资源治理中心

快速入门

文档版本 02

发布日期 2025-02-20

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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

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 准备工作

在使用资源治理中心服务之前，您需要完成本文中的准备工作：

开通企业中心

在启用RGC前，需要开通企业中心并成为组织的管理账号，请执行以下准备工作：

步骤1 进入企业中心控制台。

步骤2 单击“免费开通”，进入申请开通企业中心页面。

步骤3 勾选“我已阅读并同意《华为云企业管理服务使用声明》”，并单击“免费开通”。开通后您将自动成为企业主账号，详情参见：**开通企业中心功能**。

----结束

2 搭建并启用 Landing Zone

背景说明

通过RGC服务，预计可实现以下功能：

- RGC将会拥有必要的权限来治理Organizations内的所有组织单元以及成员账号。
- 您需要在RGC中搭建Landing Zone，并且设置您的多账号环境治理范围。RGC不会将云上环境治理扩展到您Organizations服务内现有的其他组织单元和成员账号。
- 当您将现有组织单元由RGC纳入治理范围的过程，称为注册组织单元。
- 在搭建Landing Zone后，您可以在RGC中注册现有的组织单元。

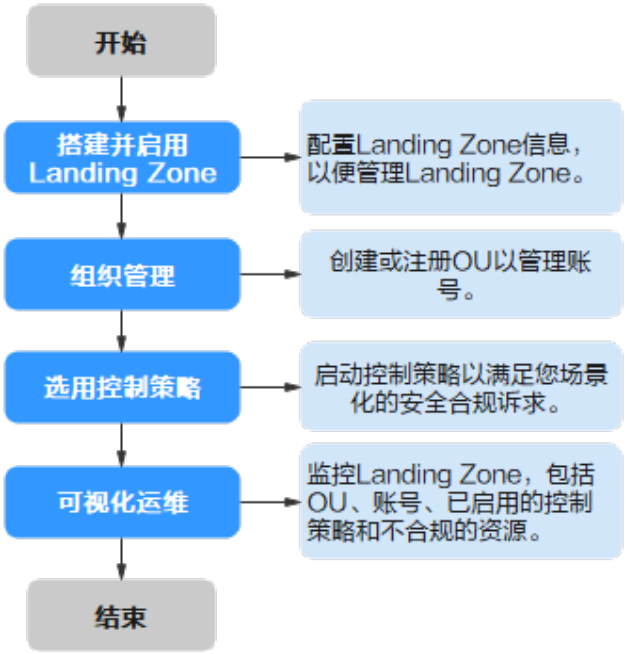
前提条件

当前账号需要先**开启企业中心**服务。

入门流程

图2-1为RGC服务入门使用流程。

图 2-1 RGC 服务入门使用流程



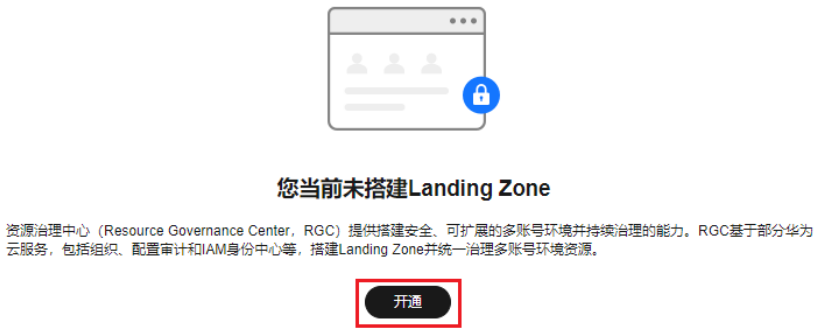
搭建 Landing Zone

步骤1 以企业主账号身份登录的华为云。

步骤2 单击“三”，选择“管理与监管 > 资源治理中心 RGC”。

步骤3 在服务开通页，单击“立即开通”。

图 2-2 开通 RGC



步骤4 设置RGC的主区域，该区域是Landing Zone部署的默认区域。

图 2-3 设置主区域

步骤5 单击“下一步”。

步骤6 在配置组织单元页面，配置核心组织单元。

- 创建核心组织单元：为了在Landing Zone中构建完善的组织单元结构，RGC将为您预设一个核心组织单元。此组织单元包含两个核心账号，分别是日志归档账号和安全审计账号（也称为审计账号）。

  组织单元名称必须是唯一的，核心组织单元的默认组织单元名称为“Security”。核心组织单元名称不支持在设置Landing Zone后进行修改。
- 不创建核心组织单元：如果不希望RGC在您的组织中创建组织单元，则选择不创建核心组织单元。

图 2-4 设置核心组织单元

步骤7 选择是否创建附加组织单元。

为了帮助设置多账号系统，建议您在搭建Landing Zone时创建附加组织单元，该组织单元可以作为业务账号的容器或分组单元。搭建Landing Zone后，您可以创建更多组织单元。

- 创建附加组织单元：在设置Landing Zone同时创建附加组织单元。组织单元的名称必须是唯一的，附加组织单元的默认组织单元名称为“Sandbox”。
- 不创建附加组织单元：设置Landing Zone后组织除预设的核心组织单元外无其他的组织单元，您可以后续自行创建更多组织单元。

图 2-5 创建附加组织单元

步骤8 单击“下一步”。

步骤9 在配置核心账号界面，配置管理账号。

- 开通IAM身份中心：输入IAM身份中心账号的邮箱地址。管理账号邮箱地址不可以与IAM身份中心其他用户所使用的邮箱地址相同。该邮箱将用于在IAM身份中心创建RGC管理员，该IAM身份中心用户拥有管理员权限。
- 不开通IAM身份中心：如果不希望RGC在IAM身份中心创建RGC管理员身份的用户以及其他用户组、权限集等资源，则选择不开通IAM身份中心。

图 2-6 配置管理账号

步骤10 配置日志存档账号。日志存档账号用于存储所有账号的API活动和资源配置的日志。

- “账号类型”选择“创建新账号”：
  - 账号邮箱：输入日志存档账号的邮箱，日志存档账号邮箱地址不得与现有华为云账号使用的邮箱地址相同。长度范围为0至64个字符。
  - 账号名称：输入日志存档账号的名称，需要确保日志存档账号名称唯一，不可以与其他账号名称相同。在设置Landing Zone后，无法修改该名称。账号名只能包含数字、英文字母、下划线（_）、中划线（-）且不能以数字开头。只能为6-32个字符。
- “账号类型”选择“使用现有账号”：

  使用的现有账号需要归属于管理账号所在的组织中，且已对该账号进行设置委托，设置委托的详细操作请参阅**设置委托**。如果现有账号中包含Config相关的资源，则必须先删除或修改现有的Config资源，Landing Zone搭建才可以将现有的账号纳管至RGC。
  - 账号邮箱：输入日志存档账号的邮箱，日志存档账号邮箱地址不得与现有华为云账号使用的邮箱地址相同。长度范围为0至64个字符。
  - 账号名称：输入华为云已注册账号的账号名称。
  - 账号ID：需要输入华为云已注册账号的账号ID。该账号ID不能为管理账号或其他组织下成员账号的账号ID。

图 2-7 配置日志存档账号

步骤11 配置审计账号。审计账号具有对组织内所有成员账号的访问权限，建议对访问该账号的身份进行强管控。

- “账号类型”选择“创建新账号”：
  - 告警邮箱：输入审计账号的告警邮箱，该邮箱用于接收RGC预置告警通知，请谨慎选择。告警邮箱地址不得与现有华为云账号使用的邮箱地址相同。长度范围为0至64个字符。
  - 账号名称：需要确保审计账号名称唯一，不可以与其他账号名称相同。在设置Landing Zone后，无法修改该名称。账号名只能包含数字、英文字母、下划线（_）、中划线（-）且不能以数字开头。只能为6-32个字符。
- “账号类型”选择“使用现有账号”：

  使用的现有账号需要归属于管理账号所在的组织中，且已对该账号进行设置委托，设置委托的详细操作请参阅**设置委托**。如果现有账号中包含Config相关的资源，则必须先删除或修改现有的Config资源，Landing Zone搭建才可以将现有的账号纳管至RGC。
  - 告警邮箱：输入审计账号的告警邮箱，该邮箱用于接收RGC预置告警通知，请谨慎选择。长度范围为0至64个字符。
  - 账号名称：输入华为云已注册账号的账号名称。
  - 账号ID：需要输入华为云已注册账号的账号ID。该账号ID不能为管理账号或其他组织下成员账号的账号ID。

图 2-8 配置审计账号

步骤12 单击“下一步”。

步骤13 配置是否启用CTS。

如果您未在搭建Landing Zone页面启用CTS，则RGC将不会管理您的CTS操作审计日志。RGC强烈建议您启用CTS。预置强制控制策略将会检测已纳管的账号是否已启用CTS。

图 2-9 启用 CTS

步骤14 配置日志存放的OBS桶。可以选择创建OBS桶或使用现有OBS桶。当选择创建新的日志存档账号时，将默认选择创建OBS桶。日志数据使用SSE-OBS加密模式进行静态加密，由OBS创建和管理密钥。

- 创建OBS桶：需要配置日志在OBS桶中的保留时长。日志将会自动存放至系统创建的两个默认OBS桶中，不支持自定义OBS桶名。
  - 日志汇聚桶数据保留时长：默认设置为1年。最长设置为15年。

    该桶用于存储组织内所有账号的CTS记录的操作审计日志和已纳管账号的Config记录的资源快照，并且存放于名为“rgcservice-managed-audit-logs-{管理账号ID}”的桶中，{}中表示变量，根据实际情况进行显示。
  - OBS桶访问日志保留时长：默认设置为10年。最长设置为15年。

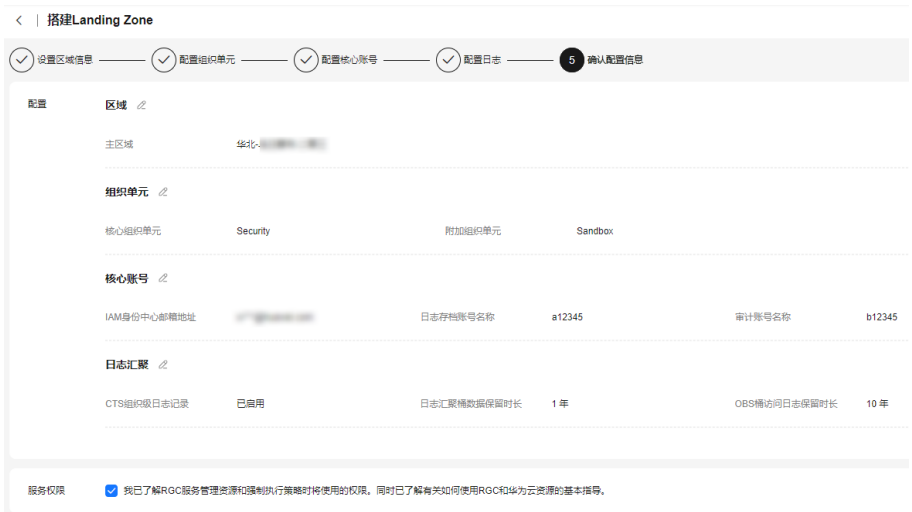
    该桶将会存放访问上述日志汇聚桶而产生的日志，并且存放于名为“rgcservice-managed-access-logs-{管理账号ID}”的桶中，{}中表示变量，根据实际情况进行显示。
- 使用现有OBS桶：需要输入日志账号下的OBS桶名称，如使用其他OBS桶则将会导致Landing Zone搭建失败。为了您的数据安全，建议使用桶策略为私有的OBS桶。

图 2-10 配置 OBS 桶日志保留时长

步骤15 确认Landing Zone配置信息，确认无误后，勾选“我已了解RGC服务管理资源和强制执行策略时将使用的权限。同时已了解有关如何使用RGC和华为云资源的基本指导。”。

可以在统一身份认证控制台中，在左侧导航栏选择“身份策略”，搜索“RGCServiceAgencyPolicy”，查看RGC服务管理资源和强制执行策略时将使用的权限。

图 2-11 确认配置信息



步骤16 单击“搭建Landing Zone”，完成Landing Zone配置。

须知

您为审计账号配置的告警邮箱将收到来自RGC支持区域的通知订阅确认电子邮件。如果您希望您的审计账号接收合规邮件，则必须在每个区域的每封邮件中单击确认订阅的链接。

----结束

相关说明

- 后续需要对现有的组织单元和成员账号进行部署和管理，请参见**组织管理概述**。
- Landing Zone搭建成功后，系统将自动为核心账号所在的组织单元绑定所有的预防性控制策略。
- Landing Zone搭建成功后，系统将为存放日志的OBS桶自动配置名为“AllowCtsAccessBucket”和“AllowConfigAccessBucket”的桶策略，详细的桶策略内容可以前往OBS控制台进行查看。
- Landing Zone搭建成功后，系统将为存放日志的OBS桶自动配置“对象读权限”，使核心账号拥有查看桶内日志的权限。

3 通过控制策略治理多账号环境

RGC提供多种控制策略，在RGC中创建的OU将会自动应用必选的控制策略，管理账号可以自行决定是否启用可选或强烈推荐的控制策略。

在组织中创建的OU需要在RGC中注册后，即可应用控制策略。

在RGC中创建的OU应用控制策略时，预防性控制策略将应用于该OU下所有的成员账号，包含已纳管或未纳管的账号，检测性控制策略仅能应用于已纳管的账号。

约束与限制

- 仅实施类型为“强烈推荐”和“可选”的控制策略可以手动启用或关闭。
- 控制策略不支持绑定至未注册的组织单元、根组织单元和核心组织单元。

启用控制策略

步骤1 以RGC管理账号的身份登录华为云，进入华为云RGC控制台。

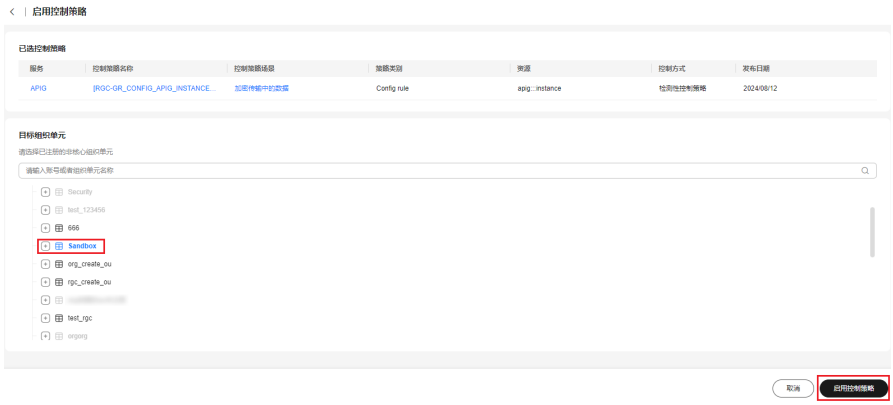
步骤2 进入“控制策略管理 > 策略列表”页面，在策略列表中，找到需要启用的策略。

步骤3 单击“操作”列下的“启用控制策略”。

图 3-1 启用控制策略

步骤4 选择需要绑定的组织单元。

图 3-2 绑定组织单元



步骤5 单击右下角“启用控制策略”，等待几分钟后，完成启用。

----结束

查看控制策略应用结果

步骤1 以RGC管理账号的身份登录华为云，进入华为云RGC控制台。

步骤2 在总览页面，可以看到Landing Zone中“组织单元和账号”、“已启用的控制策略”、“不合规资源”、“已注册组织单元”和“已纳管账号”的情况。

步骤3 在“不合规资源”区域，单击账号名称，可以查看不合规资源的详情。

针对不合规资源的情况，管理账号可以进行资源的调整。

图 3-3 不合规资源

----结束

禁用控制策略

步骤1 以RGC管理账号的身份登录华为云，进入华为云RGC控制台。

步骤2 进入“控制策略管理 > 策略列表”页面，在策略列表中，找到需要禁用的策略。

步骤3 单击策略名称，进入控制策略详情。

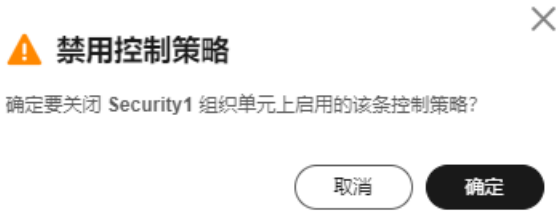
步骤4 在“已启用组织单元”的页签中，找到需要解绑的组织单元。

图 3-4 解绑控制策略

步骤5 单击“操作”列的“禁用控制策略”。

步骤6 单击“确认”，等待几分钟后，完成关闭。

图 3-5 禁用控制策略



----结束