# 迁移中心 MgC

# 产品介绍

**文档版本** 06

**发布日期** 2024-10-15

**华为技术有限公司**

## 商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 安全声明

## 漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

# 目 录



# 1 什么是迁移中心

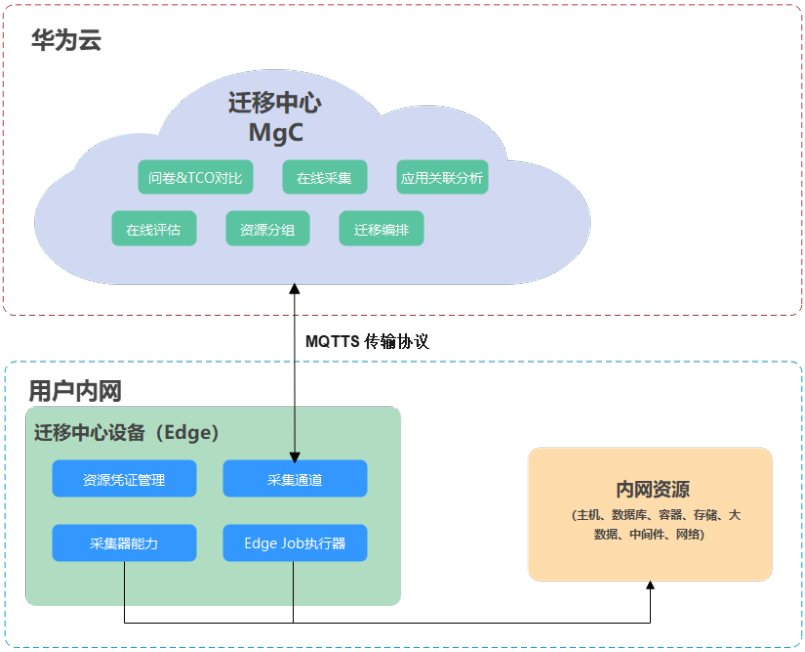
迁移中心（Migration Center，MgC）是华为云一站式迁移和现代化平台，承载华为云迁移方法论和最佳实践，该平台提供强大的应用发现能力和资源评估能力，并且通过向导式的迁移流程，帮助您轻松将应用资源迁移到华为云。

## 逻辑架构

MgC分为部署在云上的云服务和部署在客户网络中的Edge两个部分。

- MgC：部署在云上，主要包含六个业务功能(问卷&TCO对比、在线采集、应用关联分析、在线评估、资源分组、迁移编排)，通过基于服务开发服务，基于服务运维服务的方式进行设计。
- Edge：部署在客户的网络中，用来保存凭证等敏感资源和操作租户本地部署的资源。可以接收MgC的命令和上报命令执行结果。

**图 1-1** MgC 逻辑架构图



# 2 产品优势

## 简单高效

迁移中心集成了华为云多款云迁移产品，提供一站式的迁移集成能力和统一管理能力，并提供迁移工作流模板，用户可以根据不同迁移场景，简单、快速创建迁移工作流，提升用户云迁移效率。

## 多源采集

迁移中心支持多种类的资源采集，包括：**云平台**、**主机**、**数据库**、**容器**、**中间件**等。并且可以对采集到的主机、数据库、存储等信息进行调研评估，为用户上云提供配置推荐和方案设计。

## 可视化管理

为了让用户对迁移进度一目了然，迁移中心提供一站式工作流管理迁移进度，用户可实时管理和监测整个迁移过程。

## 数据安全

- 数据采集

  迁移中心为了确保采集数据的安全性，采集数据时只会读取源端数据，不会对源端数据进行修改。并提供了“导入本地文件”与“在线采集”两种采集方式。

- 数据传输

  迁移中心为了确保数据传输安全，采用加密通道（HTTPS、SSH）进行数据传输。

- 凭证加密

  在线采集时，采集凭证会加密存储在MgC服务端。用户也可以通过在源端部署Edge实施采集，采集凭证加密存储在本地Edge。

# 3 应用场景

## 应用现状调研

提供丰富的调研能力，支持其他云厂商或者自建IDC中的应用现状调研，并且绘制对应架构图和依赖图，为后续迁移计划的制定提供帮助。

## 一站式批量迁移

提供高灵活、可定制的迁移工作流，集成了华为云主机迁移服务 SMS、对象存储迁移服务 OMS、数据复制服务 DRS等迁移工具，帮助用户一站式大批量发起迁移任务。

## AZ 间迁移

迁移中心支持AZ间迁移场景，并提供AZ迁移工作流模板，帮助您高效、可视化的完成AZ间的资源迁移和业务切换。

## 存储迁移

通过独立专享迁移集群以及配置迁移专线，简单、快捷实现对象存储、文件存储一站式上云，提升上云效率。

# 4 产品功能

## 迁移成本分析（TCO）

通过迁移中心提供的TCO对比功能，可以自动完成源端云厂商消费账单分析以及和华为云的成本分析和比较，从而为您云间迁移提供参考。

## 应用关联分析

- 通过采集注册中心、配置中心、CMDB等平台，获取微服务间调用关系。配置更多采集项，可以更准确的分析出应用与应用间、应用与数据间调用的拓扑关系，提高迁移分组实施效率。
- 提供架构图和依赖图来展示应用间的关联关系和应用的组织架构，帮助用户进行迁移分析和方案设计。
- 支持批量导入/导出资源。

## 评估推荐

通过采集源端主机、数据库、对象存储等资源信息和应用的关联关系进行评估分析，根据源端资源规格、性能和应用场景以及特定的成本、可用性、性能、安全合规等需求，为您推荐最合适的华为云对应资源规格，支持导出评估结果。

## 迁移工作流模板

迁移中心 MgC内置了由最佳实践总结而来的迁移工作流模板，包含主机大批量迁移模板、AZ间ECS迁移模板以及存储数据迁移模板，用户可以根据不同迁移场景，选择合适的迁移模板构建迁移工作流，还可以插入自定义迁移阶段和步骤，支持一键式运行和实时监控迁移进展。

# 5 免责声明

- **License失效声明**

  源端服务器的系统、应用、文件等数据迁移到目的端服务器后，服务器的SID、网卡MAC地址等信息发生改变，导致OS、应用等License失效。此类问题，迁移服务概不负责。对于Windows License可以使用华为云License服务器获取新License，应用License用户自行解决。

- **源端磁盘数据安全性声明**

  迁移过程中，迁移服务无法感知磁盘内容，需要您自行保障源端磁盘数据的安全性。如果因为源端磁盘数据中存在木马或病毒等软件，导致迁移后目的端VPC内的主机受到影响，迁移中心概不负责。

- **驱动不可用免责声明**

  使用AZ迁移工作流进行**主机跨AZ迁移**时，如果源端主机为XEN架构类型，需要您自行**安装KVM驱动**，由于没有安装相关KVM驱动导致迁移后无法启动的相关问题，迁移中心概不负责。

- **密码不一致免责声明**

  主机跨AZ迁移采用备份、镜像下发目的端的形式，无法保障密码的完全一致性，由源端自动重设密码应用、周期更新密码策略等原因导致迁移后目的端密码与源端不一致（**AZ迁移注意事项**），迁移中心概不负责。

# 6 计费说明

迁移中心当前免费使用，但在进行工作流迁移时，会产生其他相关服务的费用。

## 主机迁移计费说明

在进行主机迁移过程中，会产生少量其他服务费用，详情请参见**SMS计费说明**。

## 对象存储迁移计费说明

在进行对象存储迁移过程中，会产生华为云OBS、源端云厂商API请求费用，详情请参考**OMS计费说明**。

## 创建迁移集群计费说明

在创建迁移集群时，会产生以下费用：

- 创建Master节点、迁移节点和列举节点会产生ECS服务费用。具体计费详情请参见**ECS按需计费说明**或**ECS价格计算器**。
- 如果您使用公网迁移时，会产生NAT网关服务费用。计费详情请参见**NAT网关计费说明**或**NAT价格计算器**。
- 启用LTS服务时，会产生LTS服务费用。具体计费详情请参见**LTS计费说明**或**LTS价格计算器**。

## 可用区（AZ）迁移计费说明

在进行可用区（AZ）迁移过程中会产生ECS、IMS、CBR等服务费用：

- **云备份费用**

  跨可用区（AZ）迁移，主要是使用云备份服务中的“云服务器备份”的功能，在迁移过程中，假如源端没有绑定相关的存储库，则迁移服务会按需创建一个容量为源端服务器总容量1.5倍的存储库，用于辅助迁移，该存储库在迁移结束后自动删除。

  有关云备份服务的收费标准，请参见**CBR计费说明**。

- **镜像服务费用**

  跨可用区（AZ）迁移，在迁移过程中会生成源端服务器的整机镜像，可能会产生一定的费用。

  有关镜像服务的费用说明，请参见**IMS计费说明**。

- **目的端服务器费用**

  跨可用区（AZ）迁移，不支持已有目的端的迁移方式，同时会按需创建目的端，待业务割接后，用户可自行将目的端切换为包周期的方式。

  有关按需云服务器的收费标准，请参见**ECS按需计费说明**。

**⚠ 注意**

- 以上费用仅为示例说明，仅供您迁移前评估迁移费用，具体迁移费用以实际收费为准。

# 7 采集安全性说明

## 7.1 数据采集架构

迁移中心（MgC）采集数据的方式主要包括以下两种：

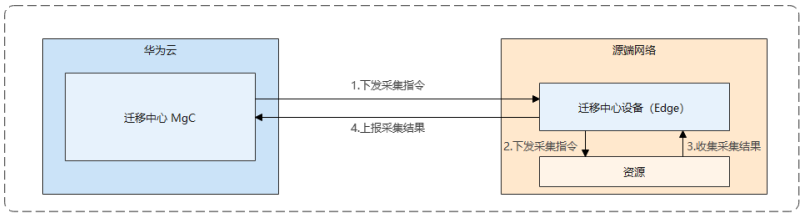
- **利用Edge远程在线采集**
- **通过调用API在线采集云平台资源**

### 利用 Edge 远程在线采集

适用于公有云、私有云（如VMware、Hyper-V等虚拟化环境）以及数据中心（IDC）部署，或者以上部署方式的混合场景。迁移中心 MgC利用部署在源端网络中的Edge设备完成数据采集。

数据采集架构图，如图7-1所示。

**图 7-1** Edge 远程在线采集架构图

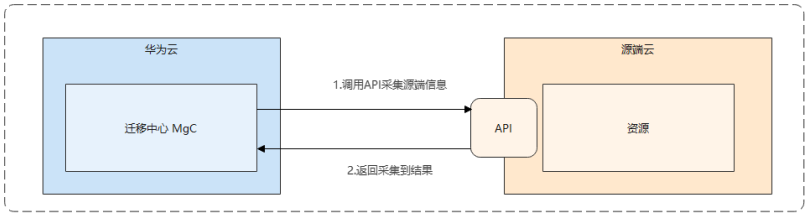



### 通过调用 API 在线采集云平台资源

适用于公有云部署场景，针对不同云服务提供商（友商）的云资源进行数据采集。使用API接口与其它云服务提供商的系统进行交互，实现数据的在线采集。不需要在源端网络中安装Edge设备。

数据采集架构图，如图7-2所示。

**图 7-2** 调用 API 在线采集云平台资源架构图




# 7.2 安全特性

## 采集安全性

- **采集时长受控**：采集任务在有限的时间内完成，采集避免长时间占用系统资源。
- **加密保存凭证**：所有用于数据采集的凭证都经过加密处理，以保护凭证的安全。线上采集的凭证仅在线上环境中保存。
- **操作权限与最小权限原则**：无论哪种采集方式，都需要具备相应的操作权限，并且遵循最小权限原则，即只授予完成特定任务所需的最小权限。
- **MgC服务侧权限要求**：云账号需要具备对应权限才能使用MgC和访问MgC调研数据，MgC相关权限请参考**权限管理**。
- **数据采集项透明性**：数据采集的具体项目参见**采集项列表**。

## 本地导出

- **具备审计日志**：导出操作会生成日志记录，这些日志可以用于审计和追踪导出活动，确保操作的透明性和可追溯性。
- **导出数据项透明展示**：所有被导出的数据项都是透明的，可以通过查看**采集项列表**来了解哪些数据将被导出。

## 数据上传

- **传输加密**：数据在上传至MgC服务侧时，使用加密通道来保护数据在传输过程中的安全。
- **通道认证**：只有经过验证的用户账号才能上传数据，增加了数据传输的安全性。
- **审计日志**: 上传操作会被记录在后台日志中，这些日志可以用于审计和监控数据上传活动，确保所有操作都是可追踪和可验证的。
- **操作权限与最小权限原则**：无论哪种采集方式，都需要具备相应的操作权限，并且遵循最小权限原则，即只授予完成特定任务所需的最小权限。
- **MgC服务侧权限要求**：云账号需要具备对应权限才能使用MgC和访问MgC调研数据，MgC相关权限请参考**权限管理**。

## 数据线上存储

- **加密保存凭证**：所有用于数据采集的凭证都经过加密处理，以保护凭证的安全。线上采集的凭证仅在线上环境中保存。
- **数据租户级隔离存储**：线上存储数据按租户隔离，每个租户的数据是独立的，不会被其他租户访问。
- **数据存储项透明**：所有被采集和存储的数据项都是透明的，采集数据项参见**采集项列表**。

### 数据分析和呈现

- **审计日志**：所有查询操作都会被记录在后台日志中，有助于确保操作的可追溯性和透明度。
- **操作权限与最小权限原则**：无论哪种采集方式，都需要具备相应的操作权限，并且遵循最小权限原则，即只授予完成特定任务所需的最小权限。
- **MgC服务侧权限要求**：云账号需要具备对应权限才能使用MgC和访问MgC调研数据，MgC相关权限请参考**权限管理**。

## 7.3 采集项列表

本节为您列出各类型采集方式所包含的采集项以及用途。

### 网段扫描

| 采集项 | 说明 | 作用 |
| --- | --- | --- |
| ip | 主机IP | 用于深度采集 |
| port | 主机端口 | 用于深度采集 |
| osType | 系统类型 | 用于深度采集 |
| name | 主机名称 | 用于深度采集 |

### 主机（含深度采集）

| 采集项 | 说明 | 作用 |
| --- | --- | --- |
| name | 主机名称 | 用于迁移前评估 |
| hostName | 主机名 | 用于迁移前评估 |
| eip | 主机公网IP | 用于迁移前评估 |
| eipId | 主机EIP的资源ID | 用于迁移前评估 |
| privateIp | 主机内网IP | 用于迁移前评估 |
| ip | 主机IP | 用于迁移前评估 |
| port | 主机端口 | 用于迁移前评估 |
| collectStatus | 主机采集状态 | 用于迁移前评估 |
| lastCollectTime | 最新采集时间 | 用于迁移前评估 |
| serverStatus | 主机状态 | 用于迁移前评估 |
| mac | 主机MAC地址 | 用于迁移前评估 |
| cpuType | CPU类型 | 用于迁移前评估 |
| cpuCores | CPU核数 | 用于迁移前评估 |

| 采集项 | 说明 | 作用 |
| --- | --- | --- |
| mem | 内存 | 用于迁移前评估 |
| hostType | 主机类型 | 用于迁移前评估 |
| virtualType | 虚拟化类型 | 用于迁移前评估 |
| osType | 操作系统类型 | 用于迁移前评估 |
| osInfo | 操作系统信息 | 用于迁移前评估 |
| architecture | 处理器架构 | 用于迁移前评估 |
| firmware | 固件 | 用于迁移前评估 |
| kernel | 内核 | 用于迁移前评估 |
| disk | 磁盘信息 | 用于迁移前评估 |
| frequency | 主频 | 用于迁移前评估 |
| isOpenOverclock | 是否超频 | 用于迁移前评估 |
| virtioDriver | 是否有virtio驱动 | 用于迁移前评估 |
| filterIds | 主机ID过滤集合 | 用于迁移前评估 |
| instanceId | 平台采集，云服务器资源ID | 用于迁移前评估 |
| platformName | 平台名称 | 用于迁移前评估 |
| platformType | 云平台类型（平台采集） | 用于迁移前评估 |
| regionId | 区域ID（平台采集） | 用于迁移前评估 |
| serverType | 主机类型 | 用于迁移前评估 |
| flavor | 规格 | 用于迁移前评估 |
| cpuUsage | CPU使用率 | 用于迁移前评估 |
| memUsage | 内存使用率 | 用于迁移前评估 |
| diskUsage | 磁盘使用率 | 用于迁移前评估 |
| networkInThroughput | 内网入带宽，单位byte/s | 用于迁移前评估 |
| networkOutThroughput | 内网出带宽，单位byte/s | 用于迁移前评估 |
| networkPpsIn | 网络PPS（个/秒）网络入包 | 用于迁移前评估 |
| networkPpsOut | 网络PPS（个/秒）网络出包 | 用于迁移前评估 |

| 采集项 | 说明 | 作用 |
| --- | --- | --- |
| networkConnections | 网络连接数 | 用于迁移前评估 |
| availableZone | 可用区 | 用于迁移前评估 |
| securityGroupList | 安全组 | 用于迁移前评估 |
| clusterId | 大数据集群ID | 用于迁移前评估 |
| chargeMode | 付费模式 | 用于迁移前评估 |
| assessStatus | 主机TCO评估状态 | 用于迁移前评估 |
| nodeType | 大数据节点类型 | 用于迁移前评估 |

## 数据库（含深度采集）

| 采集项 | 说明 | 作用 |
| --- | --- | --- |
| id | ID | 用于迁移前评估 |
| name | 数据库名称 | 用于迁移前评估 |
| connectAddress | 连接地址 | 用于迁移前评估 |
| dbType | 数据库类型 | 用于迁移前评估 |
| dbName | 数据库名称 | 用于迁移前评估 |
| dbVersion | 数据库版本 | 用于迁移前评估 |
| useSsl | 是否使用SSL | 用于迁移前评估 |
| credentialId | 凭证ID | 用于迁移前评估 |
| instanceId | 实例ID | 用于迁移前评估 |
| vpcId | VPC的ID | 用于迁移前评估 |
| vpcName | VPC名称 | 用于迁移前评估 |
| subnetId | 子网ID | 用于迁移前评估 |
| subnetName | 子网名称 | 用于迁移前评估 |
| platformId | 平台ID | 用于迁移前评估 |
| platformName | 平台名称 | 用于迁移前评估 |
| platformType | 平台类型 | 用于迁移前评估 |
| regionId | 区域ID | 用于迁移前评估 |
| privateAddress | 内网地址 | 用于迁移前评估 |
| publicAddress | 公网地址 | 用于迁移前评估 |

| 采集项 | 说明 | 作用 |
| --- | --- | --- |
| type | 类型 | 用于迁移前评估 |
| nodes | 集群节点信息 | 用于迁移前评估 |
| ids | ID列表 | 用于迁移前评估 |
| assessStatus | TCO评估状态 | 用于迁移前评估 |

## 容器（含深度采集）

| 采集项 | 说明 | 作用 |
| --- | --- | --- |
| id | 编号 | 用于规格评估 |
| name | 名称 | 用于规格评估 |
| credentialId | 绑定的凭证ID | 用于规格评估 |
| collectInfo | 采集器返回的原始信息 | 用于规格评估 |
| collectError | 采集出错时的错误信息 | 用于规格评估 |
| assessStatus | 评估状态 | 用于规格评估 |
| clusterVersion | K8S集群版本 | 用于规格评估 |
| totalNamespaces | 总命名空间数 | 用于规格评估 |
| totalCpuCores | 总CPU核数 | 用于规格评估 |
| totalMemory | 总内存大小(byte) | 用于规格评估 |
| totalNodes | 总节点数 | 用于规格评估 |
| nodes | 集群节点信息 | 用于规格评估 |
| storages | 持久卷存储信息 | 用于规格评估 |
| ingressClass | ingress资源 | 用于规格评估 |
| networkPolicy | networkPolicy状态 | 用于规格评估 |
| loadbalancerServices | loadbalancer型service资源 | 用于规格评估 |
| runtimeClass | 容器运行底座 | 用于规格评估 |
| schedulers | 调度器（用于组织将POD放到合适节点的机制） | 用于规格评估 |
| platformType | 云平台类型 | 用于规格评估 |
| platformId | 云平台ID | 用于规格评估 |
| platformName | 云平台名 | 用于规格评估 |

| 采集项 | 说明 | 作用 |
| --- | --- | --- |
| regionId | 区域ID | 用于规格评估 |
| instanceId | 集群实例ID | 用于规格评估 |
| status | 集群状态 | 用于规格评估 |
| billingMode | 付费模式 | 用于规格评估 |
| creationTime | 集群创建时间 | 用于规格评估 |
| clusterType | 集群类型 | 用于规格评估 |
| clusterSpecs | 集群规格 | 用于规格评估 |
| kubeProxyMode | 服务转发模式(网络模式)：iptables、IPVS等 | 用于规格评估 |
| networkModel | 网络模型：VPC模式、Tunnel、GlobalRouter等 | 用于规格评估 |
| vpcId | VPC的ID | 用于规格评估 |
| vpcName | VPC名称 | 用于规格评估 |
| subnetId | 子网ID | 用于规格评估 |
| subnetName | 子网名称 | 用于规格评估 |
| subnetCidr | 子网网段 | 用于规格评估 |
| containerCidr | 容器网段 | 用于规格评估 |
| serviceCidr | 服务网段 | 用于规格评估 |
| highAvailable | 是否高可用 | 用于规格评估 |
| containerEngine | 容器引擎 | 用于规格评估 |
| cpuAllocation | CPU分配率 | 用于规格评估 |
| cpuUsage | CPU使用率 | 用于规格评估 |
| memoryAllocation | 内存分配率 | 用于规格评估 |
| memoryUsage | 内存使用率 | 用于规格评估 |

## 平台（含深度采集）

| 采集项 | 说明 | 作用 |
| --- | --- | --- |
| id | ID | 用于规格评估 |
| name | 名称 | 用于规格评估 |

| 采集项 | 说明 | 作用 |
| --- | --- | --- |
| platformType | 平台类型 | 用于规格评估 |
| regionId | 区域ID | 用于规格评估 |
| credentialId | 凭证ID | 用于规格评估 |
| ip | 连接地址 | 用于规格评估 |
| serverNum | 主机数 | 用于规格评估 |
| databaseNum | 数据库资源个数 | 用于规格评估 |
| kubernetesNum | 容器资源个数 | 用于规格评估 |
| obsNum | 对象存储资源个数 | 用于规格评估 |
| eipNum | 弹性公网IP个数 | 用于规格评估 |
| elbNum | 负载均衡个数 | 用于规格评估 |
| vpcNum | VPC个数 | 用于规格评估 |
| securityGroupNum | 安全组个数 | 用于规格评估 |
| natNum | NAT网关个数 | 用于规格评估 |
| sfsNum | 文件存储个数 | 用于规格评估 |
| redisNum | Redis个数 | 用于规格评估 |
| kafkaNum | Kafka个数 | 用于规格评估 |
| bigdataNum | 大数据集群个数 | 用于规格评估 |
| pubDomainNum | 公网域名数量 | 用于规格评估 |
| vpcDomainNum | VPC域名数量 | 用于规格评估 |
| routeTableNum | 路由表个数 | 用于规格评估 |
| vpnNum | VPN网关个数 | 用于规格评估 |
| dcNum | 专线个数 | 用于规格评估 |
| cloudConnectNum | 云连接个数 | 用于规格评估 |
| rocketmqNum | RocketMQ个数 | 用于规格评估 |
| collectResourceCategory | 采集资源列表 | 用于规格评估 |

## 存储

| 采集项 | 说明 | 作用 |
| --- | --- | --- |
| taskStatus | 任务状态 | 用于规格评估 |

| 采集项 | 说明 | 作用 |
| --- | --- | --- |
| errorType | 任务类型 | 用于规格评估 |
| totalSize | 总容量大小 | 用于规格评估 |
| totalNum | 总数量 | 用于规格评估 |
| rangeLowerLimit | 最低限制 | 用于规格评估 |
| rangeUpperLimit | 最大限制 | 用于规格评估 |

# 7.4 内网采集权限与原理

## 主机深度采集

- **权限要求**：
  - Windows系统：需要提供具有Administrator权限的账号。
  - Linux系统：需要提供root账号。
- **采集原理**：
  - Windows系统：通过WinRM服务从Edge访问Windows主机，执行PowerShell脚本采集系统信息。

    Linux系统：通过SSH协议从Edge访问Linux主机，将Shell脚本传输至/root/rda目录并执行，以自动化采集系统信息。

## 网段扫描

- **权限要求**：被扫描节点开放对应的远程访问端口（内网可访问或对Edge所在主机开放白名单）。默认情况下Windows开放3389端口，Linux开放22端口，也可以单独指定。
- **采集原理**：通过枚举网段下所有IP地址，得到扫描范围，然后依次循环使用TCP连接到对应IP的远程连接端口。如果3389存在监听则判定该IP操作系统为Windows，如果22端口存在监听则判定该IP操作系统为Linux。

## 性能采集

- **权限要求**：
  - Windows系统：需要提供具有Administrator权限的账号。
  - Linux系统：需要提供root账号。
- **采集原理**：
  - Windows 系统：使用Windows远程管理（WinRM）服务，通过Edge远程访问Windows主机，将PowerShell脚本安全传输至C:/Edge-Scripts路径并执行，以自动化采集系统信息。
  - Linux 系统：通过SSH协议从Edge访问Linux主机，将Shell脚本传输至/root/rda目录并执行，以自动化采集系统信息。

### 数据库采集

- **权限要求**：需要使用具有最高权限的账号进行数据库采集，以确保能够访问所有必要的数据。对于不同的数据库系统，应使用以下账号：
  - MySQL：使用root账号。
  - PostgreSQL：使用postgres账号。
  - MongoDB： 使用admin权限账号。
  - Oracle：使用system权限账号。
  - SQL Server：使用sa账号。
- **采集原理**：连接数据库，基于数据库的查询语句进行采集。

### 中间件采集

- **权限要求**：
  - Redis：使用具有基本访问权限的普通账号即可。
  - Kafka：需要具备访问所有topic的权限以及对topic的容量等信息进行访问的权限。
- **采集原理**：利用Java语言编写的应用程序，集成对应中间件的SDK（Software Development Kit，软件开发工具包）。通过SDK提供的方法和API，与中间件进行交互，实现数据的采集。

### 容器采集

- **权限要求**：需要管理员级别权限的账号导出包含必要访问凭证的文件。
- **采集原理**：利用kspider工具进行数据采集。

### vCenter 采集

- **权限要求**：需要管理员账号，该账号应具备对vCenter环境中所有虚拟机的完全访问权限。
- **采集原理**：通过VSphere SDK提供的资源枚举能力，采集到资源的列表及详细数据。

## 7.5 公网采集权限要求

通过公网采集各云平台资源所需的权限如下：

### 阿里云资源采集

采集阿里云各类资源所需的权限参见下表。

| 资源类型 | 云服务 | Action | 最小权限策略 |
| --- | --- | --- | --- |
| 主机 | ECS | ecs:DescribeInstances | Read |
| | | ecs:DescribeDisks | List |
| | | ecs:DescribeMetricData | List |

| 资源类型 | 云服务 | Action | 最小权限策略 |
| --- | --- | --- | --- |
| 存储 | NAS | nas:DescribeFileSystems | Read |
| | OSS | ListBuckets | oss:ListBuckets |
| | | oss:DescribeMetricData | List |
| 数据库 | RDS | rds:DescribeDBInstances | Read |
| | | rds:DescribeDBInstanceAttribute | Read |
| | MongoDB | rds:DescribeDBInstances | Read |
| | | rds:DescribeDBInstanceAttribute | Read |
| 中间件 | Redis | kvstore:DescribeInstances | List |
| | | kvstore:DescribeInstanceAttribute | Read |
| | | kvstore:DescribeMetricData | List |
| | Kafka | alikafka:ListInstance | Read |
| | | kafka::DescribeMetricData | List |
| | RocketMQ | rocketmq:GetInstance | Read |
| | | rocketmq::DescribeMetricData | List |
| 容器 | K8S ACK | cs:GetClusters | Read |
| | | cs:DescribeClusterDetail | Read |
| | | k8s::DescribeMetricData | List |
| 大数据 | EMR | emr:ListClusters | List |
| 网络 | CEN | cen:ListTransitRouters | Read |
| | | cen:DescribeCenPrivateZoneRoutes | Read |
| | | cen:DescribeRouteServicesInCen | Read |
| | | cen:ListTransitRouterVpcAttachments | List |
| | | cen:ListTransitRouterVbrAttachments | List |
| | | cen:ListTransitRouterVpnAttachments | List |
| | | cen:DescribeCenAttachedChildInstances | Read |

| 资源类型 | 云服务 | Action | 最小权限策略 |
| --- | --- | --- | --- |
| | | 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 |
| | VPC | vpc:DescribePhysicalConnections | Read |

| 资源类型 | 云服务 | Action | 最小权限策略 |
| --- | --- | --- | --- |
| | | vpc:DescribeVirtualBorderRouters | Read |
| | | vpc:DescribeRouteTables | Read |
| | | vpc:DescribeRouteTableList | List |
| | DNS | alidns:DescribeDomainRecords | Read |
| | | alidns:DescribeDomains | Read |
| | Private Zone | pvtz:DescribeZoneVpcTree | Read |
| | | pvtz:DescribeZoneRecords | Read |
| | EIP | ens:DescribeEipAddresses | Read |
| | NAT | ens:DescribeNatGateways | Read |
| | | ens:DescribeSnatTableEntries | List |
| | | ens:DescribeForwardTableEntries | List |

## 华为云资源采集

采集华为云各类资源所需的权限参见下表。

| 资源类型 | 云服务 | Action | 最小权限策略 |
| --- | --- | --- | --- |
| 主机 | ECS | ecs:ListServersDetails<br>ces:BatchListMetricData<br>evs:ListVolumes<br>eip:ListPublicips | • ECS ReadOnlyAccess<br>• EVS ReadOnlyAccess<br>• EIP ReadOnlyAccess |
| 容器 | CCE | cce:ListNodes<br>cce:ListClusters<br>aom:ShowMetricsData | • CCE ReadOnlyAccess<br>• AOM ReadOnlyAccess |
| 大数据 | MRS | mrs:ListClusters<br>mrs:ListHosts | MRS ReadOnlyAccess |
| 数据库 | DDS | dds:ListInstances<br>dds:ListFlavors | DDS ReadOnlyAccess |
| | RDS | rds:ListInstances | RDS ReadOnlyAccess |

| 资源类型 | 云服务 | Action | 最小权限策略 |
| --- | --- | --- | --- |
| 中间件 | 分布式消息服务Kafka版 | dms:ListInstances<br>dms:ShowInstance<br>dms:ListAvailableZones<br>dms:ShowCluster<br>ces:BatchListMetricData | DMS ReadOnlyAccess |
| | 分布式缓存服务DCS | dcs:ListInstances<br>dcs:ListFlavors<br>dcs:ListGroupReplicationInfo<br>ces:BatchListMetricData | DCS ReadOnlyAccess |
| 存储 | OBS | obs:ListBuckets<br>obs:GetBucketPolicy<br>obs:GetBucketAcl<br>obs:GetBucketLifecycle<br>obs:GetBucketMetadata<br>obs:GetBucketVersioning<br>obs:GetBucketStorageInfo<br>obs:GetBucketStoragePolicy<br>ces:BatchListMetricData | • OBS ReadOnlyAccess<br>• CES ReadOnlyAccess<br>以上两个策略不包含的action需要创建自定义策略 |
| | SFS Turbo | sfsturbo:ListShares | SFS Turbo ReadOnlyAccess |
| 网络 | ELB | elb:ListListeners<br>elb:ListLoadbalancers<br>elb:ListPools<br>elb:ListL7policies<br>elb:ListL7rules<br>elb:ListMembers<br>elb:ListFlavors<br>vpc:ListSubnets | ELB ReadOnlyAccess |
| | DNS | dns:ListPublicZones<br>dns:ListPrivateZones<br>dns:ListRecordSetsByZone | DNS ReadOnlyAccess |
| | EIP | eip:ListPublicips | EIP ReadOnlyAccess |

| 资源类型 | 云服务 | Action | 最小权限策略 |
| --- | --- | --- | --- |
| | NAT | nat:ListNatGateways<br>nat:ListNatGatewayDnatRules<br>nat:ListNatGatewaySnatRules<br>vpc:ShowPort<br>vpc:ShowSubnet<br>vpc:ListSubnets | NAT ReadOnlyAccess |
| | VPC | vpc:ListRouteTables<br>vpc:ShowRouteTable<br>vpc:ListVpcs<br>vpc:ListSecurityGroups<br>vpc:ListSecurityGroupRules<br>vpc:ListSubnets | VPC ReadOnlyAccess |

## AWS 资源采集

采集AWS各类资源所需的权限参见下表。

| 资源类型 | 云服务 | Action | 最小权限策略 |
| --- | --- | --- | --- |
| 主机 | EC2 | ec2:DescribeInstances | AmazonEC2ReadOnlyAccess |
| | | ec2:DescribeAddresses | |
| | | ec2:DescribeImages | |
| | | ec2:DescribeVolumes | |
| | | cloudwatch:GetMetricStatistics | |
| 存储 | EFS | elasticfilesystem:DescribeFileSystems | AmazonElasticFileSystemReadOnlyAccess |
| | | elasticfilesystem:DescribeMountTargets | |
| | | cloudwatch:GetMetricStatistics | |
| | S3 | s3:ListObjectsV2 | AmazonS3ReadOnlyAccess |
| | | cloudwatch:GetMetricStatistics | |

| 资源类型 | 云服务 | Action | 最小权限策略 |
| --- | --- | --- | --- |
| 数据库 | RDS | rds:DescribeDBClusters | AmazonRDSReadOnlyAccess |
| | | rds:DescribeDBInstances | |
| | | ec2:DescribeSecurityGroups | |
| 中间件 | ElastiCache | elasticache:DescribeCacheClusters | AmazonElastiCacheReadOnlyAccess |
| | | elasticache:DescribeReplicationGroups | |
| | | cloudwatch:GetMetricStatistics | |
| | MSK | kafka:ListClustersV2 | AmazonMSKReadOnlyAccess |
| | | cloudwatch:GetMetricStatistics | |
| 容器 | EKS | eks:DescribeCluster | 无对应的权限策略，需自定义策略 |
| | | eks:ListClusters | |
| | | ec2:DescribeInstances | |
| | | ec2:DescribeSubnets | |
| | | cloudwatch:GetMetricStatistics | |
| 大数据 | EMR | elasticmapreduce:DescribeCluster | AmazonEMRReadOnlyAccessPolicy_v2 |
| | | elasticmapreduce:ListClusters | |
| | | elasticmapreduce:ListInstanceGroups | |
| | | elasticmapreduce:ListInstances | |
| | | ec2:DescribeInstances | AmazonEC2ReadOnlyAccess |
| 网络 | EIP | ec2:DescribeAddresses | AmazonEC2ReadOnlyAccess |
| | ELB | elasticloadbalancing:DescribeLoadBalancers | ElasticLoadBalancingReadOnly |
| | NAT | ec2:DescribeNatGateways | AmazonEC2ReadOnlyAccess |

| 资源类型 | 云服务 | Action | 最小权限策略 |
| --- | --- | --- | --- |
| | 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 | |
| | VPC | ec2:DescribeSubnets | AmazonEC2ReadOnlyAccess |
| | | ec2:DescribeVpcs | |

## 腾讯云资源采集

采集腾讯云各类资源所需的权限参见下表。

| 资源类型 | 云服务 | Action | 最小权限策略 |
| --- | --- | --- | --- |
| 主机 | CVM | cvm: DescribeInstances<br>cvm: DescribeImages<br>cvm:DescribeSecurityGroups<br>cbs: DescribeDisks<br>vpc: DescribeAddresses<br>vpc: DescribeNetworkInterfaces<br>vpc: DescribeSubnets<br>monitor:GetMonitorData | QcloudCVMReadOnlyAccess |
| 数据库 | CDB | cdb:DescribeDBInstances | QcloudCDBReadOnlyAccess |
| | PostgreSQL | postgres:DescribeDBInstances | QcloudPostgreSQLReadOnlyAccess |

| 资源类型 | 云服务 | Action | 最小权限策略 |
| --- | --- | --- | --- |
| | MongoDB | mongodb:DescribeDBInstances<br>mongodb:DescribeDBInstanceNodeProperty | QcloudMongoDBReadOnlyAccess |
| | SQLServer | sqlserver:DescribeDBInstances<br>sqlserver:DescribeReadOnlyGroupList | QcloudSQLServerReadOnlyAccess |
| 存储 | COS | cos:GetService<br>cos:GetBucketACL<br>cos:GetBucketLifecycle<br>cos:GetBucketVersioning<br>monitor:GetMonitorData | QcloudCOSReadOnlyAccess |
| | CFS | cfs:DescribeCfsFileSystems<br>cfs:DescribeMountTargets | QcloudCFSReadOnlyAccess |
| 网络 | DNSPod | dnspod:DescribeDomainList<br>dnspod:DescribeRecordList | QcloudDNSPodReadOnlyAccess |
| | WAF | waf:DescribeDomains<br>waf:DescribeInstances | QcloudWAFReadOnlyAccess |
| | CLB | clb:DescribeLoadBalancersDetail<br>clb:DescribeTargets<br>cvm: DescribeInstances | QcloudCLBReadOnlyAccess<br>QcloudCVMReadOnlyAccess |

## Azure 资源采集

采集Azure各类资源所需的权限参见下表。

| 资源类型 | 云服务 | 服务 | 最小权限策略 |
| --- | --- | --- | --- |
| 主机 | Virtual Machines | Microsoft Classic Compute | Microsoft.ClassicCompute/virtualMachines/read |
| | | Microsoft Azure Monitor | Microsoft.Insights/MetricDefinitions/Read |
| | | Microsoft Network | Microsoft.Network/networkInterfaces/read |

| 资源类型 | 云服务 | 服务 | 最小权限策略 |
| --- | --- | --- | --- |
| 存储 | Storage Accounts | Microsoft Azure Monitor | Microsoft.Insights/MetricDefinitions/Read |
| | | Microsoft Classic Storage | Microsoft.ClassicStorage/storageAccounts/read |
| 数据库 | 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 |
| 中间件 | Azure Cache for Redis | Microsoft Management | Microsoft.Management/getEntities/action |
| | Event Hubs | Microsoft Management | Microsoft.Management/getEntities/action |
| 容器 | Kubernetes services | Microsoft Classic Compute | Microsoft.ClassicCompute/virtualMachines/read |
| | | Microsoft Azure Monitor | Microsoft.Insights/MetricDefinitions/Read |
| | | Microsoft Management | Microsoft.Management/getEntities/action |
| 网络 | 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 |

| 资源类型 | 云服务 | 服务 | 最小权限策略 |
| --- | --- | --- | --- |
| | 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 |

## 七牛云资源采集

采集七牛云存储资源所需的权限参见下表。

| 资源类型 | 云服务 | Action | 最小权限策略 |
| --- | --- | --- | --- |
| 存储 | 对象存储(Kodo) | kodo:buckets | QiniuKodoReadOnlyAccess |

## 金山云资源采集

采集金山云存储资源所需的权限参见下表。

| 资源类型 | 云服务 | Action | 最小权限策略 |
| --- | --- | --- | --- |
| 存储 | 对象存储(KS3) | ks3:ListBuckets | KS3ReadOnlyAccess |

## 谷歌云资源采集

采集谷歌云各类资源所需的权限参见下表。

| 资源类型 | 云服务 | 权限 | 角色(角色ID) |
| --- | --- | --- | --- |
| 主机 | Compute Engine | compute.instances.list | Compute Viewer(roles/compute.viewer) |
| | | compute.machineTypes.get | |
| | | compute.disks.get | |
| | | compute.networks.get | |
| | | compute.regions.get | |

| 资源类型 | 云服务 | 权限 | 角色(角色ID) |
| --- | --- | --- | --- |
| 存储 | Cloud Storage | storage.buckets.list | Storage Admin(roles/storage.admin) 或 Viewer(roles/viewer) |
| | | storage.objects.list | Storage Object Viewer(roles/storage.objectViewer) 或 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) |
| 数据库 | Cloud SQL | cloudsql.instances.list | Cloud SQL Viewer(roles/cloudsql.viewer) |
| | | cloudsql.databases.list | |
| | | cloudsql.tiers.list | 不需要角色 |
| 中间件 | Memorystore Redis | redisService.instances.list | Cloud Memorystore Redis Viewer(roles/redis.viewer) |
| | | redisService.clusters.list | |
| 容器 | Kubernetes Engine | container.clusters.list | Kubernetes Engine Cluster Viewer(roles/container.clusterViewer) |
| | Compute Engine(k8s) | compute.regions.get | Compute Viewer(roles/compute.viewer) |
| | | compute.networks.list | |
| | | compute.subnetworks.list | |
| 网络 | Compute Engine(clb) | compute.firewalls.list | Compute Viewer(roles/compute.viewer) |
| | | compute.forwardingRules.list | |
| | | compute.globalForwardingRules.list | |
| | | compute.backendServices.get | |

| 资源类型 | 云服务 | 权限 | 角色(角色ID) |
| --- | --- | --- | --- |
| | | 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 责任共担

华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图7-3所示。

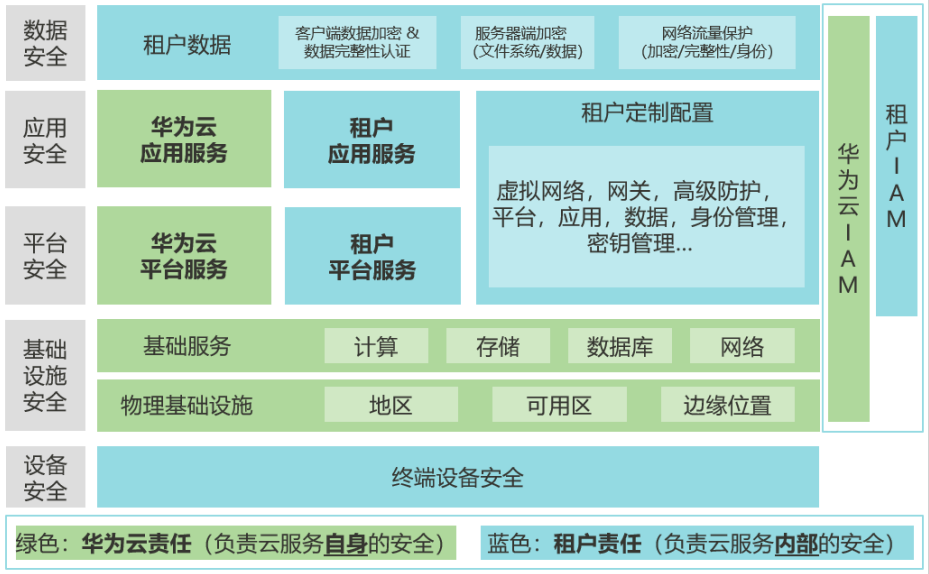
- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火

墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

**图 7-3** 华为云安全责任共担模型



# 8 权限管理

如果您需要对华为云上的迁移中心 MgC，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（ Identity and Access Management，简称IAM ）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并授权控制他们对资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有MgC的使用权限，但是不希望他们拥有删除MgC等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用MgC，但是不允许删除MgC的权限策略，控制他们对MgC资源的使用范围。

如果账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用MgC服务的其他功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**《 IAM产品介绍 》**。

## MgC 权限

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

权限根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。

如**表8-1**所示，包括了MgC的所有系统策略。

**表 8-1** MgC 系统权限

| 策略名称 | 描述 | 策略类别 | 策略内容 |
| --- | --- | --- | --- |
| MgC FullAccess | 迁移中心管理员权限，拥有操作MgC的所有权限。 | 系统策略 | **MgC FullAccess策略内容** |
| MgC ReadOnlyAccess | 迁移中心只读权限，仅能查看MgC资源，无法进行操作。 | 系统策略 | **MgC ReadOnlyAccess策略内容** |
| MgC DiscoveryAccess | 迁移中心资源发现操作权限，拥有操作资源发现功能的权限和只读权限。 | 系统策略 | **MgC DiscoveryAccess策略内容** |
| MgC AssessAccess | 迁移中心评估操作权限，拥有操作评估功能、资源发现功能的权限和只读权限。 | 系统策略 | **MgC AssessAccess策略内容** |
| MgC MigrateAccess | 迁移中心迁移操作权限，拥有操作迁移功能、评估功能、资源发现功能的权限和只读权限。 | 系统策略 | **MgC MigrateAccess策略内容** |
| MgC AppDiscoveryAccess | 迁移中心应用发现操作权限，拥有操作应用发现功能、资源发现功能的权限和只读权限。 | 系统策略 | **MgC AppDiscoveryAccess策略内容** |
| MgC MrrAccess | 迁移中心业务验证操作权限，拥有业务验证功能的权限和只读权限。 | 系统策略 | **MgC MrrAccess策略内容** |

**表8-2**列出了MgC常用操作与系统策略的授权关系，您可以参照该表选择合适的系统策略。具体操作请参考：**创建用户并授权使用MgC**。

**表 8-2** MgC 操作与系统策略关系

| 操作 | MgC FullAccess | MgC ReadOnlyAccess | MgC DiscoveryAccess | MgC AssessAccesss | MgC Migrate Access | MgC AppDiscoveryAccess |
| --- | --- | --- | --- | --- | --- | --- |
| 操作迁移中心资源 | √ | x | x | x | x | x |
| 查看迁移中心资源 | √ | √ | √ | √ | √ | √ |
| 操作迁移中心资源发现功能 | √ | x | √ | √ | √ | √ |

| 操作 | MgC FullAccess | MgC ReadOnlyAccess | MgC DiscoveryAccess | MgC AssessAccesss | MgC MigrateAccess | MgC AppDiscoveryAccess |
| --- | --- | --- | --- | --- | --- | --- |
| 操作迁移中心评估功能 | √ | x | x | √ | √ | x |
| 操作迁移中心迁移功能 | √ | x | x | x | √ | x |
| 操作迁移中心应用发现功能 | √ | x | x | x | x | √ |

## MgC FullAccess 策略内容

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "mgc:*:*",
            "iam:agencies:listAgencies",
            "iam:roles:listRoles",
            "iam:quotas:listQuotas",
            "iam:permissions:listRolesForAgency"
         ],
         "Effect": "Allow"
      }
   ]
}
```

## MgC ReadOnlyAccess 策略内容

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

## MgC DiscoveryAccess 策略内容

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

## MgC AssessAccess 策略内容

```
{
   "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 策略内容

```
{
   "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 策略内容

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

## MgC MrrAccess 策略内容

```
{
        "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 约束与限制

本文介绍迁移中心（MgC）在使用过程中的约束与限制，包括MgC服务的使用限制，进行主机迁移、跨可用区（AZ）迁移和存储迁移时存在的约束与限制。

## MgC 区域限制

MgC部署在“**亚太-新加坡**”、“**土耳其-伊斯坦布尔**”、“**拉美-圣保罗一**”、“**拉美-圣地亚哥**”四个区域。虽然MgC为Region级服务，但提供了全局服务的能力。即在一个Region开通服务后，支持所有Region的迁移。出于信息安全的考虑，所有的采集数据、任务记录等信息都会存储在开通MgC服务的区域。

## 主机迁移相关约束与限制

使用迁移中心进行主机迁移的约束与限制参见**表9-1**。

**表 9-1** 主机迁移约束与限制

| 类别 | 约束与限制 |
| --- | --- |
| 主机迁移工作流 | • 每台主机只能被一个工作流迁移。<br>• 当前主机迁移工作流在新建目的端情况下，不支持迁移源端固件类型是UEFI的主机。如果想要迁移固件类型是UEFI的主机，请提前绑定已有UEFI的目的端主机或使用SMS服务迁移。<br>• 主机迁移服务 SMS的**约束与限制**同样适用于主机迁移工作流。<br>• 源端同一台主机进行第二次迁移，需要停止第一次创建的迁移工作流，停止源端主机SMS-Agent进程，并在SMS控制台删除该主机再重新创建迁移工作流。 |
| 评估推荐 | • 评估的目的端主机磁盘大小不小于源端磁盘的大小。<br>• 评估的目的端镜像OS类型和源端OS类型一致，即Windows推荐Windows镜像，Linux推荐Linux镜像。<br>• 评估推荐的磁盘类型规格在目的端Region配额充足。 |
| 迁移前 | 迁移前请确认主机已经评估完成。 |

| 类别 | 约束与限制 |
| --- | --- |
| 迁移中 | 迁移工作流创建后，不能关闭或者重启源端主机，不能变更源端磁盘，否则会导致迁移失败，需要重新迁移。 |
| 源端主机设置 | 源端Windows主机需要**关闭防火墙**和**杀毒软件**，并**开启winrm服务**（在powershell命令窗口中输入winrm quickconfig开启）。 |
| 网络 | 请保证源端和目的端能够正常通信，目的端为Linux系统时需要对源端开放22端口，目的端为Windows系统时需要对源端开放22、8899、8900端口。 |
| 安装Edge的主机 | • 建议在源端内网环境中准备一台用于安装Edge的Windows主机，并确保该Windows主机可以连接公网。<br>• 安装Edge的Windows主机，powershell版本需要大于3.0。可以在powershell命令窗口使用$host指令查看版本号。 |

## 跨 AZ 迁移约束与限制

使用迁移中心进行跨可用区（AZ）迁移的约束与限制参见**表9-2**。

**表 9-2** 跨可用区（AZ）迁移约束与限制

| 类别 | 约束与限制 |
| --- | --- |
| 源端服务器规格 | 迁移过程中不会进行驱动安装，源端为XEN架构时，需要自行**安装KVM驱动**。 |
| 源端服务器数量 | • 简单批次最多同时迁移30台。<br>• 手动创建大批量迁移，单个项目最多同时迁移100台。<br>• 同时进行迁移的源端主机越多，迁移速度越慢。 |
| 源端服务器数据量 | • 不支持迁移系统盘超过1T的服务器。<br>• 不建议迁移容量超过4T的服务器 |
| 源端服务器状态 | 不支持迁移处于“保留期”且为冻结状态的服务器。 |
| 目的端服务器 | • 不支持已有目的端方式迁移。<br>• 采用按需计费方式创建目的端，且不支持自动切换为包周期计费模式，需要在迁移完成后自行切换计费模式。 |
| 共享文件系统 | 只支持迁移本地磁盘上的文件，不支持迁移共享文件系统。<br>例如：NFS（Network File System）、Common Internet File System、NAS（Network Attached Storage）等系统中的文件。 |
| 应用与硬件绑定 | 不支持迁移含有与硬件绑定的应用的系统。 |
| 加入域的主机 | 迁移加入域主机时，在迁移完成后，目的端服务器需要重新加入域。 |

| 类别 | 约束与限制 |
| --- | --- |
| 加密文件 | 不支持迁移含有受保护文件夹、加密卷的系统。 |
| 服务器外挂存储 | 不支持迁移服务器挂载的外部存储。 |
| 目的端服务器密码 | • Linux主机迁移后目的端密码与源端服务器保持一致。<br>• Windows主机迁移后目的端密码无法保证与源端服务器一致，详情请参考**AZ迁移注意事项**。 |

## 存储迁移约束与限制

使用迁移中心进行存储迁移的约束与限制参见**表9-3**和**表9-4**。

**表 9-3** 存储迁移通用约束与限制

| 类别 | 约束与限制 |
| --- | --- |
| 多版本对象迁移 | 默认只迁移源端多版本对象中的最新版本，不支持迁移历史版本的对象存储数据。 |
| 目的端桶存储类别 | 目的端桶的存储类别只能为**标准存储**或者**低频访问存储**。迁移完成后，可以自行修改桶的存储类别。 |
| 迁移对象 | • 对象名称不能包含特殊字符。<br>• 单个对象大小不能超过：500 MB x 10000 = 4.76837158203125 TB，否则可能会导致迁移失败。 |
| 迁移网络 | 支持公网、内网和专线迁移。 |
| 软链接 | • 不支持源端路径为软链接路径的迁移。如果源端包含软链接，请进行如下处理：<br>– 填写实际的文件路径。<br>– 迁移完成后，手动在目的端创建相应的软链接。<br>• 不支持软连接的迁移：**NAS_SMB的迁移**、**NAS_NFS到OBS的迁移**。<br>• **NAS_NFS到NAS_NFS的迁移**和**阿里云 OSS到NAS_NFS的迁移**，如果源端存在软链接，请启用“**迁移元数据**”功能。否则，迁移后软链接会变成普通文件，从而失去链接功能。<br>**须知**<br>如果迁移对象中包含软链接，在迁移过程中，可能会因为软链接指向的对象尚未完全迁移到目的端导致校验失败，进而使任务失败。对于这种情况，请等待软链接指向的对象完全迁移到目的端后重试任务。 |
| 迁移范围 | 支持单桶迁移和批量桶迁移。 |

| 类别 | 约束与限制 |
| --- | --- |
| 元数据迁移 | ● 仅支持**中文字符、英文字符、数字和中划线【-】**迁移。除上述字符外，其他所有字符均不支持。<br>– **中文字符**：迁移过程中，会被转换成URL编码形式。<br>**注意**<br>不支持**中文标点符号**迁移，由于中文标点符号不会被转换成URL编码，因此元数据中包含中文标点符号时，将无法迁移成功。<br>– **英文字符、数字与中划线【-】**：迁移过程中不需要进行编码转换，可以直接迁移。<br>● 异构迁移不支持元数据迁移。 |
| 归档数据 | 归档类型的对象存储要实现迁移，必须预先解冻，待解冻完成后再创建迁移工作流，解冻时请注意如下事项：<br>● 请务必在解冻完成后再创建迁移工作流。<br>● 请根据待迁移的数据总量评估并设置解冻有效期，以防迁移期间数据再次变成归档状态。<br>● 解冻操作可能会产生一定的费用，由源端云厂商收取，计费规则请咨询源端云厂商。 |
| 并发子任务数 | 用户自定义。配置的数目不能超过可用迁移节点数x10。<br>例如：可用的迁移节点数为2，则最大子任务数配置数目需要≤20。 |
| 列表迁移文件 | 列表文件存放地址必须与目的端桶处于同一区域。<br>● 列表文件类型必须为.txt，其他文件类型不做处理，并且该文件元数据中的“ContentType”只能为：“text/plain”。<br>● txt文件行数不超过100000行。<br>● 单个列表文件大小不能超过300 MB。<br>● 列表文件存放目录下的列表文件个数不能超过10000个。<br>● 列表文件必须是UTF-8无BOM格式编码格式。<br>● 列表文件中每行长度不要超过65535，否则会导致迁移失败。<br>● 列表文件的元数据中不能设置“ContentEncoding”，否则会导致迁移失败。<br>● 列表文件中每行使用制表符（键盘上Tab键）\t分割URL和目的端对象名称，请勿使用空格。格式为：[URL][制表符][目的端对象名称]，其中源端对象名称如果包含中文、特殊字符必须使用URL Encode对URL编码；目的端对象名称如果包含中文、特殊字符也需要使用URL Encode编码。<br>● 列表文件中每行不要添加无效空格，否则会将空格作为对象名，导致迁移失败。 |

**表 9-4** 文件系统迁移约束与限制

| 场景 | 约束与限制 |
| --- | --- |
| 源端为SMB系统 | ● 不支持迁移单个文件夹下平铺超过500万个文件的场景。<br>● 不支持断点续传。<br>● 不支持迁移软链接。 |
| 源端为NAS文件系统 | ● 支持迁移的文件类型：普通文件、目录文件、软链接文件、硬链接文件。<br>**注意**<br>文件句柄被占用或源端文件被删除，均会导致迁移失败。<br>● 不支持字符设备文件、块设备文件、套接字、管道文件等特殊文件的迁移。<br>● 软链接不支持元数据的迁移。 |

# 10 与其他服务的关系

迁移中心与其他服务的交互功能请参考表10-1。

**表 10-1** 迁移中心与其他服务的关系

| 相关服务 | 交互功能 |
| --- | --- |
| 主机迁移服务（Server Migration Service，SMS） | 提供主机迁移能力，可以将其他云厂商服务器上的应用和数据迁移到华为云。 |
| 统一身份认证服务（Identity and Access Management，IAM） | 通过IAM服务实现以下功能：<br>• 用户身份鉴权<br>• IAM用户权限设置<br>• IAM委托设置 |
| 设备接入服务（IoTDA） | 通过协同通道（IoTDA）下发插件管理、凭证管理、采集和迁移任务到Edge，同时Edge侧将资源信息同步至MgC，实现满足安全、实时和性能的双向协同通信。 |
| 对象存储迁移服务 （Object Storage Migration Service，OMS） | 提供对象存储迁移能力，可以将其他云平台对象存储服务中的数据迁移至华为云对象存储服务OBS中。 |
| 云备份（Cloud Backup and Recovery，CBR） | 提供对云硬盘、弹性云服务器的备份保护服务。 |
| 镜像服务（Image Management Service，IMS | 通过镜像创建弹性云服务器。 |
| 弹性云服务器（Elastic Cloud Server，ECS） | 将源端服务器的系统、应用和文件等数据迁移到华为云弹性云服务器。 |
| 消息通知服务（Simple Message Notification，SMN） | 及时获取迁移任务的结果。 |
| 数据加密服务（Data Encryption Workshop，DEW） | 将迁移到华为云OBS桶中的文件进行KMS加密。 |

| 相关服务 | 交互功能 |
| --- | --- |
| 对象存储服务（Object Storage Service，OBS） | 接收源端对象存储数据。 |