Migration Center

Product Introduction

Issue 06

Date 2024-10-21

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?

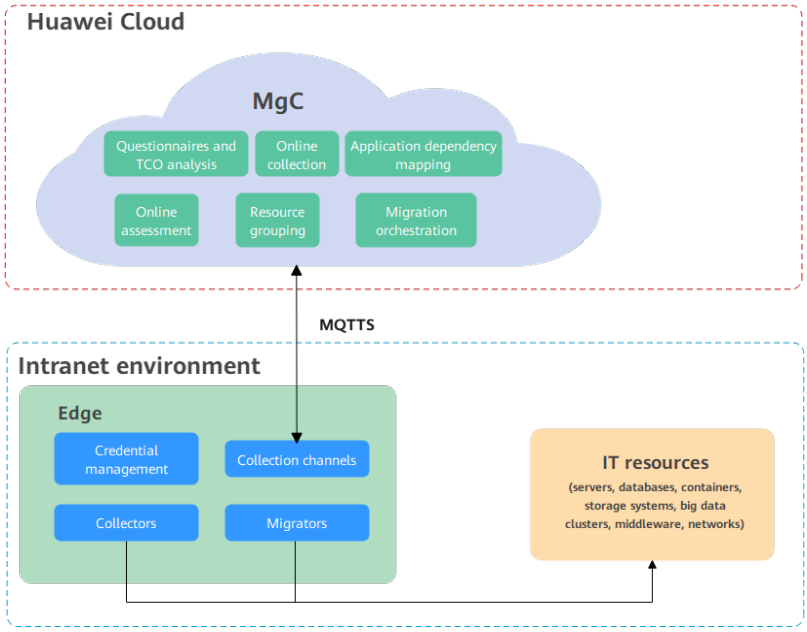
Migration Center (MgC) provides a single place for you to easily migrate, modernize, and optimize your applications using tools built based on Huawei Cloud migration methodologies and best practices.

MgC Architecture

The MgC service consists of two parts: MgC and Edge. MgC is a cloud service deployed on Huawei Cloud, and Edge 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 MgC Advantages

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.

Various Collection Sources

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

Visual Oversight

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

High Security

- Data collection

  To secure data collection, MgC only reads data from the source. It does not modify the data. In addition to online collection, you can also import details of your source environment directly into 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 MgC Application Scenarios

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 MgC Functions

TCO Analysis

MgC enables you to compare the Total Cost of Ownership (TCO) of your current environment with the projected cost on Huawei Cloud. Specifically, it automatically analyzes past bills for your source resources, matches them with Huawei Cloud alternatives, and calculates the corresponding cost on Huawei Cloud.

Application Dependency Mapping

- You can learn the call chains of microservices by collecting information about the collection registration center, configuration center, and CMDB. Collecting more items provides a more comprehensive view of the 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 scan 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 that Xen servers can start normally after being migrated across AZs, KVM drivers must be installed them before the migration. To learn how to install KVM drivers, refer to **Installing KVM Drivers**. If any server fails to start due to the missing of KVM drivers after the migration is complete, MgC is not responsible for such problems.

- Password inconsistency

  During cross-AZ migration of servers, backups and images are delivered to create target servers. If there are any automated password reset tools or periodic password update policies on a source server, the target server may use a password different from the source server after the migration is complete. For details, see **Are There Any Precautions I Need to Take When Performing a Cross-AZ Migration?** 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 for the source ECSs, MgC creates a vault 1.5 times the combined size of the source ECS disks

to facilitate the migration. The vault will be automatically deleted after the migration is complete.

For more details on CBR pricing, see **CBR Billing**.

- Images

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

  For more details on IMS pricing, 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 Collection Security

7.1 Data Collection Architecture

There are two methods MgC uses to collect data about source resources:

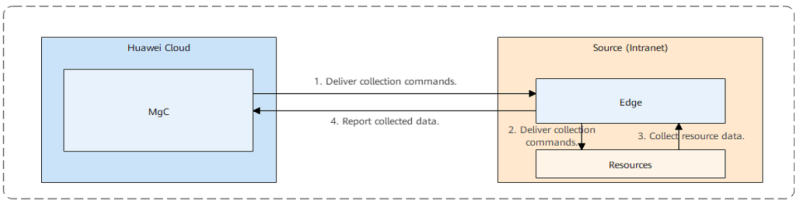
- Remote online collection using Edge
- Online collection using cloud APIs

Remote Online Collection Using Edge

MgC uses Edge, a tool you need to deploy in the source network, to collect details about source resources in public clouds, private clouds (built using such as VMware and Hyper-V), on-premises data centers (IDC), or hybrid deployment environments.

Figure 7-1 shows the data collection process.

Figure 7-1 Remote online collection using Edge

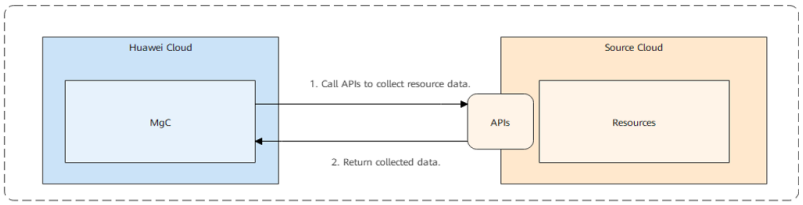


Online Collection Using Cloud APIs

MgC calls the APIs of other public clouds to collect details about source resources. Edge is not required.

Figure 7-2 shows the data collection process.

Figure 7-2 Online collection using cloud APIs



7.2 Security

Data Collection

- **Controlled collection duration**: Collection tasks run for a limited period. This prevents collection tasks from occupying system resources for too long.
- **Encrypted storage of credentials**: All credentials used for data collection are encrypted to ensure security. Credentials used for online collection are only stored on MgC.
- **Least privilege principle**: The principle of least privilege is enforced not matter which collection method is used.
- **MgC permissions control**: To use MgC or access the data collected by MgC, you must have certain permissions. For details, see **Permissions Management**.
- **Transparency of collection items**: You can see what data MgC collects in **Collection Items**.

Local Data Export

- **Audit logs**: Export actions are logged. You can use these logs to audit and trace export actions.
- **Transparency of exported data**: You can view what data is exported in **Collection Items**.

Data Upload

- **Encrypted transmission**: When data is uploaded to MgC, an encrypted channel is used to protect data in transit.
- **Channel authentication**: You must be authenticated before you can upload data to MgC. This enhances data transmission security.
- **Audit logs**: Upload actions are logged. You can use these logs for auditing and tracing.
- **Least privilege principle**: The principle of least privilege is enforced not matter which collection method is used.
- **MgC permissions control**: To use MgC or access the data collected by MgC, you must have certain permissions. For details, see **Permissions Management**.

Online Data Storage

- **Encrypted storage of credentials**: All credentials used for data collection are encrypted to ensure security. Credentials used for online collection are only stored on MgC.
- **Data storage isolated by tenant**: Data stored on MgC is isolated by tenant. Other tenants cannot access your data.
- **Transparent data storage**: You can view what data is collected and stored in **Collection Items**.

Data Analysis and Presence

- **Audit logs**: All query actions are logged to ensure action traceability and transparency.
- **Least privilege principle**: The principle of least privilege is enforced not matter which collection method is used.
- **MgC permissions control**: To use MgC or access the data collected by MgC, you must have certain permissions. For details, see **Permissions Management**.

7.3 Data Collected

This section describes what data MgC collects and what the collected data is used for.

Network Range Scan

Collection Item	Description	Purpose
ip	IP address of a server	Used for deep collection
port	Server port	Used for deep collection
osType	OS type	Used for deep collection
name	Name of a server	Used for deep collection

Servers (Deep Collection Included)

Collection Item	Description	Purpose
name	Name of a server	Used for pre-migration assessment
hostName	Hostname of a server	Used for pre-migration assessment
eip	Public IP address of a server	Used for pre-migration assessment

Collection Item	Description	Purpose
eipId	ID of a server EIP	Used for pre-migration assessment
privateIp	Private IP address of a server	Used for pre-migration assessment
ip	IP address of a server	Used for pre-migration assessment
port	Server port	Used for pre-migration assessment
collectStatus	Server data collection status	Used for pre-migration assessment
lastCollectTime	Last collection time	Used for pre-migration assessment
serverStatus	Server status	Used for pre-migration assessment
mac	MAC address of a server	Used for pre-migration assessment
cpuType	CPU model	Used for pre-migration assessment
cpuCores	Number of CPU cores	Used for pre-migration assessment
mem	Memory size	Used for pre-migration assessment
hostType	Server type	Used for pre-migration assessment
virtualType	Virtualization type	Used for pre-migration assessment
osType	OS type	Used for pre-migration assessment
osInfo	OS information	Used for pre-migration assessment
architecture	Processor architecture	Used for pre-migration assessment
firmware	Firmware	Used for pre-migration assessment
kernel	Kernel	Used for pre-migration assessment
disk	Disk information	Used for pre-migration assessment

Collection Item	Description	Purpose
frequency	CPU clock speed	Used for pre-migration assessment
isOpenOverclock	Whether overclocking is used	Used for pre-migration assessment
virtioDriver	Whether VirtIO drivers are installed	Used for pre-migration assessment
filterIds	Server ID set	Used for pre-migration assessment
instanceId	Cloud server ID. This item is available for cloud platform collection.	Used for pre-migration assessment
platformName	Platform name	Used for pre-migration assessment
platformType	Cloud platform type. This item is available for cloud platform collection.	Used for pre-migration assessment
regionId	Region ID. This item is available for cloud platform collection.	Used for pre-migration assessment
serverType	Server type	Used for pre-migration assessment
flavor	Specifications	Used for pre-migration assessment
cpuUsage	CPU usage	Used for pre-migration assessment
memUsage	Memory usage	Used for pre-migration assessment
diskUsage	Disk usage	Used for pre-migration assessment
networkInThroughput	Intranet inbound bandwidth, in byte/s	Used for pre-migration assessment
networkOutThroughput	Intranet outbound bandwidth, in byte/s	Used for pre-migration assessment
networkPpsIn	Inbound PPS (incoming packets per second)	Used for pre-migration assessment

Collection Item	Description	Purpose
networkPpsOut	Outbound PPS (outgoing packets per second)	Used for pre-migration assessment
networkConnections	Number of network connections	Used for pre-migration assessment
availableZone	AZ	Used for pre-migration assessment
securityGroupList	Security groups	Used for pre-migration assessment
clusterId	Big data cluster ID	Used for pre-migration assessment
chargeMode	Billing mode	Used for pre-migration assessment
assessStatus	Server TCO assessment status	Used for pre-migration assessment
nodeType	Big data node type	Used for pre-migration assessment

Databases (Deep Collection Included)

Collection Item	Description	Purpose
id	ID	Used for pre-migration assessment
name	Database name	Used for pre-migration assessment
connectAddress	Connection address	Used for pre-migration assessment
dbType	Database type	Used for pre-migration assessment
dbName	Database name	Used for pre-migration assessment
dbVersion	Database version	Used for pre-migration assessment
useSsl	Whether SSL is used	Used for pre-migration assessment
credentialId	Credential ID	Used for pre-migration assessment
instanceId	Instance ID	Used for pre-migration assessment
vpcId	VPC ID	Used for pre-migration assessment
vpcName	VPC name	Used for pre-migration assessment
subnetId	Subnet ID	Used for pre-migration assessment
subnetName	Subnet name	Used for pre-migration assessment

Collection Item	Description	Purpose
platformId	Platform ID	Used for pre-migration assessment
platformName	Platform name	Used for pre-migration assessment
platformType	Platform type	Used for pre-migration assessment
regionId	Region ID	Used for pre-migration assessment
privateAddress	Private IP address	Used for pre-migration assessment
publicAddress	Public IP address	Used for pre-migration assessment
type	Type	Used for pre-migration assessment
nodes	Cluster node information	Used for pre-migration assessment
ids	ID list	Used for pre-migration assessment
assessStatus	TCO assessment status	Used for pre-migration assessment

Containers (Deep Collection Included)

Collection Item	Description	Purpose
id	ID	Used for target recommendations
name	Name	Used for target recommendations
credentialId	Credential ID	Used for target recommendations
collectInfo	Original information returned by the collector	Used for target recommendations
collectError	Collection error	Used for target recommendations
assessStatus	Assessment status	Used for target recommendations
clusterVersion	Kubernetes cluster version	Used for target recommendations
totalNamespaces	Total number of namespaces	Used for target recommendations
totalCpuCores	Total number of CPU cores	Used for target recommendations
totalMemory	Total memory size (byte)	Used for target recommendations
totalNodes	Total number of nodes	Used for target recommendations

Collection Item	Description	Purpose
nodes	Cluster node information	Used for target recommendations
storages	Persistent volume storage information	Used for target recommendations
ingressClass	Ingress resources	Used for target recommendations
networkPolicy	Network policies	Used for target recommendations
loadbalancerSer-vices	LoadBalancer services	Used for target recommendations
runtimeClass	Container runtime class	Used for target recommendations
schedulers	Scheduler (used to place pods on proper nodes)	Used for target recommendations
platformType	Cloud platform type	Used for target recommendations
platformId	Cloud platform ID	Used for target recommendations
platformName	Cloud platform name	Used for target recommendations
regionId	Region ID	Used for target recommendations
instanceId	Cluster instance ID	Used for target recommendations
status	Cluster status	Used for target recommendations
billingMode	Billing mode	Used for target recommendations
creationTime	Cluster creation time	Used for target recommendations
clusterType	Cluster type	Used for target recommendations
clusterSpecs	Cluster specifications	Used for target recommendations
kubeProxyMode	Service forwarding mode (network mode): iptables, IPVS, etc	Used for target recommendations
networkModel	Network mode: VPC, Tunnel, and Global Router	Used for target recommendations
vpcId	VPC ID	Used for target recommendations
vpcName	VPC name	Used for target recommendations
subnetId	Subnet ID	Used for target recommendations
subnetName	Subnet name	Used for target recommendations

Collection Item	Description	Purpose
subnetCidr	Subnet CIDR block	Used for target recommendations
containerCidr	Container CIDR block	Used for target recommendations
serviceCidr	Service CIDR block	Used for target recommendations
highAvailable	High availability or not	Used for target recommendations
containerEngine	Container engine	Used for target recommendations
cpuAllocation	CPU allocation rate	Used for target recommendations
cpuUsage	CPU usage	Used for target recommendations
memoryAllocation	Memory allocation rate	Used for target recommendations
memoryUsage	Memory usage	Used for target recommendations

Platforms (Deep Collection Included)

Collection Item	Description	Purpose
id	ID	Used for target recommendations
name	Name	Used for target recommendations
platformType	Platform type	Used for target recommendations
regionId	Region ID	Used for target recommendations
credentialId	Credential ID	Used for target recommendations
ip	Connection address	Used for target recommendations
serverNum	Number of servers	Used for target recommendations
databaseNum	Number of databases	Used for target recommendations
kubernetesNum	Number of containers	Used for target recommendations
obsNum	Number of object storage buckets	Used for target recommendations
eipNum	Number of EIPs	Used for target recommendations
elbNum	Number of load balancers	Used for target recommendations
vpcNum	Number of VPCs	Used for target recommendations

Collection Item	Description	Purpose
securityGroupNum	Number of security groups	Used for target recommendations
natNum	Number of NAT gateways	Used for target recommendations
sfsNum	Number of file systems	Used for target recommendations
redisNum	Number of Redis instances	Used for target recommendations
kafkaNum	Number of Kafka instances	Used for target recommendations
bigdataNum	Number of big data clusters	Used for target recommendations
pubDomainNum	Number of public domain names	Used for target recommendations
vpcDomainNum	Number of VPC domain names	Used for target recommendations
routeTableNum	Number of route tables	Used for target recommendations
vpnNum	Number of VPNs	Used for target recommendations
dcNum	Number of Direct Connect connections	Used for target recommendations
cloudConnectNum	Number of Cloud Connect connections	Used for target recommendations
rocketmqNum	Number of RocketMQ instances	Used for target recommendations
collectResourceCategory	List of resource categories	Used for target recommendations

Storage

Collection Item	Description	Purpose
taskStatus	Task status	Used for target recommendations
errorType	Task type	Used for target recommendations

Collection Item	Description	Purpose
totalSize	Total capacity	Used for target recommendations
totalNum	Total number	Used for target recommendations
rangeLowerLimit	Lower limit	Used for target recommendations
rangeUpperLimit	Upper limit	Used for target recommendations

7.4 Permissions and Principles for Data Collection over an Intranet

Deep Server Collection

- **Permission requirements**
  - Windows: An account with administrator permissions is required.
  - Linux: The **root** account is required.
- **Collection principle**
  - Windows: Edge accesses Windows servers through WinRM and runs a PowerShell script to collect server details.

    Linux: Edge uses SSH to access Linux servers. A PowerShell script is uploaded to **/root/rda** and then executed to collect server details.

Network Range Scan

- **Permission requirements**: Edge can access the servers on the network range to be scanned over the required ports. By default, port 3389 is required for Windows and port 22 is required for Linux. You can also specify a different port if needed.
- **Collection principle**: After all IP addresses in the network range are listed, TCP connection requests are sent to each IP address over the required ports. If port 3389 is listened on, the IP address is used by a Windows server. If port 22 is listened on, the IP address is used by a Linux server.

Performance Collection

- **Required permissions**
  - Windows: An account with administrator permissions is required.
  - Linux: The **root** account is required.
- **Collection principle**
  - Windows: Edge uses the WinRM service to remotely access Windows servers, securely transfer a PowerShell script to the **C:/Edge-Scripts** directory of Windows servers, and executes the script to automatically collect server details.

  - Linux: Edge uses SSH to access Linux servers. A Shell script is uploaded to **/root/rda** directory and then executed to automatically collect server details.

Database Collection

- **Required permissions**: An account with full permissions is required to ensure that all necessary data can be accessed. The required account depends on the database management system.
  - MySQL: **root**
  - PostgreSQL: **postgres**
  - MongoDB: **admin**
  - Oracle: **system**
  - SQL Server: **sa**
- **Collection principle**: Source databases are connected, and query statements are sent to collect database details.

Middleware Collection

- **Required permissions**
  - Redis: A general account with basic access permissions is required.
  - Kafka: An account with the permissions to access all topics and topic information is required.
- **Collection principle**: Data is collected through the Java applications integrated with middleware SDKs. These applications interact with middleware through the methods and APIs provided by the SDKs.

Container Collection

- **Permission requirements**: An administrator account is required to export files that contain necessary access credentials.
- **Collection principle**: kSpider is used to collect data.

vCenter Server Collection

- **Permission requirements**: An administrator account is required. This account must have full access permissions to all VMs managed by the vCenter Server.
- **Collection principle**: The vSphere SDK is used to list VMs and collect their details.

7.5 Permissions Required for Data Collection over the Internet

The tables below describe the permissions required for collecting resource details from supported cloud platforms over the Internet.

Alibaba Cloud Data Collection

The following table lists the permissions required for collecting data of Alibaba Cloud resources.

Resource Type	Cloud Service	Action	Minimum Permission Policy
Servers	Elastic Compute Service (ECS)	ecs:DescribeInstances	Read
		ecs:DescribeDisks	List
		ecs:DescribeMetricData	List
Storage	NAS	nas:DescribeFileSystems	Read
	Object Storage Service (OSS)	ListBuckets	oss:ListBuckets
		oss:DescribeMetricData	List
Databases	Relational Database Service (RDS)	rds:DescribeDBInstances	Read
		rds:DescribeDBInstanceAttribute	Read
	MongoDB	rds:DescribeDBInstances	Read
		rds:DescribeDBInstanceAttribute	Read
Middleware	Redis	kvstore:DescribeInstances	List
		kvstore:DescribeInstanceAttribute	Read
		kvstore:DescribeMetricData	List
	Kafka	alikafka:ListInstance	Read
		kafka::DescribeMetricData	List
	RocketMQ	rocketmq:GetInstance	Read
		rocketmq::DescribeMetricData	List
Containers	K8S ACK	cs:GetClusters	Read
		cs:DescribeClusterDetail	Read
		k8s::DescribeMetricData	List
Big data	Elastic MapReduce (EMR)	emr:ListClusters	List
Networks	CEN	cen:ListTransitRouters	Read
		cen:DescribeCenPrivateZoneRoutes	Read
		cen:DescribeRouteServicesInCen	Read
		cen:ListTransitRouterVpcAttachments	List
		cen:ListTransitRouterVbrAttachments	List
		cen:ListTransitRouterVpnAttachments	List

Resource Type	Cloud Service	Action	Minimum Permission Policy
		cen:DescribeCenAttachedChildInstances	Read
		cen:DescribeCenAttachedChildInstanceAttribute	Read
		cen:ListTransitRouterPeerAttachments	Read
		cen:ListTransitRouterRouteTables	Read
		cen:ListTransitRouterRouteEntries	Read
		cen:ListTransitRouterRouteTableAssociations	Read
		cen:ListTransitRouterPrefixListAssociation	Read
		cen:DescribeCenRouteMaps	Read
		cen:ListTransitRouterRouteTables	Read
		cen:DescribeCenRegionDomainRouteEntries	Read
		cen:ListTransitRouters	Read
		cen:DescribeCens	Read
	ALB	alb:ListLoadBalancers	Read
		alb:ListServerGroupServers	Read
	CLB	slb:DescribeLoadBalancers	Read
		slb:DescribeLoadBalancerListeners	Read
		slb:DescribeVServerGroupAttribute	Read
		slb:DescribeMasterSlaveServerGroupAttribute	Read
		slb:DescribeHealthStatus	Read
		slb:DescribeMasterSlaveServerGroupAttribute	Read
		slb:DescribeMasterSlaveServerGroups	Read
	Virtual Private Cloud (VPC)	vpc:DescribePhysicalConnections	Read
		vpc:DescribeVirtualBorderRouters	Read
		vpc:DescribeRouteTables	Read
		vpc:DescribeRouteTableList	List

Resource Type	Cloud Service	Action	Minimum Permission Policy
	DNS	alidns:DescribeDomainRecords	Read
		alidns:DescribeDomains	Read
	Private Zone	pvtz:DescribeZoneVpcTree	Read
		pvtz:DescribeZoneRecords	Read
	Elastic IP (EIP)	ens:DescribeEipAddresses	Read
	NAT Gateway	ens:DescribeNatGateways	Read
		ens:DescribeSnatTableEntries	List
		ens:DescribeForwardTableEntries	List

Huawei Cloud Data Collection

The following table lists the permissions required for collecting data of Huawei Cloud resources.

Resource Type	Cloud Service	Action	Minimum Permission Policy
Servers	ECS	ecs:ListServersDetails ces:BatchListMetricData evs:ListVolumes eip:ListPublicips	• ECS ReadOnlyAccess • EVS ReadOnlyAccess • EIP ReadOnlyAccess
Containers	CCE	cce:ListNodes cce:ListClusters aom:ShowMetricsData	• CCE ReadOnlyAccess • AOM ReadOnlyAccess
Big data clusters	MRS	mrs:ListClusters mrs:ListHosts	MRS ReadOnlyAccess
Databases	DDS	dds:ListInstances dds:ListFlavors	DDS ReadOnlyAccess
	RDS	rds:ListInstances	RDS ReadOnlyAccess

Resource Type	Cloud Service	Action	Minimum Permission Policy
Middleware	Distributed Message Service (DMS) for Kafka	dms:ListInstances dms:ShowInstance dms:ListAvailableZones dms:ShowCluster ces:BatchListMetricData	DMS ReadOnlyAccess
	Distributed Cache Service (DCS)	dcs:ListInstances dcs:ListFlavors dcs:ListGroupReplicationInfo ces:BatchListMetricData	DCS ReadOnlyAccess
Storage	OBS	obs:ListBuckets obs:GetBucketPolicy obs:GetBucketAcl obs:GetBucketLifecycle obs:GetBucketMetadata obs:GetBucketVersioning obs:GetBucketStorageInfo obs:GetBucketStoragePolicy ces:BatchListMetricData	• OBS ReadOnlyAccess • CES ReadOnlyAccess You need to create custom policies for actions that are not included in the preceding two policies.
	SFS Turbo	sfsturbo:ListShares	SFS Turbo ReadOnlyAccess
Networks	ELB	elb:ListListeners elb:ListLoadbalancers elb:ListPools elb:ListL7policies elb:ListL7rules elb:ListMembers elb:ListFlavors vpc:ListSubnets	ELB ReadOnlyAccess
	DNS	dns:ListPublicZones dns:ListPrivateZones dns:ListRecordSetsByZone	DNS ReadOnlyAccess
	EIP	eip:ListPublicips	EIP ReadOnlyAccess

Resource Type	Cloud Service	Action	Minimum Permission Policy
	NAT	nat:ListNatGateways nat:ListNatGatewayDnatRules nat:ListNatGatewaySnatRules vpc:ShowPort vpc:ShowSubnet vpc:ListSubnets	NAT ReadOnlyAccess
	VPC	vpc:ListRouteTables vpc:ShowRouteTable vpc:ListVpcs vpc:ListSecurityGroups vpc:ListSecurityGroupRules vpc:ListSubnets	VPC ReadOnlyAccess

AWS Data Collection

The following table lists the permissions required for collecting data of AWS resources.

Resource Type	Cloud Service	Action	Minimum Permission Policy
Servers	Elastic Compute Cloud (EC2)	ec2:DescribeInstances	AmazonEC2ReadOnlyAccess
		ec2:DescribeAddresses	
		ec2:DescribeImages	
		ec2:DescribeVolumes	
		cloudwatch:GetMetricStatistics	
Storage	Elastic File System (EFS)	elasticfilesystem:DescribeFileSystems	AmazonElasticFileSystemReadOnlyAccess
		elasticfilesystem:DescribeMountTargets	
		cloudwatch:GetMetricStatistics	
	S3	s3:ListObjectsV2	AmazonS3ReadOnlyAccess
		cloudwatch:GetMetricStatistics	

Resource Type	Cloud Service	Action	Minimum Permission Policy
Databases	Relational Database Service (RDS)	rds:DescribeDBClusters	AmazonRDSReadOnlyAccess
		rds:DescribeDBInstances	
		ec2:DescribeSecurityGroups	
Middleware	ElastiCache	elasticache:DescribeCacheClusters	AmazonElastiCacheReadOnlyAccess
		elasticache:DescribeReplicationGroups	
		cloudwatch:GetMetricStatistics	
	Managed Streaming for Apache Kafka (MSK)	kafka:ListClustersV2	AmazonMSKReadOnlyAccess
		cloudwatch:GetMetricStatistics	
Containers	Elastic Kubernetes Service (EKS)	eks:DescribeCluster	No corresponding permission policy is available. You need to create one.
		eks:ListClusters	
		ec2:DescribeInstances	
		ec2:DescribeSubnets	
		cloudwatch:GetMetricStatistics	
Big data	Elastic MapReduce (EMR)	elasticmapreduce:DescribeCluster	AmazonEMRReadOnlyAccessPolicy_v2
		elasticmapreduce:ListClusters	
		elasticmapreduce:ListInstanceGroups	
		elasticmapreduce:ListInstances	
		ec2:DescribeInstances	AmazonEC2ReadOnlyAccess
Networks	Elastic IP (EIP)	ec2:DescribeAddresses	AmazonEC2ReadOnlyAccess
	Elastic Load Balancing (ELB)	elasticloadbalancing:DescribeLoadBalancers	ElasticLoadBalancingReadOnly

Resource Type	Cloud Service	Action	Minimum Permission Policy
	NAT Gateway	ec2:DescribeNatGateways	AmazonEC2ReadOnlyAccess
	Route53(Public Domain)	route53:ListHostedZones	AmazonRoute53ReadOnlyAccess
		route53:ListResourceRecordSets	
	RouteTable	ec2:DescribeRouteTables	AmazonEC2ReadOnlyAccess
	SecurityGroup	ec2:DescribeSecurityGroups	AmazonEC2ReadOnlyAccess
		ec2:DescribeSecurityGroupRules	
	Route53(VpcDomain)	route53:GetHostedZone	AmazonRoute53ReadOnlyAccess
		route53:ListHostedZones	
		route53:ListResourceRecordSets	
	Virtual Private Cloud (VPC)	ec2:DescribeSubnets	AmazonEC2ReadOnlyAccess
		ec2:DescribeVpcs	

Tencent Cloud Data Collection

The following table lists the permissions required for collecting data of Tencent Cloud resources.

Resource Type	Cloud Service	Action	Minimum Permission Policy
Servers	CVM	cvm: DescribeInstances cvm: DescribeImages cvm:DescribeSecurityGroups cbs: DescribeDisks vpc: DescribeAddresses vpc: DescribeNetworkInterfaces vpc: DescribeSubnets monitor:GetMonitorData	QcloudCVMReadOnlyAccess

Resource Type	Cloud Service	Action	Minimum Permission Policy
Databases	CDB	cdb:DescribeDBInstances	QcloudCDBReadOnlyAccess
	PostgreSQL	postgres:DescribeDBInstances	QcloudPostgreSQLReadOnlyAccess
	MongoDB	mongodb:DescribeDBInstances mongodb:DescribeDBInstanceNodeProperty	QcloudMongoDBReadOnlyAccess
	SQLServer	sqlserver:DescribeDBInstances sqlserver:DescribeReadOnlyGroupList	QcloudSQLServerReadOnlyAccess
Storage	COS	cos:GetService cos:GetBucketACL cos:GetBucketLifecycle cos:GetBucketVersioning monitor:GetMonitorData	QcloudCOSReadOnlyAccess
	CFS	cfs:DescribeCfsFileSystems cfs:DescribeMountTargets	QcloudCFSReadOnlyAccess
Networks	DNSPod	dnspod:DescribeDomainList dnspod:DescribeRecordList	QcloudDNSPodReadOnlyAccess
	WAF	waf:DescribeDomains waf:DescribeInstances	QcloudWAFReadOnlyAccess
	CLB	clb:DescribeLoadBalancersDetail clb:DescribeTargets cvm: DescribeInstances	QcloudCLBReadOnlyAccess QcloudCVMReadOnlyAccess

Azure Data Collection

The following table lists the permissions required for collecting data from Azure resources.

Resource Type	Cloud Service	Service	Minimum Permission Policy
Servers	Virtual Machines (VMs)	Microsoft Classic Compute	Microsoft.ClassicCompute/virtualMachines/read
		Microsoft Azure Monitor	Microsoft.Insights/MetricDefinitions/Read
		Microsoft Network	Microsoft.Network/networkInterfaces/read
Storage	Storage Accounts	Microsoft Azure Monitor	Microsoft.Insights/MetricDefinitions/Read
		Microsoft Classic Storage	Microsoft.ClassicStorage/storageAccounts/read
Databases	Azure Database for PostgreSQL - Flexible Server	Microsoft Management	Microsoft.Management/getEntities/action
	Azure Database for PostgreSQL	Microsoft Management	Microsoft.Management/getEntities/action
	Azure Database for MySQL	Microsoft Management	Microsoft.Management/getEntities/action
	Azure Database for MySQL - Flexible Server	Microsoft Management	Microsoft.Management/getEntities/action
	SQL servers	Microsoft Azure Arc Data	Microsoft.AzureArcData/sqlServerInstances/read
		Microsoft Management	Microsoft.Management/getEntities/action
Middleware	Azure Cache for Redis	Microsoft Management	Microsoft.Management/getEntities/action
	Event Hubs	Microsoft Management	Microsoft.Management/getEntities/action
Containers	Kubernetes services	Microsoft Classic Compute	Microsoft.ClassicCompute/virtualMachines/read
		Microsoft Azure Monitor	Microsoft.Insights/MetricDefinitions/Read

Resource Type	Cloud Service	Service	Minimum Permission Policy
		Microsoft Management	Microsoft.Management/getEntities/action
Networks	Public IP addresses	Microsoft Management	Microsoft.Management/getEntities/action
	Load Balancer	Microsoft Management	Microsoft.Management/getEntities/action
	NAT gateways	Microsoft Management	Microsoft.Management/getEntities/action
	Route tables	Microsoft Network	Microsoft.Network/networkInterfaces/read
	Network security groups	Microsoft Network	Microsoft.Network/networkInterfaces/read
	Virtual networks	Microsoft Network	Microsoft.Network/networkInterfaces/read

Qiniu Cloud Data Collection

The following table lists the permissions required for collecting data of Qiniu Cloud resources.

Resource Type	Cloud Service	Action	Minimum Permission Policy
Storage	Object storage (KODO)	kodo:buckets	QiniuKodoReadOnlyAccess

Kingsoft Cloud Data Collection

The following table lists the permissions required for collecting data of Kingsoft Cloud resources.

Resource Type	Cloud Service	Action	Minimum Permission Policy
Storage	Kingsoft Cloud Standard Storage Service (KS3)	ks3:ListBuckets	KS3ReadOnlyAccess

Google Cloud Data Collection

The following table lists the permissions required for collecting data of Google Cloud resources.

Resource Type	Cloud Service	Permission	Role (Role ID)
Servers	Compute Engine	compute.instances.list	Compute Viewer(roles/compute.viewer)
		compute.machineTypes.get	
		compute.disks.get	
		compute.networks.get	
		compute.regions.get	
Storage	Cloud Storage	storage.buckets.list	Storage Admin (roles/storage.admin) or Viewer (roles/viewer)
		storage.objects.list	Storage Object Viewer (roles/storage.objectViewer) or Storage Admin (roles/storage.admin)
	Compute Engine(obs)	compute.regions.get	Compute Viewer(roles/compute.viewer)
		compute.networks.list	
	Cloud Filestore	file.instances.list	Cloud Filestore Viewer(roles/file.viewer)
Databases	Cloud SQL	cloudsql.instances.list	Cloud SQL Viewer(roles/cloudsql.viewer)
		cloudsql.databases.list	
		cloudsql.tiers.list	No role is required.
Middleware	Memorystore Redis	redisService.instances.list	Cloud Memorystore Redis Viewer(roles/redis.viewer)
		redisService.clusters.list	
Containers	Kubernetes Engine	container.clusters.list	Kubernetes Engine Cluster Viewer(roles/container.clusterViewer)
	Compute Engine(k8s)	compute.regions.get	Compute Viewer(roles/compute.viewer)

Resource Type	Cloud Service	Permission	Role (Role ID)
		compute.networks.list	
		compute.subnetworks.list	
Networks	Compute Engine(clb)	compute.firewalls.list	Compute Viewer(roles/compute.viewer)
		compute.forwardingRules.list	
		compute.globalForwardingRules.list	
		compute.backendServices.get	
		compute.networks.list	
		compute.subnetworks.list	
	Compute Engine(eip)	compute.addresses.list	
		compute.globalAddresses.list	
		compute.regions.get	
		compute.instances.list	
	Compute Engine(route table)	compute.routes.list	
		compute.networks.list	
		compute.subnetworks.list	
	Compute Engine(vpc)	compute.networks.list	
		compute.subnetworks.list	
	Compute Engine(security group)	compute.firewalls.list	

7.6 Shared Responsibilities

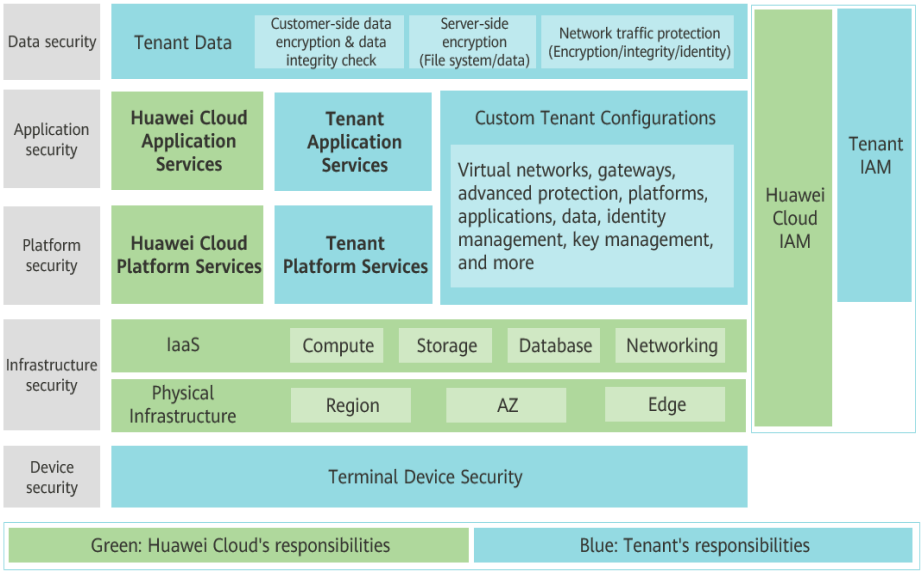
Huawei Cloud guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To address emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud has designed a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, and in line with all applicable laws, regulations, industry standards, and the overall security ecosystem.

Figure 7-3 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, more broadly, for the security and compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures used for Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 7-3 Huawei Cloud shared security responsibility model



8 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 8-1 lists all the system-defined policies supported by MgC.

Table 8-1 System-defined policies supported by MgC

Policy Name	Description	Policy Type	Policy Content
MgC FullAccess	Administrator permissions for 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 these 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 8-2 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 8-2 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:roles:listRoles",
                "iam:quotas:listQuotas",
                "iam:permissions:listRolesForAgency"
            ],
            "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:roles:listRoles",
        "iam:quotas:listQuotas",
        "iam:permissions:listRolesForAgency"
      ],
      "Effect": "Allow"
    }
  ]
}
```

MgC MigrateAccess Policy Content

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "mgc:*:query*",
        "mgc:*:discovery",
        "mgc:*:assess",
        "mgc:*:migrate",
        "iam:agencies:listAgencies",
        "iam:roles:listRoles",
        "iam:quotas:listQuotas",
        "iam:permissions:listRolesForAgency"
      ],
      "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"
          }
        ]
    }
  }
}
```


9 Notes and Constraints

This section describes the MgC constraints about region availability, server migration, cross-AZ migration, and storage migration.

Region Availability

MgC is available in AP-Singapore, TR-Istanbul, LA-Sao Paulo1, and LA-Santiago. While MgC is a region-level service, it offers global capabilities, allowing you to migrate to any region on the cloud. For information security purposes, all collected data and task records are stored in the regions where MgC is available.

Server Migration

Table 9-1 lists the constraints on server migration using MgC.

Table 9-1 Constraints on server migration

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.

Item	Constraint
Resource assessment and recommendations	• Target servers must have disks as least as large as source servers. • Target servers must use the same type of OS as source servers. • There must be sufficient quotas for recommended disk types in the target region.
Migration prerequisite	All source 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.
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 Linux target servers over port 22 and Windows source servers over ports 22, 8899, and 8900.
Server 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 3.0. You can run the **$host** command in the PowerShell command window to view the version.

Cross-AZ Server Migration

Table 9-2 lists the constraints on cross-AZ server migration using MgC.

Table 9-2 Constraints on cross-AZ migration

Item	Constraint
Source server specifications	Automated installation of KVM drivers is not supported for cross-AZ migrations. You need to manually install KVM drivers on source servers that use Xen by referring to **Installing KVM Drivers**.

Item	Constraint
Source server quantity	• A maximum of 30 servers can be migrated at a time using the automated process. • A maximum of 100 servers can be migrated at a time using the manual process. • Given the same set of environmental conditions, the more source servers there are being migrated, the slower the migration speed.
Source disk	• Servers whose system disk is larger than 1 TB cannot be migrated. • You are advised not to migrate servers whose disk capacity exceeds 4 TB.
Source server status	Frozen source servers in the retention period cannot be migrated.
Target server	• Migrating to existing target servers is not supported. • Target servers created by MgC are billed on a pay-per-use basis. You can manually change their billing mode from pay-per-use to yearly/monthly after the migration is complete.
File systems	MgC cannot migrate files from file systems such as NFS or CIFS, or from NAS devices.
Applications bound to hardware	MgC cannot migrate OSs that contain applications bound to hardware.
Servers added to a domain	After migrating servers added to a domain, you need to add them to the domain again.
Encrypted files	MgC cannot migrate OSs that contain protected folders or encrypted volumes.
External storage of servers	MgC cannot migrate data from the external storage attached to a source server.
Server passwords	• Passwords of Linux servers remain unchanged before and after the migration. • Passwords of Windows servers may change after the migration. For details, see **Are There Any Precautions I Need to Take When Performing a Cross-AZ Migration?**

Storage Migration

Table 9-3 and **Table 9-4** list the constraints on storage migration using MgC.

Table 9-3 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 must not contain special characters. • A single object cannot be larger than 4.76837158203125 TB (500 MB x 10,000). Otherwise, the migration may fail.
Migration network	Migrations are supported over public networks, private networks, and private lines.
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 creating a migration workflow. – After the migration is complete, manually create a symbolic link to the path at the target. • Migration of symbolic links is not supported for migration from NAS_SMB or migration from NAS_NFS to OBS. • For migration from NAS_NFS or Alibaba Cloud OSS to NAS_NFS, symbolic links can be migrated. To keep symbolic links valid after being migrated, enable metadata migration. Otherwise, the symbolic links will lose their link functionality and become regular files after the migration. **NOTICE** If the objects that soft links point to are not completely migrated to the target, these soft 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.
Migration scope	You can migrate a single bucket or multiple buckets in batches.

Item	Constraint
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 correponding object will fail to be migrated. – English characters, digits, and hyphens (-) are directly migrated without code conversion. • For heterogeneous migrations, metadata cannot be migrated.
Archived data	To migrate archived data from object storage, you must restore it first. You need to: • Create migration workflows after the restoration is complete. • 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.

Item	Constraint
Object list files	These files must be stored in the same region as the target bucket. • The files must be in .txt format, and their metadata **Content-Type** must be **text/plain**. • A single file can contain a maximum of 100,000 rows. • A single file cannot exceed 300 MB. • A maximum of 10,000 list files can be stored in the folder. • The files must be in UTF-8 without BOM. • The length of each line in a file cannot exceed 65,535 characters, or the migration will fail. • The **Content-Encoding** metadata of the files must be left empty, or the migration will fail. • In the files, a tab character (\t) must be used to separate the URL and new file name in each line. The format is [URL][Tab character][New file name]. Only the Chinese and special characters in the names must be URL encoded. • Spaces are not allowed in each line in a file. Spaces may cause migration failures because they may be mistakenly identified as object names.

Table 9-4 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. • Soft links cannot be migrated.
Migration source: NAS file systems	• The following types of files can be migrated: regular files, directory files, symbolic link files, and hard link files. **CAUTION** If the file handle is occupied or the source file is deleted, the file will fail to be migrated. • 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.

10 Related Services

The following table describes how MgC interacts with other services.

Table 10-1 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 Edge. It is used to deliver commands for managing plugins, credentials, and collection and migration tasks from MgC to the Edge. It is also used to synchronize source information collected by Edge to MgC.
OMS	OMS is integrated with MgC to migrate data from object storage on other cloud platforms to OBS on Huawei Cloud.
CBR	CBR backs up Elastic Volume Service (EVS) disks and Elastic Cloud Servers (ECSs) for fault recovery.
IMS	IAM enables you to manage images and 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.
OBS	OBS stores object storage data migrated to Huawei Cloud.

