资源访问管理

产品介绍

文档版本 01

发布日期 2024-12-05

华为技术有限公司

版权所有 © 华为技术有限公司 2024。 保留一切权利。

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

商标声明


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。

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

 版权所有 © 华为技术有限公司

目 录

 版权所有 © 华为技术有限公司

1 什么是资源访问管理

简介

资源访问管理（Resource Access Manager，简称RAM）服务为用户提供安全的跨账号共享资源的能力。如果您有多个华为云账号，您可以创建一次资源，并使用RAM服务将该资源共享给其他账号使用，这样您就不需要在每个账号中创建重复的资源。支持共享的云服务和资源类型请参见：**支持共享的云服务和资源类型**。

如果您的账号由**组织**管理，则您可以直接与组织、OU或成员账号共享资源，还可以输入账号ID与账号共享，无论账号是否属于组织。

产品功能

资源共享管理

使用RAM服务，资源所有者可以集中管理资源的共享。资源所有者可以将指定资源共享给指定对象（包括组织、OU以及账号），资源所有者还可以随时更新或删除资源共享实例。

资源使用者可以接受或拒绝共享邀请，查看当前正在使用的共享信息，以及在共享资源使用结束后退出共享。

共享信息查询

资源所有者可以查询当前已经共享的资源信息，以及资源使用者的相关信息。

资源使用者可以查询当前正在使用的共享资源信息，以及资源所有者信息。

与组织共享资源

RAM启用与组织共享资源功能后，资源所有者可以将指定资源共享给组织、OU或成员账号，组织内的账号默认接受该共享邀请。

工作原理

当资源所有者共享资源给另一个账号时，其实是资源所有者将该资源的访问权限授予另一个账号，且授予的权限是在配置资源共享实例时选择的共享权限。资源使用者对该共享资源的操作权限，取决于共享中配置的资源共享权限。

RAM的工作原理如下图所示：

版权所有 © 华为技术有限公司

图 1-1 RAM 工作原理

访问方式

通过管理控制台、基于HTTPS请求的API（Application Programming Interface）两种方式访问RAM。

- 管理控制台方式
  您可以通过基于浏览器的可视化界面，即控制台访问RAM。登录**管理控制台**，单击页面左上角的 ☰ ，选择“管理与监管 > 资源访问管理”。
- API方式
  如果用户需要将云平台上的RAM集成到第三方系统，用于二次开发，请使用API方式访问RAM，具体操作请参见**《资源访问管理API参考》**。

版权所有 © 华为技术有限公司

2 产品优势

降低管理复杂度

在一个账号中创建资源实例，并共享给其他账号使用，避免了在每个账号中重复创建和配置资源，降低资源管理的复杂度，减少运营开销。资源所有者可以在RAM服务中集中管理不同资源类型以及资源实例的共享配置，提升运营效率，且确保了资源配置的一致性。

提高管理安全性

RAM服务内置了不同资源类型的共享权限，资源使用者只能对资源进行权限内的访问，保证共享资源在满足资源使用者业务诉求的同时，提升资源管理的安全性。

组织级共享管理

用户通过RAM服务将资源共享给整个组织或OU时，RAM服务能够根据组织或OU下账号的调整，自动赋予或收回相应账号的共享资源访问权限。

版权所有 © 华为技术有限公司

3 权限管理

如果您需要使用华为云上的资源访问管理服务，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全地控制华为云资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并使用策略来控制员工对资源访问管理服务的访问范围。如果账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用资源管理服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

RAM 权限

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户可以基于已有权限进行对应的操作。

RAM部署时不区分物理区域，为全局级服务。授权时，在全局级服务中设置权限，访问RAM时，不需要切换区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。

如**表3-1**所示，包括了RAM的所有系统权限。

表 3-1 RAM 系统权限

权限名称	描述
RAM FullAccess	资源访问管理服务所有权限。

 版权所有 © 华为技术有限公司

权限名称	描述
RAM ReadOnlyAccess	资源访问管理服务只读权限。
RAM ResourceShareParticipantAccess	资源访问管理服务资源共享邀请的处理权限。

表3-2列出了RAM常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。“√”表示支持，“×”表示暂不支持。

表 3-2 常用操作与系统权限的关系

操作	RAM FullAccess	RAM ReadOnlyAccess	RAM ResourceShareParticipantAccess
检索共享资源权限列表	√	√	x
检索共享资源权限内容	√	√	x
创建资源共享实例	√	x	x
检索资源共享实例	√	√	√
更新资源共享实例	√	x	x
删除资源共享实例	√	x	x
绑定资源使用者和共享资源	√	x	x
移除资源使用者和共享资源	√	x	x
检索绑定的资源使用者和共享资源	√	√	x
绑定或替换共享资源权限	√	x	x
移除共享资源权限	√	x	x
检索绑定的共享资源权限	√	√	x
检索共享的资源	√	√	√
检索资源使用者	√	√	√
接受共享邀请	√	x	√
拒绝共享邀请	√	x	√

版权所有 © 华为技术有限公司

操作	RAM FullAccess	RAM ReadOnlyAccess	RAM ResourceShareParticipantAccess
检索共享邀请	√	√	√
启用与组织共享	√	x	x
关闭与组织共享	√	x	x
检索是否启用与组织共享	√	√	x

 版权所有 © 华为技术有限公司

4 约束与限制

RAM的使用限制如下表所示，如果默认配额无法满足业务需求，您可以申请扩大配额，具体请参见：**调整配额**。

⚠ 注意

不同类型的账号之间无法共享资源，具体说明如下：

- 华为云中国站与国际站账号之间无法共享资源。
- 华为内部账号与外部账号之间无法共享资源。

表 4-1 RAM 使用限制

类型	默认配额	是否支持修改
单账号创建的资源共享实例数量	1000	是
单个资源共享实例关联的资源数量	50	是
单个资源共享实例关联的权限数量	50	是
单个资源共享实例关联的资源使用者数量	50	是
单账号中所有资源共享实例关联的资源数量	5000	是
单账号中所有资源共享实例关联的权限数量	5000	是
单账号中所有资源共享实例关联的资源使用者数量	5000	是

版权所有 © 华为技术有限公司

类型	默认配额	是否支持修改
单账号中待接受的共享邀请数量（发送邀请方） **说明** • 该配额限制仅适用于给组织外的账号发送共享邀请的情况。 • 对于接受邀请的账号中可存在的待接受共享邀请数量没有配置限制。 • 当已启用与组织共享资源开关，同一组织内的账号之间进行的资源共享不涉及邀请。	50	是
单个资源共享实例的标签数	20	是
被删除的资源共享实例的保留时间	48小时	否
被解除的资源共享关联保留时间	48小时	否
单个资源使用者可以被共享的VPC子网最大数量	100	否

 版权所有 © 华为技术有限公司

5 计费说明

RAM为免费服务，使用RAM服务的相关功能不收取任何费用。

共享的资源自身的使用费用请参见各服务产品文档中的计费说明章节。

关于各付费云服务的价格详情请参见**产品价格详情**，如何了解和管理您的费用请参见**费用中心**。

 版权所有 © 华为技术有限公司

6 支持共享的云服务和资源类型

表 6-1 支持共享的云服务和资源类型

云服务	资源类型	是否支持主动退出共享	应用场景
虚拟私有云 VPC	vpc:subnet（子网）	是	共享VPC功能支持多个账号在一个集中管理、共享的VPC内创建云资源，比如ECS、ELB、RDS等。VPC的所有者可以将VPC内的子网共享给一个或者多个账号使用。通过共享VPC功能，可以简化网络配置，帮助您统一配置和运维多个账号下的资源，有助于提升资源的管控效率，降低运维成本。 更多信息请参见**共享VPC**。
云解析服务 DNS	dns:zone（内网域名）	是	基于资源访问管理（Resource Access Manager，简称RAM）服务，云解析服务可以实现跨账号共享内网域名，资源所有者将内网域名同时共享给多个其他账号使用，资源使用者接受共享邀请后就可以访问和使用共享的内网域名。 更多信息请参见**共享内网域名**。
	dns:resolverRule（解析器规则）	是	基于资源访问管理（Resource Access Manager，简称RAM）服务，云解析服务可以实现跨账号共享转发规则，资源所有者将转发规则同时共享给多个其他账号使用，资源使用者接受共享邀请后就可以访问和使用共享的转发规则。 更多信息请参见**共享转发规则**。
SSL证书管理 SCM	scm:cert（证书）	是	云证书管理服务提供共享功能，用户可以将SSL证书同时共享给同一组织单元内的所有成员账号，这些账号可以将共享证书部署到ELB、WAF和CDN等服务，以启用HTTPS协议。 更多信息请参见**共享证书**。

 版权所有 © 华为技术有限公司

云服务	资源类型	是否支持主动退出共享	应用场景
私有证书管理 PCA	pca:ca（私有CA）	是	云证书管理服务私有证书管理提供共享功能，用户可以将私有CA同时共享给同一组织单元内的所有成员账号，这些账号可以使用共享CA来签发证书。 更多信息请参见**共享私有CA**。
企业路由器 ER	er:instances（实例）	是	基于资源访问管理（Resource Access Manager，简称RAM）服务，可以实现跨账号共享企业路由器，您可以将账号A所属的企业路由器同时共享给多个其他账号，比如账号B、账号C以及账号D等。通过共享功能，可以在同一个企业路由器中接入不同账号下的虚拟私有云，构建云上同区域组网。 更多信息请参见**共享概述**。
函数工作流 Function Graph	functiongraph:function（函数）	是	基于资源访问管理（Resource Access Manager，简称RAM）服务，函数工作流服务可以实现跨账号共享函数，资源所有者将函数同时共享给多个其他账号使用，资源使用者接受共享邀请后就可以访问和使用共享的函数。 更多信息请参见**共享函数**。
云原生应用网络 ANC	anc:service（服务）	是	基于资源访问管理（Resource Access Manager，简称RAM），可以实现跨账号共享ANC的服务，您可以将账号A所属的ANC的服务同时共享给多个其他账号，比如账号B、账号C等。通过共享功能，共享ANC的服务可以接收不同账号下VPC内客户端的访问请求，有助于管理多账号下的资源，提升资源的管控效率。
	anc:anc（云原生应用网络）	是	基于资源访问管理（Resource Access Manager，简称RAM），可以实现跨账号共享云原生应用网络，您可以将账号A所属的云原生应用网络同时共享给多个其他账号，比如账号B、账号C等。通过共享功能，VPC内客户端可以访问不同账号下ANC的服务，实现统一管理多账号下的资源。

 版权所有 © 华为技术有限公司

7 基本概念

资源所有者

创建和管理该资源的账号。用户可以在该账号中通过RAM创建指定资源的共享实例。如何查看资源所有者请参见**查看资源所有者**。

资源使用者

表示被共享的对象。资源使用者可以是账号，也可以是组织或者OU（当RAM启用与组织共享资源时）。如何查看资源使用者请参见**查看资源使用者**。

资源共享实例

资源共享的管理单元，由资源所有者创建。一个资源共享实例中包括一组或多组资源、共享权限和共享对象。如何创建共享请参见**创建共享**。

共享权限

对于每种可共享的资源类型，至少有一个RAM预置的系统权限，该权限定义资源使用者对共享资源可执行的操作。每种资源类型都会有一个默认系统权限，在创建该资源的共享实例时，如果没有指定权限，则会采用默认系统权限。如何查看RAM预置的系统权限请参见**查看RAM权限库**。

共享邀请

资源所有者将资源实例共享给资源使用者时，资源使用者收到的共享请求。资源使用者可以接受或拒绝该共享邀请。当RAM启用与组织共享资源后，资源所有者将资源共享给组织内账号，则组织内的账号默认接受共享邀请。如何接受或拒绝共享邀请请参见**接受/拒绝共享邀请**。

版权所有 © 华为技术有限公司