Migration Center

Product Introduction

Issue 02

Date 2024-02-29

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Security Declaration

Vulnerability

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

Contents

1 What Is Migration Center?

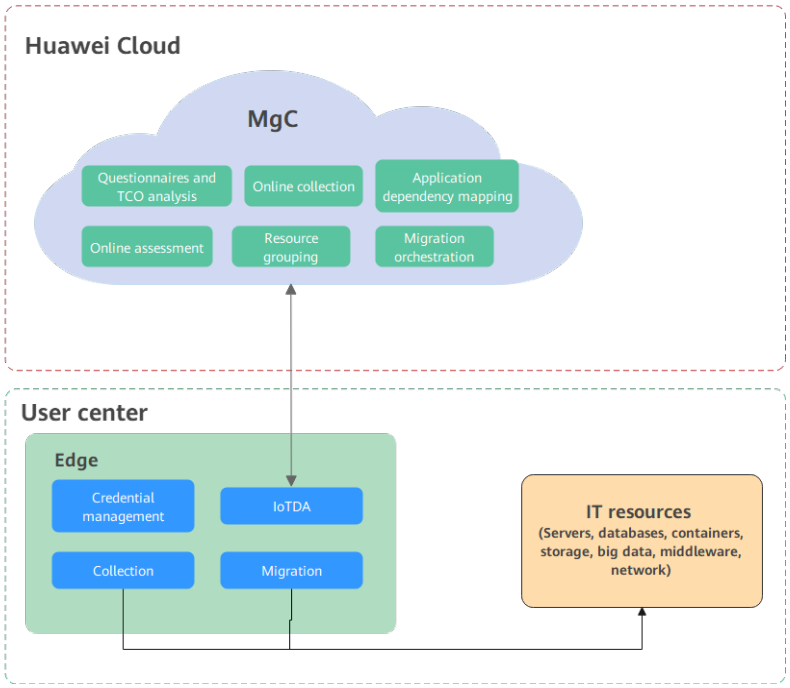
Migration Center (MgC) provides a single place for you to easily migrate, modernize, and optimize your applications using tools built based on Huawei Cloud migration methodologies and best practices.

MgC Architecture

The MgC service consists of two parts: MgC and Edge. The former is a cloud service deployed on Huawei Cloud, and the latter is a program you deploy in your source environment.

- MgC provides six service-based functions: pre-migration assessment and TCO analysis, online collection, application dependency analysis, online assessment, resource grouping, and migration orchestration.
- Edge is used to store sensitive data, such as user credentials, locally and perform operations on your local resources. Edge also executes commands from MgC and reports command execution results to MgC.

Figure 1-1 MgC architecture



2 Why MgC?

High Efficiency

MgC integrates varied migration services of Huawei Cloud to provide one-stop migration and unified management capabilities. It also provides migration workflow templates. You can easily and quickly create migration workflows for different migration scenarios, improving cloud migration efficiency.

Multi-Source Collection

MgC can collect information about various types of resources, including cloud platforms, servers, databases, containers, big data, and middleware. MgC then recommends right-sized Huawei Cloud resources and migration strategies based on the information that was collected.

Visualized Management

MgC allows you to monitor and manage the entire migration progress visually and in real time.

High Security

- Data collection

  To ensure the security of collected data, MgC only reads data from the source. It does not modify the data. In addition to online collection, you can also import information about your source environment to MgC.

- Data transfer

  MgC uses HTTPS and SSH to encrypt transmission and ensure data security.

- Credential encryption

  Credentials used for online collection are encrypted and stored on the MgC server. If you choose to deploy Edge in your source environment to collect data, your credentials are encrypted and stored on the local Edge server.

3 When to Use MgC

Application Assessment

MgC enables you to assess your applications regardless of if they are running in on-premises or cloud environments, and it visualizes application architectures and dependencies into graphs to help you develop migration plans.

One-stop Batch Migration

MgC provides flexible, customizable migration workflows and integrates migration tools such as Server Migration Service (SMS), Object Storage Migration Service (OMS), and Data Replication Service (DRS), helping you launch migrations in batches.

Cross-AZ migration

MgC enables you to migrate Elastic Cloud Servers (ECSs) across AZs within a region to help you integrate resources and switch services between AZs with ease.

Storage Migration

MgC allows you to quickly, easily migrate data to Huawei Cloud, from object storage to file storage, or from file storage to object storage. The choice is yours.

4 Functions

TCO Analysis

- MgC allows you to compare the Total Cost of Ownership (TCO) of your source environment with what it would be for running on Huawei Cloud by automatically analyzing the past bills for source resources and comparing them to the prices of mapped target resources.
- MgC enables you to learn about the TCO of your on-premises or cloud environment and what it would be if you migrate to Huawei Cloud. You can quickly obtain the list of Huawei Cloud resources and the cost model, helping you make decisions on cloud migration.

Application Dependency Mapping

- By creating an application dependency analysis task, you can automatically collect global resources in your source environment.
- You can learn the call chains of microservices by collecting information about the collection registration center, configuration center, and CMDB. More collection items means a more complete view of dependencies between applications and data. This can help you group source resources more efficiently.
- MgC provides architecture diagrams and dependency maps to visualize the associations between applications and the organizational structures of applications, helping you analyze resources and design solutions.
- MgC allows you to import and export resource details in batches.

Resource Assessment and Recommendations

MgC collects information about source servers, databases, and object storage resources and analyzes the associations between applications, so that it can recommend the best-fit Huawei Cloud resources. Recommendations are based on the specifications, performance data, and scenarios of the source resources, and your other requirements on, for example, cost, availability, performance, security, and compliance. You can export the assessment results as needed.

Migration Workflow Templates

MgC provides migration workflow templates summarized from best practices for batch server migration, cross-AZ ECS migration, and storage migration. You can

use these templates to create migration workflows for different migration scenarios. You can customize a workflow by inserting customized stages and steps to it. You can run all tasks in just one click and monitor the migration progress in real time.

5 Disclaimer

- License invalidity

  After OSs, applications, and files on source servers are migrated to target servers, the SIDs and MAC addresses of the servers will change. This means that some OS or application licenses may become invalid. SMS is not responsible for this type of issue. You can use the license server on Huawei Cloud to obtain new Windows OS licenses and update or obtain application licenses at your own expense.

- Source disk data security

  SMS does not monitor data in source disks during the migration. You need to ensure the security of your source disk data yourself. If the target servers or servers in the same VPC as the target servers are infected by any Trojans or viruses migrated from the source servers, SMS is not responsible for such problems.

- Driver unavailability

  To ensure a successful migration, KVM drivers must be installed on source servers using Xen before the migration. To learn how to install KVM drivers, refer to **Installing KVM Drivers**. If any target server fails to start due to the missing of KVM drivers after the migration is complete, MgC is not responsible for such problems.

6 Billing

MgC is available free of charge. You need to pay for migration resources you consume.

Server Migration

During server migrations from on-premises or other clouds, you are billed at standard rates for resources used in the migrations. For details, see **SMS Billing**.

Storage Migration

During object storage migrations, public APIs of Huawei Cloud and source cloud vendors are called, and additional fees are applied. For details, see **OMS Billing**.

Migration Clusters

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

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

Cross-AZ Migration

During cross-AZ migrations of ECSs, you need to pay for ECS, Image Management Service (IMS), and Cloud Backup and Recovery (CBR) resources used during the migrations.

- CBR vaults

  During a cross-AZ migration of ECSs, if no vault is configured to the source ECSs, MgC creates a vault 1.5 times the size of the source ECS disks for storing

backups created for source ECSs. The vault will be automatically deleted after the migration is complete.

For the pricing details about CBR, see **CBR Billing**.

- Images

  During a cross-AZ migration, full-ECS images are created for source ECSs.

  For pricing details about IMS, see **IMS Billing**.

- Target ECSs

  MgC cannot migrate source servers to existing ECSs. It creates pay-per-use ECSs as the target servers. After the service cutover is complete, you can change the billing mode of target ECSs from pay-per-use to yearly/monthly.

  For the pricing details of pay-per-use ECSs, see **Pay-per-Use Billing**.

⚠ CAUTION

- The prices listed in the documentation are estimates only. The actual prices may vary.

7 Permissions Management

If you need to assign different permissions to employees in your enterprise to access your MgC resources, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control. It makes it easier to secure access to your resources.

With IAM, you can use your account to create IAM users, and assign permissions to the users to control their access to specific resources. For example, you can create IAM users for software developers and grant them the permissions required for using MgC resources but not the permissions needed for performing any other operations.

If your account does not require individual IAM users for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account. For more information about IAM, see **IAM Service Overview**.

MgC Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups they have been added to and can then perform specified operations on cloud services.

You can grant permissions using roles and policies.

- Roles: A coarse-grained authorization method where you assign permissions based on user responsibilities. Only a limited number of service-level roles are available for authorization. When using roles to grant permissions, you must also assign other roles that the permissions may depend on. Roles are not ideal for fine-grained authorization and access control.
- Policies: A fine-grained authorization tool that defines permissions for operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for maintaining the principle of least privilege.

Table 7-1 lists all the system policies supported by MgC.

Table 7-1 System-defined policies supported by MgC

Policy Name	Description	Policy Type	Policy Content
MgC FullAccess	Administrator permissions of MgC. Users with these permissions can perform all operations on MgC data.	System-defined policy	**MgC FullAccess Policy Content**
MgC ReadOnlyAccess	Read-only permissions for MgC. Users with permissions can only view MgC data.	System-defined policy	**MgC ReadOnlyAccess Policy Content**
MgC DiscoveryAccess	Permissions for resource discovery of MgC. Users with these permissions can use the resource discovery function of MgC and view MgC data.	System-defined policy	**MgC DiscoveryAccess Policy Content**
MgC AssessAccess	Permissions for application assessment of MgC. Users with these permissions can use the resource discovery and application assessment functions of MgC and view MgC data.	System-defined policy	**MgC AssessAccess Policy Content**
MgC MigrateAccess	Permissions for application migration of MgC. Users with these permissions can use the resource discovery, application assessment, and application migration functions of MgC and view MgC data.	System-defined policy	**MgC MigrateAccess Policy Content**
MgC AppDiscoveryAccess	Permissions for application discovery of MgC. Users with these permissions can use the application discovery and resource discovery functions of MgC and view MgC data.	System-defined policy	**MgC AppDiscoveryAccess Policy Content**
MgC MrrAccess	Permissions for service verification of MgC. Users with these permissions can use the service verification function of MgC and view MgC data.	System-defined policy	**MgC MrrAccess Policy Content**

Table 7-2 lists the common operations supported by each system-defined policy of MgC. Select the policies as required. For details, see **Creating a User and Granting Permissions**.

Table 7-2 Common operations supported by each MgC system-defined policy

Operation	MgC FullAccess	MgC ReadOnlyAccess	MgC DiscoveryAccess	MgC AssessAccesss	MgC Migrate Access	MgC AppDiscoveryAccess
Performing operations on MgC resources	√	x	x	x	x	x
Viewing MgC resources	√	√	√	√	√	√
Discovering resources	√	x	√	√	√	√
Assessing applications	√	x	x	√	√	x
Migrating applications	√	x	x	x	√	x
Discovering applications	√	x	x	x	x	√

MgC FullAccess Policy Content

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

MgC ReadOnlyAccess Policy Content

```
{
   "Version": "1.1",
   "Statement": [
      {
```



```
            "Effect": "Allow",
            "Action": [
                "mgc:*:query*"
            ]
        }
    ]
}
```

MgC DiscoveryAccess Policy Content

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

MgC AssessAccess Policy Content

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

MgC MigrateAccess Policy Content

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

MgC AppDiscoveryAccess Policy Content

```
{
    "Version": "1.1",
    "Statement": [
        {
```



```
        "Effect": "Allow",
        "Action": [
            "mgc:*:query*",
            "mgc:*:discovery",
            "mgc:*:appdiscovery"
        ]
    }
  ]
}
```

MgC MrrAccess Policy Content

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


8 Constraints

This section describes constraints on using MgC.

Table 8-1 Restrictions on using MgC

Item	Constraint
Server migration workflows	• Each server can be migrated by only one workflow. • Server migration workflows cannot migrate servers that boot using UEFI and have no targets associated. To migrate such servers using a workflow, associate them with existing UEFI servers on Huawei Cloud in advance. You can also use the Server Migration Service (SMS) to migrate such servers. • **SMS constraints** also apply to server migration workflows. • To migrate a server again, you need to stop the workflow, stop the SMS-Agent process on the server, delete the server record from the SMS console, and create a new workflow.
Resource assessment and recommendations	• Target servers must have disks as least as large as source servers. • Target servers must have the same type of OS as source servers. • There must be a sufficient quota of recommended disk types in the target region.
Migration prerequisite	All servers have been assessed or associated with target servers.
Precautions during migration	After a migration workflow is created, the source servers must not be stopped or restarted, and disks on the source servers must not be changed. Otherwise, the migration will fail.

Item	Constraint
Source server settings	Any firewall or antivirus software must be stopped and WinRM must be started on Windows source servers. You can run **winrm quickconfig** check the WinRM settings.
Network connectivity	Source servers must be able to access target servers. Port 22 must be opened on Linux target servers, and ports 22, 8899, and 8900 must be opened on Windows target servers.
Servers where Edge is installed	• You are advised to prepare a Windows server for installing Edge in the source environment. The Windows server must be able to access the Internet. • The PowerShell version of the Windows server where the Edge is installed must be later than 4.0. You can run the **$host** command in the PowerShell command window to view the version.

9 Related Services

The following table describes how MgC interacts with other services.

Table 9-1 Relationships between MgC and other services

Service	Interaction
SMS	SMS is integrated with MgC to migrate applications and data from other clouds to Huawei Cloud.
IAM	IAM provides the following functions: • User authentication • Permissions management • Permission delegation
IoT Device Access (IoTDA)	IoTDA enables secure, real-time bidirectional communication between MgC and the Edge. It delivers commands for managing plug-ins, credentials, and collection and migration tasks from MgC to the Edge. It also synchronizes source information collected by the Edge to MgC.
OMS	OMS is integrated with MgC to migrate data from object storage on other cloud platforms to OBS on Huawei Cloud.
Cloud Backup and Recovery (CBR)	CBR backs up Elastic Volume Service (EVS) disks and Elastic Cloud Servers (ECSs) for fault recovery.
Image Management Service (IMS)	IAM provides IAM management capabilities and allows you to create ECSs from images.
ECS	ECS provides cloud servers to receive OSs, applications, and data migrated from source servers.

Service	Interaction
Simple Message Notification (SMN)	SMN notifies you of migration results.
Data Encryption Workshop (DEW)	MgC uses Key Management Service (KMS) on DEW to encrypt files migrated to Huawei Cloud OBS buckets.
OBS	OBS stores object storage data migrated to Huawei Cloud.

10 Change History

Released On	What's New
2024-02-29	This issue is the second official release. Updated **Billing**.
2023-10-30	This issue is the first official release.

