Migration Center

FAQS

Issue 27

Date 2025-02-14

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property 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 Cloud 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.

Contents

1 Product Consultation

1.1 How Do I Assign the Permissions Required for Using MgC to IAM Users?

You can assign the required permissions to an IAM user by referring to **Creating a User and Granting MgC Permissions** or **MgC Custom Policies**.

1.2 How Do I Prepare for Using MgC?

1. Sign up for a HUAWEI ID, enable Huawei Cloud services.
2. If you need to access MgC as an IAM user, **configure MgC permissions** for the IAM user.
3. Obtain an AK/SK pair for the account or IAM user you use to access MgC.

1.3 How Do I Fix the Error "Failed to access IAM. Check the current user's IAM permissions"?

Symptom

When you used the TCO analysis or resource recommendation function, the message "Failed to access IAM. Check the current user's IAM permissions" was displayed.

Possible Causes

The login account does not have the **IAM ReadOnly** permission.

Solution

Assign the **IAM ReadOnly** permission to your account. For details, see **Assigning Permissions to an IAM User**.

1.4 Why Can't I Sign the Privacy Statement and Use MgC?

Symptom

When you logged in the MgC console, a message was displayed indicating that you had not signed the privacy statement.

Possible Causes

Your account is restricted or in arrears.

Solution

Rectify account issues by referring to **In What Circumstances Will Huawei Cloud Services Be Restricted?** Return to the MgC console and try again.

1.5 How Does MgC Ensure Data Security?

MgC uses the following methods to ensure the security of collected data:

- **Encrypted data transmission**: Encryption technologies are used to ensure data security during transmission.
- **Local encrypted storage of credentials**: The credentials you provided for the MgC Agent are encrypted and stored locally and are not transmitted to the cloud over the Internet.
- **Local storage of collected data**: Data collected offline by the MgC Agent is stored locally. Before uploading the locally stored data to the cloud for analysis, you can manually review the data and confirm that there are no security risks.

1.6 Does Data Collection Affect My Source Services?

MgC uses an efficient data collection algorithm to ensure that data collection can be completed within a short period of time. This effectively prevents the collection process from occupying source resource for a long time and minimizes the impacts on source services.

2 Network Settings

2.1 What Can I Do If a Source Server Fails the Migration Readiness Check Because Its IP address or Port Is Unreachable?

Symptom

A Linux source server failed the migration readiness check, and a message is displayed indicating that its IP address or port was unreachable.

Possible Causes

The possible causes are:

- The source server is stopped.
- The IP address or port of the source server is abnormal.
- The access is blocked by the firewall or antivirus software on the source server.

You can review the error cause in the log file on the MgC Agent (formerly Edge). The error log file is stored in **C:\Edge\logs\edge-server\error.log**.

Solution

Step 1 Check whether the source server is stopped.

- If it is, start the source server and try again.
- If it is not, go to **step 2**.

Step 2 On the server where the MgC Agent is installed, open the CLI and use **ping** and **telnet** check whether the source server's public IP address and port (for example, 22) are accessible. The command formats are **ping** *{IP address of the source server}* and **telnet** *{IP address of the source server} {Port}*.

- If both the IP address and port are reachable, go to **step 3**.

- If the IP address or port is unreachable, check whether the security group of the source server allows access from the public IP address of the server with the MgC Agent installed over TCP on port 22 and over ICMP on any port. If the security group is correctly configured, perform the migration readiness check again.

Step 3 Check whether the access is blocked by the firewall or antivirus software on the source server. If it is, disable or adjust the blocking rule and try again.

----End

2.2 What Can I Do If a Source Server Fails the Migration Readiness Check Because the Username or Password Is Incorrect?

Symptom

A source server failed the migration readiness check, and the system displayed a message indicating that the username or password was incorrect.

Possible Causes

The username and password provided in the selected credential do not match the source server.

Solution

Step 1 Check the credential information.

Check whether the username and password in the credential are correct. Pay attention to letter cases and special characters.

Step 2 Verify the credential's validity.

Use the verified username and password to log in to the source server.

- If the login is successful, update the source server's credential information on the MgC Agent and perform the migration readiness check again.
- If the login fails, the username or password is incorrect. Proceed with the subsequent steps.

Step 3 Reset the password or contact the administrator of the source server.

- If you confirm that the username is correct but forget the password, reset the password. If the source server is a Huawei Cloud ECS, follow the instructions in **Resetting the Password for Logging In to an ECS on the Management Console**. If the source server is not a Huawei Cloud ECS, find an appropriate method to reset the password.
- If you are not sure whether the username is correct, contact the administrator of the source server to obtain the correct username and password.

Step 4 Update the source server's credential information on the MgC Agent, and perform the migration readiness check again.

----End

2.3 How Do I Fix the Error "Deliver Command to Edge Failed" When a Source Server Fails the Migration Readiness Check?

Symptom

A Windows source server failed the migration readiness check, and the message "Deliver command to Edge failed" was displayed.

Possible Causes

The possible causes are:

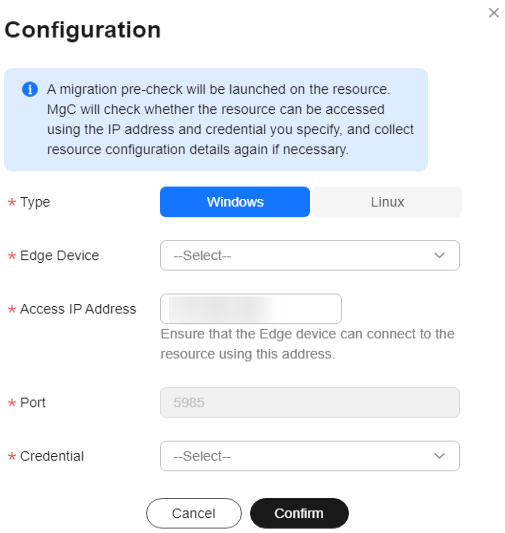
- The provided access IP address is incorrect.
- The source server is stopped.
- The IP address or port of the source server is abnormal.

You can review the error cause in the log file on the MgC Agent. The error log file is stored in **C:\Edge\logs\edge-server\error.log**.

Solution

Step 1 Check whether the access IP address configured for performing the migration readiness check is correct. Ensure that the MgC Agent can connect to the source server through the provided IP address and port.

- If the address is incorrect, correct it and try again.
- If the address is correct, go to **step 2**.



Step 2 Check whether the source server is stopped.

- If it is, start the source server and try again.
- If it is not, go to **step 3**.

Step 3 On the server where the MgC Agent is installed, open the CLI and run the **telnet** command to check whether the port (for example, port 5985) of the source server is accessible. The command format is **telnet** *{IP address of the source server} {Port}*.

- If the port is reachable, go to **step 4**.
- If the port is unreachable, check whether the security group of the source server allows access from the public IP address of the server with the MgC Agent installed over TCP on port 5985 and over ICMP on any port. If the security group is correctly configured, perform the migration readiness check again.

Step 4 Check whether the access is blocked by the firewall or antivirus software on the source server. If it is, disable or adjust the blocking rule and try again.

----End

2.4 What Can I Do If a Source Server Fails the Migration Readiness Check Due to an Unreachable Port, Incorrect Firewall Settings, or Insufficient Access Permissions?

Symptom

A source server failed the migration readiness check, and a message was displayed, indicating that the port was unreachable, the firewall settings were incorrect, or the access permissions were insufficient.

Possible Causes

The provided access port is incorrect.

Solution

Step 1 Check whether the port configured for performing the migration readiness check is correct. The default port is **5985** for Windows and **22** for Linux. You can use a different port as needed.

- If the port is incorrect, correct it and try again.
- If the port is correct, go to **step 2**.

Step 2 On the server where the MgC Agent is installed, open the CLI and run the **telnet** command to check whether the port of the source server is accessible. The command format is **telnet** *{IP address of the source server} {Port}*.

If the port is unreachable, check whether the security group of the source server allows access from the public IP address of the server with the MgC Agent

installed over TCP on port 5985 (for Windows) or port 22 (for Linux) and over ICMP on any port. If the security group is correctly configured, perform the migration readiness check again.

----End

2.5 What Can I Do If Deep Collection Fails on a Source Server Due to Disabled WinRM or an Unreachable IP Address or Port?

Symptom

Deep collection failed on a source server, and a message was displayed, indicating that WinRM was not enabled on the source server or the IP address or port was unreachable.

Possible Causes

The possible causes are:

- The IP address or port of the source server is abnormal.
- WinRM is not enabled on the Windows source server.

You can review the error cause in the log file on the MgC Agent (formerly Edge). The file is located at **C:\Edge\tools\plugins\collectors\rda-collector-server\logs\rda-collector-server\run.log**.

If the fault is not caused by the preceding two reasons, check whether the MgC Agent is being used by multiple users for data collection simultaneously. In such cases, WinRM on the MgC Agent server may disconnect from the source server.

Solution

- **Linux**

  On the server where the MgC Agent is installed, open the CLI and use **ping** and **telnet** check whether the source server's public IP address and port (22 by default) are accessible. The command formats are **ping** *{IP address of the source server}* and **telnet** *{IP address of the source server} {Port}*.

  If the IP address or port is unreachable, check whether the security group of the source server allows access from the public IP address of the server with the MgC Agent installed over TCP on port 22 and over ICMP on any port. If the security group is correctly configured, perform deep collection again.

- **Windows**

  a. Log in to the source server and enable WinRM. For details, see **How Do I Configure WinRM and Troubleshoot WinRM Connection Problems?** After WinRM is enabled, perform deep collection again. If the fault persists, go to step 2.

  b. On the server where the MgC Agent is installed, open the CLI and use **ping** and **telnet** check whether the source server's public IP address and

port (5985 by default) are accessible. The command formats are **ping** *{IP address of the source server}* and **telnet** *{IP address of the source server} {Port}*.

If the IP address or port is unreachable, check whether the security group of the source server allows access from the public IP address of the server with the MgC Agent installed over TCP on port 5985 and over ICMP on any port. If the security group is correctly configured, perform deep collection again.

3 Server Migration

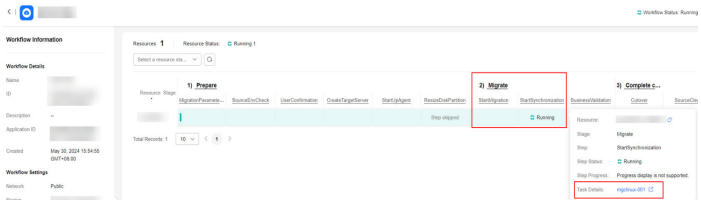
3.1 How Do I View the Migration Progress When the Migration Workflow Is in the Running State?

There are two ways you can view the migration progress:

- In the workflow list, click the workflow name. On the workflow details page, you can view the migration progress of each server in the workflow.

  When the migration of server reaches **StartMigration** or **StartSynchronization**, click the target server name to go to the task details page on the SMS console. **Figure 3-1** shows an example.

  Figure 3-1 Server migration workflow

- Go to the SMS console to view the migration progress of each server.

3.2 Why the Workflow Status Is Always "Running"?

In a migration workflow, the **StartMigration** and **StartSynchronization** steps take a long time, but other steps usually take less than 3 minutes. If your workflow has stalled for a long time, one possible cause is that the step execution results reported by the MgC Agent (formerly Edge) to MgC were lost.

Solutions

- Solution 1: Click the workflow name. On the **Servers** tab of the workflow details page, you can view the status of the workflow on each source server.
- Solution 2: Contact technical support to check whether the tasks have been properly submitted and received.

3.3 How Do I Fix the Error "Edge is not accessible" When a Step in the Migration Workflow Fails?

The MgC Agent cannot access the source servers. To resolve this problem, ensure that:

- The MgC Agent server can access port 5985 on Windows source servers.
- The MgC Agent server can access port 22 on Linux source servers.
- Any firewall or antivirus software has been stopped and WinRM has been enabled on Windows source servers. You can run **winrm quickconfig** to enable WinRM.

3.4 How Do I Fix the Error "Server Require to Bind Credential First..." When the Migration Workflow Fails on a Source Server?

Possible Causes

The source server's credential has not been added to the MgC Agent (formerly Edge).

Solution

Add the source server's credential to the MgC Agent, so the MgC Agent can collect the source server information. For details, see **Adding Credentials** and **Discovering Servers**.

3.5 How Do I Handle Resource Exceptions during a Batch Server Migration?

1. When a large number of servers are migrated, APIs are frequently called. Errors may be reported in some steps due to heavy API requests. You are advised to confirm the steps after the checkpoint in batches or try again.
2. When a large number of servers are migrated, the communication channel may be blocked, and the workflow status cannot be properly displayed.

3.6 What Are the Known Errors Related to Server Migration Workflows and How Can I Fix Them?

These error messages start with **SMS-Workflow**. You can find the solutions in **Known Errors and Solutions**.

3.7 What Can I Do If an Error Occurs During the Migration of a VMware Server?

Symptom

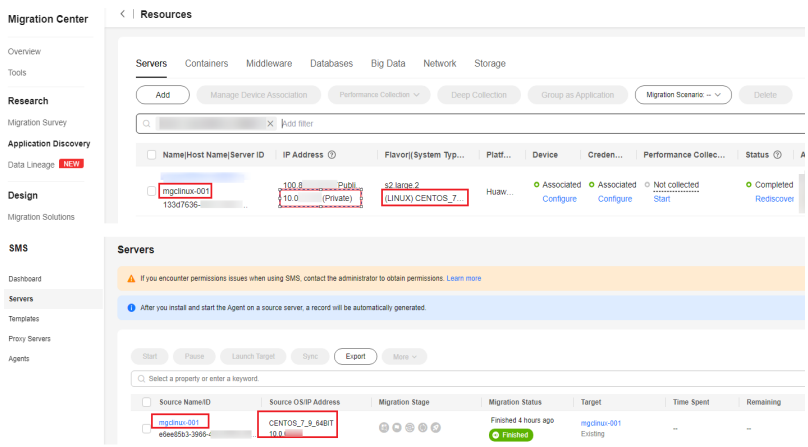
During the migration of VMware servers, an unknown error was reported during the source check in step 2.

Possible Causes

When the server was created, the preselected OS version was inconsistent with the OS version contained in the used image. For example, CentOS 6 is selected but CentOS 7 is actually used. There will be compatibility issues when the server is migrated, even though the server runs properly on VMware. You are advised to use the image with the same OS as the preselected OS when creating a server on VMware.

3.8 What Are the Information Mappings Between MgC and SMS?

The following figure shows the server information mapping between MgC and SMS.



The following table lists the mapping between the server lists on the MgC and SMS consoles.

Server List on MgC	Server List on SMS	Description
Hostname	Source Name	Hostname of a source server
IP Address	Source IP Address	IP address of a source server
Image	Source OS	OS of a source server

Server List on MgC	Server List on SMS	Description
-	Target	Name of the paired target server

Viewing a Server Migration Task Created by MgC on SMS

In a server migration workflow on MgC, after the **StartUpAgent** step is complete, a migration task is automatically created on SMS and the task is in the ready status, as shown in **Figure 3-2** and **Figure 3-3**.

Figure 3-2 Step for starting the migration Agent

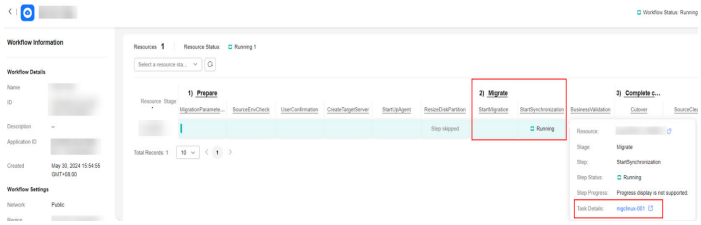
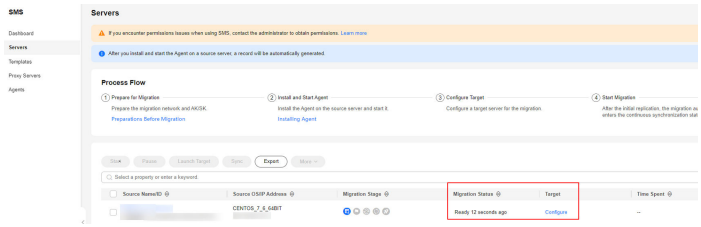


Figure 3-3 Server list on SMS



Viewing the Real-Time Migration Status

When a server migration workflow reaches the **StartMigration** or **StartSynchronization** step, you can click a server record, and in the displayed dialog box, click the task name after **Migration Task** to go to the SMS console, as shown in **Figure 3-4**. On the SMS console, you view the source server details, target server configuration, and migration status, as shown in **Figure 3-5**.

Figure 3-4 Server migration workflow

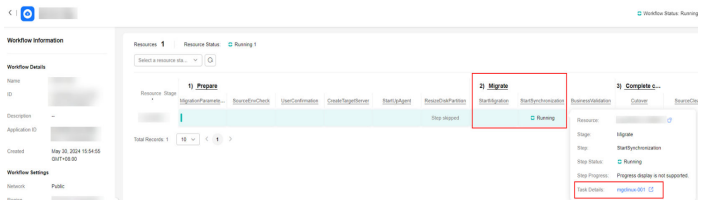
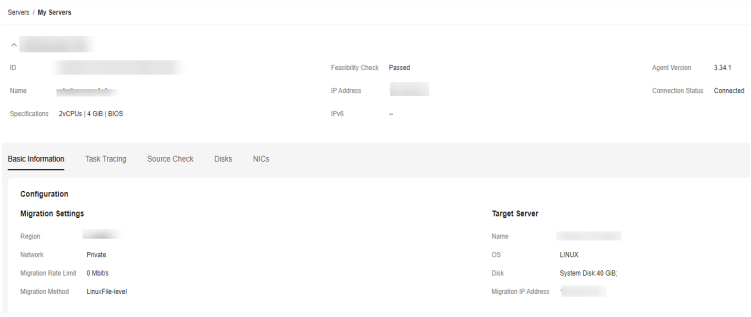


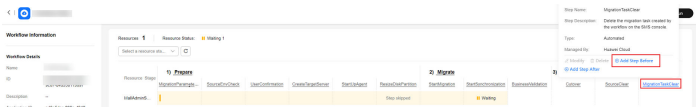
Figure 3-5 Details of a migration task on SMS



Retaining Migration Tasks on SMS

To retain the migration tasks created by MgC on SMS after a server migration workflow is complete, manually add a checkpoint before the step for clearing migration tasks in the workflow, as shown in **Figure 3-6**. For details about how to add checkpoints in a workflow and what are the precautions, see **Adding a Stage or Step**.

Figure 3-6 Adding a checkpoint



When the workflow reaches the checkpoint step for a server, do not conform it, as shown in **Figure 3-7**. In this case, the migration task on the SMS console will not be deleted and its status is **Completed**, as shown in **Figure 3-8**. If you confirm the step, the task will be deleted from the SMS console.

Figure 3-7 A checkpoint step

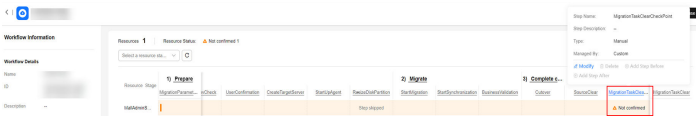
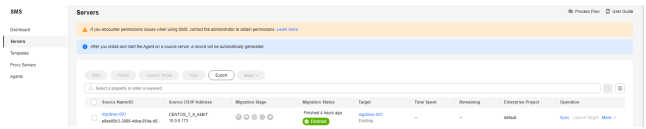


Figure 3-8 Migration completed



3.9 Why Is the Migration Progress Inconsistent Between MgC and SMS?

MgC and SMS have different methods to calculate migration progress. As a result, the migration progress of a source server may appear differently in MgC and SMS. In SMS, a migration task is divided into phases. In MgC, a migration workflow uses a simpler calculation method to estimate the progress.

SMS Migration Task Progress

The progress of an SMS migration task is divided into the following phases:

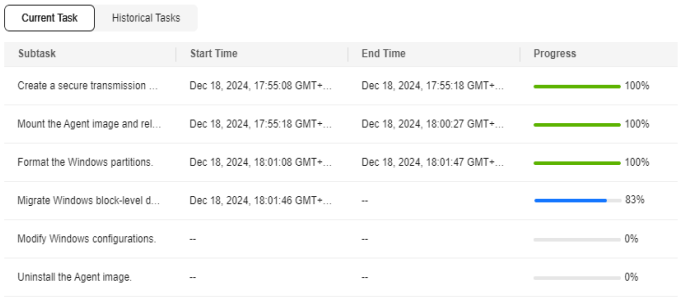
1. Task configuration: After the migration task is configured, the progress is 21%.
2. Data migration: The progress increases based on the percentage of migrated data and reaches 80% when the data migration is complete.
3. Finalization: After the configurations of the target server are modified and the disk containing the agent image is detached from it, the progress reaches 100%.

MgC Server Workflow Progress

For each source server included in an MgC migration workflow, a migration task is created in SMS. Each SMS migration task consists of several subtasks, and a subtask only starts after the previous one is 100% complete. For example, if the SMS migration task of a source server has six subtasks, the migration task can be considered complete when all six subtasks have reached 100% completion. In the MgC workflow, the migration progress of the source server is calculated as the sum of the completed subtasks' percentages divided by 600%.

Take the SMS migration task in the following figure as an example. The migration progress of the involved source server in MgC would be approximately 63% (380%/600%).

Figure 3-9 The subtask progress in SMS



3.10 What Do I Do If I Use a sudo User to Migrate a Source Server and the Server Fails the Source Environment Check?

Symptom

When a sudo user was used to migrate a source server, a message is displayed indicating that the server failed at the **SourceEnvCheck** step in the workflow.

Possible Causes

At the **SourceEnvCheck** step in the workflow, a script is uploaded to the source server. The user used for the migration only needs the permissions to read and execute the script. If the script already exists on the source servers and the sudo

user does not have sufficient permissions to modify or delete the old script, the new script cannot be uploaded. As a result, the check fails.

Solution

Step 1 Log in to the source server as the sudo user.

Step 2 Delete the **rda** folder in **/home/***Username***/**. In the preceding command, *Username* indicates the username used by the sudo user to log in to the system.

Step 3 Return to the MgC console and retry the workflow for the source server again.

----End

3.11 What Can I Do If the StartUpAgent Step Fails and the Error Message "System.OutOfMemoryException" Is Displayed?

Symptom

The migration workflow failed at the **StartUpAgent** step, and the error message "System.OutOfMemoryException" was displayed.

Possible Causes

The MgC Agent (formerly Edge) uses WinRM to connect to the source server for script transmission and execution. This problem occurs if there is not enough memory for executing the script.

Solution

Step 1 Check and modify the PowerShell memory configuration.

Run the following command in PowerShell on the source server to check the memory allocated for PowerShell:

```
Get-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB
```

- If the configured memory is too small, run the following command to increase the memory to 1024 MB and retry the migration task. If the fault persists, go to **step 2**.

  ```
  Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024
  ```

- If the configure memory is not less than 1024 MB, go to **step 2**.

Step 2 Handle the memory limit problem in OSs of old versions.

If the source server uses an earlier version of OS, for example, Windows Server 2008 or Windows Server 2012, the WinRM service may not apply the value defined by **MaxMemoryPerShellMB**. Instead, it uses the default value, which is typically 150 MB. In this case, the script may be interrupted due to insufficient memory. To handle this issue, perform the following operations:

1. Sign in to the **Huawei Cloud SMS console**. On the **Agents** page, download the Windows Agent (Python 2) installation package to the source server.

2. Install and run the Agent. Enter the AK/SK pair of your Huawei Cloud account and SMS domain name to start the Agent. For details, see **Installing the Agent on Windows**.
3. After the Agent is started, return to the MgC console and retry the migration task.

----End

3.12 How Do I Fix the Error "SMS-Workflow.0503: SMS migration task failed. SMS.xxxx?"

Symptom

In a server migration workflow, the step for executing full replication or incremental synchronization failed on a source server, and the error message "SMS-Workflow.0503: SMS migration task failed. SMS.xxxx" was displayed.

Possible Causes

During a migration, an SSH connection must be established between the source server and target server. If the SSH connection cannot be established, the migration will fail.

Solution

Step 1 Click the task name to go to the details page of the SMS task.

Step 2 Check the error cause and error code, and rectify the fault by referring to the following links:

- **SMS.380x SSH Connection Failures**
- **SMS.0303 Unable to Access Domain Name**

----End

3.13 What Do I Do If Some Disks Are Not Attached to the Target Server After the Migration Is Complete?

Symptom

After the migration was complete, some disks were not attached to the target server.

Possible Causes

During the migration, MgC collects the disk attachment information from the source server and configures disks for the target server accordingly. The system only migrates disks that are attached, used, and running migratable file systems to

the target server. These disks will be attached to the target server, while other disks will not.

Solution

Manually attach the disks to the target server by referring to **Attaching a Disk to an ECS**.

4 Storage Migration

4.1 What Are the Restrictions on Using MgC for Storage Migration?

Table 4-1 and Table 4-2 list the constraints on storage migration using MgC.

Table 4-1 General constraints on storage migration

Item	Constraint
Objects with multiple versions	By default, only the latest version of objects in source buckets is migrated.
Storage class of target buckets	The storage class of target buckets can only be Standard or Infrequent Access. You can change the storage class of target buckets after the migration is complete.
Migration object	• Object names cannot contain special characters. • A single object cannot be larger than 4.76837158203125 TB (500 MB × 10,000). Otherwise, the migration may fail.
Migration network	Migrations are supported over public networks, private networks, and private lines.

Item	Constraint
Symbolic links	• Symbolic links cannot be used for specifying migration paths which define the migration scope. If the migration path you specify is pointed to by a symbolic link, you need to: – Enter the actual path when specifying the migration path. – After the migration is complete, manually create a symbolic link to the path at the target. • For migration from NAS_SMB or migration from NAS_NFS to OBS, symbolic links cannot be migrated. • For migration from NAS_NFS to NAS_NFS, symbolic links can be migrated by enabling metadata migration. Otherwise, these files will be skipped during the migration. • For migration from Alibaba Cloud OSS to NAS_NFS, symbolic links can be migrated by enabling metadata migration. Otherwise, the symbolic links will lose their link functionality and become regular files after the migration. **NOTICE** If the objects that symbolic links point to are not completely migrated to the target, these symbolic link files may fail the verification. As a result, the task will be in a failed status. In this case, wait until the involved objects are completely migrated to the target, and try the task again.
Hard links	For migration from NAS_NFS to NAS_NFS, hard links can be migrated by enabling metadata migration. Otherwise, these files will be skipped during the migration.
Migration scope	You can migrate a single bucket or multiple buckets in batches.
Metadata migration	• Only Chinese characters, English characters, digits, and hyphens (-) can be migrated. Other characters cannot be migrated. – Chinese characters are URL encoded during the migration. **CAUTION** Chinese punctuation marks cannot be URL encoded during the migration. If metadata contains Chinese punctuation marks, the metadata and the corresponding object will fail to be migrated. – English characters, digits, and hyphens (-) are directly migrated without being encoded. • For heterogeneous migrations, metadata cannot be migrated.

Item	Constraint
Archived data	To migrate archived data from object storage, you must restore it first. You need to: • Ensure the restoration is complete before creating migration workflows. • Configure a validity period for restored data based on the total amount of data to be migrated. This helps prevent migration failures because restored data becomes archived again during the migration. • Pay your source cloud vendor for restoring archived data. To learn about the pricing details, contact your source cloud vendor.
Concurrent subtasks	You can define the number of concurrent subtasks based on the number of online migration nodes. There cannot be more than 10 concurrent subtasks for each online migration node. For example, if there are 2 online migration nodes, the maximum number of subtasks can be 20 or any number below.
Object list files	These files must be stored in the same region as the target bucket. • These files must be in .txt format, and their metadata Content-Type must be text/plain. The directory where these files are stored cannot contain any other files or folders except for .txt files. • 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 file 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.

Table 4-2 Constraints on file system migration

Scenario	Constraint
Migration source: SMB systems	• File systems where a single directory contains more than 5 million files cannot be migrated. • Resumable transfer is not supported. • Symbolic links cannot be migrated.
Migration source: NAS file systems	• The following types of files can be migrated: regular files, directories, symbolic link files, and hard link files. **CAUTION** If the file handle of a source file is occupied or the source file is deleted, the migration of the file will fail. • Special files such as character device files, block device files, sockets, and pipe files cannot be migrated. • The metadata of symbolic link files cannot be migrated.

4.2 What Are the Requirements for the Source and Target Environments?

The migration consumes a significant amount of QPS and bandwidth resources in the source and target environments. You are advised to perform a test before the migration to evaluate the QPS and bandwidth usage of the source and target environments during the migration. If the usage is too high, adjust the QPS and bandwidth limits at both ends to minimize the potential impact on existing services.

4.3 How Do I Choose the Right Specifications for a Migration Cluster?

When using MgC for storage migration, you are advised to use **c6.2xlarge.2** or **c7.2xlarge.2**. Both of the them provide 8 vCPUs and 16 GiB memory.

Specifications	Bandwidth	Used For
General computing-plus C6 | c6.2xlarge.2 | 8 vCPUs | 16 GiB	Assured bandwidth: 4.5 Gbit/s Maximum Bandwidth: 15 Gbit/s	Migration node, list node, and master node
General computing-plus C7 | c7.2xlarge.2 | 8 vCPUs | 16 GiB	Maximum Bandwidth: 15 Gbit/s	Migration node, list node, and master node

The recommended specifications can meet the needs of most migration scenarios, ensuring both speed and stability. Opting for lower specifications may slow down

the migration due to insufficient resources, which could impact efficiency and stability. It is best to choose the recommended or higher cluster specifications according to your requirements to maintain optimal performance.

4.4 What Affects the Migration Speed of Large Objects?

The migration speed of large objects is influenced by the following factors of the migration cluster:

- **Network bandwidth**: Insufficient bandwidth can slow on the migration speed.

  Suggestion: Increase the bandwidth or schedule the migration to run during off-peak hours.
- **Specifications**: Using a migration cluster with lower specifications than recommended (8 vCPUs and 16 GB memory) can hinder the migration speed.

  Suggestion: Upgrade the cluster specifications or add more nodes to enhance performance.
- **System performance management**: Other tasks consuming system resources (CPU and memory) can affect migration speed.

  Suggestion: Adjust task priorities to ensure sufficient resources for the migration, or perform the migration when the system load is low.

4.5 What Affects the Migration Speed of Small Objects?

The migration speed of small are influenced by the following factors:

- **CPU usage of the migration cluster**: Excessively high CPU usage of the cluster can slow the migration.

  Suggestion: Optimize the CPU resource allocation for the cluster, or add more migration nodes to distribute the load.
- **QPS limits of the source and target storage systems**: The QPS limits may affect the migration speed.

  Suggestion: Adjust the QPS limits based on the migration requirements.
- **Bandwidth usage of the migration cluster**: While bandwidth may not be a major factor, if the usage is near the upper limit, it can still impact migration speed.

  Suggestion: Monitor the bandwidth usage to ensure that sufficient bandwidth is available for migration. If the bandwidth is insufficient, increase the bandwidth size or perform the migration during low-usage times.

4.6 How Do I View Key Metrics that Affect the Migration Speed?

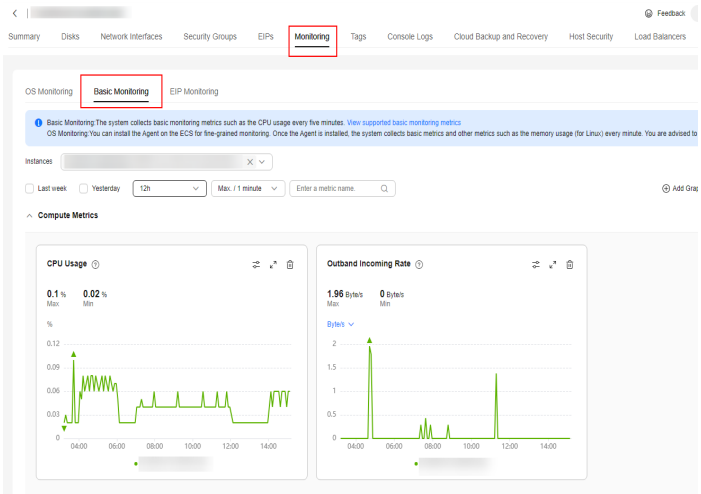
Migrating Cluster Metrics

The following table describes the key metrics of the migration cluster.

Metric	Description	Remarks
CPU usage	Used to monitor the CPU usage.	This metric is important for migration of small files. It is recommended that the CPU usage be close to but not greater than 90%.
Outband incoming and outgoing rates	Used to observe the changes in outband incoming and outgoing rates.	The metrics are important for migration of large files. The recommended rate is 2 Gbit/s to 3 Gbit/s.

To view the preceding metrics, perform the following steps:

1. On the ECS console, click the name of an ECS in the migration cluster.
2. Choose **Monitor** > **Basic Monitoring** to view the real-time CPU usage and traffic changes.

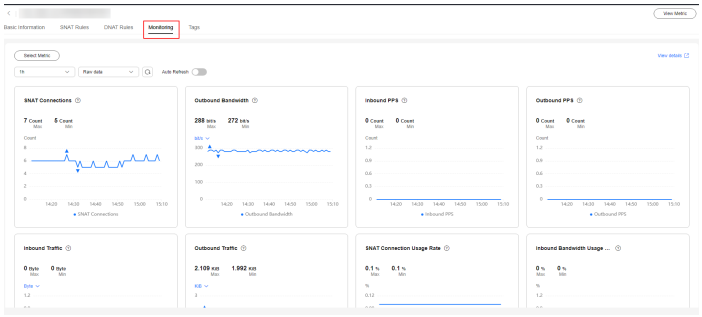


Network Metrics

The following table describes the key network metrics.

Scenario	Metric	Description	Remarks
Migration over the Internet using a NAT gateway	Incoming and outgoing traffic	Use to observe the incoming and outgoing traffic changes of the EIP used by the NAT gateway to ensure efficient data transmission and proper allocation of network resources.	It is recommended that the bandwidth usage be less than 90%. For example, if the total EIP bandwidth of the NAT gateway is 20 Gbit/s, it is recommended that the used bandwidth be less than or equal to 18 Gbit/s.
Migration over Cloud Connect, Direct Connect, or private lines	Inbound and outbound bandwidth	Used to observe the inbound and outbound bandwidth changes.	-

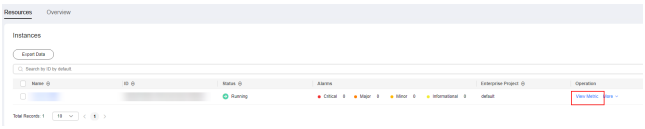
- To view the inbound and outbound bandwidths of a NAT gateway, perform the following steps:
  a. On the Huawei Cloud console, choose **Networking** > **Management & Governance** > **NAT Gateway**.
  b. On the displayed page, click the name of the public NAT gateway used for migration.
  c. Under **Monitoring**, view the inbound and outbound traffic changes of the NAT gateway.



- To view the inbound and outbound bandwidth of a private line, perform the following steps:
  a. Log in to the Huawei Cloud console and choose **Service List** > **Management & Governance** > **Cloud Eye**.
  b. In the navigation pane, choose **Cloud Service Monitoring**.

c. Click Cloud Connect or Direct Connect.

d. In the instance list, click **View Metric** in the **Operation** column. You can view the inbound and outbound bandwidth of the instance.

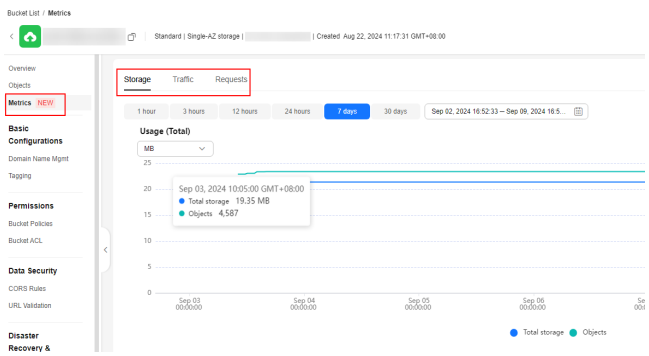


Metrics of Source and Target Storage Systems

The following table describes the key metrics of the source and target storage systems.

Vendor	Metric	Description	Remarks
Source	QPS and outbound traffic	Used to observe the QPS and outbound traffic of the source storage system to detect and handle potential performance bottlenecks in a timely manner.	If the QPS or outbound traffic is close to or exceeds 80% to 90% of the threshold provided in the official documentation, contact the source vendor to adjust the threshold.
Target	QPS and inbound traffic	Used to observe the QPS and outbound traffic of the target storage system to detect and handle potential performance bottlenecks in a timely manner.	If the QPS or outbound traffic is close to or exceeds 80% to 90% of the threshold provided in the official documentation, contact the target vendor to adjust the threshold.

You can view the QPS and inbound and outbound traffic of the source and target buckets. For details about how to view the bucket usage statistics of OBS buckets, see **Viewing Bucket Usage Metrics**.



4.7 Why Is My Storage Migration Workflow Stalled for a Long Time?

Possible Causes

The progress bar may not change for a long time if:

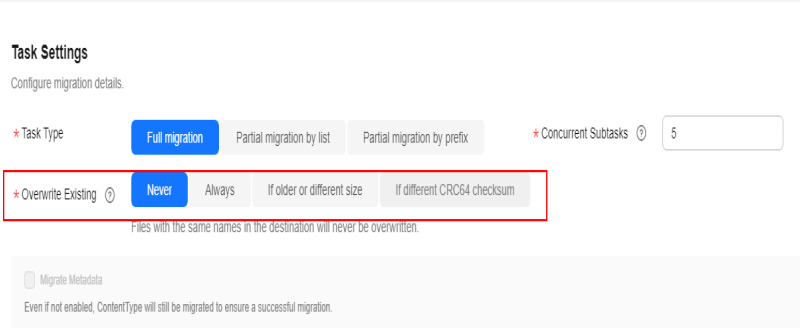
- There are multiple subtasks. The migration workflow automatically splits a large task into multiple subtasks for concurrent execution. The progress is updated only after all subtasks are complete.
- There are large objects to be migrated. It takes a long time to migrate large objects or files.
- The progress is not updated in real time. Even so, the migration process continues in the background.

Solutions

- Wait patiently, especially when there is a large amount of data to be migrated.
- Contact technical support to check if there are problems.

4.8 When I Migrate HTTP/HTTPS Data to Huawei Cloud OBS, How Are the Objects with the Same Name but Different URLs Processed?

In Huawei Cloud OBS, objects are identified using names but not URLs. When data is migrated from the HTTP/HTTPS source to Huawei Cloud OBS, how the objects with the same name are processed depends on the overwriting policy configured for the migration workflow. No matter which policy is used, no two objects in a given directory of an OBS bucket can have the same name.



- **Never**: The first migrated object will be retained in the target OBS bucket, but any source objects with the same name will be skipped during the migration, regardless of whether they have the same URL as the first migrated one or not.
- **Always**: The last migrated object will overwrite those previously migrated.

- **If older or different size**: The last migrated object will overwrite those migrated previously if:
  - It is newer than those migrated previously.
  - It was last modified at the same time as those migrated previously, but the size is different.

  If the last modification time and the size are the same, the object will not be migrated. It will be skipped.

4.9 When I Migrate Data from OBS to NAS on Huawei Cloud, How Are Objects with the Same Name but Different Capitalization Processed?

In OBS, object names are case sensitive, but in NAS, they are not. How objects with the same name but different capitalization are processed during a migration from OBS to NAS depends on the overwriting policy configured in the migration workflow. No matter which policy is used, no two objects in a given directory in the target NAS storage system can have the same name.

- **Never**: The first migrated object will be retained in the target file system, and any source objects with the same name will be skipped during the migration, even if the capitalization is different.
- **Always**: The last migrated object will overwrite any previously migrated objects with the same name even if the capitalization is different. Only the last migrated object will be retained in the target file system.
- **If older or different size**: The last migrated object will overwrite those migrated previously if:
  - It is newer than those migrated previously.
  - It was last modified at the same time as those migrated previously but the size is different.

  If the last modification time and file size are the same, the object will not be migrated. It will be skipped.

4.10 What Are the Constraints on the Length of Object Paths for Migrations Between OBS, NAS, and SMB Storage Systems on Huawei Cloud?

Different storage systems have different limitations of path length and folder name length During a heterogeneous migration, complying with the path length restrictions of the target storage system helps ensure migration success and data consistency.

The following table lists the limitations of path length and folder name length of different storage systems.

Storage System	Length Limitations
OBS	Maximum length of a folder name or path: 1023 bytes
NAS	• Maximum length of a folder name: 255 bytes • Maximum path length: 4,096 bytes
SMB	• Maximum length of a folder name: 226 bytes • Maximum path length: 32,767 bytes

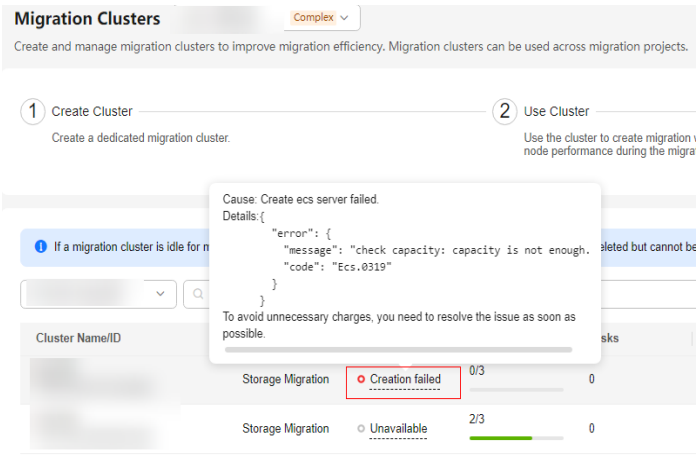
The following table lists the length limitations for different migration scenarios.

Migration Scenario	Length Limitations
OBS -> NAS	• Maximum path length: 4,096 bytes • Maximum length of a folder name: 255 bytes
SMB -> NAS	
NAS -> OBS	• Maximum path length: 1,023 bytes • Maximum length of a folder name: 1,023 bytes
SMB -> OBS	
OBS -> SMB	• Maximum path length: 32,767 bytes • Maximum length of a folder name: 226 bytes
NAS -> SMB	

4.11 How Do I Resolve the Problem that a Migration Cluster Fails to Be Created?

Symptom

When you created a migration cluster, **Creation failed** was displayed in the **Cluster Status** column.



Solution

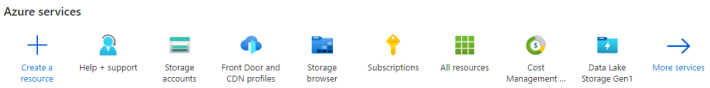
Click **Creation failed** in the **Cluster Status** column. Based on the displayed cause and details, rectify the fault. The following table lists some common errors and causes. If the fault persists, contact technical support or submit a service ticket.

Cause	Description	Solution
Ecs.0319 check capacity: capacity is not enough.	Insufficient ECS quota.	Apply for expanding the capacity. For more information, see **ECS Error Codes**.
Vpc.0702 query privateIps error.	Invalid parameters.	Check whether the parameter values are valid based on the returned error message. For more information, see: **VPC Error Codes**

4.12 How Do I Obtain Credentials for Accessing Microsoft Azure?

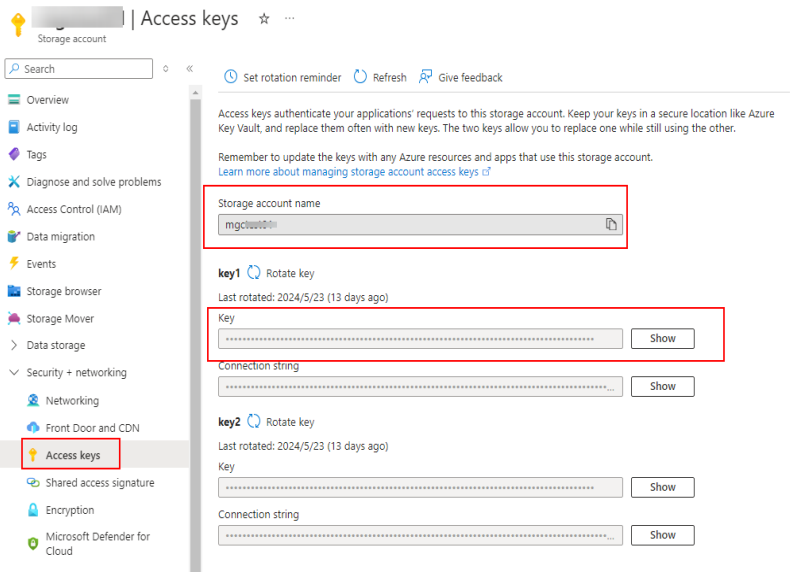
Obtain Storage Accounts and Keys

1. On the Azure portal, click **Storage accounts** and select the storage account that owns the data you want to migrate.



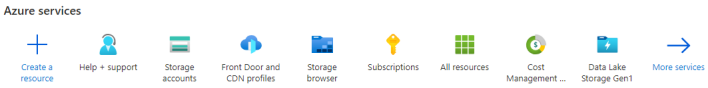
2. Under **Security + network**, choose **Access keys**. Your account access keys appear, as well as the complete connection string for each key.
3. Click **Show** to show your access keys and connection strings and to enable buttons to copy the values.

   You can use either of the two keys to access Azure Storage, but in general it is a good practice to use the first key, and reserve the use of the second key for when you are rotating keys.



Obtaining a Shared Access Signature

1. On the Azure portal, click **Storage accounts** and select the storage account that owns the data you want to migrate.



2. Under **Security & network**, choose **Shared access signature** and set the mandatory parameters listed in **Table 1 Setting parameters**. Set other parameters as needed.

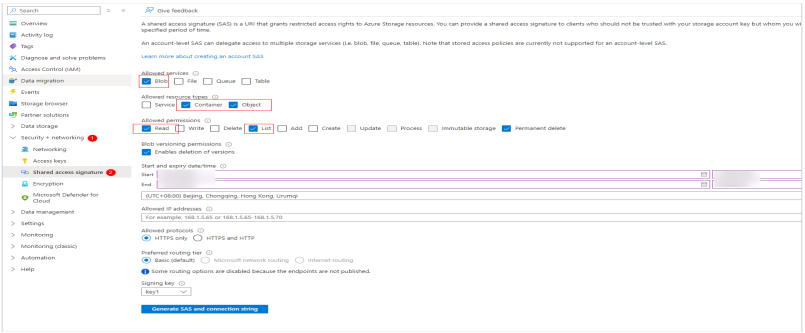


Table 4-3 Configuring parameters

Parameter	Configuration
Allowed services	Select at least **Blob**.
Allowed resource types	Select at least **Container** and **Object**.
Allowed permissions	Select at least **Read** and **List**. If you want to migrate archived objects, also select **Write**.
Start and expiry date/ time	Ensure that the connection string does not expire before the migration is complete.

3. Click **Generate SAS and connection string**. The connection string, SAS token, and Blob service SAS URL are displayed. Click the copy icon next to the connection string to copy the connection string.

   You can use the connection string to access Azure Storage.

4.13 What Do I Do If the Storage Migration Workflow Fails and "COMPARISON_ATTRIBUTE_NOT_SAME" Is Displayed?

Symptom

The migration workflow failed, and the error message "COMPARISON_ATTRIBUTE_NOT_SAME" was displayed.

Solution

This issue is caused by a failed metadata verification. There are two cases:

- Case 1: The **mtime** attribute in the metadata holds different meanings in the source and target storage systems. This happens if metadata migration is enabled for the migration from an object storage system to a PFS bucket. In the source storage system, **mtime** is a custom metadata attribute, while in the PFS bucket, this attribute represents the last modification time of a file. Even if the file can be migrated successfully, the error message indicating a metadata comparison failure will still appear. You can check whether the file has been successfully migrated to the target.
- Case 2: The metadata mismatches between the source and the target. In this case, perform the migration again. If the fault persists, contact technical support or submit a service ticket.

4.14 How Do I Choose Storage Classes?

To meet various performance and cost requirements, cloud service providers provide a range of storage levels that are different in **access frequency and latency, minimum storage time and unit, and data reliability and availability**. OBS provides the following storage classes:

- **Standard**

  This storage class features low latency and high throughput. It is therefore good for storing frequently (multiple times per month) accessed files or small files (less than 1 MB). Its application scenarios include big data analytics, mobile apps, hot videos, and social apps.

- **Infrequent Access**

This storage class is for storing data that is infrequently (less than 12 times per year) accessed, but when needed, the access has to be fast. It can be used for file synchronization, file sharing, enterprise backups, and many other scenarios.

- **Archive**

  This storage class is most suitable for archiving rarely-accessed (averagely once a year) data. Potential application scenarios include data archiving and long-term data retention for backup. This storage class is secure, durable, and inexpensive, so it can be used to replace tape libraries. To keep costs low, it may take minutes or hours to restore data from the Archive storage class.

For details about Huawei Cloud OBS storage classes, see **OBS Storage Classes**.

Storage Class Conversion for Reserving the Source Storage Class

If you choose **Reserve source storage type** for the destination storage policy, see **Table 4-4**. The numbers in parentheses indicate the monthly price per GB | the price per 10,000 read requests | the price per 10,000 write requests | the restoration price per GB (not applicable to standard storage) in turn. The prices in the table below are for reference only. The actual prices may vary depending on cloud service providers.

NOTE

- The regions used for reference in the following table are: Beijing, China for Huawei Cloud, Baidu Cloud, Alibaba Cloud, Tencent Cloud, and Kingsoft Cloud; Hong Kong, China for Google Cloud and AWS; East Asia for Microsoft Azure; and the Chinese mainland for Qiniu Cloud and UCloud. For capacity-based billing, the highest pricing tier is referenced. For AZ-based billing, if a cloud service provider offers multi-AZ storage but does not name it explicitly on the website, the pricing tier for single-AZ storage is referenced. The concurrency used here is CNY.
- The storage types that do not exist in the following table may fail to be migrated. You are advised to manually unfreeze the storage types and then migrate them to OBS.

Table 4-4 Storage class conversion between other cloud service providers and Huawei Cloud

Source Cloud Vendor	OBS Standard (0.099|0.01|0.01)	OBS Infrequent Access (0.08|0.1|0.1|0.0325)	OBS Archive (0.033|0.1|0.1|0.06)	OBS Deep Archive (0.014|0.5|0.5|0.12)
Amazon S3	• S3 Standard (0.172|0.0275|0.3441) • S3 Outposts (no pricing details on the website) • S3 Intelligent-Tiering (by assigned access tier|0.0275|0.0344) • Reduced Redundancy (no pricing details on the website)	• S3 Standard-IA (0.095|0.0688|0.6882|0.6882) • S3 One Zone-IA (0.0757|0.0688|0.6882|0.6882) • S3 Glacier Instant Retrieval (0.0344|0.6882|1.3764|2.0645)	S3 Glacier Flexible Retrieval (0.031|0.0275|2.4774|0.8258)	S3 Glacier Deep Archive (0.0138|0.0275|4.1291|1.6516)
Baidu Cloud BOS	Standard Storage (0.119|0.01|0.01)	• Infrequent Storage (0.08|0.05|0.05|0.03) • Cold Storage (0.032|0.1|0.1|0.06)	Archive (0.015|0.5|0.5|0.12)	-

Source Cloud Vendor	OBS Standard (0.099|0.01|0.01)	OBS Infrequent Access (0.08|0.1|0.1|0.0325)	OBS Archive (0.033|0.1|0.1|0.06)	OBS Deep Archive (0.014|0.5|0.5|0.12)
Tencent Cloud COS	• MAZ_Standard (0.15|0.01|0.01) • Standard (0.118|0.01|0.01) • MAZ_Intelligent Tiering (no pricing details on the website) • Intelligent Tiering (by the converted storage class|0.01|0.01)	• MAZ_Standard_IA (0.1|0.05|0.05|0.02) • Standard_IA (0.08|0.05|0.05|0.02)	Archive (0.033|0.01|0.01|0.06)	Deep Archive (0.01|0.5|0.5|0.14)
Qiniu Cloud Kodo	Standard (0.098|0.01|0.01)	Infrequent Access (0.06|0.1|0.1|0.03)	Archive (0.028|0.1|0.1|0.06)	Deep Archive (0.012|0.5|0.5|0.12)
Kingsoft Cloud KS3	Standard (0.12|0.01|0.01)	Infrequent Access (0.08|0.1|0.1|0.04)	Archive (0.033|0.1|0.1|0.06)	-
Alibaba Cloud OSS	Standard (0.12|0.01|0.01)	Infrequent Access (0.08|0.1|0.1|0.0325)	Archive (0.033|0.1|0.1|0.06)	Cold Archive (0.015|0.1|0.1|0.2)
UCloud US3	Standard (0.12|0.01|0.01)	Infrequent Access (0.06|0.1|0.1|0.03)	Archive (0.024|0.1|0.1|0.06)	-

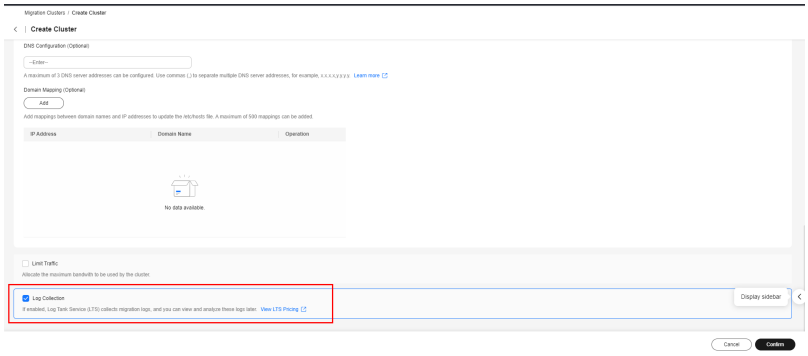
Source Cloud Vendor	OBS Standard (0.099|0.01|0.01)	OBS Infrequent Access (0.08|0.1|0.1|0.0325)	OBS Archive (0.033|0.1|0.1|0.06)	OBS Deep Archive (0.014|0.5|0.5|0.12)
Azure Blob Storage	Hot tier (0.165|0.0344|0.4469)	Cool tier (0.0756|0.0894|0.8937|0.0687)	Archive tier (0.0137|78.0989|1.5675|0.2406)	-

4.15 What Do I Do If a Migration Task Fails?

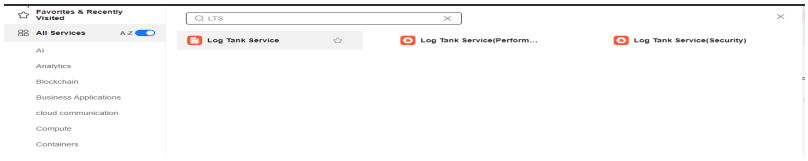
To rectify the fault if the workflow status is **Failed** after the migration is complete, use the following methods:

Method 1: Querying the Failure Cause Using LTS

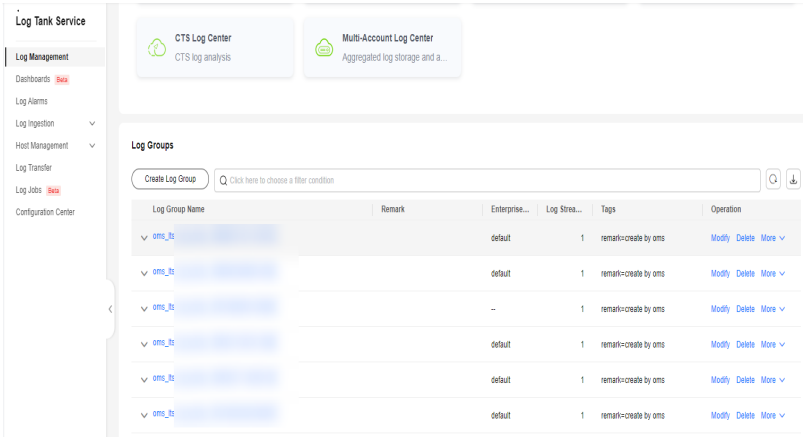
If log collection is enabled for the migration cluster used by the workflow, you can utilize this method to identify the failure cause from the error logs. Additionally, you can provide these logs to Huawei Cloud technical support for analysis, and they will offer handling suggestions.



Step 1 Search for LTS on the Huawei Cloud console.

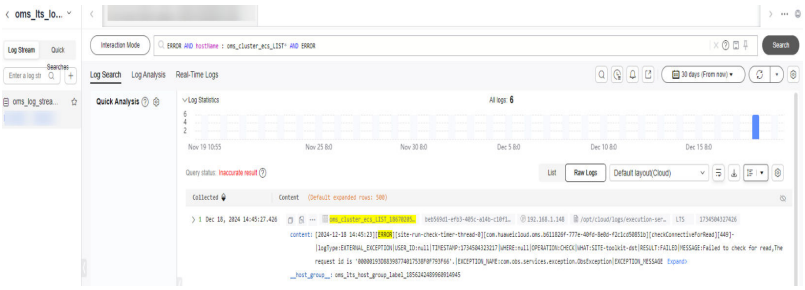


Step 2 Find the log group for the region where the migration cluster is located. Its name is in the format of **oms**_lts_log_group_*<migration-cluster-ID>*.

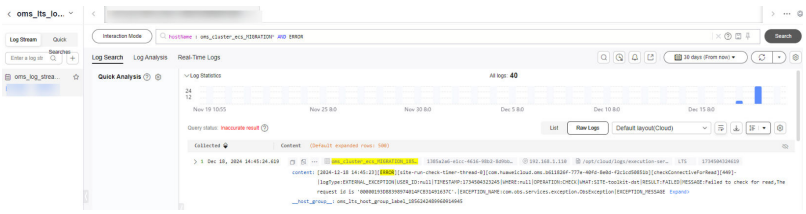


Step 3 Click the log group, adjust the time range to when the fault occurred, and search for logs.

To search for error logs of a list node, enter **hostName:oms_cluster_ecs_LIST_* AND ERROR** in the search box.



To search for error logs of a migration node, enter **hostName:oms_cluster_ecs_MIGRATION_* AND ERROR** in the search box.



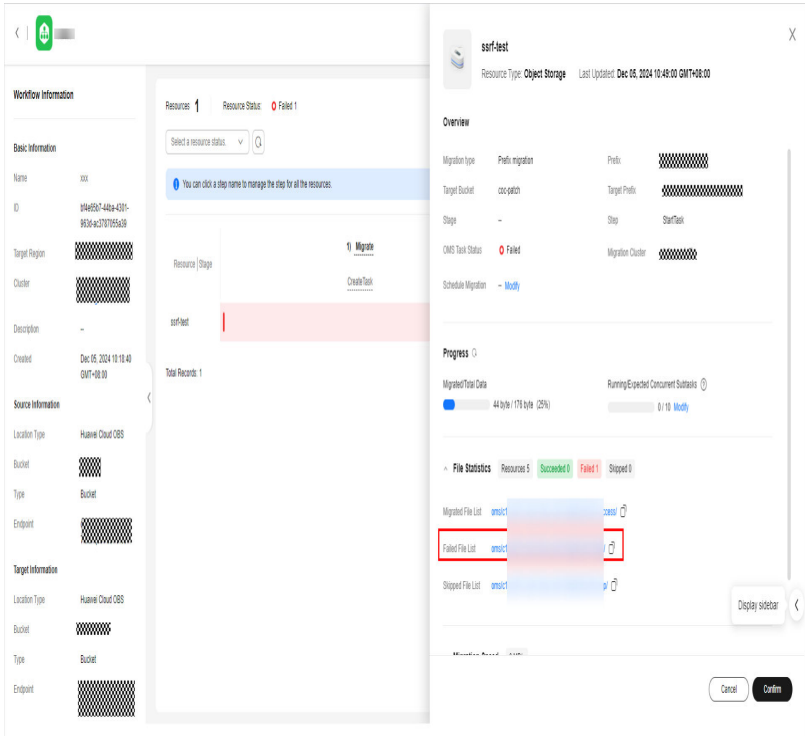
You can use the obtain error logs to analyze the failure cause or submit the logs to Huawei Cloud technical support for analysis and rectification suggestions.

----End

Method 2: Viewing the List of Failed Objects

If the OMS task status in the workflow is failed, find the path of the failed object list in the workflow. Generally, the path is in the **oms/***<oms2.0-task-ID>***/fail** directory at the target.

You can also see **Failed Object List** in the **File Statistics** area on the workflow details page.



The list of failed objects is in JSON format. Each record indicates an object. The **content_handle_result** field records the failure cause.

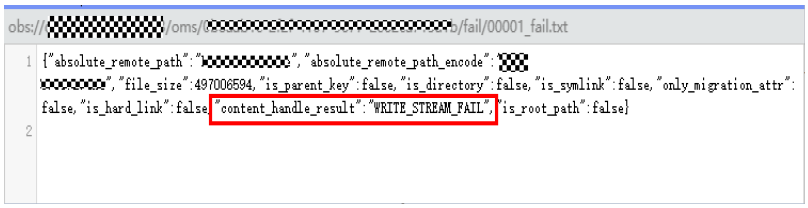


Table 4-5 Error codes in **content_handle_result**

Error Codes Returned for Failed Objects (content_handle_result)	Description	Solution
READ_ATTRIBUTE_FAIL_4_LIST	Reading attributes during listing failed.	Check whether the file attributes are normal and whether the file contains abnormal characters.

Error Codes Returned for Failed Objects (content_handle_result)	Description	Solution
COMPARISON_ATTRIBUTE_NOT_SAME	After the migration, the attributes of the source and target objects were inconsistent. The possible cause was that the source object changed after the listing.	Keep the source object unchanged and use the **Never** overwriting policy. Retry the workflow.
WRITE_STREAM_FAIL	Writing data to the target stream failed. The possible cause was that the write stream was preempted.	1. Retry the workflow. If the retry is successful, the fault is caused by stream interruption. 2. If the retry still fails, check whether you have the write permission for the target storage system.
UNSUPPORTED_FILE_TYPE	The file type was not supported.	Unsupported file types, such as pipe files, cannot be migrated.
WRITE_ATTRIBUTE_FAIL	Writing attributes at the target failed.	Check whether you have the permissions to modify metadata or attributes for the target storage system.
READ_ATTRIBUTE_FAIL	Read metadata or attributes of the source object failed.	Check whether you have the permissions to obtain the metadata of the source object.
SRC_OBJECT_IS_ARCHIVE	The source object was archived.	Archived source object must be manually restored before they can be migrated.
SRC_FILE_NOT_EXISTS	The source object was not found when it was migrated.	No solutions are available. It is impossible to migrate the source objects that were not found.

Error Codes Returned for Failed Objects (content_handle_result)	Description	Solution
COMPARISON_LAST_MODIFY_TIME_OF_SRC_IS_LATER_THAN_DST	When the object was verified for consistency after it was migrated to the target, the system found that the source object was last modified more recently than the paired target object. Generally, the cause was that the source object was modified after being migrated.	Keep the source object unchanged and retry the migration workflow.
COMPLETE_COMPARISON_KMS_NOT_SAME	When the object was verified for consistency after it was migrated to the target, the system found that the source object had a different encryption attribute from the paired target object. This was caused by the encryption setting of the migration workflow. For example, if the source object was encrypted but the encryption option was not enabled for the migration workflow, the source object will not be encrypted after being migrated to the target.	1. If the target object has your desired encryption attribute, ignore this error. 2. If the source object was encrypted and you want to retain its encryption attribute, create a migration workflow again and enable KMS encryption for the workflow.

Error Codes Returned for Failed Objects (content_handle_result)	Description	Solution
INIT_SLICE_UPLOAD_FAILED	An error was reported during multipart upload initialization.	Retry the failed object. This error is usually caused by network problems.
MIGRATION_SYM_LINK_FAILED	OBS does not support source symbolic links.	No solutions are available for this OBS compatibility issue.
CREATE_LINK_FAILED	Creating the symbolic link file failed.	Check whether this link file is required. If it is, contact Huawei Cloud technical support.
COMBINE_OBJECT_SLICE_FAILED	Combining file parts failed.	Check whether the account that owns the used AK/SK pair has the permissions to list file parts. If it does not, assign the following permissions to it and try the workflow or task again: `obs:bucket:ListBucketMultipartUploads` For details, see **How Do I Obtain Required Permissions for the Source and Destination Platform Accounts?**
HANDLE_SLICE_ERROR	Fragment processing failed due to network exceptions or insufficient permissions to read streams.	Retry the workflow or task. If the fault persists, contact Huawei Cloud technical support.
SYM_LINK_IS_NOT_SUPPORT_MIG	Symbolic link files in SMB storage systems cannot be migrated.	No solutions are available for this compatibility issue.
UNPROCESSED_ERROR	An unknown exception occurred.	Contact Huawei technical support.

Error Codes Returned for Failed Objects (content_handle_result)	Description	Solution
READ_ATTRIBUTE_FAIL_FOR_SRC	The metadata of the source object failed to be read for post-migration consistency verification. This was usually caused by flow control at the source.	Retry the workflow or task. If the fault persists, check the metadata of the source object.
READ_ATTRIBUTE_FAIL_FOR_DST	The metadata of the target object failed to be read for post-migration consistency verification. This was usually caused by flow control at the target.	Retry the workflow or task. If the fault persists, check the metadata of the target object.
FILE_SIZE_OVER_MAX_SIZE	The maximum number of file parts (10,000) exceeded.	The maximum size of each file part is 1 GB. Objects larger than 1 TB cannot be migrated.
FILE_PATH_TOO_LONG	The file path exceeded the 1,024-character limit allowed by OBS.	The maximum length of a file path in OBS is 1,024 characters. If this limit is exceeded, the file fails to be migrated.

5 Cross-AZ Migration

5.1 Are There Any Precautions I Need to Take When Performing a Cross-AZ Migration?

Password Consistency

If a source server has a password reset plug-in installed, such as Cloudbase-Init, a new password will be generated for the target server after the migration is complete. The source and target server passwords will be inconsistent. To keep the password unchanged, you need to uninstall the password reset plug-in before the migration.

Account Balance

You must ensure that your account balance is sufficient, and you need to pay for the resources created during the cross-AZ migration. The resources include vaults for storing source server backups, full-ECS images, and target servers created from the images.

5.2 How Can I Migrate Xen ECSs?

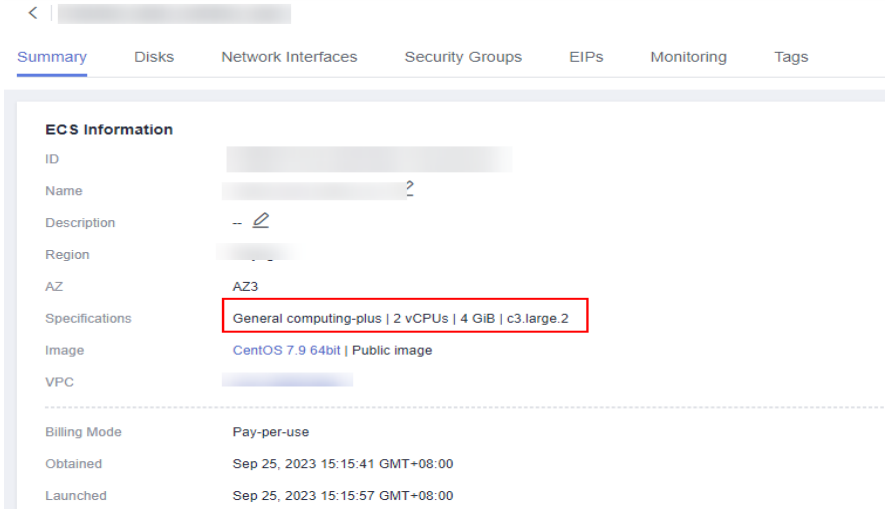
All versions of the Xen software used by Huawei Cloud have reached end of life. You need to change Xen ECSs to KVM ECSs before the migration.

Preparations

Checking Whether Your ECSs Use Xen

You can determine whether an ECS uses Xen based on its flavor in the basic information of the ECS. Xen ECSs include C1, C2, S1, M1, E1, E2, ET2, D1, H1, G1 and G2 ECSs.

Figure 5-1 Checking an ECS flavor



Installing Drivers

- For Linux servers, install the required drivers by referring to the following solutions:
  - Steps 1 and 2 in **Automatically Changing a Xen ECS to a KVM ECS (Linux)**
  - Step 1 to step 3 in **Manually Changing a Xen ECS to a KVM ECS (Linux)**
- For Windows source servers, install the required drivers by referring to step 1 to step 3 in **Changing a Xen ECS to a KVM ECS (Windows)**.

Migration

Create a cross-AZ migration workflow by referring to **Migrating Servers Across AZs**.

5.3 Why Are My Windows Data Disks Missing After the Migration?

Symptom

After a Windows source server was migrated, you logged in to the target server and found that some data disks were missing on the target server. However, the ECS console showed that the target server has the same number of disks as the source server.

Possible Causes

The SAN policy Offline Shared or Offline All was used for the source server. After the migration was complete, this setting was retained on the target server, and data disks are just offline.

Solutions

There are two solutions for you to rectify this problem.

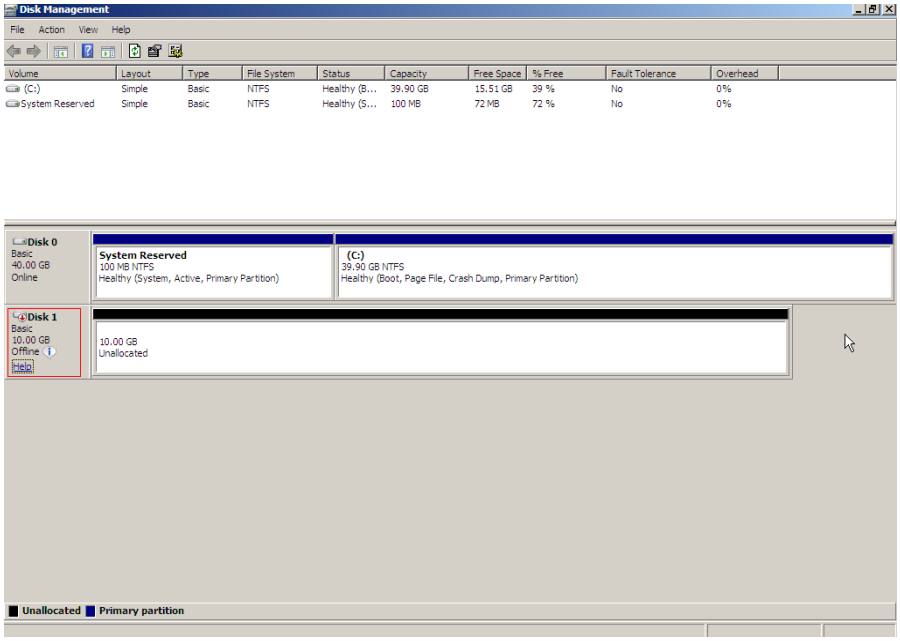
Solution 1

Step 1 Log in to the target server and choose **Start** > **Run**.

Step 2 Enter **diskmgmt.msc** and press **Enter** to open the **Disk Management** window.

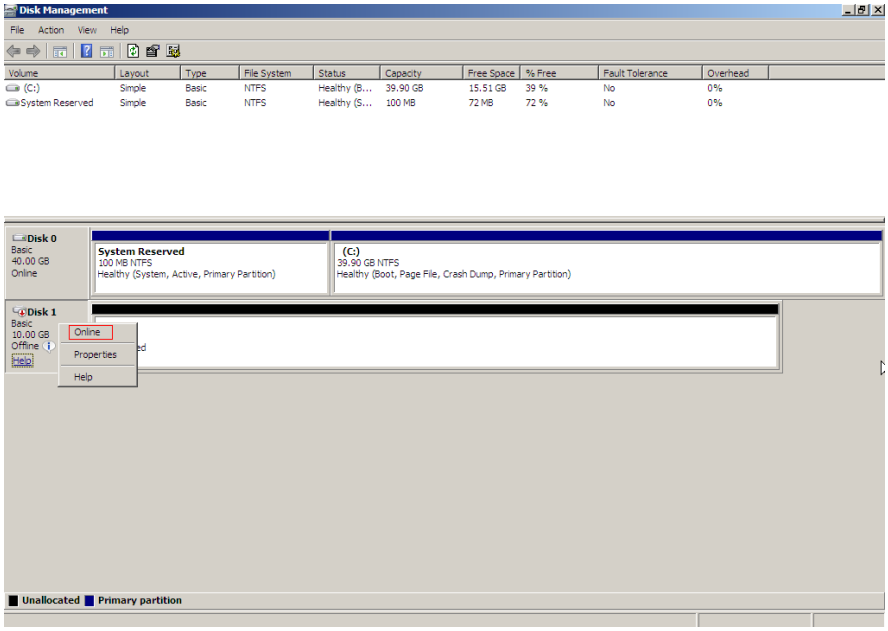
In the following figure, **disk 1** is offline.

Figure 5-2 Offline



Step 3 Right-click the offline data disk and select **online** from the pop-up menu.

Figure 5-3 Bringing the disk online



----End

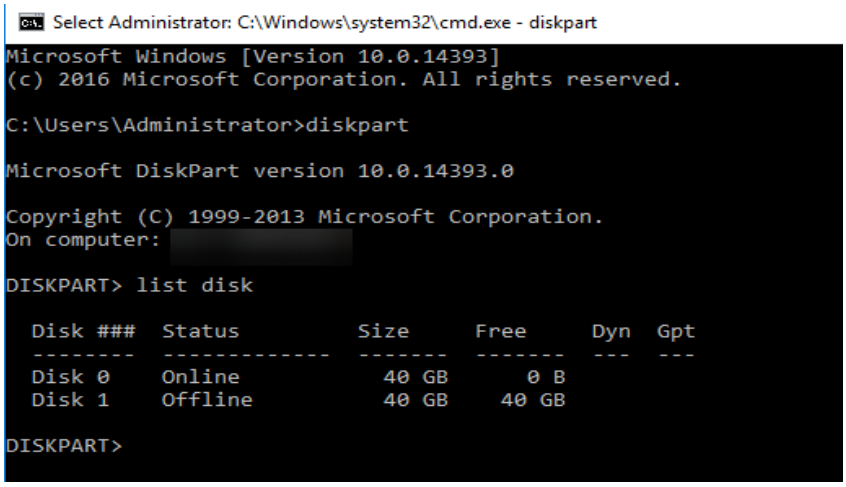
Solution 2

Step 1 Log in to the target server and right-click **Start**.

Step 2 Click **Run** and enter **cmd**.

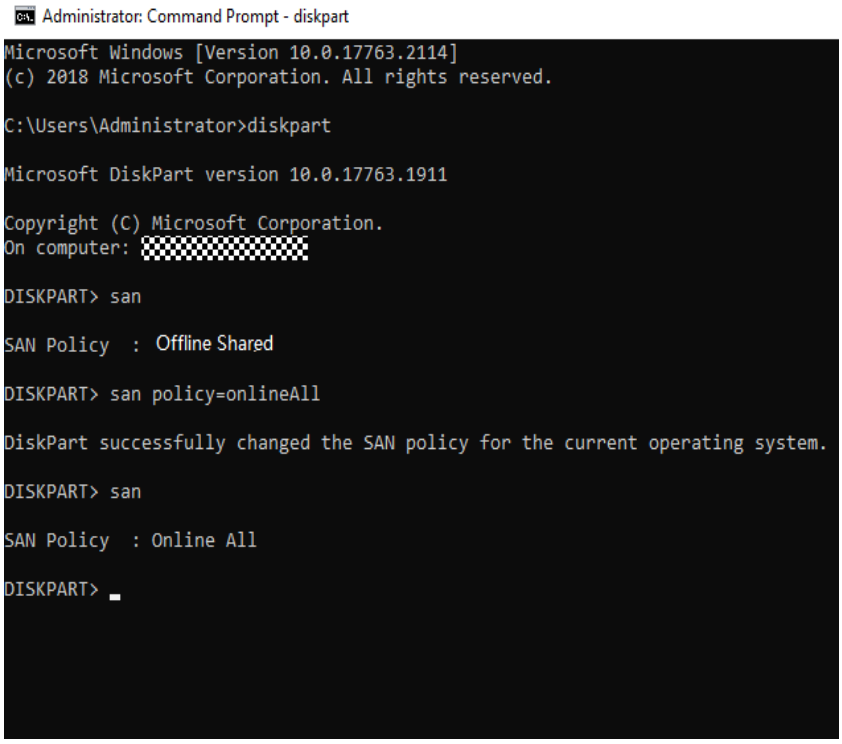
Step 3 Run **diskpart** to start the disk management tool.

Step 4 Run **list disk** to list all disks on the server. In the following figure, **disk 0** is online and **disk 1** is offline.



Step 5 Run **select disk 1**.

Step 6 Run **online disk** to change the disk status from offline to online.



Step 7 If the disk is read only after it is brought online, run the **attribute disk clear readonly** command to remove write protection from the disk.

----End

5.4 What Are the Known Errors Related to Cross-AZ Migration Workflows and How Can I Fix Them?

These error messages start with **AZworkflow**. You can find the solutions in **Known Errors and Solutions**.

6 Migration Surveys

6.1 Which Cloud Vendors Are Supported for TCO Analysis?

The supported cloud vendors and services are as follows.

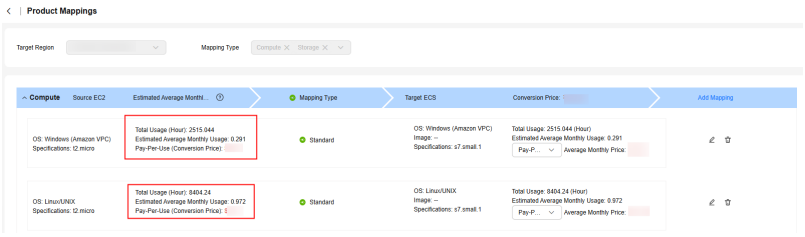
Source Cloud Vendor	Source Service	Huawei Cloud Service
AWS	Elastic Compute Cloud (EC2)	Elastic Cloud Server (ECS)
	Elastic Block Store (EBS)	Elastic Volume Service (EVS)
Alibaba Cloud	Elastic Cloud Service (ECS)	ECS
	Elastic Block Storage (EBS)	EVS

NOTICE

For some EBS product specifications, only certain billing items are considered in the TCO analysis, for instance, capacity and usage duration. Other billing items, such as IOPS and burst throughput, are ignored since their prices are calculated based on different rules on the source cloud and Huawei Cloud.

6.2 How Are the Estimated Prices Calculated?

The following describes how MgC estimates the prices of resources in the TCO analysis for a cross-cloud migration.



Total Usage

- MgC reviews your bills and refers to the usage duration or used capacity of a resource in the specified bill period.
- The time when a resource was used is not displayed.
- The unit can be hour or GB depending on the resource category.
- When calculating the total usage of a yearly/monthly compute resource, MgC treats one month as 720 hours.

Estimated Average Monthly Usage

- The collected source bills do not include the specific time when a resource was used. MgC assumes that the resource was used all of the time during the bill period. For example, if the specified bill period is two months, MgC assumes that a resource was used constantly in the two months.
- Unlike Total Usage, Estimated Average Monthly Usage is a ratio and has no unit. The formula depends on the billing mode of resources.
  - For pay-per-use resources:

    Estimated average monthly usage = Total usage/Number of months in the bill period/720

    Assume that a pay-per-use resource is used for 23.66 hours during the bill period of one month (720 hours). The estimated average monthly usage of resource is 0.0328 (23.66/1/720).
  - For yearly/monthly resources:

    Estimated average monthly usage = Number of a resource

    Assume that two yearly/monthly cloud servers are used in the bill period, one month. The average monthly usage of the servers is 2. The total usage of the servers is 1,440 hours (2 × 1 × 720).
- Estimated average monthly usage is designed to facilitate price calculation when the billing mode of a source resource differs from that of the desired target resource.

Conversion Price

- Conversion price at the source = Bill price (after discount)/Number of months in the bill period
- Conversion price on Huawei Cloud
  - Conversion price of a pay-per-use resource = Official price (before discount) × Estimated average monthly usage × 720
  - Conversion price of a yearly/monthly resource = Official price (before discount) x Estimated average monthly usage

Assume that a source resource is billed on a per-pay-use basis on the source cloud, but you want to use a yearly/monthly resource of the same specifications on Huawei Cloud. MgC uses the estimated average monthly usage to convert the pay-per-use pricing on the source cloud to a yearly/monthly equivalent on Huawei Cloud.

Examples

- Example 1: Assume that a pay-per-use source resource was used for 100 hours over a bill period of five months, and the total cost was $68.4 USD. The price of the mapped Huawei Cloud resource is $1.5 USD/hour or $684.4 USD/month.

  Table 6-1 Conversion prices

Item	Source	Huawei Cloud
Total usage	100 hours	100 hours
Estimated average monthly usage	100/5/720 = 0.0278	100/5/720 = 0.0278
Conversion price (pay-per-use)	68.4/5 = $13.68 USD	1.5 × 0.0278 × 720 = $30.02 USD
Conversion price (monthly)	-	684.4 × 0.0278 = $19.03 USD

  Based on the comparison, the source resource costs less than the Huawei Cloud resource, regardless of whether pay-per-use or yearly/monthly is used.

- Example 2: Assume that a yearly/monthly source resource costed $68.4 USD during a bill period of five months. The price of the mapped Huawei Cloud resource is $0.03 USD/hour or $11 USD/month.

  Table 6-2 Conversion prices

Item	Source	Huawei Cloud
Total usage	720 × 5 = 3600 hours	3600 hours
Estimated average monthly usage	1	1
Conversion price (pay-per-use)	-	0.03 × 1 × 720 = $21.6 USD

Item	Source	Huawei Cloud
Conversion price (monthly)	68.4/5 = $13.68 USD	11 × 1 = $11 USD

Based on the comparison, the source resource costs more than the Huawei Cloud resource if pay-per-use is used, and costs less than the Huawei Cloud resource if yearly/monthly is used.

7 Resource Discovery

7.1 Known Resource Discovery Problems and Solutions

The following table lists known issues related to resource discovery and how these issues can be addressed.

Issue	Solution
Task name already exists.	Enter another task name.
Create collection task failed.	Contact technical support or submit a service ticket.
Involved collection task not found.	Associate the collection item with another collection task.
Collection item already exists.	Check whether the collection item has already been associated with the collection task, or contact technical support.
Add collection item failed.	Contact technical support or submit a service ticket.
Add data source failed.	Contact technical support or submit a service ticket.
Delete collection task failed.	Refresh the task list to check whether the collection task has been deleted, or contact technical support.
Delete collection item failed.	Refresh the collection item list to check whether the collection item has been deleted, or contact technical support.
Collection task not found.	Refresh the collection task list and check whether the collection task exists.
Collection item not found.	Refresh the collection item list and check whether the collection item exists.

Issue	Solution
Add data source failed.	Contact technical support or submit a service ticket.
Data source not found.	Refresh the collection item list and check whether the data source exists.
Re-collect data source failed.	Refresh the collection item list and check whether the data source exists, or contact technical support.
Delete data source failed.	Refresh the collection item list and check whether the data source has been deleted, or contact technical support.
Edit data source name failed.	Refresh the collection item list and check whether the data source exists, or contact technical support.
Re-collection failed.	Refresh the collection item list and check whether the collection item exists, or contact technical support.
Incorrect data source settings.	Check whether the data source settings are correct.
Re-collect data source failed.	Check whether the collection uses APIs and the status is completed.
Delete data source failed.	Only data sources in the collection failed or completed status can be deleted.
Delete collection item failed.	Only collection items in the waiting status can be deleted.
Delete collection task failed. There are running collection items.	Refresh the collection item list and check whether there are running collection items. If there are running collection items, the collection task cannot be deleted.
The file to import is too large.	The maximum file size allowed is 10 MB.
Invalid file name.	Enter a valid file name.
Invalid file format.	Import a file in the correct format.
Add data source failed. Uploaded file not found.	Check whether the file has been successfully imported or import the file again.
Could not collect information from Alibaba Cloud RM.	Debug API SearchResources by following the instructions provided in the Alibaba Cloud Resource Management Documentation and locate the fault cause based on the returned error code, or contact Alibaba Cloud technical support.

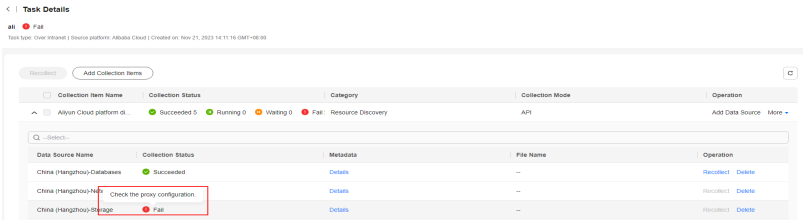
Issue	Solution
Could not collect information from Alibaba Cloud RM.	Debug API GetResourceConfiguration by following the instructions provided in the Alibaba Cloud Resource Management Documentation and locate the fault cause based on the returned error code, or contact Alibaba Cloud technical support.
Credential not found.	Check whether the selected credential can be found on the Credentials page.
Credential expired.	Update the credential on the Credentials page.
Wrong credential type. Select AK/SK credentials.	Select AK/SK credentials.
Invalid MSE configuration file.	Check whether the selected credential and regions are correct.
Incorrect file format.	Upload a file in the correct format.
Could not obtain Nacos accessToken.	Check whether the username and password entered in the configuration information are correct.
Could not parse Nacos authentication information.	Contact technical support or submit a service ticket.
Could not query domain names in pagination mode.	Debug API DescribeDomains by following the instructions provided in the Alibaba Cloud Resource Management Documentation and locate the fault cause based on the returned error code, or contact Alibaba Cloud technical support.
Could not query DNS records in pagination mode.	Debug API DescribeDomainRecords by following the instructions provided in the Alibaba Cloud Resource Management Documentation and locate the fault cause based on the returned error code, or contact Alibaba Cloud technical support.
Could not invoke the Alibaba Cloud WAF SDK.	Debug API DescribeDomains by following the instructions provided in the Alibaba Cloud Resource Management Documentation and locate the fault cause based on the returned error code, or contact Alibaba Cloud technical support.
Invalid AK/SK.	Check whether the AK/SK pair recorded in the selected credential is correct.

Issue	Solution
Could not invoke the Alibaba Cloud Kafka SDK.	Check whether the selected credential and regions are correct, or check whether the Alibaba Cloud Kafka service is enabled for the account that the credential belongs to.
Could not invoke the Alibaba Cloud Topic SDK.	Debug API GetInstanceList by following the instructions provided in the Alibaba Cloud Resource Management Documentation and locate the fault cause based on the returned error code, or contact Alibaba Cloud technical support.
Could not invoke the Alibaba Cloud RDS SDK.	Check whether the selected credential and regions are correct, or check whether the Alibaba Cloud RDS service is enabled for the account that the credential belongs to.
Could not invoke the Alibaba Cloud RDS schema SDK.	Debug API DescribeDatabases by following the instructions provided in the Alibaba Cloud Resource Management Documentation and locate the fault cause based on the returned error code, or contact Alibaba Cloud technical support.
Create Alibaba Cloud SLB SDK client failed.	Check whether the selected credential and regions are correct.
Uploaded file contains invalid data.	Enter valid values.
Uploaded file failed the verification.	Contact technical support or submit a service ticket.
Required fields are missing in uploaded file.	Specify required fields.
Table headers of uploaded file are incorrect.	Enter the correct table headers.
Table headers of uploaded file are invalid.	Check whether non-customized table headers in the template have been modified.
Unexpected domain names found in "Domain" sheet.	Ensure that domain names entered in the "Application" and "MQ" sheets have been entered in the "Domain" sheet.
Invalid file content.	Check whether the import template was modified or download the template again.
Maximum tags reached.	Delete unnecessary tags and try again.
Add tag failed.	Contact technical support or submit a service ticket.
Tag not found.	Check whether the tag is available.

Issue	Solution
The tag has been associated with resources.	Select another tag or dissociate from resources.
Update tag failed.	Contact technical support or submit a service ticket.
The parameter for querying the tag set is empty.	Set the tag query parameters.
Associate tag with resources failed.	Contact technical support or submit a service ticket.
The tag was not associated with the resources	Check whether related resources and the tag have been associated, or contact technical support.
ID not found.	Contact technical support or submit a service ticket.
Modify data failed.	Contact technical support or submit a service ticket.
Data import failed.	Contact technical support or submit a service ticket.
Name already exists.	Enter another name.
File upload failed.	Contact technical support or submit a service ticket.
File download failed.	Contact technical support or submit a service ticket.
Uploaded file not found or expired.	Upload a new file, or rename the file and upload it again.
Producer and consumer in a raw in sheet "MQ" are in different environments.	Check whether the producer and consumer environments in the MQ sheet of the imported file are consistent.
Producers or consumers specified in sheet "MQ" are not found in sheet "Application".	Ensure that the producer and consumer services or microservices in the MQ sheet have been supplemented in the Application sheet of the imported file.
Column "MICROSERVICE" in sheet "Application" is required.	Add microservices in the Application sheet to the imported file.
Columns "PRODUCER" and "CONSUMER" in sheet "MQ" are required.	Add the producer and consumer services or microservices to the MQ sheet of the imported file.

7.2 Where Can I Find the Collection Failure Cause?

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 causes, you need to delete the collection item and add it again by referring to **How Do I Collect Data from a Data Source Again If the Previous Collection Fails?**.



7.3 What Can I Do If an Internet Discovery Task Fails and the Error Message "Network connection timed out" or "Other exception" Is Displayed?

Symptom

The Internet-based discovery task failed, and the error message "Network connection timed out" or "Other exception" was reported.

Possible Causes

- **Network connection timed out**: The region where the source resources are located is not supported by MgC.
- **Other exception**: An unknown exception occurs when the source resources are connected. There are many possible reasons. You need to troubleshoot this issue by yourself.

7.4 How Do I Collect Data from a Data Source Again If the Previous Collection Fails?

After handling the failure causes, if you still want to collect this item, you need to delete the collection item and add it again.

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

Step 2 Locate the required collection item and click **Add Data Source** in the **Operation** column.

Step 3 Select a region and resource type, and click **OK**. After the data source is added, the system automatically starts to collect source data.

You can click the collection item to view the status of its data source.

----End

7.5 How Do I Obtain the Cloud Platform Credentials (AK/SK Pairs)?

Obtain the authentication information (access keys) required for accessing cloud platforms.

Obtaining Alibaba Cloud AccessKey Pairs

When providing your credential for MgC to discover your Alibaba Cloud resources, you need to provide the AK/SK pair of your Alibaba Cloud account or RAM user account that owns the resources to be discovered. For details, see **Creating an AccessKey Pair**.

Obtaining Huawei Cloud Access Keys (AK/SK Pairs)

When providing your credential for MgC to discover your Huawei Cloud resources, you need to provide the AK/SK pair of your Huawei Cloud account or IAM user account that owns the resources to be discovered. For details, see **Creating an Access Key**.

Obtaining AWS Access Keys

When providing your credential for MgC to discover your AWS resources, you need to provide the AK/SK pair of your AWS root account or IAM user account that owns the resources to be discovered. For details, see **Creating Access Keys for the Root User** or **Managing Access Keys for IAM Users**.

Obtaining Tencent Cloud Access Keys (SecretId/SecretKey Pairs)

When providing your credential for MgC to discover your Tencent Cloud resources, you need to provide the API key of the root account or IAM user account that owns the resources to be discovered. For details, see **Access Keys for the Root Account** or **Access Keys for Sub-Users**.

Obtaining Qiniu Cloud Access Keys (AccessKey/SecretKey Pairs)

When providing your credential for MgC to discover your Qiniu Cloud resources, you need to provide the access key of the account that owns the resources to be discovered. You can obtain it from the **Key Management** page of the Qiniu Cloud console.

Obtaining Kingsoft Cloud Access Keys (AK/SK Pairs)

When providing your credential for MgC to discover your Kingsoft Cloud resources, you need to provide the access key of the IAM user account that owns the resources to be discovered. For details about how to obtain the AK/SK, see **Create an AccessKey for an IAM User**.

7.6 How Do I Obtain the Information for Adding Azure Credentials to MgC?

To discover your Azure resources using MgC, you need to provide your Azure credentials including your tenant ID, client (application) ID, subscription ID, and secret. This section describes how to obtain these credentials.

Obtaining a Subscription ID

Step 1 Sign in to the **Azure** portal.

Step 2 Search for and select **Subscriptions**.

Step 3 Find the desired subscription in the list and note the subscription ID in the second column. Copy the subscription ID to the dialog box for adding credentials on MgC.

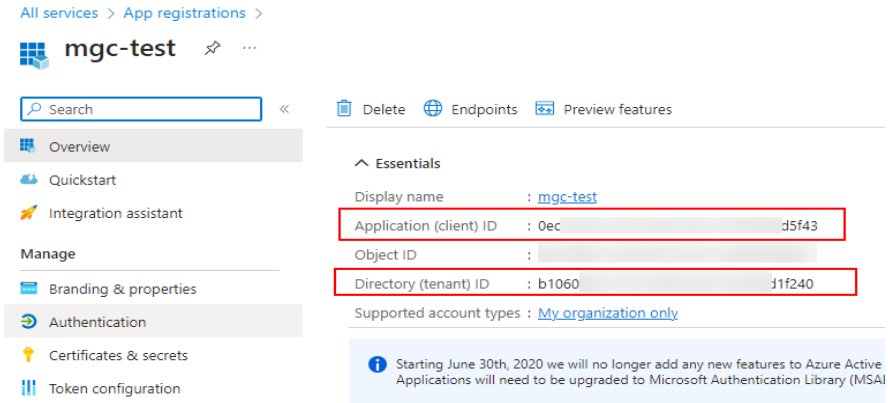
----End

Obtaining a Tenant ID, Application ID, and Secret

Step 1 Sign in to the **Azure** portal.

Step 2 Search for and select **App Registrations**.

Step 3 Click the **All Applications** tab and click the desired application. In the **Overview** area, note the application (client) ID and the directory (tenant) ID.



Step 4 In the navigation pane on the left, choose **Certificates & secrets**, click the **Client secrets** tab, and click **New client secret**. The newly created secret can only be viewed when it is created. Be sure to note the secret and keep it secure.

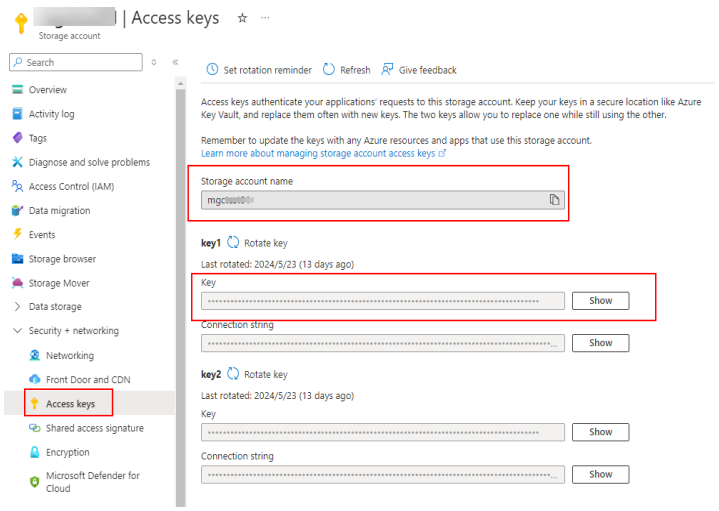
----End

7.7 How Do I Obtain the Required Credentials Before Using MgC to Perform a Deep Collection for My Azure Object Storage Resources?

To perform a deep collection for your Azure object storage resources, you need to provide your storage account and access key. This section describes how to obtain these credentials.

Step 1 In the **Azure portal**, go to your storage account.

Step 2 In the navigation pane on the left, under **Security + networking**, select **Access keys**. Your storage account name and keys appear.



Step 3 Under **key1**, click **Show** next to the key. The access key and the **Copy** button appear.

Step 4 Note your storage account name and access key and add them to your MgC Agent. For details about how to add credentials to the MgC Agent, see **Adding Resource Credentials**. When you add the credentials to the MgC Agent, set **Authentication** to **AK/SK**. Enter the storage account name in the **AK** box and the access key in the **SK** box.

----End

7.8 How Do I Configure the Permissions Required for Collecting Details of Azure Containers?

This section describes how to configure the permissions required for using MgC to collect details about Azure container resources. The application that the collection credential belongs to must have the following information in the involved resource group and subscription:

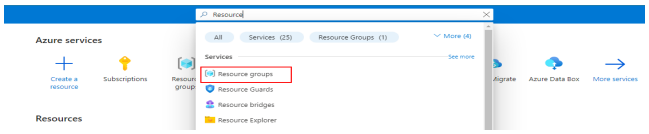
- Microsoft.ClassicCompute/virtualMachines/read
- Microsoft.Insights/MetricDefinitions/Read

- Microsoft.Management/getEntities/action

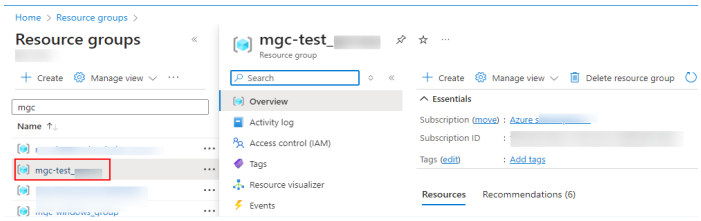
Procedure

Step 1 Sign in to the **Azure** portal.

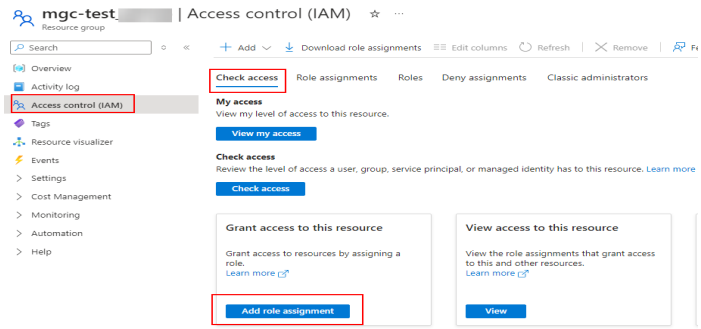
Step 2 In the upper part of the page, enter **Resource groups** in the search box and select **Resource groups**.



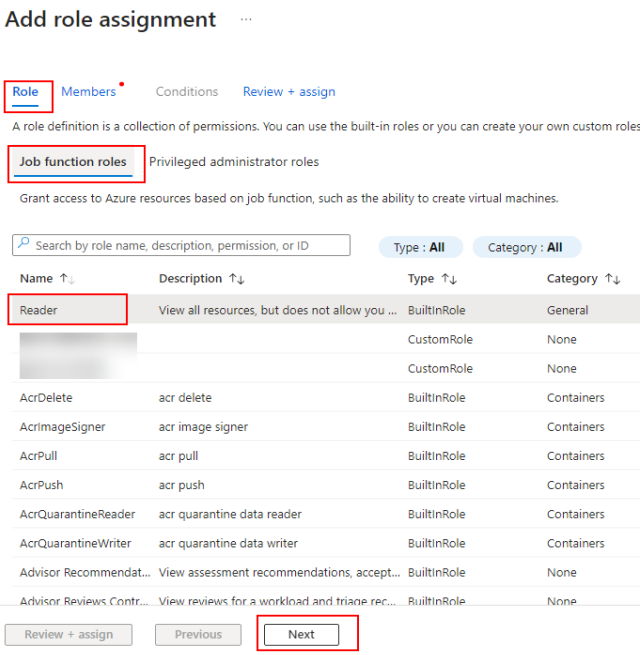
Step 3 In the resource group list, click the resource group that contains your Azure Kubernetes Service (AKS) resources.



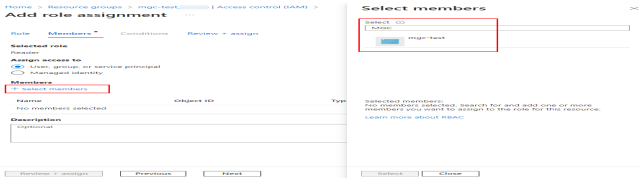
Step 4 In the navigation pane on the left, choose **Access control (IAM)**. On the **Check access** tab, click **Add role assignment**.



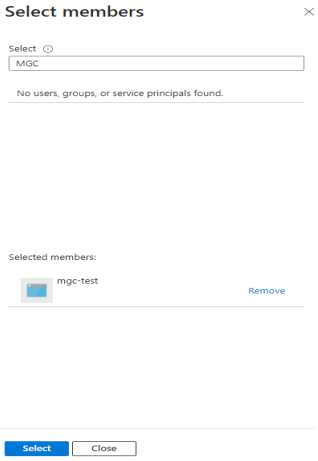
Step 5 Select **Reader** and click **Next**.



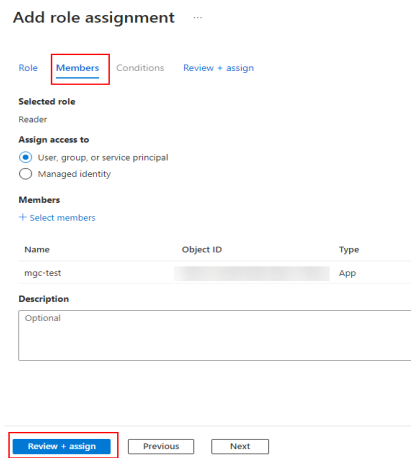
Step 6 Click **Select members**. In the dialog box displayed on the right, search for and click the application name (that the collection credential belongs to).



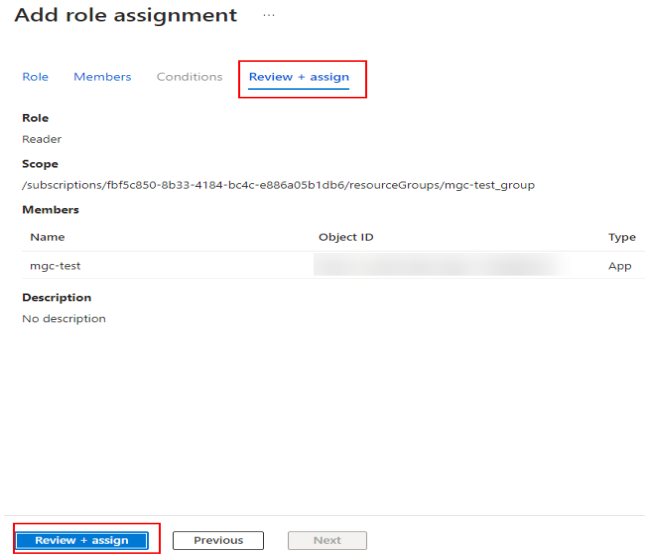
Step 7 Click **Select** to add it to the member list.



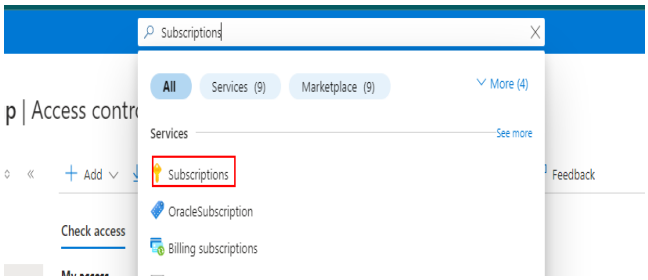
Step 8 Click **Review + assign**.



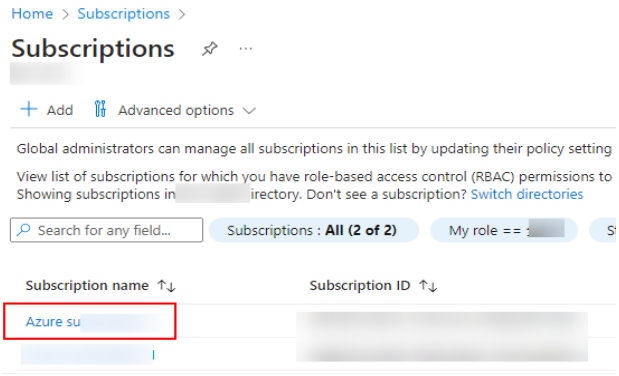
Step 9 After confirming that the role and member are correct, click **Review+ assign** to configure permissions for the application in the resource group.



Step 10 In the upper part of the page, search for and select **Subscriptions**.



Step 11 In the subscription list, click the name of the subscription that contains your AKS resources.



Step 12 Configure permissions for the application in the subscription by referring to **Step 4** to **Step 9**.

----End

7.9 How Do I Convert the Encoding Format of a CSV File to UTF-8?

To import Alibaba Cloud servers to MgC, you must upload UTF-8 encoded CSV files with English table headers. This section describes how to change the encoding format of .csv files to UTF-8.

Method 1 (for Windows)

Step 1 Right-click the CSV file and choose **Open with Notepad**.

Step 2 In the upper left corner of the Notepad window, choose **File** > **Save As**. In the **Save As** dialog box, select **UTF-8** from the **Encoding** drop-down list and click **Save**.

----End

Method 2 (for Windows)

Use Notepad++ to convert the CSV file encoding format to UTF-8. Ensure that Notepad++ has been installed. If it has not been installed, download it from the official website and install it.

Step 1 Open Notepad++, drag the CSV file to the Notepad++ window, and press Ctrl+A to select all contents.

Step 2 On the Notepad++ menu bar, choose **Encoding** > **Encode in UTF-8**. Press Ctrl+S to save the file.

----End

Method 3 (for Mac)

Use TextEdit to convert the CSV file encoding format to UTF-8.

Step 1 Open TextEdit on Mac.

Step 2 Choose **File** > **Open** in the upper left corner.

Step 3 Select the CSV file whose encoding format needs to be converted and select **Unicode (UTF-8)** for **Encoding**.

Step 4 Choose **File** > **Save** to convert the file encoding format to UTF-8.

----End

7.10 What Can I Do If the Collected Disk Information Is Empty or Incorrect After a Deep Collection Is Performed for a Windows Source Server?

Symptom

After a deep collection is performed for a Windows source server, the disk information is empty or garbled characters are displayed.

Possible Causes

The region and language settings of the Windows server are inconsistent. As a result, the disk information fails to be collected.

Solution

Perform the following steps to rectify the fault:

1. Log in to the Windows server, click **Start**, and click the **Settings** icon (gear-shaped).
2. In the displayed dialog box, click **Time and Language**.
3. In the navigation pane, choose **Language**.
4. In the **Related settings** area, click **Administrative language settings**. The **Administrative** tab of the **Region** window is displayed.
5. In the **Language for non-Unicode programs** area, click **Change system locale**.
6. Check whether the **Current system locale** is the same as **Current language for non-Unicode programs**. If they are different, select the region in the current language from the drop-down list and click **OK**.
7. Restart the server and check whether the settings are applied.

7.11 What Can I Do If the Collected OS Information Is Incorrect After a Deep Collection Is Performed for a Windows Source Server?

Symptom

After a deep collection is performed for a Windows source server, the OS information is garbled characters in the collected resource details.

Possible Causes

The region and language settings of the Windows server are inconsistent. As a result, the OS information fails to be collected.

Solution

Try the following to troubleshoot:

1. Log in to the Windows server, click **Start**, and click the **Settings** icon (gear-shaped).
2. In the displayed dialog box, click **Time and Language**.
3. In the navigation pane, choose **Language**.
4. In the **Related settings** area, click **Administrative language settings**. The **Administrative** tab of the **Region** window is displayed.
5. In the **Language for non-Unicode programs** area, click **Change system locale**.
6. Check whether the **Current system locale** is the same as **Current language for non-Unicode programs**. If they are different, select the region in the current language from the drop-down list and click **OK**.
7. Restart the server and check whether the settings are applied.

7.12 What Can I Do If an RVTools Import Fails?

Scenarios

When you tried to import RVTools data, the import failed.

Possible Causes

The Excel file exported from RVTools may have compatibility or format issues.

Solution

Step 1 Open the Excel file exported from RVTools using the Excel software on Windows.

Step 2 Copy the data in the Excel file and paste it to a new Excel file.

Step 3 Save the new Excel file in .xlsx or .xls format.

Step 4 Import the newly saved Excel file to MgC.

----End

7.13 What Do I Do If the Deep Collection Succeeds on a Source Server but Some Specifications Information Is Not Collected?

Symptom

After a deep collection was performed for a source server, some specifications information did not appear on the resource details page.

Possible Causes

The UNIX newline character is incorrect in the Linux collection script installed on the MgC Agent (formerly Edge) server. The Linux system uses LF as the newline character, but the installation script uses CR LF, which is the new character in the Windows system. The script could not be pushed to the source server during the collection.

Solution

Step 1 Uninstall the current MgC Agent and reinstall it.

Step 2 Launch a deep collection for the source server again.

----End

8 Target Recommendations

8.1 Where Can I Find the Assessment Failure Cause?

You can hover over the red exclamation mark on the left of the assessment status to view the failure cause.

8.2 Why Can't I Manually Select Target Server Specifications and Disk Types?

You must first assess source servers.

8.3 What Can I Do If a Server Assessment Fails and the System Displays a Message Indicating No Proper Specifications Are Matched?

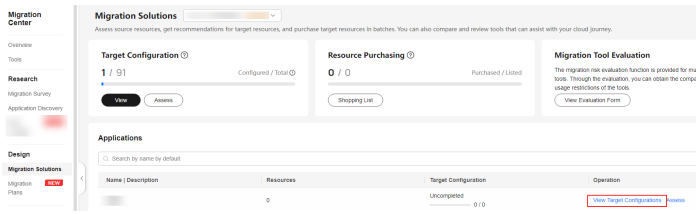
Possible Causes

Possible causes are:

- There are no specifications that match the source server in the target region.
- There are no specifications that match the custom assessment policy you specified.

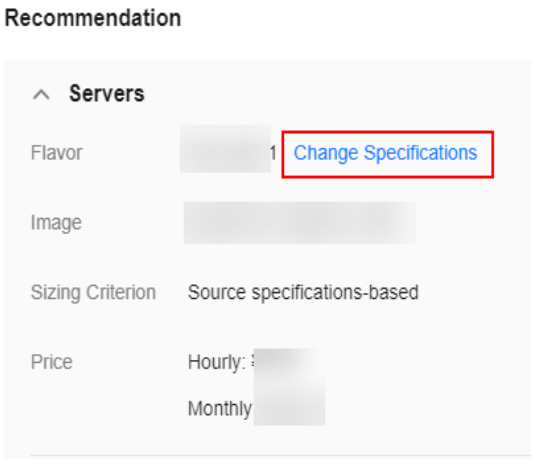
Solution

Step 1 In the application list on the **Migration Solutions** page, click **View Target Configurations** in the **Operation** column.



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

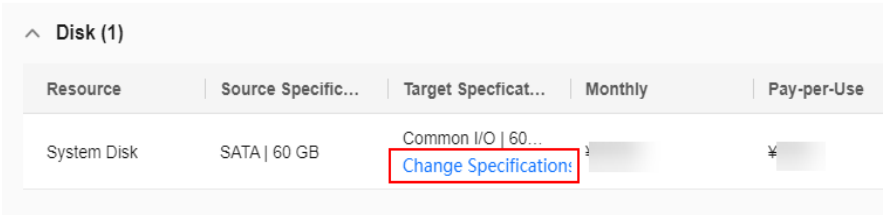
Step 3 Modify the specifications and image for the target server.



Step 4 In the disk area, locate a disk and click **Modify** in the **Target Specifications** column to modify the disk type and capacity. Only Linux disk sizes can be decreased. If you downsize a disk, the system will set **Disk Downsized** to **Yes**. The reverse also applies.

NOTICE

- The system disk capacity ranges from 40 GB to 1,024 GB.
- The data disk capacity ranges from 10 GB to 32,768 GB.
- 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.



----End

8.4 What Can I Do If a Server Assessment Fails Because the Target Server Specifications Do Not Support Windows Images?

Possible Causes

The selected target server specifications support only Linux images.

Solution

Select target server specifications that support Windows images. After selecting the target server specifications, all supported images will be displayed in the image drop-down list.

8.5 What Types of Databases Can I Assess Using MgC?

MgC can assess and generate recommendations for MySQL, PostgreSQL, MongoDB, Oracle, and SQL Server databases.

8.6 How Does MgC Generate Target Recommendations?

This section describes how MgC recommended appropriate target resources for you based on the assessment policy and preferences you configure.

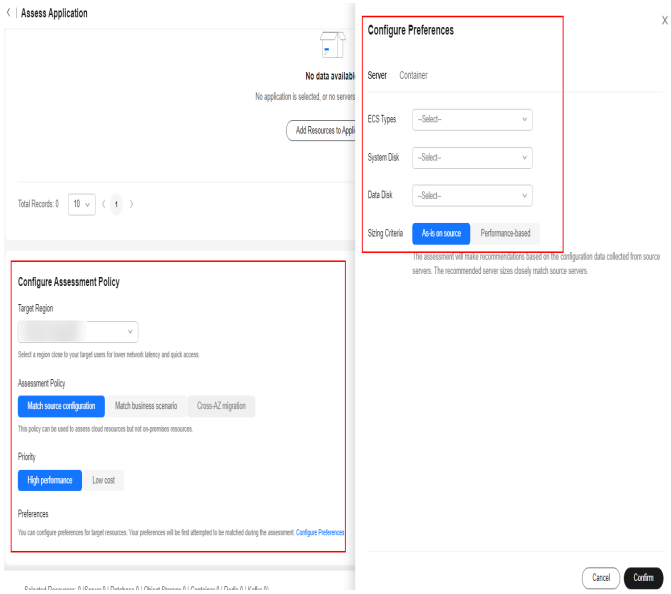


Table 8-1 Settings used for computing target recommendations

Parameter	Option	Description
Target Region	-	Select the region where you want to purchase resources on Huawei Cloud. You are advised to select a region close to your target users for lower network latency and quick access.

Parameter	Option	Description
Assessment Policy	Match source configuration	MgC will recommend Huawei Cloud resources in the same or slightly larger size as source resources. For a server manually added to MgC or automatically discovered by MgC over an intranet, the recommendation is limited to three instance types: FlexusX, General Computing ECS, and General Computing-plus ECS. MgC first sorts all flavors in these three types in descending order of price or performance as you prefer. Then it recommends the first eligible flavor that you can purchase. A flavor is considered eligible if it provides an amount of CPU and memory resources not less than the source server and within the thresholds. If no flavor is eligible, an error will be reported. If you have specific requirements for target servers (such as large memory), configure **Preferences** or select **Match business scenario** for **Assessment Policy** to obtain more accurate recommendations. **NOTICE** ● The CPU threshold is the smallest 2's power that is larger than the number of CPUs on a source server. For example, if a source server has 3 CPUs, the threshold is 4 because 4 is the smallest power of 2 greater than 3. If a source server has four CPUs, the CPU threshold is 8 because 8 is the smallest power of 2 greater than 4. ● The memory threshold is 1.5 times of the memory of a source server. For example, if the memory size of a source server is 4 GB, the memory threshold is 6, which is 1.5 times of 4. Examples: ● Assume that a source server has 6 CPUs and 8 GB of memory, and you select **Low price** for **Priority**. The FlexusX flavor **x1.6u.8g** will be recommended if it is not sold out. ● Assume that a source server has 6 CPUs and 8 GB of memory, and you select **High performance** for **Priority**. – If there is an eligible C7 flavor such as **c7.2xlarge.1** that can be purchased, this C7 flavor will be recommended. – If all eligible C7 flavors are sold out, the system will search for eligible flavors in the other General Computing-plus ECS series in descending order of performance. If no eligible flavor is found, an error will be reported.

Parameter	Option	Description
	Match business scenario	MgC recommends appropriate Huawei Cloud resources based on the business scenario of source resources and Huawei Cloud best practices. For a source server, MgC first automatically selects the instance type that matches the business scenario of the source server, and sorts all flavors of the matched instance type by price or performance as you prefer. Then it recommends the first eligible flavor that you can purchase. A flavor is considered eligible if it provides an amount of CPU and memory resources not less than the source server and within the thresholds. If no flavor is eligible, an error message is displayed. Examples: Assume that a 4U8G source server is used to run a personal application, and you select **High performance** for **Priority**. The recommendation will be limited to two instance types: FlexusX and General Computing ECS. • If the 4U8G FlexusX flavor **x1.4u.8g** can be purchased, this flavor will be recommended. • If the FlexusX flavor **x1.4u.8g** is sold out, the system will recommend another eligible FlexusX flavor that can be purchased, such as **x1.4u.10g**. • If all eligible FlexusX flavors are sold out, the system will search for eligible flavors of the General Computing ECS type. If there is an eligible General Computing ECS flavor that can be purchased, the system will recommend this flavor. If there is not, an error will be reported.
Priority	High performance	MgC recommends target resources with optimal performance.
	Low cost	MgC recommends the most cost-effective target resources that meet your demands.
Preferences	Server Types (Optional)	Select the ECS types you prefer.
	Server Series (Optional)	Select the server series you prefer. The system will generate recommendations based on your preferred server types and series. **NOTICE** If you select **Display only series allowed on DeHs**, **Server Types** will be dimmed, and the server series allowed on DeHs in the target region will be listed.

Parameter	Option	Description
	System Disk (Optional)	Select the system disk type you prefer.
	Data Disk (Optional)	Select the data disk type you prefer.

Parameter	Option	Description
	Sizing Criteria	Select the criteria that the system will follow for generating server recommendations. • If you select **As-is on source**, the recommended flavors provide at least the same amount of CPU and memory resources as source servers. – If you select your preferred server types in **Preferences**, the recommendations are limited to the server types you prefer and will be generated based on the setting of **Priority**. If no eligible flavor is found in your preferred server types, an error will be reported. – If you do not select your preferred server types in **Preferences**, the recommendations will be generated based on the settings of **Assessment Policy** and **Priority**. • If you select **Performance-based**, you need to perform a **performance collection** for the source servers, and then set assessment parameters. The system will then recommend target servers with your desired CPU and memory specifications. The more performance data is collected, the more accurate the assessment is. The collection of server performance data should take no less than seven days. The system processes the collected performance data of source servers and makes server size recommendations. The system identifies the appropriate collected data to use for rightsizing based on the percentile values for the performance history. Then the percentile values are multiplied by the comfort factors to generate recommendations. Calculation method: **Recommended number of CPUs** = CPU usage at the specified percentile x Number of CPUs on a source server x Comfort factor (rounded up) **Recommended memory size** = Memory usage at the specified percentile x Memory size of a source server x Comfort factor (rounded up) For example: Suppose that a source server has 8 CPUs and 16 GB of memory, and you set **Performance History** to **7 days**, **CPU Usage Percentile** to **100th**, **CPU Comfort Factor** to **1.2**, **Memory Usage Percentile** to **95th**, and **Memory Comfort Factor** to **1**. The system sorts performance data samples in ascending order and picks the CPU usage (for example, 40%) at the 100th percentile and the

Parameter	Option	Description
		memory usage (50%) at the 95th percentile for rightsizing. Then the recommended server size is: – 4 CPUs (rounded up from 3.8) 40% (the value at the specified percentile) x 8 (the number of the source server's CPUs) x 1.2 (the specified comfort factor) = 3.8 – 8 GB of memory 50% (the usage value at the specified percentile) x 16 (the memory size of the source server, in GB) x 1 (the specified comfort factor) = 8 Based on the **Match source configuration** assessment policy, the FlexusX instance flavor **x1.4u.8g** is recommended if it is not sold out. **CAUTION** If **Ignore Metrics with Insufficient Samples** is set to **Enable**, performance metrics with insufficient samples will not be used for rightsizing, and the corresponding configurations of source servers are retained on target servers. By default, the system collects raw performance data (samples) every five minutes. For example, theoretically, during a 7-day performance history, a total of 2,016 (7 x 288) samples can be collected for a metric. If less than 1,008 (2016 x 50%) samples are collected, the metric is marked as "insufficient samples". – If you select your preferred server types in **Preferences**, the recommendations are limited to the server types you prefer and will be generated based on the settings of **Sizing Criteria** and **Priority**. If no eligible flavor is found in your preferred server types, an error will be reported. Suppose that for an 8U16G source server, the 4U8G C7 flavor is recommended based on your preferred General Computing-plus ECS type in **Preferences** and the **Sizing Criteria** of **Performance-based**. If this C7 flavor is sold out, the next larger C7 flavor will be recommended such as the 8U8G C7 flavor. If no C7 flavor is eligible, the system will search for eligible flavors in other General Computing-plus ECS series. If no General Computing-plus ECS flavor is eligible, an error will be reported. – If you do not select your preferred server types in **Preferences**, the recommendations will be generated based the settings of **Sizing Criteria**, **Assessment Policy**, and **Priority**. Suppose that for an 8U16G source server that is used to run a personal application, a 4U8G

Parameter	Option	Description
		flavor of the General Computing ECS type is recommended based on the **Sizing Criteria** of **Performance-based**. If you set **Priority** to **High performance** and do not select your preferred server types in **Preferences**, the FlexusX flavor **x1.4u.8g** with 4U8G will be recommended if it is not sold out.

9 Big Data Migration

9.1 What Can I Do If the Data Migration Fails Because the DLI Throttling Threshold Has Been Reached?

Symptom

A big data migration task failed, and the error message "The throttling threshold has been reached" was displayed for the Spark job on DLI.

Possible Causes

The number of created resources has reached the DLI threshold.

Solution

Contact DLI technical support to adjust the threshold.

9.2 What Can I Do If Some Tables Fail to Be Migrated Due to the Error "CRC Check Failed"?

Symptom

In a big data migration task, some tables fail to be migrated, and the error message "CRC Check failed" was displayed.

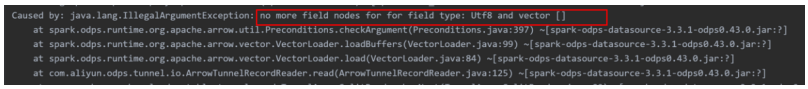
Solution

Modify the migration SQL statements of the DLI job to change the Timestamp fields at the source to String and try the migration again.

9.3 How Do I Fix the Error "no more field nodes for field %s and vector %s" When Some Tables Fail to Be Migrated?

Symptom

In a big data migration task, some tables failed to be migrated, and the error message "no more field nodes for field %s and vector %s" was displayed.



Solution

Create a temporary table based on the source table and use the temporary table to migrate data.

10 Big Data Verification

10.1 What Do I Do If the Credential List Is Empty When I Create a Data Connection for Big Data Verification?

Symptom

When you tried to create a data connection for big data verification, the credential drop-down list was empty or your credential was not found in the list.

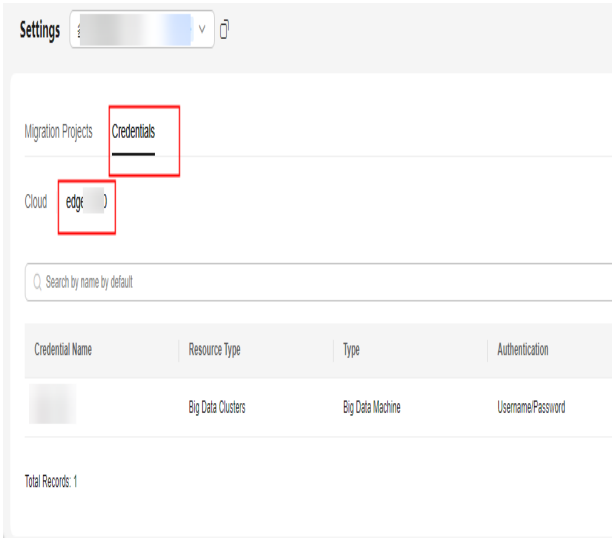
Possible Causes

The possible causes are:

- Your credential was incorrect. Specifically, the credential you added to the MgC Agent (formerly Edge) did not match the required type for the new connection.
- The credential you added to the MgC Agent was not synchronized to MgC.

Solutions

- If the credential is incorrect, go to the MgC Agent console and check whether the credential type is that required by the new connection. If the credential has not been added, add it by referring to **Adding Resource Credentials**. After the credential is added, it will be automatically synchronized to MgC.
- If the credential fails to be synchronized, go to the MgC console and choose **Settings** > **Credentials** in the navigation pane, click the MgC Agent name, and check whether the credential added to the MgC Agent can be found in the list. If the credential cannot be found, go to the MgC Agent console to synchronize the credential again. Ensure that the credential is displayed on the **Credentials** page of the MgC console.



10.2 Why Are 0 or -1 Displayed in the Hive Verification Results?

Symptom

A big data verification task for Hive was successfully executed. In the verification results, **0** or **-1** appeared in the **Source** and **Target** columns.

Possible Causes

The calculated value exceeds the range supported by Hive.

During data processing, if Hive encounters a maximum or minimum value that it cannot represent in the standard value format, these extreme values are displayed as Infinity (indicating positive infinity) or -Infinity (indicating negative infinity). These values are not valid numbers. Therefore, exceptions may occur during value conversion or calculation.

During the verification, Hive and Spark process such values in the following ways:

- If the value is Infinity or -Infinity, the value is displayed as -1 by default.
- If the value is Not a Number (NaN), it is displayed as 0 by default.

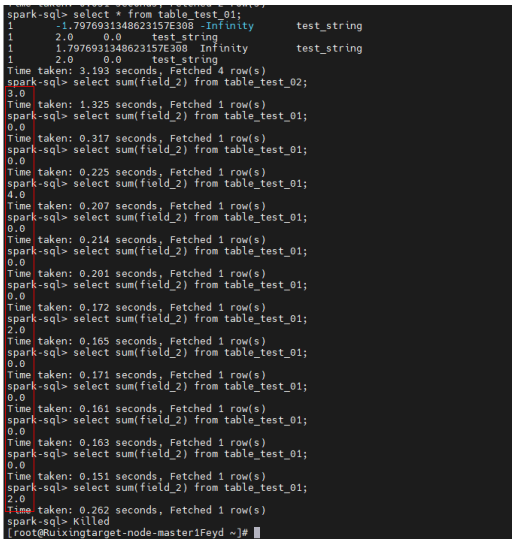
10.3 Why Does a Field in Hive Fail the Sum Verification?

Symptom

In a big data verification task for Hive, the verification rule was **sum**, and a double field that stores 1.7976931348623157E308 or -1.7976931348623157E308 failed the verification.

Possible Causes

When the Spark-SQL client is used to execute SQL statements, the returned values of the same command may be different.

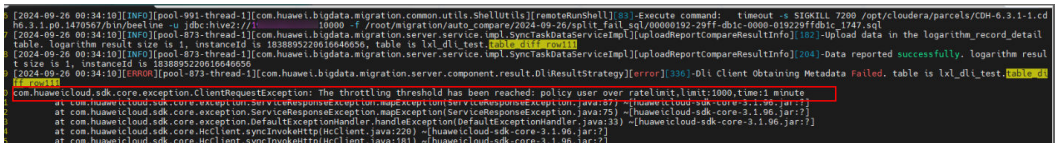


This is because in a distributed computing environment, the sequence in which calculations are performed can vary, leading to slight inconsistencies in results. During the processing of values near the maximum limit of the double type (1.7976931348623157E+308), adding even a small value like 2.0 can lead to an overflow, which essentially means the resulting value cannot be represented correctly and often just stays unchanged. It is a quirky but common phenomenon in floating-point arithmetic, due to precision limitations.

10.4 Why Do a Large Number of Tables Fail to Be Verified in a DLI Verification Task?

Symptom

When a DLI verification task is created and executed, a large number of tables fail to be verified. The figure below shows the error information in the MgC Agent (formerly Edge) logs.



Possible Causes

The number of requests reached the API request throttling threshold.

Solution

Contact technical support to increase the threshold.

10.5 How Do I Optimize the Verification Task When the Delta Lake Data Volume Is Large?

This section explores how to use MgC to verify data consistency when the source Delta Lake data volume is huge (for example, more than 10,000 tables).

Procedure

Step 1 **Create a metadata connection** to the Delta Lake cluster.

Step 2 Use the metadata connection created in **step 1** to **create a metadata synchronization task** to synchronize metadata from the source cluster to MgC.

Step 3 Create several more metadata connections to the source Delta Lake cluster using the IP addresses and ports of different executors. Keep the other parameter settings the same as the metadata connection created in **step 1**.

NOTE

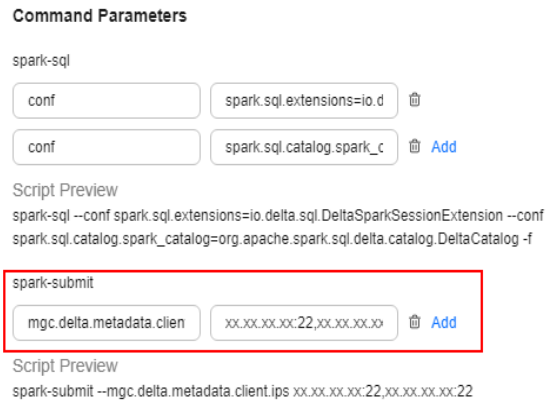
- The number of metadata connections is determined by the number of executors and tables to be verified. If the executor resources are sufficient and there are a large number of tables to be verified, increasing the number of metadata connections can improve verification efficiency.
- To avoid duplicate data, you only need to create a synchronization task using the metadata connection created in **step 1**.

Step 4 **Create a table group and add source tables to the group**. During the table group creation, select the metadata connection created in **step 1**.

Step 5 Create a connection to the source and target executors separately. For details, see **Creating an Executor Connection**.

Step 6 Create a data verification task for the source Delta Lake cluster and the target Delta Lake cluster, respectively, and execute the tasks. For more information, see **Creating and Executing Verification Tasks**. When configuring a task, in the **spark-submit** area, add parameter **mgc.delta.metadata.client.ips** and set the value to the IP addresses and ports of all metadata connections, which are separated by commas (,).

For example, mgc.delta.metadata.client.ips = xx.xx.xx.xx:22,xx.xx.xx.xx:22



----End

10.6 How Do I Replace Packages Before I Create a Connection to a Secured HBase Cluster on the Target Cloud?

Scenarios

Before you create a connection to a secured HBase cluster on the target cloud, you need to replace certain packages.

Procedure

Step 1 Replace involved packages.

1. On the server where the MgC Agent is installed, run the following command to access the specified directory of the MgC Agent:
   ```
   cd /opt/cloud/Edge/tools/plugins/collectors/bigdata-migration/hadoop3
   ```
2. Run the following command to delete the old packages from the directory:
   ```
   rm -f hadoop-s* hadoop-c* hadoop-m* hadoop-y* zookeeper-*
   ```
3. Copy the new packages from the secured cluster's client to the specified directory. Replace *xxxx@xxx.xx.xx.xx* with the username and IP address of the secured cluster.
   ```
   scp hadoop-s* hadoop-c* hadoop-m* hadoop-y* zookeeper-* xxxx@xxx.xx.xx.xx:/opt/cloud/Edge/tools/plugins/collectors/bigdata-migration/hadoop3
   ```

Step 2 Modify the permissions and owner of the new packages.

```
chmod 755 hadoop-s* hadoop-c* hadoop-m* hadoop-y* zookeeper-*
chown edge:edge hadoop-s* hadoop-c* hadoop-m* hadoop-y* zookeeper-*
```

Step 3 Restart the MgC Agent.

```
cd /opt/cloud/Edge/scripts
sh start.sh
```

----End

10.7 How Do I Replace Packages When I Create a Verification Task for an MRS 3.1.0 Cluster Using Yarn?

Scenarios

The following describes how to replace packages when you create a full or selective verification task for a HBase cluster that uses Yarn mode.

Procedure

Step 1 On the server where the MgC Agent is installed, run the following command to access the specified MgC Agent directory:

```
cd /opt/cloud/Edge/tools/plugins/collectors/bigdata-migration/hadoop3
```

Step 2 Run the following command to delete the old packages from the directory:

```
rm -f hadoop-c* hadoop-m*  hadoop-y* zookeeper-* hbase-* hadoop-h*
```

Step 3 Go to the **lib** directory of the HBase client in the cluster and run the following command to copy the new packages to the specified directory: Replace *xxxx@xxx.xx.xx.xx* with the username and IP address of the server with the MgC Agent installed.

```
scp hadoop-c* hadoop-m*  hadoop-y* zookeeper-* hbase-* opentracing-* jaeger-core-* commons-validator* hadoop-h* xxxx@xxx.xx.xx.xx:/opt/cloud/Edge/tools/plugins/collectors/bigdata-migration/hadoop3
```

Step 4 Go to the specified directory on the server with the MgC Agent installed by referring to step 1. Run the following command to change the permissions and owner for the new packages:

```
chmod 755 hadoop-c* hadoop-m* hadoop-y* zookeeper-* hbase-* opentracing-* jaeger-core-* commons-validator* hadoop-h*
chown edge:edge hadoop-c* hadoop-m* hadoop-y* zookeeper-* hbase-* opentracing-* jaeger-core-* commons-validator* hadoop-h*
```

Step 5 Restart the MgC Agent.

```
cd /opt/cloud/Edge/scripts
sh start.sh
```

----End

11 Known Issues and Solutions

Known Issues and Solutions About Server Migration Workflows

Error Code	Description	Solution
SMS-Workflow.0101	Parameter * is empty.	Check whether any recommended server parameters (image and disk) are missing, or contact MgC technical support to check whether parameter *** is empty in the workflow database.
SMS-Workflow.0102	Parameter *** contains special characters.	Contact MgC technical support to check whether parameter *** contains special characters in the workflow database.
SMS-Workflow.0103	PowerShell version must be **3.0** or later.	Open PowerShell on the server where the MgC Agent (formerly Edge) is installed and run the **$host** command to check the PowerShell version. If the current version is earlier than 3.0, you are advised to reinstall the MgC Agent on a server running Windows Server 2012 or later. Generally, Windows Server 2012 and later versions provide PowerShell 3.0 or later.
SMS-Workflow.0201	Available memory on Windows source servers must at least be 256 MB.	Run the **systeminfo** command to check available memory, release sufficient memory, and try again.
SMS-Workflow.0202	Linux source servers failed the migration feasibility check.	Find the solution based on the error code in **SMS documentation** or contact SMS technical support.

Error Code	Description	Solution
SMS-Workflow.0203	A migration program is running on a source server.	The SMS migration process is running on the source server. If you want to migrate data again, stop the migration process by running the **shutdown.sh** script in the **/root/Edge/SMS-Agent** directory on Linux or by stopping the **SMSAgentDeploy** process in the **Task Manager** on Windows. Delete the migration task on the SMS console, return to the workflow, and try the step again.
SMS-Workflow.0301	Create VM failed.	Common causes include insufficient quotas and recommended images or flavors that do not meet requirements. Locate the fault based on the error message or ECS error code.
SMS-Workflow.0302	The target VM is abnormal.	Check whether the associated target ECS is, for example, locked or frozen.
SMS-Workflow.0303	Disks not found on target VM.	Check whether the target VM has disks attached. If no, attach disks and try again.
SMS-Workflow.0304	System disk not found on target VM.	Check whether the target VM has a system disk attached. If no, attach one and try again.
SMS-Workflow.0305	Obtain IP address of target VM failed.	If you are migrating over a public network, check whether there is an EIP bound to the target VM. If there is no EIP bound, bind one and try again.
SMS-Workflow.0306	Target server does not have the same number of disks as source server.	The target server has fewer disks than the source server. Attach disks as large as the source ones to the target server. Then try again.
SMS-Workflow.0307	Target server has disks smaller than source server.	The *x*th disk (* GB) of the target server is smaller than the paired one (* GB) of the source server. Adjust the disk size of the target disk and try again.
SMS-Workflow.0308	Insufficient ECS quota. Requested: x; and Available: y	Release unnecessary ECSs or submit a service ticket to increase the quota.
SMS-Workflow.0309	Insufficient CPU quota. Requested: x; Available: y	Release unnecessary resources or submit a service ticket to increase the quota.

Error Code	Description	Solution
SMS-Workflow.0310	Insufficient memory quota. Requested: x; Available: y	Release unnecessary resources or submit a service ticket to increase the quota.
SMS-Workflow.0311	The disk type of the target server is missing. Check the disk type recommended on the "Migration Solutions" page.	Check whether the recommended target disk type is empty. If it is, assess the source server again and retry the workflow.
SMS-Workflow.0312	The disk size of the target server is missing. Check the disk size recommended on the "Migration Solutions" page.	Check whether the recommended target disk size is empty. If it is, assess the source server again and retry the workflow.
SMS-Workflow.0313	Invalid source disk IDs used for generating target recommendations. Assess the source server again.	Assess the source server and try the workflow step again. This is because if a source server is collected twice, the system generates different disk IDs for the server.
SMS-Workflow.0314	Firmware inconsistency between source and target servers.	The firmware type of the target server must be the same as that of the source server. Reconfigure the firmware type of the target server and try again.
SMS-Workflow.0315	target image ID.	Try again. If the fault persists, contact technical support or submit a service ticket.
SMS-Workflow.0401	Download SMS-Agent installation package to source server failed.	Download SMS-Agent from the SMS console, and view the error message displayed during the download. The possible causes usually are network disconnection and failed execution of the download command.

Error Code	Description	Solution
SMS-Workflow.0402	Decompress SMS-Agent installation package failed on the source server.	One possible cause is that the tar command fails to be executed. Go to the **/rda/** directory on the source server and run the **tar -zxvf SMS-Agent.tar.gz** command to view the error details.
SMS-Workflow.0403	Install SMS-Agent on Windows failed.	Check whether the **SMSAgentDeploy.exe** file is in the **C:\SMS-Agent-Py2** directory on the source server. If it is not there, delete the **SMS-Agent-Py2** folder and double-click the installation package with the same name in drive C.
SMS-Workflow.0404	Start SMS-Agent failed.	• If the reported the error message is "SMS-Agent startup failed. For details, view the SMS migration logs on the source server," go to the following directory on the source server to view SMS run logs: – Linux: /rda/SMS-Agent/agent/Logs – Windows: C:\SMS-Agent-Py2\Logs • If the reported error message is "System.OutOfMemoryException," see **What Can I Do If the StartUpAgent Step Fails and the Error Message "System.OutOfMemoryException" Is Displayed?**. • If the reported error message is " SMS-Agent startup failed, Cause: the SMS-Agent is not running, please try again", you can try again. If the retry fails, rectify the fault by referring to step 2 in **What Can I Do If the StartUpAgent Step Fails and the Error Message "System.OutOfMemoryException" Is Displayed?**. If the fault persists, contact SMS technical support to view the migration logs.
SMS-Workflow.0405	Obtain cloud-region.json failed.	Log in to the source server and view the error information in the SMS run logs located in: • Linux: /rda/SMS-Agent/agent/Logs • Windows: C:\SMS-Agent-Py2\Logs If the fault cannot be located, contact SMS technical support to view the migration logs.

Error Code	Description	Solution
SMS-Workflow.0501	Could not find the migration task on the SMS console.	Go to the SMS console and check whether the migration task has been deleted. If the migration task has been deleted by mistake, create a migration workflow again on the MgC console.
SMS-Workflow.0502	The source server is disconnected from the SMS server.	Log in to the SMS console and check whether the migration task is in the Disconnected status. If the source server runs Linux, go to the **/rda/SMS-Agent/** directory and run the **restart.sh** command to restore the connection. If the source server runs Windows, perform the migration again.
SMS-Workflow.0503	Migration task failed. SMS.xxxx	Go to the SMS console to view the error message and solution.
SMS-Workflow.0504	The migration task is paused or being paused.	Retry this step to continue the migration.
SMS-Workflow.0505	Obtain source server information failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
SMS-Workflow.0506	Obtain migration task information failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
SMS-Workflow.0507	Issue migration command failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
SMS-Workflow.0508	The current migration task is empty.	Try again. If the fault persists, contact technical support or submit a service ticket.
SMS-Workflow.0509	Delete SMS migration task failed.	Go to the SMS console and manually delete the task. After the deletion is complete, return to the MgC console and try again. **NOTICE** Only tasks in the paused, completed, or error state can be deleted.
SMS-Workflow.0510	Query migration progress failed.	Try again.

Error Code	Description	Solution
SMS-Workflow.0003	Input parameters are not in the standard JSON format.	Contact technical support or submit a service ticket to check whether the input parameters in this step are correct.
SMS-Workflow.0902	Stopping server timed out. Try again or manually stop the server and try again.	Go to the ECS console, manually stop the server, and retry the workflow. If the fault persists, contact technical support or submit a service ticket.
SMS-Workflow.0901	Failed to shut down servers in the *** status. Manually shut down the server and try again.	Go to the ECS console, manually stop the server, and retry the workflow.
SMS-Workflow.1204	Change the IP address of server *** failed. Failure cause: ***	• Failure cause: The IP address has been used. Unbind and release the private IP address and try again. If the fault persists, contact technical support or submit a service ticket. • Failure cause: The IP address is not in the subnet. Use a VPC and subnet that match the private IP address of the source server to create a migration workflow again. If the fault persists, contact technical support or submit a service ticket. • Failure cause: Success to change ip, but failed to the same private IP address as the source host Try again. If the fault persists, contact technical support or submit a service ticket. • Failure cause: Failed to switch the VPC. Try again. If the fault persists, contact technical support or submit a service ticket.
Server-Workflow.0001	Workflow step *** not found.	Contact technical support or submit a service ticket.
Server-Workflow.0002	Workflow lacks parameter ***.	Contact technical support or submit a service ticket.

Error Code	Description	Solution
Server-Workflow.0003	Workflow parameter *** contains special characters.	Contact technical support or submit a service ticket.
Server-Workflow.0004	Network error ***. Please try again.	Try again. If the fault persists, contact technical support or submit a service ticket.
Server-Workflow.0005	The Region parameter is empty.	Contact technical support or submit a service ticket.
Server-Workflow.0006	Pre-migration verification failed.	Contact technical support or submit a service ticket.
Server-Workflow.0007	An unknown error occurs during the migration.	Contact technical support or submit a service ticket.
Server-Workflow.0008	Unknown error.	Contact technical support or submit a service ticket.
Server-Workflow.0009	Clearing resources failed	Go to the CBR and IMS consoles to manually delete temporary resources (whose names start with AZM_Create_Temp__xxx), and try again.
Server-Workflow.0010	Request *** failed. Failure cause: ***. Try again.	Try again or **find a solution here**. If the fault persists, contact technical support or submit a service ticket.
Server-Workflow.0011	Query *** progress failed. Failure cause: ***	Contact technical support or submit a service ticket.
Server-Workflow.0012	Step *** is an instant action	Contact technical support or submit a service ticket.
Server-Workflow.0013	Verify template version failed.	Contact technical support or submit a service ticket.

Known Issues and Solutions About Cross-AZ Migration Workflows

Error Code	Description	Solution
AZ-Workflow.0001	Workflow step *** not found.	Contact technical support or submit a service ticket.

Error Code	Description	Solution
AZ-Workflow.0002	Workflow lacks parameter ***.	Contact technical support or submit a service ticket.
AZ-Workflow.0003	Workflow parameter *** contains special characters.	Contact technical support or submit a service ticket.
AZ-Workflow.0004	Network error ***. Please try again.	Try again. If the fault persists, contact technical support or submit a service ticket.
AZ-Workflow.0005	The Region parameter is empty.	Contact technical support or submit a service ticket.
AZ-Workflow.0006	Pre-migration verification failed.	Contact technical support or submit a service ticket.
AZ-Workflow.0007	An unknown error occurs during the migration.	Contact technical support or submit a service ticket.
AZ-Workflow.0008	Unknown error.	Contact technical support or submit a service ticket.
AZ-Workflow.0009	Clearing resources failed	Go to the CBR and IMS console to manually clear temporary resources (whose names start with AZM_Create_Temp__xxx), and try again.
AZ-Workflow.0010	Request *** failed. Failure cause: ***. Try again.	Try again. If the fault persists, contact technical support or submit a service ticket.
AZ-Workflow.0011	Query *** progress failed. Failure cause: ***	Contact technical support or submit a service ticket.
AZ-Workflow.0012	Step *** is an instant action	Contact technical support or submit a service ticket.
AZ-Workflow.0101	Source server *** not found.	Check whether the server ID is the source server ID and whether the source server can be found.
AZ-Workflow.0102	Source server *** is not ready for migration.	Check whether the source server is normal. If it is abnormal, contact ECS technical support.

Error Code	Description	Solution
AZ-Workflow.0202	AZ *** does not exist.	Delete the migration workflow, create a cross-AZ migration application, and select an available AZ.
AZ-Workflow.0201	AZ *** is unavailable.	Delete the migration workflow, create a cross-AZ migration application, and select another AZ.
AZ-Workflow.0301	Insufficient quotas.	Increase quotas and try again.
AZ-Workflow.0302	Insufficient ECS quota.	Increase the ECS quota and try again.
AZ-Workflow.0303	Insufficient vCPU quota.	Increase the vCPU quota and try again.
AZ-Workflow.0304	Insufficient memory quota.	Increase the memory quota and try again.
AZ-Workflow.0401	Flavor *** is unavailable.	Delete the migration workflow, modify the recommended target specifications, and create a migration workflow again.
AZ-Workflow.0402	Disk type *** is not available in AZ ***.	Delete the migration workflow, modify the recommended target specifications, and create a migration workflow again.
AZ-Workflow.0403	Disk type *** is sold out in AZ ***.	Delete the migration workflow, modify the recommended target specifications, and create a migration workflow again.
AZ-Workflow.0404	The source server has *** NICs. Flavor *** supports a maximum of *** NICs. Select another flavor.	Delete the migration workflow, modify the recommended target specifications, and create a migration workflow again.
AZ-Workflow.0405	Parse disk information failed.	Contact technical support or submit a service ticket.
AZ-Workflow.0406	The disk_infos parameter is empty.	Contact technical support or submit a service ticket.
AZ-Workflow.0501	Create backups failed. Failure cause: ***	Rectify the fault based on the error message. Go to the CBR console to check whether backups are created.

Error Code	Description	Solution
AZ-Workflow.0502	Unable to associate source server *** with vault ***.	Contact technical support or submit a service ticket.
AZ-Workflow.0503	Vault *** is unavailable.	Delete the vault and try again.
AZ-Workflow.0901	Failed to shut down servers in the *** status. Manually shut down the server and try again.	Go to the ECS console, manually stop the server, and retry the workflow.
AZ-Workflow.0902	Stopping server timed out. Try again or manually stop the server and try again.	Go to the ECS console, manually stop the server, and retry the workflow.
AZ-Workflow.0601	Create incremental backups failed. Failure cause: ***	Rectify the fault based on the error message, contact technical support, or submit a service ticket.
AZ-Workflow.0701	Create full-ECS image failed. Failure cause: ***	Rectify the fault based on the error message, contact technical support, or submit a service ticket.
AZ-Workflow.0801	Create target server failed. Failure cause: ***	Rectify the fault based on the error message, contact technical support, or submit a service ticket.
AZ-Workflow.0802	Servers with system disks larger than 1 TB cannot be migrated.	Contact technical support or submit a service ticket.
AZ-Workflow.0803	Invalid size of disk ***.	Contact technical support or submit a service ticket.
AZ-Workflow.0804	Source server *** not found in VPC ***.	Contact technical support or submit a service ticket.

Error Code	Description	Solution
AZ-Workflow.0805	Image *** is not found or unavailable.	Go to the IMS console to check the image status and contact IMS support to confirm whether the image can be restored automatically. If it cannot, contact technical support or submit a service ticket.
AZworflow.0901	Servers in the *** status cannot be stopped. Manually shut down servers and try again.	Go to the ECS console, manually stop the server, and retry the workflow.
AZworflow.0902	Stopping server timed out. Try again or manually stop the server and try again.	Go to the ECS console, manually stop the server, and retry the workflow.
AZ-Workflow.1001	Delete full-ECS images failed. Failure cause: ***	Go to the IMS console to manually delete these images (whose names start with AZM_Create_Temp__xxx), and try again.
AZ-Workflow.1002	Delete backups failed. Failure cause: ***	Go to the CBR console to manually delete these backups (whose names start with AZM_Create_Temp__xxx), and try again.
AZ-Workflow.1003	Delete vault *** failed. Failure cause: ***	Go to the CBR console to manually delete the vault (whose name starts with AZM_Create_Temp__xxx), and try again.
AZ-Workflow.1101	The server_id parameter is empty.	Contact technical support or submit a service ticket.
AZ-Workflow.1102	Create system disk images failed. IMS error code: ***, error message: ***	Retry the task again or contact the IMS support.
AZ-Workflow.1201	Target server has an EIP bound. Unbound the EIP and try again.	Check whether the target server has an EIP bound and whether the EIP is one bound to the source server. If it is not, unbind the EIP from the target server.

Error Code	Description	Solution
AZ-Workflow.1202	Source server *** is not stopped. Manually stop it and try again.	Check whether the source server is stopped. If it is not, stop it and try again.
AZ-Workflow.1203	Target server *** is not stopped. Manually stop it and try again.	Check whether the target server is stopped. If it is not, stop it and try again.
AZ-Workflow.1204	Change the IP address of server *** failed. Failure cause: ***	Rectify the fault based on the error message, contact technical support, or submit a service ticket.

Known Issues and Solutions About Object Storage Migration Workflows

Error Code	Description	Solution
OMS-Workflow.0002	Unknown OMS error.	Contact technical support or submit a service ticket.
OMS-Workflow.0011	System error.	Try again. If the fault persists, contact technical support or submit a service ticket.
OMS-Workflow.0013	Invalid request parameters.	Rectify the fault based on the error message. For example: If the error message is "The maxSubtaskNum more than node * 10," **add migration nodes** to the migration cluster and try again.
OMS-Workflow.0018	The project ID is different from that in the token.	Check whether the right project ID or token is used.
OMS-Workflow.0019	The region in the token is different from the region where the migration cluster is located.	Use the token of the region where the migrated cluster is located.

Error Code	Description	Solution
OMS-Workflow.0023	Abnormal node.	Check whether the ports allowed by the security group rules of the cluster node meet the requirements. For details about the requirements, see: **Migration Cluster Resources and Settings**
OMS-Workflow.0024	Cluster not found.	Check whether the cluster is in the cluster list.
OMS-Workflow.0025	Node not found.	Check whether the node exists in the corresponding cluster.
OMS-Workflow.0026	Task not found.	Check whether the task exists in the task list.
OMS-Workflow.0201	Create cluster failed.	Rectify the fault based on the keywords in **ErrorReason**. Generally, the fault is caused by insufficient resources or permission issues. **ECS Error Codes**, **VPC Error Codes**, **NAT Gateway Error Codes**, **VPCEP Error Codes**, and **LTS Error Codes**
OMS-Workflow.0202	Workflow creation failed.	Rectify the fault based on the keywords in **ErrorReason**. Generally, the fault is caused by insufficient resources or permission issues. **ECS Error Codes**, **VPC Error Codes**, **NAT Gateway Error Codes**, **VPCEP Error Codes**, and **LTS Error Codes**
OMS-Workflow.0501	Cluster deletion failed.	Rectify the fault based on the keywords in **ErrorReason**. Generally, the fault is caused by the failure to clear some resources due to permission issues. **ECS Error Codes**, **VPC Error Codes**, **NAT Gateway Error Codes**, **VPCEP Error Codes**, and **LTS Error Codes**
OMS-Workflow.0401	Execute migration task failed. Some objects might fail to be migrated.	If the error message is "Migration failed. Failure files exist," rectify the fault by referring to **Error Codes**.
OMS-Workflow.0402	Migration task execution failed.	Rectify the fault based on the exception cause. If the fault persists, contact technical support or submit a service ticket.

Error Code	Description	Solution
OMS-Workflow.0601	Delete task failed.	Rectify the fault based on the cause. If the fault persists, contact technical support or submit a service ticket.
OMS.01001	Local data write failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
OMS.01002	An exception occurred when local data uploaded to external storage device.	Try again. If the fault persists, contact technical support or submit a service ticket.
OMS.01003	Migration source or target unavailable.	Check the connection settings for source and target.
OMS.01006	Object list file too large.	Make sure that the list file does not exceed 300 MB.
OMS.01007	Metadata of object list file not found.	Check the metadata of the list file.
OMS.01008	URL decoding failed.	Check whether the URLs in the list file are correctly encoded.
OMS.01009	Invalid resource path.	Check whether the list file path is correct.
OMS.01012	List file not found.	Check whether the list file exists.
OMS.01015	Read list file failed.	Check the status of the list file and ensure that the file is readable. If the file is normal and readable, try again. If the fault persists, contact technical support or submit a service ticket.
OMS.01016	Maximum rows (100,000) reached for list file.	Modify the list file to ensure that the number of rows is less than 100,000.
OMS.01017	Content-Type of list file must be text/plain.	Check whether the list file is in TXT format and whether the Content-Type metadata is text/plain.
OMS.01018	Content-Encoding of list file not empty.	Ensure that the Content-Encoding attribute is empty.

Error Code	Description	Solution
OMS.01019	Download list failed.	Check the status of the list file and ensure that the file is readable. If the file is normal and readable, try again. If the fault persists, contact technical support or submit a service ticket.
OMS.01020	Read block file failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
OMS.01021	Listing failed object lists failed.	Check whether the failed object lists can be found. If they can, create a migration workflow again.
OMS.01023	List file must be TXT.	Ensure that the list file is a .txt file.
OMS.01024	Maximum list files (10,000) exceeded.	Ensure that the number of list files in the specified path is less than 10,000.
OMS.01025	Save task information failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
OMS.04002	List files failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
OMS.04003	Start migration failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
OMS.04006	Execute migration task failed.	Check the list of failed objects to determine the failure cause.
OMS.03003	AK/SK verification failed. Ensure AK/SK is valid.	Check whether the AK/SK pairs for accessing the source and the target are correct.
OMS.03004	List objects failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
OMS.03005	List buckets failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
OMS.03009	Source CDN verification failed.	Check whether the CDN configuration is correct.
OMS.03010	Run mount failed.	Check the connection or network settings.
OMS.03011	Write data to stream failed.	Try again. If the fault persists, contact technical support or submit a service ticket.

Error Code	Description	Solution
OMS.03015	SMB connection failed.	Check the connection or network settings.
OMS.03021	Execute command failed.	Check the connection settings for the NAS server or the network settings.

Known Issues and Solutions About MgC

Error Code	Description	Solution
MgC.00030101	Unknown error.	There are many possible causes for this error, for example, the network could be abnormal. Try this workflow step again. If the fault persists, contact technical support or submit a service ticket.
MgC.00010532	Involved collection task not found.	Associate the collection item with another collection task.
MgC.00010533	Add data source failed.	Contact technical support or submit a service ticket.
MgC.00010534	Data source not found.	Refresh the collection item list and check whether the data source exists.
MgC.00000101	Could not collect information from Alibaba Cloud RM.	Debug API SearchResources by following the instructions provided in the Alibaba Cloud Resource Management Documentation and locate the fault cause based on the returned error code, or contact Alibaba Cloud technical support.
MgC.00000102	Could not collect information from Alibaba Cloud RM.	Debug API GetResourceConfiguration by following the instructions provided in the Alibaba Cloud Resource Management Documentation and locate the fault cause based on the returned error code, or contact Alibaba Cloud technical support.
MgC.00000103	Credential not found.	Check whether the selected credential can be found on the Credentials page.
MgC.00000104	Credential expired.	Update the credential on the Credentials page.

Error Code	Description	Solution
MgC.00000105	Wrong credential type. Select AK/SK credentials.	Select AK/SK credentials.
MgC.00000106	Incorrect file format.	Upload a file in the correct format.
MgC.00000107	Could not query domain names in pagination mode.	Debug API DescribeDomains by following the instructions provided in the Alibaba Cloud Resource Management Documentation and locate the fault cause based on the returned error code, or contact Alibaba Cloud technical support.
MgC.00000108	Could not query DNS records in pagination mode.	Debug API DescribeDomainRecords by following the instructions provided in the Alibaba Cloud Resource Management Documentation and locate the fault cause based on the returned error code, or contact Alibaba Cloud technical support.
MgC.00000109	Could not invoke the Alibaba Cloud WAF SDK.	Debug API DescribeDomains by following the instructions provided in the Alibaba Cloud Resource Management Documentation and locate the fault cause based on the returned error code, or contact Alibaba Cloud technical support.
MgC.00000110	Create Alibaba Cloud SLB SDK client failed.	Check whether the selected credential and regions are correct.
MgC.00000111	Uploaded file contains invalid data.	Enter valid values.
MgC.00000112	Uploaded file failed the verification.	Contact technical support or submit a service ticket.
MgC.00000113	Required fields are missing in uploaded file.	Specify required fields.

Error Code	Description	Solution
MgC.00000114	Table headers of uploaded file are incorrect.	Enter a correct table header.
MgC.00000115	Table headers of uploaded file are invalid.	Check whether non-customized table headers in the template have been modified.
MgC.00000116	Unexpected domain names found in "Domain" sheet.	Ensure that domain names entered in the "Application" and "MQ" sheets have been entered in the "Domain" sheet.
MgC.00000117	Invalid file content.	Check whether the import template was modified or download the template again.
MgC.00000200	File upload failed.	Contact technical support or submit a service ticket.
MgC.00000201	File download failed.	Contact technical support or submit a service ticket.
MgC.00000202	Uploaded file not found or expired.	Upload a new file, or rename the file and upload it again.
MgC.00020321	Server assessment failed. Matched target specifications not found in target AZ.	Handle this issue by referring to **What Can I Do If a Server Assessment Fails and the System Displays a Message Indicating No Proper Specifications Are Matched?**
MgC.00030142	Daily workflow quota exhausted.	Switch to another project or delete a completed workflow in the current project.
MgC.00030143	Maximum resources for a workflow reached.	Ensure that no more than 100 resources are included in the workflow.

Error Code	Description	Solution
MgC.01000004	Call FunctionGraph APIs failed. Try again later.	Try again. If the fault persists, contact technical support or submit a service ticket.
MgC.00000015	Deliver command to MgC Agent failed.	Check the MgC Agent (formerly Edge) logs. If the MgC Agent logs record "channel is not opened," the network connection between the MgC Agent and the source server is abnormal. Check and restore the network connection and try again. The MgC Agent log files are located at: • Linux: **/opt/cloud/Edge/logs/the MgC Agent-server/run.log** • Windows: **C:\Edge\logs\the MgC Agent-server\run.log**
MgC.00000045	Command execution by MgC Agent timed out.	This issue is usually caused by network connection problems. Check whether the network settings of the source server meet the **requirements**. Alternatively, view the MgC Agent (formerly Edge) logs to locate the fault. The logs are located at: • Linux: **/opt/cloud/Edge/logs/the MgC Agent-server/run.log** • Windows: **C:\Edge\logs\the MgC Agent-server\run.log**

Known Issues and Solutions About Resource Assessment

Error Code	Description	Solution
MgC.00000001	Network connection error.	Try again. If the fault persists, contact technical support or submit a service ticket.
MgC.00000002	Invalid token.	Obtain a valid token.
MgC.00000003	Invalid HTTP request method or URL.	Verify that the HTTP request method and URL are correct.
MgC.00000004	Invalid parameter value.	Check the parameters and try again.
MgC.00020201	Server assessment failed. Obtain ECS flavors failed.	Try again. If the fault persists, contact technical support or submit a service ticket.

Error Code	Description	Solution
MgC.00020202	Server assessment failed. Source server ID not found.	The source server ID is missing. Perform a deep collection for the server and try again.
MgC.00020203	Server assessment failed. Query IMS images failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
MgC.00020204	Query EVS disk types failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
MgC.00020205	No EVS disk types match source server.	Modify the assessment policy and try again.
MgC.00020206	Query IMS images failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
MgC.00020207	Disk type matching source server sold out in target region.	Modify the assessment policy and try again.
MgC.00020208	Query EVS AZ availability failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
MgC.00020209	Source server runs Windows. Matched target specifications do not support Windows.	Modify the assessment policy and try again.
MgC.00020210	Source server runs Linux. Matched target specifications do not support Linux.	Modify the assessment policy and try again.
MgC.00020211	No images match source server specifications.	Query IMS images failed. Try again. If the fault persists, contact technical support or submit a service ticket.
MgC.00020007	Server assessment failed. Source disk information is missing.	The source server disk information is missing. Perform a deep collection for the server and try again.
MgC.00020212	Server assessment failed. Invalid source disk IDs.	The disk IDs of the source server are invalid. Perform a deep collection for the server and try again.
MgC.00020213	Source server being assessed. You cannot assess it again now.	The assessment is in progress. Try again after the current assessment is complete.

Error Code	Description	Solution
MgC.00020214	Server assessment results not found.	Try again. If the fault persists, contact technical support or submit a service ticket.
MgC.00020215	Modify server assessment results failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
MgC.00020216	Modify server assessment results failed. Specifications not found.	Try again. If the fault persists, contact technical support or submit a service ticket.
MgC.00020217	Modify server assessment results failed. No images match.	Try again. If the fault persists, contact technical support or submit a service ticket.
MgC.00020218	Modify server assessment results failed. Disk size too large.	Downsize disks and try again.
MgC.00020219	Failed to create an assessment for cross-AZ migration. Target AZ is missing.	Select a target AZ and try again.
MgC.00020220	Source server is already in target AZ.	Select another AZ and try again.
MgC.00020221	Selected OS is different from source OS.	Select another OS and try again.
MgC.00020222	Image not available.	Selected image has been taken offline. Select another one and try again.
MgC.00020223	Modify server assessment results failed. Specified disk size cannot be smaller than source disk size.	Modify the disk size.
MgC.00020229	Server assessment failed. Source server specifications information is missing.	The source server specifications information is missing. Perform a deep collection for the server and try again.
MgC.00020230	Server assessment failed. No proper target specifications.	Modify the assessment policy and try again.

Error Code	Description	Solution
MgC.00020231	Server assessment failed. No target specifications meet assessment policy.	Modify the assessment policy and try again.
MgC.00020232	Server assessment failed. No proper target specifications meet your preferences.	Modify the assessment policy and try again.
MgC.00020233	Server assessment failed. No target specifications meet business scenario.	Modify the assessment policy and try again.
Sms.00070040	Source performance data is missing. Perform a performance collection for source server.	Source server performance data is missing. Perform a deep collection for the server and try again.
Sms.00070041	Source server performance data is missing. Perform a performance collection for source server.	The source server's performance data is missing. Perform a deep collection for the server and try again.
Sms.00070042	Incorrect CSV file of server performance data.	Launch a performance collection for the server and try again.
MgC.00071042	Your preferences could not be met.	Selected disk type not available in current region. Modify the assessment policy and try again.
MgC.00071072	Server assessment failed. Matched target specifications not found in target AZ.	Select a target AZ and try again. or manually **modify the target specifications**.
MgC.00071066	Source server specifications are not supported. Manually associate an existing target server.	Associate an existing target server.
MgC.00070049	Server assessment failed.	Try again. If the fault persists, contact technical support or submit a service ticket.
MgC.00020271	Flavor abandoned.	Change the specifications and try again.

Error Code	Description	Solution
MgC.00020272	The flavor does not support the disk type.	Change the flavor or disk type and try again.
MgC.00020345	Server purchase failed.	Rectify the fault based on the returned error information. If the fault persists, contact technical support or submit a service ticket.
MgC.00020346	Network connection error.	Try again. If the fault persists, contact technical support or submit a service ticket.

Known Issues and Solutions About Resource Discovery

Error Code	Error Cause	Solution
MgC.00000001	Network connection error.	Check the network connection and try again.
MgC.00000020	Parameters do not match.	Check parameter settings and try again.
MgC.00000022	Decrypt data failed.	Try again later. If the fault persists, contact technical support or submit a service ticket.
MgC.00000300	Send message to device failed.	Ensure that the device is online.
MgC.00000129	Access Huawei Cloud APIs failed. Check the network.	Check whether the network connection is normal and try again.
MgC.00000130	Incorrect IAM authentication information. Check the AK/SK pair.	Check if the AK/SK pair is correct and up-to-date.
MgC.00000131	Create client on Huawei Cloud failed.	Ensure that all settings are correct and try again.
MgC.00000132	Access key not found or disabled.	Check whether the access key is correct and enabled.
MgC.00000136	Request failed. Temporary server error.	Wait until the server recovers and try again.
MgC.00000138	Request signature does not meet Alibaba Cloud requirements.	Ensure that your request signature meets Alibaba Cloud requirements and try again.

Error Code	Error Cause	Solution
MgC.00000139	Specified signature does not match calculated result.	Check your signature and try again.
MgC.00000140	Other exceptions.	Wait until the server recovers and try again.
MgC.00000144	Other exceptions.	Wait until the server recovers and try again.
MgC.00000145	File parsing failed.	Ensure that the file format and content are correct and try again.
MgC.00000146	Request to Alibaba Cloud APIs denied due to flow control.	Try again later.
MgC.00000148	Check proxy settings.	Ensure that the proxy server is configured correctly.
MgC.00000149	Create client on Huawei Cloud failed.	Ensure that all settings are correct and try again.
MgC.00000150	Request to Huawei Cloud APIs denied due to flow control.	Try again later.
MgC.00000156	Insufficient permissions.	Ensure that you have the required permissions.
MgC.00000161	Collector server error.	Try again later. If the fault persists, contact technical support or submit a service ticket.
MgC.00010526	Execute analysis task failed.	Try again later. If the fault persists, contact technical support or submit a service ticket.
MgC.00010527	Task execution timed out.	Try again later. If the fault persists, contact technical support or submit a service ticket.
MgC.00000163	Request redirected by source. Try again.	Try again later. If the fault persists, contact technical support or submit a service ticket.
MgC.00000103	Credential not found.	Upload the right credential.
MgC.00000104	Credential expired.	Upload a valid credential.
EDGE.00170020	Resource collection failed. Credential not found.	Upload the right credential.

Error Code	Error Cause	Solution
EDGE.00170021	Credential expired.	Upload a valid credential.
EDGE.00170024	The MgC Agent does not support collection using cloud credentials.	Use a valid credential.
EDGE.00170025	Resource collection failed. IP address does not match network range specified for credential.	Upload a credential that matches the IP address range.
EDGE.00260003	Incorrect username or password, or mismatch between IP address and username/password pair.	Check whether the username and password are correct and whether they match the IP address. Ensure that the IP address is correct and try again.
EDGE.00030022	Collector not installed.	Install the MgC Agent (formerly Edge) collector.
EDGE.00030023	The collector is offline.	Check whether the MgC Agent (formerly Edge) collector is online.
SERVER.00000002	Invalid IP address or WinRM not running.	Check whether WinRM is started using winrm quickconfig on the source server.
SERVER.00000003	Incorrect username or password, or mismatch between IP address and username/password pair.	Ensure the username and password are correct and they match the IP address.

Error Code	Error Cause	Solution
SERVER.00000006	Collect required information failed. Check whether .Net Framework, WMI, and COM on the source server are damaged.	Check whether necessary WMI classes are missing in the Windows system. If the WMI classes are missing, rectify the fault or reconfigure the WMI classes. After the fault is rectified, perform a deep collection again. The necessary WMI classes include: • Win32_Processor • Win32_Computersystem • Win32_DiskPartition • Win32_Volume • Win32_DiskDrive • Win32_networkadapterconfiguration • Win32_OperatingSystem • Win32_Service • Win32_PerfFormattedData_PerfDisk_PhysicalDisk • Win32_PerfFormattedData_PerfOS_Processor
SERVER.00010002	SSH connection failed. Incorrect username or password, or unreachable IP address.	Ensure that the username, password, and IP address are correct.
PLATFORM.00070003	Incorrect username or password.	Check whether your username and password are correct.
PLATFORM.00070002	Access vCenter failed. Check whether the IP address and credential are correct.	Check whether the vCenter IP address and credential are correct and whether the network connection is normal.

Known Issues and Solutions About the MgC Agent (Formerly Edge) for Windows

Error Code	Description	Solution
EDGE.00000001	Unknown error.	There are many possible causes for this error, for example, the network could be abnormal. Try this workflow step again. If the fault persists, contact technical support or submit a service ticket.

Error Code	Description	Solution
EDGE.00260001	Source IP address unreachable.	Check whether the access IP address is correct.
EDGE.00260002	Source WinRM unreachable.	Check whether WinRM is started or whether the port is being listened on. You can check that using the following PowerShell command on the source server: `winrm fastconfig`
EDGE.00260003	Invalid source credential.	Check whether the credential provided to the MgC Agent (formerly Edge) is correct.
EDGE.00260004	Insufficient credential permissions.	Check whether the account is in the administrator user group.
EDGE.00260005	Access source WinRM failed.	Check whether the firewall on the source server is disabled.
EDGE.00260006	Necessary components not found at source.	Check whether .NET Framework, WMI, and COM on the source server are damaged.
EDGE.00260007	Edge does not trust source server.	Run the following command on the server where the MgC Agent (formerly Edge) is installed to trust the source server: `set-item wsman:localhost\\client\\trustedhosts -value *`

Known Issues and Solutions About the MgC Agent (Formerly Edge) for Linux

Error Code	Description	Solution
EDGE.00261001	Source IP address unreachable.	Check whether the access IP address is correct.
EDGE.00261002	Source port unreachable.	Check whether the source port can be reached using telnet.
EDGE.00261003	SSH connection to source server failed.	Rectify the fault based on the error message. If the fault persists, contact technical support or submit a service ticket.
EDGE.00261004	Invalid source credential.	Check whether the credential provided to the MgC Agent (formerly Edge) is correct.

Error Code	Description	Solution
EDGE.00261005	Source SFTP unavailable.	Check whether the MgC Agent (formerly Edge) server can access SFTP on the source server.
EDGE.00261006	Source account directory not found.	Check whether the source account directory exists.
EDGE.00261007	tty for running sudo is not disabled.	Comment out the following default values in the source configuration file: **requiretty** in the **user!/etc/ssh/sshd_config** file or **Defaults requiretty** in the **/etc/sudoers** file

Issues About Other Cloud Services

Error Code	Description	Solution
Ecs.0319	Insufficient resources for this ECS flavor.	Go to the **Migration Solutions** or **Migration Plans** page, modify the target server specifications or use an existing server as the target server. Then try the workflow again.
Ecs.0707	Target server flavor not found or unavailable.	Go to the **Migration Solutions** or **Migration Plans** page, modify the target server specifications or use an existing server as the target server. Then try the workflow again.
Vpc.0702	Invalid parameters.	Check whether the parameter values are valid based on the returned error message. For more information, see: **VPC Error Codes**

