资源治理中心

用户指南

文档版本 01

发布日期 2023-12-22

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 申请公测

RGC服务目前正在公测，支持用户申请免费试用。

操作步骤

步骤1 登录**管理控制台**。

步骤2 在系统首页，单击管理控制台左上角的，选择“管理与监管 > 资源治理中心”。

步骤3 单击“立即申请”，进入申请公测页面。

步骤4 在公测申请页面，根据实际情况填写企业规模、研发人员比例、应用场景、业务当前阶段、业务描述等申请信息。

步骤5 勾选“同意《公测试用服务协议》”，单击“申请公测”。

----结束

公测申请提交后，5个工作日内审核结果将发送到您的邮箱和手机。

2 Landing Zone 管理

2.1 部署 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 2-1 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 2-2 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 2-3 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 2-4 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 2-5 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 2-6 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。
- 手机号：当选择直接创建新账号时，需要输入日志存档账号的手机号。
- 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 2-7 配置日志存档账号

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。
- 手机号：当选择直接创建新账号时，需要输入审计账号的手机号。
- 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 2-8 配置审计账号

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 2-9 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。

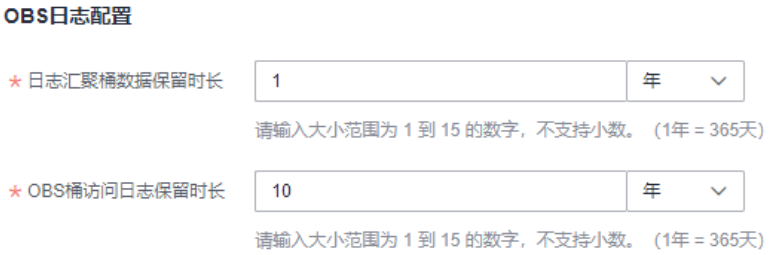
- 日志汇聚桶数据保留时长：默认设置为1年。最长设置为15年。

  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 2-10 配置 OBS 桶日志保留时长



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 2-11 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**。

2.2 查看 Landing Zone 信息

Landing Zone搭建完成后，可以在总览页面中查看Landing Zone的整体情况，包括“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。

操作步骤

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中整体情况。

步骤3 在“组织单元和账号”区域，单击数字，可以查看组织单元和账号的概览。

步骤4 在“已启用的控制策略”区域，单击数字，可以控制策略的概览。

步骤5 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 2-12 不合规资源

步骤6 在“已注册组织单元”区域，单击OU名称，可以查看OU的详情。

步骤7 在“已纳管账号”区域，单击账号名称，可以查看账号的详情。

----结束

3 组织管理

3.1 组织管理概述

什么是组织

华为云Organizations云服务是一项账号管理服务，使您能够将多个华为云账号整合到您创建并集中管理的组织中。组织是为管理多账号关系而创建的实体，一个组织由管理账号、成员账号、根组织单元、组织单元（Organizational Unit，以下简称OU）四个部分组成。一个组织有且仅有一个管理账号，若干个成员账号，一个根，若干个OU。一个根和多层级OU组成树状结构，账号可以关联根或任一层级的OU。有关Organizations云服务的介绍请参见：**什么是组织云服务**。

管理账号设置Landing Zone后，所管理的组织结构、组织单元、账号将会显示在组织管理页面中。

组织管理的基本概念

- **组织**

  为管理多账号关系而创建的实体。一个组织由**管理账号**、**成员账号**、**根组织单元**、**组织单元**四个部分组成。一个组织有且仅有一个管理账号，若干个成员账号，以及由一个根组织单元和多层级组织单元组成的树状结构。成员账号可以关联在根组织单元或任一层级的组织单元。组织管理页面所呈现的，即为一个组织。

- **根组织单元**

  根组织单元位于整个组织树的顶端，组织由根组织单元向下关联组织单元和账号。组织管理页面中的root层级，即为根组织单元。

- **核心组织单元**

  在设置Landing Zone时，配置的核心组织单元，将会自动出现在组织结构中。默认的组织单元名称为“Security”。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**

  组织单元是可以理解为成员账号的容器或分组单元，通常可以映射为企业的部门、子公司或者项目族等。组织单元可以嵌套，一个组织单元只能有一个父组织单元，一个组织单元下可以关联多个子组织单元或者成员账号。

- **管理账号**

  管理账号通常是设置Landing Zone的账号。管理账号可以注册组织单元或账号，将组织单元或账号纳管至Landing Zone中。

- **成员账号**

  成员账号为关联在根组织单元或者任一个组织单元下的账号。

- **注册组织单元**

  在RGC中创建的组织单元，系统将会自动注册。在组织中创建的组织单元需要手动进行注册，Landing Zone就可以对组织单元进行监管。

- **纳管账号**

  在RGC中创建的账号，系统将会自动纳管。在组织中创建的账号需要手动进行纳管，Landing Zone可以对账号进行监管。

3.2 创建账号

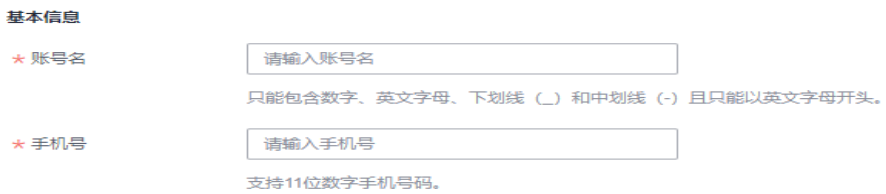
可以在RGC中创建账号，系统将会自动纳管创建成功的账号，无需手动处理。

操作步骤

步骤1 以RGC管理员身份登录华为云，进入华为云RGC控制台，进入组织管理页。

步骤2 进入组织管理页，单击“创建账号”。

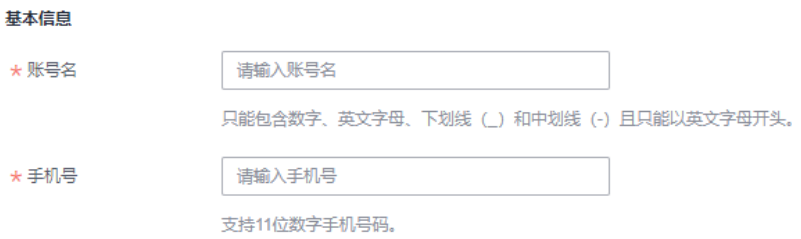
图 3-1 创建账号



步骤3 配置账号基本信息。输入账号显示名、手机号。不能与其他账号重复。

基本信息中的手机号，仅展示作用，不用于密码找回等场景。

图 3-2 填写基本信息



步骤4 配置IAM身份中心的信息。输入IAM身份中心邮箱地址和用户名。

创建账号后，系统将会同步创建一个IAM身份中心的用户。创建的用户可以使用IAM身份中心的门户URL进行登录，并且可以使用IAM身份中心邮箱地址进行密码找回等。

图 3-3 配置 IAM 身份中心信息

步骤5 配置所属组织单元。选择一个已注册的组织单元，并为此账户启用该组织单元配置的所有控制策略。

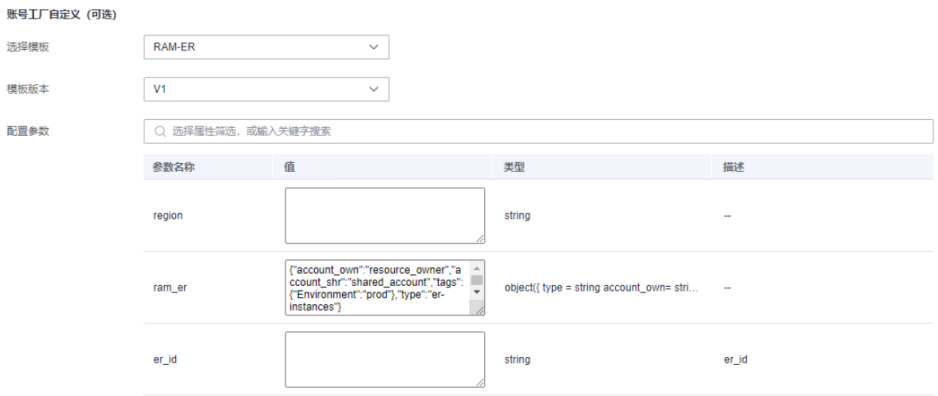
图 3-4 选择组织单元

步骤6 （可选）配置账号工厂的RFS模板。选择使用的RFS模板和模板的版本，如选择通过模板创建账号，可以实现账号的批量复制创建。

更多关于资源编排服务RFS模板的信息，请参考**RFS模板介绍**。

- 选择模板：选择在RFS中创建好的模板。
- 模板版本：选择模板的版本。
- 配置参数：根据业务需求，修改模板中的参数配置。

图 3-5 配置模板



步骤7 单击“创建账号”，创建成功的账号将会显示在列表中。

----结束

3.3 创建组织单元

组织单元是可以理解为成员账号的容器或分组单元，将账号分组到一起，作为一个单元管理，通常可以映射为企业的部门、子公司或者项目族等。OU可以嵌套，您可以在

单个OU内创建多个 OU。一个OU只能有一个父OU，一个OU下可以关联多个子OU或者成员账号。

您可以在组织管理页面的组织的根下创建OU。OU最深可嵌套至5层。

在Landing Zone中创建的OU，系统将会自动进行注册，无需再手动注册。

操作步骤

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，进入组织管理页面。

步骤2 进入组织管理页，单击“创建组织单元”。

图 3-6 创建 OU

步骤3 在弹窗中填写组织单元名称，并且选择父组织单元。

图 3-7 填写组织单元信息

步骤4 然后单击“确认”，完成OU创建。

----结束

3.4 纳管账号

在RGC设置Landing Zone前，在组织中创建的账号或邀请进组织的账号将不会在Landing Zone中自动纳管，需要手动纳管。纳管后，账号将会被Landing Zone进行监管。

约束与限制

- 如果账号在纳管前已使用配置审计Config服务且存在资源记录器，纳管后系统会将该账号的资源记录器配置进行覆盖，请谨慎操作。

- 纳管邀请进组织的账号需要根据**前提条件**完成相应配置，否则账号将会纳管失败。

前提条件

此步骤仅适用需要纳管邀请进组织的账号，纳管在组织中创建的账号请跳过此步骤直接纳管账号即可。

步骤1 以纳管账号的身份登录华为云，进入华为云IAM控制台。

步骤2 在左侧导航窗格中，选择“委托”页签，单击右上方的“创建委托”。

图 3-8 创建委托

步骤3 设置“委托名称”为“RGCServiceExecutionAgency”。

图 3-9 委托名称

步骤4 “委托类型”选择“普通账号”，在“委托的账号”中输入RGC管理账号名。

步骤5 选择“持续时间”，填写“描述”信息。

步骤6 单击“下一步”，进入给委托授权页面。

步骤7 勾选以下三个需要授予委托的权限，分别是：Security Administrator、FullAccess和Tenant Guest。

图 3-10 需要授予委托的权限

步骤8 单击“下一步”，选择权限的作用范围。

步骤9 单击“确定”，委托创建完成。RGC管理账号即可在RGC控制台中参考**纳管账号**完成账号纳管。

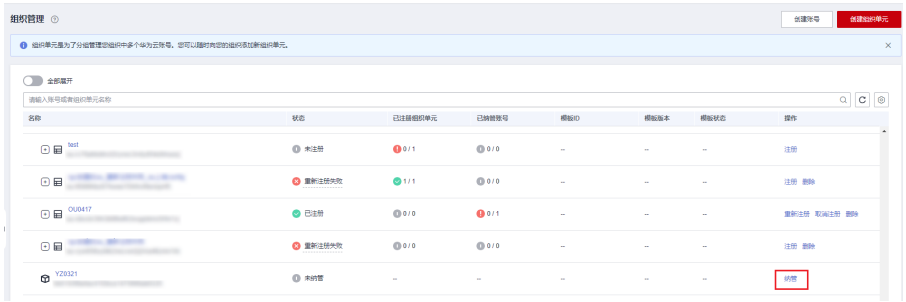
----结束

纳管账号

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，进入组织管理页面。

步骤2 进入组织管理页，单击需要纳管的账号所在行“操作”列的“纳管”。

图 3-11 纳管账号



步骤3 配置所属组织单元。选择一个已注册的组织单元，并为此账户启用该组织单元配置的所有控制策略。

图 3-12 选择组织单元

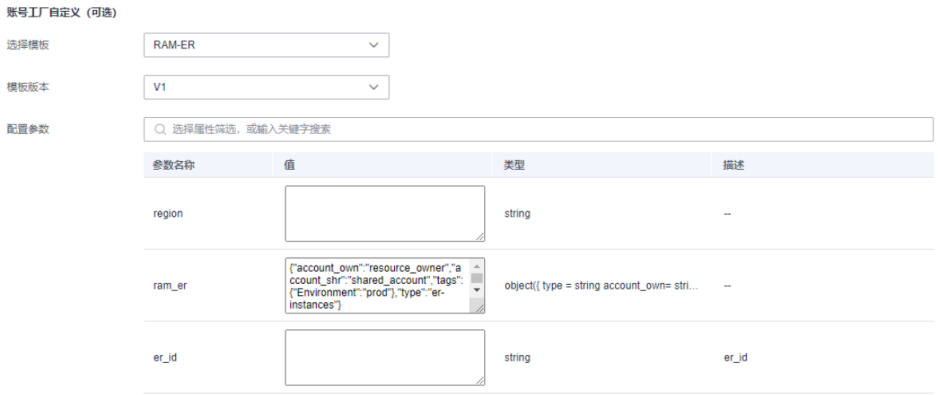
步骤4 （可选）配置账号工厂的RFS模板。选择使用的RFS模板和模板的版本，如选择通过模板创建账号，可以实现账号的批量复制创建。

更多关于资源编排服务RFS模板的信息，请参考**RFS模板介绍**。

- 选择模板：选择在RFS中创建好的模板。

- 模板版本：选择模板的版本。
- 配置参数：根据业务需求，修改模板中的参数配置。

图 3-13 配置模板



步骤5 单击“纳管账号”。可以在组织结构中确认账号的纳管结果。纳管成功后，账号将会受到Landing Zone的监管。

----结束

取消纳管账号

如果不再需要对某个账号进行管理，可以对该账号取消纳管。

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，进入组织管理页面。

步骤2 进入组织管理页，单击需要取消纳管的账号所在行“操作”列的“取消纳管”。

图 3-14 取消纳管账号

步骤3 单击“确认”。此操作无法撤销，请谨慎操作。

可以在组织结构中账号的确认取消纳管结果。取消纳管后，账号将从之前所在的组织单元移动至根组织单元下。

----结束

3.5 注册组织单元

在RGC设置Landing Zone前，在组织中创建的OU将不会在Landing Zone中自动注册，需要手动注册。注册成功后，该OU将会被Landing Zone进行监管。

操作步骤

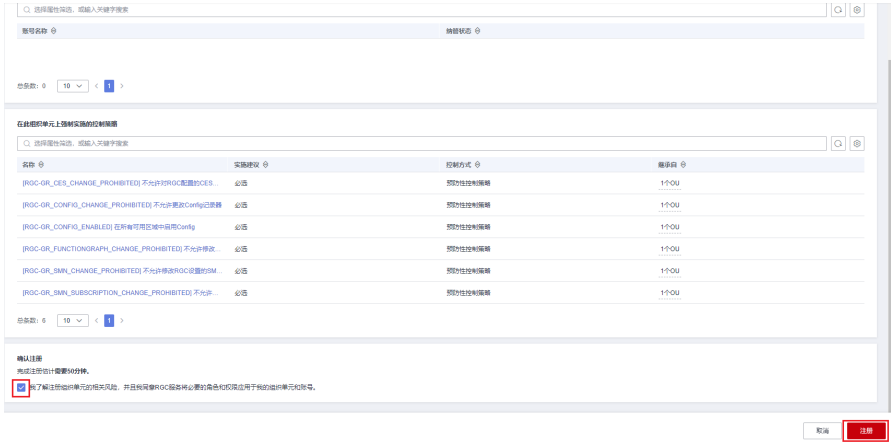
步骤1 以RGC管理账号的身份登录华为云，进入华为云RGC控制台，进入组织管理页面。

步骤2 进入组织管理页，单击需要注册OU所在行“操作”列的“注册”。

图 3-15 注册 OU

步骤3 确认子账号和OU上控制策略的信息。确认无误后，勾选“我了解重新注册组织单元的相关风险，并且我同意RGC服务将必要的角色和权限应用于我的组织单元和账号。”。

图 3-16 确认 OU 信息



步骤4 单击“注册”，注册OU需要等待一段时间。可以在组织结构中查看OU的注册结果。注册成功后，OU将会收到Landing Zone的监管。

----结束

3.6 查看组织架构详情

在RGC设置Landing Zone后，可以查看各OU的基本信息、不合规资源、已启用的控制策略、直系的组织单元，以及直系子账号。

操作步骤

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，进入组织管理页面。

步骤2 进入组织管理页，单击需要查看OU的名称。

图 3-17 查看 OU

步骤3 在基本信息中，可以查看OU的状态、父组织单元、已纳管的账号数、已启用的控制策略、已注册的组织单元数、外部SCP。

图 3-18 查看 OU 基本信息

步骤4 选择“不合规资源”页签，将会显示当前OU下存在的不合规资源，以及不合规资源ID、类型、服务和所在区域等。

图 3-19 查看不合规资源

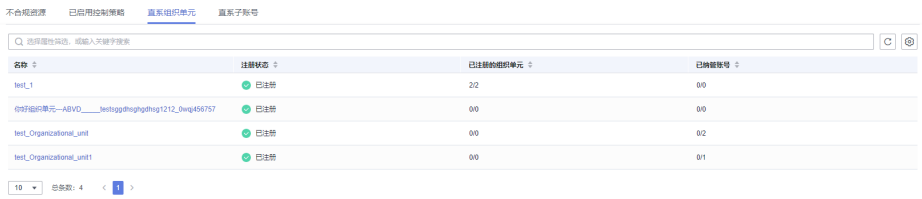
步骤5 选择“已启用控制策略”页签，将会显示当前OU下已启用的控制策略。

如需了解控制策略详情，请参考**5.4 查看控制策略详情**。

图 3-20 查看已启用控制策略

步骤6 选择“直系组织单元”页签，将会显示当前OU下的直系OU信息，包括各OU的注册状态、已注册的直系OU以及已纳管的账号。

图 3-21 查看直系 OU



步骤7 选择“直系子账号”页签，将会显示当前OU下的直系子账号信息，包括子账号的外部Config规则，Landing Zone版本，以及纳管状态。

图 3-22 查看直系子账号

----结束

4 账号工厂

4.1 创建自定义模板（可选）

管理账号可以直接在资源编排服务（RFS）设置账号的基线模板。后续管理账号在指定组织单元下创建新的成员账号，新建账号内会基于最佳实践自动配置账号基线。

当前暂不支持在RGC界面中创建自定义模板，请前往资源编排服务进行创建。

操作步骤

步骤1 以RGC管理账号的身份登录华为云，进入华为云RFS控制台。

步骤2 参考**使用可视化编辑器编写模板创建云硬盘**完成模板创建。

步骤3 返回RGC控制台，单击“创建账号”。

图 4-1 创建账号

如“账号工厂”部分显示可以选择RFS模板和版本号，表示RFS模板创建成功。

----结束

4.2 创建账号并配置模板

账号创建时，支持选择预置模板或自定义模板，在快速创建账号的基础上，实现可灵活定制的账号内自动配置。

操作步骤

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。

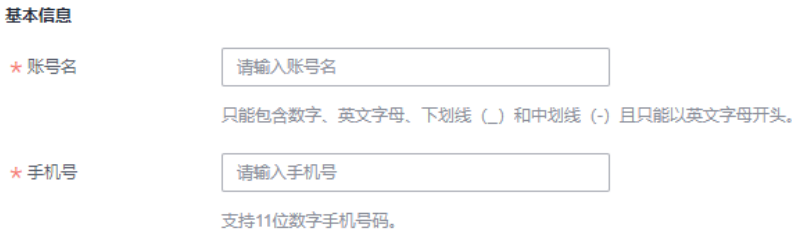
步骤2 进入账号工厂页，单击右上角“创建账号”。

图 4-2 创建账号

步骤3 配置账号基本信息。输入账号显示名、手机号。不能与其他账号重复。

基本信息中的手机号，仅展示作用，不用于密码找回等场景。

图 4-3 填写基本信息



步骤4 配置IAM身份中心的信息。输入IAM身份中心邮箱地址和用户名。

创建账号后，系统将会同步创建一个IAM身份中心的用户。创建的用户可以使用IAM身份中心的门户URL进行**登录**，并且可以使用IAM身份中心邮箱地址进行密码找回等。

图 4-4 配置 IAM 身份中心信息

步骤5 配置所属组织单元。选择一个已注册的组织单元，并为此账户启用该组织单元配置的所有控制策略。

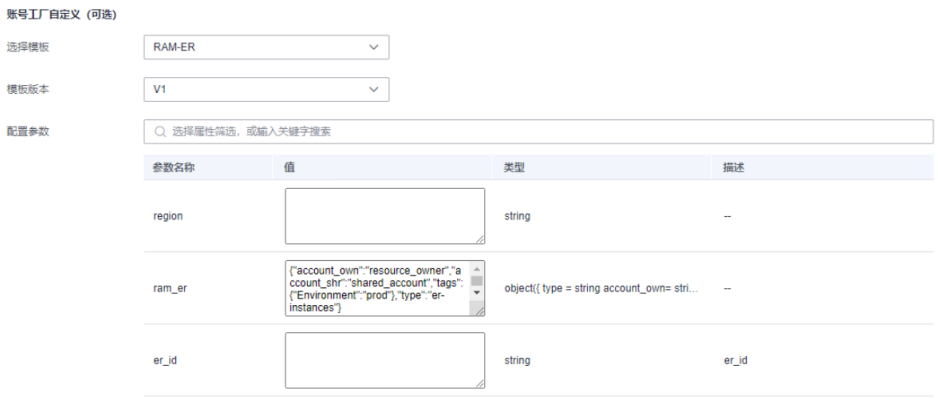
图 4-5 选择组织单元

步骤6 （可选）配置账号工厂的RFS模板。选择使用的RFS模板和模板的版本，如选择通过模板创建账号，可以实现账号的批量复制创建。

更多关于资源编排服务RFS模板的信息，请参考**RFS模板介绍**。

- 选择模板：选择在RFS中创建好的模板。
- 模板版本：选择模板的版本。
- 配置参数：根据业务需求，修改模板中的参数配置。

图 4-6 配置模板



步骤7 单击“创建账号”，创建成功的账号将会显示在列表中。

----结束

5 控制策略管理

5.1 控制策略策略概述

控制策略可以对Landing Zone的环境进行治理。通过控制策略的运作，管理账号可以快速发现Landing Zone中存在的风险，以便及时进行干预、维护，保障Landing Zone各个部分的合规性。

控制策略类型介绍

- 预防性控制策略：策略主体为SCP服务控制策略，任何在策略中显性拒绝的操作都会被拦截。预防性控制策略在指定OU上生效之后，该OU所有直系子级账号均会继承该策略。
- 检测性控制策略：策略主体为Config合规规则，不合规的资源配置会被检测发现并反馈给用户，用户可以在资源治理中心服务控制台查看不合规的资源列表。检测性控制策略在指定OU上生效后，该OU所有直系子级账号均会根据规则要求检测不合规配置的发生。

实施类型

- 必选：这部分策略在开启RGC服务并设置Landing Zone后，便在核心OU和核心账号上强制自动生效，而且无法禁用。
- 强烈推荐：基于华为云治理最佳实践强烈推荐的合规遵从管控策略，大部分企业用户在云上治理多账号环境时大概率会涉及相关场景和服务，建议Landing Zone搭建完成之后，企业用户自主启用。
- 可选：企业云上治理过程中，部分企业用户可能会涉及相关控制策略，可以根据具体情况灵活选用相关策略。

控制策略场景

- 建立日志记录和监控
- 强制执行最低权限
- 限制网络访问
- 加密静态数据。
- 保护数据完整性

- 保护配置
- 优化成本

5.2 控制策略参考

5.2.1 必选控制策略

必选控制策略由RGC提供，且无法停用。这些控制策略将会自动应用于组织结构上的每个OU。

RGC-GR_AUDIT_BUCKET_DELETION_PROHIBITED

实现：SCP

类型：Preventive

功能：防止删除RGC在日志归档账号中创建的OBS桶。

```
{
   "Version": "5.0",
   "Statement": [{
      "Sid": "AUDIT_BUCKET_DELETION_PROHIBITED",
      "Effect": "Deny",
      "Action": [
         "obs:bucket:DeleteBucket"
      ],
      "Resource": [
         "obs:*::bucket:rgcservice-managed-*-logs-*"
      ],
      "Condition": {
         "StringNotMatch": {
            "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
         }
      }
   }]
}
```

RGC-GR_CT_AUDIT_BUCKET_ENCRYPTION_CHANGES_PROHIBITED

实现：SCP

类型：Preventive

功能：防止对RGC创建的OBS桶的加密配置进行更改。

```
{
   "Version": "5.0",
   "Statement": [{
      "Sid": "AUDIT_BUCKET_ENCRYPTION_CHANGES_PROHIBITED",
      "Effect": "Deny",
      "Action": [
         "obs:bucket:PutEncryptionConfiguration"
      ],
      "Resource": [
         "obs:*::bucket:rgcservice-managed-*-logs-*"
      ],
      "Condition": {
         "StringNotMatch": {
            "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
         }
```



```
        }
    }]
}
```

RGC-GR_CT_AUDIT_BUCKET_LIFECYCLE_CONFIGURATION_CHANGES_PROHIBITED

实现：SCP

类型：Preventive

功能：防止对RGC创建的OBS桶的生命周期配置进行更改。

```
{
    "Version": "5.0",
    "Statement": [{
        "Sid": "AUDIT_BUCKET_LIFECYCLE_CONFIGURATION_CHANGES_PROHIBITED",
        "Effect": "Deny",
        "Action": [
            "obs:bucket:PutLifecycleConfiguration"
        ],
        "Resource": [
            "obs:*::bucket:rgcservice-managed-*-logs-*"
        ],
        "Condition": {
            "StringNotMatch": {
                "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            }
        }
    }]
}
```

RGC-GR_CT_AUDIT_BUCKET_LOGGING_CONFIGURATION_CHANGES_PROHIBITED

实现：SCP

类型：Preventive

功能：防止对RGC创建的OBS桶进行配置更改。

```
{
    "Version": "5.0",
    "Statement": [{
        "Sid": "AUDIT_BUCKET_LOGGING_CONFIGURATION_CHANGES_PROHIBITED",
        "Effect": "Deny",
        "Action": [
            "obs:bucket:PutBucketLogging"
        ],
        "Resource": [
            "obs:*::bucket:rgcservice-managed-*-logs-*"
        ],
        "Condition": {
            "StringNotMatch": {
                "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            }
        }
    }]
}
```

RGC-GR_CT_AUDIT_BUCKET_POLICY_CHANGES_PROHIBITED

实现：SCP

类型：Preventive

功能：防止对RGC创建的OBS桶的策略进行更改。

```
{
   "Version": "5.0",
   "Statement": [{
      "Sid": "AUDIT_BUCKET_POLICY_CHANGES_PROHIBITED",
      "Effect": "Deny",
      "Action": [
         "obs:bucket:PutBucketPolicy",
         "obs:bucket:DeleteBucketPolicy"
      ],
      "Resource": [
         "obs:*::bucket:rgcservice-managed-*-logs-*"
      ],
      "Condition": {
         "StringNotMatch": {
            "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
         }
      }
   }]
}
```

RGC-GR_DETECT_CTS_ENABLED_ON_SHARED_ACCOUNTS

实现：Config

类型：Detective

功能：检测Security组织单元下的账号是否启用了CTS。

RGC-GR_CES_CHANGE_PROHIBITED

实现：SCP

类型：Preventive

功能：防止更改RGC为监控环境而设置的CES配置。

```
{
   "Version": "5.0",
   "Statement": [{
         "Sid": "CES_CHANGE_PROHIBITED",
         "Effect": "Deny",
         "Action": [
            "ces:alarms:put*",
            "ces:alarms:delete*",
            "ces:alarms:addResources"
         ],
         "Resource": [
            "*"
         ],
         "Condition": {
            "StringNotMatch": {
               "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            },
            "StringMatch": {
               "g:ResourceTag/rgcservice-managed": "RGC-ConfigComplianceChangeEventRule"
            }
         }
      },
      {
         "Sid": "CES_TAG_CHANGE_PROHIBITED",
         "Effect": "Deny",
         "Action": [
            "ces:tags:create"
         ],
         "Resource": [
```



```
            "*"
        ],
        "Condition": {
            "StringNotMatch": {
                "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            },
            "ForAnyValue:StringMatch": {
                "g:TagKeys": "rgcservice-managed"
            }
        }
    }
  ]
}
```

RGC-GR_CONFIG_CHANGE_PROHIBITED

实现：SCP

类型：Preventive

功能：防止对Config进行配置更改。

```
{
  "Version": "5.0",
  "Statement": [{
    "Sid": "CONFIG_CHANGE_PROHIBITED",
    "Effect": "Deny",
    "Action": [
        "rms:trackerConfig:delete",
        "rms:trackerConfig:put"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotMatch": {
            "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
        }
    }
  }]
}
```

RGC-GR_CONFIG_ENABLED

实现：SCP

类型：Preventive

功能：在所有可用区域中启用Config。

```
{
  "Version": "5.0",
  "Statement": [{
    "Sid": "CONFIG_CHANGE_PROHIBITED",
    "Effect": "Deny",
    "Action": [
        "rms:trackerConfig:delete",
        "rms:trackerConfig:put"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotMatch": {
            "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
```



```
        }
      }
    }]
}
```

RGC-GR_FUNCTIONGRAPH_CHANGE_PROHIBITED

实现：SCP

类型：Preventive

功能：不允许更改RGC设置的FunctionGraph函数。

```
{
   "Version": "5.0",
   "Statement": [{
      "Sid": "FUNCTIONGRAPH_CHANGE_PROHIBITED",
      "Effect": "Deny",
      "Action": [
         "functiongraph:function:createFunction",
         "functiongraph:function:deleteFunction",
         "functiongraph:function:updateFunctionCode",
         "functiongraph:function:updateMaxInstanceConfig",
         "functiongraph:function:createVersion",
         "functiongraph:function:createEvent",
         "functiongraph:function:deleteEvent",
         "functiongraph:function:updateEvent",
         "functiongraph:function:updateReservedInstanceCount",
         "functiongraph:function:updateFunctionConfig"
      ],
      "Resource": [
         "functiongraph:*:*:function:rgcservice-managed/RGC-NotificationForwarder"
      ],
      "Condition": {
         "StringNotMatch": {
            "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
         }
      }
   }]
}
```

RGC-GR_SMN_CHANGE_PROHIBITED

实现：SCP

类型：Preventive

功能：防止更改RGC设置的SMN通知设置。

```
{
   "Version": "5.0",
   "Statement": [{
         "Sid": "SMN_CHANGE_PROHIBITED",
         "Effect": "Deny",
         "Action": [
            "smn:topic:update*",
            "smn:topic:delete*"
         ],
         "Resource": [
            "*"
         ],
         "Condition": {
            "StringNotMatch": {
               "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            },
```



```
            "ForAnyValue:StringMatch": {
               "g:ResourceTag/rgcservice-managed": [
                  "RGC-SecurityNotifications",
                  "RGC-AllConfigNotifications",
                  "RGC-AggregateSecurityNotifications"
               ]
            }
         }
      },
      {
         "Sid": "SMN_TAG_CHANGE_PROHIBITED",
         "Effect": "Deny",
         "Action": [
            "smn:tag:create",
            "smn:tag:delete"
         ],
         "Resource": [
            "*"
         ],
         "Condition": {
            "StringNotMatch": {
               "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
            },
            "ForAnyValue:StringMatch": {
               "g:TagKeys": "rgcservice-managed"
            }
         }
      }
   ]
}
```

RGC-GR_SMN_SUBSCRIPTION_CHANGE_PROHIBITED

实现：SCP

类型：Preventive

功能：防止更改RGC设置的SMN主题订阅，此订阅用于触发配置规则合规性更改的通知。

```
{
   "Version": "5.0",
   "Statement": [{
      "Sid": "SMN_SUBSCRIPTION_CHANGE_PROHIBITED",
      "Effect": "Deny",
      "Action": [
         "smn:topic:subscribe",
         "smn:topic:deleteSubscription"
      ],
      "Resource": [
         "*"
      ],
      "Condition": {
         "StringNotMatch": {
            "g:PrincipalUrn": "sts::*:assumed-agency:RGCServiceExecutionAgency/*"
         },
         "ForAnyValue:StringMatch": {
            "g:ResourceTag/rgcservice-managed": [
               "RGC-SecurityNotifications",
               "RGC-AllConfigNotifications",
               "RGC-AggregateSecurityNotifications"
            ]
         }
      }
   }]
}
```


5.2.2 强烈建议控制策略

CTS

控制策略名称	功能	场景	严重程度	资源
RGC-GR_CONFIG_MULTI_REGION_CTS_TRACKER_EXISTS	账号未在指定region列表创建并启用CTS追踪器，视为“不合规”。	建立日志记录和监控	高	cts:::tracker

IAM

控制策略名称	功能	场景	严重程度	资源
RGC-GR_CONFIG_IAM_ROOT_ACCESS_KEY_CHECK	账号存在可使用的访问密钥，视为“不合规”。	强制执行最低权限	严重	identity:::accessKey
RGC-GR_CONFIG_ROOT_ACCOUNT_MFA_ENABLED	根账号未开启MFA认证，视为“不合规”。	强制执行最低权限	高	identity:::acl
RGC-GR_CONFIG_IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS	IAM策略admin权限(*:*:*或*:*或*)，视为“不合规”。	强制执行最低权限	高	identity:::protectionPolicy
RGC-GR_CONFIG_IAM_ROLE_HAS_ALL_PERMISSIONS	IAM自定义策略具有allow的*:*权限，视为“不合规”。	强制执行最低权限	低	identity:::role
RGC-GR_CONFIG_IAM_USER_MFA_ENABLED	IAM用户未开启MFA认证，视为“不合规”。	强制执行最低权限	中	identity:::user

RDS

控制策略名称	功能	场景	严重程度	资源
RGC-GR_CONFIG_RDS_INSTANCE_NO_PUBLIC_IP	RDS资源具有公网IP，视为“不合规”。	限制网络访问	高	rds:::instance

EVS

控制策略名称	功能	场景	严重程度	资源
RGC-GR_CONFIG_VOLUME_UNUSED_CHECK	云硬盘未挂载给任何云服务器，视为“不合规”。	优化成本	高	evs:::volume

VPC

控制策略名称	功能	场景	严重程度	资源
RGC-GR_CONFIG_VPC_SG_PORTS_CHECK	当安全组入方向源地址设置为0.0.0.0/0，且开放了所有的TCP/UDP端口时，视为“不合规”。	限制网络访问	高	networking:::secgroup
RGC-GR_CONFIG_VPC_DEFAULT_SG_CLOSED	虚拟私有云的默认安全组允许入方向或出方向流量，视为“不合规”。	限制网络访问	高	networking:::secgroup
RGC-GR_CONFIG_VPC_FLOW_LOGS_ENABLED	检查是否为VPC启用了流日志，如果该VPC未启用流日志，视为“不合规”。	建立日志记录和监控	中	vpc:::flowLog
RGC-GR_CONFIG_VPC_SG_RESTRICTED_SSH	当安全组入方向源地址设置为0.0.0.0/0，且开放TCP 22端口，视为“不合规”。	限制网络访问	高	networking:::secgroup

CCE

控制策略名称	功能	场景	严重程度	资源
RGC-GR_CONFIG_CCE_ENDPOINT_PUBLIC_ACCESS	CCE集群资源具有公网IP，视为“不合规”。	限制网络访问	中	cce:::cluster

CSS

控制策略名称	功能	场景	严重程度	资源
RGC-GR_CONFIG_CSS_CLUSTER_HTTPS_REQUIRED	CSS集群未启用https，视为“不合规”。	加密传输中的数据	中	css:::cluster

DWS

控制策略名称	功能	场景	严重程度	资源
RGC-GR_CONFIG_DWS_ENABLE_LOG_DUMP	DWS集群未启用日志转储，视为“不合规”。	建立日志记录和监控	中	dws:::cluster

ECS

控制策略名称	功能	场景	严重程度	资源
RGC-GR_CONFIG_ECS_INSTANCE_NO_PUBLIC_IP	ECS资源具有公网IP，视为“不合规”。	限制网络访问	中	compute:::instance
RGC-GR_CONFIG_ECS_MULTIPLE_PUBLIC_IP_CHECK	ECS资源具有多个公网IP，视为“不合规”。	限制网络访问	低	compute:::instance

ELB

控制策略名称	功能	场景	严重程度	资源
RGC-GR_CONFIG_ELB_TLS_HTTPS_LISTENERS_ONLY	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”。	加密传输中的数据	中	elb:::listener

MRS

控制策略名称	功能	场景	严重程度	资源
RGC-GR_CONFIG_MRS_CLUSTER_NO_PUBLIC_IP	MRS集群绑定公网IP，视为“不合规”。	限制网络访问	中	mrs:::cluster

APIG

控制策略名称	功能	场景	严重程度	资源
RGC-GR_CONFIG_APIG_INSTANCES_EXECUTION_LOGGING_ENABLED	APIG专享版实例未配置访问日志，视为“不合规”。	建立日志记录和监控	中	apig:::instance
RGC-GR_CONFIG_APIG_INSTANCES_AUTHORIZATION_TYPE_CONFIGURED	APIG专享版实例中如果存在API安全认证为“无认证”，则视为“不合规”。	加密传输中的数据	中	apig:::instance
RGC-GR_CONFIG_APIG_INSTANCES_SSL_ENABLED	APIG专享版实例如果有域名未关联SSL证书，则视为“不合规”。	加密传输中的数据	中	apig:::instance

Functiongraph

控制策略名称	功能	场景	严重程度	资源
RGC-GR_CONFIG_FUNCTION_GRAPH_PUBLIC_ACCESS_PROHIBITED	函数工作流的函数允许访问公网，视为“不合规”。	限制网络访问	严重	fgs:::function

SMN

控制策略名称	功能	场景	严重程度	资源
RGC-GR_CONFIG_SMN_LTS_ENABLE	SMN主题未启用事件分析，视为“不合规”。	建立日志记录和监控	中	smn:::topic

5.2.3 可选控制策略

暂无。

5.3 启用/关闭控制策略

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。

启用后，RGC将会在管理账号中创建和管理资源。请勿修改或删除RGC创建的资源，否则可能导致控制策略失效等。

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。

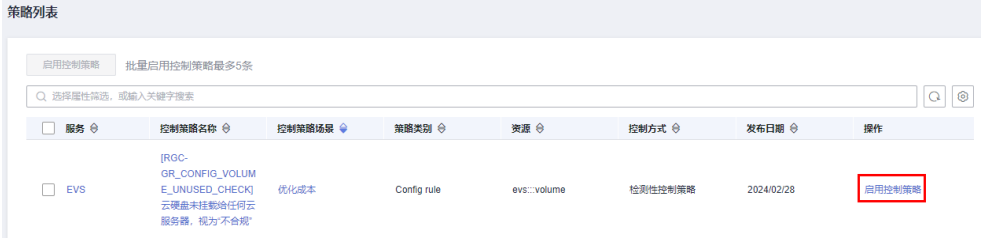
启用控制策略

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。

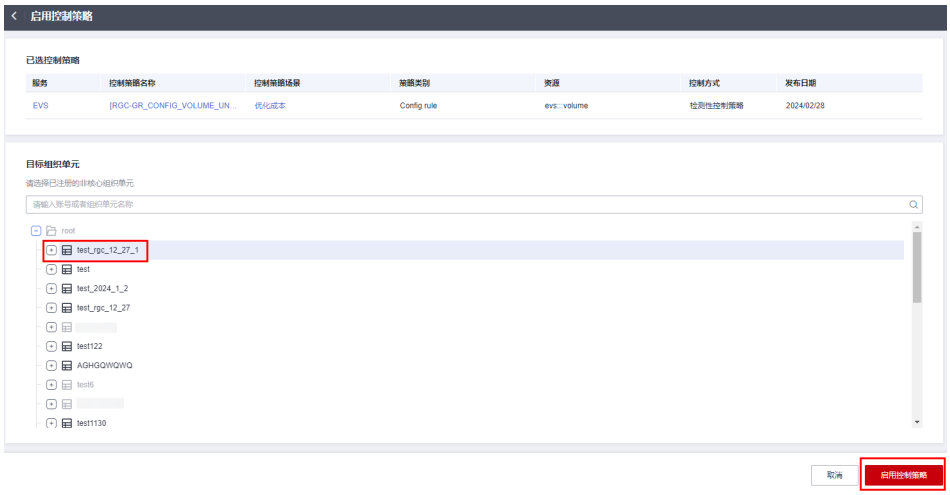
步骤3 单击“操作”列下的“启用控制策略”。

图 5-1 启用控制策略



步骤4 选择需要绑定的组织单元。

图 5-2 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

批量启用控制策略

单次仅支持批量开启5条控制策略。

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。

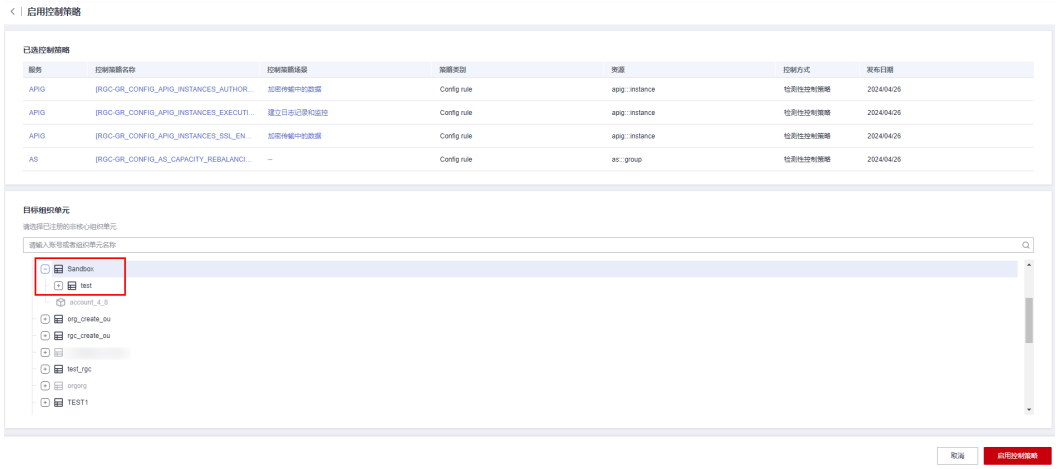
步骤2 进入“控制策略管理 > 策略列表”页面，在策略列表中，勾选需要启用的策略。

步骤3 单击列表上方的“启用控制策略”。

图 5-3 批量启用控制策略

步骤4 选择需要绑定的组织单元。

图 5-4 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

关闭控制策略

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，找到需要关闭的策略。

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 5-5 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 5-6 禁用控制策略

----结束

5.4 查看控制策略详情

通过策略目录和策略列表，均可以查看当前RGC控制策略的详细信息。

操作步骤

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，找到需要查看的策略。

步骤3 单击策略名称，进入控制策略详情。

表 5-1 控制策略参数说明

参数	描述
名称	控制策略的名称。
控制策略所有者	拥有和维护当前控制策略的云服务。
资源	受到监管的资源。

参数	描述
实施建议	建议应用在OU上的程度。分为必选、强烈推荐和可选。
控制策略场景	此控制策略执行后可以达到的预期目标。
控制方式	控制策略的类型。分为预防性控制策略、检测性控制策略。
规范	此控制策略执行的行业标准合规规范。
严重性	如果违反此控制策略所带来的风险程度。
服务	此控制策略适用的云服务。
策略类型	此控制策略的来源类型。分为服务控制策略（SCP）和Config规则。
控制策略ID	控制策略的唯一标识符。
发布日期	控制策略启用的日期。

----结束

A 修订记录

时间	修订记录
2023-12-22	第一次正式发布。