and 30 days are hourly aggregated data. To view these maximum values, ensure the collection duration exceeds 1 hour.
 - b. Click **View** in the **Operation** column to view the details and line chart about the performance metric in the collection period.
- **Stopping Collection**

Click **Stop** to pause performance data collection.

----End

4.6 Grouping Resources as Applications

You can manage resources by group using applications to facilitate subsequent resource assessment and migration.

Step 1 Log in to the [MgC](#) console.

Step 2 In the navigation pane on the left, choose **Research > Application Discovery**. Select a [migration project](#) in the upper left corner of the page.

Step 3 Click the **Resources** tab and 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** in the upper left corner of the page.

Step 5 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 the business scenario, environment, and region, and click **OK**.

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

----**End**

5 Migration Solution Design

5.1 Associating Source Servers with Target Servers

You can associate source servers with existing servers on Huawei Cloud. Then your workloads can be migrated to these Huawei Cloud servers.

For source servers with target servers bound, there is no need to [assess](#) them before you create workflows to execute migrations.

Prerequisites

You have finished resource discovery by referring to [Discovering Resources – Simple Project](#).

Precautions

A target server must meet the following requirements:

- The target server must be stopped.
- During the migration, disks on the target server are formatted and re-partitioned based on the source disk settings for receiving data migrated from the source server.
- To migrate over the Internet, the target server must be able to access the Internet.
- The target server must be in the same region as the [application](#) to which the source server is added.

Procedure

Step 1 Log in to the [MgC](#) console.

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

Step 3 Click **View Resources** in the **Target Configuration** card.

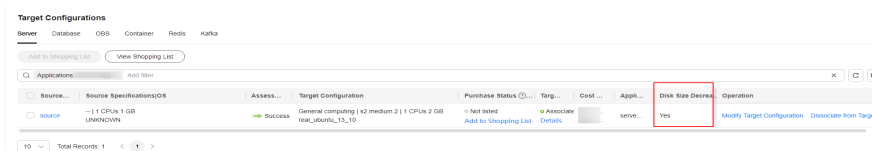
Step 4 On the displayed **Servers** tab page, locate a source server and click **Associate** in the **Target Association** column.

- Step 5** In the displayed dialog box, select the region of the **application** and select a project. You can reduce the disk capacity of the target server based on the source server disk information.

NOTICE

- 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.

- Step 6** Click **OK**. 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. The system will automatically check whether the disk capacity of the associated target server is reduced compared with the source server. If it is, **Yes** will be displayed in the **Disk Size Decreased** column. If it is not, **No** will be displayed.



----End

Dissociating a Source Server from the Target Server

- Step 1** On the **Servers** tab page, locate the source server and click **Dissociate from Target** in the **Operation** column.
- Step 2** In the displayed dialog box, click **Yes**. Please note that this operation cannot be undone.

----End

5.2 Getting Target Recommendations

This function assesses the specifications, performance, and environments of source resources and recommends Huawei Cloud resources that can meet your cost, availability, performance, security, and compliance requirements.

Currently, the following types of resources can be assessed: server, database, object storage, container, and middleware.

NOTE

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

Prerequisites

You have **discovered resources**, and **grouped the resources as applications**.

Procedure

Step 1 Log 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 numbers of resources that can be migrated and that have got target configurations as well as the list of applications in the current project.

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

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

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

Step 6 Configure the assessment policy based on **Table 5-1**.

Table 5-1 Parameters for configuring an assessment policy

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.
Sizing Criterion	<ul style="list-style-type: none">• Source specifications-based MgC recommends the most appropriate Huawei Cloud resources based on source resource specifications.• Business scenario-based MgC recommends appropriate Huawei Cloud resources based on the business scenarios 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.
Preference	<ul style="list-style-type: none">• Performance-first MgC recommends target resources based on your performance requirements.• Price-first MgC recommends target resources based on your cost requirements.

Parameter	Description
(Optional) Advanced Options	<p>Configure preferences for target servers. The servers that match your preferences are recommended first.</p> <ul style="list-style-type: none"> • ECS Types Select the expected ECS types. • System Disk Select the expected system disk type. • Data Disk Select the expected data disk type. • Match With Select a policy, which the system will follow during server recommendation. <ul style="list-style-type: none"> – If you select Source specifications, the system recommends target servers with the same or as close CPU and memory configurations as possible to the source servers. – If you select Source performance, you need to complete collecting performance data of source servers first, and then set assessment parameters. The system will then recommend target servers with your desired CPU and memory configurations. <p>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.</p> <p>For the container assessment, configure parameters such as Cluster Type, Cluster Version, and Container Network Model for getting recommendations on container resources.</p>

Step 7 Click **Create Assessment**. The assessment task is created. 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 8 (Optional) Perform the following operations:

- **Modify recommended target configurations**: You can modify recommended specifications of target servers and their disks.
- **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.

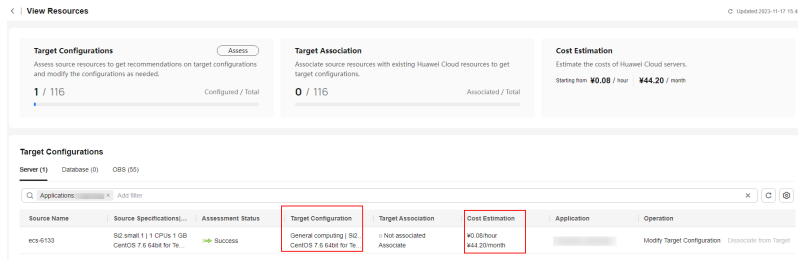
----End

Viewing the Assessment Results

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

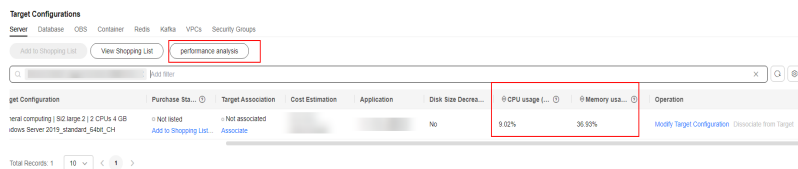
In the **Target Configurations** area, you can view the specifications of Huawei Cloud resources recommended based on the source resource specifications and

your selected preferences. It also gives you the ability to estimate what it will cost to run your services on Huawei Cloud.



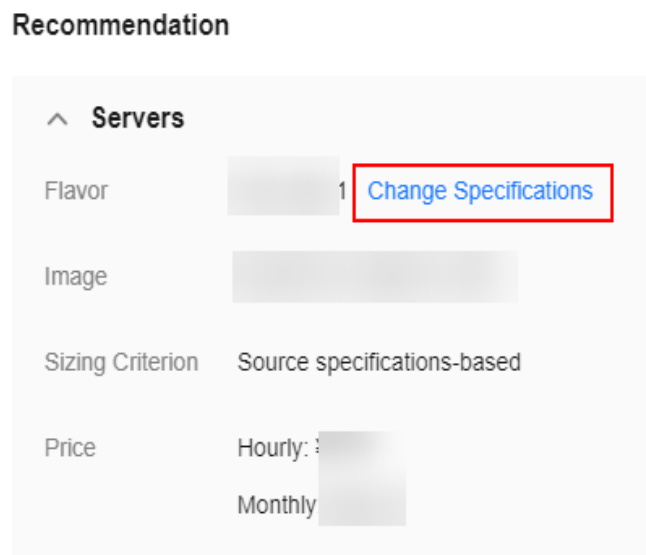
Viewing Server Performance Data

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



Modifying Recommended Target Configurations

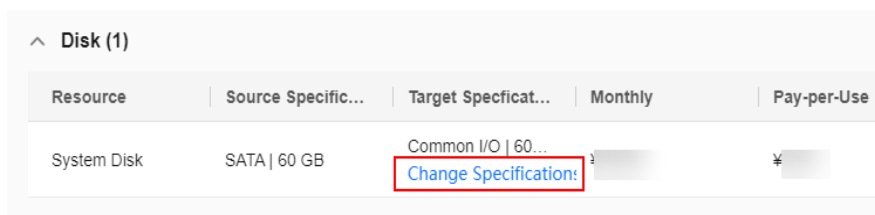
- Step 1** In the **Target Configurations** area, locate the server that you want to modify the recommended target configurations for and click **Modify Target Configuration** in the **Operation** column.
- Step 2** Modify the specifications and image for the target server.



- Step 3** In the disk area, locate a disk and click **Modify** in the **Target Specifications** column. You can modify the disk type and capacity. Only Linux disk sizes can be decreased. If you decrease a disk size, the system will set **Disk Size Decreased** 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.
- 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.



Resource	Source Specific...	Target Specificat...	Monthly	Pay-per-Use
System Disk	SATA 60 GB	Common I/O 60... Change Specification!		¥

----End

5.3 Purchasing Resources

After the specifications of target resources are configured, you can directly purchase these target resources in batches using a shopping list on MgC. Currently, only servers can be purchased using a shopping list. A shopping list makes it easier to use the repurchase migration strategy by allowing you to buy wanted target resources in batches. If you want to use the rehost strategy, you can create server migration workflows which automate the entire purchase process. Target servers purchased using a shopping list will be associated with the paired source servers automatically, and you can migrate the source servers using migration workflows as a part of your rehost strategy.

Prerequisites

Target configurations have been acquired for source resources. For details, see [Getting Target Configurations](#).

Procedure

- Step 1** Log in to the [MgC](#) console.
- Step 2** In the navigation pane on the left, choose **Design > Migration Solutions**.
- Step 3** Click **View Resources** in the **Target Configuration** card.
- Step 4** On the **Server** tab page in the **Target Configurations** area, locate a server whose **Assessment Status** is **Successful**, and click **Add to Shopping List** in the **Purchase Status** column.
- Step 5** Click **View** in the **Shopping List** card on the top of the page.
- Step 6** In the **Process Flow** area, click **View Templates**. In the **My Templates** window that is displayed on the right, click **Create Template**.

- Step 7** In the **Basic Info** area, select a template type (only server is supported currently) and specify a template name. In the **Configuration Info** area, set template parameters based on [Table 5-2](#).

Table 5-2 Parameters for configuring a shopping template

Parameter	Configuration
Region	Select the region where you want to deploy target servers.
Project	Select a region in the target region.
AZ	This parameter is set to Random by default. You can also select another AZ.
VPC	Select a VPC in the target region.
Subnet	Select a VPC subnet. The subnet CIDR block must be within the selected VPC CIDR block.
Security Group	Select a security group that meet the following requirements: <ul style="list-style-type: none">• To migrate Windows servers to this security group, the security group must be configured to allow access on ports 8899, 8900, and 22.• To migrate Linux servers to this security group, the security group must be configured to allow access on port 22.
Enterprise Project	Select a commercial enterprise project that you want add purchased target servers to. The default enterprise project is default . An enterprise project makes it easy to manage projects and group cloud resources and users. For details about creating and managing enterprise projects, see the Enterprise Management User Guide .

- Step 8** Click **Save**. You can view the created template in the template list.
- Step 9** Return to the shopping list page, and click **Attach Shopping Template** in the **Shopping Template** column. In the displayed dialog box, select the created template from the drop-down list and click **Confirm**.
- Step 10** Click **Buy** in the **Operation** column. Wait until the purchase status is **Purchased**, and view the ID of the purchased resource.

----End

5.4 Creating a Migration Plan

You can configure migration plans using templates designed for different resources, create migration workflows using the plans, and view the migration settings of resources by application.

The following migration plan template is provided:

Batch Object Storage Migration: This template can be used to migrate multiple object storage buckets in a batch. If only one object storage bucket needs to be migrated, [create an object storage migration workflow](#).

Prerequisites

- Object storage resources have been discovered over the Internet.
- (Optional) A deep collection has been performed for the resources to be migrated.

Precautions

- A migration plan can be used to migration buckets from the same source platform to a target region.
- A source bucket can be included in multiple migration plans.
- In a migration plan, a bucket can have one target prefix but multiple source prefixes.

Procedure

- Step 1** Log in to the [MgC](#) console. In the navigation pane, choose **Design > Migration Plans**.
- Step 2** 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 Configuration** area, set parameters listed in [Table 5-3](#).

Table 5-3 Basic parameters

Parameter	Configuration
Plan Name	Enter a name.
Description (Optional)	Enter a description.
Source Platform	Select the cloud platform where the source resources are located.
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 and click **Confirm**. Click **Modify** in the **Operation** column to configure the migration method for each bucket. For details about migration methods, see [Table 5-4](#).

 **CAUTION**

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

Table 5-4 Migration methods

Migration Method	Description
Full migration	Migrates all data in the source bucket or specified paths.
List migration	Migrates objects recorded in the list files. The list files must be stored in the target bucket.
Prefix migration	Migrates objects matched with the specified prefixes.

Step 7 In the list of buckets to be migrated, click **Modify** in the **Operation** column.

Step 8 Select the source credentials. It is best to enter the number of objects and the total object size. Then click **Confirm**.

- If the migration method configured for the bucket is **List migration**, in the **List Path** box, enter the directory that stores the lists of objects to be migrated. The directory must end with a slash (/).
- If the migration method configured for the bucket is **Prefix migration**, add the names or prefixes of objects to be migrated. Note that you need to click **Save** each time you add an object name or prefix.

 **NOTE**

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*.

Step 9 After you configure the migration settings for all buckets to be migrated, click **Next**.

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

Step 11 After you configure the target configuration for all source buckets, click **Next**. You can assess how large of a migration cluster is required for the migration and then create a migration cluster with the recommended specifications. Alternatively, you can skip this step and use an existing migration cluster. For details about how to create a cluster, see [Creating a Migration Cluster](#).

Step 12 Click **Next** to select an existing migration cluster. All resources in this plan will be migrated using this cluster.

Step 13 Click **Select Cluster**. The **Select Cluster** dialog box is displayed on the right.

Step 14 In the cluster list, select the cluster you want to use and click **Confirm**. If you want to modify an existing cluster to meet your requirements, see [Managing a Migration Cluster](#).

Step 15 Click **OK**. The migration plan is created. In the migration plan list, you should view the created plan.

- If you need to modify the plan settings, click **Design** in the **Operation** column.
- After design progress 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

6 Migration Clusters

6.1 Creating a Migration Cluster

After you create a migration cluster, you can manage the migration and list nodes in the cluster, such as installing or upgrading migration plug-ins on the nodes.

You pay for migration clusters and additional resources used by these clusters. For details, see [Billing](#).

Procedure

- Step 1** Log in to the [MgC](#) console. In the left navigation pane, choose **Deploy > Migration Clusters**.
- Step 2** Click **Create Cluster** in the upper right corner of the page.
- Step 3** Configure the parameters listed in [Table 6-1](#).

Table 6-1 Parameters for creating a cluster

Area	Parameter	Configuration	Constraints
Basic Settings	Cluster Name	Enter a custom name.	Cluster names in the same account must be unique.
	Region	Select the region to provision the cluster.	-
	Cluster Type	Select a cluster application scenario.	Currently, only storage migration is supported.

Area	Parameter	Configuration	Constraints
Node Settings	Master Node	Select the specifications of the master node which 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.
	Migration Node	Migration nodes are used for executing migration and verification tasks. The recommended specifications are 8 vCPUs and 16 GB of memory.	<ul style="list-style-type: none"> • The node specifications cannot be modified after the cluster is created. • The number of nodes must meet the following requirements: <ul style="list-style-type: none"> - 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 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	<ul style="list-style-type: none"> ● Public: 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. ● Private: Enter an IP address of such as Nginx or gateway that is allowed to forward or send requests over the private line. 	-
-	Traffic Limiting	<p>Allocate the maximum bandwidth to be used by the workflow during a specified period.</p> <ul style="list-style-type: none"> ● 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. <p>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.</p>	<ul style="list-style-type: none"> ● A maximum of five traffic limiting rules can be added. ● The time is the local standard time of the region you are migrating to.

Area	Parameter	Configuration	Constraints
	Log Collection	<ul style="list-style-type: none">• If this option is enabled, logs generated during storage migrations are collected for locating problems if any.• If this option is disabled, logs generated during storage migrations are not collected.	-

Step 4 Click **Confirm**. You can view the cluster status in the migration cluster list. For details about cluster statuses, see [Cluster Statuses](#).

Step 5 After the migration cluster is created, perform the following operations:

- If the cluster status is Healthy or Subhealthy, click **Create Workflow** in the **Operation** column .
- Click **Manage** in the **Operation** column to add or delete nodes and traffic control rules. For details, see [Managing a Migration Cluster](#).

----End

6.2 Managing a Migration Cluster

You can configure traffic limiting rules and add or remove nodes in the cluster as required.

Prerequisites

You have created a cluster by referring to [Creating a Migration Cluster](#).

Adding a Traffic Limiting Rule

Step 1 Log in to the [MgC](#) console. In the left navigation pane, choose **Deploy > Migration Clusters**.

Step 2 In the cluster list, click **Manage** in the **Operation** column.

Step 3 In the **Traffic Limiting** area, click **Add** to add a rule.

Step 4 Configure the start time, end time, and bandwidth limit.

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.

NOTICE

- The time is the local standard time of the region you are migrating to.
- A maximum of five rules can be added.

Step 5 Click **Confirm**.

----End

Adding Nodes

The procedure for adding a migration node is the same as that for adding a list node.

Step 1 Log in to the **MgC** console. In the left navigation pane, choose **Deploy > Migration Clusters**.

Step 2 In the cluster list, click **Manage** in the **Operation** column.

Step 3 In the node information area, choose **Add > Migration Node**.

Step 4 Enter the number of nodes to be added. The following requirements must be met:

- Number of migration nodes + Number of list nodes + 1 \leq 100
- Number of migration nodes + Number of list nodes + 1 \leq Number of unused IP addresses in the subnet

Step 5 Click **Confirm**. After the nodes are added, MgC starts to install the migration plug-in on these nodes, and you can view the added nodes in the node list.

----End

6.3 Billing

You are billed at standards rates for migration clusters and additional resources used during migrations.

- Master, migration, and list nodes in migration clusters are all ECSs, and you pay for these ECSs. For details, see [ECS Pay-per-Use Billing](#) or [ECS Price Calculator](#).
- If you migrate over the Internet, you need to pay for NAT gateways used by migration clusters. For details, see [NAT Gateway Billing](#) or [NAT Gateway Price Calculator](#).
- If you choose to enable log collection, you need to pay Log Tank Service (LTS) for resources you consume. For details, see [LTS Billing Description](#) or [LTS Price Calculator](#).

6.4 Cluster Statuses

For details about cluster statuses, see [Table 6-2](#).

Table 6-2 Cluster statuses

Status	Description
Creating	Cluster resources are being created.
Creation failed	Cluster resources fail to be created.
Connecting	The master node is waiting for going online, and other nodes are waiting for creation.
Healthy	All nodes are online.
Subhealthy	At least one migration node and one list node are online.
Unavailable	All migration nodes or all list nodes are offline.
Offline	The master node is offline. The cause may be that the network is interrupted or the ECS is deleted. Check the VPCEP service and ECS resources.
Upgrading	Plugins are being upgraded in the cluster.
Upgrade failed	Plugins failed to be upgraded in the cluster.
Discarding	The cluster is being discarded because no tasks have run in the cluster within 30 days.
Discard failed	The cluster failed to be discarded.
Deleting	The cluster is being deleted.
Deletion failed	The cluster failed to be deleted.
Discarded	The cluster is discarded since its VPCEP resources are deleted.
Pending creation	Cluster resources are waiting for creation.
Installing	Plugins are being installed on the master node.
Installation failed	Plugins failed to be installed on the master node.
Pending installation	The master node is waiting for plugin installation.
Pending upgrade	The cluster is waiting for plugin upgrade.
Pending deletion	The cluster is waiting for deletion.

7 Migration Workflow

7.1 Workflow Quotas

To ensure smooth migrations, MgC has the following limits on migration workflows.

- A maximum of 50 migration workflows can be created per day in a project.
- A maximum of 500 resources can be currently migrated in workflows in a project.
- A maximum of 100 resources can be included in a workflow.

7.2 Creating a Server Migration Workflow

This section describes how to create a server migration workflow using the standard template.

Prerequisites

- You have discovered servers by referring to [Discovering Resources – Simple Project](#).
- Servers to be migrated have been added to an application, and the application servers have been assessed. For details, see [Grouping Resources as Applications](#) and [Getting Target Recommendations](#). After the assessment is complete, you can purchase recommended target servers in batches. For details, see [Purchasing Resources](#). Servers with targets associated do not need to be assessed.

Procedure

- Step 1** Log 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 In the **Server Migration** card, click **Preview Steps** to view the steps predefined in the template and the detailed description of each step. If the type of a step is **Automated**, the step is automatically performed by MgC. If the type of a step is **Manual**, you need to perform the step manually. Click **Next: Configure Workflow** in the lower right corner.

Step 5 Configure the workflow parameters based on [Table 7-1](#).

Table 7-1 Parameters for configuring a server migration workflow

Area	Parameter	Description
Workflow Details	Name	Enter a name.
	Description	Enter a description
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 same VPC in advance to ensure that the source environment can access the target environment through the private network. <ul style="list-style-type: none">• If the source environment cannot access the Internet, you need to enter the private IP address of the source proxy server and the proxy 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.

Area	Parameter	Description
	VPC	<ul style="list-style-type: none"> • 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, you are advised to create a VPC and a subnet that both belong to network range 10.0.0.0/8.
	Subnet	The subnet has to be in the same network segment as the VPC.
	Security Group	<ul style="list-style-type: none"> • If there are Windows source servers, the security group must be configured to allow access on ports 8899, 8900, and 22. • If there are Linux source servers, the security group must be configured to allow access on port 22. <p>CAUTION</p> <ul style="list-style-type: none"> - 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.
Advanced Settings	Start Target After Migration	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • If you select No, the migration traffic is not limited. • If you select Yes, you can configure a bandwidth limit based on the source bandwidth and service requirements. <p>CAUTION</p> <p>Consider the migration scale to set an appropriate bandwidth limit. If the bandwidth allocated to the workflow is too small, migration tasks in the workflow may preempt the limited bandwidth resource, and some servers may fail to be migrated.</p>

Area	Parameter	Description
	Install rsync on Source	<ul style="list-style-type: none"> If you select No, the rsync component will not be installed on the source servers. If you select Yes, the rsync component will be automatically installed on the source servers. <p>CAUTION Linux migrations depend on rsync. If rsync is not installed on a source server, the server will fail to be migrated.</p>
	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 a stage or step](#) to the workflow, click **Cancel**. The workflow enters a **Waiting** state, and the migration is not started. 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.

- 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**, 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.

----End

7.3 Creating a Cross-AZ Migration Workflow

This section describes how to create a cross-AZ migration workflow using the standard template.

Prerequisites

- You have discovered servers by referring to [Discovering Resources – Simple Project](#).
- Servers to be migrated have been added to an application, and the application servers have been assessed or associated with existing target servers. For details, see [Grouping Resources as Applications](#), [Getting Target Recommendations](#), and [Associating Source Servers with Target Servers](#). Servers with targets associated do not need to be assessed.

Procedure

- Step 1** Log 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** In the **Cross-AZ Migration** card, click **Preview Steps** to view the steps predefined in the template and the detailed description of each step. If the type of a step is **Automated**, the step is automatically performed by MgC. If the type of a step is **Manual**, you need to perform the step manually. Click **Next: Configure Workflow** in the lower right corner.
- Step 5** Configure the workflow parameters listed in [Table 7-2](#).

Table 7-2 Parameters required for creating a cross-AZ migration workflow

Region	Parameter	Description
Workflow Details	Name	Enter a workflow name.
	Description	Describe the workflow.
Application	Application	Select the application which contains the servers to be migrated.
Migration Settings	Target Region	Select the region where the source AZ is located. The region configured in the application is populated by default. Currently, only the CN South-Guangzhou region of Huawei Cloud is supported.
	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.

Region	Parameter	Description
	Stop Target Server	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.
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.
	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. If a rollback is needed, it has to be performed manually.

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 a stage or step** to the workflow, click **Cancel**. The workflow enters a **Waiting** state, and the migration is not started. 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.

- 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.

----End

7.4 Creating a Storage Migration Workflow

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

The following regions are supported:

- CN North-Beijing4
- CN South-Guangzhou
- CN East-Shanghai1
- CN South-Guangzhou-InvitationOnly
- CN East-Qingdao

⚠ CAUTION

The size of a single object cannot exceed 5 TB. Otherwise, the migration may fail.

Prerequisites

- You have created an [OBS bucket](#) or [SFS file system](#) on Huawei Cloud.
- You have [created a migration cluster](#).

Procedure

- Step 1** Log 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** In the **Storage Migration** card, click **Preview Steps** to view the stages and steps predefined in the template and the detailed description of each stage and step. Steps of the **Automated** type will be automatically performed by MgC. Click **Configure Workflow** in the lower right corner.
- Step 5** Set workflow basics based on [Table 7-3](#).

Table 7-3 Basic parameters

Parameter	Description
Name	Enter a workflow name.
Region	Select a region where you want to migrate to.
Description	Enter a description.
Cluster	Select a migration cluster. The cluster must contain migration nodes and execution nodes. If no cluster is available, create a cluster .

- Step 6** Configure the migration source and target based on [Table 7-4](#) and [Table 7-5](#).

Table 7-4 Parameters for configuring a migration source


Parameter	Description	Remarks
Location Type	<p>The supported migration sources include:</p> <ul style="list-style-type: none"> ● 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_SMB ● NAS_NFS_V3_MOUNT ● NAS_NFS_V3_PROTOCOL ● HTTP/HTTPS data source 	-
AK	Enter the AK of the source cloud account.	These parameters are available when cloud storage is selected for Location Type .
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.	
Type	Set this parameter based on the source bucket type. You can view the bucket type in the basic information .	This parameter is available when Huawei Cloud OBS is selected for Location Type .
APPID	<p>Enter the APPID of your Tencent Cloud account.</p> <p>NOTE You can view the APPID on the account information page of the Tencent Cloud console.</p>	This parameter is available when Tencent Cloud COS is selected for Location Type .

Parameter	Description	Remarks
List Path	<p>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.</p> <p>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.</p> <p>Restrictions on list files are:</p> <ul style="list-style-type: none"> • 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. 	<p>These parameters are available when HTTP/HTTPS data source is selected for Location Type.</p>
File System Address	<p>Enter the mount address of the source file system. The format is <i>IP address:/</i> or <i>IP address:/xxx</i>, for example, 192.1.1.1:/0001.</p>	<p>These parameters are available when Location Type is set to NAS_SMB, NAS_NFS_V3_MOUNT, or NAS_NFS_V3_PROTOCOL.</p>
Path	<p>Enter the directory where files to be migrated are located. The format is <i>/Folder name</i>.</p>	

Parameter	Description	Remarks
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 source node. NOTE You only need to enter the content before .com. For example, if the domain is test.com, enter test.	

Table 7-5 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.	
Specify Prefix	Specify a prefix to rename objects migrated to the target bucket. For example, if you specify a prefix /D , source file /A/B/C.txt will be renamed /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 .	

Parameter	Description	Remarks
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.	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 <i>/Folder name</i> .	
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 task based on [Table 7-6](#).

Table 7-6 Parameters for configuring a migration task

Parameter	Value	Description
Task Type	Full migration	Migrates all data in the source bucket or specified paths.
	List migration	Migrates files recorded in the list files.
	Prefix migration	This option is only available for migrations 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. NOTE 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 their prefixes in the format of <i>Folder name/Prefix</i> .

Parameter	Value	Description
Concurrent Subtasks	-	Specify the maximum number of concurrent subtasks. The value cannot exceed the number of online migration nodes multiplied by 20. For example, if the number of online migration nodes is 2, the maximum number of subtasks can be 40 or any number below.
Overwrite Existing	Never	Files existing at the migration target are never overwritten.
	Always	Files existing at the migration target are always overwritten.
	If older or different size	Files existing at the migration target are overwritten if they are older than or have different sizes from files at the migration source.
Migrate Metadata	-	Determine whether to migrate metadata. <ul style="list-style-type: none">• If you select this option, object metadata will be migrated.• If you do not select this option, only the ContentType metadata will be migrated.
Clear Cluster	-	Determine whether to clear the migration cluster after the migration is complete. <ul style="list-style-type: none">• 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 7-7](#).

Table 7-7 Advanced options

Parameter	Description	Remarks
Enable KMS Encryption	<ul style="list-style-type: none"> If you do not select this option, objects are in the same encryption status before and after the migration. If you select this option, all migrated objects will be encrypted before they are stored in the target bucket. <p>NOTE</p> <ul style="list-style-type: none"> Using KMS to encrypt migrated data may decrease the migration speed by about 10%. This option is available only 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	<p>Only restored data can be migrated. You can select this option if the source cloud platform supports automatic restoration of archive data. Currently, the following cloud platforms can automatically restore archive objects: Huawei Cloud, Alibaba Cloud, Kingsoft Cloud, and Tencent Cloud.</p> <ul style="list-style-type: none"> If you do not select this option, the system directly 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. <p>NOTE</p> <p>The system will restore archive data before migrating it, and you will pay to the source cloud platform for the API requests and storage space generated accordingly.</p>	-
Filter Source Data	<p>Filter files to be migrated by applying filters. For details about the filters, see Source Data Filters.</p>	

Parameter	Description	Remarks
Obtain Data from CDN	<p>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 bind a custom domain name to 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.</p> <p>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.</p>	
Send SMN Notification	<p>Determine whether to use SMN to get notifications about migration results.</p> <ul style="list-style-type: none"> • 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	<p>Allocate the maximum bandwidth to be used by the workflow during a specified period.</p> <ul style="list-style-type: none"> • 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. <p>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 when the migration task is running from 08:00 to 12:00. The migration speed is not limited beyond this period.</p> <p>NOTE</p> <ul style="list-style-type: none"> - 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	Remarks
Schedule Migration	<p>Schedule the migration to run during a period.</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – 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 is 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, 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 the cursor to the progress bar. The migration details page is displayed on the right. You can view the task overview and progress details. You can perform the following operations:

Operation	Description
Modify the concurrent subtasks.	<ol style="list-style-type: none"> In the Progress area, click Modify under Expected Concurrent Subtasks to change the expected number of concurrent subtasks. The maximum number of concurrent subtasks cannot exceed the number of online migration nodes multiplied by 20. For example, if the number of online migration nodes is 2, the maximum number of concurrent subtasks is 40. Click Confirm.
Add traffic limiting rules.	<ol style="list-style-type: none"> In the Migration Speed area, click Add to add a rule to limit the bandwidth the migration can use in a specified period. <p>NOTICE</p> <ul style="list-style-type: none"> 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. Click Save.
Obtain the list of files that fail to be migrated, skipped or migrated.	In the File Statistics area, view the path for storing the list of files that fail to be migrated, skipped, or migrated. Click a path, and you will navigate to the OBS bucket where the list is stored. You can download the list from the bucket.
View 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 7-8 Filter options

Option	Description	Pattern 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.	<ul style="list-style-type: none"> • Exact match: You need to specify the absolute paths and use slashes (\) to escape special characters in the paths. 	<ul style="list-style-type: none"> • Except for {}, consecutive characters specified in pattern rules are not allowed, for example, ***, *?, **?, ?*, ?**, *{*, *}*, *}?, ?{*}, {*}, {,}, {*, , *}, and ,*.
Include Patterns	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Fuzzy match <ul style="list-style-type: none"> - 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 	<ul style="list-style-type: none"> • 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 {}.

Option	Description	Patten Rule	Constraint
		escaped by backslashes (\). In other cases, a backslash (\) means itself.	
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.		

7.5 Creating a Batch Object Storage Migration Workflow

This section describes how to create a workflow to efficiently migrate buckets in batches.

CAUTION

The size of a single object cannot exceed 5 TB. Otherwise, the migration may fail.

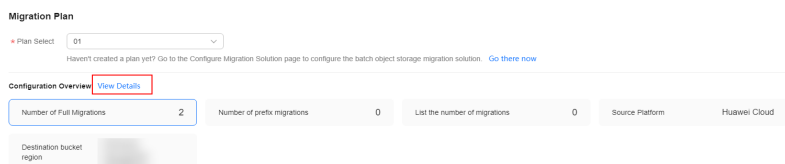
Prerequisites

You have [created a migration plan](#) that includes source buckets to be migrated together.

Procedure

- Step 1** Log 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** In the **Batch Object Storage Migration** card, click **Preview Steps** to view the stages and steps predefined in the template and the detailed description of each stage and step. Steps of the **Automated** type will be automatically performed by MgC. Click **Configure Workflow** in the lower right corner.
- Step 5** In the **Basic Information** area, enter a name and description for the workflow.

Step 6 In the **Migration Plan** area, select the created **object migration plan**. 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 selected in the migration plan is used 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 task based on **Table 7-9**.

Table 7-9 Parameters for configuring a migration task

Parameter	Value	Description
Concurrent Subtasks	-	Set the maximum number of concurrent subtasks. The value cannot exceed the number of online migration nodes multiplied by 20. For example, if there are 2 online migration nodes, the maximum number of subtasks can be 40 or any number below.
Overwrite Existing	Never	Files existing at the migration target are never overwritten.
	Always	Files existing at the migration target are always overwritten.
	If older or different size	Files existing at the migration target are overwritten if they are older than or have different sizes from files at the migration source.
Migrate Metadata	-	Decide whether to migrate metadata. <ul style="list-style-type: none"> If you select this option, object metadata will be migrated. If you do not select this option, only the ContentType metadata will be migrated.

Parameter	Value	Description
Clear Cluster	-	<p>Determine whether to clear the migration cluster after the migration is complete.</p> <ul style="list-style-type: none"> 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 9 (Optional) Configure advanced options based on [Table 7-10](#).

Table 7-10 Advanced options

Parameter	Description
Enable KMS Encryption	<ul style="list-style-type: none"> If you do not select this option, objects are in the same encryption status before and after the migration. If you select this option, all migrated objects will be encrypted before they are stored in the target bucket. <p>NOTE</p> <ul style="list-style-type: none"> 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	<p>Only restored data can be migrated. You can select this option if the source cloud platform supports automatic restoration of archive data. Currently, the following cloud platforms can automatically restore archive objects: Huawei Cloud, Alibaba Cloud, Kingsoft Cloud, and Tencent Cloud.</p> <ul style="list-style-type: none"> 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. <p>NOTE</p> <p>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.</p>

Parameter	Description
Filter Source Data	Filter files to be migrated by applying filters. For details about the filters, see Source Data Filters .
Download Data from CDN	<p>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 bind 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.</p> <p>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.</p>
Send SMN Notification	<p>Determine whether to use SMN to get notifications about migration results.</p> <ul style="list-style-type: none">• 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	<p>Allocate the maximum bandwidth to be used by the workflow during a specified period.</p> <ul style="list-style-type: none">• 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 when the migration task is running from 08:00 to 12:00. The migration speed is not limited beyond this period. <p>NOTE</p> <ul style="list-style-type: none">- 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 is 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 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, list nodes, or upgrade plug-ins for existing nodes as required.

----End

7.6 Adding a Stage or Step

You can customize a migration workflow to fit your requirements better by adding stages or steps to the workflow.

CAUTION

- You can only add a stage before or after an existing stage when the existing stage is in **Waiting** or **Paused** state. This is true for step additions.
 - If the previous stage is in **Running**, **Paused**, or **Complete** state, you can only add a stage after the existing stage. This is also true for step additions.
 - You cannot add steps after repeatable steps.
-

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 the 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 7-11](#), enter a step name and description, and click **Confirm**.

Table 7-11 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

8 Change History

Released On	What's New
2024-05-08	<ul style="list-style-type: none"> Added Performing a Deep Collection for Databases in "Discovering Resources over the Internet". Added Workflow Quotas
2024-4-17	Added Creating a Migration Plan Added Creating a Batch Object Storage Migration Workflow
2024-03-21	<ul style="list-style-type: none"> Added Agency Permissions. Added Importing Alibaba Cloud Servers.
2024-03-11	<ul style="list-style-type: none"> Added Azure to the supported sources of Internet-based discovery.
2024-02-20	Added Migration Clusters .
2024-01-31	<ul style="list-style-type: none"> Added Collecting Server Performance Data. Added performance-based recommendation to Getting Target Recommendations.
2023-12-30	Added Purchasing Resources .
2023-10-30	This issue is the first official release.