资源治理中心

用户指南

文档版本 01

发布日期 2025-02-27

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 Landing Zone 管理

1.1 搭建 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。

约束与限制

- 如您此前已选择某个区域搭建Landing Zone但未停用该区域Landing Zone，不支持通过直接删除IAM身份中心的账号信息后再切换区域搭建新的Landing Zone。
- 如果此前您已搭建Landing Zone失败，并且删除核心账号和OU，将无法再次重新搭建Landing Zone。建议您切换至其他账号后再进行Landing Zone的搭建。

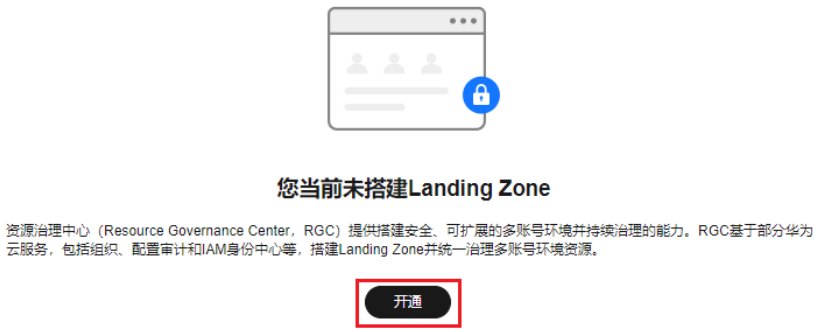
操作步骤

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 1-1 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 1-2 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 1-3 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 1-4 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 1-5 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 1-6 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 1-7 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 1-8 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。

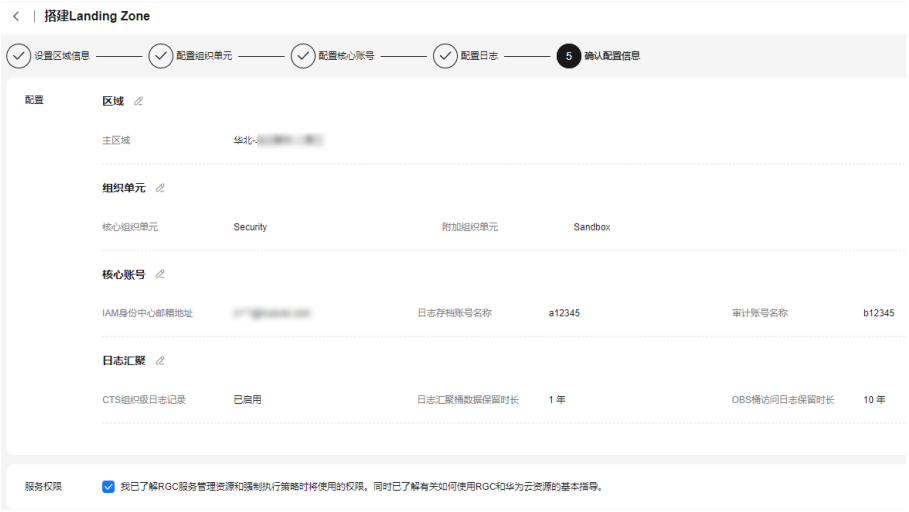
    该桶将会存放访问上述日志汇聚桶而产生的日志，并且存放于名为“rgcservice-managed-access-logs-{管理账号ID}”的桶中，{}中表示变量，根据实际情况进行显示。
- 使用现有OBS桶：需要输入日志账号下的OBS桶名称，如使用其他OBS桶则将会导致Landing Zone搭建失败。为了您的数据安全，建议使用桶策略为私有的OBS桶。

图 1-9 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 1-10 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2.1 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。

1.2 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，可以查看策略的概览。

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 1-11 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

1.3 停用 Landing Zone

清理Landing Zone中分配的所有资源的过程，称为停用Landing Zone。

如果您不需要再使用Landing Zone，则可以停用Landing Zone，系统将会自动清理Landing Zone中所分配的资源。

须知

停用Landing Zone与手动清理Landing Zone中的资源不同，手动清理则无法设置新的Landing Zone。

停用Landing Zone时，将不会通过以下方式修改您的数据和现有的组织数据：

- RGC不会删除您的数据，系统只会删除部分Landing Zone数据。
- 停用后，部分资源需要手动删除。其中包括OBS桶、用户自行创建的RFS模板、委托等。在设置新的Landing Zone前，需要手动将这些资源进行删除。
- 停用后，组织的所有组织单元和账号均不会被删除和移动。
- 停用后，原Landing Zone搭建过程中系统在IAM身份中心创建的相关资源均不会被删除。

⚠ 注意

- 请谨慎使用停用Landing Zone功能，停用后将无法再使用当前Landing Zone的功能，可以重新搭建当前Landing Zone。
- 如需停用当前Landing Zone后重新搭建新的Landing Zone，强烈建议您**提交工单**进行评估后再执行停用操作。

停用Landing Zone时，RGC会执行以下操作：

- 禁用所有在启用状态的控制策略。
- 通过删除服务控制策略（SCP）来禁用预防性控制策略。
- 删除所有系统创建的资源栈集。
- 删除每个账号工厂账号的记录。
- 删除标识主区域的内部记录。

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。

步骤2 进入Landing Zone设置页，选择“停用”页签。

步骤3 单击“停用”。停用Landing Zone基础环境的操作无法撤销，请谨慎操作。

图 1-12 停用 Landing Zone

步骤4 单击“确定”。

----结束

后续操作

停用Landing Zone后，以下资源需要进行手动删除，才能够设置新的Landing Zone。

- 如果新设置的Landing Zone需要使用和原Landing Zone同名的核心组织单元，则需要手动将原核心组织单元进行删除。删除组织单元的操作，请参考**删除组织单元**。
- 如果原Landing Zone使用了IAM身份中心，新设置的Landing Zone需要更换主区域，则需要将原IAM身份中心进行重置。重置IAM身份中心的操作，请参考**删除IAM身份中心配置**。
- 用于存放日志的OBS桶。删除OBS桶的操作，请参考**删除桶**。
- RFS中的RGCLoggingResources资源栈集。删除资源栈集的操作，请参考**删除资源栈集**。

- RFS中用户自行创建的模板。
- IAM中的委托，包括：RGCAgencyForStack、RGCBlueprintExecutionAgency、RGCBlueprintStackSetAdminAgency、RGCIAMTokenAccess、RGCAdminAgency。删除委托的操作，请参考**删除或修改委托**。

1.4 更新 Landing Zone

管理员有责任随时更新Landing Zone，以确保Landing Zone可以得到修复和更新。为了避免Landing Zone受到合规问题的影响，管理员需要及时发现提示的漂移现象并立即解决这些问题。通过更新Landing Zone，可以解决某些类型的漂移问题。

通过更新Landing Zone，您可以实现：

- 更新核心组织单元和账号
  - 更改管理账号
  - 更改审计账号邮箱
- 更新日志配置
  - 启用或停用CTS
  - 更改日志保留策略

更新Landing Zone时，您将会自动收到RGC的最新功能，可以在“Landing Zone设置”的“版本”页签中查看当前的Landing Zone。

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。

步骤2 进入Landing Zone设置页，选择“版本”页签。

步骤3 选择需要更新的版本。

图 1-13 选择版本

步骤4 单击“更新版本”。

图 1-14 更新 Landing Zone

须知

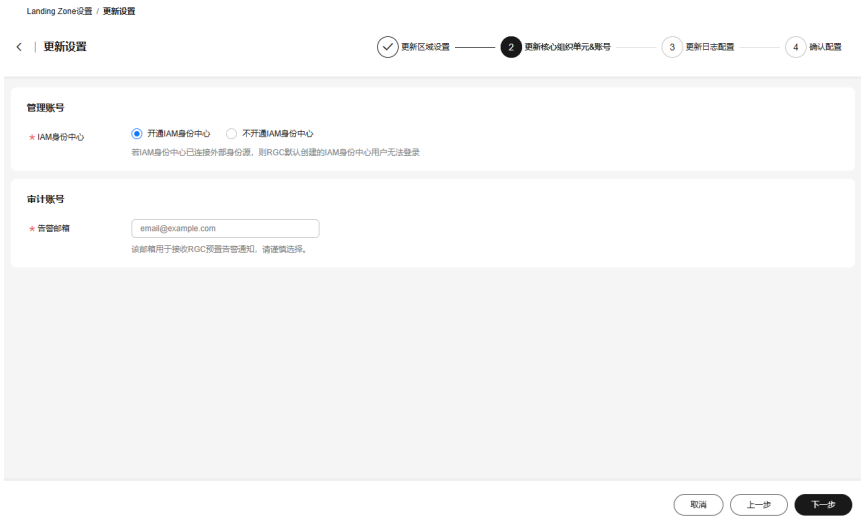
完成Landing Zone更新后，您将无法撤销更新或降级到先前的版本。

步骤5 更新核心组织单元和账号。

- 更新管理账号：
  - 开通IAM身份中心：RGC将在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。若IAM身份中心已连接外部身份源，则RGC默认创建的IAM身份中心用户无法登录。
  - 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。
- 更新告警邮箱：

  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。

图 1-15 更新核心组织单元和账号



步骤6 单击“下一步”。

步骤7 更新日志配置。

- 选择是否启用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。

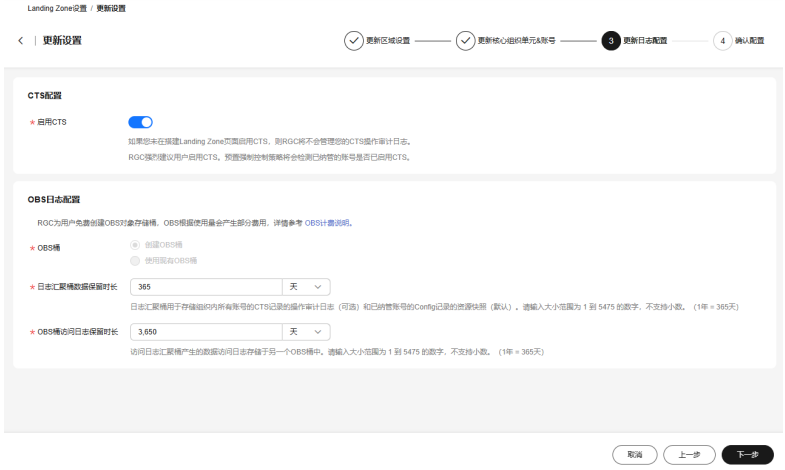
- 更新OBS日志配置：
  - 创建OBS桶：需要配置日志在OBS桶中的保留时长。日志将会自动存放至系统创建的两个默认OBS桶中，不支持自定义OBS桶名。
    - 日志汇聚桶数据保留时长：默认设置为1年。最长设置为15年。

      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 1-16 更新日志配置



步骤8 单击“下一步”。

步骤9 确认更新的设置信息无误，单击“确定”。RGC将会开始对Landing Zone进行更新。

更新成功后，RGC界面将会出现更新成功的提示。

如果更新失败，RGC不会退回到之前的Landing Zone版本，Landing Zone可能将会处于不确定的状态。如果出现该问题，请**提交工单**。

----结束

相关操作

如果需要单独更新账号，请参考**4.4 更新账号**。

2 组织管理

2.1 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。

2.2 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

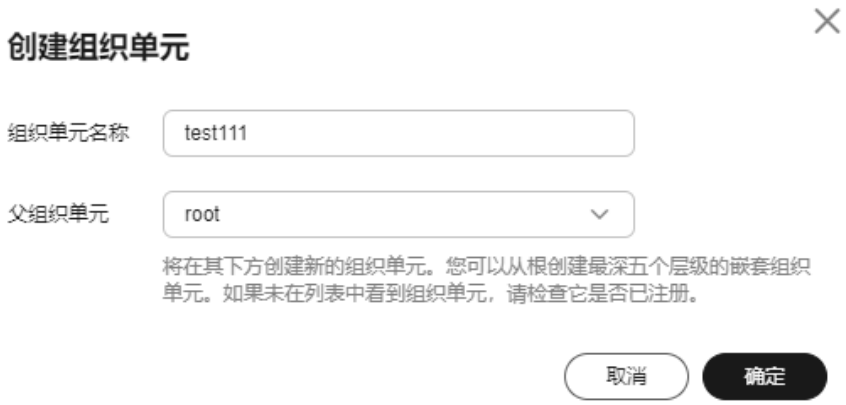
步骤1 以RGC管理账号的身份登录华为云，进入华为云RGC控制台。

步骤2 进入组织管理页，单击“创建组织单元”。

图 2-1 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 2-2 填写组织单元信息



步骤4 然后单击“确认”，完成OU创建。

----结束

2.3 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。

约束与限制

- 正在注册或者重新注册OU时，OU中的账号不能执行取消纳管、纳管、更新账号的操作。
- 不能注册或重新注册核心OU。

操作步骤

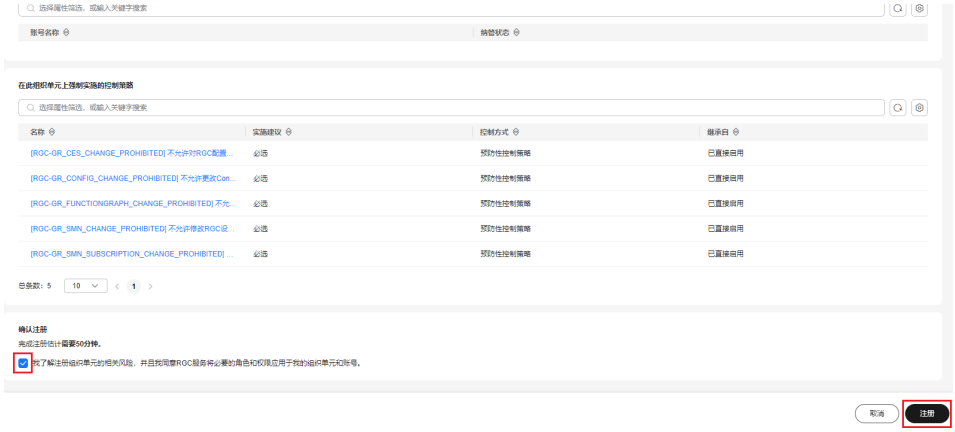
步骤1 以RGC管理账号的身份登录华为云，进入华为云RGC控制台。

步骤2 进入组织管理页，单击需要注册OU所在行“操作”列的“注册”。

图 2-3 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 2-4 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将会受到Landing Zone的监管。

----结束

2.4 重新注册组织单元

如果您需要对OU内多个账号进行更新或需要对OU的信息进行更新，可以选择重新注册OU。

约束与限制

- 重新注册OU时，如果OU中存在创建失败和取消纳管失败的账号，则OU将无法重新注册。
- 不能注册或重新注册核心OU。

操作步骤

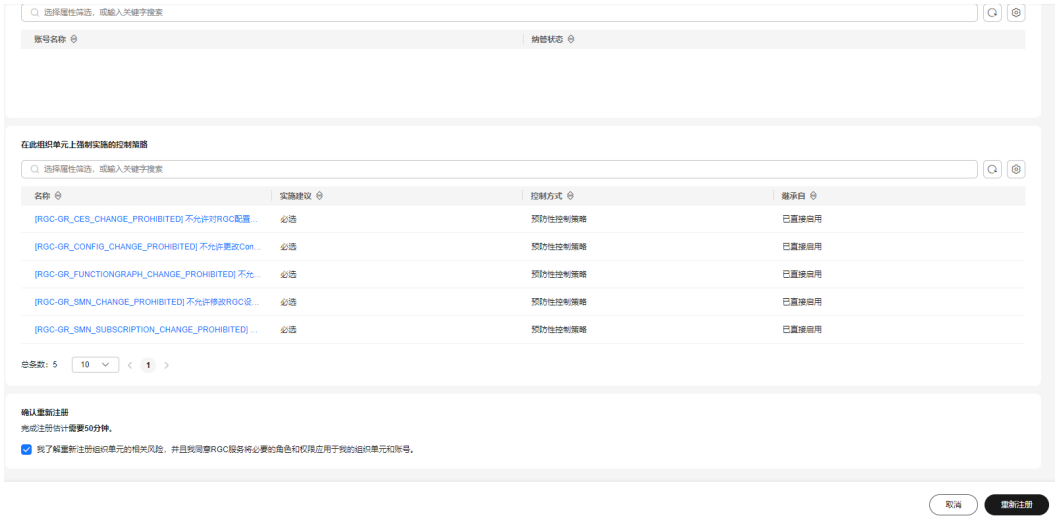
步骤1 以RGC管理账号的身份登录华为云，进入华为云RGC控制台。

步骤2 进入组织管理页，单击需要注册OU所在行“操作”列的“重新注册”。

图 2-5 重新注册 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 2-6 确认 OU 信息



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

----结束

2.5 取消注册组织单元

当您希望注册成功的OU不再受到Landing Zone的监管，或不再希望注册已注册失败的OU，您可以选择取消注册OU。

约束与限制

- 无法取消注册核心OU或根OU。
- 取消注册OU前，请确保OU中无已被注册的子OU和被纳管的账号。如果存在，请先取消注册OU和取消纳管账号。

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。

步骤2 进入组织管理页，单击需要取消注册OU所在行“操作”列的“取消注册”。

图 2-7 取消注册 OU

步骤3 确认需要取消注册的OU信息。确认无误后，单击“确定”。

图 2-8 确认 OU 信息

----结束

2.6 删除组织单元

如果您不再需要某个OU时，您可以在RGC控制台删除OU。删除后，该OU也将从组织服务控制台中删除。

约束与限制

- 无法删除未注册OU、核心OU或根OU。
- 删除OU前，请确保OU中无已被注册的子OU和被纳管的账号。如果存在，请先取消注册OU和取消纳管账号。

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。

步骤2 进入组织管理页，单击需要删除的OU所在行“操作”列的“删除”。

图 2-9 删除 OU

步骤3 确认需要删除的OU信息，输入“DELETE”。

图 2-10 确认删除 OU 信息

步骤4 确认无误后，单击“确定”。

----结束

2.7 查看组织架构详情

在RGC搭建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。

步骤2 进入组织管理页，单击需要查看OU的名称。

图 2-11 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 2-12 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 2-13 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 2-14 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 2-15 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，包括子账号的名称和纳管状态。

图 2-16 查看直系子账号

----结束

3 模板管理

3.1 模板概述

模板简介

模板是一个HCL语法文本描述文件，支持tf、tf.json、zip包文件格式，用于描述您的云资源。模板中可以定义大批量、不同服务、不同规格的资源实例，通过编写模板即可完成应用设计与资源的规划，实现众多资源的自动化部署或销毁操作，使业务的组织和管理变得轻松。且同一模板可以多次重复使用，提升了工作效率。

RGC的账号工厂功能支持通过模板快速创建账号，以满足业务需求。管理账号可以直接在RGC或RFS中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。

更多关于模板的信息，请参阅**资源编排服务用户指南**。

约束与限制

关于模板的规格、配额等约束限制，请参阅**约束与限制**。

场景预置模板

RGC提供以下场景预置模板供您使用：

- **网络规划模块**
  - DNS：该模板可进行DNS Endpoint配置、DNS规则配置以及关联VPC。
  - ER：该模板可直接创建ER及路由配置，并且创建和已有VPC的连接。
  - VPC：该模板可直接创建VPC和subnet。

3.2 上传模板

RGC支持两种方式使用模板：一是使用上传成功的模板文件，二是直接使用预置模板。本章节为您介绍如何将配置好的模板文件上传至RGC中。

约束与限制

- 上传的模板文件不能超过50KB，解压后不超过1MB，且仅支持zip格式。
- 模板的文件内容需要满足**模板约束与限制**。

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 进入模板管理页，单击右上角的“上传模板”。

步骤3 单击“添加文件”，添加已配置好的模板文件。

图 3-1 添加模板文件

步骤4 输入模板名称，模板名称不能重复。

步骤5 单击“确定”，完成模板上传。上传成功的模板将会出现在模板列表中。

----结束

3.3 使用场景预置模板

除了使用自定义上传的模板外，您还可以直接使用RGC中的场景预置模板来快速创建账号。当前RGC提供的场景预置模板请参见**场景预置模板**。

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 进入模板管理页，选择“场景预置模板”页签。

步骤3 单击需要使用的场景化模板名称。

图 3-2 单击场景化模板名称

步骤4 单击需要使用模板所在行“操作”列下的“激活”。

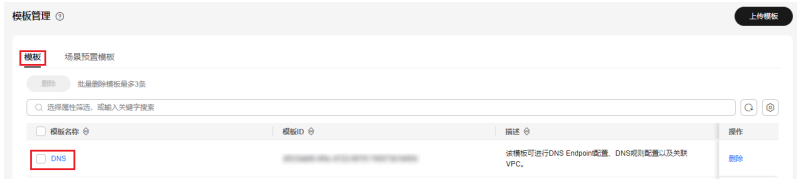
图 3-3 激活模板

步骤5 确认需要启用的模板，单击“确定”。

图 3-4 确认模板

步骤6 返回“模板”页签查看，激活成功的模板将会出现在模板列表中。

图 3-5 激活模板成功



----结束

3.4 查看、修改或删除模板

模板创建成功后，您可以在RGC控制台模板管理中查看模板信息并修改，您也可以前往资源编排服务控制台中“模板库 > 私有模板”中查看创建成功的模板信息并修改。

当模板数量已达到配额上限，或者您不再需要使用某个模板时，您可以在RGC控制台删除模板。删除后，该模板也将从资源编排服务控制台中删除。

场景预置模板删除后，如您仍需继续使用，您可以参考**3.3 使用场景预置模板**激活模板后使用。

约束与限制

- 修改模板时，模板的文件内容需要满足**模板约束与限制**。
- 执行删除操作时，仅会删除模板，不会删除使用此模板创建好的其他资源。

查看、修改模板

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 进入模板管理页，单击目标模板名称。

图 3-6 单击模板名称

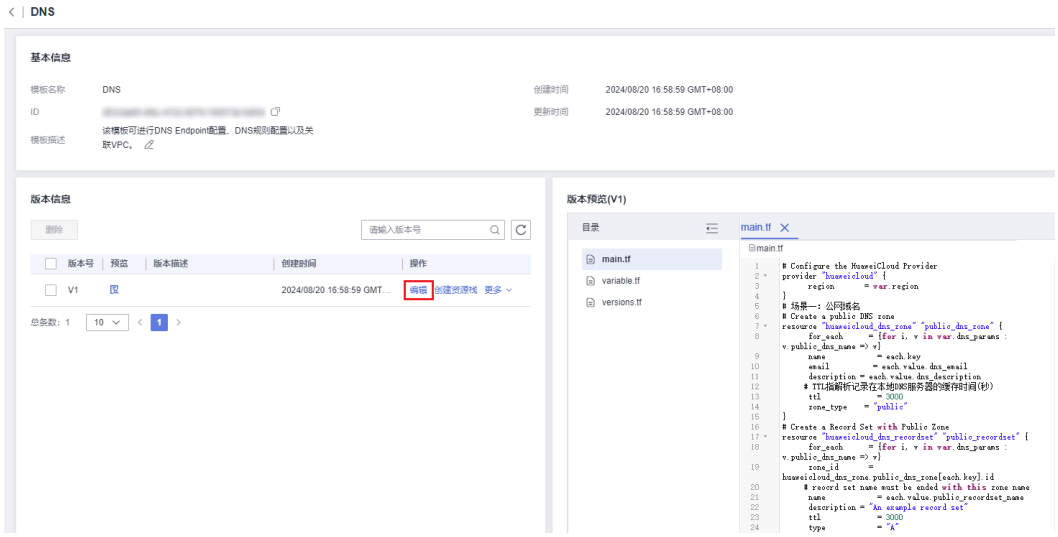
步骤3 进入模板详情页面，可以查看到模板的详细信息。

图 3-7 查看模板详情

步骤4 如果模板内容需要修改，您可以单击“版本信息”模块中目标模板版本“操作”列的“编辑”。

配置模板的相关语法等详细说明请参阅**模板简介**。

图 3-8 修改模板



步骤5 修改模板完成后，单击右上角的“保存模板”。完成模板修改。

----结束

删除模板

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 进入模板管理页，单击需要删除的模板所在行“操作”列的“删除”。

图 3-9 删除模板

步骤3 确认弹窗中删除模板的信息，输入“DELETE”。

步骤4 单击“确定”，删除成功。

----结束

4 账号管理

4.1 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。

步骤2 进入组织管理页，单击“创建账号”。

图 4-1 创建账号

步骤3 配置账号基本信息。输入邮箱地址、账号名。不能与其他账号重复。

基本信息中的邮箱地址、，仅展示作用，不用于密码找回等场景。

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 4-2 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。

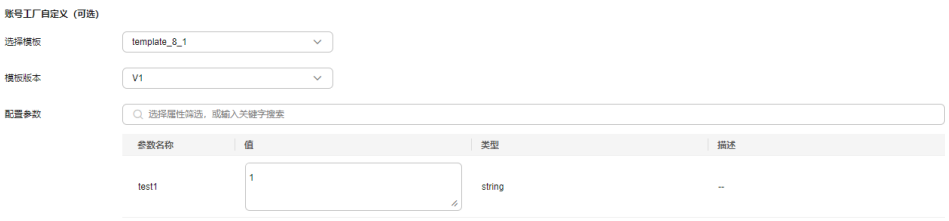
图 4-3 选择组织单元

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 4-4 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

4.2 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。
- 如果您希望将账号通过纳管账号的方式从某个Landing Zone转移至另一个Landing Zone中，请先将账号从原Landing Zone中取消纳管后，再在当前Landing Zone中执行纳管操作。如果您已在当前Landing Zone中完成账号纳管，请手动将在原Landing Zone中该账号的相关资源包括委托、策略等删除，否则将会出现错误。
- 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 4-5 创建委托

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

图 4-6 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“完成”。

步骤7 在授权的确认弹窗中，单击“立即授权”。

步骤8 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 4-7 需要授予委托的权限

步骤9 单击“下一步”，选择权限的作用范围。

步骤10 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**操作步骤**完成账号纳管。

说明

RGCServiceExecutionAgency委托创建后不允许删除，否则将会导致RGC服务不可用。

----结束

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 进入组织管理页，单击需要纳管的账号所在行“操作”列的“纳管”。

图 4-8 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。

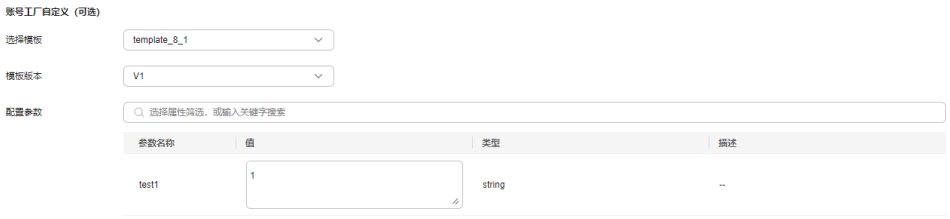
图 4-9 选择组织单元

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 4-10 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

4.3 查看账号详情

在RGC设置Landing Zone后，可以查看已纳管账号中的基本信息、不合规资源、模板详情、区域，以及使用的外部Config规则。

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 进入组织管理页，单击需要查看的账号名称。

图 4-11 查看账号详情

步骤3 在基本信息中，可以查看账号的状态、组织单元、受监管区域的数量、合规状态、以及已启用的控制策略数量。

如账号下存在不合规资源，将会展示为“不合规”状态。

图 4-12 查看账号基本信息

步骤4 选择“不合规资源”页签，将会显示当前账号下存在的不合规资源，以及不合规资源ID、相关的控制策略、类型、服务和所在区域等。

图 4-13 查看不合规资源

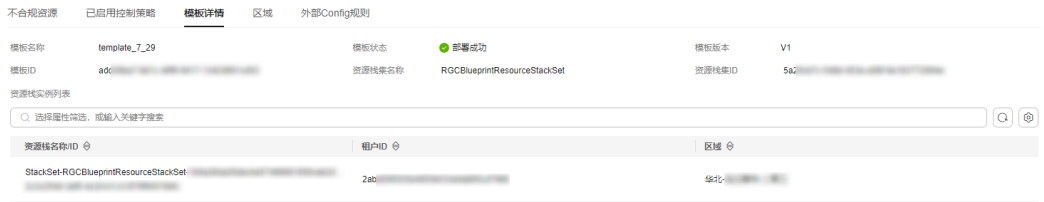
步骤5 选择“已启用控制策略”页签，将会显示针对当前账号已启用的控制策略。

如需了解控制策略详情，请参考**5.4 查看控制策略详情**。

图 4-14 查看已启用控制策略

步骤6 选择“模板详情”页签，将会显示该账号使用的RFS模板详情。如果该账号未使用模板，则将不会显示相关信息。

图 4-15 查看模板详情



步骤7 选择“区域”页签，将会显示该账号受监管的区域详情。账号以及账号的资源将在展示的区域中，受到Landing Zone的监管。其他区域的资源则不受监管。

图 4-16 查看账号受监管的区域

步骤8 选择“外部Config规则”页签，将会显示该账号除当前Landing Zone开启的Config规则外，账号下的其他Config规则，以及对应规则作用的区域。

图 4-17 查看外部 Config 规则

----结束

4.4 更新账号

如果您希望对账号所属的OU和使用的模板、模板版本进行更改，可以对账号进行更新。

更改账号所属的OU后，新的OU所应用的控制策略可能与原OU的控制策略不同，需要确认新OU所启用的控制策略符合您对账号的要求后再执行该操作。

操作步骤

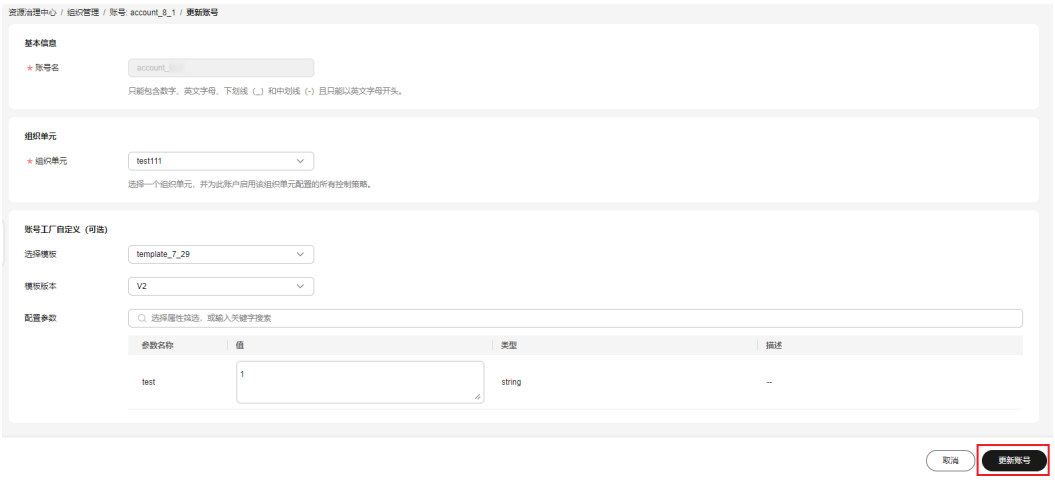
步骤1 以RGC管理账号的身份登录华为云，进入华为云RGC控制台。

步骤2 进入组织管理页，单击需要更新的账号所在行“操作”列的“更新”。

图 4-18 更新账号

步骤3 重新选择账号所属的组织单元、模板以及模板版本。

图 4-19 修改账号信息



步骤4 单击右下角“更新账号”。更新成功后，可以单击账号名称查看账号的信息。

----结束

4.5 取消纳管账号

当您希望已纳管的账号不再受到Landing Zone的监管，或不再希望继续纳管已纳管失败的账号，您可以选择取消纳管账号。

约束与限制

- 需要取消纳管的账号需要存在于RGC中。
- 只有已纳管、纳管失败、取消纳管失败状态的账号可以执行取消纳管账号。
- 取消纳管账号归属的OU不能处于正在操作的状态。

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 进入组织管理页，单击需要纳管的账号所在行“操作”列的“取消纳管”。

图 4-20 取消纳管账号

步骤3 确认弹窗中需要取消纳管账号的信息，单击“确定”。

图 4-21 确认取消纳管账号信息

步骤4 操作取消纳管成功后，账号将会出现在根OU下，并且状态为“未纳管”。

----结束

4.6 使用账号工厂创建账号

管理账号可以直接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。管理账号可以直接使用RGC

模板管理中的模板，当前暂不支持在RGC界面中创建模板，请前往资源编排服务控制台进行创建。

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 4-22 创建账号

步骤3 配置账号基本信息。输入邮箱地址、账号名。不能与其他账号重复。

基本信息中的邮箱地址、，仅展示作用，不用于密码找回等场景。

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 4-23 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 4-24 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 4-25 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。
- 主动性控制策略：主动控制策略基于ResourceFormation hook，该类型的策略在基于IaC模板编排云上资源之前，会检视IaC模板内描述的资源配置，若与策略内预置的合规配置冲突，则会拦截IaC模板进入下一步的编排动作。

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
- 加密传输中的数据
- 提高可用性
- 管理漏洞
- 使用强身份验证
- 提高韧性
- 管理机密
- 为灾难恢复做好准备
- 为事件响应做好准备
- 弹性负载均衡

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

名称：不允许删除日志桶

实现：SCP

类型：预防性控制策略

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_AUDIT_BUCKET_ENCRYPTION_CHANGES_PROHIBITED

名称：不允许修改日志桶的加密配置

实现：SCP

类型：预防性控制策略

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_AUDIT_BUCKET_LIFECYCLE_CONFIGURATION_CHANGES_PROHIBITED

名称：不允许修改日志桶的生命周期

实现：SCP

类型：预防性控制策略

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_AUDIT_BUCKET_LOGGING_CONFIGURATION_CHANGES_PROHIBITED

名称：不允许修改日志桶的桶日志配置

实现：SCP

类型：预防性控制策略

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_AUDIT_BUCKET_POLICY_CHANGES_PROHIBITED

名称：不允许修改日志桶的桶策略

实现：SCP

类型：预防性控制策略

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_CES_CHANGE_PROHIBITED

名称：不允许对RGC配置的CES进行更改

实现：SCP

类型：预防性控制策略

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

名称：不允许更改Config记录器

实现：SCP

类型：预防性控制策略

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_FUNCTIONGRAPH_CHANGE_PROHIBITED

名称：不允许修改RGC设置的FunctionGraph函数

实现：SCP

类型：预防性控制策略

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

名称：不允许修改RGC设置的SMN通知

实现：SCP

类型：预防性控制策略

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

名称：不允许订阅RGC设置的SMN通知

实现：SCP

类型：预防性控制策略

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"
              ]
          }
```



```
    }
  }]
}
```

RGC-GR_CONFIG_CTS_TRACKER_EXISTS

名称：账号未创建CTS追踪器，视为“不合规”

实现：Config rule

类型：检测性控制策略

功能：检测账号中是否创建CTS追踪器。

```
terraform {
  required_providers {
    huaweicloud = {
      source = "huaweie.com/provider/huaweicloud"

      version = ">=1.51.0"
    }
  }
}
provider "huaweicloud" {
  endpoints = {}
  insecure = true
}
variable "ConfigName" {
  description = "config name"
  type = string
  default = "cts-tracker-exists"
}
variable "PolicyAssignmentName" {
  description = "policy assignment name"
  type = string
  default = "rgc_cts_tracker_exists"
}
variable "ConfigRuleDescription" {
  description = "config rule description"
  type = string
  default = "账号未创建CTS追踪器，视为“不合规”"
}#
待补充
variable "RegionName" {
  description = "policy region"
  type = string
}
data "huaweicloud_rms_policy_definitions"
"rms_policy_definitions_check" {
  name =
    var.ConfigName
}
resource "huaweicloud_rms_policy_assignment"
"rms_policy_assignment_check" {
  name =
    var.PolicyAssignmentName
  description =
    var.ConfigRuleDescription
  policy_definition_id =
    try (data.huaweicloud_rms_policy_definitions.rms_policy_definitions_check.definitions[0].id, "")
  period = "TwentyFour_Hours"
  status = "Enabled"
}
```

RGC-GR_CONFIG_OBS_BUCKET_PUBLIC_READ_POLICY_CHECK

名称：桶可以被公开读，视为“不合规”

实现：Config rule

类型：检测性控制策略

功能：检测桶策略是否为公共读。

```
terraform {
  required_providers {
    huaweicloud = {
      source = "huawei.com/provider/huaweicloud"

      version = ">=1.51.0"
    }
  }
}
provider "huaweicloud" {
  endpoints = {}
  insecure = true
}
variable "ConfigName" {
  description = "config name"
  type = string
  default = "obs-bucket-public-read-policy-check"
}
variable "PolicyAssignmentName" {
  description = "policy assignment name"
  type = string
  default = "rgc_obs_bucket_public_read_policy_check"
}
variable "ConfigRuleDescription" {
  description = "config rule description"
  type = string
  default = "桶可以被公开读，视为“不合规”"
}
variable "ResourceProvider" {
  description = "resource provider"
  type = string
  default = "obs"
}
variable "ResourceType" {
  description = "resource type"
  type = string
  default = "buckets"
}
variable "RegionName" {
  description = "policy region"
  type = string
}
variable "IsGlobalResource" {
  description = "is global resource"
  type = bool
  default = false
}
data "huaweicloud_rms_policy_definitions"
"rms_policy_definitions_check" {
  name =
    var.ConfigName
}
resource "huaweicloud_rms_policy_assignment"
"rms_policy_assignment_check" {
  name =
    var.IsGlobalResource ? format("%s",
      var.PolicyAssignmentName) : format("%s_%s",
      var.PolicyAssignmentName,
      var.RegionName)
  description =
    var.ConfigRuleDescription
  policy_definition_id =
    try (data.huaweicloud_rms_policy_definitions.rms_policy_definitions_check.definitions[0].id, "")
  status = "Enabled"
```

```
  policy_filter {
    region =
      var.RegionName
    resource_provider =
      var.ResourceProvider
    resource_type =
      var.ResourceType
  }
}
```

RGC-GR_CONFIG_OBS_BUCKET_PUBLIC_WRITE_POLICY_CHECK

名称：桶可以被公开写，视为“不合规”

实现：Config rule

类型：检测性控制策略

功能：检测桶策略是否为公共读写。

```
terraform {
  required_providers {
    huaweicloud = {
      source = "huawei.com/provider/huaweicloud"

      version = ">=1.51.0"
    }
  }
}
provider "huaweicloud" {
  endpoints = {}
  insecure = true
}
variable "ConfigName" {
  description = "config name"
  type = string
  default = "obs-bucket-public-write-policy-check"
}
variable "PolicyAssignmentName" {
  description = "policy assignment name"
  type = string
  default = "rgc_obs_bucket_public_write_policy_check"
}
variable "ConfigRuleDescription" {
  description = "config rule description"
  type = string
  default = "桶可以被公开写，视为“不合规”"
}
variable "ResourceProvider" {
  description = "resource provider"
  type = string
  default = "obs"
}
variable "ResourceType" {
  description = "resource type"
  type = string
  default = "buckets"
}
variable "RegionName" {
  description = "policy region"
  type = string
}
variable "IsGlobalResource" {
  description = "is global resource"
  type = bool
  default = false
}
```

```
data "huaweicloud_rms_policy_definitions"
"rms_policy_definitions_check" {
  name =
    var.ConfigName
}
resource "huaweicloud_rms_policy_assignment"
"rms_policy_assignment_check" {
  name =
    var.IsGlobalResource ? format("%s",
      var.PolicyAssignmentName) : format("%s_%s",
      var.PolicyAssignmentName,
      var.RegionName)
  description =
    var.ConfigRuleDescription
  policy_definition_id =
    try (data.huaweicloud_rms_policy_definitions.rms_policy_definitions_check.definitions[0].id, "")
  status = "Enabled"

  policy_filter {
    region =
      var.RegionName
    resource_provider =
      var.ResourceProvider
    resource_type =
      var.ResourceType
  }
}
```

RGC-GR_DETECT_CTS_ENABLED_ON_SHARED_ACCOUNTS

名称：CTS追踪器未转储到LTS，视为“不合规”

实现：Config rule

类型：检测性控制策略

功能：检测CTS追踪器是否已转储到LTS。

```
terraform {
  required_providers {
    huaweicloud = {
      source = "huawei.com/provider/huaweicloud"

      version = "1.49.0"
    }
  }
}
provider "huaweicloud" {
  endpoints = {}
  insecure = true
}
variable "ConfigName" {
  description = "config name"
  type = string
  default = "cts-lts-enable"
}
variable "PolicyAssignmentName" {
  description = "policy assignment name"
  type = string
  default = "rgc_cts_lts_enable"
}
variable "ConfigRuleDescription" {
  description = "config rule description"
  type = string
  default = "CTS追踪器未转储到LTS，视为“不合规”"
}
variable "ResourceProvider" {
  description = "resource provider"
```

```
    type = string
    default = "cts"
}
variable "ResourceType" {
    description = "resource type"
    type = string
    default = "trackers"
}
variable "RegionName" {
    description = "policy region"
    type = string
}
data "huaweicloud_rms_policy_definitions"
"ctsltsenable" {
    name =
        var.ConfigName
}
resource "huaweicloud_rms_policy_assignment"
"cts_lts_enable" {
    name = format("%s_%s",
        var.PolicyAssignmentName,
        var.RegionName)
    description =
        var.ConfigRuleDescription
    policy_definition_id =
        try (data.huaweicloud_rms_policy_definitions.ctsltsenable.definitions[0].id, "")
    status = "Enabled"

    parameters = {

    }
    policy_filter {
        region =
            var.RegionName
        resource_provider =
            var.ResourceProvider
        resource_type =
            var.ResourceType
    }
}
```

5.2.2 强烈建议控制策略

APIG

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
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	不涉及
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	不涉及

AS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_AS_GROUP_IN_VPC	AS弹性伸缩组绑定的VPC不在对应VPC列表，视为“不合规”。	限制网络访问	高	as:::group	否

BMS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_BMS_KEY_PAIR_SECURITY_LOGIN	裸金属服务器未启用密钥对安全登录，视为“不合规”。	使用强身份验证	高	bms:::instance	不涉及

CBR

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CBR_BACKUP_ENCRYPTED_CHECK	CBR服务的备份未被加密，视为“不合规”。	加密静态数据	高	cbr:::checkpoint	不涉及

CCE

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
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	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CCE_CLUSTER_IN_VPC	CCE集群绑定的VPC不在对应VPC列表，视为“不合规”。	限制网络访问	高	cce:::cluster	否

CCM

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_PCA_CERTIFICATE_AUTHORITY_EXPIRATION_CHECK	私有CA在指定时间内过期，视为“不合规”。	加密传输中的数据	中	ccm:::privateCertificate	不涉及
RGC-GR_CONFIG_PCA_CERTIFICATE_EXPIRATION_CHECK	私有证书在指定时间内到期，视为“不合规”。	加密传输中的数据	中	ccm:::privateCertificate	不涉及

CDN

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CDN_ENABLE_HTTPS_CERTIFICATE	CDN未使用HTTPS，视为“不合规”。	加密传输中的数据	严重	cdn:::domain	不涉及
RGC-GR_CONFIG_CDN_ORIGIN_PROTOCOL_NO_HTTP	CDN回源方式未使用HTTPS，视为“不合规”。	加密传输中的数据	严重	cdn:::domain	不涉及
RGC-GR_CONFIG_CDN_SECURITY_POLICY_CHECK	CDN使用TLSv1.2以下的版本，视为“不合规”。	加密传输中的数据	高	cdn:::domain	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CDN_USE_MY_CERTIFICATE	CDN使用了自有证书，视为“不合规”。	加密传输中的数据	高	cdn:::domain	不涉及

CFW

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CFW_POLICY_NOT_EMPTY	CFW防火墙未配置防护策略，视为“不合规”。	限制网络访问	中	cfw:::eipProtection	不涉及

CodeArts Build

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CLOUDBUILDSERVER_ENCRYPTION_PARAMETER_CHECK	CodeArts编译构建下的项目，如果设置了未加密参数（除了预定义参数），视为“不合规”。	加密静态数据	中	codearts:::deployApplication	不涉及

CSS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CSS_CLUSTER_AUTHORITY_ENABLE	CSS集群未启用认证，视为“不合规”。	使用强身份验证	严重	css:::cluster	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CSS_CLUSTER_DISK_ENCRYPTION_CHECK	CSS集群未开启磁盘加密，视为“不合规”。	加密静态数据	高	css:::cluster	不涉及
RGC-GR_CONFIG_CSS_CLUSTER_KIBANA_NOT_ENABLE_WHITE_LIST	CSS集群kibana白名单设置为对所有IP开放，视为“不合规”。	限制网络访问	严重	css:::cluster	不涉及
RGC-GR_CONFIG_CSS_CLUSTER_NO_PUBLIC_ZONE	CSS集群开启公网访问，视为“不合规”。	加密静态数据	高	css:::cluster	不涉及
RGC-GR_CONFIG_CSS_CLUSTER_NOT_ENABLE_WHITE_LIST	CSS集群白名单设置为对所有IP开放，视为“不合规”。	限制网络访问	严重	css:::cluster	不涉及
RGC-GR_CONFIG_CSS_CLUSTER_SECURITY_MODE_ENABLE	CSS集群未开启安全模式，视为“不合规”。	强制执行最低权限	高	css:::cluster	不涉及
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	不涉及

CTS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CTS_KMS_ENCRYPTED_CHECK	CTS追踪器未通过KMS进行加密，视为“不合规”。	加密静态数据	中	cts:::tracker	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CTS_SUPPORT_VALIDATE_CHECK	CTS追踪器未打开事件文件校验，视为“不合规”。	保护数据完整性	中	cts:::tracker	不涉及

DCS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_DCS_MEMCACHED_ENABLE_SSL	dcs memcached资源可以公网访问，但不支持SSL时，视为“不合规”。	加密传输中的数据	高	dcs:::instance	不涉及
RGC-GR_CONFIG_DCS_MEMCACHED_NO_PUBLIC_IP	dcs memcached资源存在公网IP，视为“不合规”。	限制网络访问	高	dcs:::instance	不涉及
RGC-GR_CONFIG_DCS_MEMCACHED_PASSWORD_ACCESS	dcs memcached资源不需要密码访问，视为“不合规”。	使用强身份验证	中	dcs:::instance	不涉及
RGC-GR_CONFIG_DCS_REDIS_ENABLE_SSL	dcs redis资源可以公网访问，但不支持SSL时，视为“不合规”。	限制网络访问	高	dcs:::instance	不涉及
RGC-GR_CONFIG_DCS_REDIS_HIGH_TOLERANCE	dcs redis资源不是高可用时，视为“不合规”。	提高可用性	低	dcs:::instance	不涉及
RGC-GR_CONFIG_DCS_REDIS_NO_PUBLIC_IP	dcs redis资源存在公网IP，视为“不合规”。	限制网络访问	高	dcs:::instance	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_DCS_REDIS_PASSWORD_ACCESS	dcs redis资源不需要密码访问，视为“不合规”。	使用强身份验证	中	dcs:::instance	不涉及
RGC-GR_CONFIG_DCS_MEMCACHED_IN_VPC	指定虚拟私有云ID，不属于此VPC的dcs memcached资源，视为“不合规”。	限制网络访问	中	dcs:::instance	否
RGC-GR_CONFIG_DCS_REDIS_IN_VPC	指定虚拟私有云ID，不属于此VPC的dcs redis资源，视为“不合规”。	限制网络访问	中	dcs:::instance	否

DDS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_DDS_INSTANCE_ENABLE_SSL	DDS实例未开启SSL，视为“不合规”。	加密传输中的数据	高	dds:::instance	不涉及
RGC-GR_CONFIG_DDS_INSTANCE_HAS_EIP	DDS实例绑定了公网IP，视为“不合规”。	限制网络访问	高	dds:::instance	不涉及
RGC-GR_CONFIG_DDS_INSTANCE_PORT_CHECK	DDS实例的端口包含被禁止的端口，视为“不合规”。	限制网络访问	高	dds:::instance	不涉及

DEW

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CSMS_SECRETS_ROTATION_SUCCESS_CHECK	CSMS凭据轮转失败，视为“不合规”。	强制执行最低权限	高	csms:::secret	不涉及
RGC-GR_CONFIG_KMS_NOT_SCHEDULED_FOR_DELETION	KMS密钥处于“计划删除”状态，视为“不合规”。	保护数据完整性	严重	kms:::key	不涉及
RGC-GR_CONFIG_KMS_ROTATION_ENABLED	KMS密钥未启用密钥轮换，视为“不合规”。	加密静态数据	中	kms:::key	不涉及

DMS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_DMS_KAFKA_NOT_ENABLE_PRIVATE_SSL	DMS kafkas队列未打开内网SSL加密访问，视为“不合规”。	加密传输中的数据	中	dms:::kafkaInstance	不涉及
RGC-GR_CONFIG_DMS_KAFKA_NOT_ENABLE_PUBLIC_SSL	DMS kafkas队列未打开公网SSL加密访问，视为“不合规”。	加密传输中的数据	中	dms:::kafkaInstance	不涉及
RGC-GR_CONFIG_DMS_KAFKA_PUBLIC_ACCESS_ENABLED_CHECK	DMS kafkas队列开启公网访问，视为“不合规”。	限制网络访问	高	dms:::kafkaIZnstance	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_DMS_RABBITMQ_NOT_ENABLE_SSL	DMS rabbitmqs队列未打开SSL加密访问，视为“不合规”。	加密静态数据	高	dms:::rabbitmqInstance	不涉及
RGC-GR_CONFIG_DMS_ROCKETMQ_NOT_ENABLE_SSL	DMS reliabilitys队列未打开SSL加密访问，视为“不合规”。	加密静态数据	高	dms:::rocketmqInstance	不涉及
RGC-GR_CONFIG_DMS_RABBITMQ_PUBLIC_ACCESS_ENABLED_CHECK	DMS RabbitMQ实例开启公网访问，视为“不合规”。	限制网络访问	中	dms:::rabbitmqInstance	不涉及
RGC-GR_CONFIG_DMS_RELIABILITY_PUBLIC_ACCESS_ENABLED_CHECK	DMS RocketMQ实例开启公网访问，视为“不合规”。	限制网络访问	中	dms:::rocketmqInstance	不涉及

DRS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_DRS_DATA_GUARD_JOB_NOT_PUBLIC	数据复制服务实时灾备任务使用公网网络，视为“不合规”。	限制网络访问	高	drs:::job	不涉及
RGC-GR_CONFIG_DRS_MIGRATION_JOB_NOT_PUBLIC	数据复制服务实时迁移任务使用公网网络，视为“不合规”。	限制网络访问	高	drs:::job	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_DRS_SYNCHRONIZATION_JOB_NOT_PUBLIC	数据复制服务实时同步任务使用公网网络，视为“不合规”。	限制网络访问	高	drs:::job	不涉及

DWS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_DWS_ENABLE_KMS	DWS集群未启用KMS加密，视为“不合规”。	加密静态数据	中	dws:::cluster	不涉及
RGC-GR_CONFIG_DWS_ENABLE_SSL	DWS集群未启用SSL加密连接，视为“不合规”。	加密传输中的数据	中	dws:::cluster	不涉及
RGC-GR_CONFIG_DWS_CLUSTERS_NO_PUBLIC_IP	DWS集群绑定公网IP，视为“不合规”。	限制网络访问	高	dws:::cluster	不涉及
RGC-GR_CONFIG_DWS_CLUSTERS_IN_VPC	DWS集群绑定的VPC不在对应VPC列表，视为“不合规”。	限制网络访问	高	dws:::cluster	否

ECS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_ECS_INSTANCE_KEY_PAIR_LOGIN	ECS未配置密钥对，视为“不合规”。	限制网络访问	高	ecs:::instanceV1	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
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	不涉及
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	不涉及
RGC-GR_CONFIG_ECS_INSTANCE_AGENCY_ATTACH_IAM_AGENCY	ECS实例未附加IAM委托，视为“不合规”。	强制执行最低权限	低	ecs:::instanceV1	不涉及
RGC-GR_CONFIG_ECS_IN_ALLOWED_SECURITY_GROUPS	指定高危安全组ID列表，未绑定指定标签的ECS关联其中任意安全组，视为“不合规”。	限制网络访问	高	ecs:::instanceV1	• specifiedECSTagValue：否 • specifiedECSTagKey：是 • specifiedSecurityGroupIds：否

ECS、VPC

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_ECS_INSTANCE_IN_VPC	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”。	限制网络访问	中	ecs:::instanceV1	否

ELB

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_ELB_LOADBALANCERS_NO_PUBLIC_IP	ELB资源具有公网IP，视为“不合规”。	限制网络访问	中	elb:::loadBalancer	不涉及
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	不涉及
RGC-GR_CONFIG_ELB_PREDEFINED_SECURITY_POLICY_HTTPS_CHECK	独享型负载均衡器关联的HTTPS协议类型监听器未配置指定的预定义安全策略，视为“不合规”。	限制网络访问	中	elb:::loadBalancer	不涉及
RGC-GR_CONFIG_ELB_HTTP_TO_HTTPS_REDIRECTION_CHECK	检查HTTP监听器是否配置了向HTTPS监听器的重定向，如果未配置，视为“不合规”。	限制网络访问	中	elb:::listener	不涉及

EVS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_VOLUMES_ENCRYPTED_CHECK_BY_DEFAULT	云硬盘未进行加密，视为“不合规”。	加密静态数据	高	evs:::volume	不涉及

EVS、ECS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_VOLUMES_ENCRYPTED_CHECK	已挂载的云硬盘未进行加密，视为“不合规”。	加密静态数据	低	evs:::volume	不涉及

Functiongraph

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
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	不涉及

GaussDB

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_GAUSSDB_INSTANCE_IN_VPC	指定虚拟私有云ID，不属于此VPC的gaussdb资源，视为“不合规”。	限制网络访问	中	gaussdb:::opengaussInstance	否
RGC-GR_CONFIG_GAUSSDB_INSTANCE_NO_PUBLIC_IP_CHECK	gaussdb实例如绑定EIP，视为“不合规”。	限制网络访问	高	gaussdb:::opengaussInstance	不涉及
RGC-GR_CONFIG_GAUSSDB_INSTANCE_SSL_ENABLE	gaussdb实例未启用SSL数据传输加密，视为“不合规”。	加密传输中的数据	高	gaussdb:::opengaussInstance	不涉及

GeminiDB

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_GAUSSDB_NOSQL_ENABLE_DISK_ENCRYPTION	GeminiDB未使用磁盘加密，视为“不合规”。	加密静态数据	中	gaussdb:::mongoInstance	不涉及

IAM

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
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	不涉及
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	不涉及
RGC-GR_CONFIG_IAM_GROUP_HAS_USERS_CHECK	IAM用户组未添加任意IAM用户，视为“不合规”。	强制执行最低权限	中	identity:::group	不涉及
RGC-GR_CONFIG_IAM_USER_ACCESS_MODE	IAM用户同时开启控制台访问和API访问，视为“不合规”。	强制执行最低权限	中	identity:::user	不涉及
RGC-GR_CONFIG_IAM_USER_CONSOLE_AND_API_ACCESS_AT_CREATION	对于从console侧访问的IAM用户，其创建时设置访问密钥，视为“不合规”。	管理机密	中	identity:::user	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_IAM_USER_SINGLE_ACCESS_KEY	IAM用户拥有多个处于“active”状态的访问密钥，视为“不合规”。	管理机密	高	identity:::user	不涉及
RGC-GR_CONFIG_MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	通过console密码登录的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	不涉及
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	不涉及
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	不涉及
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	不涉及
RGC-GR_CONFIG_ACCESS_KEYS_ROTATED	IAM用户的访问密钥未在指定天数内轮转，视为“不合规”。	强制执行最低权限	高	identity:::accessKey	不涉及
RGC-GR_CONFIG_IAM_PASSWORD_POLICY	IAM用户密码强度不满足密码强度要求，视为“不合规”。	使用强身份验证	高	identity:::user	不涉及
RGC-GR_CONFIG_IAM_USER_LAST_LOGIN_CHECK	IAM用户在指定时间范围内无登录行为，视为“不合规”。	强制执行最低权限	低	identity:::user	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_IAM_POLICY_IN_USE	IAM策略未附加到IAM用户、用户组或委托，视为“不合规”。	强制执行最低权限	低	identity:::protectionPolicy	不涉及
RGC-GR_CONFIG_IAM_ROLE_IN_USE	IAM权限未附加到IAM用户、用户组或委托，视为“不合规”。	强制执行最低权限	低	identity:::role	不涉及
RGC-GR_CONFIG_IAM_USER_LOGIN_PROTECTION_ENABLED	IAM用户未开启登录保护，视为“不合规”。	使用强力身份验证	中	identity:::user	不涉及
RGC-GR_CONFIG_IAM_POLICY_BLACKLISTED_CHECK	IAM的用户、用户组、委托使用指定权限或策略，视为“不合规”。	强制执行最低权限	高	• identity:::user • identity:::group • identity:::agency	否
RGC-GR_CONFIG_IAM_USER_GROUP_MEMBERSHIP_CHECK	IAM用户不属于指定IAM用户组，视为“不合规”。	强制执行最低权限	中	identity:::user	否
RGC-GR_CONFIG_IAM_AGENCIES_MANAGED_POLICY_CHECK	IAM委托未绑定指定的IAM策略和权限，视为“不合规”。	强制执行最低权限	高	identity:::agency	• roleIdList：否 • policyIdList：否
RGC-GR_CREATE_ROOT_AK_PROHIBITED	不允许创建根用户访问密钥。	保护配置	严重	identity:::accessKey	不涉及
RGC-GR_ROOT_USER_PROHIBITED	不允许以根用户身份操作。	保护配置	严重	identity:::user	不涉及

IMS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_IMS_IMAGES_ENABLE_ENCRYPTION	私有镜像未开启加密，视为“不合规”。	加密静态数据	高	images:::image	不涉及

MRS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_MRS_CLUSTER_KERBEROS_ENABLED	MRS集群未开启kerberos认证，视为“不合规”。	使用强身份验证	中	mrs:::cluster	不涉及
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	不涉及
RGC-GR_CONFIG_MRS_CLUSTER_IN_ALLOWED_SECURITY_GROUPS	指定安全组ID，不属于此安全组的mrs资源，视为“不合规”。	限制网络访问	中	mrs:::cluster	否
RGC-GR_CONFIG_MRS_CLUSTER_IN_VPC	指定虚拟私有云ID，不属于此VPC的mrs资源，视为“不合规”。	限制网络访问	中	mrs:::cluster	否

NAT

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_PRIVATE_NAT_GATEWAY_AUTHORIZED_VPC_ONLY	NAT私网网关未与指定的VPC资源绑定，视为“不合规”。	限制网络访问	高	nat:::privateGateway	否

OBS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_OBS_BUCKET_POLICY_GRANTEE_CHECK	OBS桶策略授权了不被允许的访问行为，视为“不合规”。	强制执行最低权限	高	obs:::bucket	• principal：否 • sourceVpc：否 • sourceIp：否 • sourceVpce：否

RDS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
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	不涉及
RGC-GR_CONFIG_RDS_INSTANCES_ENABLE_KMS	未开启存储加密的rds资源，视为“不合规”。	加密静态数据	低	rds:::instance	不涉及
RGC-GR_CONFIG_RDS_INSTANCE_PORT_CHECK	RDS实例的端口包含被禁止的端口，视为“不合规”。	限制网络访问	高	rds:::instance	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_RDS_INSTANCE_SSL_ENABLE	RDS实例未启用SSL加密通讯，视为“不合规”。	加密静态数据	高	rds:::instance	不涉及

SFS Turbo

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_SFSTURBO_ENCRYPTED_CHECK	弹性文件服务(SFS Turbo)未通过KMS进行加密，视为“不合规”。	加密静态数据	低	sfsturbo:::dir	不涉及

TaurusDB

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_IN_VPC	TaurusDB实例绑定的VPC不在对应VPC列表，视为“不合规”。	限制网络访问	高	gaussdb:::mysqlInstance	否
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_NO_PUBLIC_IP_CHECK	TaurusDB实例如绑定弹性公网IP，视为“不合规”。	限制网络访问	高	gaussdb:::mysqlInstance	不涉及
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_SSL_ENABLE	TaurusDB实例未启用SSL数据传输加密，视为“不合规”。	加密传输中的数据	高	gaussdb:::mysqlInstance	不涉及

VPC

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
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	不涉及
RGC-GR_CONFIG_VPC_ACL_UNUSED_CHECK	检查是否存在未使用的网络ACL，如果网络ACL没有与子网关联，视为“不合规”。	保护配置	低	vpc:::networkAcl	不涉及
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	不涉及
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	不涉及
RGC-GR_CONFIG_VPC_SG_ATTACHED_PORTS	检查非默认安全组是否连接到弹性网络接口(ports)。如果安全组未关联弹性网络接口（ports），视为“不合规”	限制网络访问	中	vpc:::eip	不涉及
RGC-GR_CONFIG_VPC_SG_BY_WHITE_LIST_PORTS_CHECK	除指定的白名单端口外，其余端口的安全组策略为允许，视为“不合规”。	限制网络访问	高	vpc:::eip	否

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_VPC_SG_RESTRICTED_COMMON_PORTS	当安全组的入站流量不限制指定端口的所有IPv4地址(0.0.0.0/0)或所有IPv6端口(::/0)，视为“不合规”。	限制网络访问	高	vpc:::eip	不涉及

WAF

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_WAF_INSTANCE_POLICY_NOT_EMPTY	WAF防护域名未配置防护策略，视为“不合规”。	限制网络访问	中	waf:::cloudInstance	不涉及
RGC-GR_CONFIG_WAF_POLICY_NOT_EMPTY	WAF防护策略未配置防护规则，视为“不合规”。	限制网络访问	中	waf:::policy	不涉及
RGC-GR_CONFIG_WAF_INSTANCE_ENABLE_BLOCK_POLICY	WAF实例未启用拦截模式防护策略，视为“不合规”。	限制网络访问	中	waf:::cloudInstance	不涉及
RGC-GR_CONFIG_WAF_INSTANCE_ENABLE_PROTECT	如果账号未配置并启用WAF防护策略的域名防护，视为“不合规”。	限制网络访问	中	waf:::cloudInstance	不涉及
RGC-GR_CONFIG_WAF_POLICY_ENABLE_GEOIP	如果账号不存在启用地理位置访问控制规则的waf服务防护策略，视为“不合规”。	限制网络访问	中	waf:::policy	不涉及

5.2.3 可选控制策略

*

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_REGULAR_MATCHING_OF_NAMES	资源名称不满足正则表达式，视为“不合规”。	保护配置	低	*	是
RGC-GR_CONFIG_RESOURCE_IN_ENTERPRISE_PROJECT	指定企业项目ID，属于该企业项目的资源，视为“不合规”。	保护配置	低	*	是
RGC-GR_CONFIG_RESOURCES_IN_ALLOWED_TYPES	用户创建指定类型以外的资源，视为“不合规”。	保护配置	低	*	否
RGC-GR_CONFIG_RESOURCES_IN_NOT_ALLOWED_TYPES	用户创建指定类型的资源，视为“不合规”。	保护配置	低	*	否
RGC-GR_CONFIG_RESOURCES_IN_SUPPORTED_REGION	资源不在指定区域内，视为“不合规”。	保护配置	低	*	否

APIG

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
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	不涉及

AS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_AS_CAPACITY_REBALANCING	弹性伸缩组扩缩容时，没有使用‘EQUILIBRIUM_DISTRIBUTE’优先级策略，视为“不合规”。	提高可用性	中	as:::group	不涉及
RGC-GR_CONFIG_AS_GROUP_ELB_HEALTHCHECK_REQUIRED	与负载均衡器关联的伸缩组未使用弹性负载均衡健康检查，视为“不合规”。	提高可用性	低	as:::group	不涉及
RGC-GR_CONFIG_AS_MULTIPLE_AZ	弹性伸缩组没有启用多AZ部署，视为“不合规”。	提高可用性	中	as:::group	不涉及
RGC-GR_CONFIG_AS_GROUP_IPV6_DISABLED	弹性伸缩组绑定IPv6共享带宽，视为“不合规”。	优化成本	低	as:::group	不涉及
RGC-GR_RFS_AS_GROUP_MULTIPLE_AZ_CHECK	要求AS组拥有多个可用区。	提高可用性	中	as:::group	不涉及

CBR

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CBR_POLICY_MINIMUM_FREQUENCY_CHECK	CBR备份策略执行频率低于设定值，视为“不合规”。	为灾难恢复做好准备	中	cbr:::policy	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CBR_VAULT_MINIMUM_RETENTION_CHECK	存储库未绑定策略或绑定的策略按天数保留且保留天数低于设定值，视为“不合规”。	为灾难恢复做好准备	中	cbr:::vault	不涉及

CBR、ECS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_ECS_PROTECTED_BY_CBR	ECS资源没有关联备份存储库，视为“不合规”。	为灾难恢复做好准备	中	ecs:::instanceV1	不涉及
RGC-GR_CONFIG_ECS_LAST_BACKUP_CREATED	ECS云服务器最近一次备份创建时间超过参数要求，视为“不合规”。	为灾难恢复做好准备	低	ecs:::instanceV1	不涉及

CBR、EVS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_EVS_PROTECTED_BY_CBR	EVS磁盘没有关联备份存储库，视为“不合规”。	为灾难恢复做好准备	中	evs:::volume	不涉及
RGC-GR_CONFIG_EVS_LAST_BACKUP_CREATED	EVS磁盘最近一次备份创建时间超过参数要求，视为“不合规”。	为灾难恢复做好准备	低	evs:::volume	不涉及

CBR、SFSturbo

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_SFSTURBO_PROTECTED_BY_CBR	SFSturbo资源没有关联备份存储库，视为“不合规”。	为灾难恢复做好准备	中	sfs:::turbo	不涉及

CCE

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CCE_CLUSTER_END_OF_MAINTENANCE_VERSION	CCE集群版本为停止维护的版本，视为“不合规”。	管理漏洞	中	cce:::cluster	不涉及
RGC-GR_CONFIG_CCE_CLUSTER_OLDEST_SUPPORTED_VERSION	如果CCE集群运行的是受支持的最旧版本（等于参数“最旧版本支持”），视为“不合规”。	管理漏洞	中	cce:::cluster	不涉及
RGC-GR_CONFIG_ALLOWED_CCE_FLAVORS	CCE集群的规格不在指定的范围内，视为“不合规”。	保护配置	低	cce:::cluster	否
RGC-GR_RFS_CCE_SECRETS_ENCRYPTED_CHECK	要求使用密钥管理服务（KMS）密钥为CCE集群配置密钥加密。	加密静态数据	中	cce:::cluster	不涉及

CCM

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_PCA_CERTIFICATE_AUTHORITY_ROOT_DISABLE	私有根CA未停用，视为“不合规”。	管理机密	中	scm:::certificate	不涉及
RGC-GR_CONFIG_PCA_ALGORITHM_CHECK	私有证书管理服务使用了禁止的密钥算法或签名哈希算法，视为“不合规”	加密传输中的数据	高	ccm:::privateCertificate	• blockedKeyAlgorithm：**否** • blockedSignatureAlgorithm：**否**

CES

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_ALARM_ACTION_ENABLED_CHECK	CES告警操作未启用，视为“不合规”。	建立日志记录和监控	中	ces:::alarmRule	不涉及
RGC-GR_CONFIG_ALARM_RESOURCE_CHECK	指定的资源类型没有绑定指定指标CES告警，视为“不合规”	建立日志记录和监控	低	ces:::alarmRule	• provider：**是** • resourceType：**是** • metricName：**是**

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_ALARM_SETTINGS_CHECK	特定指标的CES告警没有进行特定配置，视为“不合规”	建立日志记录和监控	低	ces:::alarmRule	• metricName：是 • threshold：是 • count：是 • period：是 • comparisonOperator：是 • filter：是
RGC-GR_RFS_CES_ALARM_ACTION_CHECK	要求CES警报为警报状态配置操作。	建立日志记录和监控	高	ces:::alarmRule	不涉及
RGC-GR_RFS_CES_ALARM_ACTION_ENABLED_CHECK	要求CES警报激活操作。	建立日志记录和监控	严重	ces:::alarmRule	不涉及

CES、DEW

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_ALARM_KMS_DISABLE_OR_DELETE_KEY	CES未配置监控KMS禁用或计划删除密钥的事件监控告警，视为“不合规”。	建立日志记录和监控	严重	ces:::alarmRule	不涉及

CES、OBS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_ALARM_OBS_BUCKET_POLICY_CHANGE	CES未配置监控OBS桶策略变更的事件监控告警，视为“不合规”。	建立日志记录和监控	严重	ces:::alarmRule	不涉及

CES、VPC

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_ALARM_VPC_CHANGE	CES未配置监控VPC变更的事件监控告警，视为“不合规”。	建立日志记录和监控	高	ces:::alarmRule	不涉及

CFW

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_RFS_CFW_POLICY_RULE_GROUP_ASSOCIATED_CHECK	要求任何Cloud Firewall防火墙策略具有关联的规则组。	限制网络访问	中	cfw:::aclRule	不涉及

CodeArts Deploy

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CODEARTSDEPLOY_HOST_CLUSTER_RESOURCE_STATUS	CodeArts项目下的主机集群，如果状态不可用，则该主机集群视为“不合规”。	提高可用性	低	codeartsDeploy:::host	不涉及

Config

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_TRACKER_CONFIG_ENABLED_CHECK	如果账号未开启资源记录器，视为“不合规”。	建立日志记录和监控	中	rms:::resourceRecorder	不涉及

CSS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CSS_CLUSTER_BACKUP_AVAILABLE	CSS集群未启用快照，视为“不合规”。	提高韧性	中	css:::cluster	不涉及
RGC-GR_CONFIG_CSS_CLUSTER_MULTIPLE_AZ_CHECK	CSS集群没有多AZ容灾，视为“不合规”。	提高可用性	中	css:::cluster	不涉及
RGC-GR_CONFIG_CSS_CLUSTER_MULTIPLE_INSTANCES_CHECK	CSS集群没有多实例容灾，视为“不合规”。	提高可用性	中	css:::cluster	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CSS_CLUSTER_IN_VPC	CSS集群未与指定的VPC资源绑定，视为“不合规”。	限制网络访问	严重	css:::cluster	否
RGC-GR_CONFIG_CSS_CLUSTER_SLOWLOG_ENABLE	CSS集群未开启慢日志，视为“不合规”。	建立日志记录和监控	中	css:::cluster	不涉及

CTS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
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	否
RGC-GR_CONFIG_CTS_OBS_BUCKET_TRACK	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”。	建立日志记录和监控	高	cts:::tracker	是
RGC-GR_CONFIG_CTS_TRACKER_ENABLED_SECURITY	不存在满足安全最佳实践的CTS追踪器，视为“不合规”。	建立日志记录和监控	高	cts:::tracker	否
RGC-GR_RFS_CTS_LOG_FILE_VALIDATION_ENABLED_CHECK	要求CTS追踪器激活日志文件验证。	保护数据完整性	高	cts:::tracker	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_RFS_CTS_LOGS_ENABLED_CHECK	要求CTS追踪器具有LTS日志组配置。	建立日志记录和监控	低	cts:::tracker	不涉及

DDS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_DDS_INSTANCE_HAMODE	指定实例类型，不属于此的DDS实例资源，视为“不合规”。	保护配置	低	dds:::instance	否
RGC-GR_CONFIG_DDS_INSTANCE_ENGINE_VERSION_CHECK	低于指定版本的DDS实例，视为“不合规”。	管理漏洞	低	dds:::instance	否
RGC-GR_RFS_DDS_INSTANCE_ENCRYPTED_CHECK	要求对DDS实例进行静态加密。	加密静态数据	中	dds:::instance	不涉及

DEW

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_RFS_DEW_KEY_ROTATION_ENABLED_CHECK	要求任何KMS密钥配置轮换。	加密静态数据	中	kms:::key	不涉及
RGC-GR_CONFIG_CSMS_SECRETS_AUTO_ROTATION_ENABLED	CSMS凭据未启动自动轮转，视为“不合规”。	管理机密	中	csms:::secret	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_CSMS_SECRETS_PERIODIC_ROTATION	CSMS凭据未在指定天数内轮转，视为“不合规”。	管理机密	中	csms:::secret	不涉及
RGC-GR_CONFIG_CSMS_SECRETS_USING_CMK	CSMS凭据未使用指定的KMS，视为“不合规”。	加密静态数据	高	csms:::secret	否

DMS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_RFS_KAFKA_MULTIPLE_AZ_CHECK	要求Kafka实例配置多个可用区以实现高可用性。	提高可用性	低	dms:::kafkaInstance	不涉及
RGC-GR_RFS_ROCKETMQ_MULTIPLE_AZ_CHECK	要求RocketMQ实例配置多个可用区以实现高可用性。	提高可用性	低	dms:::rocketmqInstance	不涉及
RGC-GR_RFS_RABBITMQ_MULTIPLE_AZ_CHECK	要求RabbitMQ实例配置多个可用区以实现高可用性。	提高可用性	低	dms:::rabbitmqInstance	不涉及
RGC-GR_RFS_KAFKA_INSTANCE_TLS_CHECK	要求Kafka实例需要为支持的引擎类型提供传输层安全性协议（TLS）连接。	加密传输中的数据	中	dms:::kafkaInstance	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_RFS_RABBITMQ_INSTANCE_TLS_CHECK	要求RabbitMQ实例需要为支持的引擎类型提供传输层安全性协议（TLS）连接。	加密传输中的数据	中	dms:::rabbitmqInstance	不涉及
RGC-GR_RFS_ROCKETMQ_INSTANCE_TLS_CHECK	要求RocketMQ实例需要为支持的引擎类型提供传输层安全性协议（TLS）连接。	加密传输中的数据	中	dms:::rocketmqInstance	不涉及
RGC-GR_RFS_RABBITMQ_DLQ_CHECK	要求任何RabbitMQ队列配置死信队列。	提高韧性	高	dms:::rabbitmqInstance	不涉及

DWS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_DWS_ENABLE_SNAPSHOT	DWS集群未启用自动快照，视为“不合规”。	提高韧性	中	dws:::cluster	不涉及
RGC-GR_CONFIG_DWS_MAINTAIN_WINDOW_CHECK	DWS集群运维时间窗不满足配置，视为“不合规”。	为事件响应做好准备	中	dws:::cluster	不涉及
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	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_RFS_DWS_CLUSTER_ENCRYPTION_ENABLED_CHECK	要求对所有DWS集群进行静态加密。	加密静态数据	中	dws:::cluster	不涉及

ECS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_ALLOWED_ECS_FLAVORS	ECS资源的规格不在指定的范围内，视为“不合规”。	保护配置	低	ecs:::instanceV1	否
RGC-GR_CONFIG_ALLOWED_IMAGES_BY_NAME	指定允许的镜像名称列表，ECS实例的镜像名称不在指定的范围内，视为“不合规”。	管理漏洞	高	ecs:::instanceV1	是
RGC-GR_CONFIG_STOPPED_ECS_DATE_DIFF	关机状态的ECS未进行任意操作的时间超过了允许的天数，视为“不合规”。	优化成本	中	ecs:::instanceV1ecs:::instanceV1	是
RGC-GR_CONFIG_ECS_ATTACHED_HSS_AGENTS_CHECK	ECS实例未绑定HSS代理并启用防护，视为“不合规”。	管理漏洞	中	ecs:::instanceV1	不涉及

ECS、IMS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_ALLOWED_IMAGES_BY_ID	指定允许的镜像ID列表，ECS实例的镜像ID不在指定的范围内，视为“不合规”。	管理漏洞	高	ecs:::instanceV1	否
RGC-GR_CONFIG_APPROVED_IMS_BY_TAG	ECS的镜像不在指定tag的IMS的范围内，视为“不合规”。	管理漏洞	中	ecs:::instanceV1	• specifiedIMSTagKey：是 • specifiedIMSTagValue：否

EIP

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_EIP_USE_IN_SPECIFIED_DAYS	创建的EIP在指定天数后仍未绑定到资源实例，视为“不合规”。	优化成本	中	vpc:::eipAssociate	不涉及

ELB

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_ELB_MULTIPLE_AZ_CHECK	检查负载均衡器是否已从多个可用分区注册实例。如果负载均衡器的实例注册在少于2个可用区，视为“不合规”。	弹性负载均衡	中	elb:::loadbalancer	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_ELB_MEMBERS_WEIGHT_CHECK	后端服务器的权重为0，且其所属的后端服务器组的负载均衡算法不为“SOURCE_IP”时，视为“不合规”。	提高可用性	低	elb:::member	不涉及
RGC-GR_RFS_ELB_PREDEFINED_SECURITY_POLICY_CHECK	要求任何独享型ELB负载均衡器HTTPS侦听器具有一个拥有强配置的预定义安全策略。	限制网络访问	中	elb:::listener	不涉及
RGC-GR_RFS_LB_TLS_HTTPS_LISTENERS_ONLY_CHECK	要求为私网类型的ELB负载均衡器侦听器配置HTTPS终止。	加密传输中的数据	中	lb:::listener	不涉及
RGC-GR_RFS_ELB_TLS_HTTPS_LISTENERS_ONLY_CHECK	要求为独享型ELB应用程序或经典负载均衡器侦听器配置HTTPS终止。	加密传输中的数据	中	elb:::listener	不涉及
RGC-GR_RFS_ELB_DELETION_PROTECTION_ENABLED_CHECK	要求激活应用程序负载均衡器删除保护。	提高可用性	中	elb:::loadbalancer	不涉及
RGC-GR_RFS_ELB_MULTIPLE_AZ_CHECK	要求任何经典负载均衡器配置多个可用区。	提高可用性	中	elb:::loadbalancer	不涉及

ER

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_RFS_ER_INSTANCE_AUTO_VPC_ATTACH_DISABLED_CHECK	要求企业路由器拒绝自动接受共享连接创建。	限制网络访问	高	er:::instance	不涉及

EVS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_EVS_USE_IN_SPECIFIED_DAYS	创建的EVS在指定天数后仍未绑定到资源实例，视为“不合规”。	优化成本	中	evs:::volume	不涉及
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	不涉及
RGC-GR_CONFIG_ALLOWED_VOLUME_SPECS	指定允许的云硬盘类型列表，云硬盘的类型不在指定的范围内，视为“不合规”。	保护配置	低	evs:::volume	否
RGC-GR_EVS_ALL_OPERATION_PROHIBITED	不允许调用EVS的API。	保护配置	严重	evs:::volume	不涉及
RGC-GR_ECS_ATTACH_NO_ENCRYPTED_EVS_PROHIBITED	不允许对云服务器挂载一个未加密的云硬盘。	保护配置	严重	evs:::volume	不涉及

FunctionGraph

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_FUNCTION_GRAPH_CONCURRENCY_CHECK	FunctionGraph函数并发数不在指定的范围内，视为“不合规”。	提高可用性	中	fgs:::function	不涉及
RGC-GR_CONFIG_FUNCTION_GRAPH_INSIDE_VPC	函数工作流未使用指定VPC，视为“不合规”	限制网络访问	低	fgs:::function	否
RGC-GR_CONFIG_FUNCTION_GRAPH_SETTINGS_CHECK	函数工作流的运行时、超时时间、内存限制不在指定范围内，视为“不合规”	管理漏洞	中	fgs:::function	否
RGC-GR_CONFIG_FUNCTION_GRAPH_LOGGING_ENABLED	函数工作流的函数未启用日志配置，视为“不合规”。	建立日志记录和监控	中	fgs:::function	不涉及

GaussDB

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_GAUSSDB_INSTANCE_ENABLE_AUDITLOG	未开启审计日志的GaussDB资源，视为“不合规”。	建立日志记录和监控	中	gaussdb:::opengaussInstance	不涉及
RGC-GR_CONFIG_GAUSSDB_INSTANCE_ENABLE_BACKUP	未开启资源备份的GaussDB资源，视为“不合规”。	提高韧性	中	gaussdb:::opengaussInstance	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_GAUSSDB_INSTANCE_ENABLE_ERRORLOG	未开启错误日志的GaussDB资源，视为“不合规”。	建立日志记录和监控	低	gaussdb:::opengaussInstance	不涉及
RGC-GR_CONFIG_GAUSSDB_INSTANCE_ENABLE_SLOWLOG	未开启慢日志的GaussDB资源，视为“不合规”。	建立日志记录和监控	低	gaussdb:::opengaussInstance	不涉及
RGC-GR_CONFIG_GAUSSDB_INSTANCE_MULTIPLE_AZ_CHECK	GaussDB资源未跨AZ部署，视为“不合规”。	提高可用性	中	gaussdb:::opengaussInstance	不涉及

GeminiDB

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_GAUSSDB_NOSQL_DEPLOY_IN_SINGLE_AZ	GeminiDB部署在单个可用区中，视为“不合规”	提高可用性	中	gaussdb:::mongoInstance	不涉及
RGC-GR_CONFIG_GAUSSDB_NOSQL_ENABLE_BACKUP	GeminiDB未开启备份，视为“不合规”	提高韧性	中	gaussdb:::mongoInstance	不涉及
RGC-GR_CONFIG_GAUSSDB_NOSQL_ENABLE_ERROR_LOG	GeminiDB未开启错误日志，视为“不合规”。	建立日志记录和监控	低	gaussdb:::mongoInstance	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_GAUSSDB_NOSQL_SUPPORT_SLOW_LOG	GeminiDB不支持慢查询日志，视为“不合规”。	建立日志记录和监控	低	gaussdb:::mongoInstance	不涉及
RGC-GR_RFS_GAUSSDB_MONGO_INSTANCE_TLS_CHECK	要求GaussDB Mongo实例需要为支持的引擎类型提供传输层安全性协议（TLS）连接。	加密传输中的数据	中	gaussdb:::mongoInstance	不涉及
RGC-GR_RFS_GAUSSDB_MONGO_INSTANCE_AUTO_BACKUP_CHECK	要求GaussDB Mongo实例配置自动备份。	提高韧性	中	gaussdb:::mongoInstance	不涉及
RGC-GR_RFS_GAUSSDB_REDIS_INSTANCE_AUTO_BACKUP_CHECK	要求GaussDB Redis实例配置自动备份。	提高韧性	中	gaussdb:::redisInstance	不涉及
RGC-GR_RFS_GAUSSDB_REDIS_INSTANCE_TLS_CHECK	要求GaussDB Redis实例需要为支持的引擎类型提供传输层安全性协议（TLS）连接。	加密传输中的数据	中	gaussdb:::redisInstance	不涉及

GES

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_GES_GRAPHS_LTS_ENABLE	GES图未开启LTS日志，视为“不合规”。	建立日志记录和监控	中	ges:::graph	不涉及
RGC-GR_CONFIG_GES_GRAPHS_MULTI_AZ_SUPPORT	GES图不支持跨AZ高可用，视为“不合规”。	提高可用性	中	ges:::graph	不涉及

IAM

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS	IAM策略中授权KMS的任一阻拦action，视为“不合规”。	强制执行最低权限	中	• identity:::role • identity:::protectionPolicy	不涉及
RGC-GR_CONFIG_IAM_USER_CHECK_NON_ADMIN_GROUP	根用户以外的IAM用户加入admin用户组，视为“不合规”。	强制执行最低权限	低	identity:::user	不涉及
RGC-GR_CONFIG_IAM_USER_NO_POLICIES_CHECK	IAM用户直接附加了策略或权限，视为“不合规”。	强制执行最低权限	低	identity:::user	不涉及

LTS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_RFS_LTS_GROUP_RETENTION_PERIOD_CHECK	要求将LTS日志组保留至少180天。	建立日志记录和监控	中	lts:::group	不涉及

MRS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_MRS_CLUSTER_MULTIAZ_DEPLOYMENT	MRS集群没有多az部署，视为“不合规”。	提高可用性	中	mrs:::cluster	不涉及
RGC-GR_CONFIG_MRS_CLUSTER_ENCRYPT_ENABLE	KMS密钥不处于“计划删除”状态。	保护数据完整性	中	mrs:::cluster	不涉及

Network、ACL

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_RFS_NACL_NO_UNRESTRICTED_SSH_RDP_CHECK	要求任何网络ACL防止从0.0.0.0/0进入端口22或端口3389。	限制网络访问	中	network:::aclRule	不涉及

RDS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_RDS_INSTANCE_ENABLE_BACKUP	未开启备份的rds资源，视为“不合规”。	提高韧性	中	rds:::instance	不涉及
RGC-GR_CONFIG_RDS_INSTANCE_ENABLE_ERRORLOG	未开启错误日志的rds资源，视为“不合规”。	建立日志记录和监控	低	rds:::instance	不涉及
RGC-GR_CONFIG_RDS_INSTANCE_ENABLE_SLOWLOG	未开启慢日志的rds资源，视为“不合规”。	建立日志记录和监控	低	rds:::instance	不涉及
RGC-GR_CONFIG_RDS_INSTANCE_LOGGING_ENABLED	未配备任何日志的rds资源，视为“不合规”。	建立日志记录和监控	中	rds:::instance	不涉及
RGC-GR_CONFIG_RDS_INSTANCE_MULTI_AZ_SUPPORT	RDS实例仅支持一个可用区，视为“不合规”。	提高可用性	中	rds:::instance	不涉及
RGC-GR_CONFIG_ALLOWED_RDS_FLAVORS	RDS实例的规格不在指定的范围内，视为“不合规”。	保护配置	低	rds:::instance	不涉及
RGC-GR_CONFIG_RDS_INSTANCES_IN_VPC	指定虚拟私有云ID，不属于此VPC的rds资源，视为“不合规”。	限制网络访问	高	rds:::instance	否
RGC-GR_CONFIG_RDS_INSTANCE_ENABLE_AUDITLOG	未启用审计日志或者审计日志保存天数不足的rds资源，视为“不合规”。	建立日志记录和监控	中	rds:::instance	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_RDS_INSTANCE_ENGINE_VERSION_CHECK	RDS实例数据库引擎的版本低于指定版本，视为“不合规”。	管理漏洞	低	rds:::instance	• postgresqlVersion：否 • mariadbVersion：否 • mysqlVersion：否 • sqlserverVersion：否
RGC-GR_RFS_RDS_INSTANCE_DEPLOYED_IN_VPC_CHECK	要求RDS数据库实例具有VPC配置。	限制网络访问	高	rds:::instance	不涉及
RGC-GR_RFS_RDS_DB_SECURITY_GROUP_NOT_ALLOWED_CHECK	要求RDS实例配置数据库安全组。	限制网络访问	中	rds:::instance	不涉及
RGC-GR_RFS_RDS_INSTANCE_MULTIPLE_AZ_CHECK	要求为RDS实例配置多个可用区以实现高可用性。	提高可用性	中	rds:::instance	不涉及
RGC-GR_RFS_RDS_INSTANCE_TLS_CHECK	要求RDS实例需要为支持的引擎类型提供传输层安全性协议（TLS）连接。	加密传输中的数据	中	rds:::instance	不涉及
RGC-GR_RFS_RDS_INSTANCE_BACKUP_ENABLED_CHECK	要求RDS实例配置自动备份	提高韧性	中	rds:::instance	不涉及

OBS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_RFS_OBS_BUCKET_DEFAULT_ENCRYPTION_KMS_CHECK	要求OBS存储桶使用KMS密钥配置服务器端加密。	加密静态数据	中	obs:::bucket	不涉及
RGC-GR_RFS_OBS_BUCKET_VERSIONING_ENABLED_CHECK	要求OBS存储桶启用版本控制。	提高可用性	低	obs:::bucket	不涉及
RGC-GR_RFS_OBS_BUCKET_LOGGING_ENABLED_CHECK	要求OBS存储桶配置服务器访问日志记录。	建立日志记录和监控	中	obs:::bucket	不涉及

OBS、Access Analyzer

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_OBS_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED	OBS桶策略中授权任意禁止的action给外部身份，视为“不合规”。	强制执行最低权限	高	obs:::bucket	否
RGC-GR_CONFIG_OBS_BUCKET_SSL_REQUESTS_ONLY	OBS桶策略授权了无需SSL加密的行为，视为“不合规”。	加密传输中的数据	中	obs:::bucket	不涉及

Organizations

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_ACCOUNT_PART_OF_ORGANIZATIONS	账号未加入组织中，视为“不合规”。	强制执行最低权限	高	organizations:::accountAssociate	否

SFS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_RFS_SFS_ENCRYPTED_CHECK	要求SFS文件系统使用KMS对文件数据进行静态加密。	加密静态数据	中	sfs:::fileSystem	不涉及

SMN

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
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	不涉及

SWR

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_RFS_SWR_PRIVATE_IMAGE_CHECK	要求SWR为私有存储库。	管理漏洞	高	swr:::repository	不涉及

TMS

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_REQUIRED_ALL_TAGS	指定标签列表，不具有所有指定标签键的资源，视为“不合规”。	保护配置	低	tms:::resourceTags	• TagKeys：是 • TagValues：否
RGC-GR_CONFIG_REQUIRED_TAG_CHECK	指定一个标签，不具有此标签的资源，视为“不合规”。	保护配置	低	tms:::resourceTags	• specifiedTagKey：是 • specifiedTagValue：否
RGC-GR_CONFIG_REQUIRED_TAG_EXIST	指定标签列表，不具有任一指定标签的资源，视为“不合规”。	保护配置	低	tms:::resourceTags	• TagKeys：是 • TagValues：否
RGC-GR_CONFIG_RESOURCE_TAG_KEY_PREFIX_SUFFIX	指定前缀和后缀，资源不具有任意匹配前后缀的标签键，视为“不合规”。	保护配置	低	tms:::resourceTags	• tagKeyPrefix：否 • tagKeySuffix：否
RGC-GR_CONFIG_RESOURCE_TAG_NOT_EMPTY	资源未配置标签，视为“不合规”。	保护配置	低	tms:::resourceTags	不涉及

TaurusDB

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_ENABLE_AUDITLOG	未开启审计日志的TaurusDB资源，视为“不合规”。	建立日志记录和监控	中	gaussdb:::mysqlInstance	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_ENABLE_BACKUP	未开启备份的TaurusDB资源，视为“不合规”。	提高韧性	中	gaussdb:::mysqlInstance	不涉及
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_ENABLE_ERORLOG	未开启错误日志的TaurusDB资源，视为“不合规”。	建立日志记录和监控	低	gaussdb:::mysqlInstance	不涉及
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_ENABLE_SLOWLOG	未开启慢日志的TaurusDB资源，视为“不合规”。	建立日志记录和监控	低	gaussdb:::mysqlInstance	不涉及
RGC-GR_CONFIG_GAUSSDB_MYSQL_INSTANCE_MULTIPLE_AZ_CHECK	TaurusDB实例未跨AZ部署，视为“不合规”。	提高可用性	中	gaussdb:::mysqlInstance	不涉及

VPC

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_EIP_UNBOUND_CHECK	弹性公网IP未进行任何绑定，视为“不合规”。	优化成本	中	vpc:::eipAssociate	不涉及

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
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	不涉及
RGC-GR_CONFIG_EIP_BANDWIDTH_LIMIT	弹性公网IP可用带宽小于指定参数值，视为“不合规”	提高可用性	中	vpc:::eip	是
RGC-GR_RFS_VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS_CHECK	要求任何VPC安全组规则不将源IP范围0.0.0.0/0或::/0用于80和443以外的端口。	限制网络访问	高	networking:::secgroupRule	不涉及
RGC-GR_RFS_VPC_SG_RESTRICTED_COMMON_PORTS_CHECK	要求任何VPC安全组规则不将源IP范围0.0.0.0/0或::/0用于特定的高风险端口。	限制网络访问	严重	networking:::secgroupRule	不涉及

VPCEP

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_VPCEP_ENDPOINT_ENABLED	检查账号下是否存在指定服务名的终端节点，如果不存在任何一个，视为“不合规”。	限制网络访问	中	vpcep:::endpoint	是

VPN

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_CONFIG_VPN_CONNECTIONS_ACTIVE	VPN连接状态不为“正常”，视为“不合规”。	提高可用性	中	vpnaas:::siteConnectionV2	不涉及
RGC-GR_VPN_CONNECTION_PROHIBITED	不允许订阅虚拟专用网络。	保护配置	严重	• vpn:::connection • vpn:::gateway • vpn:::customerGateway	不涉及

WAF

控制策略名称	功能	场景	严重程度	资源	规则参数是否必填
RGC-GR_RFS_WAF_GLOBAL_ACL_NOT_EMPTY_CHECK	要求任何WAF全局ACL拥有规则。	限制网络访问	中	waf:::ruleGlobalProtectionWhitelist	不涉及
RGC-GR_RFS_WAF_RULEGROUP_NOT_EMPTY_CHECK	要求WAF规则组为非空。	限制网络访问	中	waf:::addressGroup	不涉及

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。

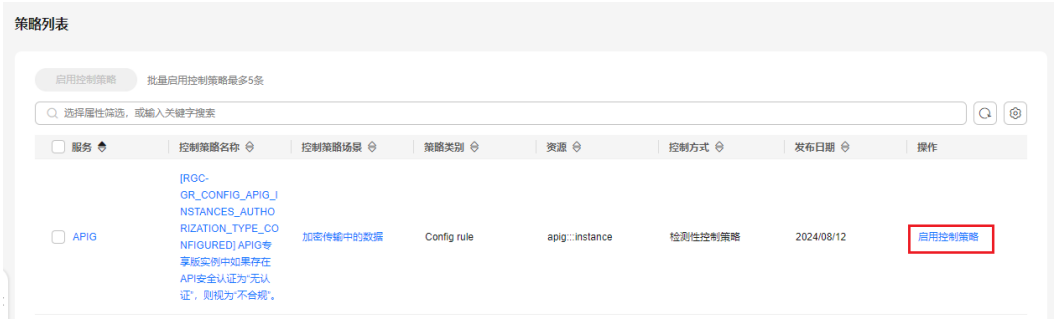
启用控制策略

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。

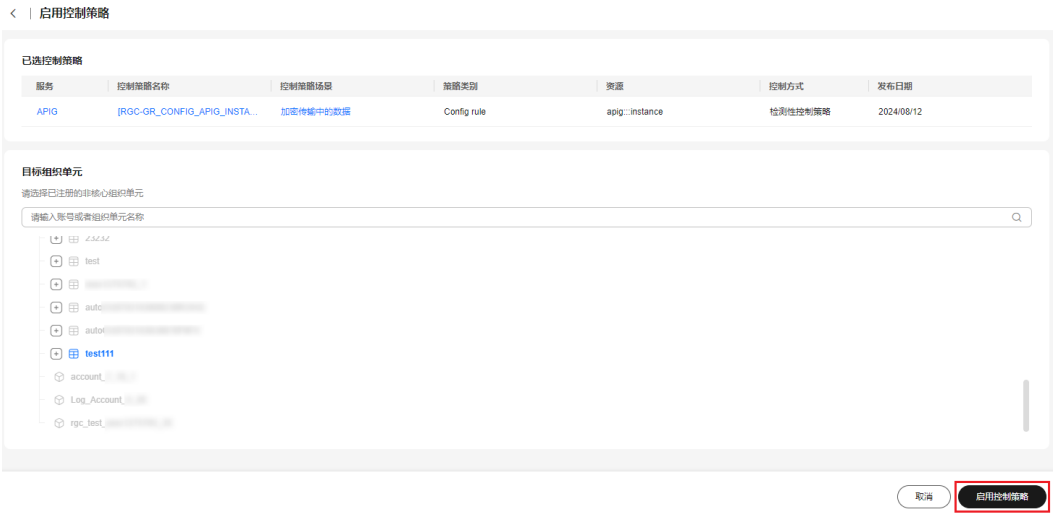
步骤3 单击“操作”列下的“启用控制策略”。

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

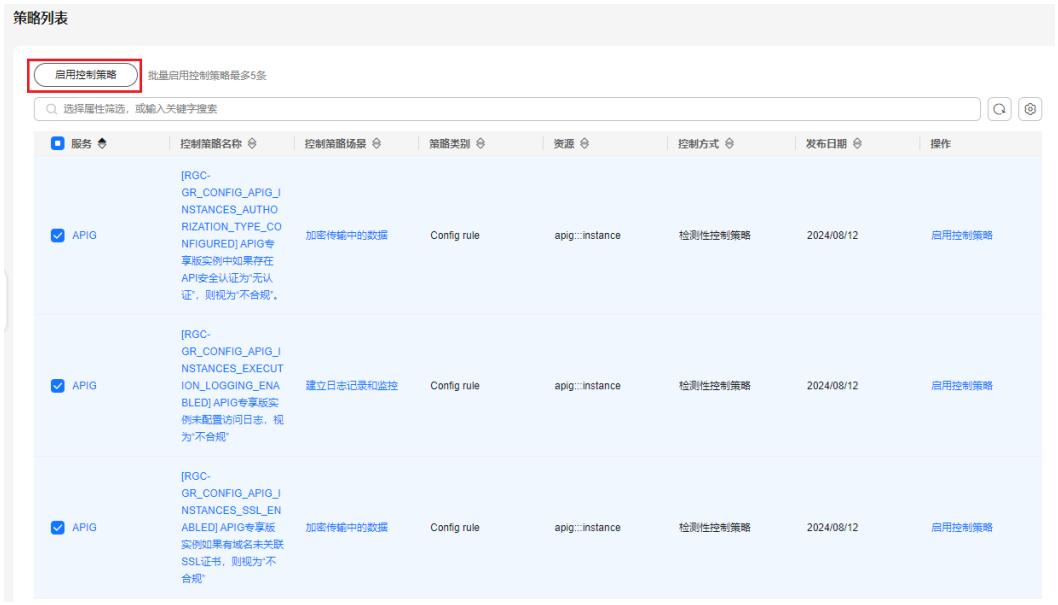
单次仅支持批量开启5条控制策略。

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。

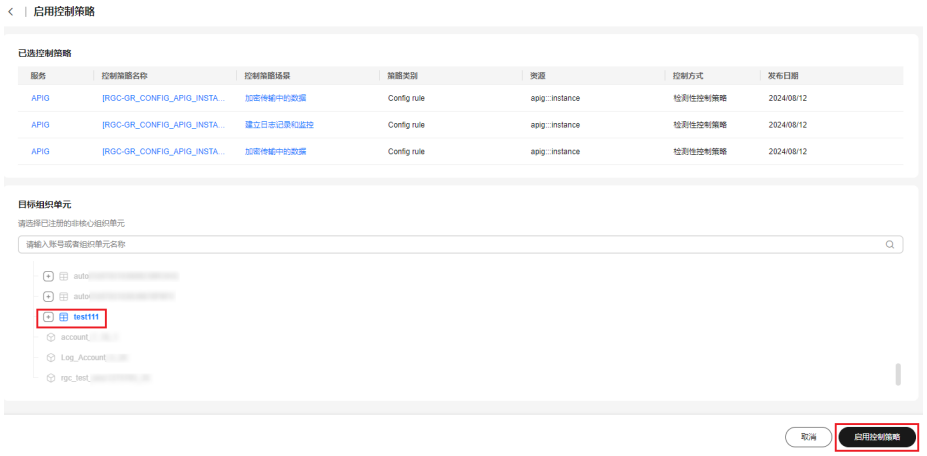
步骤3 单击列表上方的“启用控制策略”。

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。

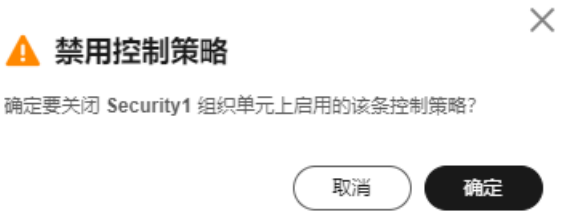
步骤4 在“已启用组织单元”的页签中，找到需要解绑的组织单元。

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。
资源	受到监管的资源。
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。

参数	描述
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。
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。
策略类别	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

6 漂移检测与修复

漂移概述

搭建Landing Zone时，账号、所有OU和资源都将符合控制策略管控下的管理规则。当您和组织成员使用Landing Zone时，由于可以同时从RGC和Organizations服务对组织和SCP进行操作，操作入口的不唯一就可能导致纳管资源的合规状态发生改变。当RGC纳管的资源不满足治理策略时，就会发生以下两类漂移现象：

- SCP：

  RGC为各个OU配置的SCP与在Organizations服务中内容不一致，或者SCP在Organizations服务中不存在。
- 组织结构

  RGC监管的OU和账号与Organizations服务里的OU或账号存在不一致。

当存在不一致时，意味着当前Landing zone环境发生了不合规情况，可能会造成意外甚至严重的后果。

当前RGC已支持定期进行账号、OU和SCP的漂移检测，并使用告警提醒您存在漂移现象。检测漂移后，您可以通过更新、修复等操作消除漂移。

当核心OU或核心账号存在漂移时，RGC的创建账号功能将无法使用。

漂移检测概述

RGC会自动检测是否存在漂移现象。检测漂移将需要RGCServiceExecutionAgency服务委托持续访问您的管理账号，RGC将会使用只读权限的API调用Organizations服务。调用API的操作将会记录在CTS事件中。

漂移现象的消息将汇总至消息通知服务（Simple Message Notification，SMN）中。管理账号可以**订阅SMN消息通知**，以便在出现漂移现象时，接收漂移信息并及时修复漂移。在RGC中可以检测到的治理漂移类型如下：

- 组织架构漂移的类型
  - SCP被更新
  - SCP被删除
  - SCP关联至OU
  - SCP关联至账号
  - SCP从OU解绑

  - SCP从账号解绑
- 账号漂移的类型
  - 账号被移动到其他OU
  - 账号被关闭
  - 账号被移出组织

说明

- 如果同一组资源多次出现相同类型的漂移，RGC将仅针对第一个出现漂移的资源发送SMN通知。
- 如果RGC检测到发生漂移的资源已得到修复，则仅当相同的资源再次出现漂移时，才会再次发送SMN通知。

例如：

- 如果您多次修改同一个SCP的策略内容，则仅在首次修改时会收到消息通知。
- 如果您通过修改SCP后修复了漂移，然后再次对其进行修改再次产生漂移，则您将会收到两条消息通知。

需要立即修复的漂移类型

当出现漂移现象时，您可以通过更新/修复等操作消除漂移，以确保Landing Zone处于合规的状态。漂移检测是系统自动进行的，但您需要在RGC控制台进行操作才可以修复漂移。

大多数类型的漂移可以由管理员解决，但有些类型的漂移则必须立即解决，包括删除RGC Landing zone所需的OU等。以下列举的是如何避免产生立即解决的漂移示例：

- 不要删除核心OU：不应在Organizations服务中删除RGC在搭建Landing Zone期间默认名为 “Security” 的核心OU。如果将其删除，则会出现漂移现象。您将会在RGC控制台看到一条错误消息，提示您立即更新/修复Landing Zone。在更新/修复完成之前，您将无法在RGC中执行任何其他操作。
- 不要删除核心账号：如果您从核心OU中删除核心账号，例如从核心OU中删除日志存档账号，则Landing Zone将处于漂移状态。您必须先更新/修复Landing Zone，然后才能继续使用RGC控制台。

修复漂移问题

当发生漂移时，您将会在RGC控制台看到一条错误消息，提示您立即更新/修复Landing Zone。您仅需根据提示，单击提示中的“更新/修复”或“重新注册OU”等，进行漂移问题修复。

如您已执行修复操作，但仍未解决漂移问题，建议您**提交工单**进行技术支持咨询。

7 使用 CTS 审计 RGC 操作事件

操作场景

资源治理中心支持通过云审计服务对资源治理中心的操作进行记录，以便查询事件列表，用以审计和回溯历史操作。

前提条件

已开通CTS。

支持审计的关键操作列表

表 7-1 云审计服务支持的 RGC 操作列表

操作名称	资源类型	事件名称
设置Landing Zone前检查	LandingZone	checkLaunch
删除Landing Zone	LandingZone	deleteLandingZone
设置Landing Zone	LandingZone	setupLandingZone
关闭控制策略	Control	DisableGovernancePolicy
开启控制策略	Control	EnableGovernancePolicy
创建账号	Account	createAccount
纳管账号	Account	enrollAccount
取消纳管账号	Account	unEnrollAccount
更新被管理账号	Account	updateManagedAccount
创建组织单元	OrganizationUnit	createManagedOrganizationalUnit
删除组织单元	OrganizationUnit	deleteManagedOrganizationalUnits

操作名称	资源类型	事件名称
重新注册组织单元	OrganizationUnit	reRegisterOrganizationalUnit
注册组织单元	OrganizationUnit	registerOrganizationalUnit
取消注册组织单元	OrganizationUnit	deregisterOrganizationalUnit
创建一个模板	Template	createTemplate
删除一个模板	Template	deleteTemplate

查看审计日志

如何查看审计日志，请参考**查询审计事件**。