

资源治理中心

快速入门

文档版本 01
发布日期 2024-01-30



版权所有 © 华为技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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>

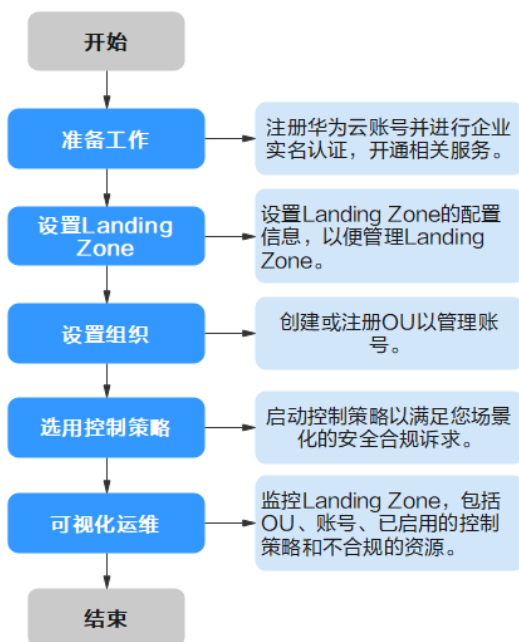
目录

1 入门流程.....	1
2 准备工作.....	2
3 搭建并启用 Landing Zone.....	3
4 通过控制策略治理多账号环境.....	8
5 修订记录.....	11

1 入门流程

图1-1为RGC服务入门使用流程。

图 1-1 RGC 服务入门使用流程



2 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：

- [注册华为账号并实名认证](#)
- [开通企业中心](#)

注册华为账号并实名认证

如果您已有一个华为账号，请跳到下一个任务。如果您还没有华为账号，请参考以下步骤创建。

1. 打开<https://www.huaweicloud.com/intl/zh-cn/>，单击“注册”。
 2. 根据提示信息完成注册，详细操作请参见“[如何注册华为云管理控制台的账户？](#)”。
- 注册成功后，系统会自动跳转至您的个人信息界面。
3. 参考“[实名认证](#)”完成企业账号实名认证。

说明

当前RGC服务暂不收取费用。但您需要根据使用情况为以下服务付费：SMN、OBS等。

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

3 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。

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 3-1 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 3-2 设置主区域



步骤5 （可选）选择除主区域之外还需要治理的区域，可以选择多个区域。添加后，该区域的资源也将被RGC治理。

图 3-3 设置其他区域



步骤6 单击“下一步”。

步骤7 在配置组织单元页面，输入核心组织单元名称。

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，不支持在设置Landing Zone后进行修改。

图 3-4 设置核心组织单元

**步骤8** 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 3-5 创建附加组织单元

**步骤9** 单击“下一步”。

步骤10 在配置核心账号界面，配置管理账号。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。

图 3-6 配置管理账号



步骤11 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：支持创建新账号或使用现有账号。使用的现有账号需要归属于管理账号所在的组织中。
- 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6-30个字符。
- 账号ID：当选择使用现有账号时，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。

步骤12 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：支持创建新账号或使用现有账号。现有的账号需要归属于管理账号所在的组织中。
- 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：输入审计账号的名称，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6-30个字符。
- 账号ID：当选择使用现有账号时，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 3-7 配置审计账号

审计账号

* 账号类型 创建新账号 使用现有账号

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。

* 告警邮箱

该邮箱用于接收RGC预置告警通知，请谨慎选择。

* 账号名称

确保审计账号名称唯一，不要与其他账号名称相同。在审计账号创建成功后，您无法修改该名称。

* 手机号

步骤13 单击“下一步”。

步骤14 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 3-8 启用 CTS

< | 搭建Landing Zone

① 设置区域信息 — ② 配置组织单元 — ③ 配置核心账号 — ④ 配置日志 — ⑤ 确认配置信息

CTS配置

* 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强烈建议用户启用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。

步骤15 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。

该桶将会存放记录Config服务资源记录器的配置快照和CTS记录的操作审计日志，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。

图 3-9 配置 OBS 桶日志保留时长

OBS日志配置

★ 日志汇聚桶数据保留时长	<input type="text" value="1"/>	年
请输入大小范围为 1 到 15 的数字，不支持小数。（1年 = 365天）		
★ OBS桶访问日志保留时长	<input type="text" value="10"/>	年
请输入大小范围为 1 到 15 的数字，不支持小数。（1年 = 365天）		

步骤16 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。”。

图 3-10 确认配置信息

步骤17 单击“搭建Landing Zone”，完成Landing Zone配置。

----结束

后续步骤

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](#)。

4 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。

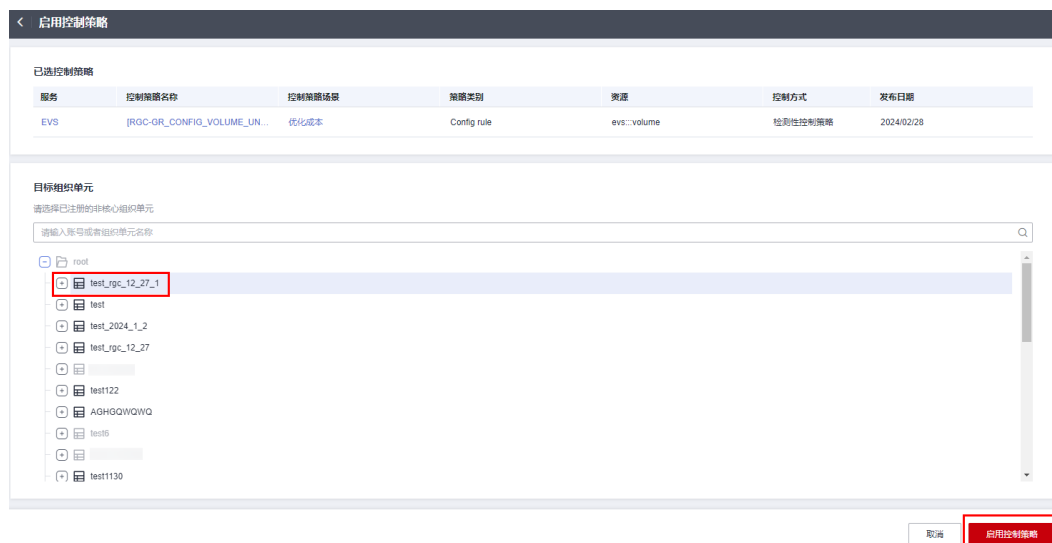
步骤3 单击“操作”列下的“启用控制策略”。

图 4-1 启用控制策略



步骤4 选择需要绑定的组织单元。

图 4-2 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 4-3 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。

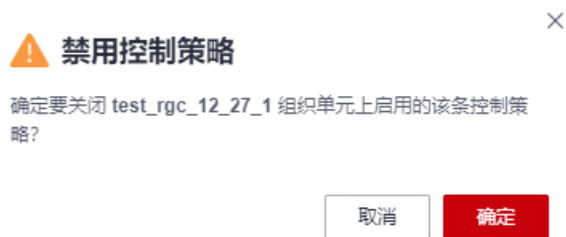
图 4-4 解绑控制策略



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 4-5 禁用控制策略



----结束

5 修订记录

时间	修订记录
2023-12-22	第一次正式发布。