资源治理中心

产品介绍

文档版本 01

发布日期 2024-01-30

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 什么是资源治理中心

资源治理中心（Resource Governance Center，简称RGC）服务为用户提供搭建安全、可扩展的多账号环境并持续治理的能力。

- 您可以通过RGC服务快速自动搭建Landing Zone基础多账号环境并纳管您现有的组织架构，实现业务快速上云。
- 您可以在搭建好的Landing Zone基础环境（以下简称Landing Zone）上设置控制策略，帮助您更快速便捷地满足云上合规诉求，而且通过RGC看板持续监控云上多账号环境的合规状态，管理控制策略启用情况并查看不合规资源详情。
- 您可以使用定义好的**IaC（Infrastructure as Code）**模板，快速创建账号，保证账号资源配置一致性的同时，实现新业务应用的快速部署上线。

2 应用场景

资源治理中心可以帮助您快速搭建和治理云上多账号环境。资源治理中心可以应用于以下场景：

自动部署 Landing Zone 多账号环境

为保障企业业务安全地，便捷地迁移上云，首先需要在云上提供一个安全、可扩展的多账号环境。通过资源治理中心自动在华为云上部署Landing Zone环境，加速企业上云。

预防并检测组织内成员不合规行为

企业上云对云上合规治理要求较高，每个企业均会有云上治理红线需要组织内所有成员遵从，资源治理中心提供场景化合规控制策略包，供企业灵活选用，快速部署，满足企业内部合规管控诉求。

图 2-1 预防并检测组织内成员不合规行为

新业务应用的快速部署上线

企业拥有多个业务模块和应用，在部署完Landing Zone多账号环境之后，用户即可搬迁应用上云，用户可以预先定义好新建账号的标准配置，通过RGC服务简单快速创建及配置新建账号，助力应用快速搬迁上线。

3 产品功能

在使用资源治理中心RGC之前，建议您先通过基本概念介绍了解账号工厂、控制策略等基本概念，以便更好地理解资源治理中心RGC提供的功能。

基础环境自动部署

用户可以通过RGC服务自动部署的符合最佳实践的Landing Zone多账号环境，它有管理账号和两个核心成员账号（审计账号和日志账号）。该环境同时提供了组织级的统一登录、集中日志和审计能力等。

账号工厂

用户可以直接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。

控制策略

用户可以灵活选用场景化的合规控制策略包，启用预防性和检测性的控制策略，满足企业合规要求。

预防控制策略

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。

检测控制策略

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。

账号自定义部署

提供灵活的账号自定义框架，创建新的成员账号之时或者直接选中已创建的成员账号，选用自定义IaC模板实现账号内部配置的自定义部署。

看板

用户可以实时查看控制策略启用情况，组织级别资源合规情况以及组织架构等，监控云上Landing Zone多账号环境合规状态。

4 约束与限制

使用约束

- 组织相关的约束限制，请参考**约束与限制**。
- 一个组织管理员账号仅允许在一个主区域开通RGC。

5 基本概念

IaC

基础设施即代码（Infrastructure as Code，简称IaC）是指使用代码而非手动交互方式来配置和管理计算基础设施的能力。

Landing Zone

Landing Zone基础环境简称，指由RGC初始部署的符合最佳实践的多账号环境。

账号

账号是租户间的安全边界，是资源隔离的基本单元。一个账号内的资源只能被授权给该账号下的IAM用户（或IAM委托）所访问。当前账号的承载实体是华为云账号。

管理账号

当一个账号启用Organizations服务之后，该账号被称为管理账号。

管理账号一般用于企业云上多账号资源架构的创建管理，以及组织级策略的管理。

成员账号

当启用Organizations服务后，通过Organizations服务所创建（或邀请加入）的账号称为成员账号。

成员账号一般用于业务或应用资源的部署及管理。

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（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，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。

根组织单元

当您开通Organizations云服务并创建组织后，系统会为您自动生成根组织单元。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。

组织单元

组织单元（Organizational Unit，OU）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。

多账号环境

多账号环境是一种适用于组织或企业的云上架构模式。它由一个管理账号和若干成员账号组成。

最佳实践

最佳实践是已被证明的能够带来良好结果的架构、流程或方法。在RGC中，是指安全、可扩展的多账号环境及一系列云服务配置。

基础环境

由RGC初始部署的符合最佳实践的多账号环境，它有管理账号和两个成员账号（审计账号和日志账号）。该环境同时提供了组织级的统一登录、集中日志和审计能力。

账号纳管

未通过RGC创建的账号由RGC接管的过程。账号纳管后，RGC会将最佳实践配置到该账号上。

模板

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。

控制策略

为持续治理云上多账号环境而提供的预定义规则。

6 修订记录

时间	修订记录
2023-12-22	第一次正式发布。