服务授权参考

文档版本 01

发布日期 2025-09-25

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2025。 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云计算技术有限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，华为云计算技术有限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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 系统角色与策略.....1
2 系统身份策略.....32
3 身份策略授权参考.....47
3.1 计算.....47
3.1.1 弹性伸缩 AS.....47
3.1.2 裸金属服务器 BMS.....61
3.1.3 弹性云服务器 ECS.....69
3.1.4 镜像服务 IMS.....82
3.1.5 函数工作流 FunctionGraph.....90
3.1.6 云化数据中心 CloudDC.....110
3.2 存储.....118
3.2.1 对象存储服务 OBS.....118
3.2.2 云备份 CBR.....152
3.2.3 云硬盘 EVS.....165
3.2.4 高性能弹性文件服务 SFS Turbo.....176
3.2.5 键值存储服务 KVS.....189
3.3 网络.....192
3.3.1 企业路由器 ER.....192
3.3.2 虚拟私有云 VPC.....203
3.3.3 弹性公网 IP EIP.....243
3.3.4 云专线 DC.....267
3.3.5 VPC 终端节点 VPCEP.....283
3.3.6 全球加速 GA.....293
3.3.7 NAT 网关 NAT.....304
3.3.8 云连接 CC.....321
3.3.9 弹性负载均衡 ELB.....350
3.4 容器.....367
3.4.1 云容器引擎 CCE.....367
3.4.2 云容器实例 CCI.....394
3.4.3 容器镜像服务 SWR.....407

 版权所有 © 华为云计算技术有限公司

3.5 CDN 与智能边缘 420
3.5.1 内容分发网络 CDN 420
3.6 数据库 429
3.6.1 云数据库 RDS 429
3.6.2 云数据库 GaussDB 460
3.6.3 文档数据库 DDS 477
3.6.4 数据复制服务 DRS 492
3.6.5 数据管理服务 DAS 527
3.7 安全与合规 537
3.7.1 数据加密服务 DEW 537
3.7.2 DDoS 防护 AAD 571
3.7.2.1 原生基础防护 571
3.7.2.2 原生高级防护 577
3.7.2.3 DDoS 高防 584
3.7.3 云防火墙 CFW 595
3.7.4 云堡垒机 CBH 610
3.7.5 云证书管理服务 CCM 618
3.7.6 数据库安全服务 DBSS 627
3.7.7 数据安全中心 DSC 658
3.7.8 Web 应用防火墙 WAF 665
3.7.9 企业主机安全 HSS 684
3.7.10 安全云脑 SecMaster 783
3.8 大数据 827
3.8.1 云搜索服务 CSS 827
3.8.2 数据治理中心 DataArts Studio 854
3.8.3 数据湖探索 DLI 862
3.8.4 MapReduce 服务 MRS 884
3.8.5 数据仓库服务 GaussDB(DWS) 888
3.9 应用中间件 960
3.9.1 微服务引擎 CSE 960
3.9.2 分布式消息服务 Kafka 版 Kafka 967
3.9.3 分布式消息服务 RabbitMQ 版 RabbitMQ 981
3.9.4 分布式消息服务 RocketMQ 版 RocketMQ 987
3.9.5 API 网关 APIG 999
3.9.6 分布式缓存服务 DCS 1041
3.10 开发与运维 1060
3.10.1 应用管理与运维平台 ServiceStage 1060
3.10.2 软件开发生产线 CodeArts 1072
3.10.3 流水线 CodeArts Pipeline 1079

 版权所有 © 华为云计算技术有限公司

3.10.4 云应用引擎 CAE 1081
3.11 企业应用 1095
3.11.1 云解析服务 DNS 1095
3.11.2 身份策略授权参考 1111
3.12 视频 1283
3.12.1 视频直播服务 Live 1283
3.12.2 媒体处理服务 MPC 1292
3.13 管理与监管 1300
3.13.1 统一身份认证服务 IAM 1300
3.13.2 组织 Organizations 1330
3.13.3 资源访问管理 RAM 1342
3.13.4 IAM 身份中心 1352
3.13.5 配置审计 Config 1364
3.13.6 标签管理服务 TMS 1386
3.13.7 企业管理 EPS 1388
3.13.8 云监控服务 CES 1391
3.13.9 消息通知服务 SMN 1404
3.13.10 云日志服务 LTS 1414
3.13.11 云审计服务 CTS 1438
3.13.12 安全令牌服务 STS 1443
3.13.13 访问分析 IAM Access Analyzer 1447
3.13.14 资源治理中心 RGC 1453
3.13.15 云运维中心 COC 1463
3.13.16 应用性能管理 APM 1480
3.13.17 应用运维管理 AOM 1492
3.13.18 优化顾问 OA 1504
3.14 迁移 1511
3.14.1 对象存储迁移服务 OMS 1511
3.14.2 主机迁移服务 SMS 1517
3.15 用户服务 1525
3.15.1 费用中心 1525
3.15.2 成本中心 1528
3.15.3 账号中心 1532
3.15.4 企业中心 1533
3.15.5 客户运营能力 1535

 版权所有 © 华为云计算技术有限公司

1 系统角色与策略

默认情况下，管理员创建的 IAM 用户没有任何权限，在 IAM 旧版控制台中需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。请参考常见系统权限设置案例为 IAM 用户授权。

作用范围：权限的作用范围，给用户组授予权限时，选择的授权区域。

- 全局服务资源：服务部署时不区分物理区域，为全局级服务，在全局服务中授权，如 OBS、CDN 等。
- 指定区域项目资源：服务部署时通过物理区域划分，在区域级项目中授权，并且只在授权区域生效，如 ECS、BMS 等。
- 所有资源：选择所有资源后，授权将对所有项目都生效，包括全局服务和所有项目（包括未来创建的项目）。

权限类别：权限根据授权粒度分为角色与策略。策略是 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。详情请参见：权限。

- **如果一个服务同时有角色与策略，建议优先选择策略进行授权。**
- 支持策略的服务，可以创建自定义策略，自定义策略是对系统策略的扩展和补充，可以精确地允许或拒绝用户对服务的某个资源类型在一定条件下进行指定的操作。单击下表中的“策略”，查看服务支持的自定义策略授权项。

BASE

服务	作用范围	系统权限	权限类别	权限描述
BASE	全局服务	FullAccess	策略	基于策略授权的所有服务的所有权限。
	所有项目	Tenant Guest	角色	除统一身份认证服务外，其他所有服务的只读权限。 说明 • 作用范围为**全局服务**，授权将对除

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
				IAM 外的全局服务生效，用户将拥有 OBS、CDN 等**全局服务的只读权限。** • 作用范围为**所有项目**，授权将对除 IAM 外的全局服务和所有项目（包括未来创建的项目）生效，用户将拥有除 IAM 外，**所有项目下所有服务的只读权限。** • 作用范围为**指定项目**，授权仅对指定项目生效，用户将拥有**指定项目下，ECS、BMS 等所有项目级服务的只读权限。** • 费用中心涉及敏感信息，如需查看费用中心，则需要单独配置业务支撑系统（BSS）相关权限。
	所有项目	Tenant Administrator		除统一身份认证服务外，其他所有服务的管理员权限。 说明 • 作用范围为**全局服务**，授权将对除 IAM 外的全局服务生效，用户将拥有 OBS、CDN 等**所有全局服务的管理员权限。** • 作用范围为**所有项目**，授权将对除 IAM 外的全局服务和所有项目（包括未来创建的项目）生效，用户将拥有除 IAM 外，**所有项目下所有服务的管理员权限。** • 作用范围为**指定项目**，授权仅对指定项目生效，用户将拥有**指定项目下，ECS、BMS 等所有项目级服务的管理员权限。**
	全局服务	Agent Operator		切换角色并访问委托方账号中的资源。

 版权所有 © 华为云计算技术有限公司

计算

服务	作用范围	系统权限	权限类别	权限描述
弹性云服务器（ECS）	区域级项目	ECS FullAccess	策略	弹性云服务器所有权限。
		ECS ReadOnlyAccess		弹性云服务器的只读访问权限。
		ECS CommonOperations		开机、关机、重启、查询弹性云服务器。
		Server Administrator	角色	弹性云服务器的所有执行权限，**该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest。** 如果在操作过程中涉及其他服务资源的创建、删除、变更等，则还需要在同项目中勾选**对应服务的Administrator 权限**。 例如：在控制台创建 ECS 时如需创建新的 VPC，则需额外授予创建 VPC 的 VPC Administrator 权限。
裸金属服务器（BMS） （项目级服务)	区域级项目	BMS FullAccess	策略	裸金属服务器的所有权限。
		BMS ReadOnlyAccess		裸金属服务器的只读权限。
		BMS CommonOperations		开机、关机、重启、查询裸金属服务器。
弹性伸缩（AS） （项目级服务）	区域级项目	AutoScaling FullAccess	策略	弹性伸缩服务的所有权限。
		AutoScaling ReadOnlyAccess		弹性伸缩服务只读权限。
		AutoScaling Administrator	角色	对弹性伸缩全部资源的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：ELB Administrator、CES Administrator、Server Administrator、Tenant Administrator。**
镜像服务（IMS）	区域级项	IMS FullAccess	策略	镜像服务的所有执行权限。
		IMS		镜像服务的只读权限。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
（项目级服务）	目	ReadOnlyAccess		
		IMS Administrator	角色	镜像服务的所有执行权限。 **该角色有依赖，需要勾选依赖的角色：Tenant Administrator。**
		Server Administrator		创建、删除、查询、修改及上传镜像，**该角色有依赖，需要在同项目中勾选依赖的角色：IMS Administrator**
函数工作流（FunctionGraph） （项目级服务）	区域级项目	FunctionGraph FullAccess	策略	FunctionGraph 服务的所有执行权限。
		FunctionGraph ReadOnlyAccess		FunctionGraph 服务的只读权限。
		FunctionGraph CommonOperations		FunctionGraph 服务的操作权限，包括查询函数和触发器以及调用函数。
		FunctionGraph Administrator	角色	FunctionGraph 函数工作流、触发器的管理权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest。**
		FunctionGraph Invoker		FunctionGraph 函数工作流、触发器的查询权限。
云手机服务器（CPH） （项目级服务）	区域级项目	CPH Administrator	角色	云手机的所有执行权限。
		CPH User		云手机的只读权限。
专属主机（DeH） （项目级服务）	区域级项目	DeH FullAccess	策略	专属主机所有执行权限。
		DeH CommonOperations		专属主机基本操作权限。
		DeH ReadOnlyAccess		专属主机只读权限，拥有该权限的用户仅能进行查询操作，可用于统计和调查。

 版权所有 © 华为云计算技术有限公司

存储

服务	作用范围	系统权限	权限类别	权限描述
对象存储服务（OBS）（全局级服务）	全局服务	OBS OperateAccess	策略	拥有该权限的用户可以执行 OBS ReadOnlyAccess 的所有操作，在此基础上还可以执行上传对象、下载对象、删除对象、获取对象 ACL 等对象基本操作。
		OBS ReadOnlyAccess		拥有该权限的用户可以执行列举桶、获取桶基本信息、获取桶元数据、列举对象的操作。
		OBS Buckets Viewer	角色	拥有该权限的用户可以执行列举桶、获取桶基本信息、获取桶元数据的操作。
云硬盘（EVS）（项目级服务）	区域级项目	EVS FullAccess	策略	云硬盘的所有权限，具有云硬盘资源的创建、扩容、挂载、卸载、查询、删除等操作权限。
		EVS ReadOnlyAccess		云硬盘的只读权限，只有云硬盘资源的查询权限。
		Server Administrator	角色	云硬盘服务的所有执行权限。
云备份（CBR）（项目级服务）	区域级项目	CBR FullAccess	策略	云备份管理员权限，拥有该权限的用户可以操作并使用所有存储库和策略。
		CBR BackupsAndVaultsFullAccess		云备份普通用户权限，拥有该权限的用户可以创建、查看和删除存储库等。
		CBR ReadOnlyAccess		云备份只读权限，拥有该权限的用户仅能查看云备份数据。
内容分发网络（CDN）（全局级服务）	全局服务	CDN DomainReadOnlyAccess	策略	内容分发网络加速域名信息的只读权限。
		CDN StatisticsReadOnlyAccess		内容分发网络统计信息的只读权限。
		CDN LogsReadOnlyAccess		内容分发网络日志的只读权限。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
		CDN RefreshAndPreheatAccess		内容分发网络刷新预热权限。
		CDN Administrator	角色	内容分发网络的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest。**
存储容灾服务（SDRS） （项目级服务）	区域级项目	SDRS Administrator	角色	存储容灾服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、Server Administrator。**
弹性文件服务（SFS） （项目级服务）	区域级项目	SFS FullAccess	策略	弹性文件服务的所有执行权限。
		SFS ReadOnlyAccess		弹性文件服务的只读权限。
		SFS Turbo FullAccess		弹性文件服务 SFS Turbo 的所有权限。
		SFS Turbo ReadOnlyAccess		弹性文件服务 SFS Turbo 的只读权限。
		SFS Administrator	角色	弹性文件服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest。**
云服务器备份（CSBS） （项目级服务）	区域级项目	CSBS Administrator	角色	云服务器备份的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Server Administrator。**
云硬盘备份（VBS） （项目级服务）	区域级项目	VBS Administrator	角色	云硬盘备份的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、Server Administrator。**

 版权所有 © 华为云计算技术有限公司

网络

服务	作用范围	系统权限	权限类别	权限描述
虚拟私有云（VPC） （项目级服务）	区域级项目	VPC FullAccess	策略	虚拟私有云的所有执行权限。
		VPC ReadOnlyAccess		虚拟私有云的只读权限。
		VPC Administrator	角色	虚拟私有云的部分操作权限，不包括创建、修改、删除、查看安全组以及安全组规则。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest。**
		Server Administrator		对弹性 IP 地址、安全组、端口进行任意操作。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest。**
弹性负载均衡（ELB） （项目级服务）	区域级项目	ELB FullAccess	策略	弹性负载均衡的所有执行权限。
		ELB ReadOnlyAccess		弹性负载均衡的只读权限。
		ELB Administrator	角色	弹性负载均衡的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest。**
NAT 网关（NAT） （项目级服务）	区域级项目	NAT FullAccess	策略	NAT 网关的所有执行权限。
		NAT ReadOnlyAccess		NAT 网关的只读权限。
		NAT Administrator	角色	NAT 网关的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest。**
云专线（DC） （项目级服务）	区域级项目	Direct Connect Administrator	角色	云专线服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest。**
		DCaaS Partner		云专线服务的合作伙伴用户权限，支持为其他用户创建托管和标准连接。
		DCAAS FullAccess	策略	云专线服务所有权限。
		DCAAS		云专线服务只读权限。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
		ReadOnlyAccess		
虚拟专用网络（VPN） （项目级服务）	区域级项目	VPN Administrator	角色	虚拟专用网络的管理员权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、VPC Administrator。**
		VPN FullAccess	策略	虚拟专用网络服务所有权限。
		VPN ReadOnlyAccess		虚拟专用网络服务只读权限。
云解析服务（DNS） （项目级服务）	区域级项目	DNS Administrator	角色	云解析服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、VPC Administrator。**
		DNS FullAccess	策略	云解析服务的所有执行权限。
		DNS ReadOnlyAccess		云解析服务只读权限，拥有该权限的用户仅能查看 DNS 的资源。
VPC 终端节点（VPCEP） （项目级服务）	区域级项目	VPCEndpoint Administrator	角色	VPC 终端节点的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Server Administrator、VPC Administrator 和 DNS Administrator。**
云连接（CC） （全局级服务）	全局服务	Cross Connect Administrator	角色	云连接服务的管理员权限，拥有该权限的用户拥有云连接服务所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、VPC Administrator。**
		CC FullAccess	策略	云连接服务所有权限。
		CC ReadOnlyAccess		云连接服务只读权限。
		CC Network Depend QueryAccess		云连接服务依赖的只读权限。
企业路由器（ER） （项目级服	区域级项目	ER FullAccess	策略	企业路由器所有权限。
		ER		企业路由器只读权限。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
务）		ReadOnlyAccess		

容器

服务	作用范围	系统权限	权限类别	权限描述
云容器引擎（CCE） （项目级服务）	区域级项目	CCE FullAccess	策略	云容器引擎服务集群资源的普通操作权限（包含集群创建、删除、更新等）。不包括集群（启用 Kubernetes RBAC 鉴权）命名空间权限以及委托授权、生成集群证书等管理员权限。 说明 IAM 用户可以在 CCE 控制台获取集群（启用 Kubernetes RBAC 鉴权）命名空间权限以及委托授权、生成集群证书等管理员权限，详情请参考：CCE 权限概述。
		CCE ReadOnlyAccess		云容器引擎服务集群资源的普通只读权限，不包括集群（启用 Kubernetes RBAC 鉴权）命名空间权限。
		CCE Administrator	角色	具有 CCE 集群及集群下所有资源（包含工作负载、服务等）的读写权限。 **该角色有依赖，需要同时又拥有以下权限：** **全局服务：OBS Buckets Viewer。** **区域级项目（在同项目中勾选）：Tenant Guest、Server Administrator、ELB Administrator、SFS Administrator、SWR Admin、APM FullAccess。** 说明 如果同时拥有 NAT Gateway

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
				Administrator 权限，则可以在集群中使用 NAT 网关的相关功能。
云容器实例（CCI）（项目级服务）	区域级项目	CCI FullAccess	策略	云容器实例所有权限，拥有该权限的用户可以执行云容器实例所有资源的创建、删除、查询、更新操作。
		CCI ReadOnlyAccess		云容器实例只读权限，拥有该权限的用户仅能查看云容器实例资源。
		CCI CommonOperations		云容器实例普通用户，拥有该权限的用户可以执行除 RBAC、network 和 namespace 子资源创建、删除、修改之外的所有操作。
		CCI Administrator	角色	云容器实例管理员权限，拥有该权限的用户可以执行云容器实例所有资源的创建、删除、查询、更新操作。
容器镜像服务（SWR）（项目级服务）	区域级项目	SWR Admin	角色	容器镜像服务的所有执行权限。
		SWR FullAccess	策略	容器镜像服务企业版所有权限。
		SWR ReadOnlyAccess		容器镜像服务企业版只读权限，可以查询制品仓库、Chart，创建临时凭证，下载制品等。
		SWR OperateAccess		容器镜像服务企业版操作权限，可以查询企业版实例，操作制品仓库、组织，创建临时凭证，上传、下载制品等。
基因容器（GCS）（项目级服务）	区域级项目	GCS Administrator	角色	基因容器服务管理员。
		GCS FullAccess	策略	基因容器服务的所有执行权限。
		GCS ReadOnlyAccess		基因容器服务的只读权限。
		GCS CommonOperations		基因容器服务的使用权限。
应用编排服务（AOS）	区域级项	CDE Admin	角色	应用编排服务（AOS）管理员，拥有该服务下的所有权限。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
（项目级服务）	目	CDE Developer		应用编排服务（AOS）开发者。
		RF FullAccess	策略	资源编排服务（RF）所有权限。
		RF ReadOnlyAccess		资源编排服务（RF）只读权限。
		RF DeployByExecutionPlanOperations		资源编排服务（RF）通过执行计划开发权限，拥有执行计划的创建、执行、读取权限和堆栈的读取权限。
华为云UCS（全局级服务）	全局服务	UCS FullAccess	策略	UCS 服务管理员权限，拥有该权限的用户拥有服务的所有权限（包含制定权限策略、安全策略等）。
		UCS CommonOperations		UCS 服务基本操作权限，拥有该权限的用户可以执行创建工作负载、流量分发等操作。
		UCS CIAOperations		UCS 服务容器智能分析管理员权限。
		UCS ReadOnlyAccess		UCS 服务只读权限（除容器智能分析只读权限）。

安全与合规

服务	作用范围	系统权限	权限类别	权限描述
Anti-DDoS流量清洗（Anti-DDoS）（项目级服务）	区域级项目	Anti-DDoS Administrator	角色	Anti-DDoS 流量清洗的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest。**
DDoS 高防（AAD）（项目级服务）	区域级项目	CAD Administrator	角色	DDoS 高防服务管理员，拥有该服务下的所有权限。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
DDoS 防护（CNAD）（全局服务）	全局服务	CNAD FullAccess	策略	DDoS 原生专业防护所有权限。
		CNAD ReadOnlyAccess		DDoS 原生专业防护只读权限。
漏洞扫描服务（VSS）（项目级服务）	区域级项目	VSS ReadOnlyAccess	角色	漏洞扫描服务只读权限。
主机安全服务（HSS）（项目级服务）	区域级项目	HSS Administrator	角色	企业主机安全的所有执行权限。
		HSS FullAccess	策略	企业主机安全服务所有权限。
		HSS ReadOnlyAccess		企业主机安全服务的只读访问权限。
数据库安全服务（DBSS）（项目级服务）	区域级项目	DBSS System Administrator	角色	数据库安全服务的所有执行权限。
		DBSS Audit Administrator		数据库安全服务的安全审计权限。
		DBSS Security Administrator		数据库安全服务的安全防护权限。
		DBSS FullAccess	策略	数据库安全服务所有权限。
		DBSS ReadOnlyAccess		数据库安全服务只读权限，拥有该权限的用户仅能查看数据库安全服务，不具备服务配置权限。
密码安全中心（项目级服务）	区域级项目	KMS Administrator	角色	密码安全中心加密密钥的管理员权限。
		KMS CMKFullAccess	策略	密码安全中心加密密钥所有权限。
		DEW KeypairFullAccess		密码安全中心密钥对所有权限。
		DEW KeypairReadOnlyAccess		密码安全中心密钥对查看权限。
		CSMS FullAccess		凭据管理服务所有权限。
		CSMS		凭据管理服务凭据只读权限。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
		ReadOnlyAccess		
Web 应用防火墙（WAF）（项目级服务）	区域级项目	WAF Administrator	角色	Web 应用防火墙的所有执行权限。**该角色有依赖，需要在全局项目中勾选 Tenant Guest 角色、在同项目中勾选 Server Administrator 角色。**
		WAF FullAccess	策略	Web 应用防火墙服务的所有权限。
		WAF ReadOnlyAccess		Web 应用防火墙服务的只读访问权限。
云防火墙（CFW）（项目级服务）	区域级项目	CFW FullAccess	策略	云防火墙服务所有权限。
		CFW ReadOnlyAccess		云防火墙服务只读权限。
SSL 证书管理（SCM）（全局级服务）（SCM 已合并到云证书管理服务 CCM）	全局服务	SCM Administrator	角色	SSL 证书管理服务的管理员权限，拥有服务的所有权限。**该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、Server Administrator**
		SCM FullAccess	策略	SSL 证书管理服务的所有权限。
		SCM ReadOnlyAccess		SSL 证书管理服务只读权限，拥有该权限的用户仅能查询证书信息，不具备对证书进行增删改权限。
云堡垒机（CBH）（项目级服务）	区域级项目	CBH FullAccess	策略	云堡垒机实例的所有权限。
		CBH ReadOnlyAccess		云堡垒机实例只读权限，拥有该权限的用户仅能查看云堡垒机服务，不具备服务配置和操作权限。
数据安全中心（DSC）（项目级服务）	区域级项目	DSC FullAccess	策略	数据安全中心服务所有权限。
		DSC ReadOnlyAccess		数据安全中心服务只读权限。
		DSC DashboardReadOnlyAccess		数据安全中心服务大屏服务只读权限。
数据库和应用迁移（UGO）	区域级项目	UGO FullAccess	策略	数据库和应用迁移服务所有权限。
		UGO ReadOnlyAccess		数据库和应用迁移服务只读权限。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
（项目级服务）		UGO CommonOperations		数据库和应用迁移服务 SQL 语句转换权限。

管理与监管

服务	作用范围	系统权限	权限类别	权限描述
统一身份认证服务（IAM） （全局服务）	全局服务	IAM ReadOnlyAccess	策略	统一身份认证服务的只读权限。
	全局服务	Security Administrator	角色	统一身份认证服务(除切换角色外)所有权限。
云监控服务（CES） （项目级服务）	区域级项目	CES Administrator	角色	云监控服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、Server Administrator。**
	区域级项目	CES FullAccess	策略	云监控服务的管理员权限，拥有该权限可以操作云监控服务的全部权限。 云服务监控功能因为涉及需要查询其他云服务的实例资源，**需要涉及服务支持策略授权特性**，才可以正常使用，支持策略授权的云服务列表请参考：使用 IAM 授权的云服务。
	区域级项目	CES ReadOnlyAccess		云监控服务的只读权限，拥有该权限仅能查看云监控服务的数据。 云服务监控功能因为涉及需要查询其他云服务的实例资源，**需要涉及服务支持策略授权特性**，才可以正常使用，支持策略授权的云服务列表请参考：使用 IAM 授权的云服务。
应用运维管理服务	区域级项	AOM FullAccess	策略	应用运维管理服务的所有执行权限。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
（AOM） （项目级服务）	目	AOM ReadOnlyAccess		应用运维管理服务的只读权限。
应用性能管理服务（APM） （项目级服务）	区域级项目	APM FullAccess	策略	应用性能管理服务的所有执行权限。
		APM ReadOnlyAccess		应用性能管理服务的只读权限。
		APM Administrator	角色	应用性能管理服务的所有执行权限。
云审计服务（CTS） （项目级服务）	区域级项目	CTS FullAccess	策略	云审计服务所有权限。 **说明** **开通云审计服务，需同时拥有** CTS FullAccess、Security Administrator **权限。**
		CTS ReadOnlyAccess		云审计服务只读权限。
		CTS Administrator	角色	云审计服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、以及 Tenant Administrator。**
云日志服务（LTS） （项目级服务）	区域级项目	LTS FullAccess	策略	云日志服务所有权限。
		LTS ReadOnlyAccess		云日志服务的只读权限。
		LTS Administrator	角色	云日志服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、以及 Tenant Administrator。**
标签管理服务（TMS） （全局级服务）	全局服务	TMS FullAccess	策略	标签管理服务所有权限。
		TMS ReadOnlyAccess		标签管理服务只读权限。
		TMS Administrator	角色	标签管理服务管理员权限。 依赖以下策略： • Tenant Guest：全局级/项目级策略，在同项目中勾选。 • Server Administrator：项目级策

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
				略，在同项目中勾选。 • Tenant Guest：全局级策略，选择“全局服务”。 • Tenant Administrator：全局级策略，选择“全局服务”。 • IMS Administrator：项目级服务，在同项目中勾选。 • AutoScaling Administrator：项目级服务，在同项目中勾选。 • VPC Administrator：项目级服务，在同项目中勾选。 • VBS Administrator：项目级服务，在同项目中勾选。
资源模板服务（RTS） （项目级服务）	区域级项目	RTS Administrator	角色	资源模板服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Server Administrator、ELB Administrator、CES Administrator。**
应用身份管理服务（OneAccess） （全局级服务）	全局服务	OneAccess FullAccess	策略	应用身份管理服务所有执行权限，包括自定义域名、修改域名证书等，但 IAM 用户不支持购买并使用 OneAccess。
		OneAccess ReadOnlyAccess		应用身份管理服务只读权限，拥有该权限的用户仅能查看应用身份管理服务，不具备服务配置权限。
配置审计（Config） （全局级服务）	全局服务	Config ConsoleFullAccess	策略	配置审计服务控制台使用所有权限。
		Config FullAccess		配置审计服务所有权限。
		Config ReadOnlyAccess		配置审计服务只读权限。
资源访问管理（RAM） （全局级服务）	全局服务	RAM FullAccess	策略	资源访问管理服务所有权限。
		RAM ReadOnlyAccess		资源访问管理服务只读权限。
		RAM ResourceSharePart		资源访问管理服务资源共享邀请的处理权限。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
		icipantAccess		
组织（Organizations）（全局级服务）	全局服务	Organizations FullAccess	策略	组织管理所有权限。
		Organizations ReadOnlyAccess		组织管理只读权限。

应用服务

服务	作用范围	系统权限	权限类别	权限描述
应用管理与运维平台（ServiceStage）（项目级服务）	区域级项目	ServiceStage Administrator	角色	应用管理与运维平台管理员，拥有该服务下的所有权限。
		ServiceStage Developer		应用管理与运维平台开发者，拥有该服务下的所有权限，但无基础设施创建权限。
		ServiceStage Operator		应用管理与运维平台操作员，拥有该服务下的只读权限。
		ServiceStage FullAccess	策略	应用管理与运维平台所有权限。
		ServiceStage ReadOnlyAccess		应用管理与运维平台只读权限。
		ServiceStage Development		应用管理与运维平台开发者权限，拥有应用、组件、环境的操作权限，但无审批权限和基础设施创建权限。
微服务引擎服务（CSE）	区域级项目	CSE FullAccess	策略	微服务引擎服务所有权限。
		CSE ReadOnlyAccess		微服务引擎服务只读权限。
分布式缓存服务（DCS）（项目级服务）	区域级项目	DCS FullAccess	策略	分布式缓存服务的所有执行权限。
		DCS UserAccess		分布式缓存服务的普通用户权限（无实例创建、修改、删除、扩缩容）。
		DCS ReadOnlyAccess		分布式缓存服务的只读权限。
		DCS Administrator	角色	分布式缓存服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、Server Administrator。**

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
分布式消息服务（DMS Kafka、DMS RabbitMQ）（项目级服务）	区域级项目	DMS UserAccess	策略（DMS Kafka） 策略（DMS RabbitMQ）	分布式消息服务（DMS Kafka、DMS RabbitMQ）普通用户权限（没有实例创建、修改、删除、扩容、转储）。
		DMS ReadOnlyAccess		分布式消息服务（DMS Kafka、DMS RabbitMQ）的只读权限，拥有该权限的用户仅能查看分布式消息服务数据。
		DMS FullAccess		分布式消息服务（DMS Kafka、DMS RabbitMQ）管理员权限，拥有该权限的用户可以操作所有分布式消息服务的功能。
消息通知服务（SMN）（项目级服务）	区域级项目	SMN Administrator	角色	消息通知服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest。**
		SMN FullAccess	策略	消息通知服务所有权限。
		SMN ReadOnlyAccess		消息通知服务的只读访问权限。
API 网关（APIG）（项目级服务）	区域级项目	APIG Administrator	角色	API 网关服务的管理员权限。拥有该权限的用户可以使用**共享版**和**专享版** API 网关服务的所有功能。 **使用 VPC 通道时，用户还需具备 VPC Administrator 角色权限** **使用自定义认证功能，用户还需具备 FunctionGraph Administrator 角色权限。**
		APIG FullAccess	策略	API 网关服务所有权限。拥有该权限的用户可以使用**专享版** API 网关服务的所有功能。
		APIG ReadOnlyAccess		API 网关服务的只读访问权限。拥有该权限的用户只能查看**专享版** API 网关的各类信息。
多云高可用服务（MAS）（项目级服务）	区域级项目	MAS FullAccess	策略	多云高可用服务所有权限。
		MAS ReadOnlyAccess		多云高可用服务只读权限。
		MAS CommonOperations		多云高可用服务基本操作权限，包括拥有应用、组件、监控器的操作权限，但无实例创建、删除权限。
区块链服务（BCS）（项目级服务）	区域级项目	BCS Administrator	角色	区块链服务的管理员权限。

 版权所有 © 华为云计算技术有限公司

专属云

服务	作用范围	系统权限	权限类别	权限描述
专属分布式存储服务（DSS） （项目级服务）	区域级项目	DSS FullAccess	角色	专属分布式存储服务的所有执行权限。
		DSS ReadOnlyAccess		专属分布式存储服务的只读权限。

数据库

服务	作用范围	系统权限	权限类别	权限描述
关系型数据库（RDS） （项目级服务）	区域级项目	RDS FullAccess	策略	关系型数据库的所有执行权限。
		RDS ReadOnlyAccess		关系型数据库的只读权限。
		RDS ManageAccess		关系型数据库除删除操作外的DBA 权限。
		RDS Administrator	角色	关系型数据库的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、Server Administrator。**
文档数据库服务（DDS） （项目级服务）	区域级项目	DDS FullAccess	策略	文档数据库服务的所有执行权限。
		DDS ReadOnlyAccess		文档数据库服务的只读权限。
		DDS ManageAccess		文档数据库服务除删除操作外的DBA 权限。
		DDS Administrator	角色	文档数据库服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、Server Administrator** 如果配置了 DDS 企业项目，需要在同项目中勾选 **DAS Admin**，才可以通过 DDS 界面登录到 DAS 服

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
				务。
数据复制服务（DRS）（项目级服务）	区域级项目	DRS Administrator	角色	数据复制服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、Server Administrator。**
		DRS FullAccess	策略	数据复制服务所有权限。
		DRS ReadOnlyAccess		数据复制服务只读权限
数据管理服务（DAS）（项目级服务）	区域级项目	DAS Administrator	角色	数据管理服务管理员，拥有该服务下的所有权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest。**
		DAS FullAccess	策略	数据管理服务的所有权限。
分布式数据库中间件（DDM）（项目级服务）	区域级项目	DDM FullAccess	策略	分布式数据库中间件的所有执行权限。
		DDM CommonOperations		分布式数据库中间件的普通权限。 普通权限与所有执行权限比较，普通权限不具备以下操作权限： • 购买 DDM 实例 • 删除 DDM 实例 • 平滑扩容 • 扩容失败-回滚、扩容失败-清理
		DDM ReadOnlyAccess		分布式数据库中间件的只读权限。
云数据库 GeminiDB（项目级服务）	区域级项目	GeminiDB FullAccess	策略	分布式多模 NoSQL 数据库服务所有权限。
		GeminiDB ReadOnlyAccess		分布式多模 NoSQL 数据库服务只读权限。
云数据库 GaussDB（项目级服务）	区域级项目	GaussDB FullAccess	策略	云数据库 GaussDB 服务的所有执行权限。
		GaussDB ReadOnlyAccess		云数据库 GaussDB 服务的只读访问权限。

 版权所有 © 华为云计算技术有限公司

迁移

服务	作用范围	系统权限	权限类别	权限描述
云数据迁移（CDM） （项目级服务）	区域级项目	CDM Administrator	角色	云数据迁移的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、Server Administrator。**
		CDM FullAccess	策略	CDM 管理员权限，拥有 CDM 服务所有权限。
		CDMFullAccessExceptUpdateEIP		拥有除绑定/解绑 EIP 外的所有 CDM 服务权限。
		CDM CommonOperations		拥有 CDM 作业和连接的操作权限。
		CDM ReadOnlyAccess		CDM 服务只读权限，拥有该权限的用户仅能查看 CDM 集群、连接、作业。
主机迁移服务（SMS） （全局级服务）	全局服务	SMS FullAccess	策略	主机迁移服务所有权限。
		SMS ReadOnlyAccess		主机迁移服务只读权限。
对象存储迁移服务（OMS） （项目级服务）	区域级项目	OMS Administrator	角色	对象存储迁移服务所有权限。 **如需使用 OMS，需要为 IAM 用户同时授予系统策略 OBS OperateAccess。**

智能边缘

服务	作用范围	系统权限	权限类别	权限描述
智能边缘云（IEC） （全局级服务）	全局服务	IEC FullAccess	策略	智能边缘云所有权限，拥有该权限的用户可以对 IEC 资源执行任意操作。
		IEC ReadOnlyAccess		智能边缘云只读权限，拥有该权限的用户可以查询 IEC 资源的利用情

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
				况，即仅拥有 IEC 读权限。

EI 企业智能

服务	作用范围	系统权限	权限类别	权限描述
ModelArts（项目级服务）	区域级项目	ModelArts FullAccess	策略	ModelArts 管理员权限，拥有 ModelArts 所有的权限。
		ModelArts CommonOperations		ModelArts 操作权限，拥有除了管理专属资源池之外的所有操作权限。
数据治理中心（DataArts Studio）（项目级服务）	区域级项目	DAYU Administrator	角色	DataArts Studio 的所有执行权限。具备对所有工作空间的所有权限。 特殊的是，仅 DAYU Administrator 具有数据开发模块的默认项配置权限（周期调度、多 IF 策略、软硬锁策略），DAYU User 不支持。
		DAYU User		数据治理中心 DataArts Studio 普通用户，拥有被授予的工作空间的指定角色的权限。 赋予 DAYU User 策略的用户具有什么权限，依赖于该用户在工作空间中被赋予什么角色。
MapReduce 服务（MRS）（项目级服务）	区域级项目	MRS FullAccess	策略	MapReduce 服务的所有执行权限。
		MRS CommonOperations		MapReduce 服务的普通用户权限（无新增、删除资源权限）。
		MRS ReadOnlyAccess		MapReduce 服务的只读权限。
		MRS Administrator	角色	MapReduce 服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、Server Administrator。**
数据仓库服	区域	DWS FullAccess	策	数据仓库服务的所有执行权限。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
务 GaussDB（DWS）（项目级服务）	级项目	DWS ReadOnlyAccess	略	数据仓库服务的只读权限。
		DWS Administrator	角色	数据仓库服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、Server Administrator。**
		DWS Database Access		数据仓库服务数据库访问权限，拥有该权限的用户，可以基于 IAM 用户生成临时数据库用户凭证以连接 DWS 集群数据库。
数据湖探索（DLI）（项目级服务）	区域级项目	DLI Service Admin	角色	数据湖探索的所有执行权限。
		DLI FullAccess	策略	数据湖探索所有权限，拥有该权限的用户拥有数据湖探索所有的执行权限。
		DLI ReadOnlyAccess		数据湖探索只读权限，拥有该权限的用户仅有查看队列列表、作业列表、作业详情、数据库列表、表列表、显示建表语句和显示表字段以及作业创建、更新、删除等作业元数据操作权限，无其他权限。
图引擎服务（GES）（项目级服务）	区域级项目	GES Administrator	角色	图引擎服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、Server Administrator。**
		GES Manager		GES 服务高级用户，可以对 GES 资源执行除创建图和删除图以外的任意操作。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest。**
		GES Operator		只读图、访问图权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest。**
		GES FullAccess	策略	图引擎服务管理员权限，拥有该权限的用户拥有图引擎服务的全部权限，包括创建、删除、访问、升级等操作。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
		GES Development		图引擎服务使用权限，拥有该权限的用户可以执行除了创建图、删除图以外所有操作。
		GES ReadOnlyAccess		图引擎服务资源只读权限，拥有该权限的用户只能做一些资源查看类的操作如查看图列表、查看元数据和查看备份等。
云搜索服务（CSS） （项目级服务）	区域级项目	CSS Administrator	角色	云搜索服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、Server Administrator。**
数据接入服务（DIS） （项目级服务）	区域级项目	DIS Administrator	角色	数据接入服务的所有执行权限。
		DIS Operator		通道管理权限，拥有创建删除等管理通道的权限，但不能使用通道上传下载数据。
		DIS User		通道使用权限，拥有使用通道上传下载数据的权限，但不能管理通道。
表格存储服务（CloudTable） （项目级服务）	区域级项目	CloudTable Administrator	角色	表格存储服务的所有执行权限。 **该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、Server Administrator。**
对话机器人服务（CBS） （项目级服务）	区域级项目	CBS Administrator	角色	对话机器人服务的所有执行权限。
		CBS Guest		对话机器人服务的只读权限。
华为HiLens （项目级服务）	区域级项目	HiLens FullAccess	策略	Huawei HiLens 管理员权限，拥有该权限的用户可以操作并使用所有Huawei HiLens 服务。 **如果需要申请公测、设置告警接收和设置技能消息的操作权限，需要在同项目中勾选 SMN Administrator 角色。**
		HiLens		Huawei HiLens 操作权限，拥有该

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
		CommonOperations		权限的用户拥有 Huawei HiLens 服务的操作权限除了注销设备、下架技能的权限。
		HiLens ReadOnlyAccess		Huawei HiLens 只读权限，拥有该权限的用户仅能查看 Huawei HiLens 服务的数据。 **如果需要申请公测、设置告警接收和设置技能消息的操作权限，需要在同项目中勾选 SMN Administrator 角色。**
可信智能计算服务（TICS） （项目级服务）	区域级项目	TICS FullAccess	策略	可信智能计算服务的所有访问权限。
		TICS ReadOnlyAccess		可信智能计算服务的只读访问权限。
		TICS CommonOperations		可信智能计算服务联盟、作业、代理、通知、数据集的管理权限
LakeFormation	全局服务	LakeFormation FullAccess	策略	LakeFormation 管理员权限，拥有该权限的用户可以操作并使用所有 LakeFormation 服务功能。
		LakeFormation ReadOnlyAccess		LakeFormation 只读权限，拥有该权限的用户可以执行 LakeFormation 所有查询类功能。
		LakeFormation CommonAccess		LakeFormation 基础权限，包含 LakeForamtion 服务协议查看/授权/取消，以及 OBS、TMS 等周边依赖服务的基础权限集合。

企业应用

服务	作用范围	系统权限	权限类别	权限描述
云桌面（Workspace	区域级项	Workspace FullAccess	策	云桌面服务所有权限。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
） （项目级服务）	目	Workspace DesktopsManager	略	云桌面服务桌面管理员权限。
		Workspace UserManager		云桌面服务用户管理员权限。
		Workspace SecurityManager		云桌面服务安全管理员权限。
		Workspace TenantManager		云桌面服务租户配置管理员权限。
		Workspace ReadOnlyAccess		云桌面服务只读权限。
应用与数据集成平台（ROMA Connect） （项目级服务）	区域级项目	ROMA Administrator	角色	ROMAConnect 管理员权限，拥有该权限的用户可以操作并使用所有 ROMAConnect 功能。 **该角色有依赖，请根据需要在同项目中勾选依赖的角色：** • 使用 VPC 通道时，用户还需具备 VPC Administrator 角色权限。 • 使用 FunctionGraph 作为 API 的后端服务时，用户还需具备 FunctionGraph Administrator 角色权限。 • 使用规则引擎转发 DIS 时，用户还需具备 DIS Administrator 角色权限。
		ROMA FullAccess	策略	ROMA Connect 服务所有权限，拥有该权限的用户可以操作所有 ROMA Connect 服务的功能。
		ROMA CommonOperations		ROMA Connect 服务普通用户权限（无实例创建、修改、删除的权限）。
		ROMA ReadOnlyAccess		ROMA Connect 服务的只读权限，拥有该权限的用户仅能查看 ROMA Connect 服务数据。
ROMA 资产中心（ROMA	所有项目	ROMAExchange FullAccess	策略	ROMA 资产中心所有权限。
		ROMAExchange CommonOperatio		ROMA 资产中心的资产操作权

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
Exchange） （全局级服务、项目级服务）		ns		限，但不包括单据审批权限。
		ROMAExchangeApprovalOperations		ROMA 资产中心的单据审批权限，但不包括资产操作权限。

云通信

服务	作用范围	系统权限	权限类别	权限描述
语音通话（VoiceCall） （项目级服务）	区域级项目	RTC Administrator	角色	语音通话、消息&短信、隐私保护通话的所有执行权限。
消息&短信（MSGSMS） （项目级服务）	区域级项目	RTC Administrator	角色	语音通话、消息&短信、隐私保护通话的所有执行权限。
		MSGSMS FullAccess	策略	消息&短信服务普通用户权限，拥有该权限的用户可以拥有消息&短信支持的全部权限，包括创建、删除、查询、变更规格等操作。
		MSGSMS ReadOnlyAccess		消息&短信服务只读权限，拥有该权限的用户仅能查看消息&短信服务数据。
隐私保护通话（PrivateNumber） （项目级服务）	区域级项目	RTC Administrator	角色	语音通话、消息&短信、隐私保护通话的所有执行权限。
		PrivateNumber FullAccess	策略	隐私保护通话服务所有权限。
		PrivateNumber ReadOnlyAccess		隐私保护通话服务只读权限。

 版权所有 © 华为云计算技术有限公司

视频

服务	作用范围	系统权限	权限类别	权限描述
媒体处理（MPC） （项目级服务）	区域级项目	MPC Administrator	角色	媒体处理的所有执行权限。
视频点播服务（VOD） （项目级服务）	区域级项目	VOD Administrator	角色	视频点播服务里的所有操作权限，操作对象为所有的媒资文件。
		VOD Group Administrator		除全局配置以及域名管理以外的其他点播服务操作权限，操作对象为用户所在组创建的媒资文件。
		VOD Group Operator		具有除审核媒资、删除媒资、全局配置、域名管理以外的其他点播服务操作权限，操作对象为用户所在组创建的媒资文件。
		VOD Group Guest		仅具备查询媒资文件的权限，操作对象为用户所在组创建的媒资文件。
		VOD Operator		具有除审核媒资、全局配置、域名管理以外的其他点播服务操作权限，操作对象为用户所在组创建的视频文件。
		VOD Guest		视频点播服务只读权限。
		VOD FullAccess	策略	视频点播服务所有权限。
		VOD ReadOnlyAccess		视频点播服务只读权限。
		VOD CommonOperations		视频点播服务基本操作权限。具有除全局配置、域名管理、权限管理、审核设置、音视频托管以外的其他点播服务操作权限。
视频直播服务（Live） （项目级服务）	区域级项目	Live FullAccess	策略	视频直播服务所有权限。
		Live ReadOnlyAccess		视频直播服务只读权限。
实时音视频（RTC） （全局服	全局服务	RTC FullAccess	策略	实时音视频服务所有权限。
		RTC		实时音视频服务只读权限。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
务）		ReadOnlyAccess		

开发与运维

服务	作用范围	系统权限	权限类别	权限描述
软件开发生产线 CodeArts（项目级服务）	区域级项目	DevCloud Console FullAccess	策略	软件开发平台控制台所有权限。
		DevCloud Console ReadOnlyAccess		软件开发平台控制台只读权限。
需求管理 CodeArts Req（项目级服务）	区域级项目	ProjectMan ConfigOperations	策略	软件开发云项目配置的所有权限。
CodeArts IDE Online（项目级服务）	区域级项目	CloudIDE FullAccess	策略	CodeArts IDE Online 所有权限。
		CloudIDE ReadOnlyAccess		CodeArts IDE Online 只读权限。
		CloudIDE Development		CodeArts IDE Online 开发权限，包括查看、启动、停止、访问实例等操作。
		CloudIDE InstanceManagement		CodeArts IDE Online 实例管理权限，用户可以管理自己拥有的实例、访问被分发给自己的实例。

域名与网站

服务	作用范围	系统权限	权限类别	权限描述
云速建站	区域	CloudSite	策	云速建站服务所有权限。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
CloudSite（项目级服务）	级项目	FullAccess	略	
		CloudSite ReadOnlyAccess		云速建站服务只读权限。
		CloudSite CommonOperations		云速建站服务基本操作权限，包括查看和修改站点信息。

用户服务

服务	作用范围	系统权限	权限类别	权限描述
业务支撑系统（BSS）（项目级服务） 须知 授权时，除了全局服务外，需要授予其他所有区域的权限。	区域级项目	BSS Administrator	角色	费用中心、资源中心、账号中心的所有执行权限。
		BSS ReadonlyAccess	策略	费用中心、成本中心、消息中心的只读权限。
		BSS FinanceAccess		费用中心（BSS）财务管理员，拥有财务操作相关的所有权限。
		Enterprise Project BSS FullAccess		企业项目支持的所有运营权限。
企业项目管理服务（EPS）（全局级服务）	全局服务	EPS FullAccess	策略	企业项目管理服务所有权限。
		EPS ReadOnlyAccess		企业项目管理服务只读权限。
工单管理（Service Ticket）（全局级服务）	全局服务	Ticket Administrator	角色	工单管理的所有执行权限。
		Ticket Group Operator		该权限用于处理同组其他用户工单，以便协同办公。
专业服务（全局级服	所有项目	PSDMFullAccess	策略	专业服务交付管理平台的所有权限。

 版权所有 © 华为云计算技术有限公司

服务	作用范围	系统权限	权限类别	权限描述
务、项目级服务）		PSDMReadOnlyAccess		专业服务交付管理平台的只读权限。
网站备案（全局级服务）	全局服务	Beian Administrator	角色	备案服务管理员，拥有备案服务的所有执行权限。

其他

服务	作用范围	系统权限	权限类别	权限描述
消息中心（全局级服务）	全局服务	MessageCenter FullAccess	策略	消息中心所有权限。
		MessageCenter ReadOnlyAccess		消息中心只读权限。
		MessageCenter RecipientManagement		消息中心消息接收管理权限，包含消息接收配置、语音接收配置和接收人管理的查看和修改权限。

 版权所有 © 华为云计算技术有限公司

2 系统身份策略

默认情况下，管理员创建的 IAM 用户没有任何权限，在新版控制台中需要将策略附加至用户，或将其加入用户组后并授权，用户才能获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

云服务在 IAM 中预置了各云服务常用授权项集，统称为系统身份策略。管理员给用户授权时，可以直接使用这些系统身份策略，系统身份策略只能使用，不能修改。

如果管理员在 IAM 新版控制台给用户、用户组、委托或者信任委托授权时，无法找到特定服务的系统身份策略，原因是该服务暂时不支持 IAM，管理员可以通过**给对应云服务**提交工单，申请该服务在 IAM 预置权限。

如果系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项、资源、条件键等，创建自定义身份策略，并通过给身份实体授予自定义身份策略来进行精细的访问控制，自定义身份策略是对系统身份策略的扩展和补充。

全局

服务	系统权限	权限描述
全局服务	ReadOnlyPolicy	所有服务的只读权限策略。
全局服务	AdministratorAccessPolicy	所有服务的所有权限。 说明 所有服务指的是支持身份策略与信任委托的云服务列表中列举的云服务。

计算

服务	系统权限	权限描述
弹性云服务器（ECS）	ECSFullPolicy	弹性云服务器所有权限。
	ECSCommonOperationsPolicy	该用户具有查询、启动、停止、重启 ECS 云服务器，管理云服务器自动恢复动作，一键重置弹性云服务器密码，云服务器网

 版权所有 © 华为云计算技术有限公司

服务	系统权限	权限描述
		卡配置私有 IP，获取弹性云服务器 VNC 地址，使用云服务器磁盘配置信息，使用云服务器安全组，云服务器组管理，浮动 IP、密钥的所有权限，Windows 云服务器密码管理，获取控制台 VNC 地址，创建镜像，设置云服务器元数据，创建云服务器标签，使用云服务器卷，磁盘查询的所有权限，服务器网卡的查询权限，创建、查询、删除 IMS 镜像权限。
	ECSReadOnlyPolicy	弹性云服务器的只读访问权限。
	ECSPartnerOperationsPolicy	弹性云服务器伙伴权限。
裸金属服务器（BMS）	BMSFullPolicy	裸金属服务所有权限。
	BMSReadOnlyPolicy	裸金属服务查看权限。
	BMSCommonOperationsPolicy	裸金属服务器基本操作权限,包括开机、关机、重启、查询裸金属服务器详情、裸金属服务器挂载数据卷、裸金属服务器卸载数据卷等操作。
弹性伸缩（AS）	ASFullPolicy	弹性伸缩所有权限。
	ASReadOnlyPolicy	弹性伸缩的只读访问权限。
	ASServiceLinkedAgencyPolicy	弹性伸缩服务的服务关联委托。
镜像服务（IMS）	IMSFullAccessPolicy	镜像服务所有权限。
	IMSReadOnlyPolicy	镜像服务只读权限。
函数工作流（FunctionGraph）	FunctionGraphFullAccessPolicy	函数服务的所有权限。
	FunctionGraphReadOnlyPolicy	函数服务的只读权限。
	FunctionGraphCommonOperationsPolicy	函数调用者权限查询函数和触发器，以及调用函数的权限。
	FunctionGraphServiceLinkedAgencyPolicy	函数服务访问租户 VPC、挂载磁盘需要的委托权限。

存储

服务	系统权限	权限描述
对象存储服务	OBSBucketsViewerPol	只有对象存储服务查看桶列表、获取桶元

 版权所有 © 华为云计算技术有限公司

服务	系统权限	权限描述
（OBS）	icy	数据、查询桶位置权限，无其他权限。
	OBSFullAccessPolicy	对象存储服务管理员权限。
	OBSConsoleFullAccessPolicy	对象存储服务控制台使用所有权限。
	OBSBasicOperationsPolicy	具有对象存储服务查看桶列表、获取桶元数据、列举桶内对象、查询桶位置、上传对象、获取对象、删除对象、获取对象ACL 等对象基本操作权限。
	OBSReadOnlyPolicy	只有对象存储服务查看桶列表、获取桶元数据、列举桶内对象、查询桶位置权限，无其他权限。
云硬盘（EVS）	EVSFullAccessPolicy	云硬盘管理员权限，拥有该权限的用户可以操作并使用所有云硬盘、快照。
	EVSReadOnlyPolicy	云硬盘服务只读权限。
云备份（CBR）	CBRFullAccessPolicy	云备份管理员权限，拥有该权限的用户可以操作并使用所有存储库、备份和策略。
	CBRReadOnlyPolicy	云备份服务只读权限。
	CBRBackupsAndVaultsFullAccessPolicy	云备份服务普通用户(除策略创建、更新、删除外的所有权限)。
	CBRServiceLinkedAgencyPolicy	跨账号云备份服务的服务关联委托策略。
内容分发网络（CDN）	CDNLogsReadOnlyPolicy	对 CDN 日志服务只读权限。
	CDNSecurityProtectionConfigurationReadOnlyPolicy	对 CDN 安全服务只读权限。
	CDNRefreshAndPreheatPolicy	CDN 刷新预热权限。
	CDNAdministratorPolicy	对 CDN 的所有执行权限。
	CDNSecurityProtectionConfigurationPolicy	对 CDN 安全服务安全防护策略的创建、修改、删除、域名绑定和解绑的操作权限。
	CDNReadOnlyPolicy	对 CDN 所有服务具有读权限。
	CDNFullPolicy	对 CDN 的所有执行权限。
	CDNStatisticsReadOnlyPolicy	对 CDN 统计服务只读权限。

 版权所有 © 华为云计算技术有限公司

服务	系统权限	权限描述
	CDNSecurityProtectionStatisticsReadOnlyPolicy	对 CDN 安全防护统计的只读权限。
	CDNDomainConfigurationPolicy	对 CDN 加速域名的配置权限。
	CDNDomainReadOnlyPolicy	对 CDN 加速域名信息的只读权限。
	CDNChargeConfigurationPolicy	具有 CDN 计费服务开通、修改、查询计费模式权限。
	CDNStatisticsFullPolicy	对 CDN 统计服务的所有执行权限。
弹性文件服务（SFS）	SFSTurboFullAccessPolicy	弹性文件服务管理员权限，拥有该权限的用户可以操作并使用所有弹性文件系统。
	SFSTurboReadOnlyPolicy	弹性文件服务只读权限。

网络

服务	系统权限	权限描述
虚拟私有云（VPC）	VPCFullAccessPolicy	虚拟私有云所有权限。
	VPCReadOnlyPolicy	虚拟私有云只读权限。
	VPCConsoleFullAccessPolicy	虚拟私有云控制台所有权限。
	VPCConsoleReadOnlyPolicy	虚拟私有云控制台只读权限。
弹性负载均衡（ELB）	ELBFullAccessPolicy	弹性负载均衡服务所有权限。
	ELBReadOnlyAccessPolicy	弹性负载均衡服务只读权限。
NAT 网关（NAT）	NATFullAccessPolicy	NAT 网关服务所有权限。
	NATReadOnlyPolicy	NAT 网关服务只读权限。
云专线（DC）	DCAASFullAccessPolicy	云专线所有权限。
	DCAASReadOnlyPolicy	云专线只读权限。
虚拟专用网络（VPN）	VPNFullAccessPolicy	虚拟专用网络所有权限。
	VPNReadOnlyPolicy	虚拟专用网络只读权限。

 版权所有 © 华为云计算技术有限公司

服务	系统权限	权限描述
云解析服务（DNS）	DNSFullAccessPolicy	云解析服务管理员权限，拥有该权限的用户可以拥有云解析服务的全部权限，包括创建、删除、查询、修改等操作。
	DNSReadOnlyAccessPolicy	云解析服务只读权限，拥有该权限的用户仅能查看云解析服务资源。
VPC 终端节点（VPCEP）	VPCEPFullAccessPolicy	VPCEP 服务所有权限。
	VPCEPReadOnlyPolicy	VPCEP 服务只读权限。
云连接（CC）	CCFullAccessPolicy	云连接服务所有权限。
	CCReadOnlyPolicy	云连接服务只读权限。
企业路由器（ER）	ERFullAccessPolicy	企业路由器所有权限。
	ERReadOnlyPolicy	企业路由器只读权限。
弹性公网 IP（EIP）	EIPReadOnlyAccessPolicy	EIP 服务只读权限。
	EIPFullAccessPolicy	EIP 服务所有权限。
全球加速（GA）	GAFullAccessPolicy	全球加速所有权限。
	GAReadOnlyPolicy	全球加速只读权限。

容器

服务	系统权限	权限描述
云容器引擎（CCE）	CCEFullPolicy	云容器引擎服务所有权限。
	CCEReadOnlyPolicy	云容器引擎服务只读访问权限。
云容器实例（CCI）	CCIFullAccessPolicy	云容器实例服务所有权限。
	CCIReadOnlyPolicy	云容器实例服务只读访问权限。
容器镜像服务（SWR）	SWRReadOnlyAccessPolicy	容器镜像仓库只读权限。
	SWROperateAccessPolicy	容器镜像仓库操作权限。
	SWRFullAccessPolicy	容器镜像仓库所有权限。

 版权所有 © 华为云计算技术有限公司

安全与合规

服务	系统权限	权限描述
DDoS 高防	AADFullAccessPolicy	DDoS 高防服务所有权限。
	AADReadOnlyAccessPolicy	DDoS 高防服务只读权限，拥有该权限的用户仅能查看 DDoS 高防。
DDoS 原生高级防护（CNAD）	CNADFullAccessPolicy	CNAD 服务所有权限。
	CNADReadOnlyPolicy	CNAD 服务只读权限，拥有该权限的用户仅能查看 CNAD。
DDoS 原生基础防护（Anti-DDoS）	Anti-DDoSFullAccessPolicy	Anti-DDoS 服务所有权限。
	Anti-DDoSReadOnlyPolicy	Anti-DDoS 服务只读权限，拥有该权限的用户仅能查看 Anti-DDoS。
企业主机安全（HSS）	HSSServiceLinkedAgencyPolicy	跨账号企业主机安全服务关联委托策略。
	HSSFullAccessPolicy	企业主机安全服务的所有权限。
	HSSReadOnlyAccessPolicy	企业主机安全服务的只读访问权限。
	HSSAdministratorPolicy	企业主机安全服务管理员，拥有该服务下的所有权限。
数据库安全服务（DBSS）	DBSSReadOnlyPolicy	数据库安全服务只读权限。
	DBSSFullAccessPolicy	数据库安全服务所有权限。
	DBSSServiceLinkedAgencyPolicy	允许 DBSS 服务操作租户资源的服务关联委托策略。
密码安全中心（DEW）	KMSReadOnlyPolicy	KMS 的只读权限策略。
	KMSFullAccessPolicy	KMS 的所有权限策略。
	CSMSFullAccessPolicy	凭据管理服务所有权限。
	CSMSReadOnlyPolicy	凭据管理服务凭据只读权限。
	CSMSServiceLinkedAgencyPolicy	跨账号凭据管理服务关联委托策略。
	DHSMFullAccessPolicy	DHSM 的管理员权限策略。
	DHSMReadOnlyPolicy	DHSM 的只读权限策略。
	KPSFullAccessPolicy	密钥对管理服务所有权限。

 版权所有 © 华为云计算技术有限公司

服务	系统权限	权限描述
	KPSReadOnlyPolicy	密钥对管理服务密钥对只读权限。
Web 应用防火墙（WAF）	WAFReadOnlyAccessPolicy	web 应用防火墙只读权限。
	WAFFullAccessPolicy	web 应用防火墙管理员。
	WAFServiceLinkedAgencyPolicy	跨账号配置管理服务的服务关联委托策略。
云防火墙（CFW）	CFWFullAccessPolicy	云防火墙服务全部权限。
	CFWReadOnlyPolicy	云防火墙只读权限。
	CFWServiceLinkedAgencyPolicy	跨账号云防火墙服务关联委托策略。
SSL 证书管理（SCM） （全局级服务） (SCM 已合并到云证书管理服务 CCM)	SCMReadOnlyPolicy	SSL 证书管理服务只读权限。
	SCMFullPolicy	SSL 证书管理服务管理员权限。
云堡垒机（CBH）	CBHFullAccessPolicy	云堡垒机服务所有权限。
	CBHReadOnlyPolicy	云堡垒机服务只读权限。
	CBHServiceLinkedAgencyPolicy	云堡垒机服务访问租户密钥管理服务、凭据管理服务需要的委托权限。
数据安全中心（DSC）	DSCDashboardReadOnlyAccessPolicy	数据安全中心服务大屏只读权限。
	DSCFullAccessPolicy	数据安全中心服务所有权限。
	DSCReadOnlyAccessPolicy	数据安全中心服务只读权限。
	DSCServiceAgencyPolicy	数据安全中心服务委托策略。
	DSCServiceLinkedAgencyPolicy	DSC 实现跨账号资源查询或操作的服务关联委托策略。
云证书管理服务（CCM）	PCAFullAccessPolicy	私有证书管理服务所有权限。
	PCAReadOnlyPolicy	私有证书管理服务只读权限。
	PCAServiceLinkedAgencyPolicy	跨账号私有证书管理服务的服务关联委托策略。
安全云脑	SecMasterFullAccess	安全云脑管理员。

 版权所有 © 华为云计算技术有限公司

服务	系统权限	权限描述
（SecMaster）	SecMasterReadOnly	安全云脑只读访问权限。
	ServiceLinkedAgencyForSecMaster	安全云脑服务的服务关联委托策略。

管理与监管

服务	系统权限	权限描述
统一身份认证服务（IAM）	IAMFullAccessPolicy	统一身份认证服务的所有权限。
	IAMReadOnlyPolicy	统一身份认证服务的只读访问权限。
	AccessAnalyzerServiceLinkedAgencyPolicy	访问分析服务的服务关联委托策略。
云监控	CESReadOnlyPolicy	云监控服务只读权限。
	CESFullAccessPolicy	云监控服务所有权限。
	CESAgentServiceLinkedAgencyPolicy	云监控服务插件服务关联委托权限。
应用运维管理服务（AOM）	AOMFullAccessPolicy	应用运维管理服务所有权限策略。
	AOMReadOnlyPolicy	应用运维管理服务只读权限。
	AOMServiceLinkedAgencyPolicy	跨账号应用运维管理服务关联委托策略。
云审计服务（CTS）	CTSFullAccessPolicy	云审计服务所有权限策略。
	CTSReadOnlyPolicy	云审计服务只读权限。
	CTSServiceLinkedAgencyPolicy	跨账号云审计服务关联委托策略。
云日志服务（LTS）	LTSFullAccessPolicy	云日志服务所有权限策略。
	LTSReadOnlyAccessPolicy	云日志服务只读权限。
	LTSServiceLinkedAgencyPolicy	跨账号云日志服务的组织管理服务权限。
标签管理服务（TMS）	TMSReadOnlyPolicy	标签管理服务只读权限。
	TMSFullAccessPolicy	标签管理服务所有权限。
配置审计（Config）	ConfigReadOnlyPolicy	配置审计服务只读权限。
	ConfigFullAccessPolicy	配置审计服务所有权限。

 版权所有 © 华为云计算技术有限公司

服务	系统权限	权限描述
	ConfigConsoleFullAccessPolicy	配置审计服务控制台使用所有权限。
	RMSRemediationServiceLinkedAgencyPolicy	合规修正的服务关联委托策略。
	RMSServiceLinkedAgencyPolicy	跨账号配置管理服务的服务关联委托策略。
	RMSConformsServiceLinkedAgencyPolicy	合规包配置管理的服务关联委托策略。
资源访问管理（RAM）	RAMFullAccessPolicy	资源访问管理所有权限。
	RAMReadOnlyPolicy	资源访问管理只读权限。
	RAMResourceShareParticipantAccessPolicy	资源访问管理资源共享邀请处理权限。
IAM 身份中心（IAM IdentityCenter）	IdentityCenterFullAccessPolicy	IAM 身份中心管理员权限，拥有该权限的用户可以操作并使用所有 IAM 身份中心资源。
	IdentityCenterReadOnlyPolicy	IAM 身份中心只读权限。拥有该权限的用户仅能查看 IAM 身份中心服务数据。
	IdentityCenterServiceLinkedAgencyPolicy	IAM 身份中心服务委托策略。
组织（Organizations）	OrganizationsReadOnlyAccessPolicy	组织管理只读权限。
	OrganizationsFullAccessPolicy	组织管理所有权限。
	OrganizationsServiceLinkedAgencyPolicy	允许创建和删除服务关联委托。
资源编排服务（RFS）	RFFullAccessPolicy	资源编排服务所有权限。
	RFReadOnlyPolicy	资源编排服务只读权限。
	RFDeployPolicy	资源编排服务部署权限。
	RFStackSetFullAccessPolicy	资源编排资源栈集服务所有权限。
	RFStackSetReadOnlyPolicy	资源编排资源栈集服务只读权限。
资源治理中心（RGC）	RGCServiceLinkedAgencyPolicy	允许删除服务关联委托。

 版权所有 © 华为云计算技术有限公司

应用服务

服务	系统权限	权限描述
应用管理与运维平台（ServiceStage）	ServiceStageFullAccessPolicy	应用管理与运维平台（ServiceStage）所有权限。
	ServiceStageReadOnlyPolicy	应用管理与运维平台（ServiceStage）只读权限。
	ServiceStageDeveloperPolicy	应用管理与运维平台（ServiceStage）开发者权限，拥有应用、组件、环境的操作权限，但无审批权限和基础设施创建权限。
微服务引擎服务（CSE）	CSEFullAccessPolicy	微服务引擎服务所有权限。
	CSEReadOnlyPolicy	微服务引擎服务查看权限。
	CSEServiceLinkedAgencyPolicy	微服务引擎服务实例创建和维护需要的委托权限。
分布式缓存服务（DCS）	DCSFullAccessPolicy	分布式缓存服务所有权限。
	DCSUserAccessPolicy	分布式缓存服务普通用户权限（无实例创建、修改、删除、扩缩容）。
	DCSReadOnlyAccessPolicy	分布式缓存服务只读权限。
	DCSServiceLinkedAgencyPolicy	分布式缓存服务实例故障迁移需要的委托权限。
分布式消息服务（DMS Kafka、DMS RabbitMQ）	DMSFullAccessPolicy	分布式消息服务所有权限。
	DMSConsoleFullAccessPolicy	分布式消息服务控制台所有权限。
	DMSUserAccessPolicy	分布式消息服务普通用户权限（无实例创建、删除、扩容、开启转储的权限）。
	DMSReadOnlyAccessPolicy	分布式消息服务只读权限。
	DMSServiceLinkedAgencyPolicy	分布式消息服务服务关联委托策略。
消息通知服务（SMN）	SMNFullAccessPolicy	消息通知服务所有权限。
	SMNReadOnlyPolicy	消息通知服务只读权限。
API 网关（APIG）	APIGFullAccessPolicy	API 网关服务所有权限。
	APIGReadOnlyAccessPolicy	API 网关服务的只读访问权限。

数据库

服务	系统权限	权限描述

 版权所有 © 华为云计算技术有限公司

服务	系统权限	权限描述
关系型数据库（RDS）	RDSFullAccessPolicy	关系型数据库服务所有权限。
	RDSReadOnlyPolicy	关系型数据库服务只读权限。
	RDSServiceLinkedAgencyPolicy	跨账号配置管理服务的服务关联委托策略。
文档数据库服务（DDS）	DDSFullAccessPolicy	云数据库 DDS 服务的所有执行权限。
	DDSReadOnlyPolicy	云数据库 DDS 服务的只读访问权限。
	DDSServiceLinkedAgencyPolicy	跨账号配置管理服务的服务关联委托策略。
数据复制服务（DRS）	DRSFullAccessPolicy	DRS 的管理员权限，拥有这些权限的用户可以操作和使用 DRS 服务。
	DRSFullWithOutDeleteAccessPolicy	DRS 服务除结束和删除任务以外的权限。
	DRSReadOnlyAccessPolicy	DRS 服务的只读权限。
	DRSServiceLinkedAgencyPolicy	跨账号配置管理服务的服务关联委托策略。
云数据库 GeminiDB	GaussDBforNoSQLFullAccessPolicy	云数据库 GaussDBforNoSQL 服务的所有执行权限。
	GaussDBforNoSQLReadOnlyPolicy	云数据库 GaussDBforNoSQL 服务的只读访问权限。
	GaussDBforNoSQLServiceLinkedAgencyPolicy	跨账号配置管理服务的服务关联委托策略。
云数据库 GaussDB	GaussDBFullAccessPolicy	云数据库 GaussDB 服务的所有执行权限。
	GaussDBReadOnlyPolicy	云数据库 GaussDB 服务的只读访问权限。
	GaussDBServiceLinkedAgencyPolicy	跨账号配置管理服务的服务关联委托策略。
云数据库 GaussDB(for MySQL)	GaussDBforMySQLReadOnlyPolicy	云数据库 GaussDBforMySQL 服务的只读访问权限。
	GaussDBforMySQLFullAccessPolicy	云数据库 GaussDBforMySQL 服务的所有执行权限。
	GaussDBforMySQLServiceLinkedAgencyPolicy	跨账号配置管理服务的服务关联委托策略。

 版权所有 © 华为云计算技术有限公司

迁移

服务	系统权限	权限描述
主机迁移服务（SMS）	SMSFullAccessPolicy	授予 SMS 的所有权限。
	SMSReadOnlyPolicy	主机迁移服务只读权限。
对象存储迁移服务（OMS）	OMSFullAccessPolicy	对象存储迁移管理员权限，拥有该权限的用户可以创建、操作、查看服务所有功能。
	OMSReadOnlyPolicy	对象存储迁移服务只读权限。

人工智能

服务	系统权限	权限描述
ModelArts	ModelArtsFullAccessPolicy	ModelArts 服务所有权限。
	ModelArtsCommonOperationsPolicy	ModelArts 服务普通用户权限（不包括创建、更新、删除专属资源池）。
	ModelArtsDependencyAccessPolicy	ModelArts 服务的常用依赖服务的权限。
	OptVerseFullAccessPolicy	OptVerse 所有权限。
	OptVerseReadOnlyPolicy	OptVerse 只读权限。
	OptVerseTaskFullAccessPolicy	OptVerse 任务管理所有权限。
MapReduce 服务（MRS）	MRSFullAccessPolicy	MRS 的管理员权限，拥有这些权限的用户可以操作和使用 MRS 集群。
	MRSReadOnlyAccessPolicy	MRS 服务的只读权限。
数据仓库服务 GaussDB（DWS）	DWSFullAccessPolicy	数据仓库服务所有权限。
	DWSReadOnlyPolicy	数据仓库服务只读权限。
	DWSAccessVPCPolicy	DWS 服务获取 VPC 权限委托策略。
	DWSAccessOBSPolicy	DWS 服务获取 OBS 权限委托策略。
	DWSAccessLTSPolicy	DWS 服务获取 LTS 权限委托策略。
	DWSAccessKMSPolic	DWS 服务获取 KMS 权限委托策略。

 版权所有 © 华为云计算技术有限公司

服务	系统权限	权限描述
	y	
	DWSAccessDWSPolicy	DWS 服务获取 DWS 权限委托策略。
数据湖探索（DLI）	DLIFullAccessPolicy	数据湖探索所有权限。
	DLIReadOnlyPolicy	数据湖探索只读权限。
云搜索服务（CSS）	CSSFullAccessPolicy	云搜索服务的所有权限。
	CSSReadOnlyPolicy	云搜索服务的只读权限。
	CSSAccessVPCPolicy	CSS 服务获取 VPC 权限委托策略。
	CSSAccessOBSPolicy	CSS 服务获取 OBS 权限委托策略。
	CSSAccessELBPolicy	CSS 服务获取 ELB 权限委托策略。
	CSSAccessCSSLogstreamPolicy	CSS 服务获取 CSS 日志权限委托策略。

大数据

服务	系统权限	权限描述
数据湖探索（DLI）	DLIFullAccessPolicy	数据湖探索所有权限。
	DLIReadOnlyPolicy	数据湖探索只读权限。
数据治理中心（DataArts Studio）	DataArtsStudioReadOnlyPolicy	拥有对 DataArts Studio 实例及工作空间的所有管理权限，不具备工作空间内的业务操作权限和依赖服务权限。
	DataArtsStudioFullAccessPolicy	拥有对 DataArts Studio 实例及工作空间的普通操作权限，不具备工作空间内的业务操作权限和依赖服务权限。
	DataArtsStudioReadOnlyPolicy	拥有对 DataArts Studio 实例及工作空间的查看权限，不具备工作空间内的业务操作权限和依赖服务权限。

视频

服务	系统权限	权限描述
媒体处理（MPC）	MPCFullAccessPolicy	媒体处理服务所有权限。
	MPCReadOnlyPolicy	媒体处理服务只读权限。

 版权所有 © 华为云计算技术有限公司

服务	系统权限	权限描述
视频直播服务（Live）	LiveFullAccessPolicy	视频直播服务所有权限。
	LiveReadOnlyPolicy	视频直播服务只读权限。
数字内容生产线（MetaStudio）	MetaStudioFullAccessPolicy	数字内容产线服务所有权限。
	MetaStudioReadOnlyPolicy	数字内容产线服务只读权限。

IoT 物联网

服务	系统权限	权限描述
设备接入（IoTDA）	IoTDAFullAccessPolicy	设备接入服务的所有权限。
	IoTDAReadOnlyPolicy	设备接入服务的只读权限。

开发与运维

服务	系统权限	权限描述
软件开发生产线 CodeArts	CODEARTSFullAccessPolicy	软件开发平台控制台所有权限。
	CODEARTSReadOnlyPolicy	软件开发平台控制台只读权限。
流水线（CodeArts Pipeline）	CODEARTSPIPELINEFullAccessPolicy	流水线所有权限。
	CODEARTSPIPELINEReadOnlyPolicy	流水线只读权限。
	CODEARTSPIPELINETemplateFullAccessPolicy	流水线模板所有权限。
	CODEARTSPIPELINERuleFullAccessPolicy	流水线规则全部权限。
	CODEARTSPIPELINEStrategyFullAccessPolicy	流水线策略所有权限。
	CODEARTSPIPELINEExtensionFullAccessPolicy	流水线扩展插件所有权限。

 版权所有 © 华为云计算技术有限公司

用户服务

服务	系统权限	权限描述
业务支撑系统（Billing）	BILLINGFullAccessPolicy	费用中心、账号中心、成本中心、企业中心、消息中心的所有执行权限。一般为管理员使用。
	BILLINGOperatorPolicy	拥有费用中心、账号中心、成本中心、企业中心、消息中心的查询权限，可以对云服务做变更、管理、使用信息等查看处理，不提供财务相关功能。一般为开发人员、运维人员等技术使用。
	BILLINGFinancePolicy	财务相关的操作权限，可以提供支付、消费、发票、成本等财务相关功能，不提供云服务的变更等功能。一般为财经人员使用。
企业中心（BusinessUnitCenter）	BusinessUnitCenterFullAccessPolicy	企业中心的所有执行权限。一般为企业组织的管理人员使用。
	BusinessUnitCenterReadOnlyPolicy	企业中心的查询权限。一般为企业组织内的成员使用。
	BusinessUnitCenterMemberFinanceReadPolicy	企业中心企业主查看企业子财务信息所需要的委托权限。一般为企业组织的管理人员使用。
企业项目管理服务（EPS）	EPSReadOnlyPolicy	企业项目管理服务只读权限。
	EPSFullAccessPolicy	企业项目管理服务所有权限。
成本中心（CostCenter）	CostCenterFullAccessPolicy	成本中心的所有执行权限。一般为成本管理员、成本分析人员使用。
	CostCenterReadOnlyPolicy	成本中心的查询权限。一般为成本报告的查看人员。

 版权所有 © 华为云计算技术有限公司

3 身份策略授权参考

3.1 计算
3.2 存储
3.3 网络
3.4 容器
3.5 CDN 与智能边缘
3.6 数据库
3.7 安全与合规
3.8 人工智能
3.9 大数据
3.10 应用中间件
3.11 开发与运维
3.12 企业应用
3.13 视频
3.14 管理与监管
3.15 迁移
3.16 用户服务

3.1 计算

3.1.1 弹性伸缩 AS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

 版权所有 © 华为云计算技术有限公司

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务基于身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 AS 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中 AS 支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 AS 定义的条件键的详细信息请参见条件（Condition）。
- **“别名”**列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 AS 的相关操作。

表3-1 AS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
as:scalingGroup:create	授予创建弹性伸缩组的权限。	write	-	• g:EnterpriseProjectId • g:RequestTag/<t	as:groups:create

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ag-key> • g:TagKeys • as:ScalingConfigId • as:VpcId • as:VpcSubnetId • as:ElbPoolId • as:MaxInstanceSize • as:MinInstanceSize	
as:scalingGroup:delete	授予删除弹性伸缩组的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:groups:delete
as:scalingGroup:list	授予查询弹性伸缩组列表的权限。	list	-	g:EnterpriseProjectId	as:groups:list
as:scalingGroup:get	授予查询弹性伸缩组详情的权限。	read	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:groups:get
as:scalingGroup:update	授予修改弹性伸缩组的权限。	write	-	• g:EnterpriseProjectId • as:ScalingConfigId • as:VpcSubnetId • as:ElbPoolId • as:MaxInstanceSize • as:MinInstanceSize	as:groups:update
as:scalingGroup:resume	授予启用弹性伸缩组的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:groups:action
as:scalingGroup:pause	授予停用弹性伸缩组的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:groups:action
as:scalingCo	授予创建弹	write	-	• as:EcsInstanceId	as:configs:cr

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
nfig:create	性伸缩配置的权限。			• as:EcsInstanceType • as:EcsFlavorId • as:ImageId • as:ImsDiskImageId • as:CbrDiskSnapshotId • as:EcsServerGroupId • as:EvsEncrypted • as:KmsKeyId • as:EvsVolumeType • as:KpsSSHKeyPairName • as:AssociatePublicIp	eate
as:scalingConfig:delete	授予删除弹性伸缩配置的权限。	write	scalingConfig*	-	as:configs:delete
as:scalingConfig:batchDelete	授予批量删除弹性伸缩配置的权限。	write	scalingConfig*	-	as:configs:batchDelete
as:scalingConfig:list	授予查询弹性伸缩配置列表的权限。	list	scalingConfig*	-	as:configs:list
as:scalingConfig:get	授予查询弹性伸缩配置详情的权限。	read	scalingConfig*	-	as:configs:get
as:scalingGroup:batchAddInstances	授予批量添加弹性伸缩实例的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:instances:batchAction
as:scalingGroup:batchRemoveInstances	授予批量移除弹性伸缩实例的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:instances:batchAction

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
as:scalingGroup:batchSetInstancesProtect	授予批量设置弹性伸缩实例保护的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:instances:batchAction
as:scalingGroup:batchSetInstancesUnprotect	授予批量取消弹性伸缩实例保护的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:instances:batchAction
as:scalingGroup:batchSetInstancesStandby	授予批量设置弹性伸缩实例备用的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:instances:batchAction
as:scalingGroup:batchSetInstancesExitStandby	授予批量设置弹性伸缩实例取消备用的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:instances:batchAction
as:scalingGroup:deleteInstance	授予移除弹性伸缩实例的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:instances:delete
as:scalingGroup:listInstances	授予查询弹性伸缩实例列表的权限。	list	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:instances:list
as:scalingPolicy:create	授予创建弹性伸缩策略的权限。	write	-	g:EnterpriseProjectId	as:policies:create
as:scalingPolicy:list	授予查询弹性伸缩策略列表的权限。	list	-	g:EnterpriseProjectId	as:policies:list
as:scalingPolicy:get	授予查询弹性伸缩策略详情的权限。	read	scalingPolicy*	g:EnterpriseProjectId	as:policies:get
as:scalingPolicy:update	授予修改弹性伸缩策略的权限。	write	-	g:EnterpriseProjectId	as:policies:update
as:scalingPo	授予删除弹性伸缩策略	write	scalingPolic	g:EnterpriseProjectI	as:policies:d

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
licy:delete	的权限。		y*	d	elete
as:scalingPolicy:execute	授予手动执行弹性伸缩策略的权限。	write	scalingPolicy*	g:EnterpriseProjectId	as:policies:action
as:scalingPolicy:resume	授予启用弹性伸缩策略的权限。	write	scalingPolicy*	g:EnterpriseProjectId	as:policies:action
as:scalingPolicy:pause	授予停用弹性伸缩策略的权限。	write	scalingPolicy*	g:EnterpriseProjectId	as:policies:action
as:scalingPolicy:batchPause	授予批量停用弹性伸缩策略的权限。	write	scalingPolicy*	g:EnterpriseProjectId	as:policies:batchAction
as:scalingPolicy:batchResume	授予批量启用弹性伸缩策略的权限。	write	scalingPolicy*	g:EnterpriseProjectId	as:policies:batchAction
as:scalingPolicy:batchDelete	授予批量删除弹性伸缩策略的权限。	write	scalingPolicy*	g:EnterpriseProjectId	as:policies:batchAction
as:scalingPolicy:listAll	授予查询租户弹性伸缩策略列表的权限。	list	-	g:EnterpriseProjectId	as:policies:list
as:scalingGroup:listActivityLogs	授予查询伸缩活动日志列表的权限。	list	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:acivityLogs:list
as:scalingPolicy:listExecuteLogs	授予查询伸缩策略执行日志列表的权限。	list	scalingPolicy*	• g:EnterpriseProjectId	as:policyExecuteLogs:list
as::tagResource	授予创建标签的权限。	tagging	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key>	as:tags:set

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:TagKeys	
as::untagResource	授予删除标签的权限。	tagging	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys • g:TagKeys	as:tags:set
as::listTags	授予查询所有资源标签列表的权限。	list	-	-	as:tags:list
as::listTagsForResource	授予查询指定资源标签的权限。	list	-	g:EnterpriseProjectId	as:tags:get
as::listResourcesByTag	授予根据标签查询资源的权限。	list	-	• g:RequestTag/<tag-key> • g:TagKeys	as:tagResources:list
as:scalingGroup:createLifecycleHook	授予创建生命周期挂钩的权限。	write	-	g:EnterpriseProjectId	as:lifecycleHooks:create
as:scalingGroup:listLifecycleHooks	授予查询生命周期挂钩列表的权限。	list	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:lifecycleHooks:list
as:scalingGroup:getLifecycleHook	授予查询生命周期挂钩详情的权限。	read	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:lifecycleHooks:get
as:scalingGroup:updateLifecycleHook	授予修改生命周期挂钩的权限。	write	-	g:EnterpriseProjectId	as:lifecycleHooks:update
as:scalingGroup:deleteLifecycleHook	授予删除生命周期挂钩的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:lifecycleHooks:delete
as:scalingGroup:callbackInstanceHook	授予生命周期挂钩回调的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:instanceHooks:action

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
as:scalingGroup:listInstanceHooks	授予查询实例挂起信息列表权限。	list	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:instanceHooks:list
as:scalingGroup:createNotification	授予创建通知的权限。	write	scalingGroup*	• g:EnterpriseProjectId	as:notifications:set
as:scalingGroup:listNotifications	授予查询通知列表的权限。	list	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:notifications:list
as:scalingGroup:deleteNotification	授予删除通知的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	as:notifications:delete
as:scalingGroup:getQuotas	授予查询伸缩实例和伸缩策略配额的权限。	read	-	• g:EnterpriseProjectId	as:quotas:get
as::listQuotas	授予查询伸缩实例和伸缩策略配额的权限。	read	-	-	as:quotas:get
as:diagnosticReport:create	授予创建弹性伸缩智能诊断报告的权限。	write	-	-	-
as:diagnosticReport:list	授予弹性伸缩智能诊断报告的列表查询权限。	list	-	-	-
as:diagnosticReport:delete	授予删除弹性伸缩智能诊断报告的权限。	write	-	-	-

AS 的 API 通常对应着一个或多个授权项。表 3-2 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

 版权所有 © 华为云计算技术有限公司

表3-2 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /autoscaling-api/v1/{project_id}/scaling_group	as:scalingGroup:create	-
DELETE /autoscaling-api/v1/{project_id}/scaling_group/{scaling_group_id}	as:scalingGroup:delete	-
GET /autoscaling-api/v1/{project_id}/scaling_group	as:scalingGroup:list	-
GET /autoscaling-api/v1/{project_id}/scaling_group/{scaling_group_id}	as:scalingGroup:get	-
PUT /autoscaling-api/v1/{project_id}/scaling_group/{scaling_group_id}	as:scalingGroup:update	-
POST /autoscaling-api/v1/{project_id}/scaling_group/{scaling_group_id}/action	as:scalingGroup:resume	-
POST /autoscaling-api/v1/{project_id}/scaling_group/{scaling_group_id}/action	as:scalingGroup:pause	-
POST /autoscaling-api/v1/{project_id}/scaling_configurationCreateScalingConfig	as:scalingConfig:create	-
DELETE /autoscaling-api/v1/{project_id}/scaling_configuration/{scaling_configuration_id}	as:scalingConfig:delete	-
POST /autoscaling-api/v1/{project_id}/scaling_configurations	as:scalingConfig:batchDelete	-
GET /autoscaling-api/v1/{project_id}/scaling_configuration	as:scalingConfig:list	-
GET /autoscaling-api/v1/{project_id}/scaling_configuration/{scaling_configuration_id}	as:scalingConfig:get	-
POST /autoscaling-api/v1/{project_id}/scaling_group_instance/{scaling_group_id}/action	• as:scalingGroup:batchAddInstances • as:scalingGroup:batchSetInstancesProtect	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	• as:scalingGroup:batchRemoveInstances • as:scalingGroup:batchSetInstancesStandby • as:scalingGroup:batchSetInstancesUnprotect • as:scalingGroup:batchSetInstancesExitStandby	
DELETE /autoscaling-api/v1/{project_id}/scaling_group_instance/{instance_id}	as:scalingGroup:deleteInstance	-
GET /autoscaling-api/v1/{project_id}/scaling_group_instance/{scaling_group_id}/list	as:scalingGroup:listInstances	-
POST /autoscaling-api/v1/{project_id}/scaling_policy	as:scalingPolicy:create	-
GET /autoscaling-api/v1/{project_id}/scaling_policy/{scaling_group_id}/list	as:scalingPolicy:list	-
GET /autoscaling-api/v1/{project_id}/scaling_policy/{scaling_policy_id}	as:scalingPolicy:get	-
PUT /autoscaling-api/v1/{project_id}/scaling_policy/{scaling_policy_id}	as:scalingPolicy:update	-
DELETE /autoscaling-api/v1/{project_id}/scaling_policy/{scaling_policy_id}	as:scalingPolicy:delete	-
POST /autoscaling-api/v1/{project_id}/scaling_policy/{scaling_policy_id}/action	• as:scalingPolicy:resume • as:scalingPolicy:pause • as:scalingPolicy:execute	-
POST /autoscaling-api/v1/{project_id}/scaling_policies/action	as:scalingPolicy:batchDelete as:scalingPolicy:batchPause as:scalingPolicy:batchResume	-
POST /autoscaling-api/v2/{project_id}/scaling_policy	as:scalingPolicy:create	-
GET /autoscaling-api/v2/{project_id}/scaling_policy	as:scalingPolicy:listAll	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /autoscaling-api/v2/{project_id}/scaling_policy/{scaling_resource_id}/list	as:scalingPolicy:list	-
GET /autoscaling-api/v2/{project_id}/scaling_policy/{scaling_policy_id}	as:scalingPolicy:get	-
PUT /autoscaling-api/v2/{project_id}/scaling_policy/{scaling_policy_id}	as:scalingPolicy:update	-
GET /autoscaling-api/v1/{project_id}/scaling_activity_log/{scaling_group_id}	as:scalingGroup:listActivityLogs	-
GET /autoscaling-api/v2/{project_id}/scaling_activity_log/{scaling_group_id}	as:scalingGroup:listActivityLogs	-
GET /autoscaling-api/v1/{project_id}/scaling_policy_execute_log/{scaling_policy_id}	as:scalingPolicy:listExecuteLogs	-
POST /autoscaling-api/v1/{project_id}/{resource_type}/{resource_id}/tags/action	as::tagResource	-
POST /autoscaling-api/v1/{project_id}/{resource_type}/{resource_id}/tags/action	as::untagResource	-
GET /autoscaling-api/v1/{project_id}/{resource_type}/tags	as::listTags	-
GET /autoscaling-api/v1/{project_id}/{resource_type}/{resource_id}/tags	as::listTagsForResource	-
POST /autoscaling-api/v1/{project_id}/{resource_type}/resource_instances/action	as::listResourcesByTag	-
POST /autoscaling-api/v1/{project_id}/scaling_lifecycle_hook/{scaling_group_id}	as:scalingGroup:createLifecycleHook	-
GET /autoscaling-api/v1/{project_id}/scaling_lifecycle_hook/{scaling_group_id}/list	as:scalingGroup:listLifecycleHooks	-
GET /autoscaling-api/v1/{project_id}/scaling_lifec	as:scalingGroup:getLifecycleHook	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ycle_hook/{scaling_group_id}/{lifecycle_hook_name}		
PUT /autoscaling-api/v1/{project_id}/scaling_lifecycle_hook/{scaling_group_id}/{lifecycle_hook_name}	as:scalingGroup:updateLifecycleHook	-
DELETE /autoscaling-api/v1/{project_id}/scaling_lifecycle_hook/{scaling_group_id}/{lifecycle_hook_name}	as:scalingGroup:deleteLifecycleHook	-
PUT /autoscaling-api/v1/{project_id}/scaling_instance_hook/{scaling_group_id}/callback	as:scalingGroup:callbackInstanceHook	-
GET /autoscaling-api/v1/{project_id}/scaling_instance_hook/{scaling_group_id}/list	as:scalingGroup:listInstanceHooks	-
PUT /autoscaling-api/v1/{project_id}/scaling_notification/{scaling_group_id}	as:scalingGroup:createNotification	-
DELETE /autoscaling-api/v1/{project_id}/scaling_notification/{scaling_group_id}/{topic_urn}	as:scalingGroup:deleteNotification	-
GET /autoscaling-api/v1/{project_id}/scaling_notification/{scaling_group_id}	as:scalingGroup:listNotifications	-
GET /autoscaling-api/v1/{project_id}/quotas/{scaling_group_id}	as:scalingGroup:getQuotas	-
GET /autoscaling-api/v1/{project_id}/quotas	as::listQuotas	-
POST /autoscaling-api/v1/{project_id}/diagnostic-reports	as:diagnosticReport:create	-
GET /autoscaling-api/v1/{project_id}/diagnostic-reports	as:diagnosticReport:list	-
DELETE /autoscaling-api/v1/{project_id}/diagnostic-reports/{report_id}	as:diagnosticReport:delete	-

 版权所有 © 华为云计算技术有限公司

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的 URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

AS 定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-3 AS 支持的资源类型

资源类型	URN
scalingGroup	as:<region>:<account-id>:scalingGroup:<scaling-group-id>
scalingConfig	as:<region>:<account-id>:scalingConfig:<scaling-config-id>
scalingPolicy	as:<region>:<account-id>:scalingPolicy:<scaling-policy-id>

条件（Condition）

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 as:）仅适用于对应服务的操作，详情请参见表 4。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

AS 定义了以下可以在身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-4 AS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
as:ScalingConfigId	String	单值	指定特定伸缩配置创

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
			建虚拟机。
as:VpcId	String	单值	限制虚拟机使用的 VPC ID。
as:VpcSubnetId	String	多值	限制虚拟机使用的子网 ID。
as:ElbPoolId	String	多值	限制虚拟机加入的 ELB 后端服务器组 ID。
as:MaxInstanceSize	Integer	单值	限制伸缩组的最大实例数。
as:MinInstanceSize	Integer	单值	限制伸缩组的最小实例数。
as:EcsInstanceId	String	单值	限制指定已有实例创建伸缩配置。
as:EcsInstanceType	String	单值	限制创建虚拟机的类型：竞价 or 按需。
as:EcsFlavorId	String	多值	限制创建虚拟机使用的规格 Id。
as:ImageId	String	单值	限制创建虚拟机使用的镜像 Id。
as:ImsDiskImageId	String	多值	限制创建虚拟机使用的磁盘镜像 Id。
as:CbrDiskSnapshotId	String	多值	限制创建虚拟机使用的磁盘云备份 ID。
as:EcsServerGroupId	String	单值	限制创建虚拟机使用的云服务器组 ID。
as:EvsEncrypted	Boolean	单值	限制是否支持磁盘加密。
as:KmsKeyId	String	多值	限制磁盘加密使用的密钥 ID。
as:EvsVolumeType	String	多值	限制创建虚拟机使用的磁盘类型。
as:KpsSSHKeyPairName	String	单值	限制创建虚拟机使用的 keypair 名称。
as:AssociatePublicIp	Boolean	单值	限制虚拟机使用 eip。

 版权所有 © 华为云计算技术有限公司

3.1.2 裸金属服务器 BMS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指示每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 BMS 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 BMS 定义的条件键的详细信息请参见条件（Condition）。
- **“别名”**列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 BMS 的相关操作。

 版权所有 © 华为云计算技术有限公司

表3-5 BMS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
bms:servers:updateBaremetalServer	授予修改裸金属服务器的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	bms:servers:put
bms:servers:showBaremetalServerInterfaceAttachments	授予查询裸金属服务器网卡的权限。	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	bms:servers:get
bms:servers:resetServerPwd	授予一键重置裸金属服务器密码的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
bms:servers:showResetPasswordFlag	授予查询是否支持一键重置密码的权限。	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	bms:servers:get
bms:servers:showWindowsBaremetalServerPwd	授予获取Windows 裸金属服务器密码的权限。	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	bms:servers:get
bms:servers:deletePassword	授予 Windows 裸金属服务器清除密码的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
bms:servers:showBaremetalServerVolumeInfo	授予查询裸金属服务器挂载的云硬盘信息的权限。	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	bms:servers:get
bms:servers:create	授予创建裸金属服务器的权限。	write	-	• g:EnterpriseProjectId • g:TagKeys • g:RequestTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• bms:Flavorld • bms:VpcId • bms:SubnetId • bms:KmsKeyId • evs:Encrypted • bms:ImageId • bms:SSHKeyPairName • bms:AvailabilityZone • bms:VolumeType	
bms:servers:showBaremetalServer	授予查询单个裸机详情的权限。	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	bms:servers:get
bms:servers:attachVolume	授予裸金属服务器挂载云硬盘的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • bms:KmsKeyId • evs:Encrypted • bms:VolumeType • bms:VolumeId	-
bms:servers:detachVolume	授予裸金属服务器卸载指定云硬盘的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
bms:servers:updateMetadata	授予更新裸金属服务器元数	write	instance*	• g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	据的权限。			• g:ResourceTag/<tag-key>	
bms:servers:reInstallOS	授予重装裸金属服务器操作系统的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • bms:KmsKeyId • evs:Encrypted • bms:SSHKeyPairName	-
bms:servers:showBaremetalServerTags	授予查询裸金属服务器标签的权限。	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	bms:servers:get
bms:servers:start	授予批量启动裸金属服务器的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
bms:servers:reboot	授予批量重启裸金属服务器的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
bms:servers:stop	授予批量关机裸金属服务器的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
bms:servers:list	授予查询裸金属服务器详情列表的权限。	list	-	g:EnterpriseProjectId	-
bms:serverFlavors:get	授予查询规格详情和规格扩展信息列表的权限。	list	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
bms:serverQuotas:get	授予查询租户配额限制的权限。	read	-	-	-
bms:servers:batchCreateBaremetalServerTags	授予批量添加标签的权限。	write	instance*	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	bms:servers:put
bms:servers:batchDeleteBaremetalServerTags	授予批量删除标签的权限。	write	instance*	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	bms:servers:put
bms:servers:addNics	授予裸金属服务器绑定网卡的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • bms:SubnetId	-
bms:server:deleteNics	授予裸金属服务器解绑网卡的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
bms:servers:serialConsole	授予获取裸金属服务器远程登录地址的权限。	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
bms:server:updateInterface	授予修改裸金属服务器网卡属性的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

BMS 的 API 通常对应着一个或多个授权项。表 3-6 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

 版权所有 © 华为云计算技术有限公司

表3-6 API 与授权项的关系

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/baremetalservers/{server_id}	bms:servers:updateBaremetalServer	-
GET /v1/{project_id}/baremetalservers/{server_id}/os-interface	bms:servers:showBaremetalServerInterfaceAttachments	-
PUT /v1/{project_id}/baremetalservers/{server_id}/os-reset-password	bms:servers:resetServerPwd	-
GET /v1/{project_id}/baremetalservers/{server_id}/os-resetpwd-flag	bms:servers:showResetPasswordFlag	-
GET /v1/{project_id}/baremetalservers/{server_id}/os-server-password	bms:servers:showWindowsBaremetalServerPwd	-
DELETE /v1/{project_id}/baremetalservers/{server_id}/os-server-password	bms:servers:deletePassword	-
GET /v1/{project_id}/baremetalservers/{server_id}/os-volume_attachments	bms:servers:showBaremetalServerVolumeInfo	-
POST /v1/{project_id}/baremetalservers	bms:servers:create	-
GET /v1/{project_id}/baremetalservers/{server_id}	bms:servers:showBaremetalServer	-
POST /v1/{project_id}/baremetalservers/{server_id}/attachvolume	bms:servers:attachVolume	evs:volumes:use
DELETE /v1/{project_id}/baremetalservers/{server_id}/detachvolume/{attachment_id}	bms:servers:detachVolume	-
POST /v1/{project_id}/baremetalservers/{server_id}/metadata	bms:servers:updateMetadata	-
POST /v1/{project_id}/baremetalserve	bms:servers:reInstallOS	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
rs/{server_id}/reinstallos		
GET /v1/{project_id}/baremetalservers/{server_id}/tags	bms:servers:showBaremetalServerTags	-
POST /v1/{project_id}/baremetalservers/action	bms:servers:start	-
POST /v1/{project_id}/baremetalservers/action	bms:servers:reboot	-
POST /v1/{project_id}/baremetalservers/action	bms:servers:stop	-
GET /v1/{project_id}/baremetalservers/detail	bms:servers:list	-
GET /v1/{project_id}/baremetalservers/flavors	bms:serverFlavors:get	-
GET /v1/{project_id}/baremetalservers/limits	bms:serverQuotas:get	-
POST /v1/{project_id}/baremetalservers/{server_id}/tags/action	bms:servers:batchCreateBaremetalServerTags	-
POST /v1/{project_id}/baremetalservers/{server_id}/tags/action	bms:servers:batchDeleteBaremetalServerTags	-
POST /v1/{project_id}/baremetalservers/{server_id}/nics	bms:servers:addNics	-
POST /v1/{project_id}/baremetalservers/{server_id}/nics/delete	bms:server:deleteNics	-
POST /v1/{project_id}/baremetalservers/{server_id}/remote_console	bms:servers:serialConsole	-
PUT /v1/{project_id}/baremetalservers/{server_id}/os-interface/{port_id}	bms:server:updateInterface	-

 版权所有 © 华为云计算技术有限公司

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的 URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

BMS 定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-7 BMS 支持的资源类型

资源类型	URN
instance	bms:<region>:<account-id>:instance:<server-id>

条件（Condition）

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 bms:）仅适用于对应服务的操作，详情请参见表 4。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

BMS 支持的服务级条件键

BMS 定义了以下可以在身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-8 BMS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
bms:KmsKeyId	string	多值	根据请求参数中指定的加密密钥 ID 过滤访问。
bms:Flavorld	string	多值	根据请求参数中指定的规格 ID 过滤访

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
			问。
bms:VpcId	string	多值	根据请求参数中指定的网络 ID 过滤访问。
bms:SubnetId	string	多值	根据请求参数中指定的子网 ID 过滤访问。
bms:ImageId	string	单值	根据请求参数中指定的镜像 ID 过滤访问。
bms:SSHKeyPairName	string	单值	按请求中的 keyName 参数筛选访问。
bms:AvailabilityZone	string	单值	按请求中的 availabilityZone 参数筛选访问。
bms:VolumeType	string	多值	根据云硬盘的类型过滤访问。
bms:VolumeId	string	单值	根据指定的卷 ID 过滤访问。

3.1.3 弹性云服务器 ECS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

 版权所有 © 华为云计算技术有限公司

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 ECS 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 ECS 定义的条件键的详细信息请参见条件（Condition）。
- **“别名”**列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 ECS 的相关操作。

表3-9 ECS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ecs:cloudServers:createServers	授予创建 ECS 云服务器的权限。	write	-	• *g:RequestTag/<tag-key>* • *g:EnterpriseProjectId* • *g:TagKeys* • ecs:imageID • ecs:FlavorId • ecs:VpcId • ecs:SubnetId • ecs:PortId • ecs:KmsKeyId • ecs:AvailabilityZone • evs:Encrypted • cbr:VaultId • ecs:SSHKeyPa	ecs:cloudServers:create

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				irName • ecs:SupportAgentType • ecs:ImageSupportAgentType • ecs:ImageType • ecs:OsVersion • ecs:OsType • ecs:ImagePlatform	
ecs:cloudServers:deleteServers	授予删除 ECS 云服务器的权限。	write	instance *	-	ecs:cloudServers:delete
ecs:cloudServers:resize	授予变更云服务器规格的权限。	write	instance *	ecs:FlavorId	-
ecs:cloudServers:attachSharedVolume	授予批量挂载指定共享盘的权限。	write	instance *	• evs:Encrypted • ecs:KmsKeyId • ecs:VolumeId	-
ecs:cloudServers:showServer	授予查询云服务器详情的权限。	read	instance *	-	ecs:cloudServers:get
ecs:cloudServers:attach	授予云服务器挂载磁盘的权限。	write	instance *	• evs:Encrypted • ecs:KmsKeyId • ecs:VolumeId	-
ecs:cloudServers:showServerBlockDevice	授予查询弹性云服务器单个磁盘信息的权限。	read	instance *	-	ecs:cloudServers:get
ecs:cloudServers:updateServerBlockDevice	授予修改云服务器挂载的单个磁盘信息的权限。	write	instance *	-	ecs:cloudServers:put
ecs:cloudServers:changeOS	授予切换弹性云服务器操作系统的权限。	write	instance *	• ecs:imageID • evs:Encrypted • ecs:KmsKeyId • ecs:SSHKeyPairName	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• ecs:ImageType • ecs:OsVersion • ecs:OsType • ecs:ImagePlatform	
ecs:cloudServers:detachVolume	授予弹性云服务器卸载磁盘的权限。	write	instance *	-	-
ecs:cloudServers:updateMetadata	授予更新云服务器元数据的权限。	write	instance *	-	-
ecs:cloudServers:deleteMetadata	授予删除云服务器指定元数据的权限。	write	instance *	-	-
ecs:cloudServers:migrate	授予冷迁移云服务器的权限。	write	instance *	-	-
ecs:cloudServers:listServerInterfaces	授予查询云服务器网卡信息的权限。	list	instance *	-	ecs:cloudServers:get
ecs:cloudServers:showResetPasswordFlag	授予查询是否支持一键重置密码的权限。	read	instance *	-	ecs:cloudServers:get
ecs:cloudServers:showServerPassword	授予云服务器获取密码的权限。	read	instance *	-	ecs:cloudServers:get
ecs:cloudServers:deletePassword	授予云服务器清除密码的权限。	write	instance *	-	-
ecs:cloudServers:listServerVolumeAttachments	授予查询弹性云服务器挂载磁盘信息的权限。	list	instance *	-	ecs:cloudServers:get
ecs:cloudServers:rebuild	授予重装弹性云服务器操作系统的权限。	write	instance *	• evs:Encrypted • ecs:KmsKeyId • ecs:SSHKeyPairName	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ecs:cloudServers:vnc	授予获取VNC 远程登录地址的权限。	read	instance *	-	-
ecs:cloudServers:updateServer	授予修改弹性云服务器的权限。	write	instance *	-	ecs:cloudServers:put
ecs:cloudServers:addNics	授予批量添加云服务器网卡的权限。	write	instance *	• ecs:SubnetId • ecs:PortId	-
ecs:cloudServerNics:delete	授予批量删除云服务器网卡的权限。	write	instance *	-	-
ecs:cloudServers:showServerTags	授予查询云服务器标签的权限。	list	instance *	-	ecs:cloudServers:get
ecs:cloudServers:batchCreateServerTags	授予批量添加云服务器标签的权限。	write	instance *	• *g:RequestTag/<tag-key>* • *g:TagKeys*	• ecs:cloudServers:put • ecs:cloudServers:batchSetServerTags
ecs:cloudServers:batchDeleteServerTags	授予批量删除云服务器标签的权限。	write	instance *	• *g:RequestTag/<tag-key>* • *g:TagKeys*	• ecs:cloudServers:put • ecs:cloudServers:batchSetServerTags
ecs:cloudServers:start	授予批量启动云服务器的权限。	write	instance *	-	-
ecs:cloudServers:stop	授予批量关闭云服务器的权限。	write	instance *	-	-
ecs:cloudServers:reboot	授予批量重启云服务器的权	write	instance *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
ecs:cloudServers:batchUpdateServersName	授予批量修改弹性云服务器信息的权限。	write	instance *	-	ecs:cloudServers:put
ecs:cloudServers:listServersDetails	授予查询云服务器详情列表的权限。	list	-	*g:EnterpriseProjectId*	ecs:cloudServers:list
ecs:cloudServerFlavors:get	授予查询云服务器规格详情和扩展信息列表的权限。	read	-	-	-
ecs:cloudServerQuotas:get	授予查询租户配额的权限。	read	-	-	-
ecs:cloudServers:resetServerPwd	授予一键重置弹性云服务器密码的权限。	write	instance *	-	-
ecs:cloudServers:listServerGroups	授予查询云服务器组列表的权限。	list	-	-	ecs:cloudServers:list
ecs:cloudServers:createServerGroup	授予创建云服务器组的权限。	write	-	-	ecs:cloudServers:create
ecs:cloudServers:showServerGroup	授予查询云服务器组详情的权限。	read	-	-	ecs:cloudServers:get
ecs:cloudServers:deleteServerGroup	授予删除云服务器组的权限。	write	-	-	ecs:cloudServers:delete
ecs:cloudServers:addServerGroupMember	授予添加云服务器组成员的权限。	write	-	-	ecs:cloudServers:create
ecs:cloudServers:deleteServerGroupMember	授予删除云服务器组成员的权限。	write	-	-	ecs:cloudServers:delete
ecs:cloudServers:listResizeFlavors	授予查询云服务器规格变更支持列表的权	list	-	-	ecs:cloudServers:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
ecs:cloudServers:listServerTags	授予查询项目标签的权限。	list	-	-	ecs:cloudServers:list
ecs:cloudServers:changeVpc	授予切换云服务器的 VPC 的权限。	write	instance *		-
ecs:cloudServers:changeChargeMode	授予变更云服务器计费方式的权限。	write	instance *	-	-

ECS 的 API 通常对应着一个或多个授权项。表 3-10 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-10 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1.1/{project_id}/cloudservers	ecs:cloudServers:createServers	• eip:publicIps:create • eip:publicIps:associateInstance • iam:agencies:pass • eip:bandwidths:insertPublicIps
POST /v1/{project_id}/cloudservers	ecs:cloudServers:createServers	• eip:publicIps:create • eip:publicIps:associateInstance • iam:agencies:pass • eip:bandwidths:insertPublicIps
POST /v1/{project_id}/cloudservers/delete	ecs:cloudServers:deleteServers	-
POST /v1.1/{project_id}/cloudservers/{server_id}/resize	ecs:cloudServers:resize	-
POST /v1/{project_id}/batchaction/attachvolumes/{volume_id}	ecs:cloudServers:attachSharedVolume	evs:volumes:use

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/cloudservers/{server_id}	ecs:cloudServers:showServer	-
POST /v1/{project_id}/cloudservers/{server_id}/attachvolume	ecs:cloudServers:attach	evs:volumes:use
GET /v1/{project_id}/cloudservers/{server_id}/block_device	ecs:cloudServers:listServerBlockDevices	-
GET /v1/{project_id}/cloudservers/{server_id}/block_device/{volume_id}	ecs:cloudServers:showServerBlockDevice	-
PUT /v1/{project_id}/cloudservers/{server_id}/block_device/{volume_id}	ecs:cloudServers:updateServerBlockDevice	-
POST /v1/{project_id}/cloudservers/{server_id}/changeos	ecs:cloudServers:changeOS	-
DELETE /v1/{project_id}/cloudservers/{server_id}/detachvolume/{volume_id}	ecs:cloudServers:detachVolume	-
POST /v1/{project_id}/cloudservers/{server_id}/metadata	ecs:cloudServers:updateMetadata	iam:agencies:pass
DELETE /v1/{project_id}/cloudservers/{server_id}/metadata/{key}	ecs:cloudServers:deleteMetadata	-
POST /v1/{project_id}/cloudservers/{server_id}/migrate	ecs:cloudServers:migrate	-
GET /v1/{project_id}/cloudservers/{server_id}/os-interface	ecs:cloudServers:listServerInterfaces	-
PUT /v1/{project_id}/cloudservers/{server_id}/os-reset-password	ecs:cloudServers:resetServerPwd	-
GET /v1/{project_id}/cloudservers/{server_id}/os-resetpwd-flag	ecs:cloudServers:showResetPasswordFlag	-
GET	ecs:cloudServers:showServerPas	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/cloudservers/{server_id}/os-server-password	sword	
DELETE /v1/{project_id}/cloudservers/{server_id}/os-server-password	ecs:cloudServers:deletePassword	-
GET /v1/{project_id}/cloudservers/{server_id}/os-volume_attachments	ecs:cloudServers:listServerVolumeAttachments	-
POST /v1/{project_id}/cloudservers/{server_id}/reinstallos	ecs:cloudServers:rebuild	-
POST /v2/{project_id}/cloudservers/{server_id}/reinstallos	ecs:cloudServers:rebuild	-
POST /v1/{project_id}/cloudservers/{server_id}/remote_console	ecs:cloudServers:vnc	-
POST /v1/{project_id}/cloudservers/{server_id}/resize	ecs:cloudServers:resize	-
GET /v1/{project_id}/cloudservers/detail?flavor={flavor}&name={name}&status={status}&limit={limit}&offset={offset}&not-tags={not-tags}&reservation_id={reservation_id}&enterprise_project_id={enterprise_project_id}&tags={tags}&ip={ip}	ecs:cloudServers:listServersDetails	-
PUT /v1/{project_id}/cloudservers/{server_id}	ecs:cloudServers:updateServer	-
POST /v1/{project_id}/cloudservers/{server_id}/actions/update-auto-terminate-time	ecs:cloudServers:setAutoTerminateTime	-
POST /v1/{project_id}/cloudservers/{server_id}/nics	ecs:cloudServers:addNics	-
POST /v1/{project_id}/cloudservers/	ecs:cloudServerNics:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
{server_id}/nics/delete		
GET /v1/{project_id}/cloudservers/{server_id}/tags	ecs:cloudServers:showServerTags	-
POST /v1/{project_id}/cloudservers/{server_id}/tags/action	ecs:cloudServers:batchCreateServerTags	-
POST /v1/{project_id}/cloudservers/{server_id}/tags/action	ecs:cloudServers:batchDeleteServerTags	-
POST /v1/{project_id}/cloudservers/action	ecs:cloudServers:start	-
POST /v1/{project_id}/cloudservers/action	ecs:cloudServers:stop	-
POST /v1/{project_id}/cloudservers/action	ecs:cloudServers:reboot	-
GET /v1/{project_id}/cloudservers/flavors?availability_zone={availability_zone}&flavor_id={flavor_id}&limit={limit}&marker={marker}	ecs:cloudServerFlavors:get	-
GET /v1/{project_id}/cloudservers/limits	ecs:cloudServerQuotas:get	-
PUT /v1/{project_id}/cloudservers/{server_id}/os-reset-password	ecs:cloudServers:resetServerPwd	-
GET /v1/{project_id}/cloudservers/os-server-groups?limit={limit}&marker={marker}	ecs:cloudServers:listServerGroups	-
POST /v1/{project_id}/cloudservers/os-server-groups	ecs:cloudServers:createServerGroup	-
GET /v1/{project_id}/cloudservers/os-server-groups/{server_group_id}	ecs:cloudServers:showServerGroup	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /v1/{project_id}/cloudservers/os-server-groups/{server_group_id}	ecs:cloudServers:deleteServerGroup	-
POST /v1/{project_id}/cloudservers/os-server-groups/{server_group_id}/action	ecs:cloudServers:addServerGroupMember	-
POST /v1/{project_id}/cloudservers/os-server-groups/{server_group_id}/action	ecs:cloudServers:deleteServerGroupMember	-
GET /v1/{project_id}/cloudservers/resize_flavors?instance_uuid={instance_uuid}&source_flavor_id={source_flavor_id}&source_flavor_name={source_flavor_name}	ecs:cloudServers:listResizeFlavors	-
GET /v1/{project_id}/cloudservers/tags	ecs:cloudServers:listServerTags	-
POST /v2/{project_id}/cloudservers/{server_id}/changeos	ecs:cloudServers:changeOS	-
PUT /v1/{project_id}/cloudservers/server-name	ecs:cloudServers:batchUpdateServersName	-
POST /v1/{project_id}/cloudservers/{server_id}/changevpc	ecs:cloudServers:changeVpc	-
POST /v1/{project_id}/cloudservers/actions/change-charge-mode	ChangeServerChargeMode	• billing:order:pay • billing:subscription:renew
GET /v2/{domain_id}/auto-launch-groups	ecs:launchTemplates:list	-
DELETE /v2/{domain_id}/auto-launch-groups/{auto_launch_group_id}	ecs:launchTemplates:delete	-
POST /v2/{domain_id}/auto-launch-groups	ecs:launchTemplates:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v2/{domain_id}/auto-launch-groups/{auto_launch_group_id}	ecs:launchTemplates:update	-
GET /v1/{project_id}/cloudservers/flavor-sell-policies?flavor_id={flavor_id}	ecs:cloudServerFlavors:get	-
GET /v1/{project_id}/cloudservers/{server_id}/autorecovery	ecs:cloudServers:getAutoRecovery	-
PUT /v1/{project_id}/cloudservers/{server_id}/autorecovery	ecs:cloudServers:setAutoRecovery	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-11 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

ECS 定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-11 ECS 支持的资源类型

资源类型	URN
instance	ecs:<region>:<account-id>:instance:<server-id>

条件（Condition）

条件键概述

条件键（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 ecs:）仅适用于对应服务的操作，详情请参见表 3-12。

 版权所有 © 华为云计算技术有限公司

- 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。

- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

ECS 支持的服务级条件键

ECS 定义了以下可以在身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化策略语句应用的条件。

表3-12 ECS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
ecs:imageID	string	多值	根据请求参数中指定的镜像 ID 过滤访问。
ecs:FlavorId	string	多值	根据请求参数中指定的规格 ID 过滤访问。
ecs:VpcId	string	多值	根据请求参数中指定的网络 ID 过滤访问。
ecs:SubnetId	string	多值	根据请求参数中指定的子网 ID 过滤访问。
ecs:KmsKeyId	string	多值	根据请求参数中指定的加密密钥 ID 过滤访问。
ecs:ServerId	string	单值	根据云服务器 ID 过滤访问。
ecs:SSHKeyPairName	string	单值	根据请求参数中指定的 SSH 密钥对的名称过滤访问。
ecs:AvailabilityZone	string	单值	根据请求参数中指定的可用区名称过滤访问。
ecs:PortId	string	多值	根据请求参数中指定的 portId 过滤访问。
ecs:SupportAgentType	string	多值	根据请求中指定的 agent 类型过滤访问。
ecs:ImageSupportAgentType	string	多值	根据请求中指定的镜像支持的 agent 类型过滤访问。

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
ecs:VolumeId	string	单值	根据请求中指定的卷 ID 过滤访问。
ecs:ImageType	string	单值	根据请求中指定镜像的类型过滤访问（如：公共镜像、私有镜像、共享镜像、市场镜像）。
ecs:OsType	string	单值	根据请求中指定镜像的操作系统类型过滤访问（如：Linux、Windows）。
ecs:OsVersion	string	单值	根据请求中指定镜像的操作系统版本过滤访问（如：CentOS 7.3 64bit）。
ecs:ImagePlatform	string	单值	根据请求中指定镜像的平台过滤访问（如：Windows、Ubuntu、Red Hat、SUSE、CentOS）。
ecs:LegacyAPIFlavor	string	单值	根据请求的 API 类型过滤访问（当前仅支持 OpenStackNative）。

3.1.4 镜像服务 IMS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。

 版权所有 © 华为云计算技术有限公司

- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指示每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 IMS 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 IMS 定义的条件键的详细信息请参见条件（Condition）。
- **“别名”**列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 IMS 的相关操作。

表3-13 IMS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ims:images:list	查看所有镜像列表。	list	-	g:EnterpriseProjectId	-
ims:images:get	查看用户指定镜像详情。	read	image *	-	-
ims:images:create	创建镜像元数据。	write	-	• g:RequestTag/<tag-key> • g:TagKeys	-
ims:images:share 说明 不推荐使用“ims:images:share”授权项分享已经存在镜像，	分享已经存在镜像。	permission_management	image *	• ims:TargetOrgPaths • g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
建议使用 • ims:images:addMember • ims:images:deleteMember • ims:images:updateMemberStatus					
ims:images:copyInRegion	区域内复制已经存在镜像。	write	image *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • ims:Encrypted	ims:images:copy
ims:images:copyCrossRegion	跨区域复制已经存在镜像。	write	image *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • ims:Region • ims:VaultId • g:RequestedRegion	ims:images:copy
ims:quotas:get	查询镜像配额。	read	-	-	-
ims:images:upload	上传镜像。	write	image *	-	-
ims:wholeImages:create	制作整机镜像。	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys • ims:Encrypted • ims:OriginBucketOrgPaths • ims:SourceAvailabilityZone • ims:InstanceId • ims:VaultId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• ims:BackupId	
ims:images:export	导出镜像。	read	image *	-	-
ims:dataImages:create	使用外部镜像文件制作数据镜像。	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	-
ims:serverImages:create	制作镜像。	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys • ims:Encrypted • ims:OriginBucketOrgPaths • ims:SourceAvailabilityZone • ims:InstanceId • ims:VolumeId	-
ims:images:setTags	更新镜像标签。	tagging	image *	• g:RequestTag/<tag-key> • g:TagKeys	ims:images:update
ims:images:getTags	查询镜像标签。	read	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	ims:images:list
ims:images:deleteImage	删除镜像。	write	image *	-	ims:images:update
ims:images:updateImage	更新镜像信息。	write	image *	-	-
ims:images:listOsVersion	查看所有镜像支持的 OS 列表权限。	list	-	-	ims:images:list
ims:images:getJob	查询异步任务进度。	read	-	-	ims:images:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ims:images:import	镜像导入。	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	-
ims:images:setOrDeleteTags	批量增加或删除镜像上标签。	write	-	• g:RequestTag/<tag-key> • g:TagKeys	-
ims:images:updateMemberStatus	更新镜像成员状态。	write	image *	g:RequestTag/<tag-key>	ims:images:share
ims:images:addMember	添加镜像成员。	write	image *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • ims:TargetOrgPaths	ims:images:share
ims:images:deleteMember	删除镜像成员。	write	image *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	ims:images:share
ims:images:listImagesByTag	按标签查询镜像。	read	-	-	ims:images:list
ims:images:showImageTags	查询镜像标签。	read	image *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	ims:images:list
ims:images:listImageTags	查询项目标签。	list	-	-	-

IMS 的 API 通常对应着一个或多个授权项。表 3-14 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-14 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v2/cloudimages	ims:images:list	-
GET /v2/images/{image_id}	ims:images:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v2/images	ims:images:create	-
POST /v2/images/{image_id}/members	ims:images:share	ims:images:get
POST /v1/cloudimages/{image_id}/copy	ims:images:copyInRegion	ims:serverImages:create
POST /v1/cloudimages/{image_id}/cross_region_copy	ims:images:copyCrossRegion	-
GET /v1/cloudimages/quota	ims:quotas:get	-
PUT /v1/cloudimages/{image_id}/upload PUT /v2/images/{image_id}/file	ims:images:upload	• ims:images:get • ims:images:update
POST /v1/cloudimages/wholeimages/action	ims:wholeImages:create	-
POST /v1/cloudimages/{image_id}/file	ims:images:export	• obs:object:GetObject • obs:object:PutObject
• POST /v2/cloudimages/quickimport/action（仅快速导入数据盘镜像需要此授权项） • POST /v1/cloudimages/dataimages/action	ims:dataImages:create	-
• PATCH /v2/cloudimages/{image_id}（仅企业项目迁移需要此授权项） • POST /v2/cloudimages/action • OST /v2/cloudimages/quickimport/action（仅快速导入系统盘镜像需要此授权项） • POST /v1/cloudimages/{image_id}/copy（仅开通企业项目用户需要此授权项）	ims:serverImages:create	-
PUT /v1/cloudimages/tags	ims:images:setTags	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/cloudimages/tags	ims:images:getTags	-
DELETE /v2/images/{image_id}	ims:images:deleteImage	-
• PATCH /v2/cloudimages/{image_id} • PATCH /v2/images/{image_id}	ims:images:updateImage	-
GET /v1/cloudimages/os_version	ims:images:listOsVersion	-
GET /v1/cloudimages/job/{job_id}	ims:images:getJob	-
POST /v2/cloudimages/quickimport/action	ims:images:import	• ims:dataImages:create • ims:serverImages:create
POST /v2/{project_id}/images/{image_id}/tags/action	ims:images:setOrDeleteTags	• ims:images:setTags • ims:images:deleteTags
• PUT /v1/cloudimages/members • PUT /v2/images/{image_id}/members/{member_id}	ims:images:updateMemberStatus	-
POST /v1/cloudimages/members	ims:images:addMember	-
DELETE /v1/cloudimages/members	ims:images:deleteMember	-
POST /v2/{project_id}/images/resource_instances/action	ims:images:listImagesByTag	-
GET /v2/{project_id}/images/{image_id}/tags	ims:images:showImageTags	-
GET /v2/{project_id}/images/tags	ims:images:listImageTags	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-15 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的策略语句中指定该资源的 URN，策略仅作用于此资源；如未指定，Resource 默认为“*”，则策略将应用到所有资源。您也可以在策略中设置条件，从而指定资源类型。

 版权所有 © 华为云计算技术有限公司

IMS 定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-15 IMS 支持的资源类型

资源类型	URN
image	ims:<region>:<account-id>:image:<image-id>

- <region>：指定授权的区域，，表示授权在此区域进行相关操作。
- <account-id>：指定授权的用户账号 ID，表示授权在此账号 ID 下进行相关操作。请在 API 凭证中获取账号 ID。
- <image-id>：镜像 ID，表示授权对此镜像进行相关操作。

说明

资源路径 URN 支持通配符号*表示所有。

条件（Condition）

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀为服务缩写，如 ims:）仅适用于对应服务的操作，详情请参见表 3-16。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

IMS 定义了以下可以在身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化策略语句应用的条件。

表3-16 ims 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
ims:TargetOrgPaths	string	多值	根据指定的共享账号的 Organizations Path 过滤访问。
ims:Encrypted	boolean	单值	根据镜像是否加密对镜像导入和复制等操作进行控制。

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
ims:TargetBucketOrgPaths	string	多值	根据指定的目标桶 owner 账号的 Organizations Path 过滤访问。
ims:OriginBucketOrgPaths	string	多值	根据指定的源桶 owner 账号账号的 Organizations Path 过滤访问。
ims:SourceAvailabilityZone	string	多值	根据指定的可用区过滤访问。
ims:InstanceId	string	单值	根据指定的虚拟机 ID 对创建镜像创建整机镜像操作进行控制。
ims:VaultId	string	单值	根据指定的存储库 ID 对整机镜像的创建及跨区域复制操作进行控制。
ims:VolumeId	string	多值	根据指定的卷 ID 对创建镜像操作进行控制。
ims:BackupId	string	单值	根据指定的备份 ID 对创建整机镜像操作进行控制。
ims:Region	string	单值	根据指定的目标 region 对跨区域复制操作进行控制。

3.1.5 函数工作流 FunctionGraph

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

 版权所有 © 华为云计算技术有限公司

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下的相关操作。

表3-17 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
functiongraph:function:createFunction	授予权限以创建函数。	Write	function *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• functiongraph:function:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
functiongraph:function:deleteFunction	授予权限以删除函数。	Write	function *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• functiongraph:function:delete
			-	• g:RequestTag/<tag-key>	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:TagKeys	
functiongraph:function:listFunctions	授予权限以查询函数列表。	List	function *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• functiongraph:function:list
			-	• g:RequestTag/<tag-key> • g:TagKeys	
functiongraph:function:getFunctionCode	授予权限以获取指定函数代码信息。	Read	function *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• functiongraph:function:getCode
			-	• g:RequestTag/<tag-key> • g:TagKeys	
functiongraph:function:updateFunctionCode	授予权限以修改指定的函数的代码。	Write	function *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• functiongraph:function:updateCode
			-	• g:RequestTag/<tag-key> • g:TagKeys	
functiongraph:function:getFunctionConfig	授予权限以获取指定函数的metadata。	Read	function *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• functiongraph:function:getConfig
			-	• g:RequestTag/<tag-key> • g:TagKeys	
functiongraph:function:updateFunctionConfig	授予权限以修改指定的函数的 metadata 信息。	Write	function *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• functiongraph:function:updateConfig

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	• g:RequestTag/<tag-key> • g:TagKeys	
functiongraph:function:updateMaxInstanceConfig	授予权限以更新函数最大实例数。	Write	function *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• functiongraph:function:updateConfig
			-	• g:RequestTag/<tag-key> • g:TagKeys	
functiongraph:function:updateSnapshot	授予权限以启动/禁用函数快照。	Write	function *	g:EnterpriseProjectId	• functiongraph:function:updateConfig
functiongraph:function:getSnapshotState	授予权限以查询函数快照制作状态。	Read	function *	g:EnterpriseProjectId	• functiongraph:function:updateConfig
functiongraph:function:createUrl	授予权限以创建函数 URL。	Write	function *	g:EnterpriseProjectId	• functiongraph:function:updateConfig
functiongraph:function:deleteUrl	授予权限以删除函数 URL。	Write	function *	g:EnterpriseProjectId	• functiongraph:function:updateConfig
functiongraph:function:updateUrl	授予权限以更新函数 URL。	Write	function *	g:EnterpriseProjectId	• functiongraph:function:updateConfig
functiongraph:function:getUrl	授予权限以获取指定函数的 URL。	Read	function *	g:EnterpriseProjectId	• functiongraph:function:updateConfig
functiongraph::getResourceInstance	授予权限以查询资源实例。	Read	-	g:EnterpriseProjectId	• functiongraph:function:updateConfig
functiongraph::createTag	授予权限以创建资源标签。	Tagging	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	• functiongraph:function:updateConfig

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
functiongraph::deleteTag	授予权限以删除资源标签。	Tagging	-	g:EnterpriseProjectId	• functiongraph:function:updateConfig
functiongraph::listTags	授予权限以获取资源标签列表。	List	-	g:EnterpriseProjectId	• functiongraph:function:updateConfig
functiongraph::createFunctionApp	授予权限以创建应用程序。	Write	-	g:EnterpriseProjectId	• functiongraph:function:list
functiongraph::deleteFunctionApp	授予权限以删除应用程序。	Write	-	g:EnterpriseProjectId	• functiongraph:function:delete
functiongraph::getFunctionApp	授予权限以查询应用程序详情。	Read	-	g:EnterpriseProjectId	• functiongraph:function:list
functiongraph::listFunctionApps	授予权限以查询应用程序列表。	List	-	g:EnterpriseProjectId	• functiongraph:function:list
functiongraph::getFunctionAppTemplate	授予权限以查询应用程序模板详情。	Read	-	g:EnterpriseProjectId	• functiongraph:function:list
functiongraph::listFunctionAppTemplates	授予权限以查询应用程序模板列表。	List	-	g:EnterpriseProjectId	• functiongraph:function:list
functiongraph::createVpcEndpoint	授予权限以创建下沉入口。	Write	-	g:EnterpriseProjectId	• functiongraph:function:updateConfig
functiongraph::deleteVpcEndpoint	授予权限以删除下沉入口。	Write	-	g:EnterpriseProjectId	• functiongraph:function:delete
functiongraph:function:export	授予权限以导出函数。	Read	function *	g:EnterpriseProjectId	• functiongraph:function:getconfig
functiongraph:function:import	授予权限以导入函数。	Write	function *	g:EnterpriseProjectId	• functiongraph:function:create
functiongraph::	授予权限以导	Read	-	g:EnterprisePro	• functiongraph:function:li

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
exportPackage	出函数应用。			jectId	st
functiongraph::importPackage	授予权限以导入函数应用。	Write	-	g:EnterpriseProjectId	• functiongraph:function:create
functiongraph:function:createVersion	授予权限以发布函数版本。	Write	function *	g:EnterpriseProjectId	-
functiongraph:function:listVersion	授予权限以获取指定函数的版本列表。	List	function *	g:EnterpriseProjectId	-
functiongraph:function:createAlias	授予权限以创建函数灰度版本别名。	Write	function *	g:EnterpriseProjectId	-
functiongraph:function:deleteAlias	授予权限以删除函数版本别名。	Write	function *	g:EnterpriseProjectId	-
functiongraph:function:listAlias	授予权限以获取指定函数所有版本别名列表。	List	function *	g:EnterpriseProjectId	-
functiongraph:function:getAlias	授予权限以获取函数版本指定别名信息。	Read	function *	g:EnterpriseProjectId	-
functiongraph:function:updateAlias	授予权限以修改函数版本别名信息。	Write	function *	g:EnterpriseProjectId	-
functiongraph::listQuota	授予权限以查询租户配额。	List	-	-	• functiongraph:function:list
functiongraph:dependency:createDependency	授予权限以创建依赖包。	Write	-	-	• functiongraph:function:create
functiongraph:dependency:deleteDependency	授予权限以删除依赖包。	Write	-	-	• functiongraph:function:delete
functiongraph:dependency:listD	授予权限以获取依赖包列	List	-	-	• functiongraph:function:li

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ependencies	表。				st
functiongraph:dependency:getDependency	授予权限以获取指定依赖包信息。	Read	-	-	• functiongraph:function:getcode
functiongraph:dependency:updateDependency	授予权限以更新指定依赖包信息。	Write	-	-	• functiongraph:function:updatecode
functiongraph:dependency:createDependencyVersion	授予权限以创建依赖包版本。	Write	-	-	• functiongraph:function:create
functiongraph:dependency:deleteDependencyVersion	授予权限以删除依赖包版本。	Write	-	-	• functiongraph:function:delete
functiongraph:dependency:listDependencyVersion	授予权限以获取依赖包版本列表。	List	-	-	• functiongraph:function:list
functiongraph:dependency:getDependencyVersion	授予权限以获取依赖包版本详细信息。	Read	-	-	• functiongraph:function:getcode
functiongraph:function:createEvent	授予权限以创建测试事件。	Write	function *	g:EnterpriseProjectId	• functiongraph:function:invoke
functiongraph:function:deleteEvent	授予权限以删除指定测试事件。	Write	function *	g:EnterpriseProjectId	• functiongraph:function:invoke
functiongraph:function:updateEvent	授予权限以更新函数测试事件。	Write	function *	g:EnterpriseProjectId	• functiongraph:function:invoke
functiongraph:function:listEvent	授予权限以获取函数测试事件列表。	List	function *	g:EnterpriseProjectId	• functiongraph:function:list
functiongraph:function:getEvent	授予权限以获取函数测试事件详细信息。	Read	function *	g:EnterpriseProjectId	• functiongraph:function:invoke

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
functiongraph:function:getTracing	授予权限以获取函数调用链配置。	Read	function *	g:EnterpriseProjectId	• functiongraph:function:create
functiongraph:function:updateTracing	授予权限以更新函数调用链配置。	Write	function *	g:EnterpriseProjectId	• functiongraph:function:create
functiongraph::listFunctionByMetric	授予权限以按指定指标获取函数列表。	List	-	-	• functiongraph:function:list
functiongraph:function:listFunctionStatistics	授予权限以获取指定时间段的函数运行指标。	List	function *	g:EnterpriseProjectId	• functiongraph:function:getconfig
functiongraph::listStatistics	授予权限以获取租户函数统计信息。	List	-	-	• functiongraph:function:getconfig
functiongraph:function:getReservedInstanceMetrics	授予权限以查询函数预留实例使用情况指标。	Read	function *	g:EnterpriseProjectId	• functiongraph:function:getconfig
functiongraph::enableLtsLogs	授予权限以开通 lts 日志上报功能。	Write	-	-	• functiongraph:function:create
functiongraph:function:getLtsLogConfiguration	授予权限以获取指定函数的 lts 日志组日志流配置。	Read	function *	g:EnterpriseProjectId	• functiongraph:function:getconfig
functiongraph:function:updateReservedInstanceCount	授予权限以修改函数预留实例数量。	Write	function *	g:EnterpriseProjectId	• functiongraph:function:updateconfig
functiongraph::listReservedInstanceCount	授予权限以获取函数预留实例数量。	List	-	-	• functiongraph:function:getconfig
functiongraph::listReservedInstanceConfig	授予权限以获取函数预留实例配置列表。	List	function	g:EnterpriseProjectId	• functiongraph:function:getconfig

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
functiongraph::getReservedInstanceState	授予权限以获取函数预留实例状态。	Read	-	-	• functiongraph:function:getconfig
functiongraph:function:invokeAsync	授予权限以异步执行函数。	Write	function *	g:EnterpriseProjectId	-
functiongraph:function:invokeSync	授予权限以同步执行函数。	Write	function *	g:EnterpriseProjectId	• functiongraph:function:invoke
functiongraph:function:invokeReservedFunctionAsync	授予权限以函数异步执行并返回预留实例ID。	Write	function *	g:EnterpriseProjectId	• functiongraph:function:invokeasync
functiongraph:function:stopAsyncInvoke	授予权限以停止函数异步调用请求。	Write	function *	g:EnterpriseProjectId	• functiongraph:function:invokeasync
functiongraph:function:listAsyncInvocation	授予权限以获取函数异步调用请求列表。	List	function *	g:EnterpriseProjectId	• functiongraph:function:list
functiongraph:function:deleteAsyncInvokeConfig	授予权限以删除函数异步配置信息。	Write	function *	g:EnterpriseProjectId	• functiongraph:function:delete
functiongraph:function:updateAsyncInvokeConfig	授予权限以设置函数异步配置信息。	Write	function *	g:EnterpriseProjectId	• functiongraph:function:updateconfig
functiongraph:function:listAsyncInvokeConfig	授予权限以获取指定函数所有版本的异步配置列表。	List	function *	g:EnterpriseProjectId	• functiongraph:function:list
functiongraph:function:getAsyncInvokeConfig	授予权限以获取指定函数某一版本的异步配置信息。	Read	function *	g:EnterpriseProjectId	• functiongraph:function:getconfig
functiongraph::updateAsyncStatusLog	授予权限以允许异步状态通知。	Write	-	-	• functiongraph:function:create

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
functiongraph::getAsyncStatusLogInfo	授予权限以查询异步日志详情。	Read	-	-	• functiongraph:function:getConfig
functiongraph:function:listActiveAsyncInvocations	授予权限以获取函数异步调用活跃请求列表。	List	function *	g:EnterpriseProjectId	• functiongraph:function:list
functiongraph:trigger:createTrigger	授予权限以创建触发器。	Write	function *	g:EnterpriseProjectId	• functiongraph:trigger:create
functiongraph:trigger:delete	授予权限以删除触发器。	Write	trigger *	g:EnterpriseProjectId	-
functiongraph:trigger:update	授予权限以更新触发器。	Write	function *	g:EnterpriseProjectId	• functiongraph:trigger:create
functiongraph:trigger:list	授予权限以获取指定函数的所有触发器。	List	function *	g:EnterpriseProjectId	• functiongraph:trigger:listSpecifiedFunctionTriggers
functiongraph:trigger:get	授予权限以获取指定触发器的信息。	Read	trigger *	g:EnterpriseProjectId	-
functiongraph:trigger:batchDelete	授予权限以删除指定函数的所有触发器。	Write	function *	g:EnterpriseProjectId	• functiongraph:trigger:deleteSpecifiedFunctionTriggers
functiongraph::listObsNotifications	授予权限以获取指定 OBS 桶的所有通知配置。	Read	-	-	• functiongraph:trigger:create
functiongraph::listObsBucket	授予权限以获取 OBS 桶列表。	List	-	-	• functiongraph:trigger:listSpecifiedFunctionTriggers
functiongraph:workflow:creat	授予权限以创	Write	workflow *	g:EnterpriseProjectId	• functiongraph:function:cr

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
e	建函数流。				eate
functiongraph:workflow:delete	授予权限以删除函数流。	Write	workflow *	g:EnterpriseProjectId	• functiongraph:function:delete
functiongraph:workflow:update	授予权限以修改指定函数流实例的元数据。	Write	workflow *	g:EnterpriseProjectId	• functiongraph:function:create
functiongraph:workflow:list	授予权限以查询函数流。	List	workflow *	g:EnterpriseProjectId	• functiongraph:function:list
functiongraph:workflow:getConfig	授予权限以获取指定函数流实例的元数据。	Read	workflow *	g:EnterpriseProjectId	• functiongraph:function:getConfig
functiongraph:workflow:invoke	授予权限以异步执行方式启动函数流。	Write	workflow *	g:EnterpriseProjectId	• functiongraph:function:invoke
functiongraph:workflow:invokeSync	授予权限以同步执行方式启动函数流。	Write	workflow *	g:EnterpriseProjectId	• functiongraph:function:invoke
functiongraph:workflow:terminate	授予权限以停止函数流。	Write	workflow *	g:EnterpriseProjectId	• functiongraph:function:invoke
functiongraph:workflow:retry	授予权限以重试函数流。	Write	workflow *	g:EnterpriseProjectId	• functiongraph:function:invoke
functiongraph:workflow:listExecutions	授予权限以获取指定函数流执行实例列表。	List	workflow *	g:EnterpriseProjectId	• functiongraph:function:list
functiongraph:workflow:getExecutionDetail	授予权限以获取指定函数流执行实例。	Read	workflow *	g:EnterpriseProjectId	• functiongraph:function:getConfig
functiongraph:workflow:getMetric	授予权限以获取指定函数流指标。	Read	workflow *	g:EnterpriseProjectId	• functiongraph:function:getConfig

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
functiongraph:workflow:listMetrics	授予权限以获取函数流指标。	List	-	-	• functiongraph:function:getConfig
functiongraph:workflow:downloadOutput	授予权限以下载函数流节点的执行结果。	Write	workflow *	g:EnterpriseProjectId	• functiongraph:function:getConfig
functiongraph:workflow:cancel	授予权限以停止执行函数流。	Write	workflow *	g:EnterpriseProjectId	• functiongraph:function:invoke
functiongraph:workflow:metadata	授予权限以获取函数流元数据。	List	-	-	• functiongraph:function:list

API 通常对应着一个或多个授权项。表 3-18 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-18 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/fgs/functions	functiongraph:function:createFunction	• lts:groups:list • lts:groups:create • lts:logstreams:list • lts:structConfig:create • obs:object:GetObject
DELETE /v2/{project_id}/fgs/functions/{function_urn}	functiongraph:function:deleteFunction	• functiongraph:trigger:batchDelete • lts:groups:list • lts:logstreams:list • lts:logstreams:delete
PUT /v2/{project_id}/fgs/functions/{function_urn}/config	functiongraph:function:updateFunctionConfig	• lts:groups:list • lts:groups:create • lts:logstreams:list • lts:structConfig:create
PUT /v2/{project_id}/fgs/functions/{function_urn	functiongraph:function:updateFunctionCode	obs:object:GetObject

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
}/code		
GET /v2/{project_id}/fgs/functions	functiongraph:function:listFunctions	-
GET /v2/{project_id}/fgs/functions/{function_urn}/config	functiongraph:function:getFunctionConfig	-
GET /v2/{project_id}/fgs/functions/{function_urn}/code	functiongraph:function:getFunctionCode	-
GET /v2/{project_id}/fgs/public-network-bandwidth	functiongraph::getPublicNetworkBandwidth	-
-	functiongraph::updatePublicNetworkBandwidth	-
GET /v2/{project_id}/fgs/resource-usage	functiongraph::getTenantResourceUsage	-
POST /v2/{project_id}/fgs/functions/{function_urn}/command	functiongraph::function:createTenantCommanmd	-
PUT /v2/{project_id}/fgs/functions/{function_urn}/config-max-instance	functiongraph:function:updateMaxInstanceConfig	-
POST /v2/{project_id}/fgs/functions/{function_urn}/snapshots/{action}	functiongraph:function:updateSnapshot	-
POST /v2/{project_id}/fgs/functions/{function_urn}/function-url	functiongraph:function:createUrl	-
DELETE /v2/{project_id}/fgs/functions/{function_urn}/function-url	functiongraph:function:deleteUrl	-
PUT /v2/{project_id}/fgs/functions/{function_urn	functiongraph:function:updateUrl	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
}/function-url		
GET /v2/{project_id}/fgs/functions/{function_urn}/function-url	functiongraph:function:getUrl	-
POST /v2/{project_id}/{resource_type}/resource-instances/{action}	functiongraph::getResourceInstance	-
POST /v2/{project_id}/{resource_type}/{resource_id}/tags/create	functiongraph::createTag	-
DELETE /v2/{project_id}/{resource_type}/{resource_id}/tags/delete	functiongraph::deleteTag	-
GET /v2/{project_id}/{resource_type}/tags	functiongraph::listTags	-
POST /v2/{project_id}/fgs/applications	functiongraph::createFunctionApp	-
DELETE /v2/{project_id}/fgs/applications/{id}	functiongraph::deleteFunctionApp	-
GET /v2/{project_id}/fgs/applications/{id}	functiongraph::getFunctionApp	-
GET /v2/{project_id}/fgs/applications	functiongraph::listFunctionApps	-
GET /v2/{project_id}/fgs/application/templates/{id}	functiongraph::getFunctionAppTemplate	-
GET /v2/{project_id}/fgs/application/templates	functiongraph::listFunctionAppTemplates	-
POST /v2/{project_id}/fgs/vpc-endpoint	functiongraph::createVpcEndpoint	-
DELETE /v2/{project_id}/fgs/v	functiongraph::deleteVpcEndp	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
pc-endpoint/{vpc_id}/{subnet_id}	oint	
GET /v2/{project_id}/fgs/functions/{func_urn}/download	functiongraph:function:getFunctionCode	-
GET /v2/{project_id}/fgs/admins/sysconfig	functiongraph:function:getFunctionConfig	-
GET /v2/{project_id}/fgs/domainname/vpc/{vpc_id}	functiongraph:function:getFunctionConfig	dns:zone:list
GET /v2/{project_id}/fgs/functions/{function_urn}/servicebridge/relation	functiongraph:function:listFunctions	-
POST /v2/{project_id}/fgs/packages	functiongraph:function:createFunction	-
DELETE /v2/{project_id}/fgs/packages/{package_name}	functiongraph:function:deleteFunction	-
PUT /v2/{project_id}/fgs/packages/{package_name}	functiongraph:function:createFunction	-
GET /v2/{project_id}/fgs/packages	functiongraph:function:listFunctions	-
PUT /v2/{project_id}/fgs/functions/{func_urn}/collect/{state}	functiongraph:function:updateFunctionConfig	-
GET /v2/{project_id}/fgs/template-labels	functiongraph:function:listFunctions	-
GET /v2/fgs/template-labels	functiongraph:function:listFunctions	-
GET /v2/{project_id}/fgs/te	functiongraph:function:listFunctions	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
mplates		
GET /v2/{project_id}/fgs/templates/{template_id}	functiongraph:function:listFunctions	-
GET /v2/fgs/runtimetypes	functiongraph:function:listFunctions	-
GET /v2/fgs/service-trusted-agencies	functiongraph:function:getFunctionConfig	-
GET /v2/{project_id}/fgs/feature	functiongraph:function:getFunctionConfig	-
POST /v2/{project_id}/fgs/agc/agency/{agency_name}	functiongraph:function:createFunction	-
POST /v2/{project_id}/fgs/functions/enable-async-status-logs	functiongraph::updateAsyncStatusLog	• lts:groups:list • lts:groups:create • lts:logstreams:list • lts:structConfig:create
GET /v2/{project_id}/fgs/functions/async-status-log-detail	functiongraph::getAsyncStatusLogInfo	-
GET /v2/{project_id}/fgs/functions/{function_urn}/active-async-invocations	functiongraph:function:listActiveAsyncInvocations	-
GET /v2/{project_id}/fgs/functions/{function_urn}/export	functiongraph:function:export	-
POST /v2/{project_id}/fgs/functions/import	functiongraph:function:import	-
GET /v2/{project_id}/fgs/packages/{package_name}/export	functiongraph::exportPackage	-
POST /v2/{project_id}/fgs/packages/import	functiongraph::importPackage	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/fgs/functions/{function_urn}/versions	functiongraph:function:createVersion	-
GET /v2/{project_id}/fgs/functions/{function_urn}/versions	functiongraph:function:listVersion	-
POST /v2/{project_id}/fgs/functions/{function_urn}/aliases	functiongraph:function:createAlias	-
DELETE /v2/{project_id}/fgs/functions/{function_urn}/aliases/{alias_name}	functiongraph:function:deleteAlias	functiongraph:trigger:list
PUT /v2/{project_id}/fgs/functions/{function_urn}/aliases/{alias_name}	functiongraph:function:updateAlias	-
GET /v2/{project_id}/fgs/functions/{function_urn}/aliases	functiongraph:function:listAlias	-
GET /v2/{project_id}/fgs/functions/{function_urn}/aliases/{alias_name}	functiongraph:function:getAlias	-
POST /v2/{project_id}/fgs/dependencies	functiongraph:dependency:createDependency	obs:object:GetObject
DELETE /v2/{project_id}/fgs/dependencies/{depend_id}	functiongraph:dependency:deleteDependency	-
PUT /v2/{project_id}/fgs/dependencies/{depend_id}	functiongraph:dependency:updateDependency	obs:object:GetObject
GET /v2/{project_id}/fgs/dependencies	functiongraph:dependency:listDependencies	-
GET /v2/{project_id}/fgs/dependencies/{depend_	functiongraph:dependency:getDependency	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
id}		
POST /v2/{project_id}/fgs/dependencies/version	functiongraph:dependency:createDependencyVersion	obs:object:GetObject
DELETE /v2/{project_id}/fgs/dependencies/{depend_id}/version/{version}	functiongraph:dependency:deleteDependencyVersion	-
GET /v2/{project_id}/fgs/dependencies/{depend_id}/version	functiongraph:dependency:listDependencyVersion	-
GET /v2/{project_id}/fgs/dependencies/{depend_id}/version/{version}	functiongraph:dependency:getDependencyVersion	-
POST /v2/{project_id}/fgs/functions/{function_urn}/events	functiongraph:function:createEvent	-
DELETE /v2/{project_id}/fgs/functions/{function_urn}/events/{event_id}	functiongraph:function:deleteEvent	-
PUT /v2/{project_id}/fgs/functions/{function_urn}/events/{event_id}	functiongraph:function:updateEvent	-
GET /v2/{project_id}/fgs/functions/{function_urn}/events	functiongraph:function:listEvent	-
GET /v2/{project_id}/fgs/functions/{function_urn}/events/{event_id}	functiongraph:function:getEvent	-
PUT /v2/{project_id}/fgs/functions/{function_urn}/tracing	functiongraph:function:updateTracing	-
GET /v2/{project_id}/fgs/functions/{function_urn}/tracing	functiongraph:function:getTracing	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/fgs/function/report	functiongraph::listFunctionByMetric	• aom:metric:get • aom:metric:list
GET /v2/{project_id}/fgs/functions/statistics	functiongraph::listStatistics	aom:metric:get
-	functiongraph:function:getReservedInstanceMetrics	• aom:metric:get • aom:metric:list
POST /v2/{project_id}/fgs/functions/enable-lts-logs	functiongraph::enableLtsLogs	• lts:groups:list • lts:groups:create • lts:logstreams:list • lts:structConfig:create
GET /v2/{project_id}/fgs/functions/{function_urn}/lts-log-detail	functiongraph:function:getLtsLogConfiguration	-
PUT /v2/{project_id}/fgs/functions/{function_urn}/reservedinstances	functiongraph:function:updateReservedInstanceCount	-
GET /v2/{project_id}/fgs/functions/reservedinstances	functiongraph::listReservedInstanceCount	-
GET /v2/{project_id}/fgs/functions/reservedinstanceconfigs	functiongraph::listReservedInstanceConfig	-
GET /v2/{project_id}/fgs/functions/reservedinstances/state	functiongraph::getReservedInstanceState	-
POST /v2/{project_id}/fgs/functions/{function_urn}/cancel	functiongraph:function:stopAsyncInvoke	lts:structConfig:get
GET /v2/{project_id}/fgs/functions/{function_urn}/async-invocations	functiongraph:function:listAsyncInvocation	• lts:structConfig:get • lts:logStream:searchStructLog
DELETE /v2/{project_id}/fgs/functions/{function_urn	functiongraph:function:deleteAsyncInvokeConfig	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
}/async-invoke-config		
PUT /v2/{project_id}/fgs/functions/{function_urn}/async-invoke-config	functiongraph:function:updateAsyncInvokeConfig	-
GET /v2/{project_id}/fgs/functions/{function_urn}/async-invoke-configs	functiongraph:function:listAsyncInvokeConfig	-
GET /v2/{project_id}/fgs/functions/{function_urn}/async-invoke-config	functiongraph:function:getAsyncInvokeConfig	-
POST /v2/{project_id}/fgs/servicebridge	functiongraph:bridge:createServiceBridge	-
DELETE /v2/{project_id}/fgs/servicebridge/{bridge_name}	functiongraph:bridge:deleteServiceBridge	-
PUT /v2/{project_id}/fgs/servicebridge/{bridge_name}/config	functiongraph:bridge:updateServiceBridgeConfig	-
GET /v2/{project_id}/fgs/servicebridge	functiongraph:bridge:listServiceBridges	-
GET /v2/{project_id}/fgs/servicebridge/{bridge_name}/config	functiongraph:bridge:getServiceBridgeConfig	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-19 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

 版权所有 © 华为云计算技术有限公司

表3-19 支持的资源类型

资源类型	URN
workflow	functiongraph:<region>:<account-id>:workflow:<workflow-id>
function	functiongraph:<region>:<account-id>:function:<package-name>/<function-name>
trigger	functiongraph:<region>:<account-id>:trigger:<trigger-id>

条件（Condition）

服务不支持在身份策略中的条件键中配置服务级的条件键。可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.1.6 云化数据中心 CloudDC

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源类型（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（List、Read、Write 和 Tagging 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（*）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。

 版权所有 © 华为云计算技术有限公司

- 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

关于 CloudDC 定义的资源类型的详细信息请参见资源类型（Resource）。

- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 CloudDC 定义的条件键的详细信息请参见条件（Condition）。

您可以在身份策略语句的 Action 元素中指定以下 CloudDC 的相关操作。

表3-20 CloudDC 支持的授权项

授权项	描述	访问级别	资源类型	资源条件键	全局条件键
clouddc:imetal:list	批量查询物理服务器	list	imetal	-	-
clouddc:imetal:get	查询物理服务器信息	read	imetal	g:ResourceTag/<tag-key>	-
clouddc:imetal:getHardwareAttribute	查询服务器硬件详细信息	read	imetal	g:ResourceTag/<tag-key>	-
clouddc:imetal:getFirmwareAttribute	查询服务器固件详细信息	read	imetal	g:ResourceTag/<tag-key>	-
clouddc:imetal:updatePowerStatus	修改物理服务器电源状态	write	imetal	g:ResourceTag/<tag-key>	-
clouddc:imetal:createDumpLog	导出服务器日志请求	write	imetal	g:ResourceTag/<tag-key>	-
clouddc:imetal:getDumpLogProgress	查询日志导出状态	read	imetal	g:ResourceTag/<tag-key>	-
clouddc:imetal:createDownloadLog	下载日志文件	write	imetal	g:ResourceTag/<tag-key>	-
clouddc:imetal:createRemoteConsoleLink	获取 console 地址信息	write	imetal	g:ResourceTag/<tag-key>	-
clouddc:instance:createBatch	批量创建实例	write	imetal	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型	资源条件键	全局条件键
clouddc:instance:list	批量查询实例	list	imetal	-	-
clouddc:instance:deleteBatch	批量删除实例	write	imetal	-	-
clouddc:instance:create	创建实例	write	imetal	-	-
clouddc:instance:delete	删除实例	write	imetal	-	-
clouddc:instance:changePassword	修改实例密码	write	imetal	-	-
clouddc:instance:reinstallOS	重新安装实例 OS	write	imetal	-	-
clouddc:instance:get	查询实例状态	read	imetal	-	-
clouddc:instance:updateIP	修改实例 ip	write	imetal	-	-
clouddc::listResourcesByTag	查询资源实例列表	list	imetal	-	g:TagKeys
clouddc::listTagsForResource	查询资源标签	list	imetal	g:ResourceTag/<tag-key>	-
clouddc::listTags	查询项目标签	list	imetal	-	-
clouddc::listResourcesByTag	查询实例数量	list	imetal	-	g:TagKeys
clouddc::tagResource	批量创建资源标签	tagging	imetal	g:ResourceTag/<tag-key>	g:RequestTag/<tag-key> g:TagKeys
clouddc::unTagResource	批量删除资源标签	tagging	imetal	g:ResourceTag/<tag-key>	g:RequestTag/<tag-key> g:TagKeys
clouddc::listStatus	服务器概览	list	imetal	-	-
clouddc::listAlarmStat	服务器告警概览	list	imetal	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型	资源条件键	全局条件键
clouddc::listAlarmTrend	服务器告警趋势	list	imetal	-	-
clouddc::listAlarm	服务器告警列表	list	imetal	-	-
clouddc::listEvent	服务器事件列表	list	imetal	-	-
clouddc::listIEventDicts	查询事件定义	list	imetal	-	-
clouddc::updateRepairs	更新/创建服务器维修数据	write	imetal	-	-
clouddc::listRepairs	服务器维修数据查询	list	imetal	-	-
clouddc::updateSpareParts	创建与更新备件	write	imetal	-	-
clouddc::listSpareParts	备件查询	list	imetal	-	-
clouddc:irack:update	修改 iRack 描述	write	irack	g:ResourceTag/<tag-key>	-
clouddc:irack:list	查询 iRack 实例列表	list	irack	-	-
clouddc:idc:update	修改 IDC 描述	write	irack	-	-
clouddc:idc:list	查询 IDC 列表	list	irack	-	-
clouddc::listResourcesByTag	查询机柜实例列表	list	irack	-	g:TagKeys
clouddc::listTagsForResource	查询机柜标签	list	irack	g:ResourceTag/<tag-key>	-
clouddc::listTags	查询机柜项目标签	list	irack	-	-
clouddc::listResourcesByTag	查询机柜实例数量	list	irack	-	g:TagKeys
clouddc::tagResource	批量创建机	tagg	irac	g:ResourceTag	g:RequestTag/

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型	资源条件键	全局条件键
	柜标签	ing	k	/<tag-key>	<tag-key> g:TagKeys
clouddc::unTagResource	批量删除机柜标签	tagging	irack	g:ResourceTag/<tag-key>	g:RequestTag/<tag-key> g:TagKeys
clouddc::createIRackOrder	授予购买资源时下单参数检查权限	write	irack	-	-

CloudDC 的 API 通常对应着一个或多个授权项。表 3-21 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-21 API 与授权项的关系

API URI	请求类型	描述	对应的授权项	依赖的授权项
/v1/{project_id}/physicalservers	GET	批量查询物理服务器	clouddc:imetal:list	-
/v1/{project_id}/physicalservers/{id}	GET	查询物理服务器信息	clouddc:imetal:get	-
/v1/{project_id}/physicalservers/{id}/hardware-attributes	GET	查询服务器硬件详细信息	clouddc:imetal:getHardwareAttribute	-
/v1/{project_id}/physicalservers/{id}/firmware-attributes	GET	查询服务器固件详细信息	clouddc:imetal:getFirmwareAttribute	-
/v1/{project_id}/physicalservers/{id}/power-state	PUT	修改物理服务器电源状态	clouddc:imetal:updatePowerStatus	-
/v1/{project_id}/physicalservers/{id}/logs/exports	POST	导出服务器日志请求	clouddc:imetal:createDumpLog	-
/v1/{project_id}/physicalservers/{i	GE	查询日志	clouddc:imetal:getD	-

 版权所有 © 华为云计算技术有限公司

API URI	请求类型	描述	对应的授权项	依赖的授权项
d}/logs/exports/{export_id}	T	导出状态	umpLogProgress	
/v1/{project_id}/physicalservers/{id}/logs/exports/{export_id}/content	GET	下载日志文件	clouddc:imetal:createDownloadLog	-
/v1/{project_id}/physicalservers/{id}/remote-console-address	GET	获取console地址信息	clouddc:imetal:createRemoteConsoleLink	-
/v1/{project_id}/instances/batch-create	POST	批量创建实例	clouddc:instance:createBatch	-
/v1/{project_id}/instances	GET	批量查询实例	clouddc:instance:list	-
/v1/{project_id}/instances/batch-delete	DELETE	批量删除实例	clouddc:instance:deleteBatch	-
/v1/{project_id}/instance	POST	创建实例	clouddc:instance:create	-
/v1/{project_id}/instances/{id}	DELETE	删除实例	clouddc:instance:delete	-
/v1/{project_id}/instances/{id}/password	PUT	修改实例密码	clouddc:instance:changePassword	-
/v1/{project_id}/instances/{id}/reinstall	PUT	重新安装实例OS	clouddc:instance:reinstallOS	-
/v1/{project_id}/instances/{id}/status	GET	查询实例状态	clouddc:instance:get	-
/v1/{project_id}/instances/{id}/ip	PUT	修改实例ip	clouddc:instance:updateIP	-
/{version}/{project_id}/{resource_type}/resource-instances/filter	POST	查询资源实例列表	clouddc::listResourcesByTag	-
/{version}/{project_id}/{resource_type}/{resource_id}/tags	GET	查询资源标签	clouddc::listTagsForResource	-
/{version}/{project_id}/{resource_type}/tags	GET	查询项目标签	clouddc::listTags	-
/{version}/{project_id}/{resource_type}/resource-instances/count	POST	查询实例数量	clouddc::listResourcesByTag	-

 版权所有 © 华为云计算技术有限公司

API URI	请求类型	描述	对应的授权项	依赖的授权项
/v1/{project_id}/{resource_type}/{resource_id}/tags/create	POST	批量创建资源标签	clouddc::tagResource	-
/v1/{project_id}/{resource_type}/{resource_id}/tags/delete	POST	批量删除资源标签	clouddc::unTagResource	-
/v1/{project_id}/physicalservers/status	GET	服务器概览	clouddc::listStatus	-
/v1/{project_id}/physicalservers/alarms/summary	GET	服务器告警概览	clouddc::listAlarmStat	ces:alarmHistory:list
/v1/{project_id}/physicalservers/alarms/trend	GET	服务器告警趋势	clouddc::listAlarmTrend	ces:alarmHistory:list
/v1/{project_id}/physicalservers/alarms	GET	服务器告警列表	clouddc::listAlarm	ces:alarmHistory:list
/v1/{project_id}/physicalservers/events	GET	服务器事件列表	clouddc::listEvent	ces:events:get
/v1/{project_id}/physicalservers/events/{event_id}	GET	查询事件定义	clouddc::listIEventDicts	-
/v1/{project_id}/repairs	PUT	更新/创建服务器维修数据	clouddc::updateRepairs	-
/v1/{project_id}/repairs	GET	服务器维修数据查询	clouddc::listRepairs	-
/v1/{project_id}/spareparts	PUT	创建与更新备件	clouddc::updateSpareParts	-
/v1/{project_id}/spareparts	GET	备件查询	clouddc::listSpareParts	-
/v1/{project_id}/iracks/{irack_id}	PUT	修改 iRack 描述	clouddc:irack:update	-
/v1/{project_id}/iracks	GET	查询 iRack 实例列表	clouddc:irack:list	-
/v1/{project_id}/idcs	PU	修改 IDC	clouddc:idc:update	-

 版权所有 © 华为云计算技术有限公司

API URI	请求类型	描述	对应的授权项	依赖的授权项
	T	描述		
/v1/{project_id}/idcs	GET	查询 IDC 列表	clouddc:idc:list	-
/{version}/{project_id}/{resource_type}/resource-instances/filter	POST	查询机柜实例列表	clouddc::listResourcesByTag	-
/{version}/{project_id}/{resource_type}/{resource_id}/tags	GET	查询机柜标签	clouddc::listTagsForResource	-
/{version}/{project_id}/{resource_type}/tags	GET	查询机柜项目标签	clouddc::listTags	-
/{version}/{project_id}/{resource_type}/resource-instances/count	POST	查询机柜实例数量	clouddc::listResourcesByTag	-
/v1/{project_id}/iracks/{id}/tags/create	POST	批量创建机柜标签	clouddc::tagResource	-
/v1/{project_id}/iracks/{id}/tags/delete	POST	批量删除机柜标签	clouddc::unTagResource	-
/v1/services/unibuy/extend	POST	授予购买资源时下单参数检查权限	clouddc::createIRackOrder	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源，如表 3-22 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的 URN，身份策略仅作用于此资源；如未指定，Resource 默认为 “*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

CloudDC 定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-22 CloudDC 支持的资源类型

资源类型	URN
imetal	clouddc:<region>:<account-id>:imetal:<resource-id>
irack	clouddc:<region>:<account-id>:irack:<resource-id>

 版权所有 © 华为云计算技术有限公司

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见表 3-23。更多全局条件键说明，可参见全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 clouddc:）仅适用于对应服务的操作，CloudDC 服务不支持在身份策略中的条件键中配置服务级的条件键。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。

CloudDC 定义了以下可以在身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-23 CloudDC 支持的全局条件键

全局级条件键	类型	说明
g:ResourceTag/<tag-key>	字符串单值属性	请求所访问的资源身上携带的标签
g:RequestTag/<tag-key>	字符串单值属性	请求中携带的标签
g:TagKeys	字符串多值属性	请求中携带的所有标签的 key 组成的列表

3.2 存储

3.2.1 对象存储服务 OBS

云服务在 IAM 预置了常用的权限，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

 版权所有 © 华为云计算技术有限公司

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “**访问级别**”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “**资源类型**”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 OBS 定义的资源类型的详细信息请参见资源类型（Resource）。
- “**条件键**”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 OBS 定义的条件键的详细信息请参见条件（Condition）。
- “**别名**”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 OBS 的相关操作。

表3-24 OBS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
obs:object:abortMultipartUploa	授予取消多段上传任务的权	Write	object *	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
d	限。		-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:object:deleteObject	授予删除非指定版本对象的权限。	Write	object*	g:EnterpriseProjectId	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:object:deleteObjectTagging	授予删除对象标签的权限。	Tagging	object*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:object:deleteObjectVersionTagging	授予删除指定对象版本标签的权限。	Tagging	object*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • obs:versionId	-
			-	• obs:EpochTime	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:object:deleteObjectVersion	授予删除指定版本对象的权限。	Write	object *	• obs:versionId • g:EnterpriseProjectId	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:object:getObject	授予下载非指定版本对象的权限。	Read	object *	g:EnterpriseProjectId	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:object:getObjectTagging	授予下载对象标签的权限。	Read	object *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:Custom	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				Domain	
obs:object:getObjectVersionTagging	授予下载指定对象版本标签的权限。	Read	object *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • obs:versionId	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:object:getObjectAcl	授予不指定版本获取对象的ACL 的权限。	Read	object *	g:EnterpriseProjectId	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:object:getObjectRetention	授予获取对象保留配置的权限。	Read	object *	g:EnterpriseProjectId	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:object:getObjectVersion	授予下载指定版本对象的权	Read	object *	• g:EnterpriseProjectId • obs:versionI	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。			d	
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:object:getObjectVersionAcl	授予获取指定版本对象的ACL 的权限。	Read	object *	• obs:versionId • g:EnterpriseProjectId	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:object:listMultipartUploadParts	授予获取一个多段上传任务所属的所有段信息的权限。	List	object *	g:EnterpriseProjectId	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:object:modifyObjectMetadata	授予修改、删除或添加桶中已经上传的对象元数据的权限。	Write	object *	g:EnterpriseProjectId	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• obs:CustomDomain	
obs:object:putObject	授予上传对象的权限。	Write	object *	g:EnterpriseProjectId	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain • obs:x-obs-acl • obs:x-obs-copy-source • obs:x-obs-metadata-directive • obs:x-obs-server-side-encryption	
obs:object:putObjectTagging	授予上传对象标签的权限。	Tagging	object *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:object:putObjectVersionTa	授予上传指定对象版本标签	Tagging	object *	• g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
gging	的权限。			• g:ResourceTag/<tag-key> • obs:versionId	
			-	• g:RequestTag/<tag-key> • g:TagKeys • obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:object:putObjectAcl	授予设置或修改非指定版本对象 ACL 的权限。	Permission_management	object *	g:EnterpriseProjectId	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain • obs:x-obs-acl	
obs:object:putObjectRetention	授予设置对象保留配置的权限。	Write	object *	g:EnterpriseProjectId	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:object:putObjectVersionAc	授予设置或修改指定版本对	Permission_	object *	• obs:versionId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
l	象 ACL 的权限。	management		• g:EnterpriseProjectId	
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain • obs:x-obs-acl	
obs:object:restoreObject	授予恢复归档或深度归档对象的权限。	Write	object *	g:EnterpriseProjectId	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:createBucket	授予创建新桶的权限。	Write	bucket *	-	-
			-	• g:EnterpriseProjectId • obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain • obs:BucketEncrypted • obs:x-obs-acl	
obs:bucket:deleteBucket	授予删除桶的	Write	bucket *	• g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	权限。			• g:ResourceTag/<tag-key>	
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:deleteBucketCustomDomainConfiguration	授予删除桶的自定义域名的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:deleteBucketInventoryConfiguration	授予删除桶的清单配置的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:deleteBucketPolicy	授予删除桶策略的权限。	Permission_manag	bucket *	• g:EnterpriseProjectId • g:ResourceT	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
		ement		ag/<tag-key>	
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:deleteBucketTagging	授予删除桶标签的权限。	Tagging	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:deleteBucketWebsite	授予删除桶的网站配置信息的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:deleteDirectColdAccessConfiguration	授予删除桶的归档直读配置信息的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				key>	
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:deleteReplicationConfiguration	授予删除桶的复制配置的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketAcl	授予获取桶ACL 的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketObjectLockConfiguration	授予查询桶WORM 默认保护策略和保护期限的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketCORS	授予查询桶的CORS 配置的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketCustomDomainConfiguration	授予查询桶的自定义域名的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketInventoryConfiguration	授予查询桶的清单配置的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTi	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				me • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketLocation	授予查询桶区域位置信息的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketLogging	授予查询桶的日志管理配置的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketPolicy	授予获取桶策略的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketQuota	授予获取桶空间配额。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketStorage	授予查询桶对象个数及对象占用空间的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketStoragePolicy	授予获取桶的默认存储类型信息。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceI	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				p • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketTagging	授予获取桶的标签的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketVersioning	授予获取桶的多版本状态的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketWebsite	授予获取桶设置的网站配置的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• obs:TlsVersion • obs:CustomDomain	
obs:bucket:getDirectColdAccessConfiguration	授予获取指定桶的归档对象状态的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getEncryptionConfiguration	授予获取桶的加密配置的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getLifecycleConfiguration	授予获取桶的生命周期配置的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersi	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• on • obs:CustomDomain	
obs:bucket:getReplicationConfiguration	授予获取桶的跨区域复制配置的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:headBucket	授予获取桶元数据的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:listAllMyBuckets	授予查询创建的桶列表的权限。	List	bucket *	-	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:listB	授予获取桶内	List	bucket	• g:Enterprise	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ucket	对象列表的权限。		*	ProjectId • g:ResourceTag/<tag-key>	
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain • obs:prefix • obs:delimiter • obs:max-keys	
obs:bucket:listBucketMultipartUploads	授予列举桶中已初始化多段任务的权限。	List	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:listBucketVersions	授予获取桶内多版本对象列表的权限。	List	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersi	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				on • obs:CustomDomain • obs:prefix • obs:delimiter • obs:max-keys	
obs:bucket:putBucketAcl	授予设置桶ACL的权限。	Permission_management	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain • obs:x-obs-acl	
obs:bucket:putBucketCORS	授予设置桶的CORS配置的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:putBucketCustomDomainConfiguration	授予设置桶的自定义域名的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				key>	
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:putBucketObjectLockConfiguration	授予设置桶级默认 WORM 策略的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:putBucketInventoryConfiguration	授予设置桶清单规则的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:putBucketLogging	授予设置桶的日志管理配置的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:putBucketPolicy	授予设置桶策略的权限。	Permission_management	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:putBucketQuota	授予设置桶配额的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:putBucketStoragePolicy	授予设置桶默认存储类型的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTi	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				me • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:putBucketTagging	授予设置桶标签的权限。	Tagging	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:putBucketVersioning	授予设置桶的多版本状态的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:putBucketWebsite	授予设置桶的网站配置的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				key>	
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:putDirectColdAccessConfiguration	授予设置桶归档对象直读策略的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:putEncryptionConfiguration	授予设置桶的加密配置的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain • obs:BucketEncrypted	
obs:bucket:putLifecycleConfiguration	授予设置桶的生命周期配置	Write	bucket *	• g:EnterpriseProjectId • g:ResourceT	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	的权限。			ag/<tag-key>	
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:putReplicationConfiguration	授予设置桶的跨区域复制配置的权限。	Write	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketPublicAccessBlock	授予获取桶BPA配置的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:putBucketPublicAccessBlock	授予设置桶BPA配置的权限。	Permission_management	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				key>	
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:deleteBucketPublicAccessBlock	授予删除桶BPA 配置的权限。	Permission_management	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketPolicyPublicStatus	授予获取桶策略公开状态的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	
obs:bucket:getBucketPublicStatus	授予获取桶公开状态的权限。	Read	bucket *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	• obs:EpochTime • obs:SourceIp • obs:TlsVersion • obs:CustomDomain	

OBS 的 API 通常对应着一个或多个授权项。表 3-25 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-25 API 与授权项的关系

API	对应的授权项	依赖的授权项
PUT /?replication	obs:bucket:putReplicationConfiguration	-
GET /?replication	obs:bucket:getReplicationConfiguration	-
DELETE /?replication	obs:bucket:deleteReplicationConfiguration	-
PUT /ObjectName?acl	obs:object:putObjectAcl	-
PUT /ObjectName?acl	obs:object:putObjectVersionAcl	-
GET /ObjectName?acl	obs:object:getObjectAcl	-
GET /ObjectName?acl	obs:object:getObjectVersionAcl	-
PUT /ObjectName?metadata	obs:object:modifyObjectMetadata	-
POST /	obs:object:putObject	• kms:cmk:create • kms:cmk:list • kms:cmk:createDataKey • functiongraph:function:invokeAsync • functiongraph:workflow:invoke

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
		• smn:topic:publish
PUT /ObjectName	obs:object:putObject	• kms:cmk:create • kms:cmk:list • kms:cmk:createDataKey • functiongraph:function:invokeAsync • functiongraph:workflow:invoke • smn:topic:publish
PUT /objectname?tagging&versionId=versionid	obs:object:putObjectTagging	-
PUT /objectName?tagging&versionId	obs:object:putObjectVersionTagging	-
GET /ObjectName	obs:object:getObject	• kms:cmk:create • kms:cmk:list • kms:cmk:decryptDataKey
GET /objectname?tagging&versionId=versionid	obs:object:getObjectTagging	-
GET /objectName?tagging&versionId	obs:object:getObjectVersionTagging	-
GET /ObjectName	obs:object:getObjectVersion	• kms:cmk:create • kms:cmk:list • kms:cmk:decryptDataKey
HEAD /ObjectName	obs:object:getObject	obs:object:getObjectRetention
HEAD /ObjectName	obs:object:getObjectVersion	obs:object:getObjectRetention
DELETE /ObjectName	obs:object:deleteObject	• functiongraph:function:invokeAsync • functiongraph:workflow:invoke • smn:topic:publish
DELETE /objectname?tagging&versionId=versionid	obs:object:deleteObjectTagging	-
DELETE /objectName?tagging&versionId	obs:object:deleteObjectVersionTagging	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /ObjectName	obs:object:deleteObjectVersion	• functiongraph:function:invokeAsync • functiongraph:workflow:invoke • smn:topic:publish
POST /ObjectName?uploads	obs:object:putObject	• kms:cmk:create • kms:cmk:list • kms:cmk:createDataKey
GET /?uploads&max-uploads=max	obs:bucket:listBucketMultipartUploads	-
PUT /ObjectName?partNumber=partNum&uploadId=uploadID	obs:object:putObject	• kms:cmk:createDataKey • kms:cmk:decryptDataKey
GET /ObjectName?uploadId=uploadid&max-parts=max&part-number-marker=marker	obs:object:listMultipartUploadParts	-
DELETE /ObjectName?uploadId=uplaodID	obs:object:abortMultipartUpload	-
POST /ObjectName?uploadId=uploadID	obs:object:putObject	• functiongraph:function:invokeAsync • functiongraph:workflow:invoke • smn:topic:publish
PUT /?website	obs:bucket:putBucketWebsite	-
GET /?website	obs:bucket:getBucketWebsite	-
DELETE /?website	obs:bucket:deleteBucketWebsite	-
PUT /?cors	obs:bucket:putBucketCORS	-
GET /?cors	obs:bucket:getBucketCORS	-
DELETE /?cors	obs:bucket:putBucketCORS	-
PUT /?directcoldaccess	obs:bucket:putDirectColdAccessConfiguration	-
GET /?directcoldaccess	obs:bucket:getDirectColdAccessConfiguration	-
DELETE	obs:bucket:deleteDirectColdAc	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/?directcoldaccess	cessConfiguration	
POST /ObjectName?restore&versionId=VersionID	obs:object:restoreObject	-
PUT /?quota	obs:bucket:putBucketQuota	-
GET /?quota	obs:bucket:getBucketQuota	-
PUT /?lifecycle	obs:bucket:putLifecycleConfiguration	-
DELETE /?lifecycle	obs:bucket:putLifecycleConfiguration	-
GET /?lifecycle	obs:bucket:getLifecycleConfiguration	-
PUT /?acl	obs:bucket:putBucketAcl	-
GET /?acl	obs:bucket:getBucketAcl	-
PUT /?logging	obs:bucket:putBucketLogging	-
GET /?logging	obs:bucket:getBucketLogging	-
PUT /?tagging	obs:bucket:putBucketTagging	-
GET /?tagging	obs:bucket:getBucketTagging	-
DELETE /?tagging	obs:bucket:deleteBucketTagging	-
PUT /?policy	obs:bucket:putBucketPolicy	-
GET /?policy	obs:bucket:getBucketPolicy	-
DELETE /?policy	obs:bucket:deleteBucketPolicy	-
GET /?storageinfo	obs:bucket:getBucketStorage	-
PUT /	obs:bucket:createBucket	-
DELETE /	obs:bucket:deleteBucket	-
HEAD /	obs:bucket:headBucket	-
GET /	obs:bucket:listBucket	-
GET /?location	obs:bucket:getBucketLocation	-
PUT /?versioning	obs:bucket:putBucketVersioning	-
GET /?versioning	obs:bucket:getBucketVersioning	-
GET /	obs:bucket:listBucketVersions	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /?encryption	obs:bucket:putEncryptionConfiguration	kms:cmk:get
GET /?encryption	obs:bucket:getEncryptionConfiguration	-
DELETE /?encryption	obs:bucket:putEncryptionConfiguration	-
PUT /?inventory&id=configuration-id	obs:bucket:putBucketInventoryConfiguration	-
GET /?inventory&id=configuration-id	obs:bucket:getBucketInventoryConfiguration	-
GET /?inventory	obs:bucket:getBucketInventoryConfiguration	-
DELETE /?inventory&id=configuration-id	obs:bucket:deleteBucketInventoryConfiguration	-
PUT /?storageClass	obs:bucket:putBucketStoragePolicy	-
GET /?storageClass	obs:bucket:getBucketStoragePolicy	-
PUT /?customdomain=domainname	obs:bucket:putBucketCustomDomainConfiguration	-
GET /?customdomain	obs:bucket:getBucketCustomDomainConfiguration	-
DELETE /?customdomain=domainname	obs:bucket:deleteBucketCustomDomainConfiguration	-
PUT /?object-lock	obs:bucket:putBucketObjectLockConfiguration	-
GET /?object-lock	obs:bucket:getBucketObjectLockConfiguration	-
PUT /ObjectName?retention&versionId=versionid	obs:object:putObjectRetention	-
PUT /ObjectName?partNumber=partNum&uploadId=UploadID	obs:object:putObject	• obs:object:getObject • kms:cmk:create • kms:cmk:list • kms:cmk:createDataKey

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
		• kms:cmk:decryptDataKey
POST /?delete	obs:object:deleteObject	• functiongraph:function:invokeAsync • functiongraph:workflow:invoke • smn:topic:publish
PUT /destinationObjectName	obs:object:putObject	• obs:object:getObject • kms:cmk:create • kms:cmk:list • kms:cmk:createDataKey • kms:cmk:decryptDataKey • functiongraph:function:invokeAsync • functiongraph:workflow:invoke • smn:topic:publish
GET /	obs:bucket:listAllMyBuckets	-
PUT /ObjectName?truncate&length=Length	obs:object:putObject	-
POST /ObjectName?append&position=Position	obs:object:putObject	• kms:cmk:create • kms:cmk:list • kms:cmk:createDataKey • kms:cmk:decryptDataKey
PUT /ObjectName?modify&position=Position	obs:object:putObject	-
POST /ObjectName?name=Name&rename	obs:object:getObject	obs:object:putObject
GET /?publicAccessBlock	obs:bucket:getBucketPublicAccessBlock	-
PUT /?publicAccessBlock	obs:bucket:putBucketPublicAccessBlock	-
DELETE /?publicAccessBlock	obs:bucket:deleteBucketPublicAccessBlock	-
GET /?policyStatus	obs:bucket:getBucketPolicyPublicStatus	-
GET /?bucketStatus	obs:bucket:getBucketPublicStatus	-

 版权所有 © 华为云计算技术有限公司

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-26 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

OBS 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-26 OBS 支持的资源类型

资源类型	URN
bucket	obs:::bucket:<bucket-name>
object	obs:::object:<bucket-name>/<object-name>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 obs:）仅适用于对应服务的操作，详情请参见表 3-27。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

OBS 支持的服务级条件键

OBS 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-27 OBS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
obs:versionId	string	单值	根据对象版本号过滤请求。
obs:prefix	string	单值	根据列举对象的前缀过滤请求。
obs:delimiter	string	单值	根据分组桶内对象的字符串过滤请求。
obs:max-keys	numeric	单值	根据最大返回的对象数过滤请求，返回按照字典顺序的最多前 max-keys 个对象。
obs:x-obs-acl	string	单值	根据头域携带的 ACL 过滤请求，取值范围为 private|public-read|public-read-write|bucketowner-read|bucket-owner-full-control|log-delivery-write。
obs:x-obs-copy-source	string	单值	根据复制对象时可操作的源桶名以及源对象名过滤请求，格式为 /bucketname/keyname。
obs:x-obs-metadata-directive	string	单值	根据新对象的元数据是从源对象中复制或使用请求中的元数据替换过滤请求，取值范围为 COPY|REPLACE。
obs:x-obs-server-side-encryption	string	单值	根据桶中对象是否加密存储过滤请求，取值为 kms。
obs:SourceIp	ip_address	单值	根据 x-forward-for 头域中的首个 IP 或请求发起的源 IP 过滤请求。
obs:EpochTime	numeric	单值	根据服务器接收请求的时间过滤请求，格式为从 1970.01.01 00:00:00 UTC 开始所经过的秒数，不考虑闰秒。
obs:BucketEncrypted	boolean	单值	根据创桶、设置桶加密、删除桶加密后桶的加密状态过滤请求。

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
obs:TlsVersion	numeric	单值	根据客户端发起请求使用的 TLS 协议版本过滤请求。
obs:CustomDomain	boolean	单值	根据客户端发起请求是否使用自定义域名来过滤请求。

3.2.2 云备份 CBR

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 CBR 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。

 版权所有 © 华为云计算技术有限公司

- 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
- 如果此列条件键没有值（-），表示此操作不支持指定条件键。

关于 CBR 定义的条件键的详细信息请参见条件（Condition）。

- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 CBR 的相关操作。

表3-28 CBR 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cbr:tasks:list	授予查询任务列表权限。	List	task *	-	-
			-	g:EnterpriseProjectId	
cbr:tasks:get	授予查询单个任务权限。	Read	task *	g:EnterpriseProjectId	-
cbr:member:create	授予添加备份成员权限。	Permission_management	backup *	g:EnterpriseProjectId	-
			-	cbr:TargetOrgPaths	
cbr:member:update	授予更新备份成员状态权限。	Write	backup *	g:EnterpriseProjectId	-
cbr:member:get	授予获取备份成员详情权限。	Read	backup *	g:EnterpriseProjectId	-
cbr:member:list	授予获取备份成员列表权限。	List	backup *	-	-
cbr:member:delete	授予删除指定备份成员权限。	Permission_management	backup *	g:EnterpriseProjectId	-
cbr:vaults:showCheckpoint	授予查询备份还原点权限。	Read	-	-	-
cbr:vaults:showSummary	授予查询存储库总览权限。	List	-	-	-
cbr:vaults:replic	授予复制备份	Write	vault *	• g:ResourceT	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ate	还原点权限。			ag/<tag-key> • g:EnterpriseProjectId	
cbr:vaults:backup	授予创建备份还原点权限。	Write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cbr:vaults:sync	授予同步备份还原点权限。	Write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cbr:vaults:create	授予创建存储库权限。	Write	vault *	-	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • cbr:PolicyId	
cbr:vaults:get	授予查询指定存储库权限。	Read	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cbr:vaults:list	授予查询存储库列表权限。	List	vault *	-	-
			-	g:EnterpriseProjectId	
cbr:vaults:update	授予修改存储库权限。	Write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cbr:vaults:delete	授予删除存储库权限。	Write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cbr:vaults:removeResources	授予移除资源权限。	Write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cbr:vaults:addResources	授予添加资源权限。	Write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cbr:vaults:setResources	授予设置存储库资源权限。	Write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cbr:vaults:associatePolicy	授予设置存储库策略权限。	Write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cbr:vaults:dissociatePolicy	授予解除存储库策略权限。	Write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cbr:vaults:listExternalVaults	授予查询其他区域的存储库列表权限。	List	vault *	-	-
cbr:vaults:migrateResources	授予迁移资源权限。	Write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cbr:backups:sync	授予同步备份权限。	Write	vault *	g:EnterpriseProjectId	-
cbr:backups:get	授予查询指定备份权限。	Read	backup *	g:EnterpriseProjectId	-
cbr:backups:showMetadata	授予查询备份	Read	backup *	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	元数据权限。				
cbr:backups:list	授予查询所有备份权限。	List	backup *	-	-
			-	g:EnterpriseProjectId	
cbr:backups:delete	授予删除备份权限。	Write	backup *	g:EnterpriseProjectId	-
cbr:backups:replicate	授予复制备份权限。	Write	backup *	g:EnterpriseProjectId	-
cbr:backups:restore	授予备份恢复权限。	Write	backup *	g:EnterpriseProjectId	-
cbr:backups:update	授予更新备份权限。	Write	backup *	g:EnterpriseProjectId	-
cbr:policies:list	授予查询策略列表权限。	List	policy *	-	-
cbr:policies:create	授予创建策略权限。	Write	policy *	-	-
			-	cbr:EnabledPolicy	
cbr:policies:get	授予查询单个策略权限。	Read	policy *	-	-
cbr:policies:update	授予修改策略权限。	Write	policy *	-	-
			-	cbr:EnabledPolicy	
cbr:policies:delete	授予删除策略权限。	Write	policy *	-	-
cbr:vaults:listProtectables	授予查询可保护资源权限。	List	-	g:EnterpriseProjectId	-
cbr:vaults:getProtectables	授予查询指定可保护资源权限。	Read	-	-	-
cbr:backups:queryReplication	授予查询复制能力权限。	List	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
Capability					
cbr:backups:checkAgent	授予查询 agent 状态权限。	Read	-	-	-
cbr:vaults:listResourceInstances	授予查询存储库资源实例权限。	List	vault *	-	-
cbr:vaults:bulkCreateOrDeleteTags	授予批量添加删除存储库资源标签权限。	Write	vault *	g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
cbr:vaults:setTags	授予添加存储库资源标签权限。	Write	vault *	g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
cbr:vaults:deleteTags	授予删除存储库资源标签权限。	Write	vault *	g:ResourceTag/<tag-key>	-
			-	g:TagKeys	
cbr:vaults:getTags	授予查询存储库资源标签权限。	Read	vault *	g:ResourceTag/<tag-key>	-
cbr:vaults:listProjectTags	授予查询存储库项目标签权限。	List	vault *	-	-
cbr:backups:listStorageUsage	授予查询容量统计权限。	List	-	-	-
cbr:vaults:updateOrder	授予变更权限。	Write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cbr:agents:addPath	授予新增备份路径权限。	Write	agent *	-	-
cbr:agents:get	授予查询指定	Read	agent	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	客户端权限。		*		
cbr:agents:update	授予修改客户端权限。	Write	agent *	-	-
cbr:agents:register	授予注册客户端权限。	Write	agent *	-	-
cbr:agents:delete	授予移除客户端权限。	Write	agent *	-	-
cbr:agents:removePath	授予移除备份路径权限。	Write	agent *	-	-
cbr:agents:list	授予查询客户端列表权限。	List	agent *	-	-
cbr:backups:migratesCreate	授予租户迁移权限。	Write	-	-	-
cbr:backups:migratesIndex	授予查询迁移权限。	Read	-	-	-
cbr:organizationPolicies:create	授予创建组织策略权限。	Write	-	-	-
cbr:organizationPolicies:listPolicyDetail	授予查询组织策略部署状态列表权限。	Read	-	-	-
cbr:organizationPolicies:delete	授予删除组织策略权限。	Write	-	-	-
cbr:organizationPolicies:update	授予修改组织策略权限。	Write	-	-	-
cbr:organizationPolicies:list	授予查询组织策略列表权限。	List	-	-	-
cbr:organizationPolicies:get	授予查询单个组织策略权限。	Read	-	-	-

CBR 的 API 通常对应着一个或多个授权项。表 3-29 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

 版权所有 © 华为云计算技术有限公司

表3-29 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/operation-logs	cbr:tasks:list	-
GET /v3/{project_id}/operation-logs/{operation_log_id}	cbr:tasks:get	-
POST /v3/{project_id}/backups/{backup_id}/members	cbr:member:create	-
PUT /v3/{project_id}/backups/{backup_id}/members/{member_id}	cbr:member:update	-
GET /v3/{project_id}/backups/{backup_id}/members/{member_id}	cbr:member:get	-
GET /v3/{project_id}/backups/{backup_id}/members	cbr:member:list	-
DELETE /v3/{project_id}/backups/{backup_id}/members/{member_id}	cbr:member:delete	-
GET /v3/{project_id}/checkpoints/{checkpoint_id}	cbr:vaults:showCheckpoint	-
GET /v3/{project_id}/vaults/summary	cbr:vaults:showSummary	-
POST /v3/{project_id}/checkpoints/replicate	cbr:vaults:replicate	-
POST /v3/{project_id}/checkpoints	cbr:vaults:backup	• ecs:cloudServers:listServersDetails • evs:volumes:list
POST /v3/{project_id}/check	cbr:vaults:sync	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
points/sync		
POST /v3/{project_id}/vaults	cbr:vaults:create	• ecs:cloudServers:listServersDetails • evs:volumes:list
POST /v3/{project_id}/vaults/order	cbr:vaults:create	• ecs:cloudServers:listServersDetails • evs:volumes:list
GET /v3/{project_id}/vaults/{vault_id}	cbr:vaults:get	-
GET /v3/{project_id}/vaults	cbr:vaults:list	-
PUT /v3/{project_id}/vaults/{vault_id}	cbr:vaults:update	-
PUT /v3/{project_id}/vaults/batch-update	cbr:vaults:update	-
DELETE /v3/{project_id}/vaults/{vault_id}	cbr:vaults:delete	-
POST /v3/{project_id}/vaults/{vault_id}/removeresources	cbr:vaults:removeResources	-
POST /v3/{project_id}/vaults/{vault_id}/addresources	cbr:vaults:addResources	• ecs:cloudServers:listServersDetails • evs:volumes:list
PUT /v3/{project_id}/vaults/{vault_id}/set-resources	cbr:vaults:setResources	-
POST /v3/{project_id}/vaults/{vault_id}/associatepolicy	cbr:vaults:associatePolicy	-
POST /v3/{project_id}/vaults/{vault_id}/dissociatepolicy	cbr:vaults:dissociatePolicy	-
GET /v3/{project_id}/vaults	cbr:vaults:listExternalVaults	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/external		
POST /v3/{project_id}/vaults/{vault_id}/migrateresources	cbr:vaults:migrateResources	-
POST /v3/{project_id}/backups/sync	cbr:backups:sync	-
GET /v3/{project_id}/backups/{backup_id}	cbr:backups:get	-
GET /v3/{project_id}/backups/{backup_id}/metadata	cbr:backups:showMetadata	-
GET /v3/{project_id}/backups	cbr:backups:list	-
DELETE /v3/{project_id}/backups/{backup_id}	cbr:backups:delete	-
POST /v3/{project_id}/backups/{backup_id}/replicate	cbr:backups:replicate	-
POST /v3/{project_id}/backups/{backup_id}/restore	cbr:backups:restore	• ecs:cloudServers:listServersDetails • evs:volumes:list
PUT /v3/{project_id}/backups/{backup_id}	cbr:backups:update	-
GET /v3/{project_id}/policies	cbr:policies:list	-
POST /v3/{project_id}/policies	cbr:policies:create	-
GET /v3/{project_id}/policies/{policy_id}	cbr:policies:get	-
PUT /v3/{project_id}/polici	cbr:policies:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
es/{policy_id}		
DELETE /v3/{project_id}/policies/{policy_id}	cbr:policies:delete	-
GET /v3/{project_id}/protectables/{protectable_type}/instances	cbr:vaults:listProtectables	• ecs:cloudServers:listServersDetails • evs:volumes:list
GET /v3/{project_id}/protectables/{protectable_type}/instances/{instance_id}	cbr:vaults:getProtectables	• ecs:cloudServers:listServersDetails • evs:volumes:list
GET /v3/{project_id}/replication-capabilities	cbr:backups:queryReplicationCapability	-
POST /v3/{project_id}/agent/check	cbr:backups:checkAgent	-
POST /v3/{project_id}/vault/resource_instances/action	cbr:vaults:listResourceInstances	-
POST /v3/{project_id}/vault/{vault_id}/tags/action	cbr:vaults:bulkCreateOrDeleteTags	-
POST /v3/{project_id}/vault/{vault_id}/tags	cbr:vaults:setTags	-
DELETE /v3/{project_id}/vault/{vault_id}/tags/{key}	cbr:vaults:deleteTags	-
GET /v3/{project_id}/vault/{vault_id}/tags	cbr:vaults:getTags	-
GET /v3/{project_id}/vault/tags	cbr:vaults:listProjectTags	-
GET /v3/{project_id}/storage_usage	cbr:backups:listStorageUsage	-
PUT /v3/{project_id}/order	cbr:vaults:updateOrder	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
s/{order_id}		
POST /v3/{project_id}/agents/{agent_id}/add-path	cbr:agents:addPath	-
GET /v3/{project_id}/agents/{agent_id}	cbr:agents:get	-
PUT /v3/{project_id}/agents/{agent_id}	cbr:agents:update	-
POST /v3/{project_id}/agents	cbr:agents:register	-
DELETE /v3/{project_id}/agents/{agent_id}	cbr:agents:delete	-
POST /v3/{project_id}/agents/{agent_id}/remove-path	cbr:agents:removePath	-
GET /v3/{project_id}/agents	cbr:agents:list	-
POST /v3/migrates	cbr:backups:migratesCreate	-
GET /v3/migrates	cbr:backups:migratesIndex	-
POST /v3/{project_id}/organization-policies	cbr:organizationPolicies:create	-
GET /v3/{project_id}/organization-policies/{organization_policy_id}/policy-detail	cbr:organizationPolicies:listPolicyDetail	-
DELETE /v3/{project_id}/organization-policies/{organization_policy_id}	cbr:organizationPolicies:delete	-
PUT /v3/{project_id}/organization-policies/{organization	cbr:organizationPolicies:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
_policy_id}		
GET /v3/{project_id}/organization-policies	cbr:organizationPolicies:list	-
GET /v3/{project_id}/organization-policies/{organization_policy_id}	cbr:organizationPolicies:get	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-30 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

CBR 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-30 CBR 支持的资源类型

资源类型	URN
vault	cbr:<region>:<account-id>:vault:<vault-id>
policy	cbr:<region>:<account-id>:policy:<policy-id>
task	cbr:<region>:<account-id>:task:<task-id>
backup	cbr:<region>:<account-id>:backup:<backup-id>
agent	cbr:<region>:<account-id>:agent:<agent-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 cbr:）仅适用于对应服务的操作，详情请参见表 3-31。

 版权所有 © 华为云计算技术有限公司

  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

CBR 支持的服务级条件键

CBR 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-31 CBR 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
cbr:TargetOrgPaths	string	单值	cbr 服务添加备份成员 API 请求中指定的目标账号所属的组织路径。
cbr:VaultId	string	单值	根据请求参数中指定的存储库 ID 过滤访问。
cbr:PolicyId	string	单值	根据请求参数中指定的策略 ID 过滤访问。
cbr:EnabledPolicy	boolean	单值	根据策略是否开启过滤访问。

3.2.3 云硬盘 EVS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

 版权所有 © 华为云计算技术有限公司

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 EVS 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 EVS 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 EVS 的相关操作。

表3-32 EVS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
evs::enableEncryptionByDefault	开启默认加密	Write	-	-	-
evs::disableEncryptionByDefault	关闭默认加密	Write	-	-	-
evs::getEncryptionByDefault	查询默认加密开关	Write	-	-	-
evs::modifyDefaultKmsKeyId	修改默认密钥	Write	-	evs:KmsKeyId	-
evs::resetDefaul	默认密钥重置	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
tKmsKeyId	回 evs/default 密钥				
evs::getDefaultKmsKeyId	查询默认密钥	Write	-	-	-
evs:volumes:create	授予创建云硬盘的权限。	Write	volume *	-	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • evs:Encrypted • cbr:VaultId • evs:KmsKeyId • evs:ImageId • evs:BackupId • evs:SnapshotId • evs:AvailabilityZone • evs:VolumeType • evs:VolumeSize • evs:VolumeIops • evs:VolumeThroughput • evs:ChargingMode • evs:ServerServiceType • ecs:ServerId • bms:ServerId • evs:SourceAvailabilityZo	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ne	
evs:volumes:list	授予查询云硬盘列表的权限。	List	-	g:EnterpriseProjectId	-
evs:volumes:get	授予查询云硬盘的权限。	Read	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
evs:volumes:delete	授予删除云硬盘的权限。	Write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
evs:volumes:update	授予更新云硬盘的权限。	Write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
evs:volumes:resize	授予扩容云硬盘的权限。	Write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	evs:volumes:extend
evs:volumes:modifyQos	授予修改云硬盘 QoS 的权限。	Write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	evs:volumes:extend
evs:volumes:retype	授予变更云硬盘的类型的权限。	Write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
evs:volumes:revert	授予从回收站还原云硬盘的权限。	Write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
evs:recycle_policy:get	授予查询回收站策略的权限。	Read	-	-	-
evs:recycle_policy:update	授予更新回收站策略的权限。	Write	-	-	-
evs:volumes:changeChargeMode	授予变更云硬盘计费模式的权限。	Write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
evs:snapshots:create	授予创建云硬盘快照的权限。	Write	snapshot *	-	-
			volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
			-	• evs:SourceAvailabilityZone • evs:AvailabilityZone	
evs:snapshots:list	授予查询云硬盘快照列表的权限。	List	-	g:EnterpriseProjectId	-
evs:snapshots:get	授予查询云硬盘快照的权限。	Read	-	g:EnterpriseProjectId	-
evs:snapshots:delete	授予删除云硬盘快照的权限。	Write	-	g:EnterpriseProjectId	-
evs:snapshots:update	授予更新云硬盘快照的权限。	Write	-	g:EnterpriseProjectId	-
evs:snapshots:rollback	授予回滚快照到云硬盘的权	Write	-	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
evs:types:get	授予查询云硬盘类型的权限。	Read	-	-	-
evs:quotas:get	授予查询云硬盘配额的权限。	Read	-	-	-
evs:volumes:tagResource	授予添加云硬盘标签的权限。	Write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	evs:volumeTags:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
evs:volumes:untagResource	授予删除云硬盘标签的权限。	Write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	evs:volumeTags:delete
			-	g:TagKeys	
evs:volumes:listTags	授予查询项目下所有云硬盘标签的权限。	List	-	-	evs:volumeTags:list
evs:volumes:listTagsForResource	授予查询云硬盘标签的权限。	Read	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	evs:volumeTags:getById
evs:volumes:listResourcesByTag	授予通过标签查询云硬盘实例列表的权限。	List	-	g:TagKeys	evs:volumeTags:get
evs:volumes:use	授予 ECS、BMS 使用磁盘的权限。	Write	-	g:EnterpriseProjectId	-
evs:imageCach	授予创建镜像	Write	image	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
e:create	缓存的权限。		Cache *		
			-	• evs:ImageId • evs:AvailabilityZone • evs:VolumeType • evs:SourceAvailabilityZone	
evs:imageCache:list	授予查询镜像缓存列表的权限。	List	-	-	-
evs:imageCache:delete	授予删除镜像缓存的权限。	Write	imageCache *	-	-

EVS 的 API 通常对应着一个或多个授权项。表 3-33 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-33 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v5/{project_id}/default-encryption/enable	evs::enableEncryptionByDefault	-
POST /v5/{project_id}/default-encryption/disable	evs::disableEncryptionByDefault	-
GET /v5/{project_id}/default-encryption/status	evs::getEncryptionByDefault	-
PUT /v5/{project_id}/default-encryption/key	evs::modifyDefaultKmsKeyId	-
PUT /v5/{project_id}/default-encryption/key/reset	evs::resetDefaultKmsKeyId	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/default-encryption/key	evs::getDefaultKmsKeyId	-
POST /v2.1/{project_id}/cloudvolumes	evs:volumes:create	billing:order:pay
POST /v2/{project_id}/cloudvolumes	evs:volumes:create	-
POST /v3/{project_id}/cloudvolumes	evs:volumes:create	-
GET /v2/{project_id}/cloudvolumes/detail	evs:volumes:list	-
GET /v2/{project_id}/cloudvolumes/{volume_id}	evs:volumes:get	-
DELETE /v2/{project_id}/cloudvolumes/{volume_id}	evs:volumes:delete	-
PUT /v2/{project_id}/cloudvolumes/{volume_id}	evs:volumes:update	-
POST /v2.1/{project_id}/cloudvolumes/{volume_id}/action	evs:volumes:resize	billing:order:pay
-	evs:volumes:resize	billing:order:pay
POST /v2/{project_id}/cloudvolumes/{volume_id}/action	evs:volumes:resize	-
PUT /v5/{project_id}/cloudvolumes/{volume_id}/qos	evs:volumes:modifyQos	-
POST /v2/{project_id}/volumes/{volume_id}/retype	evs:volumes:retype	billing:order:pay
POST /v2/{project_id}/cloud	evs:volumes:delete	billing:subscription:unsubscribe

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
volumes/unsubscribe		
POST /v2/{project_id}/cloud volumes/change-charge-mode	evs:volumes:changeChargeMode	• billing:order:pay • billing:subscription:renew
POST /v2/{project_id}/cloud snapshots	evs:snapshots:create	-
GET /v2/{project_id}/cloud snapshots/detail	evs:snapshots:list	-
GET /v2/{project_id}/cloud snapshots/{snapshot_id}	evs:snapshots:get	-
DELETE /v2/{project_id}/cloud snapshots/{snapshot_id}	evs:snapshots:delete	-
PUT /v2/{project_id}/cloud snapshots/{snapshot_id}	evs:snapshots:update	-
POST /v2/{project_id}/cloud snapshots/{snapshot_id}/rollback	evs:snapshots:rollback	-
POST /v2/{project_id}/cloud volumes/{volume_id}/tags/action	evs:volumes:tagResource	-
POST 01 /v2/{project_id}/cloud volumes/{volume_id}/tags/action	evs:volumes:unTagResource	-
GET /v2/{project_id}/cloud volumes/tags	evs:volumes:listTags	-
GET /v2/{project_id}/cloud volumes/{volume_id}/tags	evs:volumes:listTagsForResource	-
POST /v2/{project_id}/cloud	evs:volumes:listResourcesByTag	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
volumes/resource_instances/action		
GET /v1/{project_id}/image-caches	evs:imageCache:list	-
POST /v1/{project_id}/image-caches	evs:imageCache:create	-
DELETE /v1/{project_id}/image-caches/{image_cache_id}	evs:imageCache:delete	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-34 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

EVS 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-34 EVS 支持的资源类型

资源类型	URN
imageCache	evs:<region>:<account-id>:imageCache:<imageCache-id>
snapshot	evs:<region>:<account-id>:snapshot:<snapshot-id>
volume	evs:<region>:<account-id>:volume:<volume-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 evs:）仅适用于对应服务的操作，详情请参见表 3-35。

 版权所有 © 华为云计算技术有限公司

- 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。

- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

EVS 支持的服务级条件键

EVS 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-35 EVS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
evs:KmsKeyId	string	单值	根据云硬盘的密钥 ID 过滤访问。
evs:Encrypted	boolean	单值	根据云硬盘是否加密过滤访问。
evs:KmsKeyId	string	单值	根据云硬盘的密钥 ID 过滤访问。
evs:ImageId	string	单值	根据镜像 ID 过滤访问。
evs:BackupId	string	单值	根据备份 ID 过滤访问。
evs:SnapshotId	string	单值	根据快照 ID 过滤访问。
evs:AvailabilityZone	string	单值	根据云硬盘的可用区过滤访问。
evs:SourceAvailabilityZone	string	单值	根据源 AZ 过滤访问。
evs:VolumeType	string	单值	根据云硬盘的类型过滤访问。
evs:VolumeSize	numeric	单值	根据云硬盘的大小过滤访问。
evs:VolumeIops	numeric	单值	根据云硬盘的 IOPS 过滤访问。
evs:VolumeThroughput	numeric	单值	根据云硬盘的吞吐量过滤访问。

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
evs:ChargingMode	string	单值	根据云硬盘的计费模式过滤访问。
evs:ServerServiceType	string	单值	根据云服务器服务类型过滤访问。
evs:VolumeId	string	单值	根据云硬盘 ID 过滤访问。

3.2.4 高性能弹性文件服务 SFS Turbo

云服务在 IAM 预置了常用的权限，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 SFS Turbo 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。

 版权所有 © 华为云计算技术有限公司

- 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
- 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
- 如果此列条件键没有值（-），表示此操作不支持指定条件键。

关于 SFS Turbo 定义的条件键的详细信息请参见条件键。

- “**别名**”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 SFS Turbo 的相关操作。

表3-36 SFS Turbo 支持的授权项

操作项	描述	访问级别	资源类型（*为必须）	条件键
sfsturbo:shares:createShare	授予创建弹性文件系统的权限。	write	shares *	• g:EnterpriseProjectId • g:TagKeys • g:RequestTag/<tag-key> • sfsturbo:CryptKeyId • cbr:VaultId
sfsturbo:shares:deleteShare	授予删除弹性文件系统的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:getAllShares	授予查询弹性文件系统列表的权限。	list	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
sfsturbo:shares:getShare	授予查询弹性文件系统的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:extendShare	授予扩容弹性文件系统的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateHpcShare	授予更新弹性文件系统的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateSha	授予修改文件系统绑定的安	write	shares *	• g:ResourceTag/<tag-key>

 版权所有 © 华为云计算技术有限公司

操作项	描述	访问级别	资源类型（*为必须）	条件键
reSecurityGroup	全组的权限。			• g:EnterpriseProjectId
sfsturbo:shares:addTag	授予创建弹性文件系统共享标签的权限。	tagging	shares *	• g:ResourceTag/<tag-key> • g:TagKeys
sfsturbo:shares:getTag	授予查询弹性文件系统共享标签的权限。	read	shares *	g:EnterpriseProjectId
sfsturbo:shares:deleteTag	授予删除弹性文件系统共享标签的权限。	tagging	shares *	• g:ResourceTag/<tag-key> • g:TagKeys
sfsturbo:shares:batchResTag	授予批量添加弹性文件系统共享标签的权限。	tagging	shares *	• g:ResourceTag/<tag-key> • g:TagKeys
sfsturbo:shares:getAllTag	授予查询弹性文件系统共享标签列表的权限。	list	-	g:EnterpriseProjectId
sfsturbo:shares:renameShare	授予修改弹性文件系统名称的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showClientIpInfo	授予查询弹性文件系统客户端挂载 ip 列表的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:addDataRepository	授予设置弹性文件系统数据存储库的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createDataRepositoryTask	授予创建弹性文件系统数据存储库任务的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deleteDataRepositoryTask	授予删除弹性文件系统数据存储库任务的权限。	write	shares *	• g:ResourceTag/<tag-key> g:EnterpriseProjectId

 版权所有 © 华为云计算技术有限公司

操作项	描述	访问级别	资源类型（*为必须）	条件键
sfsturbo:shares:getDataRepositoryTask	授予查询弹性文件系统数据存储库任务的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:getAllDataRepositoryTasks	授予查询弹性文件系统数据存储库任务列表的权限。	list	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:getAZInfo	授予查询当前地区可用区信息的权限。	read	-	-
sfsturbo:shares:getQuota	授予查询弹性文件系统配额的权限。	read	-	-
sfsturbo:shares:getFlavors	授予查询弹性文件系统规格的权限。	read	-	-
sfsturbo:shares:checkShareName	授予检查弹性文件系统名称的权限。	read	-	-
sfsturbo:shares:createFsDir	授予创建弹性文件系统目录的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showFsDir	授予查询弹性文件系统目录的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deleteFsDir	授予删除弹性文件系统目录的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createFsDirQuota	授予创建弹性文件系统目录配额的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showFsDirQuota	授予查询弹性文件系统目录配额的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

 版权所有 © 华为云计算技术有限公司

操作项	描述	访问级别	资源类型（*为必须）	条件键
sfsturbo:shares:deleteFsDirQuota	授予删除弹性文件系统目录配额的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateFsDirQuota	授予更新弹性文件系统目录配额的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:batchCreateFsDirQuotas	授予批量创建弹性文件系统目录配额的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:listFsDirQuotas	授予查询弹性文件系统目录配额列表的权限。	list	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showFsDirUsage	授予查询弹性文件系统目录资源使用情况的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createFsAsyncTask	授予创建弹性文件系统异步任务的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showFsAsyncTask	授予查询弹性文件系统异步任务详情的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:listFsAsyncTasks	授予查询弹性文件系统异步任务列表的权限。	list	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deleteFsAsyncTask	授予删除弹性文件系统异步任务的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createBackendTarget	授予创建弹性文件系统后端存储库的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

 版权所有 © 华为云计算技术有限公司

操作项	描述	访问级别	资源类型（*为必须）	条件键
sfsturbo:shares:showBackendTargetInfo	授予查询弹性文件系统后端存储库详情的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:listBackendTargets	授予查询弹性文件系统后端存储库列表的权限。	list	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deleteBackendTarget	授予删除弹性文件系统后端存储库的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateObsTargetPolicy	授予修改弹性文件系统与 OBS 后端存储库之间自动数据流转策略的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateObsTargetAttributes	授予修改弹性文件系统后端存储库属性的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:listPermRules	授予查询弹性文件系统权限规则列表的权限。	list	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showPermRule	授予查询弹性文件系统权限规则详情的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createPermRule	授予创建弹性文件系统权限规则的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updatePermRule	授予修改文件系统权限规则的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deletePer	授予删除弹性文件系统权限	write	shares *	• g:ResourceTag/<tag-key>

 版权所有 © 华为云计算技术有限公司

操作项	描述	访问级别	资源类型（*为必须）	条件键
mRule	规则的权限。			• g:EnterpriseProjectId
sfsturbo:shares:showLdap	授予查询弹性文件系统 LDAP 配置的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createLdap	授予创建弹性文件系统 LDAP 配置的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateLdap	授予修改文件系统 LDAP 配置的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deleteLdap	授予删除弹性文件系统 LDAP 配置的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:addActiveDirectoryDomain	授予弹性文件系统加入 AD 域的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deleteActiveDirectoryDomain	授予弹性文件系统退出 AD 域的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showActiveDirectoryDomain	授予弹性文件系统查询 AD 域的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateActiveDirectoryDomain	授予弹性文件系统修改 AD 域配置的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:getJob	授予查询弹性文件系统任务详情的权限。	read	-	-
sfsturbo:shares:changeChargeMode	授予变更弹性文件系统计费模式的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

 版权所有 © 华为云计算技术有限公司

操作项	描述	访问级别	资源类型（*为必须）	条件键
sfsturbo:shares:getFlavors	授予查询弹性文件系统规格的权限。	read	shares *	-

SFS Turbo 的 API 通常对应着一个或多个操作项。表 3-37 展示了 API 与操作项的关系，以及该 API 需要依赖的操作项。

表3-37 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/sfs-turbo/shares	sfsturbo:shares:createShare	• billing:order:pay • billing:contract:viewDiscount • vpc:vpcs:get • vpc:subnets:get • vpc:securityGroups:get • vpc:securityGroups:create • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:securityGroupRules:get • vpc:securityGroupRules:create • vpc:quotas:list • cbr:backups:get • cbr:vaults:addResources • evs:types:get • kms:cmk:listGrants • kms:cmk:createGrant • kms:cmk:get • sfsturbo:shares:getAZInfo • sfsturbo:shares:getQuota • sfsturbo:shares:getFlavors • sfsturbo:shares:checkShareName • eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/sfs-turbo/shares/detail	sfsturbo:shares:getAllShares	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}	sfsturbo:shares:getShare	-
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}	sfsturbo:shares:deleteShare	• vpc:ports:get • vpc:ports:delete • vpc:securityGroupRules:delete • vpc:securityGroups:delete
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/action	sfsturbo:shares:extendShare	• billing:order:pay • vpc:vpcs:get • vpc:subnets:get • vpc:ports:get • vpc:ports:create • vpc:ports:update
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/action	sfsturbo:shares:updateShareSecurityGroup	• vpc:ports:update • vpc:securityGroups:get • vpc:securityGroupRules:create • vpc:securityGroupRules:delete
POST /v1/{project_id}/sfs-turbo/{share_id}/tags	sfsturbo:shares:addTag	-
GET /v1/{project_id}/sfs-turbo/{share_id}/tags	sfsturbo:shares:getTag	-
DELETE /v1/{project_id}/sfs-turbo/{share_id}/tags/{key}	sfsturbo:shares:deleteTag	-
POST /v1/{project_id}/sfs-turbo/{share_id}/tags/action	sfsturbo:shares:batchResTag	-
POST /v1/{project_id}/sfs-turbo/resource_instances/action	sfsturbo:shares:getAllTag	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/action	sfsturbo:shares:renameShare	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/{feature}/tasks	sfsturbo:shares:createFsAsyncTask	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/{feature}/tasks	sfsturbo:shares:listFsAsyncTasks	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/{feature}/tasks/{task_id}	sfsturbo:shares:showFsAsyncTask	-
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/{feature}/tasks/{task_id}	sfsturbo:shares:deleteFsAsyncTask	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/action	sfsturbo:shares:addDataRepository	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/targets	sfsturbo:shares:createBackendTarget	• obs:bucket:putBucketPolicy • vpc:ports:get • vpc:ports:create • vpc:subnets:get
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/targets	sfsturbo:shares:listBackendTargets	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/targets/{target_id}	sfsturbo:shares:showBackendTargetInfo	-
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/targets/{target_id}	sfsturbo:shares:deleteBackendTarget	-
POST /v1/{project_id}/sfs-turbo/{share_id}/hpc-cache/task	sfsturbo:shares:createDataRepositoryTask	obs:bucket:headBucket
GET /v1/{project_id}/sfs-turbo/{share_id}/hpc-cache/task/{task_id}	sfsturbo:shares:getDataRepositoryTask	-
GET /v1/{project_id}/sfs-turbo/{share_id}/hpc-cache/tasks	sfsturbo:shares:getAllDataRepositoryTasks	-
PUT /v1/{project_id}/sfs-turbo/shares/{share_id}	sfsturbo:shares:updateHpcShare	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-quota	sfsturbo:shares:createFsDirQuota	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-quota	sfsturbo:shares:updateFsDirQuota	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-quota	sfsturbo:shares:showFsDirQuota	-
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-quota	sfsturbo:shares:deleteFsDirQuota	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir	sfsturbo:shares:createFsDir	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir	sfsturbo:shares:showFsDir	-
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir	sfsturbo:shares:deleteFsDir	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-usage	sfsturbo:shares:showFsDirUsage	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules	sfsturbo:shares:createPermRule	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules	sfsturbo:shares:listPermRules	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules/{rule_id}	sfsturbo:shares:showPermRule	-
PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules/{rule_id}	sfsturbo:shares:updatePermRule	-
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules/{rule_id}	sfsturbo:shares:deletePermRule	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/ldap	sfsturbo:shares:createLdap	-
GET /v1/{project_id}/sfs-	sfsturbo:shares:showLdap	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
turbo/shares/{share_id}/fs/ldap		
PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/ldap	sfsturbo:shares:updateLdap	-
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/ldap	sfsturbo:shares:deleteLdap	-
GET /v1/{project_id}/sfs-turbo/jobs/{job_id}	sfsturbo:shares:getJob	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/action	sfsturbo:shares:showClientIpInfo	-
DELETE /v1/{project_id}/sfs-turbo/{share_id}/hpc-cache/task/{task_id}	sfsturbo:shares:deleteDataRepositoryTask	-
PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/targets/{target_id}/policy	sfsturbo:shares:updateObsTargetPolicy	-
PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/targets/{target_id}/attributes	sfsturbo:shares:updateObsTargetAttributes	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/active-directory-domain	sfsturbo:shares:addActiveDirectoryDomain	-
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/active-directory-domain	sfsturbo:shares:deleteActiveDirectoryDomain	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/active-directory-domain	sfsturbo:shares:showActiveDirectoryDomain	-
PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/active-directory-domain	sfsturbo:shares:updateActiveDirectoryDomain	-
POST /v2/{project_id}/sfs-turbo/shares/{share_id}/change-charge-mode	sfsturbo:shares:changeChargeMode	-
GET /v1/{project_id}/sfs-turbo/share-types	sfsturbo:shares:getFlavors	-

 版权所有 © 华为云计算技术有限公司

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-38 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，策略仅作用于此资源；如未指定，Resource 默认为“*”，则策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

SFS Turbo 定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-38 SFS Turbo 支持的资源类型

资源类型	URN
shares	shares *

条件键

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 SFS Turbo 仅适用于对应服务的操作，详情请参见表 3-39。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

SFS Turbo 支持的服务级条件键

SFS Turbo 定义了以下可以在身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-39 SFS Turbo 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
sfsturbo:CryptKeyId	string	单值	根据请求参数中指定的密钥 ID 过滤访问。

 版权所有 © 华为云计算技术有限公司

3.2.5 键值存储服务 KVS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 KVS 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 KVS 定义的条件键的详细信息请参见条件（Condition）。
- **“别名”**列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 KVS 的相关操作。

 版权所有 © 华为云计算技术有限公司

表3-40 KVS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
kvs:store:list	授予用户列举存储仓的权限。	list	store *	-	-
kvs:store:createTable	授予用户在存储仓创建表的权限。	write	store *	-	-
kvs:store:listTable	授予用户在存储仓列举表的权限。	list	store *	-	-
kvs:table:describe	授予用户在存储仓查看表的权限。	read	table *	-	-
kvs:table:putKv	授予用户在表中插入或更新 KV 的权限。	write	table *	-	-
kvs:table:getKv	授予用户在表中查询 KV 的权限。	read	table *	-	-
kvs:table:updateKv	授予用户在表中更新 KV 的权限。	write	table *	-	-
kvs:table:deleteKv	授予用户在表中删除 KV 的权限。	write	table *	-	-
kvs:table:scanKv	授予用户在表中扫描所有 KV 的权限。	read	table *	-	-
kvs:table:scanSkeyKv	授予用户在表中使用分区键扫描所有 KV 的权限。	read	table *	-	-
kvs:table:bat	授予用户在	write	table *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
chWriteKv	表中执行批量写的权限。				

KVS 的 API 通常对应着一个或多个授权项。表 3-41 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-41 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/list-store	kvs:store:list	-
POST /v1/create-table	kvs:store:createTable	-
POST /v1/list-table	kvs:store:listTable	-
POST /v1/describe-table	kvs:table:describe	-
POST /v1/put-kv	kvs:table:putKv	-
POST /v1/get-kv	kvs:table:getKv	-
POST /v1/update-kv	kvs:table:updateKv	-
POST /v1/delete-kv	kvs:table:deleteKv	-
POST /v1/scan-kv	kvs:table:scanKv	-
POST /v1/scan-skey-kv	kvs:table:scanSkeyKv	-
POST /v1/batch-write-kv	kvs:table:batchWriteKv	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3 kvs 支持的资源类型中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的 URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

kvs 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-42 kvs 支持的资源类型

资源类型	URN
store	kvs:<region>:<account-id>:store:<storename>
table	kvs:<region>:<account-

 版权所有 © 华为云计算技术有限公司

资源类型	URN
	id>:table:<storename>/<tablename>

条件（Condition）

KVS 服务不支持在身份策略中的条件键中配置服务级的条件键。

KVS 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.3 网络

3.3.1 企业路由器 ER

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

 版权所有 © 华为云计算技术有限公司

关于 er 定义的资源类型的详细信息请参见资源类型（Resource）。

- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 er 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 er 的相关操作。

表3-43 er 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
er:instances:get	授予查询实例详情权限。	Read	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:instances:create	授予创建实例权限。	Write	instances *	g:EnterpriseProjectId	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
er:instances:list	授予查询实例列表权限。	List	instances *	-	-
er:instances:update	授予更新实例权限。	Write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:instances:delete	授予删除实例权限。	Write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:instances:changeAZ	授予更改实例可用区权限。	Write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				key>	
er:instances:createVpcAttachment	授予创建 VPC 连接权限。	Write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:create
er:instances:showVpcAttachment	授予查询 VPC 连接详情权限。	Read	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:get
er:instances:listVpcAttachments	授予查询 VPC 连接列表权限。	List	instances *	-	er:attachments:list
er:instances:updateVpcAttachment	授予更新 VPC 连接权限。	Write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:update
er:instances:deleteVpcAttachment	授予删除 VPC 连接权限。	Write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:delete
er:commonAttachments:get	授予查询连接详情权限。	Read	attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:get
er:commonAttachments:list	授予查询连接列表权限。	List	attachments *	-	er:attachments:list
er:commonAttachments:update	授予更新连接权限。	Write	attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:update
er:attachments:accept	授予接受连接权限。	Write	attachments	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			*		
er:attachments:reject	授予拒绝连接权限。	Write	attachments *	g:EnterpriseProjectId	-
er:routeTables:get	授予查询路由表详情权限。	Read	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:routeTables:create	授予创建路由表权限。	Write	routeTables *	-	-
			instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
er:routeTables:list	授予查询路由表列表权限。	List	routeTables *	-	-
er:routeTables:update	授予更新路由表权限。	Write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:routeTables:delete	授予删除路由表权限。	Write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:routeTables:associate	授予将连接和路由表关联的权限。	Write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:associations:associate
			attach	• g:Enterprise	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			ments *	ProjectId • g:ResourceTag/<tag-key>	
er:routeTables:disassociate	授予解除连接和路由表关联的权限。	Write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:associations:disassociate
			attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:routeTables:listAssociations	授予查询关联列表的权限。	List	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:associations:list
er:routeTables:enablePropagation	授予允许连接将路由传播到传播路由表的权限。	Write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:propagations:enable
			attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:routeTables:disablePropagation	授予禁止连接将路由传播到指定传播路由表的权限。	Write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:propagations:disable
			attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:routeTables:l	授予查询传播	List	routeT	• g:Enterprise	er:propagations:

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
istPropagations	列表的权限。		ables *	ProjectId • g:ResourceTag/<tag-key>	list
er:staticRoutes:list	授予查询静态路由列表的权限。	List	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:list
er:staticRoutes:create	授予创建静态路由的权限。	Write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:create
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:effectiveRoutes:list	授予查询有效路由列表的权限。	List	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:list
er:staticRoutes:delete	授予删除静态路由的权限。	Write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:delete
er:staticRoutes:update	授予更新静态路由的权限。	Write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:update
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:staticRoutes:	授予查询静态	Read	routeT	• g:Enterprise	er:routes:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
get	路由的权限。		ables *	ProjectId • g:ResourceTag/<tag-key>	
er:tags:singleCreate	授予创建资源标签的权限。	Write	routeTables	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:tags:create
			instances	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:tags:delete	授予删除资源标签的权限。	Write	routeTables	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			instances	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:tags:batchOperation	授予批量创建或者删除资源标签的权限。	Write	routeTables	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:tags:create
			instan	• g:Enterprise	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			ces	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:tags:get	授予查询特定资源的标签的权限。	Read	routeTables	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			instances	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:tags:list	授予查询资源标签列表的权限。	List	-	-	-
er:quotas:list	授予查询资源配额的权限。	List	-	-	-
er:flowLogs:create	授予创建流日志的权限。	Write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			flowLogs *	-	
er:flowLogs:list	授予查询流日志列表的权限。	List	flowLogs *	-	-
er:flowLogs:get	授予查询流日志的权限。	Read	flowLogs *	-	-
er:flowLogs:update	授予更新流日志的权限。	Write	flowLogs *	-	-
er:flowLogs:delete	授予删除流日志的权限。	Write	flowLogs *	-	-
er:flowLogs:enable	授予开启流日志的权限。	Write	flowLogs *	-	-
er:flowLogs:disable	授予关闭流日志的权限。	Write	flowLogs *	-	-

er 的 API 通常对应着一个或多个授权项。表 3-44 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-44 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/enterprise-router/instances	er:instances:create	-
PUT /v3/{project_id}/enterprise-router/instances/{er_id}	er:instances:update	-
GET /v3/{project_id}/enterprise-router/instances/{er_id}	er:instances:get	-
GET /v3/{project_id}/enterprise-router/instances	er:instances:list	-
POST /v3/{project_id}/enterprise-router/instances/{er_id}/change-availability-zone-ids	er:instances:changeAZ	-
DELETE /v3/{project_id}/enterprise-router/instances/{er_id}	er:instances:delete	-
POST /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments	er:instances:createVpcAttachment	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments/{vpc_attachment_id}	er:instances:updateVpcAttachment	-
GET /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments/{vpc_attachment_id}	er:instances:showVpcAttachment	-
GET /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments	er:instances:listVpcAttachments	-
DELETE /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments/{vpc_attachment_id}	er:instances:deleteVpcAttachment	-
PUT /v3/{project_id}/enterprise-router/{er_id}/attachments/{attachment_id}	er:commonAttachments:update	-
GET /v3/{project_id}/enterprise-router/{er_id}/attachments/{attachment_id}	er:commonAttachments:get	-
GET /v3/{project_id}/enterprise-router/{er_id}/attachments	er:commonAttachments:list	-
POST /v3/{project_id}/enterprise-router/{er_id}/attachments/{attachment_id}/accept	er:attachments:accept	-
POST /v3/{project_id}/enterprise-router/{er_id}/attachments/{attachment_id}/reject	er:attachments:reject	-
POST /v3/{project_id}/enterprise-router/{er_id}/route-tables	er:routeTables:create	-
PUT /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}	er:routeTables:update	-
GET /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}	er:routeTables:get	-
GET /v3/{project_id}/enterprise-router/{er_id}/route-tables	er:routeTables:list	-
DELETE /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}	er:routeTables:delete	-
POST /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/associate	er:routeTables:associate	-
GET /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/associations	er:routeTables:listAssociations	-
POST /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/disassociate	er:routeTables:disassociate	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/enable-propagations	er:routeTables:enablePropagation	-
GET /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/propagations	er:routeTables:listPropagations	-
POST /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/disable-propagations	er:routeTables:disablePropagation	-
POST /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/static-routes	er:staticRoutes:create	-
PUT /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/static-routes/{route_id}	er:staticRoutes:update	-
GET /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/static-routes/{route_id}	er:staticRoutes:get	-
GET /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/static-routes	er:staticRoutes:list	-
GET /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/routes	er:effectiveRoutes:list	-
DELETE /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/static-routes/{route_id}	er:staticRoutes:delete	-
GET /v3/{project_id}/{resource_type}/tags	er:tags:list	-
GET /v3/{project_id}/{resource_type}/{resource_id}/tags	er:tags:get	-
POST /v3/{project_id}/{resource_type}/{resource_id}/tags	er:tags:singleCreate	-
POST /v3/{project_id}/{resource_type}/{resource_id}/tags/action	er:tags:batchOperation	-
DELETE /v3/{project_id}/{resource_type}/{resource_id}/tags/{key}	er:tags:delete	-
GET /v3/{project_id}/enterprise-router/quotas	er:quotas:list	-
POST /v3/{project_id}/enterprise-router/{er_id}/flow-logs	er:flowLogs:create	-
GET /v3/{project_id}/enterprise-router/{er_id}/flow-logs	er:flowLogs:list	-
GET /v3/{project_id}/enterprise-	er:flowLogs:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
router/{er_id}/flow-logs/{flow_log_id}		
PUT /v3/{project_id}/enterprise-router/{er_id}/flow-logs/{flow_log_id}	er:flowLogs:update	-
DELETE /v3/{project_id}/enterprise-router/{er_id}/flow-logs/{flow_log_id}	er:flowLogs:delete	-
POST /v3/{project_id}/enterprise-router/{er_id}/flow-logs/{flow_log_id}/enable	er:flowLogs:enable	-
POST /v3/{project_id}/enterprise-router/{er_id}/flow-logs/{flow_log_id}/disable	er:flowLogs:disable	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-45 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

er 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-45 er 支持的资源类型

资源类型	URN
instances	er:<region>:<account-id>:instances:<instance-id>
routeTables	er:<region>:<account-id>:routeTables:<route-table-id>
flowLogs	er:<region>:<account-id>:flowFlogs:<flow-log-id>
attachments	er:<region>:<account-id>:attachments:<attachment-id>

条件（Condition）

er 服务不支持在身份策略中的条件键中配置服务级的条件键。er 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.3.2 虚拟私有云 VPC

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

 版权所有 © 华为云计算技术有限公司

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 vpc 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 vpc 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 vpc 的相关操作。

表3-46 vpc 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
vpc:vpcs:create	授予创建虚拟私有云权限。	Write	vpc *	-	-
			-	• g:Enterprise	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ProjectId • g:RequestTag/<tag-key> • g:TagKeys • vpc:VpcBlockServiceEndpointStates	
vpc:vpcs:get	授予查询虚拟私有云详情权限。	Read	vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId	-
vpc:vpcs:list	授予查询虚拟私有云列表权限。	List	vpc *	-	-
			-	g:EnterpriseProjectId	
vpc:vpcs:update	授予更新虚拟私有云权限。	Write	vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId	-
			-	vpc:VpcBlockServiceEndpointStates	
vpc:vpcs:delete	授予删除虚拟私有云权限。	Write	vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId	-
vpc:subnets:create	授予创建子网权限。	Write	subnet *	-	-
			vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	• vpc:AvailabilityZone • vpc:SubnetIpv6Enable • g:RequestTag/<tag-key> • g:TagKeys	
vpc:subnets:get	授予查询子网详情权限。	Read	subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • vpc:AvailabilityZone • g:EnterpriseProjectId	-
vpc:subnets:list	授予查询子网列表权限。	List	subnet *	-	vpc:subnets:get
			-	g:EnterpriseProjectId	
vpc:subnets:update	授予更新子网权限。	Write	subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • vpc:AvailabilityZone • g:EnterpriseProjectId	-
			-	vpc:SubnetIpv6Enable	
vpc:subnets:delete	授予删除子网权限。	Write	subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• vpc:AvailabilityZone • g:EnterpriseProjectId	
vpc:subnets:createReservation	授予创建子网预留网段权限。	Write	subnet *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
vpc:subnets:getReservation	授予查询子网预留网段详情权限。	Read	subnet *	• g:ResourceTag/<tag-key> • vpc:VirsubnetCidrReservationId • g:EnterpriseProjectId	-
vpc:subnets:listReservations	授予查询子网预留网段列表权限。	List	subnet *	-	-
			-	g:EnterpriseProjectId	
vpc:subnets:updateReservation	授予更新子网预留网段权限。	Write	subnet *	• g:ResourceTag/<tag-key> • vpc:VirsubnetCidrReservationId • g:EnterpriseProjectId	-
vpc:subnets:deleteReservation	授予删除子网预留网段权限。	Write	subnet *	• g:ResourceTag/<tag-key> • vpc:VirsubnetCidrReservationId • g:EnterpriseProjectId	-
vpc:quotas:list	授予查询资源配额权限。	List	-	-	vpc:quotas:get
vpc:privateIps:c	授予创建私有	Write	privat	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
reate	IP 权限。		eIp *		
			subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • vpc:AvailabilityZone	
vpc:privateIps:get	授予查询私有 IP 详情权限。	Read	privateIp *	• vpc:PrivateIpId • vpc:SubnetId • vpc:VpcId	-
vpc:privateIps:list	授予查询私有 IP 列表权限。	List	privateIp *	-	-
vpc:privateIps:delete	授予删除私有 IP 权限。	Write	privateIp *	• vpc:PrivateIpId • vpc:SubnetId • vpc:VpcId	-
vpc:securityGroups:create	授予创建安全组权限。	Write	securityGroup *	-	-
			securityGroupRule	• vpc:SecurityGroupRuleDirection • vpc:SecurityGroupRuleProtocol • vpc:SecurityGroupRuleAction • vpc:SecurityGroupRulePort • vpc:SecurityGroupRuleRemoteIpAddressGroup	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• vpc:SecurityGroupRuleRemoteSecurityGroup • vpc:SecurityGroupRuleRemoteIpPrefix	
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
vpc:securityGroups:get	授予查询安全组详情权限。	Read	securityGroup *	• g:EnterpriseProjectId • vpc:SecurityGroupId • g:ResourceTag/<tag-key>	-
vpc:securityGroups:list	授予查询安全组列表权限。	List	securityGroup *	-	vpc:securityGroups:get
			-	g:EnterpriseProjectId	
vpc:securityGroups:update	授予更新安全组权限。	Write	securityGroup *	• g:EnterpriseProjectId • vpc:SecurityGroupId • g:ResourceTag/<tag-key>	-
vpc:securityGroups:delete	授予删除安全组权限。	Write	securityGroup *	• g:EnterpriseProjectId • vpc:SecurityGroupId • g:ResourceTag/<tag-key>	-
vpc:securityGro	授予创建安全	Write	securityGrou	• vpc:SecurityGroupRuleD	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
upRules:create	组规则权限。		pRule *	irection • vpc:SecurityGroupRuleProtocol • vpc:SecurityGroupRuleAction • vpc:SecurityGroupRulePort • vpc:SecurityGroupRuleRemoteIpAddressGroup • vpc:SecurityGroupRuleRemoteSecurityGroup • vpc:SecurityGroupRuleRemoteIpPrefix	
			securityGroup *	• g:EnterpriseProjectId • vpc:SecurityGroupId • g:ResourceTag/<tag-key>	
vpc:securityGroupRules:get	授予查询安全组规则详情权限。	Read	securityGroupRule *	• g:EnterpriseProjectId • vpc:SecurityGroupId	-
vpc:securityGroupRules:list	授予查询安全组规则列表权限。	List	-	g:EnterpriseProjectId	vpc:securityGroupRules:get
vpc:securityGroupRules:update	授予更新安全组规则权限。	Write	securityGroupRule *	• g:EnterpriseProjectId • vpc:SecurityGroupId	-
			-	• vpc:Security	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				GroupRuleDirection • vpc:SecurityGroupRuleProtocol • vpc:SecurityGroupRuleAction • vpc:SecurityGroupRulePort • vpc:SecurityGroupRuleRemoteIpAddressGroup • vpc:SecurityGroupRuleRemoteSecurityGroup • vpc:SecurityGroupRuleRemoteIpPrefix	
vpc:securityGroupRules:delete	授予删除安全组规则权限。	Write	securityGroupRule *	• g:EnterpriseProjectId • vpc:SecurityGroupId	-
vpc:ports:create	授予创建端口权限。	Write	port *	-	-
			subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • vpc:AvailabilityZone • g:EnterpriseProjectId	
			-	• g:RequestTag/<tag-key> • g:TagKeys	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
vpc:ports:get	授予查询端口详情权限。	Read	port *	• vpc:SubnetId • vpc:PortId • vpc:VpcId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
vpc:ports:list	授予查询端口列表权限。	List	port *	-	vpc:ports:get
			-	g:EnterpriseProjectId	
vpc:ports:update	授予更新端口权限。	Write	port *	• vpc:SubnetId • vpc:PortId • vpc:VpcId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:vips:update
vpc:ports:delete	授予删除端口权限。	Write	port *	• vpc:SubnetId • vpc:PortId • vpc:VpcId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
vpc:peerings:create	授予创建对等连接权限。	Write	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:AccepterVpcOrgPath • vpc:AccepterVpcOwner	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			vpc *	• g:ResourceTag/<tag-key> • vpc:VpcId	
vpc:peerings:get	授予查询对等连接详情权限。	Read	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:PeeringId	-
vpc:peerings:list	授予查询对等连接列表权限。	List	peering *	-	vpc:peerings:get
vpc:peerings:accept	授予接受对等连接权限。	Write	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:PeeringId • vpc:RequesterVpcOrgPath • vpc:RequesterVpcOwner	-
vpc:peerings:reject	授予拒绝对等连接权限。	Write	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:PeeringId	-
vpc:peerings:update	授予更新对等连接权限。	Write	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:PeeringId	-
vpc:peerings:delete	授予删除对等连接权限。	Write	peering *	• vpc:AccepterVpcId • vpc:Request	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				erVpcId • vpc:PeeringId	
vpc:routeTables:create	授予创建路由表权限。	Write	routeTable *	-	-
			vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId	
vpc:routeTables:get	授予查询路由表详情权限。	Read	routeTable *	• vpc:RouteTableId • vpc:VpcId • g:EnterpriseProjectId	-
vpc:routeTables:list	授予查询路由表列表权限。	List	routeTable *	-	-
			-	g:EnterpriseProjectId	
vpc:routeTables:update	授予更新路由表权限。	Write	routeTable *	• vpc:RouteTableId • vpc:VpcId • g:EnterpriseProjectId	-
vpc:routeTables:associate	授予关联路由表权限。	Write	routeTable *	• vpc:RouteTableId • vpc:VpcId	-
			subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • vpc:AvailabilityZone • g:EnterpriseProjectId	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
vpc:routeTables:delete	授予删除路由表权限。	Write	routeTable *	• vpc:RouteTableId • vpc:VpcId • g:EnterpriseProjectId	-
vpc:flowLogs:create	授予创建流日志权限。	Write	flowLog *	-	-
			port	• vpc:PortId • vpc:SubnetId • vpc:VpcId	
			subnet	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • vpc:AvailabilityZone	
			vpc	• g:ResourceTag/<tag-key> • vpc:VpcId	
			-	vpc:FlogLogResourceType	
vpc:flowLogs:get	授予查询流日志列表或详情权限。	Read	flowLog *	• vpc:FlowLogId • vpc:FlogLogResourceType	-
vpc:flowLogs:list	授予查询流日志列表权限。	List	flowLog *	-	vpc:flowLogs:get
vpc:flowLogs:update	授予更新流日志权限。	Write	flowLog *	• vpc:FlowLogId • vpc:FlogLogResourceType	-
vpc:flowLogs:d	授予删除流日	Write	flowL	• vpc:FlowLo	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
elete	志权限。		og *	gId • vpc:FlogLogResourceType	
vpc:addressGroups:create	授予创建 IP 地址组权限。	Write	addressGroup *	-	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
vpc:addressGroups:get	授予查询 IP 地址组详情权限。	Read	addressGroup *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:AddressGroupId	-
vpc:addressGroups:list	授予查询 IP 地址组列表权限。	List	addressGroup *	-	-
			-	g:EnterpriseProjectId	
vpc:addressGroups:update	授予更新 IP 地址组权限。	Write	addressGroup *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:AddressGroupId	-
vpc:addressGroups:delete	授予删除 IP 地址组权限。	Write	addressGroup *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:AddressGroupId	-
vpc:firewalls:create	授予创建网络	Write	firewall *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	ACL 权限。		-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
vpc:firewalls:get	授予查询网络 ACL 详情权限。	Read	firewall *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:FirewallId	-
vpc:firewalls:list	授予查询网络 ACL 列表权限。	List	firewall *	-	-
			-	g:EnterpriseProjectId	
vpc:firewalls:update	授予更新网络 ACL 权限。	Write	firewall *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:FirewallId • vpc:FirewallRuleDirection • vpc:FirewallRuleProtocol • vpc:FirewallRuleAction • vpc:FirewallRuleSourcePort • vpc:FirewallRuleDestinationPort • vpc:FirewallOperationType • vpc:Firewall	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				RuleSourceIp • vpc:FirewallRuleSourceIpAddressGroup • vpc:FirewallRuleDestinationIp • vpc:FirewallRuleDestinationIpAddressGroup	
			subnet	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • vpc:AvailabilityZone • g:EnterpriseProjectId	
vpc:firewalls:delete	授予删除网络ACL权限。	Write	firewall *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:FirewallId	-
vpc:vpcs:createTags	授予创建虚拟私有云资源标签权限。	Tagging	vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId	vpc:vpcTags:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
vpc:vpcs:listTags	授予查询虚拟私有云资源标	List	vpc *	-	vpc:vpcTags:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	签权限。				
vpc:vpcs:deleteTags	授予删除虚拟私有云资源标签权限。	Tagging	vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId	vpc:vpcTags:delete
			-	g:TagKeys	
vpc:subnets:createTags	授予创建子网资源标签权限。	Tagging	subnet *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId • vpc:SubnetId • vpc:AvailabilityZone	vpc:subnetTags:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
vpc:subnets:listTags	授予查询子网资源标签权限。	List	subnet *	-	vpc:subnetTags:get
vpc:subnets:deleteTags	授予删除子网资源标签权限。	Tagging	subnet *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId • vpc:SubnetId • vpc:AvailabilityZone	vpc:subnetTags:delete
			-	g:TagKeys	
vpc:addressGroups:createTags	授予创建 IP 地址组资源标签	Tagging	addressGroup *	• g:EnterpriseProjectId • g:ResourceT	vpc:addressGroupTags:create

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	权限。			ag/<tag-key> • vpc:AddressGroupId	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
vpc:addressGroups:listTags	授予查询 IP 地址组资源标签权限。	List	addressGroup *	-	vpc:addressGroupTags:get
vpc:addressGroups:deleteTags	授予删除 IP 地址组资源标签权限。	Tagging	addressGroup *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:AddressGroupId	vpc:addressGroupTags:delete
			-	g:TagKeys	
vpc:securityGroups:createTags	授予创建安全组资源标签权限。	Tagging	securityGroup *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:SecurityGroupId	vpc:securityGroupTags:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
vpc:securityGroups:listTags	授予查询安全组资源标签权限。	List	securityGroup *	-	vpc:securityGroupTags:get
vpc:securityGroups:deleteTags	授予删除安全组资源标签权限。	Tagging	securityGroup *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:SecurityGroupId	vpc:securityGroupTags:delete

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	g:TagKeys	
vpc:firewalls:createTags	授予创建网络ACL资源标签权限。	Tagging	firewall *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:FirewallId	vpc:firewallTags:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
vpc:firewalls:listTags	授予查询网络ACL资源标签权限。	List	firewall *	-	vpc:firewallTags:get
vpc:firewalls:deleteTags	授予删除网络ACL资源标签权限。	Tagging	firewall *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:FirewallId	vpc:firewallTags:delete
			-	g:TagKeys	
vpc:subNetworkInterfaces:createTags	授予创建辅助弹性网卡资源标签权限。	Tagging	subNetworkInterface *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:SubNetworkInterfaceId • vpc:SubnetId • vpc:VpcId	vpc:subNetworkInterfaceTags:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
vpc:subNetworkInterfaces:listTags	授予查询辅助弹性网卡资源	List	subNetworkInterfa	-	vpc:subNetworkInterfaceTags:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	标签权限。		ce *		
vpc:subNetworkInterfaces:deleteTags	授予删除辅助弹性网卡资源标签权限。	Tagging	subNetworkInterface *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:SubNetworkInterfaceId • vpc:SubnetId • vpc:VpcId	vpc:subNetworkInterfaceTags:delete
			-	g:TagKeys	
vpc:ports:createTags	授予创建端口资源标签权限。	Tagging	port *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:PortId • vpc:SubnetId • vpc:VpcId	vpc:portTags:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
vpc:ports:listTags	授予查询端口资源标签权限。	List	port *	-	vpc:portTags:get
vpc:ports:deleteTags	授予删除端口资源标签权限。	Tagging	port *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:PortId • vpc:SubnetId • vpc:VpcId	vpc:portTags:delete
			-	g:TagKeys	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
vpc:subNetworkInterfaces:create	授予创建辅助弹性网卡权限。	Write	subNetworkInterface *	-	-
			subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • vpc:AvailabilityZone	
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
vpc:subNetworkInterfaces:get	授予查询辅助弹性网卡详情权限。	Read	subNetworkInterface *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:SubNetworkInterfaceId • vpc:VpcId	-
vpc:subNetworkInterfaces:list	授予查询辅助弹性网卡列表权限。	List	subNetworkInterface *	-	-
			-	g:EnterpriseProjectId	
vpc:subNetworkInterfaces:update	授予更新辅助弹性网卡权限。	Write	subNetworkInterface *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:SubnetI	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				d • vpc:SubNetworkInterfaceId • vpc:VpcId	
vpc:subNetworkInterfaces:delete	授予删除辅助弹性网卡权限。	Write	subNetworkInterface *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:SubNetworkInterfaceId • vpc:VpcId	-
vpc:networks:create	授予创建网络权限。	Write	network *	-	-
vpc:networks:get	授予查询网络详情权限。	Read	network *	-	-
vpc:networks:list	授予查询网络列表权限。	List	network *	-	vpc:networks:get
vpc:networks:update	授予更新网络权限。	Write	network *	-	-
vpc:networks:delete	授予删除网络权限。	Write	addressGroup *	-	-
vpc:trafficMirrorFilters:create	授予创建流量镜像筛选条件权限。	Write	trafficMirrorFilter *	-	-
vpc:trafficMirrorFilters:get	授予查询流量镜像筛选条件详情权限。	Read	trafficMirrorFilter *	-	-
vpc:trafficMirrorFilters:list	授予查询流量镜像筛选条件列表权限。	List	trafficMirrorFilter *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
vpc:trafficMirrorFilters:update	授予更新流量镜像筛选条件权限。	Write	trafficMirrorFilter *	-	-
vpc:trafficMirrorFilters:delete	授予删除流量镜像筛选条件权限。	Write	trafficMirrorFilter *	-	-
vpc:trafficMirrorFilterRules:create	授予创建流量镜像筛选条件规则权限。	Write	trafficMirrorFilter *	-	-
			trafficMirrorFilterRule *	-	
vpc:trafficMirrorFilterRules:get	授予查询流量镜像筛选条件规则详情权限。	Read	trafficMirrorFilterRule *	vpc:TrafficMirrorFilterId	-
vpc:trafficMirrorFilterRules:list	授予查询流量镜像筛选条件规则列表权限。	List	trafficMirrorFilterRule *	-	-
vpc:trafficMirrorFilterRules:update	授予更新流量镜像筛选条件规则权限。	Write	trafficMirrorFilterRule *	vpc:TrafficMirrorFilterId	-
vpc:trafficMirrorFilterRules:delete	授予删除流量镜像筛选条件规则权限。	Write	trafficMirrorFilterRule *	vpc:TrafficMirrorFilterId	-
vpc:trafficMirrorSessions:create	授予创建流量镜像会话权限。	Write	trafficMirrorSession *	• vpc:TrafficMirrorTargetType • vpc:TrafficMirrorTargetId • vpc:TrafficMirrorSourceType	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• vpc:TrafficMirrorSourceId • vpc:TrafficMirrorFilterId	
			trafficMirrorFilter *	-	
vpc:trafficMirrorSessions:get	授予查询流量镜像会话详情权限。	Read	trafficMirrorSession *	• vpc:TrafficMirrorTargetType • vpc:TrafficMirrorTargetId • vpc:TrafficMirrorSourceType • vpc:TrafficMirrorFilterId • vpc:TrafficMirrorSourceId	-
vpc:trafficMirrorSessions:list	授予查询流量镜像会话列表权限。	List	trafficMirrorSession *	-	-
vpc:trafficMirrorSessions:update	授予更新流量镜像会话权限。	Write	trafficMirrorSession *	• vpc:TrafficMirrorTargetType • vpc:TrafficMirrorTargetId • vpc:TrafficMirrorSourceType • vpc:TrafficMirrorFilterId • vpc:TrafficMirrorSourc	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				eId	
			trafficMirrorFilter	-	
vpc:trafficMirrorSessions:addSource	授予添加流量镜像会话源资源权限。	Write	trafficMirrorSession *	• vpc:TrafficMirrorTargetType • vpc:TrafficMirrorTargetId • vpc:TrafficMirrorSourceType • vpc:TrafficMirrorFilterId • vpc:TrafficMirrorSourceId	-
vpc:trafficMirrorSessions:removeSource	授予移除流量镜像会话源资源权限。	Write	trafficMirrorSession *	• vpc:TrafficMirrorTargetType • vpc:TrafficMirrorTargetId • vpc:TrafficMirrorSourceType • vpc:TrafficMirrorFilterId • vpc:TrafficMirrorSourceId	-
vpc:trafficMirrorSessions:delete	授予删除流量镜像会话权限。	Write	trafficMirrorSession *	• vpc:TrafficMirrorTargetType • vpc:TrafficMirrorTargetId • vpc:TrafficMirrorSourc	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				eType • vpc:TrafficMirrorFilterId • vpc:TrafficMirrorSourceId	

vpc 的 API 通常对应着一个或多个授权项。表 3-47 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-47 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/vpcs	vpc:vpcs:create	-
GET /v1/{project_id}/vpcs/{vpc_id}	vpc:vpcs:get	-
GET /v1/{project_id}/vpcs	vpc:vpcs:list	-
PUT /v1/{project_id}/vpcs/{vpc_id}	vpc:vpcs:update	-
DELETE /v1/{project_id}/vpcs/{vpc_id}	vpc:vpcs:delete	-
POST /v1/{project_id}/subnets	vpc:subnets:create	-
GET /v1/{project_id}/subnets/{subnet_id}	vpc:subnets:get	-
GET /v1/{project_id}/subnets	vpc:subnets:list	-
PUT /v1/{project_id}/vpcs/{vpc_id}/subnets/{sub	vpc:subnets:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
net_id}		
DELETE /v1/{project_id}/vpcs/{vpc_id}/subnets/{subnet_id}	vpc:subnets:delete	-
GET /v1/{project_id}/quotas	vpc:quotas:list	-
POST /v1/{project_id}/privateips	vpc:privateIps:create	-
GET /v1/{project_id}/privateips/{privateip_id}	vpc:privateIps:get	-
GET /v1/{project_id}/subnets/{subnet_id}/privateips	vpc:privateIps:list	-
DELETE /v1/{project_id}/privateips/{privateip_id}	vpc:privateIps:delete	-
POST /v1/{project_id}/security-groups	vpc:securityGroups:create	-
GET /v1/{project_id}/security-groups/{security_group_id}	vpc:securityGroups:get	-
GET /v1/{project_id}/security-groups	vpc:securityGroups:list	-
DELETE /v1/{project_id}/security-groups/{security_group_id}	vpc:securityGroups:delete	-
POST /v1/{project_id}/security-group-rules	vpc:securityGroupRules:create	-
POST /v3/{project_id}/vpc/security-groups/{security_grou	vpc:securityGroupRules:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
p_id}/security-group-rules/batch-create		
GET /v1/{project_id}/security-group-rules/{security_group_rule_id}	vpc:securityGroupRules:get	-
GET /v1/{project_id}/security-group-rules	vpc:securityGroupRules:list	-
DELETE /v1/{project_id}/security-group-rules/{security_group_rule_id}	vpc:securityGroupRules:delete	-
POST /v1/{project_id}/ports	vpc:ports:create	-
GET /v1/{project_id}/ports/{port_id}	vpc:ports:get	-
GET /v1/{project_id}/ports	vpc:ports:list	-
PUT /v1/{project_id}/ports/{port_id}	vpc:ports:update	-
DELETE /v1/{project_id}/ports/{port_id}	vpc:ports:delete	-
POST /v2.0/vpc/peerings	vpc:peerings:create	-
PUT /v2.0/vpc/peerings/{pering_id}/accept	vpc:peerings:accept	-
PUT /v2.0/vpc/peerings/{pering_id}/reject	vpc:peerings:reject	-
GET /v2.0/vpc/peerings/{pering_id}	vpc:peerings:get	-
GET /v2.0/vpc/peerings	vpc:peerings:list	-
PUT /v2.0/vpc/peerings/{pe	vpc:peerings:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ering_id}		
DELETE /v2.0/vpc/peerings/{peering_id}	vpc:peerings:delete	-
POST /v1/{project_id}/routetables	vpc:routeTables:create	-
GET /v1/{project_id}/routetables/{routetable_id}	vpc:routeTables:get	-
GET /v1/{project_id}/routetables	vpc:routeTables:list	-
PUT /v1/{project_id}/routetables/{routetable_id}	vpc:routeTables:update	-
POST /v1/{project_id}/routetables/{routetable_id}/action	vpc:routeTables:associate	-
POST 01 /v1/{project_id}/routetables/{routetable_id}/action	vpc:routeTables:associate	-
DELETE /v1/{project_id}/routetables/{routetable_id}	vpc:routeTables:delete	-
POST /v1/{project_id}/fl/flow_logs	vpc:flowLogs:create	-
GET /v1/{project_id}/fl/flow_logs/{flowlog_id}	vpc:flowLogs:get	-
GET /v1/{project_id}/fl/flow_logs	vpc:flowLogs:list	-
PUT /v1/{project_id}/fl/flow_logs/{flowlog_id}	vpc:flowLogs:update	-
DELETE /v1/{project_id}/fl/flow_logs/{flowlog_id}	vpc:flowLogs:delete	-
PUT	vpc:vpcs:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v3/{project_id}/vpc/vpcs/{vpc_id}/add-extend-cidr		
PUT /v3/{project_id}/vpc/vpcs/{vpc_id}/remove-extend-cidr	vpc:vpcs:update	-
PUT /v3/{project_id}/vpc/security-groups/{security_group_id}	vpc:securityGroups:update	-
POST /v3/{project_id}/vpc/address-groups	vpc:addressGroups:create	-
GET /v3/{project_id}/vpc/address-groups/{address_group_id}	vpc:addressGroups:get	-
GET /v3/{project_id}/vpc/address-groups	vpc:addressGroups:list	-
PUT /v3/{project_id}/vpc/address-groups/{address_group_id}	vpc:addressGroups:update	-
DELETE /v3/{project_id}/vpc/address-groups/{address_group_id}	vpc:addressGroups:delete	-
DELETE /v3/{project_id}/vpc/address-groups/{address_group_id}/force	vpc:addressGroups:delete	-
POST /v3/{project_id}/vpc/firewalls	vpc:firewalls:create	-
PUT /v3/{project_id}/vpc/firewalls/{firewall_id}	vpc:firewalls:update	-
PUT	vpc:firewalls:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v3/{project_id}/vpc/firewalls/{firewall_id}/associate-subnets		
PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/disassociate-subnets	vpc:firewalls:update	-
PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/insert-rules	vpc:firewalls:update	-
PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/remove-rules	vpc:firewalls:update	-
PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/update-rules	vpc:firewalls:update	-
DELETE /v3/{project_id}/vpc/firewalls/{firewall_id}	vpc:firewalls:delete	-
GET /v3/{project_id}/vpc/firewalls	vpc:firewalls:list	-
GET /v3/{project_id}/vpc/firewalls/{firewall_id}	vpc:firewalls:get	-
POST /v2.0/{project_id}/vpcs/{vpc_id}/tags/action	vpc:vpcs:createTags	-
POST 01 /v2.0/{project_id}/vpcs/{vpc_id}/tags/action	vpc:vpcs:deleteTags	-
POST /v2.0/{project_id}/vpcs/{vpc_id}/tags	vpc:vpcs:createTags	-
POST /v2.0/{project_id}/vpcs/resource_instances/action	vpc:vpcs:listTags	-
GET /v2.0/{project_id}/vpcs/tags	vpc:vpcs:listTags	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v2.0/{project_id}/vpcs/{vpc_id}/tags	vpc:vpcs:listTags	-
DELETE /v2.0/{project_id}/vpcs/{vpc_id}/tags/{key}	vpc:vpcs:deleteTags	-
POST 01 /v2.0/{project_id}/subnets/{subnet_id}/tags/action	vpc:subnets:createTags	-
POST /v2.0/{project_id}/subnets/{subnet_id}/tags/action	vpc:subnets:deleteTags	-
POST /v2.0/{project_id}/subnets/{subnet_id}/tags	vpc:subnets:createTags	-
POST /v2.0/{project_id}/subnets/resource_instances/action	vpc:subnets:listTags	-
GET /v2.0/{project_id}/subnets/tags	vpc:subnets:listTags	-
GET /v2.0/{project_id}/subnets/{subnet_id}/tags	vpc:subnets:listTags	-
DELETE /v2.0/{project_id}/subnets/{subnet_id}/tags/{key}	vpc:subnets:deleteTags	-
POST /v3/{project_id}/vpc/sub-network-interfaces	vpc:subNetworkInterfaces:create	-
POST /v3/{project_id}/vpc/sub-network-interfaces/batch-create	vpc:subNetworkInterfaces:create	-
GET /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}	vpc:subNetworkInterfaces:get	-
GET	vpc:subNetworkInterfaces:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v3/{project_id}/vpc/sub-network-interfaces		
GET /v3/{project_id}/vpc/sub-network-interfaces/count	vpc:subNetworkInterfaces:list	-
PUT /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}	vpc:subNetworkInterfaces:update	-
DELETE /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}	vpc:subNetworkInterfaces:delete	-
POST /v3/{project_id}/firewalls/{firewall_id}/tags/create	vpc:firewalls:createTags	-
POST /v3/{project_id}/firewalls/{firewall_id}/tags/delete	vpc:firewalls:deleteTags	-
POST /v3/{project_id}/firewalls/{firewall_id}/tags	vpc:firewalls:createTags	-
POST /v3/{project_id}/firewalls/resource-instances/filter	vpc:firewalls:listTags	-
POST /v3/{project_id}/firewalls/resource-instances/count	vpc:firewalls:listTags	-
GET /v3/{project_id}/firewalls/tags	vpc:firewalls:listTags	-
GET /v3/{project_id}/firewalls/{firewall_id}/tags	vpc:firewalls:listTags	-
DELETE /v3/{project_id}/firewalls/{firewall_id}/tags/{tag_key}	vpc:firewalls:deleteTags	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST 01 /v2.0/{project_id}/security-groups/{security_group_id}/tags/action	vpc:securityGroups:createTags	-
POST /v2.0/{project_id}/security-groups/{security_group_id}/tags/action	vpc:securityGroups:deleteTags	-
POST /v2.0/{project_id}/security-groups/{security_group_id}/tags	vpc:securityGroups:createTags	-
POST /v2.0/{project_id}/security-groups/resource_instances/action	vpc:securityGroups:listTags	-
GET /v2.0/{project_id}/security-groups/tags	vpc:securityGroups:listTags	-
GET /v2.0/{project_id}/security-groups/{security_group_id}/tags	vpc:securityGroups:listTags	-
DELETE /v2.0/{project_id}/security-groups/{security_group_id}/tags/{key}	vpc:securityGroups:deleteTags	-
POST /v3/{project_id}/vpc/traffic-mirror-filters	vpc:trafficMirrorFilters:create	-
PUT /v3/{project_id}/vpc/traffic-mirror-filter/{traffic_mirror_filter_id}	vpc:trafficMirrorFilters:update	-
GET /v3/{project_id}/vpc/traffic-mirror-filter/{traffic_mirror_filter_id}	vpc:trafficMirrorFilters:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/vpc/traffic-mirror-filters	vpc:trafficMirrorFilters:list	-
DELETE /v3/{project_id}/vpc/traffic-mirror-filter/{traffic_mirror_filter_id}	vpc:trafficMirrorFilters:delete	-
POST /v3/{project_id}/vpc/traffic-mirror-filter-rules	vpc:trafficMirrorFilterRules:create	-
PUT /v3/{project_id}/vpc/traffic-mirror-filter-rules/{traffic_mirror_filter_rule_id}	vpc:trafficMirrorFilterRules:update	-
GET /v3/{project_id}/vpc/traffic-mirror-filter-rules/{traffic_mirror_filter_rule_id}	vpc:trafficMirrorFilterRules:get	-
GET /v3/{project_id}/vpc/traffc-mirror-filter-rules	vpc:trafficMirrorFilterRules:list	-
DELETE /v3/{project_id}/vpc/traffic-mirror-filter-rules/{traffic_mirror_filter_rule_id}	vpc:trafficMirrorFilterRules:delete	-
POST /v3/{project_id}/vpc/traffic-mirror-sessions	vpc:trafficMirrorSessions:create	-
PUT /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}/add-sources	vpc:trafficMirrorSessions:addSource	-
PUT /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}/remove-sources	vpc:trafficMirrorSessions:removeSource	-
PUT /v3/{project_id}/vpc/tr	vpc:trafficMirrorSessions:upda	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
affic-mirror-sessions/{traffic_mirror_session_id}	te	
GET /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}	vpc:trafficMirrorSessions:get	-
GET /v3/{project_id}/vpc/traffic-mirror-sessions	vpc:trafficMirrorSessions:list	-
DELETE /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}	vpc:trafficMirrorSessions:delete	-
PUT /v3/{project_id}/ports/{port_id}/insert-security-groups	vpc:ports:update	-
PUT /v3/{project_id}/ports/{port_id}/remove-security-groups	vpc:ports:update	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-48 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

vpc 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-48 vpc 支持的资源类型

资源类型	URN
network	vpc:<region>:<account-id>:network:<network-id>
securityGroupRule	vpc:<region>:<account-id>:securityGroupRule:<security-group-rule-id>
addressGroup	vpc:<region>:<account-id>:addressGroup:<address-group-id>
firewall	vpc:<region>:<account-id>:firewall:<firewall-id>
port	vpc:<region>:<account-id>:port:<port-id>

 版权所有 © 华为云计算技术有限公司

资源类型	URN
trafficMirrorFilter	vpc:<region>:<account-id>:trafficMirrorFilter:<traffic-mirror-filter-id>
securityGroup	vpc:<region>:<account-id>:securityGroup:<security-group-id>
routeTable	vpc:<region>:<account-id>:routeTable:<route-table-id>
vpc	vpc:<region>:<account-id>:vpc:<vpc-id>
publicip	vpc:<region>:<account-id>:publicip:<publicip-id>
flowLog	vpc:<region>:<account-id>:flowLog:<flow-log-id>
trafficMirrorFilterRule	vpc:<region>:<account-id>:trafficMirrorFilterRule:<traffic-mirror-filter-rule-id>
bandwidth	vpc:<region>:<account-id>:bandwidth:<bandwidth-id>
trafficMirrorSession	vpc:<region>:<account-id>:trafficMirrorSession:<traffic-mirror-session-id>
subNetworkInterface	vpc:<region>:<account-id>:subNetworkInterface:<sub-network-interface-id>
subnet	vpc:<region>:<account-id>:subnet:<subnet-id>
privateIp	vpc:<region>:<account-id>:privateIp:<private-ip-id>
peering	vpc:<region>:<account-id>:peering:<peering-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 vpc:）仅适用于对应服务的操作，详情请参见表 3-49。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

 版权所有 © 华为云计算技术有限公司

vpc 支持的服务级条件键

vpc 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-49 vpc 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
vpc:VpcId	string	多值	根据指定的虚拟私有云资源 ID 过滤访问。
vpc:VpcBlockServiceEndpointStates	string	单值	根据指定的虚拟私有云资源阻止服务终结点状态过滤访问，有效的条件值应为"on"、"off"。
vpc:SubnetId	string	多值	根据指定的子网资源 ID 过滤访问。
vpc:SecurityGroupId	string	多值	根据指定的安全组资源 ID 过滤访问。
vpc:PeeringId	string	多值	根据指定的对等连接资源 ID 过滤访问。
vpc:AccepterVpcId	string	多值	根据指定的接收方 VPC 资源 ID 过滤访问。
vpc:AccepterVpcOrgPath	string	多值	根据指定的对等连接接收方 VPC 资源所有者的 OrgPath 过滤访问。
vpc:AccepterVpcOwner	string	多值	根据指定的对等连接接收方 VPC 资源所有者的账号 ID 过滤访问。
vpc:RequesterVpcOrgPath	string	多值	根据指定的对等连接请求方 VPC 资源所有者的 OrgPath 过滤访问。
vpc:RequesterVpcOwner	string	多值	根据指定的对等连接请求方 VPC 资源所有者的账号 ID 过滤访问。
vpc:RequesterVpcId	string	多值	根据指定的请求方 VPC 资源 ID 过滤访问。
vpc:RouteTableId	string	多值	根据指定的路由表资源 ID 过滤访问。
vpc:FlowLogId	string	多值	根据指定的流日志资源 ID 过滤访问。

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
vpc:AddressGroupId	string	多值	根据指定的 IP 地址组资源 ID 过滤访问。
vpc:FirewallId	string	多值	根据指定的网络 ACL 资源 ID 过滤访问。
vpc:PrivateIpId	string	多值	根据指定的私有 IP 资源 ID 过滤访问。
vpc:PortId	string	多值	根据指定的端口资源 ID 过滤访问。
vpc:SubNetworkInterfaceId	string	多值	根据指定的辅助弹性网卡资源 ID 过滤访问。
vpc:FirewallRuleDirection	string	多值	根据指定的网络 ACL 规则方向过滤访问，有效的条件值应为 ingress、egress。
vpc:FirewallRuleProtocol	string	多值	根据指定的网络 ACL 规则协议过滤访问，有效的条件值应为 tcp、udp、icmp、icmpv6、any。
vpc:FirewallRuleAction	string	多值	根据指定的网络 ACL 规则策略过滤访问，有效的条件值应为 allow、deny。
vpc:FirewallRuleSourcePort	numeric	多值	根据指定的网络 ACL 规则源端口过滤访问。
vpc:FirewallRuleDestinationPort	numeric	多值	根据指定的网络 ACL 规则目的端口过滤访问。
vpc:FirewallOperationType	string	多值	根据指定的网络 ACL 操作类型过滤访问，有效的条件值应为 updateAcl、associateSubnet、disassociateSubnet、insertRule、updateRule、removeRule。
vpc:TrafficMirrorFilterId	string	多值	根据指定的流量镜像筛选条件 ID 过滤访问。

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
vpc:TrafficMirrorTargetType	string	多值	根据指定的流量镜像会话目的资源类型过滤访问，有效的条件值应为eni、elb。
vpc:TrafficMirrorTargetId	string	多值	根据指定的流量镜像会话目的资源 ID 过滤访问。
vpc:TrafficMirrorSourceType	string	多值	根据指定的流量镜像会话源资源类型过滤访问，有效的条件值应为eni。
vpc:TrafficMirrorSourceId	string	多值	根据指定的流量镜像会话源资源 ID 过滤访问。
vpc:FirewallRuleSourceIp	ip_address	单值	根据指定的网络 ACL 规则中源地址过滤访问。
vpc:FirewallRuleSourceIpAddressGroup	string	单值	根据指定的网络 ACL 规则中源地址使用的 Ip 地址组唯一标识 Id 过滤访问。
vpc:FirewallRuleDestinationIp	ip_address	单值	根据指定的网络 ACL 规则中目的地址过滤访问。
vpc:FirewallRuleDestinationIpAddressGroup	string	单值	根据指定的网络 ACL 规则中目的地址使用的 Ip 地址组唯一标识 Id 过滤访问。
vpc:AvailabilityZone	string	单值	根据指定的可用区唯一标识 Id 过滤访问。
vpc:LegacyAPIFlavor	string	单值	根据指定的原生 API 接口过滤访问。
vpc:SecurityGroupRuleDirection	string	单值	根据指定的安全组规则方向过滤访问，有效的条件值应为 ingress、egress。
vpc:SecurityGroupRuleProtocol	string	单值	根据指定的安全组规则协议过滤访问，有效的条件值应为 tcp、udp、icmp、icmpv6、gre、

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
			any。
vpc:SecurityGroupRuleAction	string	单值	根据指定的安全组规则生效策略过滤访问，有效的条件值应为allow、deny。
vpc:SecurityGroupRulePort	numeric	多值	根据指定的安全组规则端口过滤访问。
vpc:SecurityGroupRuleRemoteIpAddressGroup	string	单值	根据指定的安全组规则中远端地址组使用的 Ip 地址组唯一标识 Id 过滤访问。
vpc:SecurityGroupRuleRemoteSecurityGroup	string	单值	根据指定的安全组规则中远端安全组使用的安全组唯一标识 Id 过滤访问。
vpc:SecurityGroupRuleRemoteIpPrefix	ip_address	单值	根据指定的安全组规则中远端 IP 使用的 Ip 地址过滤访问。
vpc:VirsubnetCidrReservationId	string	多值	根据指定的子网预留网段资源 ID 过滤访问。
vpc:SubnetIpv6Enable	boolean	单值	根据指定的子网 ipv6 启用状态过滤访问。

3.3.3 弹性公网 IP EIP

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

 版权所有 © 华为云计算技术有限公司

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 EIP 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 EIP 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 EIP 的相关操作。

表3-50 EIP 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
eip:publicIps:createTags	授予创建弹性 IP 资源标签权限。	Tagging	public ip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:publicipTags:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
eip:publicIps:listTags	授予查询弹性 IP 资源标签权限。	List	public ip *	-	vpc:publicipTags:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
eip:publicIps:deleteTags	授予删除弹性公网 IP 资源标签权限。	Tagging	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:publicipTags:delete
			-	g:TagKeys	
eip:publicIps:count	授予查询弹性公网 IP 数量的权限。	List	publicip *	-	vpc:publicIps:list
eip:bandwidths:create	授予创建共享带宽的权限。	Write	bandwidth *	-	vpc:bandwidths:create
			-	g:EnterpriseProjectId	
eip:bandwidths:batchCreate	授予批量创建共享带宽的权限。	Write	bandwidth *	-	-
eip:bandwidths:list	授予查询带宽列表的权限。	List	bandwidth *	-	vpc:bandwidths:list
			-	g:EnterpriseProjectId	
eip:bandwidths:update	授予更新带宽的权限。	Write	bandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:bandwidths:update
eip:bandwidths:get	授予查询带宽的权限。	Read	bandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	vpc:bandwidths:get
eip:bandwidths:delete	授予删除共享带宽的权限。	Write	bandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	vpc:bandwidths:delete
eip:bandwidthPkgs:list	授予查询带宽加油包列表的权限。	List	bandwidthPkg *	-	vpc:bandwidths:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
eip:bandwidthPkgs:update	授予更新带宽加油包的权限。	Write	bandwidthPkg *	-	vpc:bandwidths:update
eip:publicIps:create	授予申请弹性公网 IP 的权限。	Write	publicip *	-	vpc:publicIps:create
			-	g:EnterpriseProjectId	
eip:publicIps:batchCreate	授予批量创建弹性公网 IP 的权限。	Write	publicip *	-	vpc:publicIps:create
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
eip:publicIps:list	授予查询弹性公网 IP 列表的权限。	List	publicip *	-	vpc:publicIps:list
			-	g:EnterpriseProjectId	
eip:publicIps:get	授予查询指定弹性公网 IP 的权限。	Read	publicip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	vpc:publicIps:get
eip:publicIps:update	授予更新弹性公网 IP 的权限。	Write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:publicIps:update
eip:publicIps:disassociateInstance	授予将弹性公网 IP 解绑网卡的权限。	Write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:publicIps:update
eip:publicIps:delete	授予删除弹性公网 IP 的权限。	Write	publicip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	vpc:publicIps:delete

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
eip:publicIps:create	授予申请弹性公网 IP 的权限。	Write	publicip *	-	vpc:publicIps:create
			-	g:EnterpriseProjectId	
eip:publicIps:batchCreate	授予批量创建弹性公网 IP 的权限。	Write	publicip *	-	vpc:publicIps:create
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
eip:publicIps:list	授予查询弹性公网 IP 列表的权限。	List	publicip *	-	vpc:publicIps:list
			-	g:EnterpriseProjectId	
eip:publicIps:count	授予查询弹性公网 IP 数量的权限。	List	publicip *	-	vpc:publicIps:list
eip:publicIps:get	授予查询指定弹性公网 IP 的权限。	Read	publicip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	vpc:publicIps:get
eip:publicIps:update	授予更新弹性公网 IP 的权限。	Write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:publicIps:update
eip:publicIps:enableNat64	授予使能弹性公网 IP NAT64 的权限。	Write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:publicIps:update
eip:publicIps:disableNat64	授予使能弹性公网 IP NAT64 的权限。	Write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:publicIps:update

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
eip:publicIps:associateInstance	授予将弹性公网 IP 绑定网卡的权限。	Write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:publicIps:update
eip:publicIps:disassociateInstance	授予将弹性公网 IP 解绑网卡的权限。	Write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:publicIps:update
eip:publicIps:attachBandwidth	授予将弹性公网 IP 绑定带宽的权限。	Write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:publicIps:update
			bandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
eip:publicIps:detachBandwidth	授予将弹性公网 IP 从共享带宽中解绑的权限。	Write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:publicIps:update
			bandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
eip:publicIps:delete	授予删除弹性公网 IP 的权限。	Write	publicip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	vpc:publicIps:delete
eip:publicIps:createTags	授予创建弹性 IP 资源标签权限。	Tagging	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:publicipTags:create

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	• g:RequestTag/<tag-key> • g:TagKeys	
eip:publicIps:listTags	授予查询弹性IP资源标签权限。	List	publicip *	-	vpc:publicipTags:get
eip:publicIps:deleteTags	授予删除弹性公网IP资源标签权限。	Tagging	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:publicipTags:delete
			-	g:TagKeys	
eip:bandwidths:insertPublicIps	授予共享带宽插入弹性公网IP的权限。	Write	bandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	vpc:publicIps:insert
eip:bandwidths:removePublicIps	授予共享带宽移除弹性公网IP的权限。	Write	bandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	vpc:publicIps:insert
eip:bandwidths:create	授予创建共享带宽的权限。	Write	bandwidth *	-	vpc:bandwidths:create
			-	g:EnterpriseProjectId	
eip:bandwidths:batchCreate	授予批量创建共享带宽的权限。	Write	bandwidth *	-	-
eip:bandwidths:list	授予查询带宽列表的权限。	List	bandwidth *	-	vpc:bandwidths:list
			-	g:EnterpriseProjectId	
eip:bandwidths:update	授予更新带宽的权限。	Write	bandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:bandwidths:update

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
eip:bandwidths:get	授予查询带宽的权限。	Read	bandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	vpc:bandwidths:get
eip:bandwidths:delete	授予删除共享带宽的权限。	Write	bandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	vpc:bandwidths:delete
eip:bandwidthRules:list	授予查询带宽规则列表的权限。	List	bandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:bandwidths:get
			bandwidthRule *	-	
eip:bandwidthRules:get	授予查询带宽规则的权限。	Read	bandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:bandwidths:get
			bandwidthRule *	-	
eip:bandwidthRules:update	授予更新带宽规则的权限。	Write	bandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:bandwidths:update
			bandwidthRule *	-	
eip:bandwidthRules:delete	授予删除带宽规则的权限。	Write	bandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:bandwidths:delete

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			bandwidthRule *	-	
eip:bandwidthRules:create	授予创建共享带宽规则的权限。	Write	bandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	vpc:bandwidths:update
			bandwidthRule *	-	
eip:bandwidthPkgs:list	授予查询带宽加油包列表的权限。	List	bandwidthPkg *	-	vpc:bandwidths:get
eip:bandwidthPkgs:get	授予查询带宽加油包的权限。	Read	bandwidthPkg *	-	vpc:bandwidths:get
eip:bandwidthPkgs:update	授予更新带宽加油包的权限。	Write	bandwidthPkg *	-	vpc:bandwidths:update
eip:bandwidthPkgs:create	授予创建带宽加油包的权限。	Write	bandwidthPkg *	-	vpc:bandwidths:update
eip:publicipPools:create	授予创建公网IP池的权限。	Write	publicipPool *	-	vpc:publicIps:create
eip:publicipPools:get	授予查询公网IP池的权限。	Read	publicipPool *	-	vpc:publicIps:get
eip:publicipPools:update	授予更新公网IP池的权限。	Write	publicipPool *	-	vpc:publicIps:update
eip:vpcIgws:list	授予查询互联网网关列表的权限。	List	vpcIgw *	-	vpc:vpcs:list
eip:vpcIgws:get	授予查询互联网网关的权	Read	vpcIgw *	-	vpc:vpcs:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
eip:vpcIgws:update	授予更新互联网网关的权限。	Write	vpcIgw *	-	vpc:vpcs:update
eip:vpcIgws:delete	授予删除互联网网关的权限。	Write	vpcIgw *	-	vpc:vpcs:delete
eip:vpcIgws:create	授予创建互联网网关的权限。	Write	vpcIgw *	-	vpc:vpcs:create
eip:globalEips:list	授予查询全域弹性公网 IP 列表的权限。	List	globalEip *	-	-
			-	g:EnterpriseProjectId	
eip:globalEips:count	授予查询全域弹性公网 IP 数量的权限。	List	globalEip *	-	eip:globalEips:list
eip:globalEips:get	授予查询指定全域弹性公网 IP 的权限。	Read	globalEip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
eip:globalEips:create	授予申请全域弹性公网 IP 的权限。	Write	globalEip *	-	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
eip:globalEips:updateGeip	授予更新全域弹性公网 IP 的权限。	Write	globalEip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	eip:globalEips:update
eip:globalEips:disassociateInstance	授予从全域弹性公网 IP 解绑实例的权限。	Write	globalEip *	• g:EnterpriseProjectId • g:ResourceT	eip:globalEips:update

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ag/<tag-key>	
eip:globalEips:associateInstance	授予给全域弹性公网 IP 绑定实例的权限。	Write	global Eip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	eip:globalEips:update
eip:globalEips:delete	授予删除全域弹性公网 IP 的权限。	Write	global Eip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
eip:globalEips:attachBandwidth	授予将弹性公网 IP 绑定公网带宽的权限。	Write	global Eip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	eip:globalEips:insert
			internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
eip:globalEips:detachBandwidth	授予将弹性公网 IP 从公网带宽中移除的权限。	Write	global Eip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	eip:globalEips:remove
			internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
eip:globalEips:createTags	授予创建全域弹性 IP 资源标签权限。	Tagging	global Eip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
eip:globalEips:getTags	授予查询全域弹性 IP 资源标签权限。	Read	global Eip *	-	-
eip:globalEips:listTags	授予查询项目里所有全域弹性 IP 资源标签权限。	List	global Eip *	-	-
eip:globalEips:deleteTags	授予删除全域弹性公网 IP 资源标签权限。	Tagging	global Eip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	g:TagKeys	
eip:internetBandwidths:createTags	授予创建全域公网带宽资源标签权限。	Tagging	internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
eip:internetBandwidths:getTags	授予查询全域公网带宽资源标签权限。	Read	internetBandwidth *	-	-
eip:internetBandwidths:listTags	授予查询项目里所有全域公网带宽资源标签权限。	List	internetBandwidth *	-	-
eip:internetBandwidths:deleteTags	授予删除全域公网带宽资源标签权限。	Tagging	internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	g:TagKeys	
eip:internetBandwidths:list	授予查询全域公网带宽列表	List	internetBandwidt	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	的权限。		h *		
			-	g:EnterpriseProjectId	
eip:internetBandwidths:count	授予查询全域公共带宽数量的权限。	List	internetBandwidth *	-	eip:internetBandwidths:list
eip:internetBandwidths:get	授予查询指定全域公网带宽的权限。	Read	internetBandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
eip:internetBandwidths:create	授予申请全域公网带宽的权限。	Write	internetBandwidth *	-	-
			-	g:EnterpriseProjectId	
eip:internetBandwidths:update	授予更新全域公网带宽的权限。	Write	internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
eip:internetBandwidths:delete	授予删除全域公网带宽的权限。	Write	internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
eip:geipSegments:list	授予查询全域弹性公网 IP 段列表的权限。	List	geipSegment *	-	-
			-	g:EnterpriseProjectId	
eip:geipSegments:count	授予查询全域弹性公网 IP 段数量的权限。	List	geipSegment *	-	-
eip:geipSegments:get	授予查询指定全域弹性公网 IP 段的权限。	Read	geipSegment *	• g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:EnterpriseProjectId	
eip:geipSegments:create	授予申请全域弹性公网 IP 段的权限。	Write	geipSegment *	-	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
eip:geipSegments:update	授予更新全域弹性公网 IP 段的权限。	Write	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
eip:geipSegments:disassociateInstance	授予从全域弹性公网 IP 段解绑实例的权限。	Write	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
eip:geipSegments:associateInstance	授予给全域弹性公网 IP 段绑定实例的权限。	Write	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
eip:geipSegments:delete	授予删除全域弹性公网 IP 段的权限。	Write	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
eip:geipSegments:attachBandwidth	授予将弹性公网 IP 段绑定公网带宽的权限。	Write	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
eip:geipSegments:detachBandwidth	授予将弹性公网 IP 段从公网带宽中移除的权限。	Write	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
eip:geipSegments:createTags	授予创建全域弹性 IP 段资源标签权限。	Tagging	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
eip:geipSegments:getTags	授予查询全域弹性 IP 段资源标签权限。	Read	geipSegment *	-	-
eip:geipSegments:listTags	授予查询项目里所有全域弹性 IP 段资源标签权限。	List	geipSegment *	-	-
eip:geipSegments:deleteTags	授予删除全域弹性公网 IP 段资源标签权限。	Tagging	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	g:TagKeys	
eip:userDisclaimer:sign	授予签署免责条款的权限。	Write	-	-	-
eip:userDisclaimer:cancel	授予撤销免责条款的权限。	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

EIP 的 API 通常对应着一个或多个授权项。表 3-51 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-51 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/elasticips	eip:publicIps:count	-
GET /v2/{project_id}/publicip/instances	eip:publicIps:count	-
POST /v2.0/{project_id}/publicips/{publicip_id}/tags/action	eip:publicIps:createTags	-
POST 01 /v2.0/{project_id}/publicips/{publicip_id}/tags/action	eip:publicIps:deleteTags	-
POST /v2.0/{project_id}/publicips/{publicip_id}/tags	eip:publicIps:createTags	-
DELETE /v2.0/{project_id}/publicips/{publicip_id}/tags/{key}	eip:publicIps:deleteTags	-
POST /v2.0/{project_id}/publicips/resource_instances/action	eip:publicIps:listTags	-
GET /v2.0/{project_id}/publicips/tags	eip:publicIps:listTags	-
GET /v2.0/{project_id}/publicips/{publicip_id}/tags	eip:publicIps:listTags	-
POST /v2.0/{project_id}/bandwidths	eip:bandwidths:create	-
POST /v2.0/{project_id}/batch-bandwidths	eip:bandwidths:batchCreate	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/bandwidths	eip:bandwidths:list	-
DELETE /v2.0/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:delete	-
GET /v1/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:get	-
PUT /v1/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:update	-
PUT /v2.0/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:update	-
POST /v2.0/{project_id}/bandwidths/change-to-period	eip:bandwidths:update	bss:renewal:update
GET /v2/{project_id}/bandwidthpkgs	eip:bandwidthPkgs:list	-
PUT /v2/{project_id}/bandwidthpkgs/{id}	eip:bandwidthPkgs:update	-
PUT /v2/{project_id}/batch-bandwidths/modify	eip:bandwidths:update	-
POST /v2.0/{project_id}/bandwidths/{bandwidth_id}/insert	eip:bandwidths:insertPublicIps	-
POST /v2.0/{project_id}/bandwidths/{bandwidth_id}/remove	eip:bandwidths:removePublicIps	-
POST /v2.0/{project_id}/publicips	eip:publicIps:create	-
POST	eip:publicIps:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/publicips		
POST /v2/{project_id}/batch publicips	eip:publicIps:batchCreate	-
GET /v1/{project_id}/publicips	eip:publicIps:list	-
GET /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:get	-
PUT /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:update	-
POST /v2.0/{project_id}/publicips/change-to-period	eip:publicIps:update	bss:renewal:update
PATCH /v2/{project_id}/batch publicips	eip:publicIps:disassociateInstance	-
DELETE /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:delete	-
DELETE /v2/{project_id}/batch publicips	eip:publicIps:delete	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/associate-instance	eip:publicIps:associateInstance	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/disassociate-instance	eip:publicIps:disassociateInstance	-
POST /v3/{project_id}/eip/publicips/attach-share-bandwidth	eip:publicIps:attachBandwidth	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/attach-share-bandwidth	eip:publicIps:attachBandwidth	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/eip/publicips/detach-share-bandwidth	eip:publicIps:detachBandwidth	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/detach-share-bandwidth	eip:publicIps:detachBandwidth	-
POST /v3/{project_id}/eip/bandwidths	eip:bandwidths:create	-
GET /v3/{project_id}/eip/bandwidths/{bandwidth_id}/bandwidth-rules	eip:bandwidthRules:list	-
GET /v3/{project_id}/eip/bandwidths/{bandwidth_id}/bandwidth-rule/{bandwidth_rules_id}	eip:bandwidthRules:get	-
PUT /v3/{project_id}/eip/bandwidths/{bandwidth_id}/bandwidth-rule/{bandwidth_rules_id}	eip:bandwidthRules:update	-
POST /v3/{project_id}/eip/bandwidths/{bandwidth_id}/bandwidth-rules	eip:bandwidthRules:create	-
DELETE /v3/{project_id}/eip/bandwidths/{bandwidth_id}/bandwidth-rule/{bandwidth_rules_id}	eip:bandwidthRules:delete	-
GET /v3/{project_id}/eip/publicip-pools/{publicip_pool_id}	eip:publicipPools:get	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/	eip:publicIps:enableNat64	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
enable-nat64		
POST /v3/{project_id}/eip/publicips/{publicip_id}/disable-nat64	eip:publicIps:disableNat64	-
GET /v3/{project_id}/eip-bandwidths	eip:bandwidths:list	-
GET /v3/{project_id}/eip/bandwidths	eip:bandwidths:list	-
GET /v3/{project_id}/eip/publicips	eip:publicIps:list	-
GET /v3/{project_id}/eip/publicips/{publicip_id}	eip:publicIps:get	-
GET /v3/{project_id}/geip/vpc-igws	eip:vpcIgws:list	-
GET /v3/{project_id}/geip/vpc-igws/{vpc_igw_id}	eip:vpcIgws:get	-
PUT /v3/{project_id}/geip/vpc-igws/{vpc_igw_id}	eip:vpcIgws:update	-
DELETE /v3/{project_id}/geip/vpc-igws/{vpc_igw_id}	eip:vpcIgws:delete	-
POST /v3/{project_id}/geip/vpc-igws	eip:vpcIgws:create	-
GET /v3/{domain_id}/global-eips	eip:globalEips:list	-
GET /v3/{domain_id}/global-eips/count	eip:globalEips:count	-
GET /v3/{domain_id}/global-	eip:globalEips:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
eips/{global_eip_id}		
POST /v3/{domain_id}/global-eips	eip:globalEips:create	-
DELETE /v3/{domain_id}/global-eips/{global_eip_id}	eip:globalEips:delete	-
PUT /v3/{domain_id}/global-eips/{global_eip_id}	eip:globalEips:updateGeip	-
POST /v3/{domain_id}/global-eips/{global_eip_id}/associate-instance	eip:globalEips:associateInstance	-
POST /v3/{domain_id}/global-eips/{global_eip_id}/disassociate-instance	eip:globalEips:disassociateInstance	-
POST /v3/{domain_id}/global-eips/{global_eip_id}/attach-internet-bandwidth	eip:globalEips:attachBandwidth	-
POST /v3/{domain_id}/global-eips/{global_eip_id}/detach-internet-bandwidth	eip:globalEips:detachBandwidth	-
GET /v3/global-eip/{resource_id}/tags	eip:globalEips:getTags	-
GET /v3/global-eip/tags	eip:globalEips:listTags	-
POST /v3/global-eip/{resource_id}/tags	eip:globalEips:createTags	-
DELETE /v3/global-eip/{resource_id}/tags/{tag_key}	eip:globalEips:deleteTags	-
GET	eip:internetBandwidths:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v3/{domain_id}/geip/internet-bandwidths		
GET /v3/{domain_id}/geip/internet-bandwidths/count	eip:internetBandwidths:count	-
GET /v3/{domain_id}/geip/internet-bandwidths/{internet_bandwidth_id}	eip:internetBandwidths:get	-
PUT /v3/{domain_id}/geip/internet-bandwidths/{internet_bandwidth_id}	eip:internetBandwidths:update	-
DELETE /v3/{domain_id}/geip/internet-bandwidths/{internet_bandwidth_id}	eip:internetBandwidths:delete	-
POST /v3/{domain_id}/geip/internet-bandwidths	eip:internetBandwidths:create	-
GET /v3/internet-bandwidth/{resource_id}/tags	eip:internetBandwidths:getTags	-
GET /v3/internet-bandwidth/tags	eip:internetBandwidths:listTags	-
POST /v3/internet-bandwidth/{resource_id}/tags	eip:internetBandwidths:createTags	-
DELETE /v3/internet-bandwidth/{resource_id}/tags/{tag_key}	eip:internetBandwidths:deleteTags	-
GET /v3/{domain_id}/global-eip-segments	eip:geipSegments:list	-
GET /v3/{domain_id}/global-eip-segments/count	eip:geipSegments:count	-
GET /v3/{domain_id}/global-eip-	eip:geipSegments:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
segments/{global_eip_segment_id}		
POST /v3/{domain_id}/global-eip-segments	eip:geipSegments:create	-
DELETE /v3/{domain_id}/global-eip-segments/{global_eip_segment_id}	eip:geipSegments:delete	-
PUT /v3/{domain_id}/global-eip-segments/{global_eip_segment_id}	eip:geipSegments:update	-
POST /v3/{domain_id}/global-eip-segments/{global_eip_segment_id}/associate-instance	eip:geipSegments:associateInstance	-
POST /v3/{domain_id}/global-eip-segments/{global_eip_segment_id}/disassociate-instance	eip:geipSegments:disassociateInstance	-
POST /v3/{domain_id}/global-eip-segments/batch-attach-internet-bandwidths	eip:geipSegments:attachBandwidth	-
POST /v3/{domain_id}/global-eip-segments/batch-detach-internet-bandwidths	eip:geipSegments:detachBandwidth	-
GET /v3/global-eip-segment/{resource_id}/tags	eip:geipSegments:getTags	-
GET /v3/global-eip-segment/tags	eip:geipSegments:listTags	-
POST /v3/global-eip-segment/{resource_id}/tags	eip:geipSegments:createTags	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /v3/global-eip-segment/{resource_id}/tags/{tag_key}	eip:geipSegments:deleteTags	-
POST /v3/{domain_id}/geip/user-disclaimer-records	eip:userDisclaimer:sign	-
DELETE /v3/{domain_id}/geip/user-disclaimer-records	eip:userDisclaimer:cancel	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-52 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

EIP 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-52 EIP 支持的资源类型

资源类型	URN
bandwidthRule	eip:<region>:<account-id>:bandwidthRule:<bandwidthRule-id>
bandwidth	vpc:<region>:<account-id>:bandwidth:<bandwidth-id>
bandwidthPkg	eip:<region>:<account-id>:bandwidthPkg:<bandwidthPkg-id>
publicipPool	eip:<region>:<account-id>:publicipPool:<publicipPool-id>
geipSegment	eip:<region>:<account-id>:geipSegment:<geipSegment-id>
vpcIgw	eip:<region>:<account-id>:vpcIgw:<vpcIgw-id>
internetBandwidth	eip:<region>:<account-id>:internetBandwidth:<internetBandwidth-id>
publicip	vpc:<region>:<account-id>:publicip:<publicip-id>
globalEip	eip:<region>:<account-id>:globalEip:<globalEip-id>

 版权所有 © 华为云计算技术有限公司

条件（Condition）

EIP 服务不支持在身份策略中的条件键中配置服务级的条件键。EIP 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.3.4 云专线 DC

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 DC 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 DC 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

 版权所有 © 华为云计算技术有限公司

您可以在身份策略语句的 Action 元素中指定以下 DC 的相关操作。

表3-53 DC 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dcaas:directConnect:create	授予创建物理连接。	Write	directConnect *	-	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	
dcaas:directConnect:update	授予更新指定物理连接信息。	Write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:directConnect:delete	授予删除指定物理连接。只适用于按需计费物理连接，对于包周期购买的物理连接通过订单退订的方式删除指定物理连接。	Write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:directConnect:get	授予查询指定物理连接详细信息。	Read	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:directConnect:list	授予查询租户创建的所有物理连接。	List	directConnect *	-	-
			-	g:EnterpriseProjectId	
dcaas:directConnect:createHostedDirectConnect	授予合作伙伴创建托管物理连接。	Write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-	dcaas:directConnect:create

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				key>	
dcaas:directConnect:updateHostedDirectConnect	授予合作伙伴更新指定托管物理连接。	Write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	dcaas:directConnect:update
dcaas:directConnect:deleteHostedDirectConnect	授予合作伙伴删除指定托管物理连接。	Write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	dcaas:directConnect:delete
dcaas:directConnect:getHostedDirectConnect	授予合作伙伴查询指定托管物理连接。	Read	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	dcaas:directConnect:get
dcaas:directConnect:listHostedDirectConnect	授予合作伙伴查询所有托管物理连接列表。	List	directConnect *	g:EnterpriseProjectId	dcaas:directConnect:list
dcaas:directConnect:createOnestopDirectConnect	授予创建一站式物理连接。	Write	directConnect *	-	dcaas:directConnect:create
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	
dcaas:directConnect:updateOnestopDirectConnect	授予更新指定一站式物理连接。	Write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	dcaas:directConnect:update
dcaas:directConnect:createOrder	授予创建订单用来购买物理连接。	Write	directConnect *	-	dcaas:directConnect:create
dcaas:directConnect:updateOrder	授予更新指定订单，用于物理连接升配或	Write	directConnect *	-	dcaas:directConnect:update

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	降配。				
dcaas:vgw:create	授予创建虚拟网关。	Write	vgw *	-	-
			vpc	-	
			instances	-	
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
dcaas:vgw:update	授予更新指定虚拟网关的信息。	Write	vgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:vgw:delete	授予删除指定的虚拟网关。	Write	vgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:vgw:get	授予查询指定虚拟网关的详细信息。	Read	vgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:vgw:list	授予查询虚拟网关列表。	List	vgw *	-	-
			-	g:EnterpriseProjectId	
dcaas:vif:create	授予创建虚拟接口。	Write	vif *	-	-
			directConnect	-	
			lag	-	
			vgw	-	
			gdgw	-	
			conne	-	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			ctGateway		
			lgw	-	
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
dcaas:vif:update	授予更新指定虚拟接口。	Write	vif *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:vif:delete	授予删除指定虚拟接口。	Write	vif *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:vif:get	授予查询指定虚拟接口。	Read	vif *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:vif:list	授予查询指定租户所有虚拟接口列表。	List	vif *	-	-
			-	g:EnterpriseProjectId	
dcaas:vif:updateVifExtendAttribute	授予更新指定虚拟接口扩展属性。	Write	vif *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:vifPeer:create	授予创建虚拟接口对等体。	Write	vifPeer *	-	-
			vif *	-	
dcaas:vifPeer:update	授予更新指定虚拟接口对等体信息。	Write	vifPeer *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dcaas:vifPeer:delete	授予删除指定虚拟接口对等体。	Write	vifPeer *	-	-
dcaas:vifPeer:get	授予查询指定虚拟接口对等体。	Read	vifPeer *	-	-
dcaas:vifPeer:list	授予查询虚拟接口对等体列表。	List	vifPeer *	-	-
dcaas:lag:list	授予查询链路聚合组详细信息列表。	List	lag *	-	-
			-	g:EnterpriseProjectId	
dcaas:gdgw:create	授予创建全域接入网关实例。	Write	gdgw *	-	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
dcaas:gdgw:update	授予更新指定全域接入网关信息。	Write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:gdgw:delete	授予删除指定的全域接入网关。	Write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:gdgw:get	授予查询指定全域接入网关实例详情信息。	Read	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:gdgw:list	授予查询全域接入网关列表。	List	gdgw *	-	-
			-	g:EnterprisePro	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				jectId	
dcaas:gdgw:createPeerlink	授予创建指定全域接入网关的关联连接。	Write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:gdgw:updatePeerlink	授予更新指定全域接入网关的指定关联连接。	Write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:gdgw:deletePeerlink	授予删除指定全域接入网关的指定对等连接。	Write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:gdgw:getPeerlink	授予查询指定全域接入网关的指定关联连接。	Read	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:gdgw:listPeerlink	授予查询指定全域接入网关的所有关联连接列表。	List	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:connectGateway:create	授予权限以创建互联网关。	Write	connectGateway *	-	-
dcaas:connectGateway:update	授予权限以更新互联网关。	Write	connectGateway *	-	-
dcaas:connectGateway:delete	授予权限以删除互联网关。	Write	connectGateway *	-	-
dcaas:connectGateway:get	授予权限以查询互联网关详情。	Read	connectGateway *	-	-
dcaas:connectG	授予权限以查	List	conne	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ateway:list	询互联网关列表。		ctGateway *		
dcaas:connectGateway:listGlobalEip	授予权限以查询绑定的 geip 列表。	List	connectGateway *	-	-
dcaas:connectGateway:bindGlobalEip	授予权限以绑定 geip。	Write	connectGateway *	-	-
dcaas:connectGateway:unbindGlobalEip	授予权限以解绑定 geip。	Write	connectGateway *	-	-
dcaas:vif:switchoverTest	授予权限以进行倒换测试。	Write	vif *	-	-
dcaas:vif:listSwitchoverTestRecord	授予权限以获取倒换测试执行记录。	List	vif *	-	-
dcaas:vif:getSwitchoverTestRecord	授予权限以获取单条倒换测试执行记录。	Read	vif *	-	-
dcaas:resources:batchTagUntag	授予权限以批量增加删除云专线的资源标签。	Tagging	directConnect	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			lag	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			vgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			vif	• g:EnterpriseProjectId • g:ResourceTag/<tag-	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				key>	
			gdgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
dcaas:resources:listResourceTag	授予权限以查询云专线的资源标签。	List	direct Connect	-	-
			lag	-	
			vgw	-	
			vif	-	
			gdgw	-	
dcaas:resources:listTag	授予权限以查询云专线某个资源类型的标签。	List	direct Connect	-	-
			lag	-	
			vgw	-	
			vif	-	
			gdgw	-	
dcaas:resources:tag	授予权限以添加云专线的资源标签。	Tagging	direct Connect	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			lag	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			vgw	• g:EnterpriseProjectId • g:ResourceT	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ag/<tag-key>	
			vif	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			gdgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
dcaas:resources:unTag	授予权限以删除云专线的资源标签。	Tagging	directConnect	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			lag	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			vgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			vif	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			gdgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	g:TagKeys	
dcaas:resources:listByTag	授予根据标签查询云专线资源列表权限。	List	directConnect	-	-
			lag	-	
			vgw	-	
			vif	-	
			gdgw	-	
dcaas:gdgw:listGdgwRouteTable	授予权限以获取专线全域接入网关的路由表。	List	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:gdgw:updateGdgwRouteTable	授予权限以更新专线全域接入网关的路由表。	Write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:vgw:listVgwRouteTable	授予权限以获取专线虚拟网关的路由表。	List	vgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:vgw:updateVgwRouteTable	授予权限以更新专线虚拟网关的路由表。	Write	vgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
dcaas:quota:listVgwUsage	授予权限以获取专线的 VPC 下 VGW 配额。	List	-	-	-
dcaas:quota:listUsage	授予权限以获取专线的配额。	List	-	-	-
dcaas:lgw:create	授予创建本地网关权限。	Write	lgw *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dcaas:lgw:update	授予更新本地网关权限。	Write	lgw *	-	-
dcaas:lgw:delete	授予删除本地网关权限。	Write	lgw *	-	-
dcaas:lgw:get	授予查询本地网关详情权限。	Read	lgw *	-	-
dcaas:lgw:list	授予查询本地网关列表权限。	List	lgw *	-	-
dcaas:lgwTable:create	授予创建本地网关路由表权限。	Write	lgwTable *	-	-
			lgw *	-	
dcaas:lgwTable:update	授予更新本地网关路由表权限。	Write	lgwTable *	-	-
dcaas:lgwTable:delete	授予删除本地网关路由表权限。	Write	lgwTable *	-	-
dcaas:lgwTable:get	授予查询本地网关路由表详情权限。	Read	lgwTable *	-	-
dcaas:lgwTable:list	授予查询本地网关路由表列表权限。	List	lgwTable *	-	-
dcaas:lgwTable:createLgwTableRoute	授予创建本地网关路由表路由权限。	Write	lgwTable *	-	-
dcaas:lgwTable:updateLgwTableRoute	授予更新本地网关路由表路由权限。	Write	lgwTable *	-	-
dcaas:lgwTable:deleteLgwTableRoute	授予删除本地网关路由表路由权限。	Write	lgwTable *	-	-
dcaas:lgwTable	授予查询本地	Read	lgwTa	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
:getLgwTableRoute	网关路由表路由详情权限。		ble *		
dcaas:lgwTable:listLgwTableRoute	授予查询本地网关路由表路由列表权限。	List	lgwTable *	-	-
dcaas:lgwTable:batchDeleteLgwTableRoute	授予批量删除本地网关路由表路由权限。	Write	lgwTable *	-	-
dcaas:lgwTable:createLgwTableVpc	授予将本地网关路由表关联至虚拟私有云的权限。	Write	lgwTable *	-	-
			vpc *	-	
dcaas:lgwTable:updateLgwTableVpc	授予更新本地网关路由表虚拟私有云权限。	Write	lgwTable *	-	-
dcaas:lgwTable:deleteLgwTableVpc	授予解除本地网关路由表与虚拟私有云关联的权限。	Write	lgwTable *	-	-
dcaas:lgwTable:getLgwTableVpc	授予查询本地网关路由表虚拟私有云详情权限。	Read	lgwTable *	-	-
dcaas:lgwTable:listLgwTableVpc	授予查询本地网关路由表虚拟私有云列表权限。	List	lgwTable *	-	-

DC 的 API 通常对应着一个或多个授权项。表 3-54 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-54 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/dcaas	dcaas:directConnect:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/direct-connects/{direct_connect_id}		
GET /v3/{project_id}/dcaas/direct-connects	dcaas:directConnect:list	-
PUT /v3/{project_id}/dcaas/direct-connects/{direct_connect_id}	dcaas:directConnect:update	-
DELETE /v3/{project_id}/dcaas/direct-connects/{direct_connect_id}	dcaas:directConnect:delete	-
GET /v3/{project_id}/dcaas/hosted-connects	dcaas:directConnect:listHostedDirectConnect	-
POST /v3/{project_id}/dcaas/hosted-connects	dcaas:directConnect:createHostedDirectConnect	-
PUT /v3/{project_id}/dcaas/hosted-connects/{hosted_connect_id}	dcaas:directConnect:updateHostedDirectConnect	-
DELETE /v3/{project_id}/dcaas/hosted-connects/{hosted_connect_id}	dcaas:directConnect:deleteHostedDirectConnect	-
GET /v3/{project_id}/dcaas/virtual-gateways/{virtual_gateway_id}	dcaas:vgw:get	-
GET /v3/{project_id}/dcaas/virtual-gateways	dcaas:vgw:list	-
PUT /v3/{project_id}/dcaas/virtual-gateways/{virtual_gateway_id}	dcaas:vgw:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /v3/{project_id}/dcaas/virtual-gateways/{virtual_gateway_id}	dcaas:vgw:delete	-
POST /v3/{project_id}/dcaas/virtual-gateways	dcaas:vgw:create	• er:instances:get • vpc:vpcs:get
GET /v3/{project_id}/dcaas/virtual-interfaces/{virtual_interface_id}	dcaas:vif:get	-
GET /v3/{project_id}/dcaas/virtual-interfaces	dcaas:vif:list	-
PUT /v3/{project_id}/dcaas/virtual-interfaces/{virtual_interface_id}	dcaas:vif:update	-
DELETE /v3/{project_id}/dcaas/virtual-interfaces/{virtual_interface_id}	dcaas:vif:delete	-
POST /v3/{project_id}/dcaas/virtual-interfaces	dcaas:vif:create	-
PUT /v3/{project_id}/dcaas/vif-peers/{vif_peer_id}	dcaas:vifPeer:update	-
DELETE /v3/{project_id}/dcaas/vif-peers/{vif_peer_id}	dcaas:vifPeer:delete	-
POST /v3/{project_id}/dcaas/vif-peers	dcaas:vifPeer:create	-
GET /v3/{project_id}/dcaas/global-dc-gateways/{global_dc_gateway_id}	dcaas:gdgw:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/dcaas/global-dc-gateways/{global_dc_gateway_id}/peer-links/{peer_link_id}	dcaas:gdgw:getPeerlink	-
POST /v3/{project_id}/dcaas/switchover-test	dcaas:vif:switchoverTest	-
GET /v3/{project_id}/dcaas/switchover-test	dcaas:vif:listSwitchoverTestRecord	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-55 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

DC 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-55 DC 支持的资源类型

资源类型	URN
instances	er:<region>:<account-id>:instances:<instance-id>
lgw	dcaas:<region>:<account-id>:lgw:<lgw-id>
vif	dcaas:<region>:<account-id>:vif:<vif-id>
lgwTable	dcaas:<region>:<account-id>:lgwTable:<lgwTable-id>
gdgw	dcaas:<region>:<account-id>:gdgw:<gdgw-id>
vifPeer	dcaas:<region>:<account-id>:vifPeer:<vifPeer-id>
vpc	vpc:<region>:<account-id>:vpc:<vpc-id>
vgw	dcaas:<region>:<account-id>:vgw:<vgw-id>
directConnect	dcaas:<region>:<account-id>:directConnect:<directConnect-id>
lag	dcaas:<region>:<account-id>:lag:<lag-id>
connectGateway	dcaas:<region>:<account-id>:connectGateway:<connectGateway-id>

 版权所有 © 华为云计算技术有限公司

条件（Condition）

DC 服务不支持在身份策略中的条件键中配置服务级的条件键。DC 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.3.5 VPC 终端节点 VPCEP

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 VPCEP 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 VPCEP 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

 版权所有 © 华为云计算技术有限公司

您可以在身份策略语句的 Action 元素中指定以下 VPCEP 的相关操作。

表3-56 VPCEP 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
vpcep:endpoints:create	授予指定服务创建 VPC 终端节点的权限。	Write	endpoints *	• vpcep:VpceServiceName • vpcep:VpceServiceOrgPath • vpcep:VpceServiceOwner	-
			vpc *	-	
			routeTable	-	
			subnet	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	
vpcep:endpoints:delete	授予权限删除终端节点。	Write	endpoints *	• g:ResourceTag/<tag-key> • vpcep:VpceServiceName	-
vpcep:endpoints:list	授予查询终端节点列表。	List	endpoints *	-	-
			-	g:EnterpriseProjectId	
vpcep:endpoints:get	授予权限查询终端节点详情。	Read	endpoints *	g:ResourceTag/<tag-key>	-
vpcep:endpoints:update	授予权限更新终端节点的白名单。	Write	endpoints *	• vpcep:VpceServiceName • vpcep:VpceServiceOrgP	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ath • vpcep:VpceServiceOwner • g:ResourceTag/<tag-key>	
			routeTable	-	
			subnet	-	
vpcep:endpoints:upgrade	升级终端节点为专业型终端节点。	Write	endpoints *	• vpcep:VpceServiceName • vpcep:VpceServiceOrgPath • vpcep:VpceServiceOwner • g:ResourceTag/<tag-key>	-
vpcep:endpoints:updateRouteTables	授予权限修改终端节点路由表。	Write	endpoints *	g:ResourceTag/<tag-key>	vpcep:endpoints:update
			routeTable *	-	
vpcep:endpoints:updatePolicy	授予权限修改终端节点策略。	Write	endpoints *	g:ResourceTag/<tag-key>	vpcep:endpoints:update
vpcep:endpoints:deletePolicy	授予权限删除终端节点策略。	Write	endpoints *	g:ResourceTag/<tag-key>	vpcep:endpoints:delete
vpcep:endpointServices:create	授予权限创建终端节点服务。	Write	endpointServices *	vpcep:VpceServicePrivateDnsName	vpcep:epservices:create
			vpc *	-	
			-	• g:RequestTag/<tag-key>	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:TagKeys • g:EnterpriseProjectId	
vpcep:endpointServices:list	授予权限查询终端节点服务列表。	List	endpointServices *	-	vpcep:epservices:list
			-	g:EnterpriseProjectId	
vpcep:endpointServices:get	授予权限查询终端节点服务详情。	Read	endpointServices *	g:ResourceTag/<tag-key>	vpcep:epservices:get
vpcep:endpointServices:update	授予权限修改终端节点服务。	Write	endpointServices *	g:ResourceTag/<tag-key>	vpcep:epservices:update
vpcep:endpointServices:delete	授予权限删除终端节点服务。	Write	endpointServices *	g:ResourceTag/<tag-key>	vpcep:epservices:delete
vpcep:endpointServices:updateName	授予权限修改终端节点服务的名称。	Write	endpointServices *	-	vpcep:epservices:update
vpcep:endpointServices:describe	授予权限查询终端节点服务概要。	Read	-	-	vpcep:epserviceDesc:get
vpcep:endpointServices:listPublic	授予权限查询公共终端节点服务列表。	List	endpointServices *	-	vpcep:pubEpservices:list
vpcep:endpointServices:listPermissions	授予权限查询终端节点服务的白名单列表。	List	endpointServices *	-	vpcep:permissions:list
vpcep:endpointServices:updatePermissions	授予权限批量添加或移除终端节点服务的白名单。	Permission_management	endpointServices *	-	vpcep:permissions:update
			-	• vpcep:VpceEndpointOrgPath • vpcep:Vpce	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				EndpointOwner	
vpcep:endpointServices:createPermissions	授予权限批量添加终端节点服务的白名单。	Permission_management	endpointServices *	-	vpcep:permissions:update
			-	• vpcep:VpceEndpointOrgPath • vpcep:VpceEndpointOwner	
vpcep:endpointServices:deletePermissions	授予权限批量移除终端节点服务的白名单。	Permission_management	endpointServices *	-	vpcep:permissions:update
vpcep:endpointServices:updatePermissionsDescription	授予权限更新终端节点服务白名单描述。	Write	endpointServices *	-	vpcep:permissions:update
vpcep:endpointServices:listConnections	授予权限查询连接终端节点服务的连接列表。	List	endpointServices *	-	vpcep:connections:list
vpcep:endpointServices:updateConnections	授予权限接受或拒绝终端节点的连接。	Write	endpointServices *	-	vpcep:connections:update
vpcep:endpointServices:updateConnectionDescription	授予权限更新终端节点连接描述。	Write	endpointServices *	-	vpcep:connections:update
vpcep::listResourceTags	授予权限根据标签查询资源实例。	List	endpoints	-	vpcep:resource:list
			endpointServices	-	
vpcep::updateResourceTags	授予权限为指定 Endpoint Service 或 Endpoint 批量	Tagging	endpoints	-	vpcep:tags:update
			endpointServ	-	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	添加或删除标签。		ices		
vpcep::getProjectTags	授予权限查询租户资源标签。	Read	endpoints	-	vpcep:tags:list
			endpointServices	-	
vpcep::listQuotas	授予权限查询用户的资源配额，包括终端节点服务和终端节点。	Read	-	-	vpcep:quotas:get
vpcep::listVersionDetails	授予权限查询VPC 终端节点接口版本列表。	List	-	-	-
vpcep::listSpecifiedVersion	授予权限查询指定 VPC 终端节点接口版本信息。	List	-	-	-

VPCEP 的 API 通常对应着一个或多个授权项。表 3-57 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-57 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/vpc-endpoints	vpcep:endpoints:create	-
DELETE /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}	vpcep:endpoints:delete	-
GET /v1/{project_id}/vpc-endpoints	vpcep:endpoints:list	-
GET	vpcep:endpoints:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}		
PUT /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}	vpcep:endpoints:update	-
PUT /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}/routetables	vpcep:endpoints:updateRouteTables	-
PUT /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}/policy	vpcep:endpoints:updatePolicy	-
DELETE /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}/policy	vpcep:endpoints:deletePolicy	-
POST /v1/{project_id}/vpc-endpoint-services	vpcep:endpointServices:create	-
GET /v1/{project_id}/vpc-endpoint-services	vpcep:endpointServices:list	-
GET /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}	vpcep:endpointServices:get	-
PUT /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}	vpcep:endpointServices:update	-
DELETE /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}	vpcep:endpointServices:delete	-
PUT /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/name	vpcep:endpointServices:updateName	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/vpc-endpoint-services/describe	vpcep:endpointServices:describe	-
GET /v1/{project_id}/vpc-endpoint-services/public	vpcep:endpointServices:listPublic	-
GET /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions	vpcep:endpointServices:listPermissions	-
POST /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions/action	vpcep:endpointServices:updatePermissions	-
POST /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions/batch-create	vpcep:endpointServices:createPermissions	-
POST /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions/batch-delete	vpcep:endpointServices:deletePermissions	-
PUT /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions/{permission_id}	vpcep:endpointServices:updatePermissionsDescription	-
GET /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/connections	vpcep:endpointServices:listConnections	-
POST /v1/{project_id}/vpc-endpoint-	vpcep:endpointServices:updateConnections	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
services/{vpc_endpoint_service_id}/connections/action		
PUT /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/connections/description	vpcep:endpointServices:updateConnectionDescription	-
POST /v1/{project_id}/{resource_type}/resource_instances/action	vpcep::listResourceTags	-
POST /v1/{project_id}/{resource_type}/{resource_id}/tags/action	vpcep::updateResourceTags	-
GET /v1/{project_id}/{resource_type}/tags	vpcep::getProjectTags	-
GET /v1/{project_id}/quotas	vpcep::listQuotas	-
GET /	vpcep::listVersionDetails	-
GET /{version}	vpcep::listSpecifiedVersion	-
POST /v2/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/add-server-resources	vpcep:endpointServices:update	-
POST /v2/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/remove-server-resources	vpcep:endpointServices:update	-
POST /v2/{project_id}/vpc-endpoints/{vpc_endpoint_id}/add-availability-zones	vpcep:endpointServices:updateConnections	-
POST /v2/{project_id}/vpc-endpoints/{vpc_endpo	vpcep:endpointServices:updateConnections	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
int_id}/remove-availability-zones		

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-58 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

VPCEP 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-58 VPCEP 支持的资源类型

资源类型	URN
routeTable	vpc:<region>:<account-id>:routeTable:<route-table-id>
vpc	vpc:<region>:<account-id>:vpc:<vpc-id>
endpointServices	vpcep:<region>:<account-id>:endpointServices:<endpoint-service-id>
subnet	vpc:<region>:<account-id>:subnet:<subnet-id>
endpoints	vpcep:<region>:<account-id>:endpoints:<endpoint-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 vpcep:）仅适用于对应服务的操作，详情请参见表 3-59。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

 版权所有 © 华为云计算技术有限公司

VPCEP 支持的服务级条件键

VPCEP 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-59 VPCEP 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
vpcep:VpceServiceName	string	单值	按照终端节点服务名称进行筛选。
vpcep:VpceServiceOwner	string	单值	按照终端节点服务所有者进行筛选。
vpcep:VpceServicePrivateDnsName	string	单值	按您传入的终端节点服DNS 名称筛选访问权限。
vpcep:VpceServiceOrgPath	string	单值	按照终端节点服务所有者的组织路径进行筛选。
vpcep:VpceEndpointOrgPath	string	多值	按照终端节点所有者的组织路径进行筛选。
vpcep:VpceEndpointOwner	string	多值	按照终端节点所有者的账号进行筛选。

3.3.6 全球加速 GA

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

 版权所有 © 华为云计算技术有限公司

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 GA 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 GA 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 GA 的相关操作。

表3-60 GA 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ga:accelerator:list	授予查询加速器列表权限。	List	accelerator *	-	-
ga:accelerator:create	授予创建加速器权限。	Write	accelerator *	g:EnterpriseProjectId	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
ga:accelerator:get	授予查询加速器详情权限。	Read	accelerator *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
ga:accelerator:update	授予更新加速器权限。	Write	accelerator *	• g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:ResourceTag/<tag-key>	
ga:accelerator:delete	授予删除加速器权限。	Write	accelerator *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
ga:listener:list	授予查询监听器列表权限。	List	listener *	-	-
ga:listener:create	授予创建监听器权限。	Write	listener *	-	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
ga:listener:get	授予查询监听器详情权限。	Read	listener *	g:ResourceTag/<tag-key>	-
ga:listener:update	授予更新监听器权限。	Write	listener *	g:ResourceTag/<tag-key>	-
ga:listener:delete	授予删除监听器权限。	Write	listener *	g:ResourceTag/<tag-key>	-
ga:endpointgroup:list	授予查询终端节点组列表权限。	List	endpointgroup *	-	-
ga:endpointgroup:create	授予创建终端节点组权限。	Write	endpointgroup *	-	-
			-	ga:RequestRegionId	
ga:endpointgroup:get	授予查询终端节点组详情权限。	Read	endpointgroup *	ga:RegionId	-
ga:endpointgroup:update	授予更新终端节点组权限。	Write	endpointgroup *	ga:RegionId	-
ga:endpointgro	授予删除终端	Write	endpointgrou	ga:RegionId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
up:delete	节点组权限。		p *		
ga:endpoint:list	授予查询终端节点列表权限。	List	endpoint *	-	-
ga:endpoint:create	授予创建终端节点权限。	Write	endpoint *	-	-
			-	• ga:RequestResourceType • ga:RequestResourceId • ga:RequestIpAddress • ga:RequestDomainName	
ga:endpoint:get	授予查询终端节点详情权限。	Read	endpoint *	• ga:ResourceType • ga:ResourceId • ga:IpAddress • ga:DomainName	-
ga:endpoint:update	授予更新终端节点权限。	Write	endpoint *	• ga:ResourceType • ga:ResourceId • ga:IpAddress • ga:DomainName	-
ga:endpoint:delete	授予删除终端节点权限。	Write	endpoint *	• ga:ResourceType • ga:ResourceId • ga:IpAddress • ga:DomainName	-
ga:healthcheck:	授予查询健康	List	health	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
list	检查列表权限。		check *		
ga:healthcheck:create	授予创建健康检查权限。	Write	healthcheck *	-	-
ga:healthcheck:get	授予查询健康检查详情权限。	Read	healthcheck *	-	-
ga:healthcheck:update	授予更新健康检查权限。	Write	healthcheck *	-	-
ga:healthcheck:delete	授予删除健康检查权限。	Write	healthcheck *	-	-
ga:tag:create	授予批量创建资源的标签权限。	Tagging	accelerator	g:ResourceTag/<tag-key>	-
			listener	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
ga:tag:delete	授予批量删除资源的标签权限。	Tagging	accelerator *	g:ResourceTag/<tag-key>	-
			listener *	g:ResourceTag/<tag-key>	
			-	g:TagKeys	
ga:tag:get	授予查询资源的标签权限。	Read	accelerator	g:ResourceTag/<tag-key>	-
			listener	g:ResourceTag/<tag-key>	
ga:tag:list	授予查询标签列表的权限。	List	-	-	-
ga::listResourcesByTag	授予通过标签查询资源实例列表的权限。	List	-	g:TagKeys	ga:tag:listResourcesByTag
ga:ipgroup:list	授予查询 IP 地	List	ipgrou	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	址组列表权限。		p *		
ga:ipgroup:create	授予创建 IP 地址组权限。	Write	ipgroup *	-	-
ga:ipgroup:get	授予查询 IP 地址组详情权限。	Read	ipgroup *	-	-
ga:ipgroup:update	授予更新 IP 地址组权限。	Write	ipgroup *	-	-
ga:ipgroup:delete	授予删除 IP 地址组权限。	Write	ipgroup *	-	-
ga:ipgroup:addIps	授予为 IP 地址组批量添加 IP 权限。	Write	ipgroup *	-	-
ga:ipgroup:removeIps	授予为 IP 地址组批量删除 IP 权限。	Write	ipgroup *	-	-
ga:ipgroup:associateListener	授予为 IP 地址组绑定监听器权限。	Write	ipgroup *	-	-
ga:ipgroup:disassociateListener	授予为 IP 地址组解绑监听器权限。	Write	ipgroup *	-	-
ga::listByoipPools	授予查询自带 IP（BYOIP）地址池列表权限。	List	-	-	ga:byoippool:list
ga:logtank:list	授予查询云日志列表的权限。	List	logtank *	-	-
ga:logtank:create	授予创建云日志的权限。	Write	logtank *	-	-
ga:logtank:get	授予获取云日志详情的权限。	Read	logtank *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ga:logtank:update	授予修改云日志的权限。	Write	logtank *	-	-
ga:logtank:delete	授予删除云日志的权限。	Write	logtank *	-	-

GA 的 API 通常对应着一个或多个授权项。表 3-61 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-61 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1/accelerators	ga:accelerator:list	-
POST /v1/accelerators	ga:accelerator:create	-
GET /v1/accelerators/{accelerator_id}	ga:accelerator:get	-
PUT /v1/accelerators/{accelerator_id}	ga:accelerator:update	-
DELETE /v1/accelerators/{accelerator_id}	ga:accelerator:delete	-
GET /v1/listeners	ga:listener:list	-
POST /v1/listeners	ga:listener:create	-
GET /v1/listeners/{listener_id}	ga:listener:get	-
PUT /v1/listeners/{listener_id}	ga:listener:update	-
DELETE /v1/listeners/{listener_id}	ga:listener:delete	-
GET /v1/endpoint-groups	ga:endpointgroup:list	-
POST /v1/endpoint-	ga:endpointgroup:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
groups		
GET /v1/endpoint-groups/{endpoint_group_id}	ga:endpointgroup:get	-
PUT /v1/endpoint-groups/{endpoint_group_id}	ga:endpointgroup:update	-
DELETE /v1/endpoint-groups/{endpoint_group_id}	ga:endpointgroup:delete	-
GET /v1/endpoint-groups/{endpoint_group_id}/endpoints	ga:endpoint:list	-
POST /v1/endpoint-groups/{endpoint_group_id}/endpoints	ga:endpoint:create	-
GET /v1/endpoint-groups/{endpoint_group_id}/endpoints/{endpoint_id}	ga:endpoint:get	-
PUT /v1/endpoint-groups/{endpoint_group_id}/endpoints/{endpoint_id}	ga:endpoint:update	-
DELETE /v1/endpoint-groups/{endpoint_group_id}/endpoints/{endpoint_id}	ga:endpoint:delete	-
GET /v1/health-checks	ga:healthcheck:list	-
POST /v1/health-checks	ga:healthcheck:create	-
GET /v1/health-checks/{health_check_id}	ga:healthcheck:get	-
PUT /v1/health-checks/{health_check_id}	ga:healthcheck:update	-
DELETE /v1/health-checks/{health_check_id}	ga:healthcheck:delete	-
POST	ga:tag:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{resource_type}/{resource_id}/tags/create		
DELETE /v1/{resource_type}/{resource_id}/tags/delete	ga:tag:delete	-
GET /v1/{resource_type}/{resource_id}/tags	ga:tag:get	-
POST /v1/{resource_type}/resource-instances/filter	ga::listResourcesByTag	-
POST /v1/{resource_type}/resource-instances/count	ga::listResourcesByTag	-
GET /v1/{resource_type}/tags	ga:tag:list	-
GET /v1/ip-groups	ga:ipgroup:list	-
POST /v1/ip-groups	ga:ipgroup:create	-
GET /v1/ip-groups/{ip_group_id}	ga:ipgroup:get	-
PUT /v1/ip-groups/{ip_group_id}	ga:ipgroup:update	-
DELETE /v1/ip-groups/{ip_group_id}	ga:ipgroup:delete	-
POST /v1/ip-groups/{ip_group_id}/add-ips	ga:ipgroup:addIps	-
POST /v1/ip-groups/{ip_group_id}/remove-ips	ga:ipgroup:removeIps	-
POST /v1/ip-groups/{ip_group_id}/associate-listener	ga:ipgroup:associateListener	-
POST /v1/ip-groups/{ip_group_id}/disassociate-listener	ga:ipgroup:disassociateListener	-
GET /v1/byoip-pools	ga::listByoipPools	-
GET /v1/logtanks	ga:logtank:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/logtanks	ga:logtank:create	-
GET /v1/logtanks/{logtank_id}	ga:logtank:get	-
PUT /v1/logtanks/{logtank_id}	ga:logtank:update	-
DELETE /v1/logtanks/{logtank_id}	ga:logtank:delete	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-62 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

GA 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-62 GA 支持的资源类型

资源类型	URN
ipgroup	ga::<account-id>:ipgroup:<ipgroup-id>
endpoint	ga::<account-id>:endpoint:<endpoint-id>
accelerator	ga::<account-id>:accelerator:<accelerator-id>
logtank	ga::<account-id>:logtank:<logtank-id>
listener	ga::<account-id>:listener:<listener-id>
healthcheck	ga::<account-id>:healthcheck:<healthcheck-id>
endpointgroup	ga::<account-id>:endpointgroup:<endpointgroup-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。

 版权所有 © 华为云计算技术有限公司

  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 ga:）仅适用于对应服务的操作，详情请参见表 3-63。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。

- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

GA 支持的服务级条件键

GA 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-63 GA 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
ga:RequestRegionId	string	单值	按照在请求中传递的地域 ID 筛选访问权限。
ga:RequestResourceType	string	单值	按照在请求中传递的资源类型筛选访问权限。
ga:RequestResourceId	string	单值	按照在请求中传递的资源 ID 筛选访问权限。
ga:RequestIpAddress	string	单值	按照在请求中传递的 IP 地址筛选访问权限。
ga:RequestDomainName	string	单值	按照在请求中传递的域名筛选访问权限。
ga:RegionId	string	单值	按照终端节点组的地域筛选访问权限。
ga:ResourceType	string	单值	按照终端节点的资源类型筛选访问权限。
ga:ResourceId	string	单值	按照终端节点的资源 ID 筛选访问权限。
ga:IpAddress	string	单值	按照终端节点的 IP 地址筛选访问权限。
ga:DomainName	string	单值	按照终端节点的域名筛选访问权限。

 版权所有 © 华为云计算技术有限公司

3.3.7 NAT 网关 NAT

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 NAT 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 NAT 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 NAT 的相关操作。

 版权所有 © 华为云计算技术有限公司

表3-64 NAT 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
nat:privateNatGateways:list	授予权限以查询私网 NAT 网关列表。	List	privateGateway *	g:EnterpriseProjectId	-
nat:privateNatGateways:create	授予权限以创建私网 NAT 网关。	Write	privateGateway *	-	-
			subnet *	-	
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
nat:privateNatGateways:delete	授予权限以删除指定的私网 NAT 网关。	Write	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
nat:privateNatGateways:get	授予权限以查询指定的私网 NAT 网关。	Read	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
nat:privateNatGateways:update	授予权限以更新指定的私网 NAT 网关。	Write	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
nat:privateNatDnatRules:list	授予权限以查询私网 NAT 网关 DNAT 规则列表。	List	privateDnatRule *	g:EnterpriseProjectId	-
nat:privateNatDnatRules:create	授予权限以创建私网 NAT 网关 DNAT 规则。	Write	privateGateway *	g:ResourceTag/<tag-key>	-
			privateDnat	-	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			Rule *		
			privateTransitIp *	g:ResourceTag/<tag-key>	
			port	-	
			-	g:EnterpriseProjectId	
nat:privateNatDnatRules:delete	授予权限以删除指定的私网NAT网关DNAT规则。	Write	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			privateDnatRule *	g:EnterpriseProjectId	
nat:privateNatDnatRules:get	授予权限以查询指定的私网NAT网关DNAT规则。	Read	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			privateDnatRule *	g:EnterpriseProjectId	
nat:privateNatDnatRules:update	授予权限以更新指定的私网NAT网关DNAT规则。	Write	privateGateway *	g:ResourceTag/<tag-key>	-
			privateDnatRule *	-	
			privateTransitIp	g:ResourceTag/<tag-key>	
			port	-	
			-	g:EnterpriseProjectId	
nat:privateNatSnatRules:list	授予权限以查询私网NAT网关SNAT规	List	privateSnatRule *	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	则列表。				
nat:privateNatSnatRules:create	授予权限以创建私网 NAT 网关 SNAT 规则。	Write	privateGateway *	g:ResourceTag/<tag-key>	-
			privateSnatRule *	-	
			privateTransitIp *	g:ResourceTag/<tag-key>	
			subnet	-	
			-	g:EnterpriseProjectId	
nat:privateNatSnatRules:delete	授予权限以删除指定的私网 NAT 网关 SNAT 规则。	Write	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			privateSnatRule *	g:EnterpriseProjectId	
nat:privateNatSnatRules:get	授予权限以查询指定的私网 NAT 网关 SNAT 规则。	Read	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			privateSnatRule *	g:EnterpriseProjectId	
nat:privateNatSnatRules:update	授予权限以更新指定的私网 NAT 网关 SNAT 规则。	Write	privateGateway *	g:ResourceTag/<tag-key>	-
			privateSnatRule *	-	
			privateTransitIp	g:ResourceTag/<tag-key>	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	g:EnterpriseProjectId	
nat:privateNatTransitIps:list	授予权限以查询私网 NAT 中转 IP 地址列表。	List	privateTransitIp *	g:EnterpriseProjectId	nat:transitIps:list
nat:privateNatTransitIps:create	授予权限以创建私网 NAT 中转 IP 地址。	Write	privateTransitIp *	-	nat:transitIps:create
			subnet	g:ResourceTag/<tag-key>	
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
nat:privateNatTransitIps:delete	授予权限以删除指定的私网 NAT 中转 IP 地址。	Write	privateTransitIp *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	nat:transitIps:delete
nat:privateNatTransitIps:get	授予权限以查询指定的私网 NAT 中转 IP 地址。	Read	privateTransitIp *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	nat:transitIps:get
nat:transitSubnets:list	授予权限以查询中转子网列表。	List	transitSubnet *	-	-
nat:transitSubnets:create	授予权限以创建中转子网。	Write	transitSubnet *	-	-
			subnet *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
nat:transitSubnets:delete	授予权限以删除指定的中转子网。	Write	transitSubnet *	g:ResourceTag/<tag-key>	-
nat:transitSubnets:get	授予权限以查询指定的中转子网。	Read	transitSubnet *	g:ResourceTag/<tag-key>	-
nat:transitSubnets:update	授予权限以更新指定的中转子网。	Write	transitSubnet *	g:ResourceTag/<tag-key>	-
nat:privateNatGateways:createTags	授予权限以创建私网 NAT 网关标签。	Tagging	privateGateway *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	nat:privateNatGatewayTags:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
nat:privateNatGateways:deleteTags	授予权限以删除指定的私网 NAT 网关标签。	Tagging	privateGateway *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	nat:privateNatGatewayTags:delete
			-	• g:RequestTag/<tag-key> • g:TagKeys	
nat:privateNatGateways:listTags	授予权限以查询私网 NAT 网关标签。	List	privateGateway	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	nat:privateNatGatewayTags:list
nat:privateNatTransitIps:createTags	授予权限以创建私网 NAT 中转 IP 标签。	Tagging	privateTransitIp *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	nat:transitIpTags:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
nat:privateNatTransitIps:deleteTags	授予权限以删除指定的私网NAT 中转 IP 标签。	Tagging	privateTransitIp *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	nat:transitIpTags:delete
			-	• g:RequestTag/<tag-key> • g:TagKeys	
nat:privateNatTransitIps:listTags	授予权限以查询私网 NAT 中转 IP 标签。	List	privateTransitIp	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	nat:transitIpTags:list
nat:transitSubnets:createTags	授予权限以创建中转子网标签。	Tagging	transitSubnet *	g:ResourceTag/<tag-key>	nat:transitSubnetTags:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
nat:transitSubnets:deleteTags	授予权限以删除指定的中转子网标签。	Tagging	transitSubnet *	g:ResourceTag/<tag-key>	nat:transitSubnetTags:delete
			-	• g:RequestTag/<tag-key> • g:TagKeys	
nat:transitSubnets:listTags	授予权限以查询中转子网标签。	List	transitSubnet	g:ResourceTag/<tag-key>	nat:transitSubnetTags:list
nat:natGateways:list	授予权限以查询公网 NAT 网关列表。	List	gateway *	g:EnterpriseProjectId	-
nat:natGateways:create	授予权限以创建公网 NAT 网关。	Write	gateway *	-	-
			vpc *	-	
			subnet *	-	
			-	• g:Enterprise	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ProjectId • g:RequestTag/<tag-key> • g:TagKeys	
nat:natGateways:delete	授予权限以删除指定的公网NAT 网关。	Write	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
nat:natGateways:get	授予权限以查询指定的公网NAT 网关。	Read	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
nat:natGateways:update	授予权限以更新指定的公网NAT 网关。	Write	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
nat:dnatRules:list	授予权限以查询公网 NAT 网关 DNAT 规则列表。	List	dnatRule *	g:EnterpriseProjectId	-
nat:dnatRules:create	授予权限以创建公网 NAT 网关 DNAT 规则。	Write	gateway *	g:ResourceTag/<tag-key>	-
			dnatRule *	-	
			publicip	-	
			globalEip	-	
			port	-	
			-	g:EnterpriseProjectId	
nat:dnatRules:get	授予权限以查询指定的公网NAT 网关	Read	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	DNAT 规则。			key>	
			dnatRule *	g:EnterpriseProjectId	
nat:dnatRules:update	授予权限以更新指定的公网 NAT 网关 DNAT 规则。	Write	gateway *	g:ResourceTag/<tag-key>	-
			dnatRule *	-	
			public ip	-	
			global Eip	-	
			port	-	
			-	g:EnterpriseProjectId	
nat:dnatRules:delete	授予权限以删除指定的公网 NAT 网关 DNAT 规则。	Write	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			dnatRule *	g:EnterpriseProjectId	
nat:snatRules:list	授予权限以查询公网 NAT 网关 SNAT 规则列表。	List	snatRule *	g:EnterpriseProjectId	-
nat:snatRules:create	授予权限以创建公网 NAT 网关 SNAT 规则。	Write	gateway *	g:ResourceTag/<tag-key>	-
			snatRule *	-	
			public ip	-	
			global Eip	-	
			subnet	-	
			-	g:EnterpriseProjectId	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
nat:snatRules:get	授予权限以查询指定的公网NAT 网关SNAT 规则。	Read	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			snatRule *	g:EnterpriseProjectId	
nat:snatRules:update	授予权限以更新指定的公网NAT 网关SNAT 规则。	Write	gateway *	g:ResourceTag/<tag-key>	-
			snatRule *	-	
			publicip	-	
			globalEip	-	
			-	g:EnterpriseProjectId	
nat:snatRules:delete	授予权限以删除指定的公网NAT 网关SNAT 规则。	Write	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			snatRule *	g:EnterpriseProjectId	
nat:natGateways:createTags	授予权限以创建公网 NAT 网关标签。	Tagging	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	nat:natGatewayTags:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
nat:natGateways:deleteTags	授予权限以删除指定的公网NAT 网关标签。	Tagging	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	nat:natGatewayTags:delete
			-	• g:RequestTa	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				g/<tag-key> • g:TagKeys	
nat:natGateways:listTags	授予权限以查询公网 NAT 网关标签。	List	gateway	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	nat:natGatewayTags:get

NAT 的 API 通常对应着一个或多个授权项。表 3-65 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-65 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/private-nat/gateways	nat:privateNatGateways:list	-
POST /v3/{project_id}/private-nat/gateways	nat:privateNatGateways:create	-
DELETE /v3/{project_id}/private-nat/gateways/{gateway_id}	nat:privateNatGateways:delete	-
GET /v3/{project_id}/private-nat/gateways/{gateway_id}	nat:privateNatGateways:get	-
PUT /v3/{project_id}/private-nat/gateways/{gateway_id}	nat:privateNatGateways:update	-
GET /v3/{project_id}/private-nat/dnat-rules	nat:privateNatDnatRules:list	-
POST /v3/{project_id}/privat	nat:privateNatDnatRules:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
e-nat/dnat-rules		
DELETE /v3/{project_id}/private-nat/dnat-rules/{dnat_rule_id}	nat:privateNatDnatRules:delete	-
GET /v3/{project_id}/private-nat/dnat-rules/{dnat_rule_id}	nat:privateNatDnatRules:get	-
PUT /v3/{project_id}/private-nat/dnat-rules/{dnat_rule_id}	nat:privateNatDnatRules:update	-
GET /v3/{project_id}/private-nat/snat-rules	nat:privateNatSnatRules:list	-
POST /v3/{project_id}/private-nat/snat-rules	nat:privateNatSnatRules:create	-
DELETE /v3/{project_id}/private-nat/snat-rules/{snat_rule_id}	nat:privateNatSnatRules:delete	-
GET /v3/{project_id}/private-nat/snat-rules/{snat_rule_id}	nat:privateNatSnatRules:get	-
PUT /v3/{project_id}/private-nat/snat-rules/{snat_rule_id}	nat:privateNatSnatRules:update	-
GET /v3/{project_id}/private-nat/transit-ips	nat:privateNatTransitIps:list	-
POST /v3/{project_id}/private-nat/transit-ips	nat:privateNatTransitIps:create	-
DELETE /v3/{project_id}/private-nat/transit-ips/{transit_ip_id}	nat:privateNatTransitIps:delete	-
GET /v3/{project_id}/private-nat/transit-	nat:privateNatTransitIps:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ips/{transit_ip_id}		
POST /v3/{project_id}/private-nat-gateways/resource_instances/action	nat:privateNatGateways:listTags	-
POST /v3/{project_id}/private-nat-gateways/{resource_id}/tags/action	nat:privateNatGateways:createTags	nat:privateNatGateways:deleteTags
POST /v3/{project_id}/private-nat-gateways/{resource_id}/tags	nat:privateNatGateways:createTags	-
GET /v3/{project_id}/private-nat-gateways/{resource_id}/tags	nat:privateNatGateways:listTags	-
DELETE /v3/{project_id}/private-nat-gateways/{resource_id}/tags/{key}	nat:privateNatGateways:deleteTags	-
GET /v3/{project_id}/private-nat-gateways/tags	nat:privateNatGateways:listTags	-
POST /v3/{project_id}/transit-ips/resource_instances/action	nat:privateNatTransitIps:listTags	-
POST /v3/{project_id}/transit-ips/{resource_id}/tags/action	nat:privateNatTransitIps:createTags	nat:privateNatTransitIps:deleteTags
POST /v3/{project_id}/transit-ips/{resource_id}/tags	nat:privateNatTransitIps:createTags	-
GET /v3/{project_id}/transit-	nat:privateNatTransitIps:listTags	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ips/{resource_id}/tags		
DELETE /v3/{project_id}/transit-ips/{resource_id}/tags/{key}	nat:privateNatTransitIps:deleteTags	-
GET /v3/{project_id}/transit-ips/tags	nat:privateNatTransitIps:listTags	-
POST /v3/{project_id}/private-nat/transit-subnets	nat:transitSubnets:create	-
DELETE /v3/{project_id}/private-nat/transit-subnets/{transit_subnet_id}	nat:transitSubnets:delete	-
GET /v3/{project_id}/private-nat/transit-subnets/{transit_subnet_id}	nat:transitSubnets:get	-
PUT /v3/{project_id}/private-nat/transit-subnets/{transit_subnet_id}	nat:transitSubnets:update	-
POST /v3/{project_id}/transit-subnets/resource_instances/action	nat:transitSubnets:listTags	-
POST /v3/{project_id}/transit-subnets/{resource_id}/tags/action	nat:transitSubnets:createTags	nat:transitSubnets:deleteTags
POST /v3/{project_id}/transit-subnets/{resource_id}/tags	nat:transitSubnets:createTags	-
GET /v3/{project_id}/transit-subnets/{resource_id}/	nat:transitSubnets:listTags	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
tags		
DELETE /v3/{project_id}/transit-subnets/{resource_id}/tags/{key}	nat:transitSubnets:deleteTags	-
GET /v3/{project_id}/transit-subnets/tags	nat:transitSubnets:listTags	-
GET /v2/{project_id}/nat_gateways	nat:natGateways:list	-
POST /v2/{project_id}/nat_gateways	nat:natGateways:create	-
DELETE /v2/{project_id}/nat_gateways/{nat_gateway_id}	nat:natGateways:delete	-
GET /v2/{project_id}/nat_gateways/{nat_gateway_id}	nat:natGateways:get	-
PUT /v2/{project_id}/nat_gateways/{nat_gateway_id}	nat:natGateways:update	-
GET /v2/{project_id}/dnat_rules	nat:dnatRules:list	-
POST /v2/{project_id}/dnat_rules	nat:dnatRules:create	eip:publicIps:associateInstance
GET /v2/{project_id}/dnat_rules/{dnat_rule_id}	nat:dnatRules:get	-
PUT /v2/{project_id}/dnat_rules/{dnat_rule_id}	nat:dnatRules:update	• eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
POST /v2/{project_id}/dnat_rules/batch	nat:dnatRules:create	eip:publicIps:associateInstance

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /v2/{project_id}/nat_gateways/{nat_gateway_id}/dnat_rules/{dnat_rule_id}	nat:dnatRules:delete	eip:publicIps:disassociateInstance
GET /v2/{project_id}/snat_rules	nat:snatRules:list	-
POST /v2/{project_id}/snat_rules	nat:snatRules:create	eip:publicIps:associateInstance
GET /v2/{project_id}/snat_rules/{snat_rule_id}	nat:snatRules:get	-
PUT /v2/{project_id}/snat_rules/{snat_rule_id}	nat:snatRules:update	• eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
DELETE /v2/{project_id}/nat_gateways/{nat_gateway_id}/snat_rules/{snat_rule_id}	nat:snatRules:delete	eip:publicIps:disassociateInstance
POST /v3/{project_id}/nat_gateways/resource_instances/action	nat:natGateways:listTags	-
POST /v3/{project_id}/nat_gateways/{nat_gateway_id}/tags/action	nat:natGateways:createTags	nat:natGateways:deleteTags
POST /v3/{project_id}/nat_gateways/{nat_gateway_id}/tags	nat:natGateways:createTags	-
GET /v3/{project_id}/nat_gateways/{nat_gateway_id}/tags	nat:natGateways:listTags	-
DELETE /v3/{project_id}/nat_gateways/{nat_gateway_id}/tags/{key}	nat:natGateways:deleteTags	-
GET /v3/{project_id}/nat_g	nat:natGateways:listTags	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ateways/tags		

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-66 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

NAT 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-66 NAT 支持的资源类型

资源类型	URN
snatRule	nat:<region>:<account-id>:snatRule:<snat-rule-id>
privateSnatRule	nat:<region>:<account-id>:privateSnatRule:<private-snat-rule-id>
port	vpc:<region>:<account-id>:port:<port-id>
privateGateway	nat:<region>:<account-id>:privateGateway:<private-gateway-id>
vpc	vpc:<region>:<account-id>:vpc:<vpc-id>
publicip	vpc:<region>:<account-id>:publicip:<publicip-id>
gateway	nat:<region>:<account-id>:gateway:<gateway-id>
privateTransitIp	nat:<region>:<account-id>:privateTransitIp:<private-transit-ip-id>
dnatRule	nat:<region>:<account-id>:dnatRule:<dnat-rule-id>
globalEip	eip:<region>:<account-id>:globalEip:<geip-id>
privateDnatRule	nat:<region>:<account-id>:privateDnatRule:<private-dnat-rule-id>
subnet	vpc:<region>:<account-id>:subnet:<subnet-id>
transitSubnet	nat:<region>:<account-id>:transitSubnet:<transit-subnet-id>

条件（Condition）

NAT 服务不支持在身份策略中的条件键中配置服务级的条件键。NAT 可以使用适用于所有服务的全局条件键，请参考全局条件键。

 版权所有 © 华为云计算技术有限公司

3.3.8 云连接 CC

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 CC 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 CC 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 CC 的相关操作。

 版权所有 © 华为云计算技术有限公司

表3-67 CC 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cc:cloudConnections:create	授予创建云连接权限。	Write	cloud Connection *	-	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
cc:cloudConnections:delete	授予删除云连接权限。	Write	cloud Connection *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cc:cloudConnections:update	授予更新云连接权限。	Write	cloud Connection *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cc:cloudConnections:get	授予查询云连接详情权限。	Read	cloud Connection *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cc:cloudConnections:list	授予查询云连接列表权限。	List	cloud Connection *	-	-
cc:cloudConnections:tag	授予为云连接实例打标签权限。	Tagging	cloud Connection *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
cc:cloudConnections:unTag	授予为云连接实例删除标签权限。	Tagging	cloud Connection *	• g:EnterpriseProjectId • g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
cc:cloudConnections:listTags	授予查询为云连接资源的标签列表权限。	List	cloud Connection *	-	-
cc:networkInstances:create	授予创建网络实例权限。	Write	networkInstance *	-	-
			cloud Connection *	g:ResourceTag/<tag-key>	
			-	• g:EnterpriseProjectId • cc:VpcId • cc:VirtualGatewayId • cc:EnterpriseRouterId	
cc:networkInstances:delete	授予删除网络实例权限。	Write	networkInstance *	• cc:VpcId • cc:VirtualGatewayId • cc:EnterpriseRouterId	-
			cloud Connection *	g:ResourceTag/<tag-key>	
			-	g:EnterpriseProjectId	
cc:networkInstances:update	授予更新网络实例权限。	Write	networkInstance *	• cc:VpcId • cc:VirtualGatewayId • cc:EnterpriseRouterId	-
			cloud Connection *	g:ResourceTag/<tag-key>	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	g:EnterpriseProjectId	
cc:networkInstances:get	授予查询网络实例详情权限。	Read	networkInstance *	-	-
			cloudConnection *	g:ResourceTag/<tag-key>	
			-	g:EnterpriseProjectId	
cc:networkInstances:list	授予查询网络实例列表权限。	List	networkInstance *	-	-
cc:bandwidthPackages:create	授予创建带宽包权限。	Write	bandwidthPackage *	-	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
cc:bandwidthPackages:delete	授予删除带宽包权限。	Write	bandwidthPackage *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cc:bandwidthPackages:update	授予更新带宽包权限。	Write	bandwidthPackage *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cc:bandwidthPackages:get	授予查询带宽包详情权限。	Read	bandwidthPackage *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cc:bandwidthPackages:list	授予查询带宽	List	bandwidthPa	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	包列表权限。		ckage *		
cc:bandwidthPackages:tag	授予为带宽包打标签权限。	Tagging	bandwidthPackage *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
cc:bandwidthPackages:unTag	授予为带宽包删除标签权限。	Tagging	bandwidthPackage *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
cc:bandwidthPackages:listTags	授予查询带宽包资源的标签列表权限。	List	bandwidthPackage *	-	-
cc:bandwidthPackages:associate	授予关联带宽包权限。	Write	bandwidthPackage *	g:ResourceTag/<tag-key>	-
			cloud Connection *	g:ResourceTag/<tag-key>	
			-	g:EnterpriseProjectId	
cc:bandwidthPackages:disassociate	授予解关联带宽包权限。	Write	bandwidthPackage *	g:ResourceTag/<tag-key>	-
			cloud Connection *	g:ResourceTag/<tag-key>	
			-	g:EnterprisePro	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				jectId	
cc:interRegionBandwidths:create	授予创建域间带宽权限。	Write	interRegionBandwidth *	-	-
			cloudConnection *	g:ResourceTag/<tag-key>	
			-	• g:EnterpriseProjectId • cc:BandwidthPackageId	
cc:interRegionBandwidths:delete	授予删除域间带宽权限。	Write	interRegionBandwidth *	cc:BandwidthPackageId	-
			cloudConnection *	g:ResourceTag/<tag-key>	
			-	g:EnterpriseProjectId	
cc:interRegionBandwidths:update	授予更新域间带宽权限。	Write	interRegionBandwidth *	cc:BandwidthPackageId	-
			cloudConnection *	g:ResourceTag/<tag-key>	
			-	g:EnterpriseProjectId	
cc:interRegionBandwidths:get	授予查询域间带宽详情权限。	Read	interRegionBandwidth *	-	-
			cloudConne	g:ResourceTag/<tag-key>	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			ction *		
			-	g:EnterpriseProjectId	
cc:interRegionBandwidths:list	授予查询域间带宽列表权限。	List	interRegionBandwidth *	-	-
cc:cloudConnectionRoutes:get	授予查询云连接路由详情权限。	Read	-	-	-
cc:cloudConnectionRoutes:list	授予查询云连接路由列表权限。	List	-	-	-
cc:authorisation:create	授予创建虚拟私有云授权的权限。	Write	-	-	-
cc:authorisation:delete	授予删除虚拟私有云授权的权限。	Write	-	-	-
cc:authorisation:update	授予更新虚拟私有云授权基本信息的权限。	Write	-	-	-
cc:authorisation:list	授予查询虚拟私有云授权列表权限。	List	-	-	-
cc:authorisation:listPermissions	授予查询被授权的虚拟私有云列表权限。	List	-	-	-
cc:crossBorderConsent:show	授予查询明示同意跨境转移个人数据的权限。	Read	-	-	-
cc:crossBorderConsent:create	授予允许用户明示同意跨境转移个人数据	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	的权限。				
cc:quota:list	授予查询配额列表权限。	List	-	-	-
cc:capability:list	授予查询云连接、中心网络和分支网络能力列表权限。	List	-	-	-
cc:centralNetwork:create	授予创建中心网络权限。	Write	centralNetwork *	-	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys • cc:MultipleEnterpriseRouterIds	
cc:centralNetwork:delete	授予删除中心网络权限。	Write	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cc:centralNetwork:update	授予更新中心网络权限。	Write	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
cc:centralNetwork:get	授予查询中心网络详情权限。	Read	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cc:centralNetwork:list	授予查询中心网络列表权	List	centralNetwork *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
cc:centralNetwork:tag	授予为中心网络添加标签权限。	Tagging	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
cc:centralNetwork:unTag	授予删除中心网络标签权限。	Tagging	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
cc:centralNetwork:listTags	授予查询中心网络标签权限。	List	centralNetwork *	-	-
cc:centralNetwork:createPolicy	授予创建中心网络策略权限。	Write	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	cc:MultipleEnterpriseRouterIds	
cc:centralNetwork:applyPolicy	授予应用中心网络策略权限。	Write	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cc:centralNetwork:deletePolicy	授予删除中心网络策略权限。	Write	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cc:centralNetw	授予查询中心	List	centralNetwo	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ork:listPolicies	网络策略列表权限。		rk *		
cc:centralNetwork:listChangeSet	授予查询当前策略与被应用策略变化集权限。	List	centralNetwork *	-	-
cc:centralNetwork:listConnections	授予查询中心网络连接列表权限。	List	centralNetwork *	-	-
cc:centralNetwork:updateConnection	授予更新中心网络连接权限。	Write	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	cc:GlobalConnectionBandwidthId	
cc:centralNetworkAttachment:createGdgw	授予创建中心网络 GDGW 附件权限。	Write	centralNetworkAttachment *	-	-
			centralNetwork *	g:ResourceTag/<tag-key>	
			-	• g:EnterpriseProjectId • cc:EnterpriseRouterId • cc:GlobalDcGatewayId	
cc:centralNetworkAttachment:updateGdgw	授予更新中心网络 GDGW 附件权限。	Write	centralNetworkAttachment *	• cc:GlobalDcGatewayId • cc:EnterpriseRouterId	-
			centralNetwork *	g:ResourceTag/<tag-key>	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	g:EnterpriseProjectId	
cc:centralNetworkAttachment:getGdgw	授予查询中心网络 GDGW 附件详情权限。	Read	centralNetworkAttachment *	• cc:GlobalDcGatewayId • cc:EnterpriseRouterId	-
			centralNetwork *	g:ResourceTag/<tag-key>	
			-	g:EnterpriseProjectId	
cc:centralNetworkAttachment:listGdgws	授予查询中心网络 GDGW 附件列表权限。	List	centralNetworkAttachment *	-	-
			centralNetwork *	g:ResourceTag/<tag-key>	
			-	g:EnterpriseProjectId	
cc:centralNetworkAttachment:createErRouteTable	授予创建中心网络 er-route-table 附件权限。	Write	centralNetworkAttachment *	-	-
			centralNetwork *	g:ResourceTag/<tag-key>	
			-	• g:EnterpriseProjectId • cc:MultipleEnterpriseRouterIds	
cc:centralNetworkAttachment:updateErRouteTable	授予更新中心网络 er-route-table 附件权限。	Write	centralNetworkAttachment *	cc:MultipleEnterpriseRouterIds	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			centralNetwork *	g:ResourceTag/<tag-key>	
			-	g:EnterpriseProjectId	
cc:centralNetworkAttachment:getErRouteTable	授予查询中心网络 er-route-table 附件详情权限。	Read	centralNetworkAttachment *	cc:MultipleEnterpriseRouterIds	-
			centralNetwork *	g:ResourceTag/<tag-key>	
			-	g:EnterpriseProjectId	
cc:centralNetworkAttachment:listErRouteTables	授予查询中心网络 er-route-table 附件列表权限。	List	centralNetworkAttachment *	-	-
			centralNetwork *	g:ResourceTag/<tag-key>	
			-	g:EnterpriseProjectId	
cc:centralNetworkAttachment:delete	授予删除中心网络附件权限。	Write	centralNetworkAttachment *	• cc:GlobalDcGatewayId • cc:EnterpriseRouterId • cc:MultipleEnterpriseRouterIds	-
			centralNetwork *	g:ResourceTag/<tag-key>	
			-	g:EnterpriseProjectId	
cc:centralNetworkAttachment:	授予查询中心网络附件列表	List	centralNetworkAtta	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
list	权限。		chment *		
			centralNetwork *	g:ResourceTag/<tag-key>	
			-	g:EnterpriseProjectId	
cc:siteNetwork:createP2P	授予创建 P2P 类型的分支网络权限。	Write	siteNetwork *	-	-
cc:siteNetwork:list	授予查询分支网络列表权限。	List	siteNetwork *	-	-
cc:siteNetwork:get	授予查询分支网络详情权限。	Read	siteNetwork *	-	-
cc:siteNetwork:update	授予更新分支网络权限。	Write	siteNetwork *	-	-
cc:siteNetwork:delete	授予删除分支网络权限。	Write	siteNetwork *	-	-
cc:siteNetwork:disassociateBandwidth	授予解关联分支网络带宽权限。	Write	siteNetwork *	-	-
cc:siteNetwork:associateBandwidth	授予关联分支网络带宽权限。	Write	siteNetwork *	-	-
cc:siteNetwork:updateBandwidthSize	授予更新分支网络带宽大小权限。	Write	siteNetwork *	-	-
cc:siteNetwork:updateBandwidth	授予更新分支网络带宽权限。	Write	siteNetwork *	-	-
cc:gcbandwidth:list	授予查询骨干带宽列表的权	List	gcbandwidth *	-	cc:gcbandwidths:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。		-	g:EnterpriseProjectId	
cc:gcbandwidth:get	授予查询骨干带宽详情的权限。	Read	gcbandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	cc:gcbandwidths:get
cc:gcbandwidth:create	授予创建骨干带宽的权限。	Write	gcbandwidth *	-	cc:gcbandwidths:create
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
cc:gcbandwidth:update	授予更新骨干带宽的权限。	Write	gcbandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	cc:gcbandwidths:update
cc:gcbandwidth:delete	授予删除骨干带宽的权限。	Write	gcbandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	cc:gcbandwidths:delete
cc:gcbandwidth:getRelations	授予查询骨干带宽绑定关系的权限。	Read	gcbandwidth *	g:EnterpriseProjectId	cc:gcbandwidths:get
cc:gcbandwidth:associateInstance	授予实例绑定骨干带宽的权限。	Write	gcbandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	cc:gcbandwidths:update
			-	cc:gcbAssociateResourceType	
cc:gcbandwidth:disassociateInstance	授予取消实例绑定骨干带宽的权限。	Write	gcbandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-	cc:gcbandwidths:update

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				key> • cc:gcbAssociateResourceType	
cc:gcbandwidth:listSupportBinding	授予查询支持绑定的骨干带宽的权限。	List	gcbandwidth *	-	cc:gcbandwidths:list
			-	g:EnterpriseProjectId	
cc:gcbandwidth:listTags	授予查询骨干带宽资源标签权限。	List	gcbandwidth *	-	cc:gcbandwidths:listByTag
cc:gcbandwidth:tag	授予创建骨干带宽资源标签权限。	Tagging	gcbandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	cc:gcbandwidths:createTags
			-	• g:RequestTag/<tag-key> • g:TagKeys	
cc:gcbandwidth:unTag	授予删除骨干带宽资源标签权限。	Tagging	gcbandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	cc:gcbandwidths:deleteTags
			-	g:TagKeys	

CC 的 API 通常对应着一个或多个授权项。表 3-68 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-68 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v3/{domain_id}/ccaas/cloud-connections	cc:cloudConnections:create	-
PUT /v3/{domain_id}/ccaas	cc:cloudConnections:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/cloud-connections/{id}		
DELETE /v3/{domain_id}/ccaas/cloud-connections/{id}	cc:cloudConnections:delete	-
GET /v3/{domain_id}/ccaas/cloud-connections/{id}	cc:cloudConnections:get	-
GET /v3/{domain_id}/ccaas/cloud-connections	cc:cloudConnections:list	-
POST /v3/{domain_id}/ccaas/cloud-connections/filter	cc:cloudConnections:list	-
POST /v3/{domain_id}/ccaas/cloud-connections/{id}/tag	cc:cloudConnections:tag	-
POST /v3/{domain_id}/ccaas/cloud-connections/{id}/untag	cc:cloudConnections:unTag	-
GET /v3/{domain_id}/ccaas/cloud-connections/tags	cc:cloudConnections:listTags	-
POST /v3/{domain_id}/ccaas/network-instances	cc:networkInstances:create	-
PUT /v3/{domain_id}/ccaas/network-instances/{id}	cc:networkInstances:update	-
DELETE /v3/{domain_id}/ccaas/network-instances/{id}	cc:networkInstances:delete	-
GET /v3/{domain_id}/ccaas/network-instances/{id}	cc:networkInstances:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v3/{domain_id}/ccaas/network-instances	cc:networkInstances:list	-
POST /v3/{domain_id}/ccaas/bandwidth-packages	cc:bandwidthPackages:create	-
PUT /v3/{domain_id}/ccaas/bandwidth-packages/{id}	cc:bandwidthPackages:update	-
DELETE /v3/{domain_id}/ccaas/bandwidth-packages/{id}	cc:bandwidthPackages:delete	-
GET /v3/{domain_id}/ccaas/bandwidth-packages/{id}	cc:bandwidthPackages:get	-
GET /v3/{domain_id}/ccaas/bandwidth-packages	cc:bandwidthPackages:list	-
POST /v3/{domain_id}/ccaas/bandwidth-packages/filter	cc:bandwidthPackages:list	-
POST /v3/{domain_id}/ccaas/bandwidth-packages/{id}/tag	cc:bandwidthPackages:tag	-
POST /v3/{domain_id}/ccaas/bandwidth-packages/{id}/untag	cc:bandwidthPackages:unTag	-
GET /v3/{domain_id}/ccaas/bandwidth-packages/tags	cc:bandwidthPackages:listTags	-
POST /v3/{domain_id}/ccaas/bandwidth-packages/{id}/associate	cc:bandwidthPackages:associate	-
POST /v3/{domain_id}/ccaas/bandwidth-	cc:bandwidthPackages:disassociate	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
packages/{id}/disassociate		
POST /v3/{domain_id}/ccaas/inter-region-bandwidths	cc:interRegionBandwidths:create	-
PUT /v3/{domain_id}/ccaas/inter-region-bandwidths/{id}	cc:interRegionBandwidths:update	-
DELETE /v3/{domain_id}/ccaas/inter-region-bandwidths/{id}	cc:interRegionBandwidths:delete	-
GET /v3/{domain_id}/ccaas/inter-region-bandwidths/{id}	cc:interRegionBandwidths:get	-
GET /v3/{domain_id}/ccaas/inter-region-bandwidths	cc:interRegionBandwidths:list	-
GET /v3/{domain_id}/ccaas/cloud-connection-routes/{id}	cc:cloudConnectionRoutes:get	-
GET /v3/{domain_id}/ccaas/cloud-connection-routes	cc:cloudConnectionRoutes:list	-
POST /v3/{domain_id}/ccaas/authorisations	cc:authorisation:create	-
DELETE /v3/{domain_id}/ccaas/authorisations/{id}	cc:authorisation:delete	-
PUT /v3/{domain_id}/ccaas/authorisations/{id}	cc:authorisation:update	-
GET /v3/{domain_id}/ccaas/authorisations	cc:authorisation:list	-
GET /v3/{domain_id}/ccaas	cc:authorisation:listPermissions	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/permissions		
GET /v3/{domain_id}/ccaas/quotas	cc:quota:list	-
GET /v3/{domain_id}/gcn/quotas	cc:quota:list	-
GET /v3/{domain_id}/ccaas/capabilities	cc:capability:list	-
GET /v3/{domain_id}/gcn/capabilities	cc:capability:list	-
POST /v3/{domain_id}/gcn/central-networks	cc:centralNetwork:create	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
DELETE /v3/{domain_id}/gcn/central-networks/{central_network_id}	cc:centralNetwork:delete	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
PUT /v3/{domain_id}/gcn/central-networks/{central_network_id}	cc:centralNetwork:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v3/{domain_id}/gcn/central-networks/{central_network_id}	cc:centralNetwork:get	-
GET /v3/{domain_id}/gcn/central-networks	cc:centralNetwork:list	-
POST /v3/{domain_id}/gcn/central-networks/filter	cc:centralNetwork:list	-
POST /v3/{domain_id}/gcn/central-networks/{central_network_id}/tag	cc:centralNetwork:tag	-
POST /v3/{domain_id}/gcn/central-networks/{central_network_id}/untag	cc:centralNetwork:unTag	-
GET /v3/{domain_id}/gcn/central-networks/tags	cc:centralNetwork:listTags	-
POST /v3/{domain_id}/gcn/central-network/{central_network_id}/policies	cc:centralNetwork:createPolicy	• er:instances:get • er:routeTables:get
POST /v3/{domain_id}/gcn/central-network/{central_network_id}/policies/{policy_id}/apply	cc:centralNetwork:applyPolicy	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
DELETE /v3/{domain_id}/gcn/central-network/{central_netw	cc:centralNetwork:deletePolicy	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ork_id}/policies/{policy_id}		
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/policies	cc:centralNetwork:listPolicies	-
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/policies/{policy_id}/change-set	cc:centralNetwork:listChangeSet	-
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/connections	cc:centralNetwork:listConnections	-
PUT /v3/{domain_id}/gcn/central-network/{central_network_id}/connections/{connection_id}	cc:centralNetwork:updateConnection	-
POST /v3/{domain_id}/gcn/central-network/{central_network_id}/gdgw-attachments	cc:centralNetworkAttachment:createGdgw	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
PUT /v3/{domain_id}/gcn/central-network/{central_network_id}/gdgw-attachments/{gdgw_attachment_id}	cc:centralNetworkAttachment:updateGdgw	-
GET /v3/{domain_id}/gcn/central-	cc:centralNetworkAttachment:getGdgw	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
network/{central_network_id}/gdgw-attachments/{gdgw_attachment_id}		
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/gdgw-attachments	cc:centralNetworkAttachment:listGdgws	-
POST /v3/{domain_id}/gcn/central-network/{central_network_id}/er-route-table-attachments	cc:centralNetworkAttachment:createErRouteTable	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
PUT /v3/{domain_id}/gcn/central-network/{central_network_id}/er-route-table-attachments/{er_route_table_attachment_id}	cc:centralNetworkAttachment:updateErRouteTable	-
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/er-route-table-attachments/{er_route_table_attachment_id}	cc:centralNetworkAttachment:getErRouteTable	-
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/er-route-table-attachments	cc:centralNetworkAttachment:listErRouteTables	-
DELETE /v3/{domain_id}/gcn/central-network/{central_network_id}/attachments/{	cc:centralNetworkAttachment:delete	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
attachment_id}		• er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/attachments	cc:centralNetworkAttachment:list	-
GET /v3/{domain_id}/ccaas/domain-cross-border-consents	cc:crossBorderConsent:show	-
POST /v3/{domain_id}/ccaas/domain-cross-border-consents	cc:crossBorderConsent:create	-
POST /v3/{domain_id}/dcaas/p2p-site-networks	cc:siteNetwork:createP2P	-
GET /v3/{domain_id}/dcaas/site-networks	cc:siteNetwork:list	-
GET /v3/{domain_id}/dcaas/site-networks/{site_network_id}	cc:siteNetwork:get	-
PUT /v3/{domain_id}/dcaas/site-networks/{site_network_id}	cc:siteNetwork:update	-
DELETE /v3/{domain_id}/dcaas/site-networks/{site_network_id}	cc:siteNetwork:delete	-
POST /v3/{domain_id}/dcaas/site-	cc:siteNetwork:disassociateBandwidth	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
network/{site_network_id}/connections/{site_connection_id}/disassociate		
POST /v3/{domain_id}/dcaas/site-network/{site_network_id}/connections/{site_connection_id}/associate	cc:siteNetwork:associateBandwidth	-
POST /v3/{domain_id}/dcaas/site-network/{site_network_id}/connections/{site_connection_id}/update-bandwidth-size	cc:siteNetwork:updateBandwidthSize	-
POST /v3/{domain_id}/dcaas/site-network/{site_network_id}/connections/{site_connection_id}/update-bandwidth	cc:siteNetwork:updateBandwidth	-
GET /v3/{domain_id}/dcaas/site-network/capabilities	cc:capability:list	-
GET /v3/{domain_id}/dcaas/site-network/quotas	cc:quota:list	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-69 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

CC 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-69 CC 支持的资源类型

资源类型	URN
cloudConnection	cc::<account-id>:cloudConnection:<cloud-connection-id>

 版权所有 © 华为云计算技术有限公司

资源类型	URN
gcbandwidth	cc::<account-id>:gcbandwidth:<gcbandwidth-id>
interRegionBandwidth	cc::<account-id>:interRegionBandwidth:<inter-region-bandwidth-id>
networkInstance	cc::<account-id>:networkInstance:<network-instance-id>
siteNetwork	cc::<account-id>:siteNetwork:<site-network-id>
bandwidthPackage	cc::<account-id>:bandwidthPackage:<bandwidth-package-id>
centralNetwork	cc::<account-id>:centralNetwork:<central-network-id>
centralNetworkAttachment	cc::<account-id>:centralNetworkAttachment:<central-network-attachment-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 cc:）仅适用于对应服务的操作，详情请参见表 3-70。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

CC 支持的服务级条件键

CC 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-70 CC 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
cc:VpcId	string	单值	根据指定的虚拟私有云资源 ID 过滤访问。

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
cc:VirtualGatewayId	string	单值	根据指定的专线虚拟网络资源 ID 过滤访问。
cc:EnterpriseRouterId	string	单值	根据指定的企业路由器资源 ID 过滤访问。
cc:MultipleEnterpriseRouterIds	string	多值	根据指定的多个企业路由器资源 ID 过滤访问。
cc:BandwidthPackageId	string	单值	根据指定的带宽包资源 ID 过滤访问。
cc:GlobalConnectionBandwidthId	string	单值	根据指定的全域互联带宽资源 ID 过滤访问。
cc:GlobalDcGatewayId	string	单值	根据指定的全球接入网关资源 ID 过滤访问。
cc:gcbAssociateResourceType	string	单值	根据绑定的全球互联带宽资源资源类型过滤访问。

条件键示例

- cc:VpcId

  示例：根据指定的虚拟私有云资源 ID 过滤访问网络实例的权限。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:networkInstances:create",
        "cc:networkInstances:delete",
        "cc:networkInstances:update"
      ],
      "Condition": {
        "StringEquals": {
          "cc:VpcId": [
            "xxx"
          ]
        }
      }
    }
  ]
}
```

- cc:VirtualGatewayId

  示例：根据指定的专线虚拟网络资源 ID 过滤访问网络实例的权限。

 版权所有 © 华为云计算技术有限公司

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:networkInstances:create",
        "cc:networkInstances:delete",
        "cc:networkInstances:update"
      ],
      "Condition": {
        "StringEquals": {
          "cc:VirtualGatewayId": [
            "xxx"
          ]
        }
      }
    }
  ]
}
```

- cc:EnterpriseRouterId

  示例：根据指定的企业路由器资源 ID 过滤访问中心网络全球接入网关附件的权限。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:centralNetworkAttachment:createGdgw",
        "cc:centralNetworkAttachment:updateGdgw",
        "cc:centralNetworkAttachment:getGdgw",
        "cc:centralNetworkAttachment:delete"
      ],
      "Condition": {
        "StringEquals": {
          "cc:EnterpriseRouterId": [
            "xxx"
          ]
        }
      }
    }
  ]
}
```

- cc:MultipleEnterpriseRouterIds

  示例：根据指定的多个企业路由器资源 ID 过滤访问中心网络及中心网络路由表附件的权限。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:centralNetwork:create",
```

 版权所有 © 华为云计算技术有限公司

```
      "cc:centralNetwork:createPolicy",
      "cc:centralNetworkAttachment:createErRouteTable",
      "cc:centralNetworkAttachment:updateErRouteTable",
      "cc:centralNetworkAttachment:getErRouteTable",
      "cc:centralNetworkAttachment:delete"
    ],
    "Condition": {
      "StringEquals": {
        "cc:MultipleEnterpriseRouterIds": [
          "xxx"
        ]
      }
    }
  }
 ]
}
```

- cc:BandwidthPackageId

  示例：根据指定的带宽包资源 ID 过滤访问域间带宽实例的权限。

```
{
 "Version": "5.0",
 "Statement": [
   {
    "Effect": "Allow",
    "Action": [
      "cc:interRegionBandwidths:create",
      "cc:interRegionBandwidths:delete",
      "cc:interRegionBandwidths:update"
    ],
    "Condition": {
      "StringEquals": {
        "cc:BandwidthPackageId": [
          "xxx"
        ]
      }
    }
   }
 ]
}
```

- cc:GlobalConnectionBandwidthId

  示例：根据指定的全域互联带宽资源 ID 过滤访问更新中心网络连接的权限。

```
{
 "Version": "5.0",
 "Statement": [
   {
    "Effect": "Allow",
    "Action": [
      "cc:centralNetwork:updateConnection"
    ],
    "Condition": {
      "StringEquals": {
        "cc:GlobalConnectionBandwidthId": [
          "xxx"
        ]
```

 版权所有 © 华为云计算技术有限公司

```
        }
      }
    }
  ]
}
```

- cc:GlobalDcGatewayId

  示例：根据指定的全球接入网关资源 ID 过滤访问中心网络全球接入网关附件的权限。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:centralNetworkAttachment:createGdgw",
        "cc:centralNetworkAttachment:updateGdgw",
        "cc:centralNetworkAttachment:getGdgw",
        "cc:centralNetworkAttachment:delete"
      ],
      "Condition": {
        "StringEquals": {
          "cc:GlobalDcGatewayId": [
            "xxx"
          ]
        }
      }
    }
  ]
}
```

- cc:gcbAssociateResourceType

  示例：根据全球互联带宽资源资源类型过滤访问资源绑定或解绑骨干带宽的权限。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:gcbandwidth:associateInstance",
        "cc:gcbandwidth:disassociateInstance",
      ],
      "Condition": {
        "StringEquals": {
          "cc:gcbAssociateResourceType": [
            "xxx"
          ]
        }
      }
    }
  ]
}
```

 版权所有 © 华为云计算技术有限公司

3.3.9 弹性负载均衡 ELB

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 ELB 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 ELB 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 ELB 的相关操作。

 版权所有 © 华为云计算技术有限公司

表3-71 ELB 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
elb:flavors:show	授予查询指定规格的详情。	Read	flavor *	-	elb:flavors:get
elb:flavors:list	授予查询规格详情列表的权限。	List	flavor *	-	-
elb:quotas:list	授予查询配额列表的权限。	List	-	-	-
elb:quotas:show	授予查询可以创建指定类型资源的最大数量的权限。	Read	-	-	elb:quotas:get
elb:availability-zones:list	授予查询可用区列表的权限。	List	availabilityZone *	-	-
			-	g:EnterpriseProjectId	
elb:loadbalancers:list	授予查询负载均衡器实例列表。	List	loadbalancer *	-	-
			-	g:EnterpriseProjectId	
elb:loadbalancers:show	授予获取负载均衡器实例详情的权限。	Read	loadbalancer *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	elb:loadbalancers:get
elb:loadbalancers:create	授予创建负载均衡器实例的权限。	Write	loadbalancer *	-	-
			subnet	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • elb:Associat	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ePublicips	
elb:loadbalancers:update	授予更新负载均衡器实例的权限。	Write	subnet	-	elb:loadbalancers:put
			loadbalancer *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
			-	elb:AssociatePublicips	
elb:loadbalancers:delete	授予删除负载均衡器实例的权限。	Write	loadbalancer *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
elb:listeners:create	授予创建监听器的权限。	Write	listener *	g:EnterpriseProjectId	-
			loadbalancer *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
elb:listeners:update	授予修改监听器的权限。	Write	listener *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • elb:UpdateListenerIpgroup • elb:OnlyUpdateListenerIpgroup	elb:listeners:put
elb:listeners:list	授予查询监听器列表的权限。	List	listener *	-	-
			-	g:EnterpriseProjectId	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
elb:listeners:show	授予获取监听器详情的权限。	Read	listener *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	elb:listeners:get
elb:listeners:delete	授予删除监听器的权限。	Write	listener *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
elb:certificates:list	授予查询证书列表的权限。	List	certificate *	-	-
			-	g:EnterpriseProjectId	
elb:certificates:show	授予获取证书详情的权限。	Read	certificate *	-	elb:certificates:get
elb:certificates:create	授予创建证书的权限。	Write	certificate *	-	-
			-	g:EnterpriseProjectId	
elb:certificates:update	授予修改证书的权限。	Write	certificate *	-	elb:certificates:put
elb:certificates:delete	授予删除证书的权限。	Write	certificate *	-	-
elb:certificates:setPrivateKeyEcho	授予设置证书私钥回显开关的权限。	Write	-	-	-
elb:certificates:getPrivateKeyEcho	授予查询证书私钥回显开关的权限。	Write	-	-	-
elb:healthmonitors:create	授予创建健康检查的权限。	Write	healthmonitor *	g:EnterpriseProjectId	-
			pool *	g:EnterpriseProjectId	
elb:healthmonit	授予修改健康	Write	healthmonit	g:EnterprisePro	elb:healthmonit

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ors:update	检查的权限。		or *	jectId	ors:put
elb:healthmonitors:delete	授予删除健康检查的权限。	Write	healthmonitor *	g:EnterpriseProjectId	-
elb:healthmonitors:show	授予获取健康检查详情的权限。	Read	healthmonitor *	g:EnterpriseProjectId	elb:healthmonitors:get
elb:healthmonitors:list	授予查询健康检查列表的权限。	List	healthmonitor *	-	-
			-	g:EnterpriseProjectId	
elb:ipgroups:list	授予查询 IP 地址组列表的权限。	List	ipgroup *	-	-
			-	g:EnterpriseProjectId	
elb:ipgroups:show	授予获取 IP 地址组详情的权限。	Read	ipgroup *	-	elb:ipgroups:get
elb:ipgroups:create	授予创建 IP 地址组的权限。	Write	ipgroup *	-	-
			-	g:EnterpriseProjectId	
elb:ipgroups:update	授予修改 IP 地址组的权限。	Write	ipgroup *	-	elb:ipgroups:put
elb:ipgroups:delete	授予删除 IP 地址组的权限。	Write	ipgroup *	-	-
elb:ipgroups:showRelatedListeners	授予获取 IP 地址组关联的监听器的权限。	Read	ipgroup *	-	elb:ipgroups:related-listeners
elb:l7policies:create	授予创建 7 层转发策略的权限。	Write	listener *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			l7poli	g:EnterprisePro	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			cy *	jectId	
			pool	g:EnterpriseProjectId	
elb:l7policies:update	授予修改 7 层转发策略的权限。	Write	l7policy *	g:EnterpriseProjectId	elb:l7policies:put
			listener	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			pool	g:EnterpriseProjectId	
elb:l7policies:delete	授予删除 7 层转发策略的权限。	Write	l7policy *	g:EnterpriseProjectId	-
elb:l7policies:show	授予获取转发策略详情的权限。	Read	l7policy *	g:EnterpriseProjectId	elb:l7policies:get
elb:l7policies:list	授予查询转发策略的权限。	List	l7policy *	-	-
			-	g:EnterpriseProjectId	
elb:l7rules:create	授予创建 7 层转发规则的权限。	Write	l7rule *	g:EnterpriseProjectId	-
			l7policy *	g:EnterpriseProjectId	
elb:l7rules:update	授予修改 7 层转发规则的权限。	Write	l7rule *	g:EnterpriseProjectId	elb:l7rules:put
elb:l7rules:list	授予查询转发规则的权限。	List	l7policy *	-	-
			l7rule *	-	
			-	g:EnterpriseProjectId	
elb:l7rules:sho	授予获取 7 层	Read	l7rule	g:EnterprisePro	elb:l7rules:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
w	转发规则详情的权限。		*	jectId	
elb:l7rules:delete	授予删除 7 层转发规则的权限。	Write	l7rule *	g:EnterpriseProjectId	-
elb:logtanks:list	授予查询云日志列表的权限。	List	logtank *	-	-
			-	g:EnterpriseProjectId	
elb:logtanks:show	授予获取云日志详情的权限。	Read	logtank *	g:EnterpriseProjectId	elb:logtanks:get
elb:logtanks:create	授予创建云日志的权限。	Write	logtank *	g:EnterpriseProjectId	-
			loadbalancer *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
elb:logtanks:update	授予修改云日志的权限。	Write	logtank *	g:EnterpriseProjectId	elb:logtanks:put
elb:logtanks:delete	授予删除云日志的权限。	Write	logtank *	g:EnterpriseProjectId	-
elb:pools:list	授予查询后端服务器组列表的权限。	List	pool *	-	-
			-	g:EnterpriseProjectId	
elb:pools:show	授予获取后端服务器组详情的权限。	Read	pool *	g:EnterpriseProjectId	elb:pools:get
elb:pools:create	授予创建后端服务器组的权限。	Write	loadbalancer	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			listener	• g:EnterpriseProjectId	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:ResourceTag/<tag-key>	
			pool *	g:EnterpriseProjectId	
elb:pools:update	授予修改后端服务器组的权限。	Write	pool *	g:EnterpriseProjectId	elb:pools:put
elb:pools:delete	授予删除后端服务器组的权限。	Write	pool *	g:EnterpriseProjectId	-
elb:members:list	授予查询后端服务器列表的权限。	List	pool	-	-
			member *	-	
			-	g:EnterpriseProjectId	
elb:members:show	授予获取后端服务器详情的权限。	Read	member *	g:EnterpriseProjectId	elb:members:get
elb:members:create	授予创建后端服务器的权限。	Write	member *	g:EnterpriseProjectId	-
			pool *	g:EnterpriseProjectId	
			subnet	-	
elb:members:update	授予修改后端服务器的权限。	Write	member *	g:EnterpriseProjectId	elb:members:put
elb:members:delete	授予删除后端服务器的权限。	Write	member *	g:EnterpriseProjectId	-
elb:security-policies:list	授予查询安全策略的权限。	List	securityPolicy *	-	-
			-	g:EnterpriseProjectId	
elb:security-	授予获取安全	Read	securit	-	elb:security-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
policies:show	策略详情的权限。		yPolicy *		policies:get
elb:security-policies:create	授予创建安全策略的权限。	Write	securityPolicy *	-	-
			-	g:EnterpriseProjectId	
elb:security-policies:update	授予修改安全策略的权限。	Write	securityPolicy *	-	elb:security-policies:put
elb:security-policies:delete	授予删除安全策略的权限。	Write	securityPolicy *	-	-
elb:loadbalancers:export	授予导出负载均衡器的权限。	Read	loadbalancer *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
elb:listeners:export	授予导出监听器的权限。	Read	listener *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

ELB 的 API 通常对应着一个或多个授权项。表 3-72 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-72 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/elb/flavors	elb:flavors:list	-
GET /v3/{project_id}/elb/flavors/{flavor_id}	elb:flavors:show	-
GET /v3/{project_id}/elb/quotas/details	elb:quotas:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/elb/quotas	elb:quotas:show	-
POST /v3/{project_id}/elb/loadbalancers	elb:loadbalancers:create	-
DELETE /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}	elb:loadbalancers:delete	-
DELETE /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/force-elb	elb:loadbalancers:delete	-
GET /v3/{project_id}/elb/loadbalancers	elb:loadbalancers:list	-
GET /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}	elb:loadbalancers:show	-
GET /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/statuses	elb:loadbalancers:show	-
PUT /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}	elb:loadbalancers:update	-
POST /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/availability-zone/batch-remove	elb:loadbalancers:update	-
POST /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/availability-zone/batch-add	elb:loadbalancers:update	-
POST /v3/{project_id}/elb/loadbalancers/change-charge-mode	elb:loadbalancers:create	-
POST /v3/{project_id}/elb/ip	elb:ipgroups:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
groups		
DELETE /v3/{project_id}/elb/ipgroups/{ipgroup_id}	elb:ipgroups:delete	-
GET /v3/{project_id}/elb/ipgroups	elb:ipgroups:list	-
GET /v3/{project_id}/elb/ipgroups/{ipgroup_id}	elb:ipgroups:show	-
PUT /v3/{project_id}/elb/ipgroups/{ipgroup_id}	elb:ipgroups:update	-
POST /v3/{project_id}/elb/ipgroups/{ipgroup_id}/iplist/create-or-update	elb:ipgroups:update	-
POST /v3/{project_id}/elb/ipgroups/{ipgroup_id}/iplist/batch-delete	elb:ipgroups:update	-
GET /v3/{project_id}/elb/ipgroups/{ipgroup_id}/related-listeners	elb:ipgroups:showRelatedListeners	-
POST /v3/{project_id}/elb/security-policies	elb:security-policies:create	-
DELETE /v3/{project_id}/elb/security-policies/{security_policy_id}	elb:security-policies:delete	-
GET /v3/{project_id}/elb/security-policies	elb:security-policies:list	-
GET /v3/{project_id}/elb/system-security-policies	elb:security-policies:list	-
GET /v3/{project_id}/elb/security-policies/{security_policy_id}	elb:security-policies:show	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v3/{project_id}/elb/security-policies/{security_policy_id}	elb:security-policies:update	-
POST /v3/{project_id}/elb/pools/{pool_id}/members	elb:members:create	-
DELETE /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}	elb:members:delete	-
GET /v3/{project_id}/elb/pools/{pool_id}/members	elb:members:list	-
GET /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}	elb:members:show	-
PUT /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}	elb:members:update	-
POST /v3/{project_id}/elb/pools/{pool_id}/members/batch-update	elb:members:update	-
GET /v3/{project_id}/elb/members	elb:members:list	-
POST /v3/{project_id}/elb/pools/{pool_id}/members/batch-add	elb:members:create	-
POST /v3/{project_id}/elb/pools/{pool_id}/members/batch-delete	elb:members:delete	-
POST /v3/{project_id}/elb/pools	elb:pools:create	-
DELETE /v3/{project_id}/elb/p	elb:pools:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ools/{pool_id}		
GET /v3/{project_id}/elb/pools	elb:pools:list	-
GET /v3/{project_id}/elb/pools/{pool_id}	elb:pools:show	-
PUT /v3/{project_id}/elb/pools/{pool_id}	elb:pools:update	-
POST /v3/{project_id}/elb/master-slave-pools	elb:pools:create	-
GET /v3/{project_id}/elb/master-slave-pools	elb:pools:list	-
GET /v3/{project_id}/elb/master-slave-pools/{pool_id}	elb:pools:show	-
DELETE /v3/{project_id}/elb/master-slave-pools/{pool_id}	elb:pools:delete	-
POST /v3/{project_id}/elb/listeners	elb:listeners:create	-
DELETE /v3/{project_id}/elb/listeners/{listener_id}	elb:listeners:delete	-
DELETE /v3/{project_id}/elb/listeners/{listener_id}/force	elb:listeners:delete	-
GET /v3/{project_id}/elb/listeners	elb:listeners:list	-
GET /v3/{project_id}/elb/listeners/{listener_id}	elb:listeners:show	-
PUT /v3/{project_id}/elb/listeners/{listener_id}	elb:listeners:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/elb/healthmonitors	elb:healthmonitors:create	-
DELETE /v3/{project_id}/elb/healthmonitors/{healthmonitor_id}	elb:healthmonitors:delete	-
GET /v3/{project_id}/elb/healthmonitors	elb:healthmonitors:list	-
GET /v3/{project_id}/elb/healthmonitors/{healthmonitor_id}	elb:healthmonitors:show	-
PUT /v3/{project_id}/elb/healthmonitors/{healthmonitor_id}	elb:healthmonitors:update	-
GET /v3/{project_id}/elb/availability-zones	elb:availability-zones:list	-
GET /v3/{project_id}/elb/preoccupy-ip-num	elb:loadbalancers:show	-
POST /v3/{project_id}/elb/logtanks	elb:logtanks:create	-
DELETE /v3/{project_id}/elb/logtanks/{logtank_id}	elb:logtanks:delete	-
GET /v3/{project_id}/elb/logtanks	elb:logtanks:list	-
GET /v3/{project_id}/elb/logtanks/{logtank_id}	elb:logtanks:show	-
PUT /v3/{project_id}/elb/logtanks/{logtank_id}	elb:logtanks:update	-
POST /v3/{project_id}/elb/certificates	elb:certificates:create	-
DELETE	elb:certificates:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v3/{project_id}/elb/certificates/{certificate_id}		
GET /v3/{project_id}/elb/certificates	elb:certificates:list	-
GET /v3/{project_id}/elb/certificates/{certificate_id}	elb:certificates:show	-
PUT /v3/{project_id}/elb/certificates/{certificate_id}	elb:certificates:update	-
POST /v3/{project_id}/elb/certificates/settings/private-key-echo	elb:certificates:setPrivateKeyEcho	-
GET /v3/{project_id}/elb/certificates/settings/private-key-echo	elb:certificates:getPrivateKeyEcho	-
POST /v3/{project_id}/elb/l7policies	elb:l7policies:create	-
DELETE /v3/{project_id}/elb/l7policies/{l7policy_id}	elb:l7policies:delete	-
GET /v3/{project_id}/elb/l7policies	elb:l7policies:list	-
GET /v3/{project_id}/elb/l7policies/{l7policy_id}	elb:l7policies:show	-
PUT /v3/{project_id}/elb/l7policies/{l7policy_id}	elb:l7policies:update	-
POST /v3/{project_id}/elb/l7policies/batch-update-priority	elb:l7policies:update	-
POST /v3/{project_id}/elb/l7policies/{l7policy_id}/	elb:l7rules:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
rules		
DELETE /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}	elb:l7rules:delete	-
GET /v3/{project_id}/elb/l7policies/{l7policy_id}/rules	elb:l7rules:list	-
GET /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}	elb:l7rules:show	-
PUT /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}	elb:l7rules:update	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-73 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

ELB 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-73 ELB 支持的资源类型

资源类型	URN
pool	elb:<region>:<account-id>:pool:<pool-id>
loadbalancer	elb:<region>:<account-id>:loadbalancer:<loadbalancer-id>
certificate	elb:<region>:<account-id>:certificate:<certificate-id>
healthmonitor	elb:<region>:<account-id>:healthmonitor:<healthmonitor-id>
ipgroup	elb:<region>:<account-id>:ipgroup:<ipgroup-id>
securityPolicy	elb:<region>:<account-id>:securityPolicy:<security-policy-id>
logtank	elb:<region>:<account-id>:logtank:<logtank-id>
availabilityZone	elb:<region>:<account-id>:availabilityZone:<availability-zone-id>
member	elb:<region>:<account-id>:member:<pool-id>/<member-id>

 版权所有 © 华为云计算技术有限公司

资源类型	URN
l7policy	elb:<region>:<account-id>:l7policy:<l7policy-id>
l7rule	elb:<region>:<account-id>:l7rule:<l7policy-id>/<l7rule-id>
flavor	elb:<region>:<account-id>:flavor:<flavor-id>
subnet	vpc:<region>:<account-id>:subnet:<subnet-id>
listener	elb:<region>:<account-id>:listener:<listener-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 elb:）仅适用于对应服务的操作，详情请参见表 3-74。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

ELB 支持的服务级条件键

ELB 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-74 ELB 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
elb:AssociatePublicips	boolean	单值	根据创建或修改负载均衡器时是否涉及创建或绑定公网操作筛选访问权限。若要完全限制弹性负载均衡器的公网访问，则需要同时使用弹性公网 IP 的相关 Action 进行策略管理。

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
elb:UpdateListenerIpgroup	boolean	单值	根据修改监听器时是否涉及更新访问控制筛选访问权限。
elb:OnlyUpdateListenerIpgroup	boolean	单值	根据修改监听器时是否仅涉及更新访问控制筛选访问权限。

3.4 容器

3.4.1 云容器引擎 CCE

云服务在 IAM 预置了常用的权限，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

 版权所有 © 华为云计算技术有限公司

关于 CCE 定义的资源类型的详细信息请参见资源类型（Resource）。

- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 CCE 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 CCE 的相关操作。

表3-75 CCE 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cce:imageCache:create	授予创建镜像缓存的权限。	Write	-	-	-
cce:imageCache:delete	授予删除镜像缓存的权限。	Write	imageCache *	-	-
cce:imageCache:list	授予查看镜像缓存列表的权限。	List	-	-	-
cce:imageCache:get	授予查看用户指定镜像缓存详情的权限。	Read	imageCache *	-	-
cce:packageProduct:list	授予查看套餐包列表的权限。	List	-	-	-
cce:packageProduct:subscribe	授予订购套餐包的权限。	Write	-	-	-
cce:cluster:createCluster	授予创建集群的权限。	Write	cluster *	-	• cce:cluster:create
			-	• g:EnterpriseProjectId • g:TagKeys • g:RequestTag/<tag-key> • cce:AssociatePublicIp	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• cce:VpcId • cce:SubnetId	
cce:cluster:delete	授予删除集群的权限。	Write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cce:cluster:updateCluster	授予更新集群的权限。	Write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• cce:cluster:update
cce:cluster:upgrade	授予执行集群版本升级的权限。	Write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cce:cluster:start	授予唤醒休眠集群的权限。	Write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cce:cluster:stop	授予对集群执行休眠操作的权限。	Write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cce:cluster:list	授予查看集群详情列表的权限。	List	cluster *	-	-
cce:cluster:getCluster	授予查看用户指定集群详情的权限。	Read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• cce:cluster:get
cce:cluster:getEndpoints	授予查看用户指定集群访问地址的权限。	Read	cluster *	• g:ResourceTag/<tag-key> • g:Enterprise	• cce:cluster:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				g:EnterpriseProjectId	
cce:cluster:resize	授予对集群进行规格变更的权限。	Write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cce:cluster:toperiod	授予对集群按需转包周期的权限。	Write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cce:cluster:eipBinding	授予对集群绑定/解绑公网 IP 的权限。	Write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• cce:cluster:update
cce:cluster:generateClientCredential	授予生成集群客户端访问凭据的权限。	Read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• cce:cluster:get
cce:cluster:revokeClientCredential	授予吊销集群证书的权限。	Write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cce:cluster:rotateCredentials	授予轮转集群证书的权限。	Write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cce:cluster:addTags	授予添加集群标签的权限。	Tagging	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• cce:tag:operate
			-	• g:TagKeys • g:RequestTag/<tag-key>	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cce:cluster:removeTags	授予删除集群标签的权限。	Tagging	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• cce:tag:operate
			-	• g:TagKeys • g:RequestTag/<tag-key>	
cce:cluster:listTags	授予列举项目下所有集群标签的权限。	Read	-	-	• cce:tag:list
cce:cluster:listTagsForCluster	授予查询项目标签的权限。	Read	cluster *	g:ResourceTag/<tag-key>	• cce:cluster:get
cce:cluster:listClustersByTag	授予按标签查询集群列表的权限。	Read	-	g:TagKeys	• cce:cluster:list
cce:cluster:validate	授予对集群参数进行合法性校验的权限。	Read	cluster *	-	• cce:cluster:create
			-	• g:EnterpriseProjectId • g:TagKeys • g:RequestTag/<tag-key>	
cce:cluster:getConfigurationTemplate	授予查询集群配置模板信息的权限。	Read	cluster *	-	• cce:cluster:get
			-	• cce:ClusterId • g:EnterpriseProjectId	
cce:cluster:getConfiguration	授予查询集群当前配置的权限。	Read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	• cce:cluster:get
cce:cluster:updateConfiguration	授予更新集群配置的权限。	Write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-	• cce:cluster:update

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				key>	
cce:cluster:getLogConfig	授予查询集群当前日志采集配置的权限。	Read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cce:cluster:updateLogConfig	授予更新集群日志采集配置的权限。	Write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cce:cluster:checkLock	授予检查并释放集群上 CBC 相关锁的权限。	Write	-	-	-
cce:partition:create	授予接入分区的权限。	Write	cluster *	-	-
			-	• cce:ClusterId • g:EnterpriseProjectId	
cce:partition:update	授予更新分区的权限。	Write	cluster *	g:EnterpriseProjectId	-
cce:partition:get	授予查询指定分区详情的权限。	Read	cluster *	g:EnterpriseProjectId	-
cce:partition:list	授予查看指定集群的分区列表。	List	cluster *	-	-
			-	• cce:ClusterId • g:EnterpriseProjectId	
cce:nodepool:create	授予创建节点池的权限。	Write	cluster *	-	-
			-	• cce:ClusterId • evs:Encrypted	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:EnterpriseProjectId • cce:Subnets • cce:KmsKeys • cce:AvailableZones	
cce:nodepool:delete	授予删除节点池的权限。	Write	cluster *	g:EnterpriseProjectId	-
cce:nodepool:updateNodepool	授予更新节点池的权限。	Write	cluster *	-	• cce:nodepool:update
			-	• evs:Encrypted • g:EnterpriseProjectId • cce:Subnets • cce:KmsKeys • cce:AvailableZones	
cce:nodepool:upgradeNodepool	授予升级节点池的权限。	Write	cluster *	-	• cce:nodepool:update
			-	g:EnterpriseProjectId	
cce:nodepool:scale	授予扩缩容节点池的权限。	Write	cluster *	g:EnterpriseProjectId	-
cce:nodepool:getNodepool	授予查询指定节点池详情的权限。	Read	cluster *	g:EnterpriseProjectId	• cce:nodepool:get
cce:nodepool:list	授予查看指定集群的节点池列表。	List	cluster *	-	-
			-	• cce:ClusterId • g:EnterpriseProjectId	
cce:nodepool:getQuota	授予查询节点池配额的权	Read	cluster *	-	• cce:nodepool:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。		-	• cce:ClusterId • g:EnterpriseProjectId	
cce:nodepool:migrate	授予在节点池间迁移节点的权限。	Write	cluster *	-	• cce:nodepool:update
			-	• cce:ClusterId • g:EnterpriseProjectId	
cce:nodepool:sync	授予对节点池中节点进行配置同步的权限。	Write	cluster *	g:EnterpriseProjectId	• cce:nodepool:get
cce:nodepool:getConfigurationTemplate	授予查询节点池配置模板的权限。	Read	cluster *	g:EnterpriseProjectId	• cce:nodepool:get
cce:nodepool:getConfiguration	授予查询节点池配置的权限。	Read	cluster *	g:EnterpriseProjectId	• cce:nodepool:get
cce:nodepool:updateConfiguration	授予更新节点池配置的权限。	Write	cluster *	g:EnterpriseProjectId	• cce:nodepool:update
cce:node:createNode	授予创建节点的权限。	Write	cluster *	-	• cce:node:create
			-	• cce:ClusterId • evs:Encrypted • g:EnterpriseProjectId • cce:AssociatePublicIp • cce:Subnets • cce:KmsKeys • cce:AvailableZones	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cce:node:reportStatus	授予节点上报状态的权限。	Write	cluster *	g:EnterpriseProjectId	• cce:node:get
cce:node:delete	授予删除节点的权限。	Write	cluster *	g:EnterpriseProjectId	-
cce:node:update	授予更新节点的权限。	Write	cluster *	g:EnterpriseProjectId	-
cce:node:getNode	授予查询指定节点详情的权限。	Read	cluster *	g:EnterpriseProjectId	• cce:node:get
cce:node:list	授予查看指定集群的节点列表。	List	cluster *	-	-
			-	• cce:ClusterId • g:EnterpriseProjectId	
cce:node:reset	授予重置节点的权限。	Write	cluster *	-	• cce:node:create
			-	• cce:ClusterId • evs:Encrypted • g:EnterpriseProjectId • cce:KmsKeys	
cce:node:add	授予纳管节点的权限。	Write	cluster *	-	• cce:node:create
			-	• cce:ClusterId • evs:Encrypted • g:EnterpriseProjectId • cce:KmsKeys	
cce:node:remove	授予释放节点	Write	cluster *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	的权限。		-	• cce:ClusterId • g:EnterpriseProjectId	
cce:node:migrate	授予在集群间迁移节点的权限。	Write	cluster *	-	-
			-	• cce:nodeTransferSourceCluster • cce:nodeTransferTargetCluster • g:EnterpriseProjectId	
cce:node:unlock	授予解锁节点的权限（用于节点 ECS 资源防呆场景，内部交互使用）。	Write	cluster *	-	• cce:node:update
			-	• cce:ClusterId • g:EnterpriseProjectId	
cce:node:sync	授予同步节点基础设施资源状态的权限。	Read	cluster *	g:EnterpriseProjectId	• cce:node:get
cce:node:toperiod	授予批量将节点从按需转成包周期的权限。	Write	cluster *	-	-
			-	• cce:ClusterId • g:EnterpriseProjectId	
cce:job:delete	授予删除任务的权限。	Write	cluster *	• cce:ClusterId • g:EnterpriseProjectId	-
cce:job:get	授予查询指定任务详情的权限。	Read	cluster *	• cce:ClusterId • g:EnterpriseProjectId	-
cce:job:list	授予查看任务	List	cluster	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	列表。		*		
			-	cce:ClusterId	
cce:quota:get	授予查询 CCE 服务相关资源配额的权限。	Read	-	-	-
cce:addonInstance:create	授予创建插件实例的权限。	Write	cluster *	-	-
			-	• cce:ClusterId • g:EnterpriseProjectId	
cce:addonInstance:delete	授予删除插件实例的权限。	Write	cluster *	• cce:ClusterId • g:EnterpriseProjectId	-
cce:addonInstance:update	授予更新插件实例的权限。	Write	cluster *	• cce:ClusterId • g:EnterpriseProjectId	-
cce:addonInstance:get	授予查询指定插件实例详情的权限。	Read	cluster *	• cce:ClusterId • g:EnterpriseProjectId	-
cce:addonInstance:list	授予查看指定集群的插件实例列表的权限。	List	cluster *	-	-
			-	• cce:ClusterId • g:EnterpriseProjectId	
cce:addonInstance:rollback	授予回滚指定插件实例的权限。	Write	cluster *	• cce:ClusterId • g:EnterpriseProjectId	-
cce:chart:upload	授予上传应用模板的权限。	Write	-	-	-
cce:chart:delete	授予删除应用模板的权限。	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cce:chart:update	授予更新应用模板的权限。	Write	-	-	-
cce:chart:listChart	授予查看应用模板详情列表的权限。	List	-	-	• cce:chart:list
cce:chart:getChart	授予查看用户指定应用模板详情的权限。	Read	-	-	• cce:chart:get
cce:chart:download	授予查看用户下载应用模板的权限。	Read	-	-	• cce:chart:get
cce:chart:getQuota	授予查看应用模板配额的权限。	Read	-	-	• cce:chart:list
cce:release:create	授予创建应用实例的权限。	Write	-	• cce:ClusterId • g:EnterpriseProjectId	-
cce:release:delete	授予删除应用实例的权限。	Write	cluster*	• cce:ClusterId • g:EnterpriseProjectId	-
cce:release:update	授予更新应用实例的权限。	Write	cluster*	• cce:ClusterId • g:EnterpriseProjectId	-
cce:release:get	授予查询指定应用实例详情的权限。	Read	cluster*	• cce:ClusterId • g:EnterpriseProjectId	-
cce:release:list	授予查看指定集群的应用实例列表的权限。	List	cluster* -	- • cce:ClusterId • g:EnterpriseProjectId	-
cce:permission	授予创建（白	Write	-	-	• cce:cluster:u

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ApplyOrder:create	名单）权限申请的权限。				pgrade
cce:permissionApplyOrder:list	授予查看（白名单）权限申请列表的权限。	List	-	-	• cce:cluster:list
cce:longaksk:getConfig	授予获取longAKSK配置的权限。	Read	-	-	-
cce:longaksk:updateConfig	授予更新longAKSK配置的权限。	Write	-	-	-
cce:cluster:getLongAKSKConfig	授予获取集群longAKSK配置的权限。	Read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cce:cluster:updateLongAKSKConfig	授予更新集群longAKSK配置的权限。	Write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cce:accessPolicy:get	授予获取访问策略的权限。	Read	-	-	-
cce:accessPolicy:list	授予获取访问策略列表的权限。	Read	-	-	-
cce:accessPolicy:post	授予创建访问策略的权限。	Write	-	-	-
cce:accessPolicy:put	授予更新访问策略的权限。	Write	-	-	-
cce:accessPolicy:delete	授予删除访问策略的权限。	Write	-	-	-
cce:imageCache:get	授予查看指定镜像缓存详情的权限。	Read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cce:imageCache:list	授予查看镜像缓存列表的权限。	List	-	-	-
cce:imageCache:create	授予创建镜像缓存的权限。	Write	-	-	-
cce:imageCache:delete	授予删除镜像缓存的权限。	Write	-	-	-
cce:hypernode:list	授予查看集群内超节点列表的权限。	List	cluster *	-	-
cce:packageProduct:list	授予查看套餐包列表的权限。	List	-	-	-
cce:packageProduct:subscribe	授予订购套餐包的权限。	Write	-	-	-

CCE 的 API 通常对应着一个或多个授权项。表 3-76 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-76 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v5/imagecaches	cce:imageCache:create	-
DELETE /v5/imagecaches/{image_cache_id}	cce:imageCache:delete	-
GET /v5/imagecaches/{image_cache_id}	cce:imageCache:get	-
GET /v5/imagecaches	cce:imageCache:list	-
GET /v5/package-products	cce:packageProduct:list	-
POST /v5/package-products/subscribe	cce:packageProduct:subscribe	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /api/v3/projects/{project_id}/longaksk/config	cce:longaksk:getConfig	-
PUT /api/v3/projects/{project_id}/longaksk/config	cce:longaksk:updateConfig	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/longaksk/config	cce:cluster:getLongAKSKConfig	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/longaksk/config	cce:cluster:updateLongAKSKConfig	-
GET /api/v3/access-policies/{policy_id}	cce:accessPolicy:get	-
GET /api/v3/access-policies	cce:accessPolicy:list	-
POST /api/v3/access-policies	cce:accessPolicy:post	-
PUT /api/v3/access-policies/{policy_id}	cce:accessPolicy:put	-
DELETE /api/v3/access-policies/{policy_id}	cce:accessPolicy:delete	-
GET /api/v3/projects/{project_id}/quotas	cce:quota:get	-
POST /api/v3/projects/{project_id}/clusters	cce:cluster:createCluster	-
DELETE /api/v3/projects/{project_id}/clusters/{cluster_id}	cce:cluster:delete	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}	cce:cluster:updateCluster	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrad	cce:cluster:upgrade	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
e		
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/retry	cce:cluster:upgrade	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/tasks/{task_id}	cce:cluster:getCluster	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/continue	cce:cluster:upgrade	-
GET /api/v3.1/projects/{project_id}/clusters/{cluster_id}/operation/snapshot/tasks	cce:cluster:getCluster	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows	cce:cluster:upgrade	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows	cce:cluster:getCluster	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/tasks	cce:cluster:getCluster	-
PATCH /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows/{upgrade_workflow_id}	cce:cluster:upgrade	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows/{upgrade_	cce:cluster:getCluster	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
workflow_id}		
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/pause	cce:cluster:upgrade	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/awake	cce:cluster:start	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/hibernate	cce:cluster:stop	-
GET /api/v3/projects/{project_id}/clusters	cce:cluster:list	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}	cce:cluster:getCluster	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/openapi	cce:cluster:getEndpoints	-
GET /v5/imagecaches/{image_cache_id}	cce:imageCache:get	-
GET /v5/imagecaches	cce:imageCache:list	-
POST /v5/imagecaches	cce:imageCache:create	-
DELETE /v5/imagecaches/{image_cache_id}	cce:imageCache:delete	-
GET /v5/package-products	cce:packageProduct:list	-
POST /v5/package-products/subscribe	cce:packageProduct:subscribe	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/resize	cce:cluster:resize	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/mastereip	cce:cluster:eipBinding	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/clustercert	cce:cluster:generateClientCredential	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/clustercertrevoke	cce:cluster:revokeClientCredential	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/tags/create	cce:cluster:addTags	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/tags/delete	cce:cluster:removeTags	-
PUT /v1/services/checklock/cce	cce:cluster:checkLock	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/partitions	cce:partition:create	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/partitions/{partition_name}	cce:partition:update	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/partitions/{partition_name}	cce:partition:get	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/partitions	cce:partition:list	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools	cce:nodepool:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}	cce:nodepool:delete	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}	cce:nodepool:updateNodepool	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}/operation/upgrade	cce:nodepool:upgradeNodepool	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}/operation/scale	cce:nodepool:scale	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}	cce:nodepool:getNodepool	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools	cce:nodepool:list	-
PUT /api/v3.1/projects/{project_id}/clusters/{cluster_id}/nodepool/{nodepool_id}/sync	cce:nodepool:sync	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}/configuration/detail	cce:nodepool:getConfigurationTemplate	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes	cce:node:createNode	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/{node_id}	cce:node:delete	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/{node_id}	cce:node:update	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/{node_id}	cce:node:getNode	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes	cce:node:list	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/sync	cce:node:update	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}/nodes/add	cce:node:add	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/reset	cce:node:reset	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/add	cce:node:add	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/operation/remove	cce:node:remove	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/operation/migrateto/{target_cluster_id}	cce:node:migrate	-
GET /api/v2/projects/{proje	cce:node:sync	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ct_id}/clusters/{cluster_id}/nodes/{node_id}/sync		
DELETE /api/v2/projects/{project_id}/jobs/{job_id}	cce:job:delete	-
GET /api/v3/projects/{project_id}/jobs/{job_id}	cce:job:get	-
GET /api/v2/projects/{project_id}/jobs	cce:job:list	-
GET /api/v3/addontemplates	cce:cluster:list	-
POST /api/v3/addons	cce:addonInstance:create	-
DELETE /api/v3/addons/{id}	cce:addonInstance:delete	-
PUT /api/v3/addons/{id}	cce:addonInstance:update	-
GET /api/v3/addons/{id}	cce:addonInstance:get	-
GET /api/v3/addons	cce:addonInstance:list	-
POST /api/v3/addons/{id}/operation/rollback	cce:addonInstance:rollback	-
POST /v2/charts	cce:chart:upload	-
DELETE /v2/charts/{chart_id}	cce:chart:delete	-
PUT /v2/charts/{chart_id}	cce:chart:update	-
GET /v2/charts/{chart_id}	cce:chart:getChart	-
GET /v2/charts	cce:chart:listChart	-
GET /v2/charts/{chart_id}/archive	cce:chart:download	-
POST /cce/cam/v3/clusters/{cluster_id}/releases	cce:release:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /cce/cam/v3/clusters/{cluster_id}/namespace/{namespace}/releases/{name}	cce:release:delete	-
PUT /cce/cam/v3/clusters/{cluster_id}/namespace/{namespace}/releases/{name}	cce:release:update	-
GET /cce/cam/v3/clusters/{cluster_id}/namespace/{namespace}/releases/{name}	cce:release:get	-
GET /cce/cam/v3/clusters/{cluster_id}/releases	cce:release:list	-
POST /autopilot/v3/projects/{project_id}/clusters	cce:cluster:createCluster	-
POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/clustercert	cce:cluster:generateClientCredential	-
DELETE /autopilot/v3/projects/{project_id}/clusters/{cluster_id}	cce:cluster:delete	-
GET /autopilot/v3/projects/{project_id}/clusters	cce:cluster:list	-
GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}	cce:cluster:getCluster	-
GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/openapi	cce:cluster:getEndpoints	-
GET /autopilot/v3/projects/{project_id}/jobs/{job_id}	cce:job:get	-
PUT	cce:cluster:updateCluster	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/autopilot/v3/projects/{project_id}/clusters/{cluster_id}		
PUT /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/mastereip	cce:cluster:eipBinding	-
POST /autopilot/v3/addons	cce:addonInstance:create	-
DELETE /autopilot/v3/addons/{id}	cce:addonInstance:delete	-
PUT /autopilot/v3/addons/{id}	cce:addonInstance:update	-
GET /autopilot/v3/addons/{id}	cce:addonInstance:get	-
GET /autopilot/v3/addons	cce:addonInstance:list	-
POST /autopilot/v3/addons/{id}/operation/rollback	cce:addonInstance:rollback	-
POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade	cce:cluster:upgrade	-
POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/retry	cce:cluster:upgrade	-
GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/tasks/{task_id}	cce:cluster:getCluster	-
GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/precheck/tasks/{task_id}	cce:cluster:getCluster	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /autopilot/v3.1/projects/{project_id}/clusters/{cluster_id}/operation/snapshot/tasks	cce:cluster:getCluster	-
POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows	cce:cluster:upgrade	-
POST /autopilot/v3.1/projects/{project_id}/clusters/{cluster_id}/operation/snapshot	cce:cluster:upgrade	-
GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows	cce:cluster:getCluster	-
POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/precheck	cce:cluster:upgrade	-
GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/precheck/tasks	cce:cluster:getCluster	-
GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/upgradeinfo	cce:cluster:getCluster	-
GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/tasks	cce:cluster:getCluster	-
PATCH /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows/{upgrade_workflow_id}	cce:cluster:upgrade	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/postcheck	cce:cluster:upgrade	-
GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows/{upgrade_workflow_id}	cce:cluster:getCluster	-
GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/upgradeplans	cce:cluster:getCluster	-
PUT /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/upgradeplans/{upgrade_plan_id}	cce:cluster:upgrade	-
POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/tags/create	cce:cluster:addTags	-
POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/tags/delete	cce:cluster:removeTags	-
GET /autopilot/v3/projects/{project_id}/quotas	cce:quota:get	-
POST /autopilot/v2/charts	cce:chart:upload	-
DELETE /autopilot/v2/charts/{chart_id}	cce:chart:delete	-
PUT /autopilot/v2/charts/{chart_id}	cce:chart:update	-
GET /autopilot/v2/charts/{chart_id}	cce:chart:getChart	-
GET /autopilot/v2/charts	cce:chart:listChart	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /autopilot/v2/charts/{chart_id}/archive	cce:chart:download	-
GET /autopilot/v2/charts/{project_id}/quotas	cce:chart:getQuota	-
GET /autopilot/v2/charts/{chart_id}/values	cce:chart:getChart	-
POST /autopilot/cam/v3/clusters/{cluster_id}/releases	cce:release:create	-
DELETE /autopilot/cam/v3/clusters/{cluster_id}/namespace/{namespace}/releases/{name}	cce:release:delete	-
PUT /autopilot/cam/v3/clusters/{cluster_id}/namespace/{namespace}/releases/{name}	cce:release:update	-
GET /autopilot/cam/v3/clusters/{cluster_id}/namespace/{namespace}/releases/{name}	cce:release:get	-
GET /autopilot/cam/v3/clusters/{cluster_id}/releases	cce:release:list	-
GET /autopilot/cam/v3/clusters/{cluster_id}/namespace/{namespace}/releases/{name}/history	cce:release:get	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-77 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

 版权所有 © 华为云计算技术有限公司

CCE 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-77 CCE 支持的资源类型

资源类型	URN
cluster	cce:<region>:<account-id>:cluster:<cluster-name>
imageCache	cce:<region>:<account-id>:imageCache:<imageCache-name>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 cce:）仅适用于对应服务的操作，详情请参见表 3-78。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

CCE 支持的服务级条件键

CCE 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-78 CCE 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
cce:ClusterId	string	单值	按照在请求中传递的集群 ID 筛选访问权限。
cce:nodeTransferSourceCluster	string	单值	按照节点迁移的源集群 ID 筛选访问权限。
cce:nodeTransferTargetCluster	string	单值	按照节点迁移的目的集群 ID 筛选访问权限。
cce:AssociatePublicIp	boolean	单值	按照关联 eip 开关值筛

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
			选节点绑定 eip 的权限。
cce:VpcId	string	单值	按照 vpc id 筛选访问权限。
cce:SubnetId	string	单值	按照 subnet id 筛选访问权限。
cce:Subnets	string	多值	按照 subnet id 列表筛选访问权限。
cce:KmsKeys	string	多值	按照 kms 密钥列表筛选访问权限。
cce:AvailableZones	string	多值	按照 AvailableZone 列表筛选访问权限。

3.4.2 云容器实例 CCI

Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）可以使用以下授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。

本章节介绍组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为 SCP 中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在 SCP 中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在 SCP 语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 CCI 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在 SCP 语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。

 版权所有 © 华为云计算技术有限公司

- 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
- 如果此列条件键没有值（-），表示此操作不支持指定条件键。

关于 CCI 定义的条件键的详细信息请参见条件（Condition）。

您可以在策略语句的 Action 元素中指定以下 CCI 的相关操作。

表3-79 CCI 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
cci:namespace:list	授予查询所有命名空间的权限。	List	namespace *	-
cci:namespace:create	授予创建命名空间的权限。	Write	namespace *	-
cci:namespace:get	授予查询命名空间的权限。	Read	namespace *	g:ResourceTag/<tag-key>
cci:namespace:delete	授予删除命名空间的权限。	Write	namespace *	g:ResourceTag/<tag-key>
cci:network:list	授予查询所有网络的权限。	List	network *	-
cci:network:create	授予创建网络的权限。	Write	network *	-
cci:network:get	授予查询网络的权限。	Read	network *	-
cci:network:delete	授予删除网络的权限。	Write	network *	-
cci:network:update	授予更新网络的权限。	Write	network *	-
cci:configmap:list	授予查询所有配置项(ConfigMap)的权限。	List	configmap *	-
cci:configmap:create	授予创建配置项(ConfigMap)的权限。	Write	configmap *	-
cci:configmap:get	授予查询配置项(ConfigMap)的权限。	Read	configmap *	-
cci:configmap:delete	授予删除配置项(ConfigMap)的权	Write	configmap *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
	限。			
cci:configmap:update	授予更新配置项(ConfigMap)的权限。	Write	configmap *	-
cci:pod:list	授予查询所有容器组(Pod)的权限。	List	pod *	-
cci:pod:create	授予创建容器组(Pod)的权限。	Write	pod *	cci:AssociatePublicIp
cci:pod:get	授予查询容器组(Pod)的权限。	Read	pod *	-
cci:pod:delete	授予删除容器组(Pod)的权限。	Write	pod *	-
cci:pod:update	授予更新容器组(Pod)的权限。	Write	pod *	-
cci:pod:getLog	授予查询容器组(Pod)输出的权限。	Read	pod *	-
cci:pod:exec	授予进入容器组(Pod)执行命令的权限。	Write	pod *	cci:ContainerName
cci:secret:list	授予查询所有密钥(Secret)的权限。	List	secret *	-
cci:secret:create	授予创建密钥(Secret)的权限。	Write	secret *	-
cci:secret:get	授予查询密钥(Secret)的权限。	Read	secret *	-
cci:secret:delete	授予删除密钥(Secret)的权限。	Write	secret *	-
cci:secret:update	授予更新密钥(Secret)的权限。	Write	secret *	-
cci:persistentvolume:list	授予查询所有存储卷(PersistentVolume)的权限。	List	persistentvolume *	-
cci:persistentvolume:create	授予创建存储卷(PersistentVolume)	Write	persistentvolume *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
	的权限。			
cci:persistentvolume:get	授予查询存储卷(PersistentVolume)的权限。	Read	persistentvolume *	-
cci:persistentvolume:update	授予更新存储卷(PersistentVolume)的权限。	Write	persistentvolume *	-
cci:persistentvolume:delete	授予删除存储卷(PersistentVolume)的权限。	Write	persistentvolume *	-
cci:persistentvolumeclaim:list	授予查询所有存储卷声明(PersistentVolumeClaim)的权限。	List	persistentvolumeclaim *	-
cci:persistentvolumeclaim:create	授予创建存储卷声明(PersistentVolumeClaim)的权限。	Write	persistentvolumeclaim *	-
cci:persistentvolumeclaim:get	授予查询存储卷声明(PersistentVolumeClaim)的权限。	Read	persistentvolumeclaim *	-
cci:persistentvolumeclaim:update	授予更新存储卷声明(PersistentVolumeClaim)的权限。	Write	persistentvolumeclaim *	-
cci:persistentvolumeclaim:delete	授予删除存储卷声明(PersistentVolumeClaim)的权限。	Write	persistentvolumeclaim *	-
cci:storageclass:list	授予查询所有存储类(StorageClass)的权限。	List	-	-
cci:imagesnapshot:list	授予查询所有镜像快照(ImageSnapshot)的权限。	List	imagesnapshot *	-
cci:imagesnapshot:create	授予创建镜像快照(ImageSnapshot)的	Write	imagesnapshot *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
	权限。			
cci:imagesnapshot:get	授予查询镜像快照(ImageSnapshot)的权限。	Read	imagesnapshot *	-
cci:imagesnapshot:delete	授予删除镜像快照(ImageSnapshot)的权限。	Write	imagesnapshot *	-
cci:deployment:list	授予查询所有无状态负载(Deployment)的权限。	List	deployment *	-
cci:deployment:create	授予创建无状态负载(Deployment)的权限。	Write	deployment *	cci:AssociatePublicIp
cci:deployment:get	授予查询无状态负载(Deployment)的权限。	Read	deployment *	-
cci:deployment:delete	授予删除无状态负载(Deployment)的权限。	Write	deployment *	-
cci:deployment:update	授予更新无状态负载(Deployment)的权限。	Write	deployment *	cci:AssociatePublicIp
cci:service:list	授予查询所有服务(Service)的权限。	List	service *	-
cci:service:create	授予创建服务(Service)的权限。	Write	service *	-
cci:service:get	授予查询服务(Service)的权限。	Read	service *	-
cci:service:delete	授予删除服务(Service)的权限。	Write	service *	-
cci:service:update	授予更新服务(Service)的权限。	Write	service *	-
cci:horizontalpodautoscaler:list	授予查询所有水平弹性伸缩(HorizontalPodAutoscaler)的权限。	List	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
cci:horizontalpodautoscaler:create	授予创建水平弹性伸缩(HorizontalPodAutoscaler)的权限。	Write	-	-
cci:horizontalpodautoscaler:get	授予查询水平弹性伸缩(HorizontalPodAutoscaler)的权限。	Read	-	-
cci:horizontalpodautoscaler:delete	授予删除水平弹性伸缩(HorizontalPodAutoscaler)的权限。	Write	-	-
cci:horizontalpodautoscaler:update	授予更新水平弹性伸缩(HorizontalPodAutoscaler)的权限。	Write	-	-
cci::updateobservabilityconfiguration	授予更新可观测性配置项(ObservabilityConfiguration)的权限。	Write	-	-
cci::getobservabilityconfiguration	授予查询可观测性配置项(ObservabilityConfiguration)的权限。	Read	-	-
cci:poolbinding:list	授予查询所有后端服务器组关联配置(PoolBinding)的权限。	List	-	-
cci:poolbinding:create	授予创建后端服务器组关联配置(PoolBinding)的权限。	Write	-	-
cci:poolbinding:get	授予查询后端服务器组关联配置(PoolBinding)的权限。	Read	-	-
cci:poolbinding:delete	授予删除后端服务器组关联配置(PoolBinding)的权	Write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
	限。			

CCI 的 API 通常对应着一个或多个授权项。表 3-80 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-80 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /apis/cci/v2/namespaces	cci:namespace:list	-
POST /apis/cci/v2/namespaces	cci:namespace:create	-
GET /apis/cci/v2/namespaces/{name}	cci:namespace:get	-
DELETE /apis/cci/v2/namespaces/{name}	cci:namespace:delete	-
GET /apis/cci/v2/namespaces/{namespace}/configmaps	cci:configmap:list	-
POST /apis/cci/v2/namespaces/{namespace}/configmaps	cci:configmap:create	-
GET /apis/cci/v2/namespaces/{namespace}/configmaps/{name}	cci:configmap:get	-
PUT /apis/cci/v2/namespaces/{namespace}/configmaps/{name}	cci:configmap:update	-
DELETE /apis/cci/v2/namespaces/{namespace}/configmaps/{name}	cci:configmap:delete	-
GET	cci:pod:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/apis/cci/v2/namespaces/{namespace}/pods		
POST /apis/cci/v2/namespaces/{namespace}/pods	cci:pod:create	-
GET /apis/cci/v2/namespaces/{namespace}/pods/{name}	cci:pod:get	-
PUT /apis/cci/v2/namespaces/{namespace}/pods/{name}	cci:pod:update	-
DELETE /apis/cci/v2/namespaces/{namespace}/pods/{name}	cci:pod:delete	-
PATCH /apis/cci/v2/namespaces/{namespace}/pods/{name}	cci:pod:update	-
GET /apis/cci/v2/namespaces/{namespace}/secrets	cci:secret:list	-
POST /apis/cci/v2/namespaces/{namespace}/secrets	cci:secret:create	-
GET /apis/cci/v2/namespaces/{namespace}/secrets/{name}	cci:secret:get	-
PUT /apis/cci/v2/namespaces/{namespace}/secrets/{name}	cci:secret:update	-
DELETE /apis/cci/v2/namespaces/{namespace}/secrets/{name}	cci:secret:delete	-
GET /apis/yangtse/v2/namespaces/{namespace}/networks	cci:network:list	-
POST	cci:network:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/apis/yangtse/v2/namespaces/{namespace}/networks		
GET /apis/yangtse/v2/namespaces/{namespace}/networks/{name}	cci:network:get	-
PUT /apis/yangtse/v2/namespaces/{namespace}/networks/{name}	cci:network:update	-
DELETE /apis/yangtse/v2/namespaces/{namespace}/networks/{name}	cci:network:delete	-
POST /apis/cci/v2/namespaces/{namespace}/pods/{name}/exec	cci:pod:exec	-
GET /apis/cci/v2/namespaces/{namespace}/pods/{name}/log	cci:pod:getLog	-
GET /apis/cci/v2/persistentvolumes	cci:persistentvolume:list	-
POST /apis/cci/v2/persistentvolumes	cci:persistentvolume:create	-
GET /apis/cci/v2/persistentvolumes/{name}	cci:persistentvolume:get	-
PUT /apis/cci/v2/persistentvolumes/{name}	cci:persistentvolume:update	-
DELETE /apis/cci/v2/persistentvolumes/{name}	cci:persistentvolume:delete	-
GET /apis/cci/v2/namespaces/{namespace}/persistentvolumeclaims	cci:persistentvolumeclaim:list	-
POST /apis/cci/v2/namespace	cci:persistentvolumeclaim:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
s/{namespace}/persistentvolumeclaims		
GET /apis/cci/v2/namespaces/{namespace}/persistentvolumeclaims/{name}	cci:persistentvolumeclaim:get	-
PUT /apis/cci/v2/namespaces/{namespace}/persistentvolumeclaims/{name}	cci:persistentvolumeclaim:update	-
DELETE /apis/cci/v2/namespaces/{namespace}/persistentvolumeclaims/{name}	cci:persistentvolumeclaim:delete	-
GET /apis/cci/v2/storageclasses	cci:storageclass:list	-
GET /apis/cci/v2/imagesnapshots	cci:imagesnapshot:list	-
POST /apis/cci/v2/imagesnapshots	cci:imagesnapshot:create	-
GET /apis/cci/v2/imagesnapshots/{name}	cci:imagesnapshot:get	-
DELETE /apis/cci/v2/imagesnapshots/{name}	cci:imagesnapshot:delete	-
GET /apis/cci/v2/namespaces/{namespace}/services	cci:service:list	-
POST /apis/cci/v2/namespaces/{namespace}/services	cci:service:create	-
GET /apis/cci/v2/namespaces/{namespace}/services/{name}	cci:service:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /apis/cci/v2/namespaces/{namespace}/services/{name}	cci:service:update	-
DELETE /apis/cci/v2/namespaces/{namespace}/services/{name}	cci:service:delete	-
PATCH /apis/cci/v2/namespaces/{namespace}/services/{name}	cci:service:update	-
GET /apis/cci/v2/namespaces/{namespace}/deployments	cci:deployment:list	-
POST /apis/cci/v2/namespaces/{namespace}/deployments	cci:deployment:create	-
GET /apis/cci/v2/namespaces/{namespace}/deployments/{name}	cci:deployment:get	-
PUT /apis/cci/v2/namespaces/{namespace}/deployments/{name}	cci:deployment:update	-
DELETE /apis/cci/v2/namespaces/{namespace}/deployments/{name}	cci:deployment:delete	-
PATCH /apis/cci/v2/namespaces/{namespace}/deployments/{name}	cci:deployment:update	-
GET /apis/cci/v2/namespaces/{namespace}/horizontalpodautoscalers	cci:horizontalpodautoscaler:list	-
POST /apis/cci/v2/namespaces/{namespace}/horizontalpodautoscalers	cci:horizontalpodautoscaler:create	-
GET	cci:horizontalpodautoscaler:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/apis/cci/v2/namespaces/{namespace}/horizontalpodautoscalers/{name}		
PUT /apis/cci/v2/namespaces/{namespace}/horizontalpodautoscalers/{name}	cci:horizontalpodautoscaler:update	-
DELETE /apis/cci/v2/namespaces/{namespace}/horizontalpodautoscalers/{name}	cci:horizontalpodautoscaler:delete	-
PATCH /apis/cci/v2/namespaces/{namespace}/horizontalpodautoscalers/{name}	cci:horizontalpodautoscaler:update	-
PUT /v1/observabilityconfiguration	cci::updateobservabilityconfiguration	-
GET /v1/observabilityconfiguration	cci::getobservabilityconfiguration	-
GET /apis/loadbalancer.networking.openvessel.io/v1/namespaces/{namespace}/poolbindings	cci:poolbinding:list	-
POST /apis/loadbalancer.networking.openvessel.io/v1/namespaces/{namespace}/poolbindings	cci:poolbinding:create	-
GET /apis/loadbalancer.networking.openvessel.io/v1/namespaces/{namespace}/poolbindings/{name}	cci:poolbinding:get	-
DELETE /apis/loadbalancer.networking.openvessel.io/v1/namespaces/{namespace}/poolbindings/{	cci:poolbinding:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
name}		

⚠ 注意

如果您需要在 SCP 策略中禁用 OpenStack 接口，不能禁用如下 2 个 action：“vpc:nativeSubnets:get”、“vpc:subnets:get”，否则会导致 CCI 服务的网络功能异常。

资源类型（Resource）

资源类型（Resource）表示 SCP 所作用的资源。如表 3-81 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的 SCP 语句中指定该资源的 URN，SCP 仅作用于此资源；如未指定，Resource 默认为“*”，则 SCP 将应用到所有资源。您也可以在 SCP 中设置条件，从而指定资源类型。

CCI 定义了以下可以在自定义 SCP 的 Resource 元素中使用的资源类型。

表3-81 CCI 支持的资源类型

资源类型	URN
deployment	cci:<region>:<account-id>:deployment:<namespace-name>/<deployment-name>
secret	cci:<region>:<account-id>:secret:<namespace-name>/<secret-name>
namespace	cci:<region>:<account-id>:namespace:<namespace-name>
service	cci:<region>:<account-id>:service:<namespace-name>/<service-name>
network	cci:<region>:<account-id>:network:<namespace-name>/<network-name>
persistentvolume	cci:<region>:<account-id>:persistentvolume:<persistentvolume-name>
imagesnapshot	cci:<region>:<account-id>:imagesnapshot:<imagesnapshot-name>
configmap	cci:<region>:<account-id>:configmap:<namespace-name>/<configmap-name>
pod	cci:<region>:<account-id>:pod:<namespace-name>/<pod-name>
persistentvolumeclaim	cci:<region>:<account-id>:persistentvolumeclaim:<namespace-name>/<persistentvolumeclaim-name>

 版权所有 © 华为云计算技术有限公司

条件（Condition）

条件键概述

条件（Condition）是 SCP 生效的特定条件，包括条件键和运算符。

- 条件键表示 SCP 语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 cci:）仅适用于对应服务的操作，详情请参见表 3-82。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，SCP 才能生效。支持的运算符请参见：运算符。

CCI 支持的服务级条件键

CCI 定义了以下可以在自定义 SCP 的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化 SCP 语句应用的条件。

表3-82 CCI 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
cci:AssociatePublicIp	boolean	单值	按照关联 eip 开关值筛选 pod 绑定 eip 的权限。
cci:ContainerName	string	单值	按照容器名称筛选 pod 执行命令的权限。

3.4.3 容器镜像服务 SWR

Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）可以使用以下授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。

本章节介绍组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

 版权所有 © 华为云计算技术有限公司

操作（Action）

操作（Action）即为 SCP 中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在 SCP 中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在 SCP 语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 SWR 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在 SCP 语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 SWR 定义的条件键的详细信息请参见条件（Condition）。

您可以在 SCP 语句的 Action 元素中指定以下 SWR 的相关操作。

表3-83 SWR 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
swr:namespace:createNamespace	授予共享版仓库创建组织的权限。	Write	namespace *	-
swr:namespace:deleteNamespace	授予共享版仓库删除组织的权限。	Write	namespace *	-
swr:namespace:listNamespaces	授予共享版仓库查询组织列表的权限。	List	namespace *	-
swr:namespace:getNamespace	授予共享版仓库获取组织详情的权限。	Read	namespace *	-
swr:repo:createRepo	授予共享版仓库创建镜像仓库的权限。	Write	repo *	-
			-	swr:AllowPublicAccess
swr:repo:deleteRepo	授予共享版仓库删除镜像仓库的权限。	Write	repo *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
swr:repo:listRepos	授予共享版仓库查询镜像仓库列表的权限。	List	repo *	-
swr:repo:listSharedRepos	授予共享版仓库查询共享镜像列表的权限。	List	repo *	-
swr:repo:getRepo	授予共享版仓库查询镜像仓库概要信息的权限。	Read	repo *	-
swr:repo:updateRepo	授予共享版仓库更新镜像仓库的概要信息的权限。	Write	repo *	-
			-	swr:AllowPublicAccess
swr:repo:deleteRepoTag	授予共享版仓库删除镜像仓库中指定版本的镜像的权限。	Write	repo *	-
swr:repo:createRepoTag	授予共享版仓库创建镜像版本的权限。	Write	repo *	-
swr:repo:listRepoTags	授予共享版仓库查询镜像版本列表的权限。	List	repo *	-
swr:repo:createRepoDomain	授予共享版仓库创建共享账号的权限。	Permission_management	repo *	-
			-	• swr:TargetAccountId • swr:TargetOrgPath • swr:TargetOrgId
swr:repo:deleteRepoDomain	授予共享版仓库删除共享账号的权限。	Permission_management	repo *	-
swr:repo:listRepoDomains	授予共享版仓库获取共享账号列表的权限。	List	repo *	-
swr:repo:getRepoDomain	授予共享版仓库判断共享账号是否存在的权限。	Read	repo *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
swr:repo:updateRepoDomain	授予共享版仓库更新共享账号的权限。	Permission_management	repo *	-
swr:repo:createRepoShare	授予共享版仓库创建镜像共享规则的权限。	Permission_management	repo *	-
			-	• swr:TargetAccountId • swr:TargetOrgPath • swr:TargetOrgId
swr:repo:deleteRepoShare	授予共享版仓库删除镜像共享规则的权限。	Permission_management	repo *	-
swr:repo:listRepoShares	授予共享版仓库获取镜像共享规则列表的权限。	List	repo *	-
swr:repo:getRepoShare	授予共享版仓库查看镜像共享规则的权限。	Read	repo *	-
swr:repo:updateRepoShare	授予共享版仓库更新镜像共享规则的权限。	Permission_management	repo *	-
swr:repo:createAutoSyncRepoJob	授予共享版仓库创建镜像自动同步任务的权限。	Write	repo *	-
			-	swr:TargetRegion
swr:repo:createManualSyncRepoJob	授予共享版仓库手动同步镜像的权限。	Write	repo *	-
			-	swr:TargetRegion
swr:repo:deleteAutoSyncRepoJob	授予共享版仓库删除镜像自动同步任务的权限。	Write	repo *	-
swr:repo:listAutoSyncRepoJobs	授予共享版仓库获取镜像自动同步任务列表的权限。	List	repo *	-
swr:repo:getSyncRepoJobInfo	授予共享版仓库获取镜像自动同步任务信息的权限。	Read	repo *	-
swr:repo:createTrigg	授予共享版仓库创	Write	repo *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
er	建触发器的权限。			
swr:repo:deleteTrigger	授予共享版仓库删除触发器的权限。	Write	repo *	-
swr:repo:listTriggers	授予共享版仓库获取镜像仓库下的触发器列表的权限。	List	repo *	-
swr:repo:getTrigger	授予共享版仓库获取触发器详情的权限。	Read	repo *	-
swr:repo:updateTrigger	授予共享版仓库更新触发器配置的权限。	Write	repo *	-
swr:repo:createRetention	授予共享版仓库创建镜像老化规则的权限。	Write	repo *	-
swr:repo:deleteRetention	授予共享版仓库删除镜像老化规则的权限。	Write	repo *	-
swr:repo:listRetentionHistories	授予共享版仓库获取镜像老化记录的权限。	List	repo *	-
swr:repo:listRetentions	授予共享版仓库获取镜像老化规则列表的权限。	List	repo *	-
swr:repo:getRetention	授予共享版仓库获取镜像老化规则记录的权限。	Read	repo *	-
swr:repo:updateRetention	授予共享版仓库修改镜像老化规则的权限。	Write	repo *	-
swr::createLoginSecret	授予共享版仓库生成临时登录指令的权限。	Write	-	-
swr::createAuthorizationToken	授予共享版仓库生成新的临时登录指令的权限。	Write	-	-
swr::listQuotas	授予共享版仓库获	List	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
	取配额信息的权限。			
swr::getDomainOverview	授予共享版仓库获取租户总览信息的权限。	Read	-	-
swr::getDomainResourceReports	授予共享版仓库获取租户资源统计信息的权限。	Read	-	-
swr:namespace:multipartUpload	授予共享版仓库分段上传镜像的权限。	Write	namespace *	-
swr:namespace:createNamespaceAccess	授予共享版仓库创建组织权限的权限。	Permission_management	namespace *	-
swr:namespace:deleteNamespaceAccess	授予共享版仓库删除组织权限的权限。	Permission_management	namespace *	-
swr:namespace:getNamespaceAccess	授予共享版仓库查询组织权限的权限。	Read	namespace *	-
swr:namespace:updateNamespaceAccess	授予共享版仓库更新组织权限的权限。	Permission_management	namespace *	-
swr:repo:createRepoAccess	授予共享版仓库创建镜像权限的权限。	Permission_management	repo *	-
swr:repo:deleteRepoAccess	授予共享版仓库删除镜像权限的权限。	Permission_management	repo *	-
swr:repo:getRepoAccess	授予共享版仓库查询镜像权限的权限。	Read	repo *	-
swr:repo:updateRepoAccess	授予共享版仓库更新镜像权限的权限。	Permission_management	repo *	-
swr:repo:upload	授予共享版仓库上传镜像的权限。	Write	repo *	-
			-	swr:AllowCredential

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
				Type
swr:repo:download	授予共享版仓库下载镜像的权限。	Read	repo *	-
			-	swr:AllowCredentialType
swr:repo:getRepoTag	授予共享版仓库查询镜像仓库中指定版本的镜像的权限。	Read	repo *	-

SWR 的 API 通常对应着一个或多个授权项。表 3-84 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-84 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v2/manage/namespaces	swr:namespace:createNamespace	-
DELETE /v2/manage/namespaces/{namespace}	swr:namespace:deleteNamespace	-
GET /v2/manage/namespaces	swr:namespace:listNamespaces	-
GET /v2/manage/namespaces/{namespace}	swr:namespace:getNamespace	-
POST /v2/manage/namespaces/{namespace}/repos	swr:repo:createRepo	-
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}	swr:repo:deleteRepo	-
GET /v2/manage/repos	swr:repo:listRepos	-
GET /v2/manage/shared-repositories	swr:repo:listSharedRepos	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v2/manage/namespaces/{namespace}/repos/{repository}	swr:repo:getRepo	-
PATCH /v2/manage/namespaces/{namespace}/repos/{repository}	swr:repo:updateRepo	-
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/tags/{tag}	swr:repo:deleteRepoTag	-
POST /v2/manage/namespaces/{namespace}/repos/{repository}/tags	swr:repo:createRepoTag	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/tags	swr:repo:listRepoTags	-
POST /v2/manage/namespaces/{namespace}/repositories/{repository}/access-domains	swr:repo:createRepoDomain	-
DELETE /v2/manage/namespaces/{namespace}/repositories/{repository}/access-domains/{access_domain}	swr:repo:deleteRepoDomain	-
GET /v2/manage/namespaces/{namespace}/repositories/{repository}/access-domains	swr:repo:listRepoDomains	-
GET /v2/manage/namespaces/{namespace}/repositories/{repository}/access-domains/{access_domain}	swr:repo:getRepoDomain	-
PATCH	swr:repo:updateRepoDomain	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v2/manage/namespaces/{namespace}/repositories/{repository}/access-domains/{access_domain}		
POST /v2/manage/namespaces/{namespace}/repos/{repository}/shares	swr:repo:createRepoShare	-
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/shares/{share_id}	swr:repo:deleteRepoShare	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/shares	swr:repo:listRepoShares	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/shares/{share_id}	swr:repo:getRepoShare	-
PATCH /v2/manage/namespaces/{namespace}/repos/{repository}/shares/{share_id}	swr:repo:updateRepoShare	-
POST /v2/manage/namespaces/{namespace}/repos/{repository}/sync_repo	swr:repo:createAutoSyncRepoJob	• swr::createLoginSecret • swr:repo:download • swr:repo:upload
POST /v2/manage/namespaces/{namespace}/repos/{repository}/sync_images	swr:repo:createManualSyncRepoJob	• swr::createLoginSecret • swr:repo:download • swr:repo:upload
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/sync_repo	swr:repo:deleteAutoSyncRepoJob	-
GET /v2/manage/namespaces/{namespace}/repos/	swr:repo:listAutoSyncRepoJobs	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
{repository}/sync_repo		
GET /v2/manage/namespaces/{namespace}/repos/{repository}/sync_job	swr:repo:getSyncRepoJobInfo	-
POST /v2/manage/namespaces/{namespace}/repos/{repository}/triggers	swr:repo:createTrigger	-
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/triggers/{trigger}	swr:repo:deleteTrigger	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/triggers	swr:repo:listTriggers	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/triggers/{trigger}	swr:repo:getTrigger	-
PATCH /v2/manage/namespaces/{namespace}/repos/{repository}/triggers/{trigger}	swr:repo:updateTrigger	-
POST /v2/manage/namespaces/{namespace}/repos/{repository}/retentions	swr:repo:createRetention	-
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/retentions/{retention_id}	swr:repo:deleteRetention	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/retentions/histories	swr:repo:listRetentionHistories	-
GET /v2/manage/namespaces/{namespace}/repos/	swr:repo:listRetentions	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
{repository}/retentions		
GET /v2/manage/namespaces/{namespace}/repos/{repository}/retentions/{retention_id}	swr:repo:getRetention	-
PATCH /v2/manage/namespaces/{namespace}/repos/{repository}/retentions/{retention_id}	swr:repo:updateRetention	-
POST /v2/manage/utils/secret	swr::createLoginSecret	-
POST /v2/manage/utils/authorizationtoken	swr::createAuthorizationToken	sts::createServiceBearerToken
GET /v2/manage/projects/{project_id}/quotas	swr::listQuotas	-
GET /v2/manage/overview	swr::getDomainOverview	-
GET /v2/manage/reports/{resource_type}/{frequency}	swr::getDomainResourceReports	-
POST /v2/manage/namespaces/{namespace}/access	swr:namespace:createNamespaceAccess	-
DELETE /v2/manage/namespaces/{namespace}/access	swr:namespace:deleteNamespaceAccess	-
GET /v2/manage/namespaces/{namespace}/access	swr:namespace:getNamespaceAccess	-
PATCH /v2/manage/namespaces/{namespace}/access	swr:namespace:updateNamespaceAccess	-
POST /v2/manage/namespaces/{namespace}/repos/	swr:repo:createRepoAccess	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
{repository}/access		
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/access	swr:repo:deleteRepoAccess	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/access	swr:repo:getRepoAccess	-
PATCH /v2/manage/namespaces/{namespace}/repos/{repository}/access	swr:repo:updateRepoAccess	-

资源类型（Resource）

资源类型（Resource）表示 SCP 所作用的资源。如表 3-85 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的 SCP 语句中指定该资源的 URN，SCP 仅作用于此资源；如未指定，Resource 默认为“*”，则 SCP 将应用到所有资源。您也可以在 SCP 中设置条件，从而指定资源类型。

SWR 定义了以下可以在 SCP 的 Resource 元素中使用的资源类型。

表3-85 SWR 支持的资源类型

资源类型	URN
repo	swr:<region>:<account-id>:repo:<namespace-name>/<repo-name>
repository	swr:<region>:<account-id>:repository:<instance-name>/<repository-path>
instance	swr:<region>:<account-id>:instance:<instance-name>
namespace	swr:<region>:<account-id>:namespace:<namespace-name>

条件（Condition）

条件（Condition）是 SCP 生效的特定条件，包括条件键和运算符。

- 条件键表示 SCP 语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。

 版权所有 © 华为云计算技术有限公司

  - 服务级条件键（前缀通常为服务缩写，如 SWR 仅适用于对应服务的操作，详情请参见表 3-86。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，SCP 才能生效。支持的运算符请参见：运算符。

SWR 定义了以下可以在 SCP 的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化 SCP 语句应用的条件。

表3-86 SWR 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
swr:TargetOrgPath	string	单值	按照共享目标账号所处的组织路径进行权限控制。
swr:TargetOrgId	string	单值	按照共享目标账号所处的组织 Id 进行权限控制。
swr:TargetAccountId	string	单值	按照共享目标账号 Id 进行权限控制。
swr:VpcId	string	单值	按照用户 VPC ID 进行权限控制。
swr:SubnetId	string	单值	按照用户 Subnet ID 进行权限控制。
swr:EnablePublicNameSpace	boolean	单值	限制企业仓库是否允许创公开组织。
swr:EnableObsEncrypt	boolean	单值	限制企业版实例是否必须使用加密桶。
swr:AllowPublicAccess	boolean	单值	对镜像是否可以公开进行权限控制。
swr:TargetRegion	string	单值	根据目标区域进行权限控制。
swr:SourceRegion	string	单值	根据源区域进行权限控制。
swr:TargetUrls	string	多值	根据目标 URL 地址进行权限控制。

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
swr:SourceUrls	string	多值	根据源 URL 地址进行权限控制。
swr:AllowCredentialType	string	单值	根据登录指令类型(长期登录指令,临时登录指令)进行权限控制。

3.5 CDN 与智能边缘

3.5.1 内容分发网络 CDN

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

 版权所有 © 华为云计算技术有限公司

关于 CDN 定义的资源类型的详细信息请参见资源类型（Resource）。

- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 CDN 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 CDN 的相关操作。

表3-87 CDN 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cdn:statistics:queryStats	授予权限查询域名统计数据。	list	domain *	g:EnterpriseProjectId	cdn:statistics:queryTopUrl
cdn:statistics:downloadExcel	授予权限下载域名统计数据。	list	domain *	g:EnterpriseProjectId	-
cdn:log:queryLogs	授予权限查询日志数据。	read	domain *	g:EnterpriseProjectId	-
cdn:charge:modifyChargeMode	授予权限创建或者修改计费模式。	write	-	-	cdn:configuration:modifyChargeMode
cdn:charge:queryChargeMode	授予权限查询计费模式。	list	-	-	cdn:configuration:queryChargeMode
cdn:statistics:querySubscriptionTasks	授予权限查询运营报表。	list	-	-	-
cdn:statistics:createSubscriptionTasks	授予权限创建运营报表。	write	domain *	-	-
cdn:statistics:updateSubscriptionTasks	授予权限修改运营报表。	write	domain *	-	-
cdn:statistics:deleteSubscription	授予权限删除运营报表。	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
Tasks					
cdn:configuration:queryDomainList	授予权限查询域名信息列表。	list	domain *	g:EnterpriseProjectId	cdn:configuration:queryDomains
cdn:configuration:queryDomains	授予权限查询域名。	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:modifyDomainConfigs	授予权限修改域名配置信息。	write	domain *	g:EnterpriseProjectId	-
cdn:configuration:modifyOriginConfInfo	授予权限修改域名源站信息配置。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:log:queryLogs	授予权限查询日志数据。	read	domain *	g:EnterpriseProjectId	-
cdn:statistics:queryStats	授予权限查询域名统计数据。	list	domain *	g:EnterpriseProjectId	cdn:statistics:queryTopUrl
cdn:configuration:queryDomainList	授予权限查询域名信息列表。	list	domain *	g:EnterpriseProjectId	cdn:configuration:queryDomains
cdn:configuration:createDomains	授予权限创建域名。	write	domain *	g:EnterpriseProjectId	-
cdn:configuration:queryDomains	授予权限查询域名。	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:deleteDomains	授予权限删除域名相关信息。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cdn:configuration:disableDomains	授予权限禁用域名。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:enableDomains	授予权限启用域名。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:modifyOriginServerInfo	授予权限修改域名源站信息。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:modifyOriginConfInfo	授予权限修改域名源站信息配置。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:queryOriginConfInfo	授予权限查询域名源站配置信息。	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:modifyReferConf	授予权限修改refer白名单配置。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:queryReferConf	授予权限查询refer白名单配置。	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:queryIpAcl	授予权限查询ip黑白名单。	list	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cdn:configuration:modifyIpAcl	授予权限修改ip 黑白名单。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:queryCacheRule	授予权限查询域名缓存规则。	list	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:modifyCacheRule	授予权限修改域名缓存规则。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:modifyHttpsConf	授予权限修改域名证书配置。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:queryHttpsConf	授予权限查询域名 https 配置。	read	domain	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:queryIpInfo	授予权限查 ip 归属信息。	list	-	-	cdn:configuration:queryDomains
cdn:configuration:createResHeader	授予权限创建响应头信息。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:queryResponseHeaderList	授予权限查询响应头信息。	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cdn:configuration:batchModify	授予权限批量修改域名证书	write	domain *	g:EnterpriseProjectId	cdn:configuration:modifyHttps

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
HttpsConf	配置。				Conf
cdn:configuration:queryTags	授予权限查询域名标签列表。	list	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cdn:configuration:queryDomains
cdn:configuration:modifyTags	授予权限修改资源标签。	tagging	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	-
cdn:configuration:deleteTags	授予权限删除资源标签。	tagging	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	cdn:configuration:modifyTags
cdn:configuration:refreshCache	授予权限刷新缓存。	write	-	g:EnterpriseProjectId	-
cdn:configuration:queryRefreshAndPreheatHistoryTask	授予权限查询刷新预热任务记录信息。	list	-	-	cdn:configuration:queryCacheHistoryTask
cdn:configuration:queryCacheHistoryTask	授予权限查询缓存历史任务信息。	list	-	-	-
cdn:configuration:preheatCache	授予权限修改预热相关配置。	write	-	g:EnterpriseProjectId	-
cdn:configuration:queryQuota	授予权限查询当前用户域名、刷新文件、刷新目录	list	-	-	cdn:configuration:queryDomains

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	和预热的配额。				

CDN 的 API 通常对应着一个或多个授权项。表 3-88 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-88 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1.0/cdn/domains	cdn:configuration:queryDomainList	-
POST /v1.0/cdn/domains	cdn:configuration:createDomains	-
DELETE /v1.0/cdn/domains/{domain_id}	cdn:configuration:deleteDomains	-
PUT /v1.0/cdn/domains/{domain_id}/disable	cdn:configuration:disableDomains	-
PUT /v1.0/cdn/domains/{domain_id}/enable	cdn:configuration:enableDomains	-
GET /v1.0/cdn/ip-info	cdn:configuration:queryIpInfo	-
PUT /v1.0/cdn/domains/{domain_id}/private-bucket-access	cdn:configuration:modifyOriginConfInfo	-
PUT /v1.0/cdn/domains/config-https-info	cdn:configuration:batchModifyHttpsConf	-
GET /v1.0/cdn/domains/https-certificate-info	cdn:configuration:queryDomainList	-
PUT /v1.1/cdn/configuration/domains/{domain_name}/configs	cdn:configuration:modifyOriginConfInfo	• cdn:configuration:modifyBusinessType • cdn:configuration:modifyOriginServerInfo • cdn:configuration:modifyB

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
		ackSourceUrlConfig • cdn:configuration:modifyHttpsConf • cdn:configuration:modifyCacheRule • cdn:configuration:modifyReferConf • cdn:configuration:modifyIpAcl • cdn:configuration:modifyUserAgent • cdn:configuration:modifyUrlAuth • cdn:configuration:createResHeader • cdn:configuration:modifyErrorCodeRedirectRule • cdn:configuration:modifyVideoSeek • cdn:configuration:modifyRemoteAuth • cdn:configuration:modifyServiceArea
GET /v1.1/cdn/configuration/domains/{domain_name}/configs	cdn:configuration:queryDomains	-
GET /v1.0/cdn/configuration/tags	cdn:configuration:queryTags	-
POST /v1.0/cdn/configuration/tags	cdn:configuration:modifyTags	-
POST /v1.0/cdn/configuration/tags/batch-delete	cdn:configuration:deleteTags	-
POST /v1.0/cdn/content/refresh-tasks	cdn:configuration:refreshCache	-
POST /v1.0/cdn/content/preheating-tasks	cdn:configuration:preheatCache	-
GET /v1.0/cdn/historytasks	cdn:configuration:queryCacheHistoryTask	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1.0/cdn/historytasks/{history_tasks_id}/detail	cdn:configuration:queryCacheHistoryTask	-
GET /v1.0/cdn/contentgateway/url-tasks	cdn:configuration:queryRefreshAndPreheatHistoryTask	-
GET /v1.0/cdn/quota	cdn:configuration:queryQuota	-
GET /v1.0/cdn/statistics/top-url	cdn:statistics:queryStats	-
GET /v1.0/cdn/statistics/domain-location-stats	cdn:statistics:queryStats	-
GET /v1.0/cdn/statistics/domain-stats	cdn:statistics:queryStats	-
GET /v1.0/cdn/logs	cdn:log:queryLogs	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-89 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

CDN 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-89 CDN 支持的资源类型

资源类型	URN
domain	cdn::<account-id>:domain:<domain-name>

条件（Condition）

CDN 服务不支持在身份策略中的条件键中配置服务级的条件键。CDN 可以使用适用于所有服务的全局条件键，请参考全局条件键。

 版权所有 © 华为云计算技术有限公司

3.6 数据库

3.6.1 云数据库 RDS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，服务中的（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考。
- 如何使用这些元素编辑 SCP 自定义策略，请参考。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 RDS 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 RDS 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见。

您可以在身份策略语句的 Action 元素中指定以下 RDS 的相关操作。

 版权所有 © 华为云计算技术有限公司

表3-90 RDS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rds:param:apply	授予应用参数模板的权限。	write	-	-	-
rds:instance:updateParameter	授予修改指定实例的参数的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:param:modify
rds:instance:restoreInPlace	授予恢复到已有或当前实例。	write	-	-	-
rds:instance:tableRestore	授予表级恢复的权限。	write	-	-	-
rds:database:drop	授予删除数据库的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:log:getSlowLogs	授予查询慢日志统计信息的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:log:list
rds:instance:listDatabaseVersion	授予查询数据库版本信息的权限。	read	-	-	-
rds:instance:listFlavors	授予查询规格列表的权限。	read	-	-	-
rds:instance:listStorageType	授予查询数据库磁盘类型的权限。	read	-	-	-
rds:instance:create	授予创建数据库实例的权限。	write	-	-	-
rds:instance:stop	授予停止实例的权	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-	rds:insta

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。			key>	nce:operateServer
rds:instance:start	授予开启实例的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:operateServer
rds:instance:updateName	授予修改实例名称的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:modify
rds:instance:updateRemark	授予修改实例备注的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:modify
rds:instance:createDns	授予创建内网 DNS 的权限。	write	-	-	-
rds:instance:updateDnsName	授予修改域名的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:modifyDns
rds:instance:getDnsName	授予查询实例域名的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:list
rds:instance:getDnsName	授予查询实例 IPv6 域名的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:list
rds:instance:getReplicaStatus	授予实例复制状态的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:list
rds:instance:m	授予变更	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
odifySpec	数据库实例的规格的权限。				
rds:instance:extendSpace	授予扩容数据库实例的磁盘空间的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:setAutoEnlargePolicy	授予设置自动扩容策略的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:modifyDns
rds:instance:getAutoEnlargePolicy	授予查询自动扩容策略的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:list
rds:instance:singleToHa	授予单机转主备实例的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:restart	授予重启数据库实例的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:deleteInstance	授予删除数据库实例。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:delete
rds:instance:listAll	授予查询数据库实例列表的权限。	read	-	-	rds:instance:list
rds:instance:modifyPublicAccess	授予绑定和解绑弹性公网 IP 的权限。	write	-	-	-
rds:instance:modifyStrategy	授予主备实例倒换策略的权	permission_manageme	instance	g:EnterpriseProjectId g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。	nt		key>	
rds:instance:switchover	授予手动主备切换的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:modifySynchronizeModel	授予设置主备实例数据同步方式的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:openReadonly	授予设置只读参数的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:create	授予迁移主备实例备机的权限。	write	-	-	-
rds:instance:updateOpsWindow	授予设置实例可维护时间窗的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:modify
rds:instance:upgradeDatabaseVersion	授予升级数据库版本的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:modify
rds:instance:enableSecondLevelMonitoring	授予开启秒级监控的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:log:switch
rds:instance:getSecondLevelMonitoringConfig	授予查询秒级监控配置的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:log:list
rds:instance:buildDrRelation	授予配置主实例容灾能力权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:buildDrRelation	授予配置灾备实例容灾能力	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	权限。			key>	
rds:instance:buildDrRelation	授予灾备升主权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:getReplicaStatus	授予查询容灾复制状态权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:list
rds:instance:listAll	授予批量查询容灾实例信息权限。	read	-	-	rds:instance:list
rds:instance:modifySSL	授予关闭或开启SSL 的权限。	permission_management	-	-	-
rds:instance:modifySSL	授予获取SSL 证书下载地址的权限。	permission_management	-	-	-
rds:instance:modifyPort	授予修改端口的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:modifySecurityGroup	授予修改安全组的权限。	write	-	-	-
rds:instance:modifyIp	授予修改内网 IP 的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:modifyBackupPolicy	授予设置自动备份策略的权限。	permission_management	instance	g:EnterpriseProjectId rds:BackupEnabled g:ResourceTag/<tag-key>	-
rds:instance:modifyBackupPolicy	授予设置跨区域自动备份策略的权限。	permission_management	instance	g:EnterpriseProjectId rds:BackupEnabled g:ResourceTag/<tag-key>	-
rds:instance:g	授予查询	read	instance	g:EnterpriseProjectId	rds:i

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
etBackupPolicy	自动备份策略的权限。			g:ResourceTag/<tag-key>	nstance:list
rds:instance:getBackupPolicy	授予查询跨区域自动备份策略的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:list
rds:backup:create	授予创建手动备份的权限。	write	-	-	-
rds:backup:list	授予获取备份列表的权限。	list	-	-	-
rds:backup:list	授予查询跨区域备份列表的权限。	list	-	-	-
rds:instance:listAll	授予查询跨区域备份实例列表的权限。	read	-	-	rds:instance:list
rds:backup:download	授予获取备份下载链接的权限。	read	-	-	-
rds:backup:delete	授予删除手动备份的权限。	write	-	-	-
rds:instance:getRestoreTime	授予查询实例的可恢复时间段的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:list
rds:instance:getRestoreTime	授予查询跨区域备份可恢复时间段的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rds:instance:create	授予恢复到新实例的权限。	write	-	-	-
rds:instance:tableRestore	授予查询实例是否能在库表恢复时使用极速恢复的权限。	write	-	-	-
rds:backup:list	授予查询指定时间点可恢复的库的权限。	list	-	-	-
rds:instance:tableRestore	授予库级时间点恢复的权限。	write	-	-	-
rds:instance:listAll	授予查询实例可升级的目标版本的权限。	read	-	-	rds:instance:list
rds:instance:listAll	授予大版本升级前检查的权限。	read	-	-	rds:instance:list
rds:instance:listAll	授予查询大版本检查状态或升级状态的权限。	read	-	-	rds:instance:list
rds:instance:listAll	授予查询实例大版本升级检查历史的权限。	read	-	-	rds:instance:list
rds:instance:update	授予大版本升级的	read	-	-	rds:instance:

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	权限。				modify
rds:instance:listAll	授予查询实例大版本升级历史的权限。	read	-	-	rds:instance:list
rds:log:getSlowLogs	授予查询慢日志的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:log:list
rds:log:getErrorLogs	授予查询数据库错误日志的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:log:list
rds:log:setSlowLogSensitiveStatus	授予日志开关的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:log:switch
rds:log:getSlowLogs	授予查询慢日志文件列表的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:log:list
rds:log:getErrorLogs	授予查询扩展日志的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:log:list
rds:log:download	授予生成扩展日志链接的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:log:download	授予慢日志下载的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:auditlog:operate	授予设置审计日志策略的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:auditlog:list	授予查询审计日志策略的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rds:auditlog:list	授予实例获取审计日志列表的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:auditlog:download	授予生成审计日志下载链接的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:binlog:setPolicy	授予设置Binlog 策略的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:binlog:get	授予获取Binlog 的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:listAll	授予获取诊断后的实例数的权限。	read	-	-	rds:instance:list
rds:instance:listAll	授予获取指定诊断项的诊断结果的权限。	read	-	-	rds:instance:list
rds:instance:modifyProxy	授予开启/关闭数据库代理的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:getDBProxy	授予查询数据库代理信息的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:list
rds:instance:getProxyFlavors	授予查询数据库代理规格信息的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:list
rds:instance:modifyProxy	授予设置读写分离路由模式	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	的权限。				
rds:database:createDatabase	授予创建数据库的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:database:create
rds:database:list	授予查询数据库列表的权限。	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:database:update	授予修改指定实例的数据库备注的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:database:create
rds:database:drop	授予删除数据库的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databaseUser:create	授予创建数据库用户的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databaseUser:list	授予查询数据库用户列表的权限。	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databaseUser:list	授予查询指定数据库的已授权用户的权限。	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databaseUser:update	授予修改数据库用户名备注的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databaseUser:drop	授予删除数据库用户的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:password:	授予修改	write	instance	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
update	数据库密码的权限。			g:ResourceTag/<tag-key>	
rds:databasePrivilege:grant	授予数据库帐号或用户的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databasePrivilege:revoke	授予解除数据库帐号权限的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:password:update	授予重置数据库 root 账号密码的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:database:createDatabase	授予创建数据库的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:database:create
rds:databaseUser:create	授予创建数据库用户的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:database:update	授予创建数据库 SCHEMA 的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:database:create
rds:databasePrivilege:grant	授权数据库账号的读写权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databasePrivilege:grant	授权数据库账号的操作权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:password:update	授予修改数据库密码的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rds:database:list	授予查询数据库列表的权限。	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databaseUser:list	授予查询数据库用户列表的权限。	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:database:list	授予查询数据库SCHEMA列表的权限。	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databasePrivilege:grant	设置数据库用户权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:database:update	授予修改指定实例的数据库备注的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:database:create
rds:databaseUser:update	授予修改数据库用户名备注的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:database:drop	授予删除数据库的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databaseUser:drop	授予删除数据库用户的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databaseUser:list	授权查询实例的pg_hba.conf文件配置。	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databaseUser:update	授权修改pg_hba.conf文件的单	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	个或多个配置。				
rds:databaseUser:create	授权覆盖当前pg_hba.conf 文件的配置。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databaseUser:drop	授权删除pg_hba.conf 文件的单个或多个配置。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databaseUser:list	授权查询实例的pg_hba.conf 文件修改历史。	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:database:list	授权查询SQL Server可用字符集。	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:database:createDatabase	授予创建数据库的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:database:create
rds:database:list	授权查询数据库列表。	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databaseUser:create	授予创建数据库用户的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:password:update	授予修改数据库密码的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databaseUser:list	授予查询数据库用户列表的权限。	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rds:databaseUser:list	授予查询指定数据库的已授权用户的权限。	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databaseUser:drop	授予删除数据库用户的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databasePrivilege:grant	授予数据库帐号或用户的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:databasePrivilege:revoke	授予解除数据库帐号权限的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:SetMsdtcHosts	授予添加MSDTC 主机的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:modify
rds:instance:getMsdtcHosts	授予查询MSDTC 的hosts 的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:list
rds:param:listAll	授予获取参数模板列表的权限。	list	-	-	rds:param:list
rds:param:createTemplate	授予创建参数模板的权限。	write	-	-	rds:param:create
rds:param:updateTemplate	授予修改参数模板参数的权限。	write	-	-	rds:param:modify
rds:param:copy	授予复制参数模板	write	-	-	rds:para

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	的权限。				m:create
rds:param:listInstanceParamHistories	授予查询实例参数修改历史列表的权限。	list	-	-	rds:param:list
rds:instance:getParameter	授予获取指定实例的参数模板的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:param:list
rds:param:get	授予获取指定参数模板参数的权限。	read	-	-	rds:param:list
rds:param:get	授予删除参数模板的权限。	read	-	-	-
rds:database:update	授予创建插件的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:database:create
rds:database:list	授予查询插件的权限。	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:database:drop	授予删除插件的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:updateParameter	授予修改实例指定参数值的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:param:modify
rds:instance:getParameter	授予获取实例指定参数值的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:param:list
rds:instance:se	授予设置	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
tRecycleBin	回收站策略的权限。				
rds:instance:listAll	授予查询回收站策略的权限。	read	-	-	rds:instance:list
rds:instance:listAll	授予查询回收站实例信息的权限。	read	-	-	rds:instance:list
rds:instance:createTag	授予批量增加标签的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:dealTag
rds:instance:deleteTag	授予批量删除标签的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:dealTag
rds:tag:list	授予查询项目标签的权限。	list	-	-	-
rds:instance:listQuotas	授予查询资源配额的权限。	read	-	-	rds:instance:list
rds:task:listAll	授予获取任务信息的权限。	list	-	-	rds:task:list
rds:task:listAll	授予获取指定实例和时间范围的任务信息的权限。	list	-	-	rds:task:list
rds:instance:tde	授予开启tde 的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:d	授予删除	write	instance	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
eleteDisasterRecovery	容灾关系权限。			g:ResourceTag/<tag-key>	
rds:instance:showReplayDelayStatus	授予查询日志回放延时状态的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:list
rds:instance:switchLogReplay	授予中止&恢复日志回放的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:modify
rds:instance:queryRecoveryTimeWindow	授予查询wal日志恢复时间窗权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:list
rds:binlog:setPolicy	授予设置Binlog本地保留时长的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:binlog:get	授予获取Binlog本地保留时长的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	-
rds:instance:listAll	授予获取诊断后的实例数的权限。	read	-	-	rds:instance:list
rds:instance:listAll	授予获取指定诊断项的诊断结果的权限。	read	-	-	rds:instance:list
rds:instance:update	授予新增SQL限流的权限。	read	-	-	rds:instance:modify
rds:instance:update	授予删除SQL限流	read	-	-	rds:instance:

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	的权限。				modify
rds:instance:update	授予修改SQL限流的权限。	read	-	-	rds:instance:modify
rds:instance:get	授予查询SQL限流列表的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>	rds:instance:list
rds:instance:update	授予开启/关闭/禁用所有SQL限流的权限。	read	-	-	rds:instance:modify
rds:instance:update	授予解除节点只读状态的权限。	read	-	-	rds:instance:modify

RDS的API通常对应着一个或多个授权项。表3-91展示了API与授权项的关系，以及该API需要依赖的授权项。

表3-91 API与授权项的关系

API	对应的授权项	依赖的授权项
PUT /v3.1/{project_id}/configurations/{config_id}/apply	rds:param:apply	-
PUT https://{Endpoint}/v3.1/{project_id}/instances/{instance_id}/configurations	rds:instance:updateParameter	-
POST /v3.1/{project_id}/instances/recovery	rds:instance:restoreInPlace	-
POST /v3.1/{project_id}/instances/{instance_id}/restore/tables	rds:instance:tableRestore	-
DELETE /v3.1/{project_id}/instances/{instance_id}/database/{db_name}	rds:database:drop	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v3.1/{project_id}/instances/{instance_id}/slow-logs/statistics	rds:log:getSlowLogs	-
GET /v3/{project_id}/datastores/{database_name}	rds:instance:listDatabaseVersion	-
GET /v3/{project_id}/flavors/{database_name}?version_name={version_name}&spec_code={spec_code}&is_serverless={is_serverless}	rds:instance:listFlavors	-
GET /v3/{project_id}/storage-type/{database_name}?version_name={version_name}&ha_mode={ha_mode}	rds:instance:listStorageType	-
POST /v3/{project_id}/instances	rds:instance:create	-
POST /v3/{project_id}/instances/{instance_id}/action/shutdown	rds:instance:stop	-
POST /v3/{project_id}/instances/{instance_id}/action/startup	rds:instance:start	-
PUT /v3/{project_id}/instances/{instance_id}/name	rds:instance:updateName	-
PUT /v3/{project_id}/instances/{instance_id}/alias	rds:instance:updateRemark	-
POST /v3/{project_id}/instances/{instance_id}/create-dns	rds:instance:createDns	-
PUT /v3/{project_id}/instances/{instance_id}/modify-dns	rds:instance:updateDnsName	-
GET /v3/{project_id}/instances/{instance_id}/dns	rds:instance:getDnsName	-
GET /v3/{project_id}/instances/{instance_id}/dns-ipv6	rds:instance:getDnsName	-
GET /v3/{project_id}/instances/{instance_id}/replication/status	rds:instance:getReplicaStatus	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:modifySpec	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:extendSpace	-
PUT /v3/{project_id}/instances/{instance_id}/disk-auto-expansion	rds:instance:setAutoEnlargePolicy	-
GET /v3/{project_id}/instances/{instance_id}/disk-auto-expansion	rds:instance:getAutoEnlargePolicy	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:singleToHa	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:restart	-
DELETE /v3/{project_id}/instances/{instance_id}	rds:instance:deleteInstance	-
GET /v3/{project_id}/instances	rds:instance:listAll	-
PUT /v3/{project_id}/instances/{instance_id}/public-ip	rds:instance:modifyPublicAccess	-
PUT /v3/{project_id}/instances/{instance_id}/failover/strategy	rds:instance:modifyStrategy	-
PUT /v3/{project_id}/instances/{instance_id}/failover	rds:instance:switchover	-
PUT /v3/{project_id}/instances/{instance_id}/failover/mode	rds:instance:modifySynchronizeModel	-
PUT /v3/{project_id}/instances/{instance_id}/readonly-status	rds:instance:openReadonly	-
POST /v3/{project_id}/instances/{instance_id}/migrateslave	rds:instance:create	-
PUT /v3/{project_id}/instances/{instance_id}/ops-window	rds:instance:updateOpsWindow	-
POST /v3/{project_id}/instances/{instance_id}/db-upgrade	rds:instance:upgradeDatabaseVersion	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v3/{project_id}/instances/{instance_id}/second-level-monitor	rds:instance:enableSecondLevelMonitoring	-
GET /v3/{project_id}/instances/{instance_id}/second-level-monitor	rds:instance:getSecondLevelMonitoringConfig	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:buildDrRelation	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:buildDrRelation	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:buildDrRelation	-
GET /v3/{project_id}/instances/{instance_id}/disaster-recovery	rds:instance:getReplicaStatus	-
GET /v3/{project_id}/instances/disaster-recovery-relation	rds:instance:listAll	-
PUT /v3/{project_id}/instances/{instance_id}/ssl	rds:instance:modifySSL	-
GET /v3/{project_id}/instances/{instance_id}/ssl-cert/download-link	rds:instance:modifySSL	-
PUT /v3/{project_id}/instances/{instance_id}/port	rds:instance:modifyPort	-
PUT /v3/{project_id}/instances/{instance_id}/security-group	rds:instance:modifySecurityGroup	-
PUT /v3/{project_id}/instances/{instance_id}/ip	rds:instance:modifyIp	-
PUT /v3/{project_id}/instances/{instance_id}/backups/policy	rds:instance:modifyBackupPolicy	-
PUT /v3/{project_id}/instances/{instance_id}/backups/offsite-policy	rds:instance:modifyBackupPolicy	-
GET /v3/{project_id}/instances/{instance_id}/backups/policy	rds:instance:getBackupPolicy	-
GET	rds:instance:getBack	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
https://{endpoint}/v3/0483b6b16e954cb88930a360d2c4e663/instances/dsfae23fsfdsae3435in01/backups/offsite-policy	upPolicy	
POST /v3/{project_id}/backups	rds:backup:create	-
GET /v3/{project_id}/backups?instance_id={instance_id}&backup_id={backup_id}&backup_type={backup_type}&offset={offset}&limit={limit}&begin_time={begin _time}&end_time={end_time}	rds:backup:list	-
GET /v3/{project_id}/offsite-backups?instance_id={instance_id}&backup_id={backup_id}&backup_type={backup_type}&offset={offset}&limit={limit}&begin_time={begin _time}&end_time={end_time}	rds:backup:list	-
GET /v3/backups/offsite-backup-instance?offset={offset}&limit={limit}	rds:instance:listAll	-
GET /v3/{project_id}/backup-files?backup_id={backup_id}	rds:backup:download	-
DELETE /v3/{project_id}/backups/{backup_id}	rds:backup:delete	-
GET /v3/{project_id}/instances/{instance_id}/restore-time?date=2020-12-26	rds:instance:getRestoreTime	-
GET /v3/{project_id}/instances/{instance_id}/offsite-restore-time?date=2020-12-26	rds:instance:getRestoreTime	-
POST /v3/{project_id}/instances	rds:instance:create	-
POST /v3/{project_id}/instances/fast-restore	rds:instance:tableRestore	-
POST /v3/{project_id}/{engine}/instances/history/databases	rds:backup:list	-
POST /v3/{project_id}/instances/batch/restore/databases	rds:instance:tableRestore	-
GET /v3/{project_id}/instances/{instance_id}/major-version/available-version	rds:instance:listAll	-
POST /v3/{project_id}/instances/{instance_id}/major-version/inspection	rds:instance:listAll	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/instances/{instance_id}/major-version/status?action={current_action}	rds:instance:listAll	-
GET /v3/{project_id}/instances/{instance_id}/major-version/inspection-histories?offset={offset}&limit={limit}&order={order}&sort_field={sort_field}&target_version={target_version}&is_available={is_available}	rds:instance:listAll	-
POST /v3/{project_id}/instances/{instance_id}/major-version/upgrade	rds:instance:update	-
GET /v3/{project_id}/instances/{instance_id}/major-version/upgrade-histories?offset={offset}&limit={limit}&order={order}&sort_field={sort_field}	rds:instance:listAll	-
POST /v3/{project_id}/instances/{instance_id}/slow-logs	rds:log:getSlowLogs	-
POST /v3/{project_id}/instances/{instance_id}/error-logs	rds:log:getErrorLogs	-
PUT /v3/{project_id}/instances/{instance_id}/slowlog-sensitization/{status}	rds:log:setSlowLogSensitiveStatus	-
GET /v3/{project_id}/instances/{instance_id}/slowlog-files	rds:log:getSlowLogs	-
GET /v3/{project_id}/instances/{instance_id}/xellog-files	rds:log:getErrorLogs	-
POST /v3/{project_id}/instances/{instance_id}/xellog-download	rds:log:download	-
POST /v3/{project_id}/instances/{instance_id}/slowlog-download	rds:log:download	-
PUT /v3/{project_id}/instances/{instance_id}/auditlog-policy	rds:auditlog:operate	-
GET /v3/{project_id}/instances/{instance_id}/aud	rds:auditlog:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
itlog-policy		
GET /v3/{project_id}/instances/{instance_id}/auditlog?start_time={start_time}&end_time={end_time}&offset={offset}&limit={limit}	rds:auditlog:list	-
POST /v3/{project_id}/instances/{instance_id}/auditlog-links	rds:auditlog:download	-
PUT /v3/{project_id}/instances/{instance_id}/binlog/clear-policy	rds:binlog:setPolicy	-
GET /v3/{project_id}/instances/{instance_id}/binlog/clear-policy	rds:binlog:get	-
GET /v3/{project_id}/instances/diagnosis	rds:instance:listAll	-
GET /v3/{project_id}/instances/diagnosis/info	rds:instance:listAll	-
POST /v3/{project_id}/instances/{instance_id}/proxy/open	rds:instance:modifyProxy	-
GET /v3/{project_id}/instances/{instance_id}/proxy-list	rds:instance:getDBProxy	-
GET /v3/{project_id}/instances/{instance_id}/proxy/flavors	rds:instance:getProxyFlavors	-
POST /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/route-mode	rds:instance:modifyProxy	-
DELETE /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}	rds:instance:modifyProxy	-
POST /v3/{project_id}/instances/{instance_id}/database	rds:database:createDatabase	-
GET /v3/{project_id}/instances/{instance_id}/database/detail?page={page}&limit={limit}	rds:database:list	-
POST /v3/{project_id}/instances/{instance_id}/database/update	rds:database:update	-
DELETE	rds:database:drop	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v3/{project_id}/instances/{instance_id}/database/{db_name}		
POST /v3/{project_id}/instances/{instance_id}/db_user	rds:databaseUser:create	-
GET /v3/{project_id}/instances/{instance_id}/db_user/detail?page={page}&limit={limit}	rds:databaseUser:list	-
GET /v3/{project_id}/instances/{instance_id}/database/db_user?db-name={db-name}&page={page}&limit={limit}	rds:databaseUser:list	-
PUT /v3/{project_id}/instances/{instance_id}/db-users/{user_name}/comment	rds:databaseUser:update	-
DELETE /v3/{project_id}/instances/{instance_id}/db_user/{user_name}	rds:databaseUser:drop	-
POST /v3/{project_id}/instances/{instance_id}/db_user/resetpwd	rds:password:update	-
POST /v3/{project_id}/instances/{instance_id}/db_privilege	rds:databasePrivilege:grant	-
DELETE /v3/{project_id}/instances/{instance_id}/db_privilege	rds:databasePrivilege:revoke	-
POST /v3/{project_id}/instances/{instance_id}/password	rds:password:update	-
POST /v3/{project_id}/instances/{instance_id}/database	rds:database:createDatabase	-
POST /v3/{project_id}/instances/{instance_id}/db_user	rds:databaseUser:create	-
POST /v3/{project_id}/instances/{instance_id}/schema	rds:database:update	-
POST /v3/{project_id}/instances/{instance_id}/db_privilege	rds:databasePrivilege:grant	-
POST	rds:databasePrivilege	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v3/{project_id}/instances/{instance_id}/db-user-privilege	:grant	
POST /v3/{project_id}/instances/{instance_id}/db_user/resetpwd	rds:password:update	-
GET /v3/{project_id}/instances/{instance_id}/database/detail?page={page}&limit={limit}	rds:database:list	-
GET /v3/{project_id}/instances/{instance_id}/db_user/detail?page={page}&limit={limit}	rds:databaseUser:list	-
GET /v3/{project_id}/instances/{instance_id}/schema/detail?db_name={name}&page={page}&limit={limit}	rds:database:list	-
POST /v3/{project_id}/instances/{instance_id}/user-privilege	rds:databasePrivilege:grant	-
POST /v3/{project_id}/instances/{instance_id}/database/update	rds:database:update	-
PUT /v3/{project_id}/instances/{instance_id}/db-users/{user_name}/comment	rds:databaseUser:update	-
DELETE /v3/{project_id}/instances/{instance_id}/database/{db_name}	rds:database:drop	-
DELETE /v3/{project_id}/instances/{instance_id}/db_user/{user_name}	rds:databaseUser:drop	-
GET /v3/{project_id}/instances/{instance_id}/hba-info	rds:databaseUser:list	-
PUT /v3/{project_id}/instances/{instance_id}/hba-info	rds:databaseUser:update	-
POST /v3/{project_id}/instances/{instance_id}/hba-info	rds:databaseUser:create	-
DELETE /v3/{project_id}/instances/{instance_id}/hba-info	rds:databaseUser:drop	-
GET	rds:databaseUser:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v3/{project_id}/instances/{instance_id}/hba-info/history		
GET /v3/{project_id}/collations	rds:database:list	-
POST /v3/{project_id}/instances/{instance_id}/database	rds:database:createDatabase	-
GET /v3/{project_id}/instances/{instance_id}/database/detail?page={page}&limit={limit}&db-name={db-name}&recover_model={recover_model}	rds:database:list	-
POST /v3/{project_id}/instances/{instance_id}/db_user	rds:databaseUser:create	-
POST /v3/{project_id}/instances/{instance_id}/db_user/resetpwd	rds:password:update	-
GET /v3/{project_id}/instances/{instance_id}/db_user/detail?page={page}&limit={limit}	rds:databaseUser:list	-
GET /v3/{project_id}/instances/{instance_id}/database/db_user?db-name={db-name}&page={page}&limit={limit}	rds:databaseUser:list	-
DELETE /v3/{project_id}/instances/{instance_id}/db_user/{user_name}	rds:databaseUser:drop	-
POST /v3/{project_id}/instances/{instance_id}/db_privilege	rds:databasePrivilege:grant	-
DELETE /v3/{project_id}/instances/{instance_id}/db_privilege	rds:databasePrivilege:revoke	-
POST /v3/{project_id}/instances/{instance_id}/msdtc/host	rds:instance:SetMsdtcHosts	-
GET /v3/{project_id}/instances/{instance_id}/msdtc/hosts?offset={offset}&limit={limit}	rds:instance:getMsdtcHosts	-
GET /v3/{project_id}/configurations	rds:param:listAll	-
POST /v3/{project_id}/configurations	rds:param:createTemplate	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v3/{project_id}/configurations/{config_id}	rds:param:updateTemplate	-
POST /v3/{project_id}/configurations/{config_id}/copy	rds:param:copy	-
GET /v3/{project_id}/instances/{instance_id}/configuration-histories?offset={offset}&limit={limit}&start_time={start_time}&end_time={end_time}&param_name={param_name}	rds:param:listInstanceParamHistories	-
GET /v3/{project_id}/instances/{instance_id}/configurations	rds:instance:getParameter	-
GET /v3/{project_id}/configurations/{config_id}	rds:param:get	-
DELETE /v3/{project_id}/configurations/{config_id}	rds:param:get	-
POST /v3/{project_id}/instances/{instance_id}/extensions	rds:database:update	-
GET /v3/{project_id}/instances/{instance_id}/extensions?database_name={database_name}&offset={offset}&limit={limit}	rds:database:list	-
DELETE /v3/{project_id}/instances/{instance_id}/extensions	rds:database:drop	-
PUT /v3/{project_id}/instances/{instance_id}/parameter/{name}	rds:instance:updateParameter	-
GET /v3/{project_id}/instances/{instance_id}/parameter/{name}	rds:instance:getParameter	-
PUT /v3/{project_id}/instances/recycle-policy	rds:instance:setRecycleBin	-
GET /v3/{project_id}/instances/recycle-policy	rds:instance:listAll	-
GET /v3/{project_id}/recycle-instances?offset={offset}&limit={limit}	rds:instance:listAll	-
POST /v3/{project_id}/instances/{instance_id}/tags	rds:instance:createTag	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/action		
POST /v3/{project_id}/instances/{instance_id}/tags/action	rds:instance:deleteTag	-
GET /v3/{project_id}/tags	rds:tag:list	-
GET /v3/{project_id}/quotas	rds:instance:listQuotas	-
GET /v3/{project_id}/jobs?id={id}	rds:task:listAll	-
GET /v3/{project_id}/instances/{instance_id}/tasklist/detail?start_time={start_time}&end_time={end_time}	rds:task:listAll	-
PUT /v3/{project_id}/instances/{instance_id}/tde	rds:instance:tde	-
DELETE /v3/{project_id}/instances/{instance_id}/delete-disaster-recovery	rds:instance:deleteDisasterRecovery	-
GET /v3/{project_id}/instances/{instance_id}/replay-delay/show	rds:instance:showReplayDelayStatus	-
PUT /v3/{project_id}/instances/{instance_id}/log-replay/update	rds:instance:switchLogReplay	-
GET /v3/{project_id}/instances/{instance_id}/recovery-time	rds:instance:queryRecoveryTimeWindow	-
PUT /v3/{project_id}/instances/{instance_id}/binlog/clear-policy	rds:binlog:setPolicy	-
GET /v3/{project_id}/instances/{instance_id}/binlog/clear-policy	rds:binlog:get	-
GET /v3/{project_id}/instances/diagnosis	rds:instance:listAll	-
GET /v3/{project_id}/instances/diagnosis/info	rds:instance:listAll	-
POST /v3/{project_id}/instances/{instance_id}/sql-limit	rds:instance:update	-
DELETE /v3/{project_id}/instances/{instance_id}/sql-limit	rds:instance:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v3/{project_id}/instances/{instance_id}/sql-limit/update	rds:instance:update	-
GET /v3/{project_id}/instances/{instance_id}/sql-limit?db_name={db_name}&offset={offset}&limit={limit}	rds:instance:get	-
PUT /v3/{project_id}/instances/{instance_id}/sql-limit/switch	rds:instance:update	-
PUT /v3/{project_id}/instances/{instance_id}/unlock-node-readonly-status	rds:instance:update	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的 URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

RDS 定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-92 RDS 支持的资源类型

资源类型	URN
instance	rds:<region>:<account-id>:instance:<instance-id>

条件（Condition）

条件（Condition）是身份策略生效的特定条件，包括和。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：。
  - 服务级条件键（前缀通常为服务缩写，如 rds:）仅适用于对应服务的操作，详情请参见表 4。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是

 版权所有 © 华为云计算技术有限公司

多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。

- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：。

RDS 定义了以下可以在身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化策略语句应用的条件。

表3-93 RDS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
rds:Encrypted	Boolean	单值	按照请求参数中传递的是否开启磁盘加密标签键筛选访问权限。
rds:BackupEnabled	Boolean	单值	按照请求参数中传递的是否开启备份策略标签键筛选访问权限。

3.6.2 云数据库 GaussDB

云服务在 IAM 预置了常用授权项，称为系统策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，服务中的（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

 版权所有 © 华为云计算技术有限公司

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 GaussDB 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中 GaussDB 支持指定的键值。如果此列没有值（-），表示此操作不支持指定条件键。

  关于 GaussDB 定义的条件键的详细信息请参见条件（Condition）。
- “**别名**”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 GaussDB 的相关操作。

表3-94 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
gaussdb:backup:createBackup	授予创建数据库实例手动备份的权限。	write	instance	-	gaussdb:backup:create
gaussdb:backup:deleteBackup	授予删除备份的权限。	write	instance	-	gaussdb:backup:delete
gaussdb:backup:listAll	授予查询备份列表的权限。	list	instance	-	gaussdb:backup:list
gaussdb:instance:updateBackupPolicy	授予设置备份策略的权限。	write	instance	gaussdb:BackupEnabled	• gaussdb:backup:enable • gaussdb:backup:switchTableBackup • gaussdb:instance:modifyBackupPolicy
gaussdb:param:applyParam	授予应用参数模板的权限。	write	instance	-	• gaussdb:param:apply • gaussdb:par

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
					am:modify • gaussdb:instance:modifyParameter
gaussdb:tag:create	授予添加资源标签的权限。	tagging	instance	-	gaussdb:instance:dealTag
gaussdb:instance:bindEIP	授予绑定弹性公网 IP 的权限。	write	instance	-	• gaussdb:instance:bindPublicIp • gaussdb:instance:modify
gaussdb:instance:check	授予校验实例相关信息的权限。	read	instance	-	gaussdb:instance:list
gaussdb:instance:createInstance	授予创建数据库实例的权限。	write	instance	• gaussdb:BackupEnabled • gaussdb:Encrypted	rds:instance:create
gaussdb:instance:createDatabase	授予创建数据库的权限。	write	instance	-	gaussdb:instance:modify
gaussdb:instance:createDatabaseSchema	授予创建数据库 Schema 的权限。	write	instance	-	gaussdb:instance:modify
gaussdb:instance:createDatabaseUser	授予创建数据库用户的权限。	write	instance	-	gaussdb:instance:modify
gaussdb:instance:deleteInstance	授予删除数据库实例的权限。	write	instance	-	gaussdb:instance:delete
gaussdb:instance:get	授予查询实例详情的权限。	read	instance	-	gaussdb:instance:list
gaussdb:instance:getBackupPolicy	授予查询自动备份策略的权限。	read	instance	-	• gaussdb:instance:list • gaussdb:backup:list
gaussdb:instan	授予查询实	read	instance	-	gaussdb:instanc

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ce:getBalanceStatus	例主备平衡状态的权限。				e:list
gaussdb:instance:getDiskUsage	授予查询磁盘使用率的权限。	read	instance	-	gaussdb:instance:list
gaussdb:instance:getRecyclePolicy	授予查看实例回收备份策略的权限。	read	instance	-	gaussdb:instance:list
gaussdb:instance:downloadSslCert	授予下载实例 SSL 证书的权限。	read	instance	-	gaussdb:instance:list
gaussdb:instance:grantDatabasePrivilege	授予授权数据库账号的权限。	write	instance	-	gaussdb:instance:modify
gaussdb:instance:listAll	授予查询数据库实例列表的权限。	list	instance	-	gaussdb:instance:list
gaussdb:instance:listPublicIps	授予查询实例已绑定 EIP 列表的权限。	list	instance	-	gaussdb:instance:list
gaussdb:instance:listComponents	授予查询实例组件列表的权限。	list	instance	-	gaussdb:instance:list
gaussdb:instance:listDatabases	授予查询数据库列表的权限。	list	instance	-	gaussdb:instance:list
gaussdb:instance:listDatabaseUsers	授予查询数据库用户列表的权限。	list	instance	-	gaussdb:instance:list
gaussdb:tag:listAll	授予查询资源标签列表的权限。	list	instance	-	gaussdb:instance:list
gaussdb:quota:listAll	授予查询配额列表的权限。	list	instance	-	gaussdb:instance:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
gaussdb:instance:listRecoverableTimes	授予查询备份可恢复时间段的权限。	list	instance	-	• gaussdb:instance:list • gaussdb:backup:list
gaussdb:instance:listSchemas	授予查询数据库 Schema 列表的权限。	list	instance	-	gaussdb:instance:list
gaussdb:instance:renameInstance	授予重置实例名称的权限。	write	instance	-	• gaussdb:instance:modify • gaussdb:instance:rename
gaussdb:instance:resetPassword	授予重置数据库密码的权限。	write	instance	-	• gaussdb:instance:modify • gaussdb:instance:modifyPasswd • gaussdb:instance:modifyDatabasePasswd
gaussdb:instance:resizeFlavor	授予变更实例规格的权限。	write	instance	-	• gaussdb:instance:modify • gaussdb:instance:modifySpec
gaussdb:instance:restartInstance	授予重启数据库实例的权限。	write	instance	-	• gaussdb:instance:modify • gaussdb:instance:restart
gaussdb:instance:setRecyclePolicy	授予设置实例回收备份策略的权限。	write	instance	-	gaussdb:instance:modifyBackupPolicy
gaussdb:instance:switchShard	授予分片节点主备切换的权限。	write	instance	-	gaussdb:instance:modify
gaussdb:instance:extend	授予扩容相关操作的权	write	instance	-	gaussdb:instance:modifySpec

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
gaussdb:param:update	授予修改参数组的权限。	write	instance	-	• gaussdb:param:modify • gaussdb:instance:modify • gaussdb:instance:modifyParameter
gaussdb:param:check	授予校验参数组的权限。	read	instance	-	• gaussdb:param:list • gaussdb:instance:list
gaussdb:param:copy	授予复制参数模板的权限。	write	instance	-	gaussdb:param:create
gaussdb:param:createParam	授予创建参数组的权限。	write	instance	-	• gaussdb:param:create • gaussdb:param:modify
gaussdb:param:deleteParam	授予删除参数组的权限。	write	instance	-	gaussdb:param:delete
gaussdb:param:get	授予查询参数配置详情的权限。	read	instance	-	• gaussdb:param:list • gaussdb:instance:list
gaussdb:param:compare	授予比较两个参数模板之间差异的权限。	read	instance	-	gaussdb:param:list
gaussdb:param:listAll	授予查询参数组列表的权限。	list	instance	-	• gaussdb:param:list • gaussdb:instance:list
gaussdb:param:reset	授予重置参数模板的权限。	write	instance	-	gaussdb:param:modify
gaussdb:quota:update	授予修改配额的权限。	write	instance	-	gaussdb:quota:modify

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
gaussdb:task:listAll	授予查询任务列表的权限。	list	instance	-	gaussdb:instance:list
gaussdb:task:delete	授予删除任务记录的权限。	write	instance	-	gaussdb:instance:list
gaussdb:task:get	授予查询任务详情的权限。	read	instance	-	gaussdb:instance:list

GaussDB 的 API 通常对应着一个或多个授权项。如下表展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-95 实例管理

权限	API	对应的授权项	依赖的授权项
创建数据库实例	POST /v3/{project_id}/instances	gaussdb:instance:createInstance	-
删除数据库实例	DELETE /v3/{project_id}/instances/{instance_id}	gaussdb:instance:delete	-
查询数据库实例列表	GET /v3/{project_id}/instances	gaussdb:instance:listAll	-
重置数据库密码	POST /v3/{project_id}/instances/{instance_id}/password	gaussdb:instance:resetPassword	-
修改实例名称	PUT /v3/{project_id}/instances/{instance_id}/name	gaussdb:instance:rename	-
重启数据库实例	POST /v3/{project_id}/instances/{instance_id}/restart	gaussdb:instance:restart	-
分片节点主备切换	POST /v3/{project_id}/instances/{instance_id}/swit	gaussdb:instance:switchShard	-

 版权所有 © 华为云计算技术有限公司

权限	API	对应的授权项	依赖的授权项
	ch-shard		
查询实例的组件列表	GET /v3/{project_id}/instances/{instance_id}/components	gaussdb:instance:listComponents	-
规格变更	PUT /v3/{project_id}/instance/{instance_id}/flavor	gaussdb:instance:resizeFlavor	-
查询实例主备平衡状态	GET /v3/{project_id}/instances/{instance_id}/balance	gaussdb:instance:getBalanceStatus	-
查询解决方案模板配置	GET /v3/{project_id}/deployment-form	gaussdb:instance:listAll	-
查询已绑定的 EIP 列表	GET /v3/{project_id}/instances/{instance_id}/public-ips?offset={offset}&limit={limit}	gaussdb:instance:listPublicIps	-
弱密码校验	POST /v3/{project_id}/weak-password-verification	gaussdb:instance:check	-
绑定/解绑弹性公网 IP	POST /v3/{project_id}/instances/{instance_id}/nodes/{node_id}/public-ip	gaussdb:instance:bindPublicIp	-
查询实例 SSL 证书下载地址	GET /v3/{project_id}/instances/{instance_id}/ssl-cert/download-link	gaussdb:instance:downloadSslCert	-
查询租户的实例配额	GET /v3/{project_id}/project-quotas?type={type}	gaussdb:quota:listAll	-

表3-96 参数配置

权限	API	对应的授权项	依赖的授权项
获取参数模板列表	GET /v3/{project_id}/config	gaussdb:param:listAll	-

 版权所有 © 华为云计算技术有限公司

权限	API	对应的授权项	依赖的授权项
	urations?offset={offset}&limit={limit}		
获取指定实例的参数	GET /v3/{project_id}/instances/{instance_id}/configurations	gaussdb:instance:get	-
修改指定实例的参数	PUT /v3/{project_id}/instances/{instance_id}/configurations	gaussdb:param:update	-
创建参数模板	POST /v3/{project_id}/configurations	gaussdb:param:createParam	-
删除参数模板	DELETE /v3/{project_id}/configurations/{config_id}	gaussdb:param:delete	-
查询参数模板详情	GET /v3/{project_id}/configurations/{config_id}	gaussdb:param:get	-
复制参数模板	POST /v3/{project_id}/configurations/{config_id}/copy	gaussdb:param:copy	-
重置参数组	POST /v3/{project_id}/configurations/{config_id}/reset	gaussdb:param:reset	-
比较两个参数组模板之间的差异	POST /v3/{project_id}/configurations/comparison	gaussdb:param:compare	-
查询可应用实例列表	GET /v3/{project_id}/configurations/{config_id}/applicable-instances	gaussdb:instance:listAll	-
校验参数组名称是否存在	GET /v3/{project_id}/configurations/name-validation?name={name}	gaussdb:param:check	-
应用参数模板	PUT /v3/{project_id}/configurations/{config_id}/apply	gaussdb:param:apply	-

 版权所有 © 华为云计算技术有限公司

权限	API	对应的授权项	依赖的授权项
查询参数模板的应用记录	GET /v3/{project_id}/configurations/{config_id}/applied-histories	gaussdb:param:listAll	-
查询参数模板的修改历史	GET /v3/{project_id}/configurations/{config_id}/histories	gaussdb:param:listAll	-

表3-97 备份管理

权限	API	对应的授权项	依赖的授权项
设置自动备份策略	PUT /v3/{project_id}/instances/{instance_id}/backups/policy	gaussdb:instance:updateBackupPolicy	-
查询自动备份策略	GET /v3/{project_id}/instances/{instance_id}/backups/policy	gaussdb:instance:getBackupPolicy	-
查询备份列表	GET /v3/{project_id}/backups?instance_id={instance_id}&backup_id={backup_id}&backup_type={backup_type}&offset={offset}&limit={limit}&begin_time={begin_time}&end_time={end_time}	gaussdb:backup:listAll	-
创建手动备份	POST /v3/{project_id}/backups	gaussdb:backup:create	-
删除手动备份	DELETE /v3/{project_id}/backups/{backup_id}	gaussdb:backup:delete	-
查询可恢复时间段	GET /v3/{project_id}/instances/{instance_id}/restore-time?date={date}	gaussdb:instance:listRecoverableTimes	-
恢复到新实例	POST /v3/{project_id}/instan	gaussdb:instance:createInstance	-

 版权所有 © 华为云计算技术有限公司

权限	API	对应的授权项	依赖的授权项
	ces		
查询可用于备份恢复的实例列表	GET /v3/{project_id}/restorable-instances	gaussdb:instance:listAll	-
根据时间点或者备份文件查询原实例信息	GET /v3/{project_id}/instance-snapshot?instance_id={instance_id}&backup_id={backup_id}&restore_time={restore_time}	gaussdb:instance:get	-

表3-98 引擎版本和规格

权限	API	对应的授权项	依赖的授权项
查询数据库引擎的版本	GET /v3/{project_id}/datastore/versions	gaussdb:instance:listAll	-
查询数据库规格	GET /v3/{project_id}/flavors?limit={limit}&offset={offset}&ha_mode={ha_mode}&version={version}&spec_code={spec_code}	gaussdb:instance:listAll	-
查询引擎列表	GET /v3/{project_id}/datastores	gaussdb:instance:listAll	-
查询实例可变更规格	GET /v3/{project_id}/instances/{instance_id}/available-flavors	gaussdb:instance:listAll	-

表3-99 管理数据库和用户

权限	API	对应的授权项	依赖的授权项
创建数据库	POST /v3/{project_id}/instances/{instance_id}/database	gaussdb:instance:createDatabase	-

 版权所有 © 华为云计算技术有限公司

权限	API	对应的授权项	依赖的授权项
创建数据库用户	POST /v3/{project_id}/instances/{instance_id}/db-user	gaussdb:instance:createDatabaseUser	-
创建数据库SCHEMA	POST /v3/{project_id}/instances/{instance_id}/schema	gaussdb:instance:createDatabaseSchema	-
授权数据库账号	POST /v3/{project_id}/instances/{instance_id}/db-privilege	gaussdb:instance:grantDatabasePrivilege	-
重置数据库账号密码	PUT /v3/{project_id}/instances/{instance_id}/db-user/password	gaussdb:instance:resetPassword	-
查询数据库列表	GET /v3/{project_id}/instances/{instance_id}/databases	gaussdb:instance:listDatabases	-
查询数据库用户列表	GET /v3/{project_id}/instances/{instance_id}/db-users	gaussdb:instance:listDatabaseUsers	-
查询数据库SCHEMA 列表	GET /v3/{project_id}/instances/{instance_id}/schemas	gaussdb:instance:listSchemas	-

表3-100 标签管理

权限	API	对应的授权项	依赖的授权项
查询实例标签	GET /v3/{project_id}/instances/{instance_id}/tags	gaussdb:tag:listAll	-
查询项目标签	GET /v3/{project_id}/tags	gaussdb:tag:listAll	-
查询预定义标签	GET /v3/{project_id}/predefined-tags	gaussdb:tag:listAll	-
添加实例标签	POST	gaussdb:tag:create	-

 版权所有 © 华为云计算技术有限公司

权限	API	对应的授权项	依赖的授权项
	/v3/{project_id}/instances/{instance_id}/tags		

表3-101 磁盘管理

权限	API	对应的授权项	依赖的授权项
查询实例存储空间使用信息	GET /v3/{project_id}/instances/{instance_id}/volume-usage	gaussdb:instance:getDiskUsage	-
查询数据库磁盘类型	GET /v3/{project_id}/storage-type?version={version}&ha_mode={ha_mode}	gaussdb:instance:listAll	-

表3-102 配额管理

权限	API	对应的授权项	依赖的授权项
修改企业项目配额	PUT /v3/{project_id}/enterprise-projects/quotas	gaussdb:quota:update	-
查询企业项目配额组	GET /v3/{project_id}/enterprise-projects/quotas	gaussdb:quota:listAll	-

表3-103 任务管理

权限	API	对应的授权项	依赖的授权项
获取任务信息	GET /v3/{project_id}/jobs?id={id}	gaussdb:task:get	-
查询任务列表	GET /v3/{project_id}/tasks	gaussdb:task:listAll	-
删除任务记录	DELETE /v3/{project_id}/jobs/{	gaussdb:task:delete	-

 版权所有 © 华为云计算技术有限公司

权限	API	对应的授权项	依赖的授权项
	job_id}		

表3-104 回收站

权限	API	对应的授权项	依赖的授权项
设置回收站策略	PUT /v3/{project_id}/recycle-policy	gaussdb:instance:setRecyclePolicy	-
查看回收站策略	GET /v3/{project_id}/recycle-policy	gaussdb:instance:getRecyclePolicy	-
查询回收站所有引擎实例列表	GET /v3/{project_id}/recycle-instances	gaussdb:instance:listAll	-

表3-105 容灾管理

API 功能	授权项	授权范围	对应 API 接口
查询可搭建容灾实例列表	gaussdb:disasterRecovery:list	• 支持： VDC 资源集(Project)	/v3.1/{project_id}/disaster/instances/candidates
容灾操作校验	gaussdb:disasterRecovery:list	• 支持： VDC 资源集(Project)	/v3.1/{project_id}/instances/{instance_id}/disaster/operation-precheck
查询实例容灾监控实时状态	gaussdb:disasterRecovery:list	• 支持： VDC 资源集(Project)	/v3.1/{project_id}/instances/{instance_id}/disaster/monitor
查询容灾关系列表	gaussdb:disasterRecovery:list	• 支持： VDC 资源集(Project)	/v3.1/{project_id}/disaster/relations
搭建容灾关系	gaussdb:disasterRecovery:construct	• 支持： VDC 资源集(Project)	/v3.1/{projectId}/instances/{instanceId}/disaster/construct
备实例容灾升主	gaussdb:disasterRecovery:failover	• 支持： VDC 资源集	/v3.2/{projectId}/instances/{instanceId}/failover

 版权所有 © 华为云计算技术有限公司

API 功能	授权项	授权范围	对应 API 接口
		(Project)	
解除容灾关系	gaussdb:disasterRecovery:release	• 支持： VDC 资源集(Project)	/v3.1/{projectId}/instances/{instanceId}/disaster/relations/{synchronizationId}/release
灾备实例主从切换	gaussdb:disasterRecovery:switchover	• 支持： VDC 资源集(Project)	/v3.1/{projectId}/instances/{instanceId}/disaster/relations/{synchronizationId}/switchover
容灾回切	gaussdb:disasterRecovery:construct	• 支持： VDC 资源集(Project)	/v3.1/{projectId}/instances/{instanceId}/disaster/relations/{synchronizationId}/restore
容灾演练开始	gaussdb:disasterRecovery:simulation	• 支持： VDC 资源集(Project)	/v3.1/{projectId}/instances/{instanceId}/disaster-simulation/start
容灾演练结束	gaussdb:disasterRecovery:simulation	• 支持： VDC 资源集(Project)	/v3.1/{projectId}/instances/{instanceId}/disaster-simulation/stop
容灾日志保持开始	gaussdb:disasterRecovery:keeplog	• 支持： VDC 资源集(Project)	/v3/{projectId}/instances/{instanceId}/disaster-data-cache/start
容灾日志保持结束	gaussdb:disasterRecovery:keeplog	• 支持： VDC 资源集(Project)	/v3/{projectId}/instances/{instanceId}/disaster-data-cache/stop
查询容灾关系列表	gaussdb:disasterRecovery:list	• 支持： VDC 资源集(Project)	/v3.5/{project_id}/disaster-recovery/relations
查询实例容灾监控实时状态	gaussdb:disasterRecovery:list	• 支持： VDC 资源集(Project)	/v3.5/{project_id}/instances/{instance_id}/disaster-recovery/monitor
重置容灾配置	gaussdb:disasterRecovery:construct	• 支持： VDC 资源集(Project)	/v3.5/{project_id}/instances/{instance_id}/reset-dr-config
搭建容灾关系	gaussdb:disasterRecovery:construct	• 支持：	/v3.5/{project_id}/instances/{instance_

 版权所有 © 华为云计算技术有限公司

API 功能	授权项	授权范围	对应 API 接口
		VDC 资源集(Project)	id}/disaster-recovery/construct
备实例容灾升主	gaussdb:disasterRecovery:failover	• 支持： VDC 资源集(Project)	/v3.5/{project_id}/instances/{instance_id}/disaster-recovery/failover
解除容灾关系	gaussdb:disasterRecovery:release	• 支持： VDC 资源集(Project)	/v3.5/{project_id}/instances/{instance_id}/disaster-recovery/release
灾备实例主从切换	gaussdb:disasterRecovery:switchover	• 支持： VDC 资源集(Project)	/v3.5/{project_id}/instances/{instance_id}/disaster-recovery/switchover
容灾回切	gaussdb:disasterRecovery:construct	• 支持： VDC 资源集(Project)	/v3.5/{project_id}/instances/{instance_id}/disaster-recovery/restore
容灾演练开始	gaussdb:disasterRecovery:simulation	• 支持： VDC 资源集(Project)	/v3.5/{project_id}/instances/{instance_id}/disaster-recovery/simulation-start
容灾演练结束	gaussdb:disasterRecovery:simulation	• 支持： VDC 资源集(Project)	/v3.5/{project_id}/instances/{instance_id}/disaster-recovery/simulation-stop
容灾日志保持开始	gaussdb:disasterRecovery:keeplog	• 支持： VDC 资源集(Project)	/v3.5/{project_id}/instances/{instance_id}/disaster-recovery/keep-log-start
容灾日志保持结束	gaussdb:disasterRecovery:keeplog	• 支持： VDC 资源集(Project)	/v3.5/{project_id}/instances/{instance_id}/disaster-recovery/keep-log-stop

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的 URN，

 版权所有 © 华为云计算技术有限公司

身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

GaussDB 定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-106 GaussDB 支持的资源类型

资源类型	URN
instance	gaussdb:<region>:<account-id>:instance:<instance-id>

条件（Condition）

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 gaussdb:）仅适用于对应服务的操作，详情请参见表 4。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

GaussDB 定义了以下可以在身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-107 GaussDB 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
gaussdb:BackupEnabled	boolean	单值	按照请求参数中传递的是否开启备份策略标签键筛选访问权限。限定词选择“默认”。
gaussdb:Encrypted	boolean	单值	按照请求参数中传递的是否开启磁盘加密标签键筛选访问权限。限定词选择“默

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
			认”。

3.6.3 文档数据库 DDS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 DDS 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 DDS 定义的条件键的详细信息请参见条件（Condition）。

 版权所有 © 华为云计算技术有限公司

- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 DDS 的相关操作。

表3-108 DDS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dds:instance:setSsl	授予切换 SSL 开关的权限。	permission_management	instance	-	-
dds:instance:unbindEIP	授予解绑弹性公网 IP 的权限。	write	-	-	-
dds:instance:migrateAz	授予实例迁移可用区的权限。	write	-	-	-
dds:instance:listMigrateAz	授予查询实例可迁移的可用区列表的权限。	list	-	-	-
dds:instance:updateIp	授予修改内网 IP 地址的权限。	write	instance	-	-
dds:instance:bindEIP	授予绑定弹性公网 IP 的权限。	write	-	-	-
dds:instance:resetPassword	授予重置数据库用户密码的权限。	write	instance	-	-
dds:instance:checkPassword	授予检查数据库密码的权限。	read	instance	-	-
dds:instance:updatePort	授予修改数据库端口的权限。	write	instance	-	-
dds:backup:download	授予下载备份文件的权限。	read	instance	-	-
dds:instance:setAuditLogPol	授予设置审计日志策略	permission_	instance	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
icy	的权限。	management			
dds:instance:getAuditLogPolicy	授予查看审计日志策略的权限。	list	instance	-	-
dds:instance:listAuditLog	授予查看审计日志的权限。	list	instance	-	-
dds:instance:listSlowLog	授予查看慢日志的权限。	list	instance	-	-
dds:instance:downloadSlowLog	授予下载慢日志的权限。	read	instance	-	-
dds:instance:listErrorLog	授予查看错误日志的权限。	list	instance	-	-
dds:instance:downloadErrorLog	授予下载错误日志的权限。	read	instance	-	-
dds:configuration:delete	授予删除参数组的权限。	write	-	g:EnterpriseProjectId	-
dds:configuration:update	授予修改参数组中参数值的权限。	write	-	g:EnterpriseProjectId	-
dds:backup:listAll	授予查询备份列表的权限。	list	-	-	-
dds:instance:updateConfiguration	授予修改实例或实例节点的参数组配置的权限。	write	instance	-	-
dds:instance:applyConfiguration	授予应用参数配置到实例或实例节点的权限。	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dds:instance:createIp	授予创建 IP 的权限。	write	-	-	-
dds:backup:delete	授予删除备份的权限。	write	-	-	-
dds:instance:updateSecurityGroup	授予变更实例安全组的权限。	write	instance	-	-
dds:configuration:listAll	授予查询参数组列表的权限。	list	-	g:EnterpriseProjectId	-
dds:instance:getConfiguration	授予查询实例参数配置的权限。	read	instance	-	-
dds:configuration:get	授予查询参数配置详情的权限。	read	-	g:EnterpriseProjectId	-
dds:instance:updateSpec	授予变更实例规格的权限。	write	instance	-	-
dds:instance:getSecondLevelMonitoringConfig	授予查询秒级监控配置的权限。	read	instance	-	-
dds:instance:setSecondLevelMonitoringConfig	授予开启秒级监控的权限。	write	instance	-	-
dds:instance:switchover	授予切换主备节点的权限。	write	instance	-	-
dds:instance:extendVolume	授予扩容实例存储容量的权限。	write	instance	-	-
dds:instance:listAll	授予查询数据库实例列表的权限。	list	-	-	-
dds:instance:setRecyclePolicy	授予设置实例回收备份策略的权	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
dds:instance:getRecyclePolicy	授予查看实例回收备份策略的权限。	read	-	-	-
dds:instance:listRecycleInstances	授予查询回收站实例列表的权限。	list	-	-	-
dds:instance:getUpgradeDuration	授予查询数据库补丁升级预估时长的权限。	read	instance	-	-
dds:instance:getDiskUsage	授予查询磁盘使用率的权限。	read	instance	-	-
dds:configuration:listAppliedHistory	授予查询参数模板被应用历史的权限。	list	-	-	-
dds:configuration:listUpdatedHistory	授予查询参数模板修改历史的权限。	list	-	-	-
dds:configuration:compare	授予比较两个参数模板之间差异的权限。	read	-	-	-
dds:configuration:copy	授予复制参数模板的权限。	write	-	-	-
dds:configuration:reset	授予重置参数模板的权限。	write	-	-	-
dds:instance:getSslCertDownloadAddress	授予获取下载 ssl 证书地址的权限。	read	instance	-	-
dds:instance:addNode	授予扩容实例节点数量的权限。	write	instance	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dds:instance:deleteEnlargeFailedNode	授予删除扩容失败的实例节点的权限。	write	instance	-	-
dds:task:listAll	授予查询任务列表的权限。	list	-	-	-
dds:task:getDetail	授予查询任务详情的权限。	read	-	-	-
dds:instance:restart	授予重启数据库实例的权限。	write	instance	-	-
dds:instance:deleteAuditLog	授予删除审计日志的权限。	write	instance	-	-
dds:instance:delete	授予删除数据库实例的权限。	write	instance	-	-
dds:instance:updateName	授予修改实例名称的权限。	write	instance	-	-
dds:instance:updateRemark	授予修改实例备注的权限。	write	instance	-	-
dds:instance:setTag	授予批量添加或删除指定实例标签的权限。	tagging	instance	-	-
dds:instance:listTags	授予查询指定实例的标签信息的权限。	read	-	-	-
dds:instance:setBackupPolicy	授予设置自动备份策略的权限。	write	-	dds:BackupEnabled	-
dds:instance:getBackupPolicy	授予查询自动备份策略	read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	的权限。				
dds:configuration:create	授予创建参数组的权限。	write	-	g:EnterpriseProjectId	-
dds:instance:setSlowLogPlaintextStatus	授予切换慢日志明文显示开关的权限。	permission_management	instance	-	-
dds:instance:getSlowLogPlaintextStatus	授予查看慢日志明文开关状态的权限。	read	instance	-	-
dds:instance:downloadAuditLog	授予下载审计日志的权限。	read	instance	-	-
dds:instance:create	授予创建数据库实例的权限。	write	-	dds:Encrypted dds:BackupEnabled	-
dds:instance:restore	授予备份恢复原实例的权限。	write	-	-	-
dds:backup:getRestoreTimeList	授予查询实例可恢复时间段的权限。	read	-	-	-
dds:backup:getRestoreCollections	授予获取可恢复的数据库集合列表的权限。	list	-	-	-
dds:backup:getRestoreDatabases	授予获取可恢复的数据库列表的权限。	list	-	-	-
dds:instance:getConnectionStatistics	授予查询实例连接数统计信息的权限。	read	instance	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dds:instance:getQuotas	授予查询配额的权限。	read	-	-	-
dds:instance:createDatabaseUser	授予创建数据库用户的权限。	write	instance	-	-
dds:instance:getDatabaseUser	授予查询数据库用户列表的权限。	read	instance	-	-
dds:instance:deleteDatabaseUser	授予删除数据库用户的权限。	write	instance	-	-
dds:instance:createDatabaseRole	授予创建数据库角色的权限。	write	instance	-	-
dds:instance:deleteDatabaseRole	授予删除数据库角色的权限。	write	instance	-	-
dds:instance:getDatabaseRole	授予查询数据库角色列表的权限。	read	instance	-	-
dds:instance:setSourceSubnet	授予网段配置的权限。	write	instance	-	-
dds:instance:upgradeDatabaseVersion	授予升级数据库版本的权限。	write	instance	-	-
dds:backup:create	授予创建数据库实例手动备份的权限。	write	-	-	-
dds:instance:deleteSession	授予删除节点会话的权限。	write	-	-	-
dds:instance:listSession	授予查询节点会话列表的权限。	list	-	-	-
dds:instance:getShardingBal	授予查询集群实例负载	read	instance	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ancer	均衡的权限。				
dds:instance:setShardingBalancer	授予设置集群实例负载均衡的权限。	write	instance	-	-
dds:instance:setBalancerWindow	授予设置集群均衡活动时间窗的权限。	write	instance	-	-
dds:instance:updateOpsWindow	授予设置实例可维护时间窗的权限。	write	instance	-	-
dds:instance:listFlavors	授予查询规格列表的权限。	read	-	-	-
dds:instance:listStorageType	授予查询数据库磁盘类型的权限。	read	-	-	-
dds:instance:listDatabaseVersion	授予查询数据库版本信息的权限。	read	-	-	-
dds:tag:listAll	授予查询项目下所有标签信息的权限。	list	-	-	-
dds:instance:reduceNode	授予缩容集群实例的节点数量的权限。	write	instance	-	-
dds:instance:createDomainName	授予创建DNS 的权限。	write	-	-	-
dds:instance:updateDomainName	授予修改DNS 名称的权限。	write	-	-	-
dds:instance:updateReplicaS	授予修改数据库复制集	write	instance	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
etName	名称的权限。				
dds:instance:getDetail	授予查询实例详情的权限。	read	instance	-	-
dds:instance:getNodeList	授予查询实例节点列表的权限。	read	instance	-	-
dds:instance:updateTag	授予修改实例标签的权限。	tagging	instance	-	-
dds:instance:deleteTag	授予删除实例标签的权限。	tagging	instance	-	-
dds:backup:get	授予查询备份信息的权限。	read	-	-	-
dds:offsiteBackup:listRegion	授予获取指定实例异地备份区域的权限。	read	-	-	-
dds:offsiteBackup:listInstance	授予获取异地备份实例的权限。	read	-	-	-
dds:offsiteBackup:listAll	授予获取异地备份列表的权限。	read	-	-	-
dds:instance:saveLogConfig	授予批量保存日志配置的权限。	write	-	-	-
dds:instance:deleteLogConfig	授予批量删除日志配置的权限。	write	-	-	-

DDS 的 API 通常对应着一个或多个授权项。表 3-109 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

 版权所有 © 华为云计算技术有限公司

表3-109 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/instances	dds:instance:create vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get vpc:ports:get	-
GET /v3/{project_id}/instances?id={id}&name={name}&mode={mode}&datastore_type={datastore_type}&vpc_id={vpc_id}&subnet_id={subnet_id}&offset={offset}&limit={limit}	dds:instance:listAll	-
DELETE /v3/{project_id}/instances/{instance_id}	dds:instance:delete	-
POST /v3/{project_id}/instances/{instance_id}/restart	dds:instance:restart	-
POST /v3/{project_id}/instances/{instance_id}/enlarge-volume	dds:instance:extendVolume	-
POST /v3/{project_id}/instances/{instance_id}/enlarge	dds:instance:addNode vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get vpc:ports:get	-
POST /v3/{project_id}/instances/{instance_id}/resize	dds:instance:updateSpec	-
POST /v3/{project_id}/instances/{instance_id}/switchover	dds:instance:switchover	-
POST/v3/{project_id}/instances/{instance_id}/switch-ssl	dds:instance:setSSL	-
PUT /v3/{project_id}/instances/{instance_id}/modify-name	dds:instance:updateName	-
POST /v3/{project_id}/instances/{instance_id}/modify-port	dds:instance:updatePort	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/instances/{instance_id}/modify-security-group	dds:instance:updateSecurityGroup	-
POST /v3/{project_id}/nodes/{node_id}/bind-eip	dds:instance:bindEIP	-
POST /v3/{project_id}/nodes/{node_id}/unbind-eip	dds:instance:unbindEIP	-
POST /v3/{project_id}/instances/{instance_id}/modify-internal-ip	dds:instance:updateIp	-
POST /v3/{project_id}/instances/{instance_id}/create-ip	dds:instance:createIp	-
GET /v3/{project_id}/instances/{instance_id}/migrate/az	dds:instance:listMigrateAz	-
POST /v3/{project_id}/instances/{instance_id}/migrate	dds:instance:migrateAz	-
GET /v3/{project_id}/nodes/{node_id}/sessions	dds:instance:lisSession	-
POST /v3/{project_id}/nodes/{node_id}/session	dds:instance:deleteSession	-
GET /v3/{projectId}/instances/{instance_id}/conn-statistics	dds:instance:getConnectionStatistics	-
POST /v3/{project_id}/backups	dds:backup:create	-
DELETE /v3/{project_id}/backups/{backups_id}	dds:backup:delete	-
GET /v3/{project_id}/backups?instance_id={instance_id}&backup_id={backup_id}&backup_type={backup_type}&offset={offset}&limit={limit}&begin_time={begin_time}&end_time={end_time}&mode={mode}	dds:backup:listAll	-
GET /v3/{project_id}/instances/{instance_id}/backups/policy	dds:instance:getBackupPolicy	-
PUT /v3/{project_id}/instances/{instance_id}/backups/policy	dds:instance:setBackupPolicy	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/instances	dds:instance:create vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get vpc:ports:get	-
GET /v3/{projectId}/backups/download-file	dds:backup:download	-
GET /v3/{project_id}/instances/{instance_id}/restore-time	dds:backup:getRestoreTimeList	-
GET /v3/{project_id}/instances/{instance_id}/restore-database	dds:backup:getRestoreDatabases	-
GET /v3/{project_id}/instances/{instance_id}/restore-collection	dds:backup:getRestoreCollections	-
POST /v3/{project_id}/instances/recovery	dds:backup:restore	-
POST /v3/{project_id}/instances/{instance_id}/restore/collections	dds:backup:restore	-
GET /v3/{project_id}/configurations	dds:configuration:listAll	-
PUT /v3/{project_id}/configurations	dds:configuration:create	-
DELETE /v3/{project_id}/configurations/{config_id}	dds:configuration:delete	-
GET /v3/{projectId}/configurations/{configId}	dds:configuration:get	-
PUT /v3/{project_id}/configurations/{config_id}	dds:configuration:update	-
PUT /v3/{project_id}/configurations/{config_id}/apply	dds:instance:applyConfiguration	-
GET /v3/{project_id}/instances/{instance_id}/configurations	dds:instance:getConfiguration	-
PUT /v3/{project_id}/instances/{instance_id}/configurations	dds:instance:updateConfiguration	-
GET /v3/{project_id}/instances/{instance_id}/slowlog	dds:instance:listSlowLog	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/instances/{instance_id}/slowlog-download	dds:instance:downloadSlowLog	-
GET /v3/{project_id}/instances/{instance_id}/errorlog	dds:instance:listErrorLog	-
POST /v3/{project_id}/instances/{instance_id}/errorlog-download	dds:instance:downloadErrorLog	-
POST /v3/{project_id}/instances/{instance_id}/auditlog-policy	dds:instance:setAuditLogPolicy	-
GET /v3/{project_id}/instances/{instance_id}/auditlog-policy	dds:instance:getAuditLogPolicy	-
GET /v3/{project_id}/instances/{instance_id}/auditlog	dds:instance:listAuditLog	-
POST /v3/{project_id}/instances/{instance_id}/auditlog-links	dds:instance:downloadAuditLog	-
POST /v3/{project_id}/instances/{instance_id}/tags/action	dds:instance:setTag	-
GET /v3/{project_id}/instances/{instance_id}/tags	dds:instance:listTags	-
POST /v3/{project_id}/instances/{instance_id}/db-user	dds:instance:createDatabaseUser	-
POST /v3/{project_id}/instances/{instance_id}/db-role	dds:instance:createDatabaseRole	-
DELETE /v3/{project_id}/instances/{instance_id}/db-user	dds:instance:deleteDatabaseUser	-
DELETE /v3/{project_id}/instances/{instance_id}/db-role	dds:instance:deleteDatabaseRole	-
PUT /v3/{project_id}/instances/{instance_id}/reset-password	dds:instance:resetPasswd	-
GET /v3/{project_id}/instances/{instance_id}/db-	dds:instance:getDatabase	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
user/detail? offset ={offset}&limit={limit}&user_name={user_name }&db_name={db_name}	User	
GET /v3/{project_id}/instances/{instance_id}/db-roles?role_name={role_name}&db_name={db_name}&offset={offset}&limit={limit}	dds:instance:getDatabaseRole	-
GET /v3/{project_id}/instances/{instance_id}/balancer	dds:instance:getShardingBalancer	-
PUT /v3/{project_id}/instances/{instance_id}/balancer/{action}	dds:instance:setShardingBalancer	-
PUT /v3/{project_id}/instances/{instance_id}/balancer/active-window	dds:instance:setBalancerWindow	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 9 DDS 支持的资源类型中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的策略语句中指定该资源的 URN，策略仅作用于此资源；如未指定，Resource 默认为“*”，则策略将应用到所有资源。您也可以在策略中设置条件，从而指定资源类型。

DDS 定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-110 DDS 支持的资源类型

资源类型	URN	条件键
instanceName	dds:<region>:<account-id>:instanceName:<instance-name>	- g:EnterpriseProjectId - g:ResourceTag/<tag-key>

条件（Condition）

条件键（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀为服务缩写，如 DDS:）仅适用于对应服务的操作，详情请参见表 3-111。

 版权所有 © 华为云计算技术有限公司

- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

DDS 定义了以下可以在 IAM 自定义策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化策略语句应用的条件。

表3-111 DDS 支持的服务级条件键

服务级条件键	类型	说明
dds:Encrypted	boolean	按照请求参数中传递的是否开启磁盘加密标签键筛选访问权限。
dds:BackupEnabled	boolean	按照请求参数中传递的是否开启备份策略标签键筛选访问权限。

3.6.4 数据复制服务 DRS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员帐号时，并没有直接对组织单元或成员帐号授予操作权限，而是规定了成员帐号或组织单元包含的成员帐号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考。

操作（Action）

操作（Action）即为 IAM 自定义策略中支持的操作项，在 IAM 自定义策略中的 Action 中写入授权项，可以实现授权项对应的权限功能。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在策略中使用操作时，相应操作授予的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。

 版权所有 © 华为云计算技术有限公司

- 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

关于 DRS 定义的资源类型的详细信息请参见资源类型（Resource）。

- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该操作项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该操作项资源类型列没有值（-），则表示条件键对整个操作项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 DRS 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 DRS 的相关操作。

表3-112 DRS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
drs:backupMigrationJob:createJob	授予创建离线迁移任务的权限。	write	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys	drs:backupMigrationJob:create
drs:backupMigrationJob:deleteJob	授予删除离线迁移任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:backupMigrationJob:delete
drs:backupMigrationJob:getJobDetail	授予查询离线迁移任务详细信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:backupMigrationJob:get
drs:backupMigrationJob:modifyOfflineTaskInfo	授予修改离线迁移任务信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:backupMigrationJob:modify
drs:cloudDataGuardJob:getChartMonitor	授予查询报表图的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:disasterRecoveryJob:get
drs:cloudDataGuardJob:getDataGuardMonitor	授予查询容灾监控数据的权限。	list	job	g:EnterpriseProjectId g:ResourceTa	drs:disasterRecoveryJob:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				g/<tag-key>	
drs:cloudDataGuardJob:getLastDataDisplay	授予查询灾备最后数据的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:dataGuardJob:list
drs:cloudDataGuardJob:getRpoAndRto	授予查询指定任务的 RPO 和 RTO 的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:dataGuardJob:list
drs:compareJob:createDataCompareJob	授予创建数据级表对比任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationCompareJob:create
drs:compareJob:createObjectCompareJob	授予创建对象级表对比任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationCompareJob:create
drs:compareJob:deleteDataCompareJob	授予取消数据级表对比任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationCompareJob:delete
drs:migrationJob:getTopicInfo	授予查询已创建全部主题信息的权限。	list	-	-	drs:migrationJob:get
drs:migrationJob:listAllSmnInfo	授予查询已录入全部信息的权限。	list	-	-	drs:migrationJob:get
drs:configuration:getPublicIp	授予查询 EIP 列表或者 Eip 信息的权限。	list	-	-	drs:migrationJob:get
drs:configuration:getVpcs	授予查询 VPC 列表的权限。	list	-	-	drs:migrationJob:get
drs:configuration:listSubnets	授予查询子网列表的权限。	list	-	-	drs:migrationJob:get
drs:configuration:getFeatures	授予查询特性白名单的权	list	-	-	drs:featureWhiteJob:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
drs:configuration:addTag	授予添加资源标签的权限。	tagging	-	-	drs:tag:add
drs:compareJob:exportAccountCompareResult	授予导出并下载用户比对任务比对结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:compareJob:list
drs:compareJob:exportCompareReport	授予下载比对结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:compareJob:list
drs:configuration:getInstancesTag	授予批量查询资源标签的权限。	list			drs:tag:get
drs:compareJob:exportContentsCompareResult	授予导出内容比对任务比对结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:compareJob:list
drs:configuration:getProjectTags	授予查询项目标签的权限。	list	-	-	drs:tag:get
drs:compareJob:exportLinesCompareResult	授予导出行比对任务比对结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:compareJob:list
drs:compareJob:exportObjectsCompareResult	授予导出对象比对任务比对结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:compareJob:list
drs:compareJob:getAccountCompare	授予查询账户对比概览的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:compareJob:getOverview
drs:compareJob:getAccountCompareDetail	授予查询账户对比详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:healthCompareJob:getAccountDetails
drs:compareJob:getA	授予查询账户	list	job	g:EnterpriseP	drs:CompareJob

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ccountCompareDetails	对比详情的权限。			rojectId g:ResourceTag/<tag-key>	:getAccountDetails
drs:subscriptionJob:exportJobs	授予导出订阅任务列表的权限。	list	-	-	drs:subscriptionJob:get
drs:compareJob:getAccountDetails	授予查询行对比总览的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:healthCompareJob:getAccountDetails
drs:compareJob:getCompareJobEstimatedTime	授予查询对比预估时间的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:CompareJob:getEstimateTime
drs:compareJob:getComparePolicy	授予查询对比策略的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:healthPolicyCompare:list
drs:subscriptionJob:listJobs	授予查询订阅任务列表的权限。	list			drs:subscriptionJob:get
drs:compareJob:getContentCompare	授予查询内容对比总览的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:CompareJob:getContentOverview
drs:compareJob:getContentCompareDetail	授予查询内容对比详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:CompareJob:getContentDetail
drs:compareJob:getContentCompareDiff	授予查询内容对比差异的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:CompareJob:getContentDiff
drs:compareJob:getDataCompareDetail	授予查询行对比详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:healthCompareJob:getLineDetail
drs:compareJob:getD	授予查询数据	list	job	g:EnterpriseP	drs:CompareJob

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ataCompareResult	级表对比任务结果的权限。			rojectId g:ResourceTag/<tag-key>	:getResult
drs:compareJob:getFlowObjectsCompare	授予查询动态对象级迁移对比概览的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:getCompareStruct
drs:compareJob:getHealthCompareJobDetail	授予查询健康对比任务详情信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:healthCompareJob:list
drs:compareJob:getLineCompare	授予查询行对比总览的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:CompareJob:getLineOverview
drs:compareJob:getLineCompareDetail	授予查询行对比详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:CompareJob:getLineDetail
drs:compareJob:getObjectCompare	授予根据对比任务 ID 查询对象级迁移对比概览的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:healthCompareJob:getOverview
drs:compareJob:getObjectsCompareDetail	授予查询对象级对比详细信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:healthCompareJob:getLineDetail
drs:compareJob:getObjectsMigrateCompare	授予根据任务 ID 查询对象级迁移对比概览的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:CompareJob:list
drs:compareJob:getObjectsMigrateCompareDetail	授予查询对象级迁移对比详细信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:CompareJob:getDetails
drs:compareJob:getTableCompareDetail	授予查询数据级表对比任务	list	job	g:EnterpriseProjectId	drs:CompareJob:getContentsInf

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	详情的权限。			g:ResourceTag/<tag-key>	o
drs:compareJob:listDataCompare	授予查询数据级表对比任务列表的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:CompareJob:list
drs:compareJob:listHealthCompareJobs	授予查询健康对比报告列表的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:healthCompareJob:list
drs:compareJob:modifyComparePolicy	授予修改对比策略的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:healthCompare:modify
drs:compareJob:startJob	授予立即启动数据级表对比任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationCompareJob:start
drs:compareJob:stopJob	授予停止对比任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:healthCompare:stop
drs:configuration:addDataTransformationInfo	授予添加数据加工的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:dataTransformation:add
drs:configuration:batchModifyTag	授予批量添加修改资源标签的权限。	tagging	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys	drs:tags:delete
drs:configuration:batchReplaceTags	授予批量重置资源标签的权限。	tagging	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key>	drs:tags:delete

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				g:TagKeys	
drs:configuration:checkDataTransformationInfo	授予校验数据加工信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:dataTransformation:check
drs:configuration:deleteDataTransformationInfo	授予删除数据加工数据的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:dataTransformation:delete
drs:configuration:deleteSmnInfo	授予删除已录入单个信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:action
drs:configuration:deleteSmnInfoForTopic	授予删除已录入单个主题信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:action
drs:configuration:deleteTag	授予删除资源标签的权限。	tagging	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys	drs:tags:delete
drs:configuration:downloadTemplate	授予导入对象信息前下载Excel 模板的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:configuration:getAddColumns	授予查询数据加工信息(多表归一 加多个列)的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationTransformationJob:get
drs:configuration:getAddColumnsFromDb	授予查询数据加工信息(多表归一 加多个列)-任务启动后查询的权	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationTransformationJob:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
drs:configuration:getFlavorInfo	授予查询引擎的规格信息的权限。	list	-	-	drs:flavors:get
drs:backupMigrationJob:checkOfflineTaskName	授予校验离线迁移任务名称的权限。	write	-	-	drs:backupMigrationJob:check
drs:configuration:getColumnInfo	授予查询对象的列信息（列映射、列过滤）的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:configuration:getDatabaseName	授予查询目标库名称的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:configuration:getDatabaseParams	授予查询数据库参数的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:databaseParameters:get
drs:backupMigrationJob:exportJobList	授予导出离线迁移任务列表的权限。	list	-	-	drs:backupMigrationJob:list
drs:backupMigrationJob:getBackupFileDbList	授予查询备份文件数据库列表的权限。	list	-	-	drs:backupMigrationJob:get
drs:configuration:getDataTransformationData	授予查询数据加工数据的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationTransformationJob:get
drs:backupMigrationJob:getRedisInstList	授予查询Redis 数据库实例列表的权限。	list	-	-	drs:backupMigrationJob:get
drs:backupMigrationJob:listBuckets	授予查询桶列表的权限。	list	-	-	drs:backupMigrationJob:get
drs:backupMigration	授予查询离线	list	-	-	drs:backupMigr

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
Job:listJobs	迁移任务列表的权限。				ationJob:list
drs:backupMigrationJob:listObsObject	授予查询当前桶对象列表的权限。	list	-	-	drs:backupMigrationJob:get
drs:configuration:getDataTransformationInfo	授予查询数据加工信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationTransformationJob:get
drs:configuration:listFeature	授予查询支持特性列表的权限。	list	-	-	drs:supportFeature:get
drs:configuration:listLinks	授予查询可用链路信息的权限。	list	-	-	drs:supportFeature:get
drs:configuration:getEffectTime	授予查询指定任务数据库影响时间的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:getEffectTime
drs:configuration:getESConfig	授予查询ElasticSearch的配置信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:configuration:getInstanceTag	授予查询资源标签的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:tag:get
drs:configuration:getSupportDataTransformationType	授予查询数据加工数据类型的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationTransformationJob:get
drs:configuration:getTableInfo	授予查询表结构和表数据的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:configuration:importSmnInfo	授予录入收件方式与信息的	write	job	g:EnterpriseProjectId	drs:migrationJob:action

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	权限。			g:ResourceTag/<tag-key>	
drs:configuration:listTopics	授予查询涉及到的 kafka 的 topic 信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:kafkaJob:get
drs:configuration:modifyDatabaseParams	授予修改数据库参数的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:dataBaseParams:modify
drs:configuration:modifyESConfig	授予修改 ElasticSearch 的配置信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:configuration:modifySmnInfo	授予修改收件方式与信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:action
drs:configuration:modifyTag	授予修改资源标签的权限。	tagging	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys	drs:tag:modify
drs:configuration:modifyUserInfo	授予更新迁移用户信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:modifyUserInfo
drs:configuration:setMigrationTransSpeed	授予设置迁移速度的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:setMigrationTransSpeed
drs:configuration:getInstanceNum	授予查询任务数量的权限。	list	-	-	drs:instances:list
drs:configuration:getInstanceQuotas	授予查询配额的权限。	list	-	-	drs:quota:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
drs:configuration:getQuota	授予查询租户在 DRS 服务下的配额信息的权限。	list	-	-	drs:quota:get
drs:migrationJoAb:batchDeleteJobs	授予批量结束或删除任务的权限。	write	-	-	drs:migrationJobs:delete
drs:configuration:updateDataTransformationInfo	授予更新数据加工信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:dataTransformation:update
drs:migrationJob:addSubscribeJob	授予创建包周期订购的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:action
drs:migrationJob:associateSmnInfo	授予关联管控主题信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:action
drs:migrationJob:batchPauseJob	授予批量暂停任务的权限。	write	-	-	drs:migrationJob:action
drs:migrationJob:batchPreCheckJob	授予批量预检查的权限。	write	-	-	drs:migrationJob:action
drs:migrationJob:batchRetryJob	授予重试任务的权限。	write	-	-	drs:migrationJob:action
drs:migrationJob:batchSetTransformation	授予加工同步对象的权限。	write	-	-	drs:migrationJob:action
drs:migrationJob:batchStartJob	授予批量启动任务的权限。	write	-	-	drs:migrationJob:action
drs:migrationJob:batchTestClusterConnection	授予批量测试连接（集群模式）的权限。	write	-	-	drs:migrationJobs:connect
drs:migrationJob:batchTestConnection	授予批量测试连接的权限。	write	-	-	drs:migrationJobs:connect
drs:migrationJob:downloadBatchCreateT	授予下载批量创建任务模板	list	-	-	drs:migrationJo

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
emplate	的权限。				b:get
drs:migrationJob:importBatchCreateJobs	授予导入批量创建任务的权限。	write	-	-	drs:migrationJobs:create
drs:migrationJob:listAsyncJobDetail	授予查询租户指定 ID 批量异步任务详情的权限。	list	-	-	drs:migrationJob:get
drs:migrationJob:listAsyncJobs	授予查询批量异步创建任务列表的权限。	list	-	-	drs:migrationJob:get
drs:migrationJob:listJobInfo	授予根据任务 ID 批量查询任务详情的权限。	list	-	-	drs:migrationJob:get
drs:migrationJob:listJobStatus	授予根据任务 ID 批量查询任务状态的权限。	list	-	-	drs:migrationJob:get
drs:migrationJob:asyncBatchCreateJobByAsyncId	授予批量异步创建任务的权限。	write	job	drs:netTypeg:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys	drs:migrationJob:action
drs:migrationJob:getJobList	授予查询租户任务列表的权限。	list	-	-	drs:migrationJob:get
drs:migrationJob:listPrecheckResult	授予查询批量任务的预检查结果的权限。	list	-	-	drs:migrationJob:get
drs:migrationJob:selectDatabaseObject	授予选择需要迁移的数据库或者表的权限。	write	-	-	drs:migrationJobs:select
drs:configuration:list	授予查询企业	list	-	-	drs:tag:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
EPs	项目的权限。				
drs:migrationJob:asyncBatchSaveJob	授予批量异步保存任务信息的权限。	write	job	drs:netTypeg:EnterpriseProjectIdg:RequestTag/<tag-key>g:TagKeys	drs:migrationJobs:create
drs:migrationJob:asyncBatchUpdateJobByAsyncId	授予批量异步更新租户指定ID任务详情的权限。	write	job	drs:netTypeg:EnterpriseProjectIdg:RequestTag/<tag-key>g:ResourceTag/<tag-key>g:TagKeys	drs:migrationJob:action
drs:migrationJob:batchCreateJob	授予批量同步创建任务的权限。	write	job	drs:netTypeg:EnterpriseProjectIdg:RequestTag/<tag-key>g:TagKeys	drs:migrationJobs:create
drs:migrationJob:changeFlavor	授予创建规格变更的权限。	write	job	g:EnterpriseProjectIdg:ResourceTag/<tag-key>	drs:migrationJob:action
drs:migrationJob:getCesJobs	授予查询迁移任务列表的权限。	list	-	-	drs:migrationJob:list
drs:migrationJob:changeFlavorByNeed	授予按需页面进行node规格变更的权限。	write	job	g:EnterpriseProjectIdg:ResourceTag/<tag-key>	drs:migrationJob:modify
drs:compareJob:createJob	授予创建对比任务的权限。	write	-	-	drs:migrationCompareJob:create
drs:migrationJob:checkInheritJob	授予判断任务能否继承的权限。	write	job	g:EnterpriseProjectIdg:ResourceTa	drs:migrationJob:check

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				g/<tag-key>	
drs:migrationJob:checkRestartPoint	授予检查跳跃续传位点的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:check
drs:migrationJob:checkTableExist	授予查询表结构和表数据是否存在的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:copyJobAction	授予复制任务下发动作的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:check
drs:migrationJob:createJob	授予创建在线迁移任务的权限。	write	job	drs:netType g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys	drs:migrationJob:create
drs:migrationJob:createJobs	授予创建任务的权限。	write	job	drs:netType g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys	drs:migrationJobs:create
drs:migrationJob:deleteColumnInfo	授予删除对象的列信息（列映射、列过滤）的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:deleteJob	授予删除在线迁移任务 V1 的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:delete
drs:migrationJob:downloadDbObjectTemplate	授予下载对象选择模板的权限。	read	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
drs:migrationJob:endJob	授予结束在线迁移任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:terminate
drs:migrationJob:exportAddedDeletedObjectsInfo	授予导出增删的对象信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:compareJob:getCompareResult	授予查询对比结果的权限。	list	-	-	drs:CompareJob:getResult
drs:migrationJob:exportErrorInfo	授予导出错误信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:migrationJob:exportObjectsSentInfo	授予导出已经下发的对象信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:migrationJob:getAccess	授予查询指定任务允许操作信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:getAggregationTable	授予查询内存中多表映射信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:getCesJob	授予查询迁移任务的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:getDbObjectCollectionStatus	授予获取提交查询数据库对象信息的结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:getDbObjects	授予查询数据库对象信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
drs:migrationJob:getDbObjectsCollectAsync	授予提交查询数据库对象信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:getDbObjectTemplateProgress	授予查询对象选择导入进度的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:migrationJob:getDbObjectTemplateResult	授予获取对象选择导入结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:migrationJob:getFullJobDetails	授予查询全量同步的详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:migrationJob:getImportExcelProcess	授予查询解析 excel 的进度的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:migrationJob:getIncreComponentsDetails	授予查询增量组件的详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:migrationJob:getJob	授予查询在线迁移任务详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:getJobDetail	授予查询任务详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:getJobMeteringPrice	授予查询任务价格信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:MigrationJob:getMeteringPrice
drs:migrationJob:getObjectHasColumn	授予查询有列信息（列映	list	job	g:EnterpriseProjectId	drs:migrationJob:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	射、列过滤）的对象的权限。			g:ResourceTag/<tag-key>	
drs:migrationJob:getObjectsCompareOverviewa	授予查询数据级流式对比的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:getStreamComparison
drs:migrationJob:getObjectSelectInfo	授予查询任务对象选择信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:getOperationInfo	授予查询指定任务操作统计信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:getProgress	授予查询指定任务迁移进度的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:getSpecifiedProgress
drs:configuration:listDatabaseParams	授予查询源库和目标库的数据库参数的权限。	list	-	-	drs:databaseParameters:get
drs:migrationJob:getSmnInfo	授予查询已录入单个信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:getSmnInfoForTopic	授予查询已录入单个主题信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:getSrcUsers	授予查询源库迁移用户列表的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:getSrcUsers
drs:configuration:getOpenStreamResult	授予查询开启流结果的权限。	list	-	-	drs:migrationTransformationJob:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
drs:migrationJob:getSupportObject	授予查询任务是否支持对象选择/列映射等的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:getSupportSearchObjectType	授予查询任务支持查询用户选择对象的类型的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:getSwitchVipStatus	授予查询 VIP 倒换结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:batchDeleteJob	授予批量删除任务的权限。	write	-	-	drs:migrationJob:delete
drs:migrationJob:batchOperateJob	授予批量操作租户指定 ID 任务的权限。	write	-	-	drs:migrationJob:action
drs:migrationJob:getTaskLog	授予获取迁移日志的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:getLog
drs:migrationJob:getTuningParams	授予查询调优参数的值的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:migrationJob:checkAction	授予校验任务名称的权限。	write	-	-	drs:migrationJob:check
drs:migrationJob:getUpdateObjectSavingStatus	授予获取对象保存进度的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:getUserSelectedObjectInfo	授予查询用户选择的同步映射关系的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:cloneJobs	授予克隆 mysql 同步任	write	-	-	drs:migrationJob:create

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	务的权限。				
drs:migrationJob:getUserSetObjectInfo	授予查询已同步的对象信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:jobAction	授予执行任务特定的操作的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:action
drs:migrationJob:jobUpdateAction	授予任务、抓取和回放的启停操作的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:migrationJob:exportJobs	授予导出在线迁移任务列表的权限。	list	-	-	drs:migrationJob:list
drs:migrationJob:listJobs	授予查询租户任务列表的权限。	list	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys	drs:migrationJob:list
drs:migrationJob:getBatchTaskLog	授予批量获取迁移日志的权限。	list	-	-	drs:migrationJob:getLog
drs:migrationJob:getCountdown	授予查询云服务倒计时信息的权限。	list	-	-	drs:migrationJob:get
drs:migrationJob:getDrsJobByRdsInstanceId	授予查询 rds 实例相关的迁移任务的权限。	list	-	-	drs:migrationJob:list
drs:migrationJob:listJobs		list	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys	
drs:migrationJob:list	授予查询回放	list	job	g:EnterpriseP	drs:replayFaults

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ReplayFaultsJobs	故障列表的权限。			rojectId g:ResourceTag/<tag-key>	Job:list
drs:migrationJob:modifyColumnInfo	授予修改对象的列信息（列映射、列过滤）的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:modifyCommonSetting	授予更新任务配置的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:updateJobConfig
drs:migrationJob:modifyConflictPolicy	授予更新同步任务忽略策略的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:synchronizationJob:update
drs:migrationJob:getJobs	授予查询在线迁移任务列表的权限。	list	-	-	drs:migrationJob:list
drs:migrationJob:getNodeNumByDDMInstance	授予根据 ddm sharding 个数计算对应子任务数量的权限。	list	-	-	drs:migrationJob:get
drs:migrationJob:modifyGroupAndStream	授予开启或者关闭对接 LTS 服务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:migrationJob:getPrecheckResult	授予查询迁移任务预检查结果的权限。	list	-	-	drs:precheckJob:get
drs:migrationJob:modifyIncreStartPosition	授予更新增量任务的启动位点的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:updateJobConfig
drs:migrationJob:getResourceInstances	授予查询资源实例以及关联资源信息的权限。	list	-	-	drs:migrationJob:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
drs:migrationJob:modifyJob	授予修改在线迁移任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:modify
drs:migrationJob:modifySyncTypePolicy	授予更新同步类型策略的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:create
drs:migrationJob:getSubscribeNumber	授予查询包周期订购规格信息的权限。	list	-	-	drs:migrationJob:get
drs:migrationJob:operateJobByJobId	授予操作租户指定 ID 任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:action
drs:migrationJob:selectGroupAndStream	授予查询用户当前任务是否开启 lts 服务的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:migrationJob:sendImportCheck	授予上传 excel 文件的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:migrationJob:switchVip	授予双 VIP 倒换的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:action
drs:migrationJob:updateDDLPolicy	授予更新过滤 DDL 策略的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:updateDDLPolicy
drs:migrationJob:listProgressInfo	授予根据任务 ID 批量查询迁移进度、增量时延信息的权限。	list	-	-	drs:migrationJobs:getProgress
drs:migrationJob:updateJobInfo	授予更新租户指定 ID 任务	write	job	g:EnterpriseProjectId	drs:migrationJob:update

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	详情的权限。			g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys	
drs:migrationJob:updateObjectInfo	授予更新数据库对象选择信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:migrationJob:updateTuningParams	授予修改调优参数的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:migrationJob:uploadDbObjectTemplate	授予对象选择导入数据的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:update
drs:replayJob:downloadReport	授予下载流量回放相关文件的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:compareJob:list
drs:replayJob:exportAbnormalSqlData	授予下载流量回放异常SQL 的权限。	list	job	drs:netType g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys	drs:supportFeature:get
drs:migrationJob:resourceCheck	授予创建在线迁移任务资源检查的权限。	write	-	-	drs:migrationJob:create
drs:migrationJob:skipPrecheck	授予跳过预检查的权限。	write	-	-	drs:migrationJob:check
drs:replayJob:exportSlowSqlData	授予导出流量回放 SQL 的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:supportFeature:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
drs:replayJob:getAbnormalSqlData	授予查询流量回放异常量SQL 的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:supportFeature:get
drs:replayJob:getAllSqlFile	授予查询流量回放全量SQL 文件的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:supportFeature:get
drs:replayJob:getExecuteResultData	授予查询流量回放结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:supportFeature:get
drs:replayJob:getExportSlowSqlStatus	授予查询流量回放文件导出状态的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:supportFeature:get
drs:replayJob:getReplayErrorTemplate	授予查询异常sql 模板的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:supportFeature:get
drs:replayJob:getReplayFile	授予查询流量回放文件的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:supportFeature:get
drs:cloudDataGuardJob:getMonitoringData	授予根据任务ID 查询容灾监控数据的权限。	list	-	-	drs:disasterRecoveryJob:get
drs:cloudDataGuardJob:batchSwitchover	授予批量主备倒换的权限。	write	-	-	drs:disasterRecoveryJob:switchover
drs:cloudDataGuardJob:listJobInfo	授予根据任务ID 批量查询灾备初始化对象详情的权限。	list	-	-	drs:disasterRecoveryJob:get
drs:cloudDataGuardJob:listRpoAndRto	授予批量查询RPO 和 RTO	list	-	-	drs:dataGuardJob:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	的权限。				
drs:cloudDataGuardJob:listStructProcess	授予根据任务ID批量查询灾备初始化进度的权限。	list	-	-	drs:disasterRecoveryJob:get
drs:migrationJob:batchSetSmn	授予批量设置告警信息的权限。	write	-	-	drs:migrationJob:action
drs:migrationJob:batchSetSpeedLimit	授予批量设置任务限速的权限。	write	-	-	drs:migrationJobs:update
drs:migrationJob:batchUpdateDefinerMigrateSetting	授予批量设置Definer迁移是否迁移到到该用户下的权限。	write	-	-	drs:migrationJob:updateJobConfig
drs:migrationJob:batchUpdateJobInfo	授予批量修改任务名称或描述，设置异常通知信息的权限。	write	-	-	drs:migrationJob:modify
drs:migrationJob:batchUpdateUserMigrate	授予批量设置需要迁移的用户和角色的权限。	write	-	-	drs:migrationJob:modifyUserInfo
drs:migrationJob:changeSrcOrTargetPwd	授予修改任务源或目标数据库密码的权限。	write	-	-	drs:migrationJobs:update
drs:migrationJob:setBatchSyncPolicy	授予批量设置同步策略的权限。	write	-	-	drs:migrationJobs:add
drs:replayJob:getReplayRecord	授予查询流量报告的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:supportFeature:get
drs:replayJob:getRep	授予查询慢	list	job	g:EnterpriseP	drs:supportFeat

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
laySlowTemplate	sql 模板的权限。			rojectId g:ResourceTag/<tag-key>	ure:get
drs:replayJob:getSlowSqlData	授予查询流量回放慢 SQL 的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:supportFeature:get
drs:replayJob:listReplayData	授予查询流量回放统计列表的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:supportFeature:get
drs:subscriptionJob:createJob	授予创建订阅任务的权限。	write	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys	drs:subscriptionJob:create
drs:subscriptionJob:deleteJob	授予删除订阅任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:subscriptionJob:delete
drs:subscriptionJob:editJobInfo	授予编辑订阅任务信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:subscriptionJob:edit
drs:subscriptionJob:getJobDetail	授予查询订阅任务详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:subscriptionJob:get
drs:subscriptionJob:getSubscriptionRecord	授予查询详细的订阅内容的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:subscriptionJob:get
drs:subscriptionJob:jobAction	授予订阅任务操作的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:subscriptionJob:subscribe
drs:configuration:getUserGuideInfo	授予获取用户指引详情的权	list	-	-	drs:userGuide:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
drs:configuration:modifyUserGuideInfo	授予更新用户指引的权限。	write	-	-	drs:userGuide:update
drs:subscriptionJob:updateConsumeTime	授予修改消费时间点的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:subscriptionJob:UpdateConsumeTime
drs:subscriptionJob:updateJob	授予修改订阅任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:subscriptionJob:update
drs:cloudDataGuardJob:getRdsInstanceCount	授予查询指定 DDM 下面 rds 实例的数量的权限。	list	-	-	drs:dataGuardJob:list
drs:configuration:getAvailableNodeType	授予查询可用的 node 规格的权限。	list	-	-	drs:migrationJob:get
drs:configuration:getAvailableZoneWithoutSellOut	授予查询 node 规格未售罄的可用 AZ 的权限。	list	-	-	drs:migrationJob:get
drs:configuration:listAvailableZoneStatus	授予查询 AZ 状态的权限。	list	-	-	drs:migrationJob:get
drs:configuration:listAvailableZone	授予查询可用 AZ 的权限。	list	-	-	drs:configuration:list
drs:migrationJob:listAvailableZone	授予查询规格未售罄的可用区的权限。	list	-	-	drs:migrationJob:get
drs:configuration:listResourcesByTag	授予根据标签查询任务的权限。	list	-	-	drs:tag:get
drs::listDrivers	授予查询驱动列表的权限。	list	-	-	drs:migrationJob:get
drs::uploadDriver	授予上传驱动	write	-	-	drs:migrationJob:update

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	的权限。				
drs::deleteDriver	授予删除驱动的权限。	write	-	-	drs:migrationJob:delete
drs:migrationJob:syncDriver	授予同步驱动的权限。	write	-	-	drs:migrationJob:update
drs:configuration:modifyConfigInfo	授予更新任务的参数信息。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:modify
drs:configuration:getJobParameters	授予查询任务的参数配置列表信息。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:configuration:getJobParametersHistory	授予查询任务的参数配置修改历史。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:migrationJob:get
drs:replayJob:showReplayTimeScope	授予查询录制回放时间窗口的权限。	read	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:supportFeature:get
drs:replayJob:showReplayResults	授予查询录制回放结果数据的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:supportFeature:get
drs:replayJob:exportReport	授予导出录制回放报表文件的权限。	read	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:supportFeature:get
drs:replayJob:showReportExportStatus	授予查询录制回放报表导出状态的权限。	read	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:supportFeature:get
drs:replayJob:showReportFileObsUris	授予查询录制回放报表下载链接的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>	drs:supportFeature:get

 版权所有 © 华为云计算技术有限公司

DRS 的 API 通常对应着一个或多个授权项。表 3-113 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-113 API 与授权项的关系

API	对应的授权项	依赖的授权项
DELETE /v3/{project_id}/jobs/batch-jobs	drs:migrationJoAb:batchDeleteJobs	-
DELETE /v5/{project_id}/jdbc-drivers	drs::deleteDriver	-
DELETE /v5/{project_id}/jobs	drs:migrationJob:batchDeleteJob	-
DELETE /v5/{project_id}/jobs/{job_id}	drs:migrationJob:deleteJob	-
GET /v3/{project_id}/jobs/{job_id}/get-src-user	drs:migrationJob:getSrcUsers	-
GET /v3/{project_id}/node-type	drs:configuration:getAvailableNodeType	-
GET /v3/{project_id}/quotas	drs:configuration:getQuota	-
GET /v5.1/{project_id}/jobs/{job_id}/db-object	drs:migrationJob:getDbObjects	-
GET /v5/{project_id}/{resource_type}/{resource_id}/tags	drs:configuration:getInstanceTag	-
GET /v5/{project_id}/{resource_type}/tags	drs:configuration:getProjectTags	-
GET /v5/{project_id}/batch-async-jobs	drs:migrationJob:listAsyncJobs	-
GET /v5/{project_id}/batch-async-jobs/{async_job_id}	drs:migrationJob:listAsyncJobDetail	-
GET /v5/{project_id}/enterprise-projects	drs:configuration:listEPs	-
GET /v5/{project_id}/jdbc-drivers	drs::listDrivers	-
GET /v5/{project_id}/job/{job_id}/columns	drs:configuration:getColumnInfo	-
GET /v5/{project_id}/job/{job_id}/data-filtering/result	drs:configuration:getDataTransformationData	-
GET /v5/{project_id}/jobs	drs:migrationJob:g	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	etJobList	
GET /v5/{project_id}/jobs/{job_id}	drs:migrationJob:getJobDetail	-
GET /v5/{project_id}/jobs/{job_id}/actions	drs:migrationJob:getAccess	-
GET /v5/{project_id}/jobs/{job_id}/compare-policy	drs:compareJob:getComparePolicy	-
GET /v5/{project_id}/jobs/{job_id}/configuration-histories	drs:configuration:getJobParametersHistory	-
GET /v5/{project_id}/jobs/{job_id}/configurations	drs:configuration:getJobParameters	-
GET /v5/{project_id}/jobs/{job_id}/data-processing-rules	drs:configuration:getDataTransformationInfo	-
GET /v5/{project_id}/jobs/{job_id}/data-processing-rules/result	drs:configuration:getDataTransformationInfo	-
GET /v5/{project_id}/jobs/{job_id}/db-object/template	drs:migrationJob:downloadDbObjectTemplate	-
GET /v5/{project_id}/jobs/{job_id}/db-object/template/progress	drs:migrationJob:getDbObjectTemplateProgress	-
GET /v5/{project_id}/jobs/{job_id}/db-object/template/result	drs:migrationJob:getDbObjectTemplateResult	-
GET /v5/{project_id}/jobs/{job_id}/db-objects	drs:migrationJob:getDbObjects	-
GET /v5/{project_id}/jobs/{job_id}/db-objects/collection-status	drs:migrationJob:getDbObjectCollectionStatus	-
GET /v5/{project_id}/jobs/{job_id}/db-objects/saving-status	drs:migrationJob:getUpdateObjectSavingStatus	-
GET /v5/{project_id}/jobs/{job_id}/db-position	drs:migrationJob:checkAction	-
GET /v5/{project_id}/jobs/{job_id}/dirty-data	drs:migrationJob:listReplayFaultsJobs	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/jobs/{job_id}/health-compare-jobs	drs:compareJob:listHealthCompareJobs	-
GET /v5/{project_id}/jobs/{job_id}/increment-components-detail	drs:migrationJob:getIncreComponentsDetails	-
GET /v5/{project_id}/jobs/{job_id}/metering	drs:migrationJob:getJobMeteringPrice	-
GET /v5/{project_id}/jobs/{job_id}/monitor-data	drs:cloudDataGuardJob:getDataGuardMonitor	-
GET /v5/{project_id}/jobs/{job_id}/object/support	drs:migrationJob:getSupportObject	-
GET /v5/{project_id}/jobs/{job_id}/progress-data/{type}	drs:migrationJob:getObjectsCompareOverviewa	-
GET /v5/{project_id}/jobs/{resource_type}/{job_id}/tags	drs:configuration:getInstanceTag	-
GET /v5/{project_id}/jobs/{resource_type}/tags	drs:configuration:getProjectTags	-
GET /v5/{project_id}/jobs/template	drs:migrationJob:downloadBatchCreateTemplate	-
GET /v5/{project_id}/links	drs:configuration:listLinks	-
POST /v3/{project_id}/available-zone	drs:migrationJob:listAvailableZone	-
POST /v3/{project_id}/jobs	drs:migrationJob:listJobs	-
POST /v3/{project_id}/jobs/{job_id}/params	drs:configuration:modifyDatabaseParams	-
POST /v3/{project_id}/jobs/{type}/batch-struct-detail	drs:cloudDataGuardJob:listJobInfo	-
POST /v3/{project_id}/jobs/batch-connection	drs:migrationJob:batchTestConnection	-
POST /v3/{project_id}/jobs/batch-creation	drs:migrationJob:batchCreateJob	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/jobs/batch-detail	drs:migrationJob:listJobInfo	-
POST /v3/{project_id}/jobs/batch-get-params	drs:configuration:listDatabaseParams	-
POST /v3/{project_id}/jobs/batch-pause-task	drs:migrationJob:batchPauseJob	-
POST /v3/{project_id}/jobs/batch-precheck	drs:migrationJob:batchPreCheckJob	-
POST /v3/{project_id}/jobs/batch-precheck-result	drs:migrationJob:listPrecheckResult	-
POST /v3/{project_id}/jobs/batch-progress	drs:migrationJob:listProgressInfo	-
POST /v3/{project_id}/jobs/batch-replace-definer	drs:migrationJob:batchUpdateDefinerMigrateSetting	-
POST /v3/{project_id}/jobs/batch-retry-task	drs:migrationJob:batchRetryJob	-
POST /v3/{project_id}/jobs/batch-rpo-and-rto	drs:cloudDataGuardJob:listRpoAndRto	-
POST /v3/{project_id}/jobs/batch-set-smn	drs:migrationJob:batchSetSmn	-
POST /v3/{project_id}/jobs/batch-starting	drs:migrationJob:batchStartJob	-
POST /v3/{project_id}/jobs/batch-status	drs:migrationJob:listJobStatus	-
POST /v3/{project_id}/jobs/batch-struct-process	drs:cloudDataGuardJob:listStructProcess	-
POST /v3/{project_id}/jobs/batch-switchover	drs:cloudDataGuardJob:batchSwitchover	-
POST /v3/{project_id}/jobs/batch-sync-policy	drs:migrationJob:setBatchSyncPolicy	-
POST /v3/{project_id}/jobs/batch-transformation	drs:migrationJob:batchSetTransformation	-
POST /v3/{project_id}/jobs/cluster/batch-connection	drs:migrationJob:batchTestClusterConnection	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/jobs/create-compare-task	drs:compareJob:createJob	-
POST /v3/{project_id}/jobs/disaster-recovery-monitoring-data	drs:cloudDataGuardJob:getMonitoringData	-
POST /v3/{project_id}/jobs/query-compare-result	drs:compareJob:getCompareResult	-
POST /v5.1/{project_id}/jobs/{job_id}/db-objects/collect	drs:migrationJob:getDbObjectsCollectAsync	-
POST /v5/{project_id}/{resource_type}/{resource_id}/tags/create	drs:configuration:addTag	-
POST /v5/{project_id}/{resource_type}/{resource_id}/tags/delete	drs:configuration:deleteTag	-
POST /v5/{project_id}/{resource_type}/resource-instances/count	drs:configuration:listResourcesByTag	-
POST /v5/{project_id}/{resource_type}/resource-instances/filter	drs:configuration:listResourcesByTag	-
POST /v5/{project_id}/batch-async-jobs/{async_job_id}/commit	drs:migrationJob:asyncBatchCreateJobByAsyncId	-
POST /v5/{project_id}/jdbc-driver	drs::uploadDriver	-
POST /v5/{project_id}/job/{job_id}/columns/collect	drs:configuration:getColumnInfo	-
POST /v5/{project_id}/job/{job_id}/data-filtering/check	drs:configuration:checkDataTransformationInfo	-
POST /v5/{project_id}/jobs	drs:migrationJob:createJobs	-
POST /v5/{project_id}/jobs/{job_id}/action	drs:migrationJob:operateJobByJobId	-
POST /v5/{project_id}/jobs/{job_id}/collect-db-position	drs:migrationJob:checkAction	-
POST /v5/{project_id}/jobs/{job_id}/db-object/template	drs:migrationJob:uploadDbObjectTemplate	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v5/{project_id}/jobs/{job_id}/db-objects/collect	drs:migrationJob:getDbObjectsCollectAsync	-
POST /v5/{project_id}/jobs/{job_id}/object-mappings	drs:migrationJob:getUserSelectedObjectInfo	-
POST /v5/{project_id}/jobs/{job_id}/operation-statistics/export	drs:migrationJob:getOperationInfo	-
POST /v5/{project_id}/jobs/{job_id}/stop	drs:migrationJob:deleteJob	-
POST /v5/{project_id}/jobs/{resource_type}/{job_id}/tags/action	drs:configuration:batchReplaceTags	-
POST /v5/{project_id}/jobs/action	drs:migrationJob:batchOperateJob	-
POST /v5/{project_id}/jobs/batch-async-create	drs:migrationJob:asyncBatchSaveJob	-
POST /v5/{project_id}/jobs/batch-stop	drs:migrationJob:deleteJob	-
POST /v5/{project_id}/jobs/clone	drs:migrationJob:cloneJobs	-
POST /v5/{project_id}/jobs/name-validation	drs:migrationJob:checkAction	-
POST /v5/{project_id}/jobs/template	drs:migrationJob:importBatchCreateJobs	-
PUT /v3/{project_id}/job/{job_id}/tuning-params/modify-params	drs:migrationJob:updateTuningParams	-
PUT /v3/{project_id}/jobs/batch-limit-speed	drs:migrationJob:batchSetSpeedLimit	-
PUT /v3/{project_id}/jobs/batch-modification	drs:migrationJob:batchUpdateJobInfo	-
PUT /v3/{project_id}/jobs/batch-modify-pwd	drs:migrationJob:changeSrcOrTargetPwd	-
PUT /v3/{project_id}/jobs/batch-select-objects	drs:migrationJob:selectDatabaseObject	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v3/{project_id}/jobs/batch-update-user	drs:migrationJob:batchUpdateUserMigrate	-
PUT /v5/{project_id}/batch-async-jobs/{async_job_id}	drs:migrationJob:asyncBatchUpdateJobByAsyncId	-
PUT /v5/{project_id}/jobs/{job_id}	drs:migrationJob:updateJobInfo	-
PUT /v5/{project_id}/jobs/{job_id}/data-processing-rules	drs:configuration:addDataTransformationInfo	-
PUT /v5/{project_id}/jobs/{job_id}/modify-configuration	drs:configuration:modifyConfigInfo	-
PUT /v5/{project_id}/jobs/{job_id}/start-position	drs:migrationJob:modifyIncreStartPosition	-
PUT /v5/{project_id}/jobs/{job_id}/update-jdbc-driver	drs:migrationJob:syncDriver	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 2 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的策略语句中指定该资源的 URN，策略仅作用于此资源；如未指定，Resource 默认为“*”，则策略将应用到所有资源。您也可以在策略中设置条件，从而指定资源类型。

表3-114 DRS 支持的资源类型

资源类型	URN
job	drs:<region>:<account-id>:job:<job-id>

条件（Condition）

DRS 不支持在身份策略中的条件键中配置服务级的条件键。DRS 可以使用适用于所有服务的全局条件键，请参考全局条件键。

 版权所有 © 华为云计算技术有限公司

3.6.5 数据管理服务 DAS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 DAS 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 DAS 定义的条件键的详细信息请参见条件（Condition）。
- **“别名”**列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 DAS 的相关操作。

 版权所有 © 华为云计算技术有限公司

表3-115 DAS 支持的授权项

授权项	描述	访问级别	资源类型（* 为必须）	条件键	别名
das:instance:createConnection	授予新增数据库实例登录的权限。	write	instance	-	das:connections:create
das:connection:login	授予登录连接的权限。	write	connection	-	das:connections:login
das:instance:dbsLogin	授予从 DBS 登录连接的权限。	write	instance	-	das:connections:login
das:connection:modify	授予修改数据库登录信息的权限。	write	connection	-	das:connections:modify
das:connection:delete	授予删除数据库登录信息的权限。	write	connection	-	das:connections:delete
das:connection:list	授予获取登录信息列表的权限。	list	connection	-	das:connections:list
das:connection:createShareConnections	授予创建共享连接的权限。	write	connection	das:TargetOrgPath das:TargetOrgId das:TargetAccountId	-
das:connection:cancelShareConnections	授予删除共享连接的权限。	write	connection	-	-
das:clouddba:getDbUser	授予获取数据库用户信息的权限。	read	instance	-	-
das:clouddba:registerDbUser	授予新增数据库登录的权限。	write	instance	-	-
das:clouddba:listDbUser	授予查询数据库用户列表的权限。	list	instance	-	-
das:clouddba:modifyDbUser	授予修改数据库用户的权限。	write	instance	-	-
das:clouddba:dele	授予删除数据库	write	instanc	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（* 为必须）	条件键	别名
teDbUser	用户的权限。		e		
das:clouddba:listInnodbLock	授予展示 InnoDB 锁等待列表的权限。	list	instance	-	-
das:clouddba:listMetadataLock	授予查询元数据锁列表的权限。	list	instance	-	-
das:clouddba:deleteProcess	授予删除实例会话的权限。	write	instance	-	-
das:clouddba:listSlowSql	授予查询慢 SQL 列表的权限。	list	instance	-	das:clouddba:slowSqlList
das:clouddba:slowSqlExport	授予导出慢 SQL 数据的权限。	list	instance	-	-
das:clouddba:listFullSql	授予查询全量 SQL 列表的权限。	list	instance	-	das:clouddba:fullSqlList
das:clouddba:fullSqlExport	授予导出全量 SQL 数据的权限。	list	instance	-	-
das:clouddba:listTopSql	授予查询 TopSQL 列表的权限。	list	instance	-	das:clouddba:topSqlList
das:clouddba:listProcess	授予查询实例会话列表的权限。	list	instance	-	-
das:clouddba:changePaymentMode	授予设置付费/免费模式的权限。	write	instance	-	-
das:clouddba:dailyReportsSubscribe	授予订阅日报的权限。	write	instance	-	-
das:clouddba:listDailyReports	授予查询日报列表的权限。	list	instance	-	das:clouddba:dailyReportsList
das:clouddba:listSpaceAnalysis	授予查询空间诊断任务列表的权限。	list	instance	-	-
das:clouddba:listSqlLimitRules	授予查询 SQL 限流规则列表的权限。	list	instance	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
das:clouddba:showSqlExecutionPlan	授予展示 SQL 执行计划的权限。	read	connection instance	-	das:clouddba:getSqlExecutionPlan
das:clouddba:sqlDiagnosis	授予执行 SQL 诊断的权限。	write	connection instance	-	-
das:clouddba:showSqlLimitJobInfo	授予查询 SQL 限流任务信息的权限。	read	instance	-	-
das:clouddba:showSqlLimitSwitchStatus	授予查询 SQL 限流开关状态的权限。	read	instance	-	-
das:clouddba:showSqlSwitchStatus	授予查询全量 SQL 和慢 SQL 开关状态的权限。	read	instance	-	-
das:clouddba:deleteSqlLimitRules	授予删除 SQL 限流规则的权限。	write	instance	-	-
das:clouddba:modifySqlLimitRules	授予修改 SQL 限流规则的权限。	write	instance	-	-
das:clouddba:changeSqlLimitSwitchStatus	授予修改 SQL 限流开关的权限。	write	instance	-	-
das:clouddba:changeSqlSwitch	授予修改全量 SQL 和慢 SQL 开关的权限。	write	instance	-	-
das:clouddba:createSpaceAnalysisTask	授予创建空间诊断任务的权限。	write	instance	-	-
das:clouddba:createSqlLimitRules	授予创建 SQL 限流规则的权限。	write	instance	-	-
das:clouddba:executeSql	授予执行 SQL 命令的权限。	write	instance	-	-
das:clouddba:listBinlog	授予查看 binlog 列表的权限。	list	instance	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（* 为必须）	条件键	别名
das:clouddba:createBinlogAnalysisTask	授予创建 binlog 解析任务的权限。	write	instance	-	-
das::addQuota	授予添加配额的权限。	write	-	-	das:clouddba:changePaymentMode
das::showQuotas	授予查询资源配额的权限。	read	-	-	das:clouddba:menuList
das::getSupported	授予查询当前 region 支持引擎类型的权限。	read	-	-	das:connections:list
das::getWhitelist	授予查询当前 region 支持的功能白名单的的权限。	read	-	-	das:connections:list
das::listInstances	授予查询所有类型引擎实例列表的权限。	list	-	-	das:connections:list
das:instance:executeTestConnection	授予执行测试连接的权限。	write	instance	-	das:connections:login
das:connection:getSharedList	授予获取某个连接的共享列表的权限。	list	connection	-	das:connections:list
das:connection:updateSharedInfo	授予更新共享连接信息的权限。	write	connection	-	das:connections:modify
das:connection:getConnection	授予查看连接信息的权限。	read	connection	-	das:connections:list
das::getGlobalPrivacy	授予查看隐私说明的权限。	read	-	-	das:connections:list
das::putGlobalPrivacy	授予更新隐私说明的权限。	write	-	-	das:connections:list
das::showCloudDBAInfo	授予查看 DBA 智能运维信息的权限。	read	-	-	-
das:clouddba:sho	授予查看持续 kill	read	instanc	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（* 为必须）	条件键	别名
wKillTaskSwitch	会话任务开关的权限。		e		
das:clouddba:changeKillTaskSwitch	授予修改持续 kill 会话任务开关的权限。	write	instance	-	-
das:clouddba:listKillTaskRecord	授予查看持续 kill 会话任务列表的权限。	list	instance	-	-
das:clouddba:createKillTask	授予创建持续 kill 会话任务的权限。	write	instance	-	-
das:clouddba:stopKillTask	授予停止持续 kill 会话任务的权限。	write	instance	-	-

DAS 的 API 通常对应着一个或多个授权项。表 3-116 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-116 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/instances/{instance_id}/db-users	das:clouddba:listDbUser	-
POST /v3/{project_id}/instances/{instance_id}/db-users	das:clouddba:registerDbUser	-
GET /v3/{project_id}/instances/{instance_id}/db-users/{db_user_id}	das:clouddba:getDbUser	-
PUT /v3/{project_id}/instances/{instance_id}/db-users/{db_user_id}	das:clouddba:modifyDbUser	-
DELETE /v3/{project_id}/instances/{instance_id}/db-users/{db_user_id}	das:clouddba:deleteDbUser	-
GET /v3/{project_id}/instances/{instance_id}/sql/	das:clouddba:showSqlExecutionPlan	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
explain		
POST /v3/{project_id}/instances/{instance_id}/sql/explain	das:clouddba:showSqlExecutionPlan	-
GET /v3/{project_id}/instances/{instance_id}/processes	das::showCloudDBAInfo	-
DELETE /v3/{project_id}/instances/{instance_id}/process	das:clouddba:deleteProcess	-
GET /v3/{project_id}/instances/{instance_id}/metadata-locks	das:clouddba:listMetadataLock	-
GET /v3/{project_id}/instances/{instance_id}/innodb-locks	das:clouddba:listInnodbLock	-
GET /v3/{project_id}/instances/{instance_id}/slow-query-logs	das:clouddba:slowSqlExport	-
GET /v3/{project_id}/instances/{instance_id}/sql-statements	das:clouddba:fullSqlExport	-
GET /v3/{project_id}/instances/{instance_id}/full-sql-tasks	das:clouddba:listFullSql	-
GET /v3/{project_id}/instances/{instance_id}/full-sql-search	das:clouddba:listFullSql	-
GET /v3/{project_id}/instances/{instance_id}/sql/switch	das:clouddba:showSqlSwitchStatus	-
POST /v3/{project_id}/instances/{instance_id}/sql/switch	das:clouddba:changeSqlSwitch	-
GET /v3/{project_id}/instances/{instance_id}/transaction/switch	das::showCloudDBAInfo	-
POST /v3/{project_id}/instances/{instance_id}/transaction/switch	das:clouddba:changeTransactionSwitch	-
GET /v3/{project_id}/instances/{instance_id}/transaction	das::showCloudDBAInfo	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/instances/{instance_id}/space-analysis	das:clouddba:listSpaceAnalysis	-
POST /v3/{project_id}/instances/{instance_id}/space-analysis	das:clouddba:createSpaceAnalysisTask	-
GET /v3/{project_id}/instances/{instance_id}/sql-limit/switch	das:clouddba:showSqlLimitSwitchStatus	-
POST /v3/{project_id}/instances/{instance_id}/sql-limit/switch	das:clouddba:changeSqlLimitSwitchStatus	-
GET /v3/{project_id}/instances/{instance_id}/sql-limit/job	das:clouddba:showSqlLimitJobInfo	-
GET /v3/{project_id}/instances/{instance_id}/sql-limit/rules	das:clouddba:listSqlLimitRules	-
POST /v3/{project_id}/instances/{instance_id}/sql-limit/rules	das:clouddba:createSqlLimitRules	-
DELETE /v3/{project_id}/instances/{instance_id}/sql-limit/rules	das:clouddba:deleteSqlLimitRules	-
PUT /v3/{project_id}/instances/{instance_id}/sql-limit/rules	das:clouddba:updateSqlLimitRules	-
POST /v3/{project_id}/instances/{instance_id}/sql-limit/parse	das:clouddba:createSqlLimitRules	-
GET /v3/{project_id}/quotas	das::showQuotas	-
GET /v3/{project_id}/instances/{instance_id}/top-sql-templates	das:clouddba:listTopSql	-
GET /v3/{project_id}/instances/{instance_id}/top-sql-trend	das:clouddba:listTopSql	-
GET /v3/{project_id}/instances/{instance_id}/slow-sql-templates	das:clouddba:slowSqlExport	-
GET /v3/{project_id}/instances/{instance_id}/slo	das:clouddba:slowSqlExport	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
w-sql-trend		
POST /v3/{project_id}/instances/{instance_id}/slow-sql-statistics	das::showCloudDBAInfo	-
POST /v3/{project_id}/connections/{connectionId}/tuning/create-tuning	das:clouddba:sqlDiagnosis	-
GET /v3/{project_id}/connections/{connectionId}/tuning/{messageId}/show-tuning-result	das:clouddba:sqlDiagnosis	-
GET /v3/{project_id}/instances/top-risk	das::showCloudDBAInfo	-
GET /v3/{project_id}/instances/risk-trend	das::showCloudDBAInfo	-
GET /v3/{project_id}/instances/distribution	das::showCloudDBAInfo	-
GET /v3/{project_id}/instances/top-slow-log	das::showCloudDBAInfo	-
GET /v3/{project_id}/instances/{instance_id}/top-slow-log	das::showCloudDBAInfo	-
GET /v3/{project_id}/metric-names/support	das::showCloudDBAInfo	-
GET /v3/{project_id}/instance/nodes-info	das::showCloudDBAInfo	-
POST /v3/{project_id}/multi-nodes/single-metric	das::showCloudDBAInfo	-
GET /v3/{project_id}/get-risk-items	das::showCloudDBAInfo	-
POST /v3/{project_id}/set-metric-threshold	das::setMetricThreshold	-
GET /v3/{project_id}/instances	das::listInstances	-
POST /v3/{project_id}/instances/{instance_id}/create-instance-health-report-task	das:clouddba:dailyReportsSubscribe	-
GET /v3/{project_id}/instances/{instance_id}/get-instance-health-report-task-list	das:clouddba:listDailyReports	-
GET /v3/{project_id}/instances/{instance_id}/get-instance-health-report	das:clouddba:listDailyReports	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/instances/synchronize-instance-list	das::showCloudDBAInfo	-
POST /v3/{project_id}/cloud-dba/change-payment-mode	das:clouddba:changePaymentMode	-
POST /v3/{project_id}/instances/{instance_id}/full-sql/add-task	das:clouddba:listFullSql	-
POST /v3/{project_id}/connections/share	das:connection:createShareConnections	-
DELETE /v3/{project_id}/connections/share	das:connection:cancelShareConnections	-
POST /v3/{project_id}/instances/{instance_id}/create-connection	das:instance:createConnection	-
GET /v3/{project_id}/list-connections	das::showCloudDBAInfo	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的 URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

DAS 定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-117 DAS 支持的资源类型

资源类型	URN	条件键
instance	das:<region>:<account-id>:instance:<instance-id>	-
connection	das:<region>:<account-id>:connection:<connection-id>	-

条件（Condition）

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。

 版权所有 © 华为云计算技术有限公司

  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀为服务缩写，如 DAS:）仅适用于对应服务的操作，详情请参见表 3-118。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

DAS 定义了以下可以在 IAM 自定义策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化策略语句应用的条件。

表3-118 DAS 支持的服务级条件键

服务级条件键	类型	说明
das:TargetOrgPath	string	按照共享目标账号所处的组织路径进行权限控制。
das:TargetOrgId	string	按照共享目标账号所处的组织 Id 进行权限控制。
das:TargetAccountId	string	按照共享目标账号 Id 进行权限控制。

3.7 安全与合规

3.7.1 数据加密服务 DEW

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

 版权所有 © 华为云计算技术有限公司

本章节介绍 DEW 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在策略中使用操作时，相应操作授予的访问级别。
- “资源类型”列指示每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于密码安全中心（Data Encryption Workshop, DEW）定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

  关于密码安全中心（Data Encryption Workshop, DEW）定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 DEW 的相关操作。

表3-119 KMS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
kms:cmk:create	授予创建 KMS 密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				key> • g:TagKeys	
kms:cmk:list	授予查看用户所有 KMS 密钥信息的权限。	list	KeyId *	-	-
			-	g:EnterpriseProjectId	
kms:cmk:enable	授予更改 KMS 密钥状态为已启用的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
kms:cmk:disable	授予禁用 KMS 密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
kms:cmk:get	授予查看 KMS 密钥的详细信息的权限。	read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			-	• kms:RequestAlias • kms:ResourceAliases	
kms:cmk:createDataKey	授予使用 KMS 密钥生成数据密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	kms:dek:create
			-	• kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext	
kms:cmk:createDataKeyWithoutPlaintext	授予使用 KMS 密钥生成不包含明文版本数据密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId	kms:dek:create

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:ResourceTag/<tag-key>	
			-	• kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext	
kms:cmk:encryptDataKey	授予加密数据密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	kms:dek:crypto
			-	• kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext	
kms:cmk:decryptDataKey	授予解密数据密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	kms:dek:crypto

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	• kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext	
kms:cmk:encryptData	授予使用指定的KMS 密钥加密小数据的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	kms:cmk:crypto
			-	• kms:EncryptionAlgorithm • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext	
kms:cmk:decryptData	授予使用指定的KMS 密钥解密数据的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId	kms:cmk:crypto

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:ResourceTag/<tag-key>	
			-	• kms:EncryptionAlgorithm • kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext	
kms::generateRandom	授予生成安全随机字符串的权限。	write	-	kms:RecipientAttestation	kms:cmk:generate
kms:cmk:sign	授予为生成数字签名的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• kms:MessageType • kms:SigningAlgorithm • kms:RequestAlias • kms:ResourceAliases	
kms:cmk:verify	授予使用指定的KMS 密钥验证	write	KeyId *	• kms:KeyOrigin • kms:KeySp	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	数字签名的权限。			ec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			-	• kms:MessageType • kms:SigningAlgorithm • kms:RequestAlias • kms:ResourceAliases	
kms:cmk:generateMac	授予生成消息验证码的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• kms:MacAlgorithm • kms:RequestAlias • kms:ResourceAliases	
kms:cmk:verifyMac	授予使用指定的KMS 密钥验证消息验证码的权	write	KeyId *	• kms:KeyOrigin • kms:KeySpec	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。			• kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			-	• kms:MacAlgorithm • kms:RequestAlias • kms:ResourceAliases	
kms:cmk:getPublicKey	授予查询 KMS 密钥公钥的权限。	read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• kms:RequestAlias • kms:ResourceAliases	
kms::getVersions	授予查询服务版本的权限。	read	-	-	-
kms::getVersion	授予查询服务密钥 API 版本的权限。	read	-	-	-
kms::getInstance	授予查询用户密钥实例个数的权限。	read	-	-	kms:cmk:getInstance

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
kms::getQuota	授予查询用户配额的权限。	read	-	-	kms:cmk:getQuota
kms:cmk:scheduleKeyDeletion	授予定时删除KMS 密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	kms:cmk:update
			-	kms:ScheduleKeyDeletionPendingWindowInDays	
kms:cmk:cancelKeyDeletion	授予取消定时删除 KMS 密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	kms:cmk:update
kms:cmk:updateKeyAlias	授予更改密钥别名的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType	kms:cmk:update

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
kms:cmk:updateKeyDescription	授予更改密钥描述的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	kms:cmk:update
kms:cmk:createGrant	授予给特定密钥创建授权的权限。	permission_management	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	kms:grant:create
			-	• kms:GranteePrincipalType • kms:GrantOperations • kms:GranteePrincipal • kms:RetiringPrincipal	
kms:cmk:l	授予查询特定密	list	KeyId *	• kms:KeyOr	kms:grant:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
istGrants	钥已授权列表的权限。			igin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
kms::listRetirableGrants	授予查询密钥可退役授权列表的权限。	list	-	-	kms:grant:list
kms:cmk:retireGrant	授予给特定密钥退役授权的权限。	permission_management	KeyId *	g:ResourceTag/<tag-key>	kms:grant:retire
kms:cmk:revokeGrant	授予给特定密钥撤销授权的权限。	permission_management	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	kms:grant:revoke
kms:cmk:getMaterial	授予获取密钥导入参数的权限。	read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyT	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ype • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			-	kms:WrappingAlgorithm	
kms:cmk:importMaterial	授予导入密钥材料的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	kms:ExpirationTime	
kms:cmk:deleteMaterial	授予删除密钥材料的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
kms:cmk:enableRotation	授予开启指定密钥轮换的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUs	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				age • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
kms:cmk:updateRotation	授予更改指定密钥轮换周期的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
kms:cmk:disableRotation	授予关闭密钥轮换的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
kms:cmk:getRotation	授予查询指定密钥轮换状态的权限。	read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
kms:keystore:create	授予创建专属密钥库的权限。	write	keystore *	-	-
kms:keystore:delete	授予删除专属密钥库的权限。	write	keystore *	-	-
kms:keystore:enable	授予启用专属密钥库的权限。	write	keystore *	-	-
kms:keystore:disable	授予禁用专属密钥库的权限。	write	keystore *	-	-
kms:keystore:list	授予查询专属密钥库列表的权限。	list	keystore *	-	-
kms:keystore:get	授予获取专属密钥库的权限。	read	keystore *	-	-
kms:cmk:createTag	授予给指定密钥添加标签的权限。	tagging	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	kms:cmkTag:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
kms:cmk:createTags	授予给指定密钥批量添加或者删除密钥标签的权限。	tagging	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	kms:cmkTag:batch
			-	• g:RequestTag/<tag-key> • g:TagKeys	
kms:cmk:listKeysByTag	授予查询指定密钥实例的权限。	list	KeyId *	-	kms:cmkTag:listInstance
kms:cmk:deleteTag	授予删除指定密钥标签的权限。	tagging	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	kms:cmkTag:delete
			-	g:TagKeys	
kms:cmk:getTags	授予查询指定密钥标签的权限。	read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage	kms:cmkTag:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
kms::listAllTags	授予查询指定密钥项目标签的权限。	list	-	-	-
kms:cmk:replicate	授予复制 KMS 密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
kms:cmk:updatePrimaryRegion	授予更新主区域的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	- -
			-	kms:PrimaryRegion	
kms:alias:create	授予创建别名的	write	KeyId *	• kms:KeyOrigin	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	权限。			• kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			alias *	-	
kms:alias:delete	授予删除别名的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			alias *	-	
kms:alias:list	授予查询别名列表的权限。	list	-	-	-
kms:alias:associate	授予关联别名的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:Resource	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				Tag/<tag-key>	
			alias *	-	

表3-120 KPS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
kps:SSHKeyPair:create	授予创建和导入 SSH 密钥对的权限。	write	SSHKeyPair *	• kps:KmsKeyId • kps:Algorithm	kps:domainKeypairs:create
kps:SSHKeyPair:delete	授予删除 SSH 密钥对的权限。	write	SSHKeyPair *	-	kps:domainKeypairs:delete
kps:SSHKeyPair:get	授予查询 SSH 密钥对详细信息的权限。	read	SSHKeyPair *	-	kps:domainKeypairs:get
kps:SSHKeyPair:list	授予查询 SSH 密钥对列表的权限。	list	SSHKeyPair *	-	kps:domainKeypairs:list
kps:SSHKeyPair:update	授予更新 SSH 密钥对描述的权限。	write	SSHKeyPair *	-	kps:domainKeypairs:update
kps:SSHKeyPair:bind	授予虚拟机绑定新 SSH 密钥对的权限。	write	SSHKeyPair *	-	kps:domainKeypairs:bind
kps::deleteFailedTask	授予删除失败任务的权限。	write	-	-	kps:domainKeypairs:deletefailtask
kps:SSHKeyPair:unbind	授予虚拟机解绑 SSH 密钥对的权	write	SSHKeyPair *	-	kps:domainKeypairs:unbind

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
kps::getFailedTask	授予查询失败任务信息的权限。	list	-	-	kps:domainKeypairs:getfailtask
kps::getTask	授予查询当前任务执行状态的权限。	list	-	-	kps:domainKeypairs:gettask
kps::getRunningTask	授予查询正在处理的任务信息的权限。	list	-	-	kps:domainKeypairs:getrunningtask
kps:SSHKeyPair:importPrivateKey	授予导入私钥到密钥对的权限。	write	SSHKeyPair *	kps:KmsKeyId	kps:domainKeypairs:importpk
kps:SSHKeyPair:exportPrivateKey	授予导出密钥对私钥的权限。	write	SSHKeyPair *	-	kps:domainKeypairs:exportpk
kps:SSHKeyPair:clearPrivateKey	授予清除密钥对私钥的权限。	write	SSHKeyPair *	-	kps:domainKeypairs:clearpk

表3-121 CSMS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
csms:secret:create	授予创建和恢复凭据的权限。	write	secretName *	• csms:Type • csms:KmsKeyId	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
csms:secret:delete	授予立即删除	write	secretName *	• csms:Type • g:EnterprisePro	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	凭据的权限。			jectId • g:ResourceTag/<tag-key>	
csms:secret:update	授予更新凭据元数据信息的权限。	write	secretName *	• csms:Type • csms:KmsKeyId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
csms:secret:get	授予查询和下载凭据信息的权限。	read	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
csms:secret:list	授予查询当前用户在本项目下创建的所有凭据的权限。	list	secretName *	g:EnterpriseProjectId	-
csms:secret:createVersion	授予指定凭据中创建新凭据版本的权限。	write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	csms:secretVersion:create
csms:secret:getVersion	授予查询指定凭据版本的信息和其明文凭据值的权限。	read	secretName *	• csms:Type • csms:VersionId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	csms:secretVersion:get
csms:secret:listVersion	授予查询指定凭据下的版本列表信息的权限。	list	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	csms:secretVersion:list
csms:secret:createStage	授予创建凭据版本状态的权限。	write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/	csms:secretStage:create

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				<tag-key>	
csms:secret:getStage	授予查询指定凭据版本状态标记的版本信息的权限。	read	secretName *	• csms:Type • csms:VersionStage • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	csms:secretStage:get
csms:secret:updateStage	授予更新凭据版本状态的权限。	write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	csms:secretStage:update
csms:secret:deleteStage	授予删除指定凭据版本状态的权限。	write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	csms:secretStage:delete
csms::getSecretQuota	授予查询指定项目凭据配额的权限。	read	-	-	csms:secretQuota:get
csms:secret:scheduleDeletion	授予创建凭据定时删除任务的权限。	write	secretName *	• csms:Type • csms:RecoveryWindowInDays • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	csms:secret:deleteScheduled
csms:secret:restoreSecret	授予取消凭据定时删除任务的权限。	write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	csms:secret:deleteCancelled
csms:secret:rotate	授予轮转凭据的权限。	write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
csms:secret:	授予通过标签	list	secretNam	-	csms:tag:getSe

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
getSecretsByTag	过滤,返回凭据列表的权限。		e *		cretByTag
csms:secret:batchCreateOrDeleteTags	授予批量添加或删除凭据标签的权限。	tagging	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	csms:tag:batch
			-	• g:RequestTag/<tag-key> • g:TagKeys	
csms:secret:createTag	授予添加凭据标签的权限。	tagging	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	csms:tag:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
csms:secret:deleteTag	授予删除凭据标签的权限。	tagging	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	csms:tag:delete
			-	g:TagKeys	
csms:secret:listTags	授予查询凭据标签的权限。	list	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>	csms:tag:getBySecret
csms::listProjectTags	授予查询用户在指定项目下的所有凭据标签集合的权限。	list	-	-	csms:tag:getAll
csms:secret:updateVersion	授予更新凭据版本有效期的权限。	write	secretName *	• csms:Type • csms:VersionId • g:EnterpriseProjectId	csms:secretVersion:update

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:ResourceTag/<tag-key>	
csms::createEvent	授予创建凭据事件的权限。	write	-	-	csms:event:create
csms::listEvents	授予查询当前用户在本项目下创建的所有事件通知的权限。	list	-	-	csms:event:list
csms::getEvent	授予查询指定事件通知信息的权限。	read	-	-	csms:event:get
csms::updateEvent	授予更新指定事件通知的元数据信息的权限。	write	-	-	csms:event:update
csms::deleteEvent	授予立即删除指定的事件通知的权限。	write	-	-	csms:event:delete
csms::listNotificationRecords	授予查询已触发事件通知记录的权限。	list	-	-	csms:event:listNotificationRecords
csms::listTasks	授予查询凭据轮转任务的权限。	List	-	-	csms:task:list

DEW 的 API 通常对应着一个或多个授权项。表 API 与 KMS 操作项的关系、表 API 与 CSMS 操作项的关系、表 API 与 KPS 操作项的关系展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-122 API 与 KMS 授权项的关系

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/kms/create-key	kms:cmk:create	-
POST /v1.0/{project_id}/kms/list-keys	kms:cmk:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/kms/enable-key	kms:cmk:enable	-
POST /v1.0/{project_id}/kms/disable-key	kms:cmk:disable	-
POST /v1.0/{project_id}/kms/describe-key	kms:cmk:get	-
POST /v1.0/{project_id}/kms/create-datakey	kms:cmk:createDataKey	-
POST /v1.0/{project_id}/kms/create-datakey-without-plaintext	kms:cmk:createDataKeyWithoutPlaintext	-
POST /v1.0/{project_id}/kms/encrypt-datakey	kms:cmk:encryptDataKey	-
POST /v1.0/{project_id}/kms/decrypt-datakey	kms:cmk:decryptDataKey	-
POST /v1.0/{project_id}/kms/encrypt-data	kms:cmk:encryptData	-
POST /v1.0/{project_id}/kms/decrypt-data	kms:cmk:decryptData	-
POST /v1.0/{project_id}/kms/gen-random	kms::generateRandom	-
POST /v1.0/{project_id}/kms/sign	kms:cmk:sign	-
POST /v1.0/{project_id}/kms/verify	kms:cmk:verify	-
POST /v1.0/{project_id}/kms/get-publickey	kms:cmk:getPublicKey	-
GET /	kms::getVersions	-
GET /{version_id}	kms::getVersion	-
POST /v1.0/{project_id}/kms/schedule-key-deletion	kms:cmk:scheduleKeyDeletion	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/kms/cancel-key-deletion	kms:cmk:cancelKeyDeletion	-
GET /v1.0/{project_id}/kms/user-instances	kms::getInstance	-
GET /v1.0/{project_id}/kms/user-quotas	kms::getQuota	-
POST /v1.0/{project_id}/kms/update-key-alias	kms:cmk:updateKeyAlias	-
POST /v1.0/{project_id}/kms/update-key-description	kms:cmk:updateKeyDescription	-
POST /v1.0/{project_id}/kms/create-grant	kms:cmk:createGrant	-
POST /v1.0/{project_id}/kms/list-grants	kms:cmk:listGrants	-
POST /v1.0/{project_id}/kms/list-retirable-grants	kms::listRetirableGrants	-
POST /v1.0/{project_id}/kms/retire-grant	kms:cmk:retireGrant	-
POST /v1.0/{project_id}/kms/revoke-grant	kms:cmk:revokeGrant	-
POST /v1.0/{project_id}/kms/get-parameters-for-import	kms:cmk:getMaterial	-
POST /v1.0/{project_id}/kms/import-key-material	kms:cmk:importMaterial	-
POST /v1.0/{project_id}/kms/delete-imported-key-material	kms:cmk:deleteMaterial	-
POST /v1.0/{project_id}/kms/enable-key-rotation	kms:cmk:enableRotation	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/kms/update-key-rotation-interval	kms:cmk:updateRotation	-
POST /v1.0/{project_id}/kms/disable-key-rotation	kms:cmk:disableRotation	-
POST /v1.0/{project_id}/kms/get-key-rotation-status	kms:cmk:getRotation	-
POST /v1.0/{project_id}/keystores	kms:keystore:create	-
DELETE /v1.0/{project_id}/keystores/{keystore_id}	kms:keystore:delete	-
POST /v1.0/{project_id}/keystores/{keystore_id}/enable	kms:keystore:enable	-
POST /v1.0/{project_id}/keystores/{keystore_id}/disable	kms:keystore:disable	-
GET /v1.0/{project_id}/keystores	kms:keystore:list	-
GET /v1.0/{project_id}/keystores/{keystore_id}	kms:keystore:get	-
POST /v1.0/{project_id}/kms/{key_id}/tags	kms:cmk:createTag	-
POST /v1.0/{project_id}/kms/{key_id}/tags/action	kms:cmk:createTags	-
POST /v1.0/{project_id}/kms/{resource_instances}/action	kms:cmk:listKeysByTag	-
DELETE /v1.0/{project_id}/kms/{key_id}/tags/{key}	kms:cmk:deleteTag	-
GET /v1.0/{project_id}/kms/{key_id}/tags	kms:cmk:getTags	-
GET /v1.0/{project_id}/kms/tags	kms::listAllTags	-
POST	kms:cmk:replicate	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v2/{project_id}/kms/keys/{key_id}/replicate		
PUT /v2/{project_id}/kms/keys/{key_id}/update-primary-region	kms:cmk:updatePrimaryRegion	-

表3-123 API 与 CSMS 授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/secrets	csms:secret:create	kms:cmk:createDataKey
POST /v1/{project_id}/secrets/{secret_name}/backup	csms:secret:get	• kms:cmk:createDataKey • kms:cmk:decryptDataKey • kms:cmk:list
POST /v1/{project_id}/secrets/restore	csms:secret:create	kms:cmk:decryptDataKey
DELETE /v1/{project_id}/secrets/{secret_name}	csms:secret:delete	-
PUT /v1/{project_id}/secrets/{secret_name}	csms:secret:update	-
GET /v1/{project_id}/secrets/{secret_name}	csms:secret:get	-
GET /v1/{project_id}/secrets	csms:secret:list	-
POST /v1/{project_id}/secrets/{secret_name}/versions	csms:secret:createVersion	kms:cmk:createDataKey
GET /v1/{project_id}/secrets/{secret_name}/versions/{version_id}	csms:secret:getVersion	kms:cmk:decryptDataKey
GET /v1/{project_id}/secrets/{secret_name}/versions	csms:secret:listVersion	-
GET /v1/{project_id}/secrets/{secret_name}/stages/{stage_name}	csms:secret:getStage	-
PUT /v1/{project_id}/secrets/{secret_name}/stages/{stage_name}	csms:secret:updateStage	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /v1/{project_id}/secrets/{secret_name}/stages/{stage_name}	csms:secret:deleteStage	-
POST /v1/{project_id}/secrets/{secret_name}/scheduled-deleted-tasks/create	csms:secret:scheduleDeletion	-
POST /v1/{project_id}/secrets/{secret_name}/scheduled-deleted-tasks/cancel	csms:secret:restoreSecret	-
POST /v1/{project_id}/secrets/{secret_name}/rotate	csms:secret:rotate	• rds:password:update • kms:cmk:createGrant • kms:cmk:retireGrant
POST /v1/{project_id}/csms/{resource_instances}/action	csms:secret:getSecretsByTag	-
POST /v1/{project_id}/csms/{secret_id}/tags/action	csms:secret:batchCreateOrDeleteTags	-
POST /v1/{project_id}/csms/{secret_id}/tags	csms:secret:createTag	-
DELETE /v1/{project_id}/csms/{secret_id}/tags/{key}	csms:secret:deleteTag	-
GET /v1/{project_id}/csms/{secret_id}/tags	csms:secret:listTags	-
GET /v1/{project_id}/csms/tags	csms::listProjectTags	-
PUT /v1/{project_id}/secrets/{secret_name}/versions/{version_id}	csms:secret:updateVersion	-
POST /v1/{project_id}/csms/events	csms::createEvent	-
GET /v1/{project_id}/csms/events	csms::listEvents	-
GET /v1/{project_id}/csms/events/{event_name}	csms::getEvent	-
PUT /v1/{project_id}/csms/events/{event_name}	csms::updateEvent	-
DELETE	csms::deleteEvent	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/csms/events/{event_name}		
GET /v1/{project_id}/csms/notification-records	csms::listNotificationRecords	-
GET /v1/{project_id}/csms/tasks	csms::listTasks	-

表3-124 API 与 KPS 授权项的关系

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/keypairs	kps:SSHKeyPair:create	• kms:cmk:createDataKey • kms:cmk:list
DELETE /v3/{project_id}/keypairs/{keypair_name}	kps:SSHKeyPair:delete	-
GET /v3/{project_id}/keypairs/{keypair_name}	kps:SSHKeyPair:get	-
GET /v3/{project_id}/keypairs	kps:SSHKeyPair:list	-
PUT /v3/{project_id}/keypairs/{keypair_name}	kps:SSHKeyPair:update	-
POST /v3/{project_id}/keypairs/associate	kps:SSHKeyPair:bind	• ecs:cloudServers:createServers • ecs:cloudServers:deleteServers • ecs:cloudServers:showServer • ecs:cloudServers:attach • ecs:cloudServers:listServerBlockDevices • ecs:cloudServers:showServerBlockDevice • ecs:cloudServers:detachVolume • ecs:cloudServers:listServerInterfaces • ecs:cloudServers:listServersDetails • ecs:cloudServerFlavors:g

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
		et • ecs:cloudServerQuotas:get • evs:types:get • evs:volumes:use • ims:images:get • vpc:subnets:list
DELETE /v3/{project_id}/failed-tasks	kps::deleteFailedTask	-
DELETE /v3/{project_id}/failed-tasks/{task_id}	kps::deleteFailedTask	-
POST /v3/{project_id}/keypairs/disassociate	kps:SSHKeyPair:unbind	• ecs:cloudServers:createServers • ecs:cloudServers:deleteServers • ecs:cloudServers:showServer • ecs:cloudServers:attach • ecs:cloudServers:listServerBlockDevices • ecs:cloudServers:showServerBlockDevice • ecs:cloudServers:detachVolume • ecs:cloudServers:listServerInterfaces • ecs:cloudServers:listServersDetails • ecs:cloudServerFlavors:get • ecs:cloudServerQuotas:get • evs:types:get • evs:volumes:use • ims:images:get • vpc:subnets:list
GET /v3/{project_id}/failed-tasks	kps::getFailedTask	-
GET /v3/{project_id}/tasks/{task_id}	kps::getTask	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/running-tasks	kps::getRunningTask	-
POST /v3/{project_id}/keypairs/private-key/import	kps:SSHKeyPair:importPrivateKey	• kms:cmk:createDataKey • kms:cmk:list
POST /v3/{project_id}/keypairs/private-key/export	kps:SSHKeyPair:exportPrivateKey	kms:cmk:decryptDataKey
POST /v3/{project_id}/keypairs/batch-associate	kps:SSHKeyPair:bind	• ecs:cloudServers:createServers • ecs:cloudServers:deleteServers • ecs:cloudServers:showServer • ecs:cloudServers:attach • ecs:cloudServers:listServerBlockDevices • ecs:cloudServers:showServerBlockDevice • ecs:cloudServers:detachVolume • ecs:cloudServers:listServerInterfaces • ecs:cloudServers:listServersDetails • ecs:cloudServerFlavors:get • ecs:cloudServerQuotas:get • evs:types:get • evs:volumes:use • ims:images:get • vpc:subnets:list
DELETE /v3/{project_id}/keypairs/{keypair_name}/private-key	kps:SSHKeyPair:clearPrivateKey	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 DEW 支持的资源类型中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的策略语句中指定

 版权所有 © 华为云计算技术有限公司

该资源的 URN，策略仅作用于此资源；如未指定，Resource 默认为“*”，则策略将应用到所有资源。您也可以在策略中设置条件键，从而定义资源类型。

DEW 定义了以下可以在 IAM 自定义策略的 Resource 元素中使用的资源类型。

表3-125 DEW 支持的资源类型

资源类型	URN
KeyId	kms:<region>:<account-id>:KeyId:<cmk-id>
alias	kms:<region>:<account-id>:alias:<alias-name>
keystore	kms:<region>:<account-id>:keystore:<keystore-id>
secretName	csms:<region>:<account-id>:secretName:<secret-name>
SSHKeyPair	kps:<region>:<account-id>:SSHKeyPair:<keypair-name>

条件（Condition）

条件键（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，组织将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 DEW:）仅适用于对应服务的操作，详情请参见表 DEW 支持的服务级条件键。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，策略才能生效。支持的运算符请参见：运算符。

DEW 定义了以下可以在身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化策略语句应用的条件。

说明

KPS 服务不支持在身份策略中的条件键中配置服务级的条件键。

 版权所有 © 华为云计算技术有限公司

表3-126 DEW 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
kms:EncryptionAlgorithm	string	单值	根据请求中的加解密算法的值过滤对加解密操作的访问。
kms:GranteePrincipalType	string	单值	根据请求中的授权主体类型约束过滤对 CreateGrant 操作的访问。
kms:GrantOperations	string	多值	根据需要授权的操作过滤对 CreateGrant 操作的访问权限。
kms:GranteePrincipal	string	单值	根据授权中的被授权方主体过滤对 CreateGrant 操作的访问权限。
kms:KeyOrigin	string	单值	根据创建或使用操作 KMS 密钥的 origin 属性过滤对 API 操作的访问。
kms:KeySpec	string	单值	根据创建或使用操作 KMS 密钥的 key_spec 属性过滤对 API 操作的访问。
kms:KeyUsage	string	单值	根据创建或使用操作 KMS 密钥的 key_usage 属性过滤对 API 操作的访问。
kms:MessageType	string	单值	根据请求中的 message_type 参数的值过滤对签名和验证签名操作的访问。
kms:RetiringPrincipal	string	单值	根据授权中的 retiring_principal 筛选对 CreateGrant 操作的访问。
kms:SigningAlgorithm	string	单值	根据请求中的 signing_algorithm 过滤对签名和验证操作的访问。
kms:ExpirationTime	date	单值	根据请求中的 expiration_time 参数的值过滤对 ImportKeyMaterial 操作的访问。
kms:WrappingAlgorithm	string	单值	根据请求中的 wrapping_algorithm 参数的值过滤对 CreateParametersForImport 操作的访问。
kms:RecipientAttestation	string	单值	根据请求中证明文档的平台配置寄存器（PCR）值控制 CreateDatakey、DecryptData、DecryptDatakey 和 CreateRandom 操作的访问。
kms:MacAlgorithm	string	单值	根据请求中的 mac_algorithm 过滤对生成/校验消息验证码操作的访问。
kms:RequestAlias	string	单值	根据请求中的 key_id 属性过滤对 API 操作的访问。
kms:ResourceAliases	string	多值	根据使用操作 KMS 密钥的 alias 属性过滤对 API 操作的访问。

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
kms:MultiRegionKeyType	string	单值	根据使用操作 KMS 密钥的多区域密钥类型属性过滤对 API 操作的访问。
kms:PrimaryRegion	string	单值	根据请求中的 primary_region 属性过滤对 API 操作的访问。
kms:EncryptionContext	string	单值	根据请求中的 additional_authenticated_data 属性过滤对 API 操作的访问。
kms:ScheduleKeyDeletionPendingWindowInDays	numeric	单值	根据请求中的 pending_days 属性过滤对 API 操作的访问。
csms:Type	string	单值	根据凭据的类型筛选访问权限。
csms:KmsKeyId	string	单值	根据 KMS 密钥 ID 筛选访问权限。
csms:VersionId	string	单值	根据凭据版本 ID 筛选访问权限。
csms:VersionStage	string	单值	根据凭据版本状态筛选访问权限。
csms:RecoveryWindowInDays	numeric	单值	根据凭据删除等待时间筛选访问权限。
kps:KmsKeyId	string	单值	根据请求中的 kms 密钥的 ID 过滤访问权限。
kps:Algorithm	string	单值	根据请求中的 SSH 密钥对密钥算法过滤访问权限。

3.7.2 DDoS 防护 AAD

3.7.2.1 原生基础防护

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

 版权所有 © 华为云计算技术有限公司

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 Anti-DDoS 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 Anti-DDoS 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 Anti-DDoS 的相关操作。

表3-127 Anti-DDoS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
anti-ddos:task:list	授予查询 Anti-DDoS 任务权限。	List	-	-	-
anti-ddos:quota:list	授予查询配额权限。	List	-	-	-
anti-ddos:optionalDefensePolicy:list	授予查询 Anti-DDoS 配置可选范围权限。	List	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
anti-ddos:logConfig:update	授予更新云日志服务配置权限。	Write	-	-	-
anti-ddos:logConfig:get	授予查询云日志服务配置权限。	Read	-	-	-
anti-ddos:ip:updateDefensePolicy	授予更新 Anti-DDoS 服务权限。	Write	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
anti-ddos:ip:untagResource	授予批量删除标签权限。	Write	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
anti-ddos:ip:tagResource	授予批量添加标签权限。	Write	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
anti-ddos:ip:listTagsForResource	授予查询资源标签列表权限。	List	ip *	-	-
anti-ddos:ip:listDefenseStatuses	授予查询 EIP 防护状态列表权限。	List	ip *	-	-
anti-ddos:ip:getWeeklyReport	授予查询周防护统计情况权限。	Read	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
anti-ddos:ip:getDefenseStatus	授予查询指定 EIP 防护状态权限。	Read	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
anti-ddos:ip:getDefe	授予查询 Anti-	Read	ip *	• g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
nsePolicy	DDoS 服务权限。			key> • g:EnterpriseProjectId	
anti-ddos:ip:getDailyTrafficReport	授予查询指定 EIP 防护流量权限。	Read	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
anti-ddos:ip:getDailyEventReport	授予查询指定 EIP 异常事件权限。	Read	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
anti-ddos:ip:enableDefensePolicy	授予开通 Anti-DDoS 服务权限。	Write	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
anti-ddos:ip:disableDefensePolicy	授予关闭 Anti-DDoS 服务权限。	Write	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
anti-ddos:defaultDefensePolicy:get	授予查询 Anti-DDoS 默认防护策略权限。	Read	-	-	-
anti-ddos:defaultDefensePolicy:delete	授予删除 Anti-DDoS 默认防护策略权限。	Write	-	-	-
anti-ddos:defaultDefensePolicy:create	授予配置 Anti-DDoS 默认防护策略权限。	Write	-	-	-
anti-ddos:alertConfig:update	授予更新告警配置信息权限。	Write	-	-	-
anti-ddos:alertConfi	授予查询告警配置信息权	Read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
g:get	限。				

Anti-DDoS 的 API 通常对应着一个或多个授权项。表 3-128 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-128 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/query-task-status	anti-ddos:task:list	-
GET /v1/{project_id}/antiddos/quotas	anti-ddos:quota:list	-
GET /v1/{project_id}/antiddos/query-config-list	anti-ddos:optionalDefensePolicy:list	-
PUT /v1/{project_id}/antiddos/lts-config	anti-ddos:logConfig:update	-
GET /v1/{project_id}/antiddos/lts-config	anti-ddos:logConfig:get	-
PUT /v1/{project_id}/antiddos/{floating_ip_id}	anti-ddos:ip:updateDefensePolicy	-
DELETE /v1/{project_id}/antiddos-ip/{resource_id}/tags/delete	anti-ddos:ip:untagResource	-
POST /v1/{project_id}/antiddos-ip/{resource_id}/tags/create	anti-ddos:ip:tagResource	-
GET /v1/{project_id}/antiddos-ip/{resource_id}/tags	anti-ddos:ip:listTagsForResource	-
GET /v1/{project_id}/antiddos-ip/tags	anti-ddos:ip:listTagsForResource	-
GET /v1/{project_id}/antiddos	anti-ddos:ip:listDefenseStatuses	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/antiddos-ip/resource-instances/count	anti-ddos:ip:listDefenseStatuses	-
POST /v1/{project_id}/antiddos-ip/resource-instances/filter	anti-ddos:ip:listDefenseStatuses	-
GET /v1/{project_id}/antiddos/weekly	anti-ddos:ip:getWeeklyReport	-
GET /v1/{project_id}/antiddos/weekly-export	anti-ddos:ip:getWeeklyReport	-
GET /v1/{project_id}/antiddos/{floating_ip_id}/status	anti-ddos:ip:getDefenseStatus	-
GET /v1/{project_id}/antiddos/{floating_ip_id}	anti-ddos:ip:getDefensePolicy	-
GET /v1/{project_id}/antiddos/queryIsEnabledResult/query	anti-ddos:ip:getDefensePolicy	-
GET /v1/{project_id}/antiddos/{floating_ip_id}/daily	anti-ddos:ip:getDailyTrafficReport	-
GET /v1/{project_id}/antiddos/{floating_ip_id}/daily-export	anti-ddos:ip:getDailyTrafficReport	-
GET /v1/{project_id}/antiddos/{floating_ip_id}/logs	anti-ddos:ip:getDailyEventReport	-
POST /v1/{project_id}/antiddos/{floating_ip_id}	anti-ddos:ip:enableDefensePolicy	-
POST /v1/{project_id}/antiddos/immediate_protection	anti-ddos:ip:enableDefensePolicy	-
DELETE /v1/{project_id}/antiddos/{floating_ip_id}	anti-ddos:ip:disableDefensePolicy	-
DELETE /v1/{project_id}/antiddos/{floating_ip_id}/closeAndReason	anti-ddos:ip:disableDefensePolicy	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/antiddos/default/config	anti-ddos:defaultDefensePolicy:get	-
DELETE /v1/{project_id}/antiddos/default/config	anti-ddos:defaultDefensePolicy:delete	-
POST /v1/{project_id}/antiddos/default/config	anti-ddos:defaultDefensePolicy:create	-
POST /v2/{project_id}/warnalert/alertconfig/update	anti-ddos:alertConfig:update	-
GET /v2/{project_id}/warnalert/alertconfig/query	anti-ddos:alertConfig:get	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-129 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

Anti-DDoS 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-129 Anti-DDoS 支持的资源类型

资源类型	URN
ip	anti-ddos:<region>:<account-id>:ip:<ip-id>

条件（Condition）

Anti-DDoS 服务不支持在身份策略中的条件键中配置服务级的条件键。Anti-DDoS 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.7.2.2 原生高级防护

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

 版权所有 © 华为云计算技术有限公司

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 CNAD 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 CNAD 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 CNAD 的相关操作。

表3-130 CNAD 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cnad:schedule:update	授予更新调度规格的权限。	Write	schedule *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cnad:schedule:list	授予查询调度规则列表的权限。	List	schedule *	-	-
cnad:schedule:get	授予查询调度规则的权限。	Read	schedule *	-	-
cnad:schedule:delete	授予删除调度规则的权限。	Write	schedule *	-	-
cnad:schedule:create	授予创建调度规则的权限。	Write	schedule *	-	-
cnad:quota:update	授予修改配额的权限。	Write	-	-	-
cnad:blockade:release	授予解封 IP 的权限。	Write	-	-	-
cnad:blockade:list	授予查询封堵记录列表的权限。	List	-	-	-
cnad:blockade:get	授予查询封堵记录的权限。	Read	-	-	-
cnad:alarmConfig:update	授予修改告警通知的权限。	Write	-	-	-
cnad:alarmConfig:create	授予创建告警通知的权限。	Write	-	-	-
cnad:alarmConfig:delete	授予删除告警通知的权限。	Write	-	-	-
cnad:alarmConfig:get	授予查询告警通知的权限。	Read	-	-	-
cnad:attackReport:list	授予查询攻击事件的权限。	List	-	-	-
cnad:attackReport:update	授予更新攻击事件配置的权限。	Write	-	-	cnad:attackReport:list
cnad:attackTop:list	授予查询 Top10 被攻击 IP 的权限。	List	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cnad:attackTypeReport:list	授予查询攻击类型分布的权限。	List	-	-	-
cnad:bindPolicy:create	授予绑定防护策略到防护 IP 的权限。	Write	-	-	-
cnad:blackWhiteIpList:create	授予创建 IP 黑白名单的权限。	Write	-	-	-
cnad:blackWhiteIpList:delete	授予删除 IP 黑白名单的权限。	Write	-	-	-
cnad:cleanCountReport:list	授予查询 DDoS 防护趋势的权限。	List	-	-	-
cnad:cleanKbpsReport:list	授予查询清洗流量峰值统计数据的权限。	List	-	-	-
cnad:cleanScaleDropList:list	授予查询清洗范围的权限。	List	-	-	-
cnad:countReport:get	授予查询统计数据的权限。	Read	-	-	-
cnad:ipTag:put	授予更新防护 IP 标签的权限。	Write	-	-	-
cnad:package:create	授予创建实例的权限。	Write	package *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cnad:package:get	授予查询实例信息的权限。	Read	package *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cnad:package:li	授予查询实例	List	packa	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
st	列表的权限。		ge *		
cnad:package:put	授予更新实例的权限。	Write	package *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
cnad:packageDropList:list	授予查询实例摘要列表的权限。	List	-	-	-
cnad:packetAttackReport:list	授予查询攻击数据包的权限。	List	-	-	-
cnad:policy:create	授予创建防护策略的权限。	Write	policy *	g:EnterpriseProjectId	-
cnad:policy:delete	授予删除防护策略的权限。	Write	policy *	g:EnterpriseProjectId	-
cnad:policy:get	授予查询单个防护策略详情的权限。	Read	policy *	g:EnterpriseProjectId	-
cnad:policy:list	授予查询防护策略详情的权限。	List	policy *	-	-
cnad:policy:put	授予更新防护策略的权限。	Write	policy *	g:EnterpriseProjectId	-
cnad:policyDropList:list	授予查询防护策略列表的权限。	List	-	-	-
cnad:protectedIp:create	授予绑定防护IP到实例的权限。	Write	-	-	-
cnad:protectedIp:list	授予查询防护IP列表的权限。	List	-	-	-
cnad:protectedIpDropList:list	授予查询防护IP下拉列表的	List	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	权限。				
cnad:quota:get	授予查询配额的权限。	Read	-	-	-
cnad:securityStatusReport:get	授予查询资产安全状态的权限。	Read	-	-	-
cnad:trafficAttackReport:list	授予查询攻击流量的权限。	List	-	-	-
cnad:policy:unbind	授予移除防护IP的防护策略的权限。	Write	-	-	cnad:unbindPolicy:create
cnad:weekStatisticsReport:get	授予查询每周安全统计数据的权限。	Read	-	-	-

CNAD的API通常对应着一个或多个授权项。表 3-131 展示了API与授权项的关系，以及该API需要依赖的授权项。

表3-131 API与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1/unblockservice/{domain_id}/unblock-quota-statistics	cnad:quota:get	-
POST /v1/unblockservice/{domain_id}/unblock	cnad:blockade:release	-
GET /v1/unblockservice/{domain_id}/unblock-record	cnad:blockade:list	-
GET /v1/unblockservice/{domain_id}/block-statistics	cnad:blockade:get	-
POST /v1/cnad/alarm-config	cnad:alarmConfig:update	-
DELETE /v1/cnad/alarm-config	cnad:alarmConfig:de	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	lete	
GET /v1/cnad/alarm-config	cnad:alarmConfig:get	-
POST /v1/cnad/policies/{policy_id}/bind	cnad:bindPolicy:create	-
POST /v1/cnad/policies/{policy_id}/ip-list/add	cnad:blackWhiteIpList:create	-
POST /v1/cnad/policies/{policy_id}/ip-list/delete	cnad:blackWhiteIpList:delete	-
PUT /v1/cnad/protected-ips/tags	cnad:ipTag:put	-
GET /v1/cnad/packages	cnad:package:list	-
PUT /v1/cnad/packages/{package_id}/name	cnad:package:put	-
POST /v1/cnad/policies	cnad:policy:create	-
DELETE /v1/cnad/policies/{policy_id}	cnad:policy:delete	-
GET /v1/cnad/policies/{policy_id}	cnad:policy:get	-
GET /v1/cnad/policies	cnad:policy:list	-
PUT /v1/cnad/policies/{policy_id}	cnad:policy:put	-
POST /v1/cnad/packages/{package_id}/protected-ips	cnad:protectedIp:create	-
GET /v1/cnad/protected-ips	cnad:protectedIp:list	-
GET /v1/cnad/packages/{package_id}/unbound-protected-ips	cnad:protectedIpDropList:list	-
POST /v1/cnad/policies/{policy_id}/unbind	cnad:policy:unbind	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-132 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

 版权所有 © 华为云计算技术有限公司

CNAD 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-132 CNAD 支持的资源类型

资源类型	URN
policy	cnad::<account-id>:policy:<policy-id>
schedule	cnad::<account-id>:schedule:<schedule-id>
package	cnad::<account-id>:package:<package-id>

条件（Condition）

CNAD 服务不支持在身份策略中的条件键中配置服务级的条件键。CNAD 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.7.2.3 DDoS 高防

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。

 版权所有 © 华为云计算技术有限公司

  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 AAD 定义的资源类型的详细信息请参见资源类型（Resource）。

- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 AAD 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 AAD 的相关操作。

表3-133 AAD 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
aad:alarmConfig:create	授予创建告警设置的权限。	Write	alarmConfig *	-	-
aad:alarmConfig:put	授予修改告警设置的权限。	Write	alarmConfig *	-	-
aad:alarmConfig:get	授予查询告警设置的权限。	Read	alarmConfig *	-	-
aad:alarmConfig:delete	授予删除告警设置的权限。	Write	alarmConfig *	-	-
aad:certificate:delete	授予删除证书的权限。	Write	certificate *	-	-
aad:certificate:list	授予查询证书列表的权限。	List	certificate *	-	-
aad:certificate:set	授予修改域名对应证书的权限。	Write	certificate *	-	-
			domain *	g:EnterpriseProjectId	
aad:dashboard:delete	授予删除报表日志配置的权限。	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
aad:dashboard:get	授予获取报表数据和日志配置的权限。	Read	-	-	-
aad:dashboard:set	授予修改报表日志配置的权限。	Write	-	-	-
aad:domain:create	授予添加防护域名的权限。	Write	domain *	g:EnterpriseProjectId	-
aad:domain:delete	授予删除防护域名的权限。	Write	domain *	g:EnterpriseProjectId	-
aad:domain:get	授予查询防护域名详情的权限。	Read	domain *	g:EnterpriseProjectId	-
aad:domain:list	授予查询域名列表的权限。	List	domain *	g:EnterpriseProjectId	-
aad:domain:put	授予修改域名防护属性的权限。	Write	domain *	g:EnterpriseProjectId	-
aad:forwardingRule:create	授予添加转发规则的权限。	Write	forwardingRule *	g:EnterpriseProjectId	-
aad:forwardingRule:delete	授予删除转发规则的权限。	Write	forwardingRule *	g:EnterpriseProjectId	-
aad:forwardingRule:get	授予查询转发规则的权限。	Read	forwardingRule *	g:EnterpriseProjectId	-
aad:forwardingRule:list	授予导出转发规则的权限。	List	forwardingRule *	g:EnterpriseProjectId	-
aad:forwardingRule:put	授予修改转发规则中的回源IP 的权限。	Write	forwardingRule *	g:EnterpriseProjectId	-
aad:instance:create	授予创建实例的权限。	Write	instance *	g:EnterpriseProjectId	-
aad:instance:get	授予查询实例	Read	instan	g:EnterprisePro	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	属性的权限。		ce *	jectId	
aad:instance:list	授予查询实例列表的权限。	List	instance *	g:EnterpriseProjectId	-
aad:instance:put	授予修改实例属性的权限。	Write	instance *	g:EnterpriseProjectId	-
aad:policy:create	授予添加防护规则的权限。	Write	policy *	g:EnterpriseProjectId	-
aad:policy:delete	授予删除防护规则的权限。	Write	policy *	g:EnterpriseProjectId	-
aad:policy:get	授予查询防护规则详情的权限。	Read	policy *	g:EnterpriseProjectId	-
aad:policy:list	授予查询防护规则列表的权限。	List	policy *	g:EnterpriseProjectId	-
aad:policy:put	授予修改防护规则的权限。	Write	policy *	g:EnterpriseProjectId	-
aad:quotas:get	授予查询防护规格的权限。	Read	-	-	-
aad:whiteBlackIpRule:create	授予添加防护黑白名单的权限。	Write	whiteBlackIpRule *	g:EnterpriseProjectId	-
aad:whiteBlackIpRule:delete	授予删除防护黑白名单的权限。	Write	whiteBlackIpRule *	g:EnterpriseProjectId	-
aad:whiteBlackIpRule:list	授予查询防护黑白名单列表的权限。	List	whiteBlackIpRule *	g:EnterpriseProjectId	-
aad:protectedIp:put	授予修改防护对象标签的权限。	Write	-	-	-
aad:protectedIp:list	授予查询防护对象列表的权	List	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
aad:package:put	授予修改防护包的权限。	Write	package *	-	-
aad:package:list	授予查询防护包列表的权限。	List	package *	-	-
aad:block:put	授予解封 IP 的权限。	Write	-	-	-
aad:block:list	授予查询封堵 ip 列表的权限。	List	-	-	-
aad:block:get	授予查询封堵和解封信息的权限。	Read	-	-	-

AAD 的 API 通常对应着一个或多个授权项。表 3-134 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-134 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/cad/alart/config	aad:alarmConfig:create	-
POST /v1/cnad/alarm-config	aad:alarmConfig:put	-
DELETE /v1/cnad/alarm-config	aad:alarmConfig:delete	-
GET /v1/{project_id}/cad/alart/list	aad:alarmConfig:get	-
GET /v1/cnad/alarm-config	aad:alarmConfig:get	-
DELETE /v1/aad/certificate/del	aad:certificate:delete	-
GET /v1/{project_id}/cad/domains/certificatelist	aad:certificate:list	-
GET /v1/aad/certificate-details	aad:certificate:list	-
POST /v1/{project_id}/cad/domains/certifi	aad:certificate:set	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
cate		
POST /v1/aad/configs/lts/delete	aad:dashboard:delete	-
GET /v1/{project_id}/cad/ddosinfo/events_type	aad:dashboard:get	-
GET /v1/aad/configs/lts_region	aad:dashboard:get	-
GET /v1/aad/configs/lts	aad:dashboard:get	-
GET /v1/{project_id}/waf/event/timeline	aad:dashboard:get	-
GET /v1/{project_id}/waf/event/request/peak	aad:dashboard:get	-
GET /v1/{project_id}/waf/event/attack/type	aad:dashboard:get	-
GET /v1/{project_id}/waf/event/attack/source/num	aad:dashboard:get	-
GET /v1/{project_id}/waf/event/attack/source	aad:dashboard:get	-
GET /v1/{project_id}/cad/instances/flow_pps	aad:dashboard:get	-
GET /v1/{project_id}/cad/instances/flow_bps	aad:dashboard:get	-
GET /v1/{project_id}/cad/instances/events	aad:dashboard:get	-
GET /v1/{project_id}/cad/ddosinfo/peak	aad:dashboard:get	-
POST /v1/aad/configs/lts	aad:dashboard:set	-
POST /v1/{project_id}/aad/domains	aad:domain:create	-
POST /v1/{project_id}/cad/domains/del	aad:domain:delete	-
GET /v1/{project_id}/aad/domains/{domain_id}/service-config	aad:domain:get	-
GET	aad:domain:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/cad/domains/ports		
GET /v1/{project_id}/cad/domains/name	aad:domain:get	-
GET /v1/{project_id}/cad/domains/line/{enterprise_project_id}	aad:domain:list	-
GET /v1/{project_id}/cad/domains/instances	aad:domain:get	-
GET /v1/{project_id}/cad/domains/brief	aad:domain:get	-
GET /v1/{project_id}/aad/domains/waf-list	aad:domain:list	-
GET /v1/{project_id}/cad/domains	aad:domain:list	-
POST /v1/{project_id}/aad/domains/{domain_id}/service-config	aad:domain:put	-
POST /v1/{project_id}/cad/domains/switch	aad:domain:put	-
POST /v1/{project_id}/cad/domains/cnameDispatchSwitch	aad:domain:put	-
POST /v1/{project_id}/cad/domains/cname/switch	aad:domain:put	-
POST /v1/{project_id}/cad/instances/protocol_rule	aad:forwardingRule:create	-
POST /v1/{project_id}/cad/instances/protocol_rule/import	aad:forwardingRule:create	-
DELETE /v1/{project_id}/cad/instances/protocol_rule/{rule_id}	aad:forwardingRule:delete	-
POST /v1/{project_id}/cad/instances/protocol_rule/batchdel	aad:forwardingRule:delete	-
GET /v1/{project_id}/cad/instances/rules	aad:forwardingRule:get	-
GET /v1/{project_id}/cad/instances/proto	aad:forwardingRule:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
col_rule/export		
PUT /v1/{project_id}/cad/instances/protocol_rule/{rule_id}	aad:forwardingRule:put	-
POST /v1/{project_id}/cad/instances/cad_open	aad:instance:create	-
GET /v1/{project_id}/cad/products	aad:instance:create	-
GET /v1/{project_id}/{resource_type}/{resource_id}/tags	aad:instance:get	-
GET /v1/{project_id}/cad/upgradeproducts/{instance_id}	aad:instance:get	-
GET /v1/{project_id}/cad/instances/detail/{instance_id}	aad:instance:get	-
GET /v1/{project_id}/aad/instances/brief-list	aad:instance:list	-
GET /v1/{project_id}/cad/sourceip	aad:instance:list	-
GET /v1/{project_id}/cad/instances	aad:instance:list	-
POST /v1/{project_id}/{resource_type}/{resource_id}/tags/action	aad:instance:put	-
POST /v1/{project_id}/cad/instances/cad_spec_upgrade	aad:instance:put	-
PUT /v1/{project_id}/cad/instances/{instance_id}/name	aad:instance:put	-
PUT /v1/{project_id}/cad/instances/{instance_id}/elastic/{ip_id}	aad:instance:put	-
POST /v1/{project_id}/aad/policies/waf/cc	aad:policy:create	-
POST /v1/cnad/policies	aad:policy:create	-
DELETE /v1/{project_id}/aad/policies/waf/cc/{rule_id}	aad:policy:delete	-
DELETE	aad:policy:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/cnad/policies/{policy_id}		
GET /v1/{project_id}/cad/flowblock	aad:policy:get	-
GET /v1/cnad/policies/{policy_id}	aad:policy:get	-
GET /v1/{project_id}/aad/policies/waf/cc	aad:policy:list	-
GET /v1/cnad/policies	aad:policy:list	-
PUT /v1/{project_id}/aad/policies/waf/cc/{rule_id}	aad:policy:put	-
POST /v1/{project_id}/cad/flowblock/udp	aad:policy:put	-
POST /v1/{project_id}/cad/flowblock/foreign	aad:policy:put	-
POST /v1/cnad/policies/{policy_id}/ip-list/add	aad:policy:put	-
POST /v1/cnad/policies/{policy_id}/bind	aad:policy:put	-
POST /v1/cnad/policies/{policy_id}/ip-list/delete	aad:policy:put	-
POST /v1/cnad/policies/{policy_id}/unbind	aad:policy:put	-
PUT /v1/cnad/policies/{policy_id}	aad:policy:put	-
GET /v1/{project_id}/aad/quotas/domain-port	aad:quotas:get	-
GET /v1/{project_id}/scc/waf/quota	aad:quotas:get	-
GET /v1/{project_id}/cad/quotas	aad:quotas:get	-
GET /v1/{project_id}/cad/ip/quotas	aad:quotas:get	-
GET /v1/{project_id}/cad/bwlist/quota	aad:quotas:get	-
GET /v1/{project_id}/aad/user-configs	aad:quotas:get	-
POST /v1/{project_id}/cad/bwlist	aad:whiteBlackIpRule:create	-
POST /v1/{project_id}/cad/bwlist/delete	aad:whiteBlackIpRule:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/cad/bwlist	aad:whiteBlackIpRule:list	-
PUT /v1/cnad/protected-ips/tags	aad:protectedIp:put	-
GET /v1/cnad/protected-ips	aad:protectedIp:list	-
POST /v1/cnad/packages/{package_id}/protected-ips	aad:package:put	-
PUT /v1/cnad/packages/{package_id}/name	aad:package:put	-
GET /v1/cnad/packages	aad:package:list	-
GET /v1/cnad/packages/{package_id}/unbound-protected-ips	aad:package:list	-
POST /v1/unblockservice/{domain_id}/unblock	aad:block:put	-
GET /v1/unblockservice/{domain_id}/block-list	aad:block:list	-
GET /v1/unblockservice/{domain_id}/unblock-quota-statistics	aad:block:get	-
GET /v1/unblockservice/{domain_id}/block-statistics	aad:block:get	-
GET /v1/unblockservice/{domain_id}/unblock-record	aad:block:get	-
GET /v1/{project_id}/cad/instances/{instance_id}/elastic_count/{ip_id}	aad:instance:get	-
GET /v1/{project_id}/cad/instances/{data_center}/elastic/{line}/{ip_id}	aad:instance:get	-
GET /v1/aad/remain-vip-number	aad:quotas:get	-
GET /v1/aad/instance/connection-num	aad:dashboard:get	-
PUT /v1/{project_id}/cad/instances/{instance_id}/pp-switch	aad:instance:put	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/aad-service/ces/{domain_id}/dims-info	aad:instance:list	-
GET /v1/aad-service/ces/v2/{domain_id}/instances	aad:instance:list	-
GET /v1/{project_id}/cad/instances/security-statistics	aad:instance:list	-
GET /v1/aad/domain/instances/rules	aad:domain:list	-
POST /v1/aad/policy/modify	aad:policy:put	-
POST /v1/aad/geoip	aad:policy:put	-
GET /v1/aad/geoip	aad:policy:get	-
DELETE /v1/aad/geoip/{ruleId}	aad:policy:delete	-
PUT /v1/aad/geoip/{ruleId}	aad:policy:put	-
POST /v1/aad/whiteip	aad:policy:put	-
GET /v1/aad/whiteip	aad:policy:get	-
DELETE /v1/aad/whiteip	aad:policy:delete	-
POST /v1/aad/custom	aad:policy:put	-
GET /v1/aad/custom	aad:policy:get	-
PUT /v1/aad/custom/{ruleId}	aad:policy:put	-
DELETE /v1/aad/custom/{ruleId}	aad:policy:delete	-
GET /v1/aad/policy/details	aad:policy:get	-
POST /v1/aad/cc/intelligent/modify	aad:policy:put	-
GET /v1/aad/geoip/map	aad:policy:get	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-135 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

AAD 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-135 AAD 支持的资源类型

资源类型	URN

 版权所有 © 华为云计算技术有限公司

资源类型	URN
forwardingRule	aad::<account-id>:forwardingRule:<forwarding-rule-id>
package	aad::<account-id>:package:<package-id>
policy	aad::<account-id>:policy:<policy-id>
alarmConfig	aad::<account-id>:alarmConfig:<alarm-config-id>
domain	aad::<account-id>:domain:<domain-id>
certificate	aad::<account-id>:certificate:<certificate-id>
instance	aad::<account-id>:instance:<instance-id>
whiteBlackIpRule	aad::<account-id>:whiteBlackIpRule:<white-black-ip-rule-id>

条件（Condition）

AAD 服务不支持在身份策略中的条件键中配置服务级的条件键。AAD 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.7.3 云防火墙 CFW

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。

 版权所有 © 华为云计算技术有限公司

  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 CFW 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 CFW 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 CFW 的相关操作。

表3-136 CFW 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cfw:instance:listDomainParseServers	授予查询域名解析服务器列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:domain:get
cfw:instance:updateDomainParseServer	授予更新域名解析服务器的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:acl:put
cfw:domainGroup:update	授予更新域名组的权限。	Write	domainGroup *	-	cfw:ipGroup:put
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
cfw:domainGroup:delete	授予删除域名组的权限。	Write	domainGroup *	-	cfw:ipGroup:delete

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
cfw:domainGroup:list	授予列出域名组列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:ipGroup:list
cfw:instance:listAdvanceIpsRules	授予查询云防火墙高级 ips 规则列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:ipsMode:get
cfw:instance:updateCustomRule	授予更新云防火墙用户自定义 ips 的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:ipsMode:operate
cfw:instance:updateLogConfig	授予更新云防火墙 LTS 日志配置的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:instance:upgrade
			-	cfw:LogGroupId	
cfw:instance:createCaptureTask	授予创建云防火墙抓包任务的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:captureTask:create
cfw:instance:createCustomRule	授予创建云防火墙自定义 IPS 规则的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:ipsMode:operate
cfw:instance:createTags	授予创建云防火墙标签的权	Tagging	instance *	• g:EnterpriseProjectId • g:ResourceT	cfw:instance:upgrade

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。			ag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
cfw:instance:deleteInstance	授予删除云防火墙实例的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:instance:delete
cfw:instance:deleteCaptureTask	授予删除云防火墙抓包任务的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:captureTask:delete
cfw:instance:deleteCustomRule	授予删除云防火墙用户自定义 IPS 规则的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:ipsMode:operate
cfw:instance:deleteTags	授予删除云防火墙标签的权限。	Tagging	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:instance:upgrade
			-	g:TagKeys	
cfw:instance:getCaptureTaskResult	授予查询云防火墙抓包任务结果的权限。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:captureTask:getResult
cfw:instance:listProjectTags	授予查询云防火墙项目标签列表的权限。	List	-	-	cfw:instance:list
cfw:instance:getRegionDb	授予查询云防火墙地理位置库的权限。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:acl:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cfw:instance:listAccessControlLog	授予查询云防火墙访问控制日志列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:accessControlLog:list
cfw:instance:listAttackLog	授予查询云防火墙攻击日志列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:attackLog:list
cfw:instance:listCaptureTask	授予查询云防火墙抓包任务列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:captureTask:list
cfw:instance:listCustomRule	授予查询云防火墙用户自定义 IPS 列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:ipsMode:get
cfw:instance:getEw	授予查询云防火墙东西向墙的权限。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:instance:list
cfw:instance:listFlowLog	授予展示云防火墙流量日志列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:flowLog:list
cfw:instance:listIpsRule	授予展示云防火墙 IPS 规则列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:ipsMode:get
cfw:instance:updateAdvanceIpsRule	授予更新云防火墙高级 ips 规则的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:ipsMode:operate

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cfw:instance:saveTags	授予替换云防火墙标签的权限。	Tagging	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:instance:upgrade
			-	• g:RequestTag/<tag-key> • g:TagKeys	
cfw:instance:stopCaptureTask	授予停止云防火墙抓包任务的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:captureTask:stop
cfw:instance:updateAlarmConfig	授予更新云防火墙告警配置的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:instance:create
cfw:instance:getAlarmConfig	授予查询云防火墙告警配置的权限。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	cfw:instance:list
cfw:instance:enableMultiAccount	授予开启云防火墙多账号管理的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cfw:instance:listAccounts	授予查看多账号列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cfw:instance:listOrganizationTree	授予查看组织树的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cfw:instance:addAccount	授予添加账号	Write	instance *	• g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	的权限。			key> • g:EnterpriseProjectId	
cfw:instance:updateAntiVirusRule	授予更新云防火墙反病毒规则的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cfw:instance:getAntiVirusRule	授予查看云防火墙反病毒规则的权限。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cfw:instance:createReportProfile	授予创建防火墙周报模板的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cfw:instance:updateReportProfile	授予更新防火墙周报模板的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
cfw:instance:deleteReportProfile	授予删除防火墙周报模板的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

CFW 的 API 通常对应着一个或多个授权项。表 3-137 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-137 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/cfw/logs/flow	cfw:instance:listFlowLog	-
GET	cfw:instance:listAccessControl	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/cfw/logs/access-control	Log	
GET /v1/{project_id}/cfw/logs/attack	cfw:instance:listAttackLog	-
PUT /v1/{project_id}/cfw/logs/configuration	cfw:instance:updateLogConfig	-
GET /v1/{project_id}/acl-rule/import-status	cfw:acl:getImportStatus	-
POST /v1/{project_id}/firewall/east-west	cfw:instance:createInstance	• er:instances:list • er:instances:listVpcAttachments • er:attachments:create • vpc:vpcs:list • vpc:subnets:get • vpc:subnets:create • vpc:routeTables:list • vpc:routeTables:update • vpc:quotas:list • nat:natGateways:list
DELETE /v2/{project_id}/firewall/{resource_id}	cfw:instance:deleteInstance	-
GET /v1/{project_id}/ips-rule	cfw:instance:listIpsRule	-
GET /v1/{project_id}/regions	cfw:instance:getRegionDb	-
GET /v1/{project_id}/advanced-ips-rules	cfw:instance:listAdvanceIpsRules	-
POST /v1/{project_id}/advanced-ips-rule	cfw:instance:updateAdvanceIpsRule	-
GET /v1/{project_id}/ips/custom-rule	cfw:instance:listCustomRule	-
PUT /v1/{project_id}/ips/cu	cfw:instance:updateCustomRule	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
stom-rule/{ips_cfw_id}		
POST /v1/{project_id}/ips/custom-rule/batch-delete	cfw:instance:deleteCustomRule	-
POST /v1/{project_id}/ips/custom-rule	cfw:instance:createCustomRule	-
GET /v1/{project_id}/cfw/alarm/config	cfw:instance:getAlarmConfig	-
PUT /v1/{project_id}/cfw/alarm/config	cfw:instance:updateAlarmConfig	-
GET /v1/{project_id}/firewall/east-west	cfw:instance:getEw	• er:instances:listVpcAttachments • vpc:vpcs:list • nat:natGateways:list • er:instances:listVpcAttachments • er:instances:get
POST /v2/{project_id}/cfw-cfw/{fw_instance_id}/tags/create	cfw:instance:createTags	-
DELETE /v2/{project_id}/cfw-cfw/{fw_instance_id}/tags/delete	cfw:instance:deleteTags	-
PUT /v2/{project_id}/cfw-cfw/{fw_instance_id}/tags/save	cfw:instance:saveTags	-
GET /v2/{project_id}/cfw-cfw/tags	cfw:instance:listProjectTags	-
GET /v1/{project_id}/capture-task	cfw:instance:listCaptureTask	-
POST /v1/{project_id}/capture-task	cfw:instance:createCaptureTask	-
POST	cfw:instance:stopCaptureTask	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/capture-task/stop		
POST /v1/{project_id}/capture-task/batch-delete	cfw:instance:deleteCaptureTask	-
GET /v1/{project_id}/capture-task/capture-result	cfw:instance:getCaptureTaskResult	-
GET /v1/{project_id}/dns/servers	cfw:instance:listDomainParseServers	-
PUT /v1/{project_id}/dns/servers	cfw:instance:updateDomainParseServer	-
PUT /v1/{project_id}/domain-set/{set_id}	cfw:domainGroup:update	-
DELETE /v1/{project_id}/domain-set/{set_id}	cfw:domainGroup:delete	-
GET /v1/{project_id}/domain-sets	cfw:domainGroup:list	-
POST /v1/{project_id}/system/multi-account/enable	cfw:instance:enableMultiAccount	• organizations:trustedServices:list • organizations:organizations:get • organizations:trustedServices:enable
GET /v1/{project_id}/system/multi-account/accounts	cfw:instance:listAccounts	• organizations:trustedServices:list • organizations:organizations:get • organizations:delegatedAdministrators:list
POST /v1/{project_id}/system/multi-account/accounts	cfw:instance:addAccount	• organizations:trustedServices:list • organizations:organizations:get • organizations:delegatedAdministrators:list • organizations:roots:list
GET	cfw:instance:listOrganizationT	• organizations:trustedServic

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/system/multi-account/organization-tree	ree	es:list • organizations:organizations:get • organizations:delegatedAdministrators:list • organizations:roots:list • organizations:ous:list • organizations:accounts:list
GET /v1/{project_id}/anti-virus/rule	cfw:instance:getAntiVirusRule	-
PUT /v1/{project_id}/anti-virus/rule	cfw:instance:updateAntiVirusRule	-
PUT /v1/{project_id}/report-profile/{report_profile_id}	cfw:instance:updateReportProfile	-
DELETE /v1/{project_id}/report-profile/{report_profile_id}	cfw:instance:deleteReportProfile	-
POST /v1/{project_id}/report-profile	cfw:instance:createReportProfile	-
DELETE /v1/{project_id}/address-items	cfw:ipGroup:deleteIpGroupMember	-
GET /v1/{project_id}/address-sets/{set_id}	cfw:ipGroup:getIpGroup	-
GET /v1/{project_id}/address-items	cfw:ipGroup:listIpGroupMember	-
GET /v1/{project_id}/address-sets	cfw:ipGroup:listIpGroups	-
DELETE /v1/{project_id}/domain-set/domains/{set_id}	cfw:domainGroup:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/service-items	cfw:serviceGroup:listServiceGroupMember	-
DELETE /v1/{project_id}/service-items/{item_id}	cfw:serviceGroup:deleteServiceGroupMember	-
POST /v1/{project_id}/black-white-list	cfw:blackWhiteList:create	-
DELETE /v1/{project_id}/service-sets/{set_id}	cfw:serviceGroup:delete	-
POST /v1/{project_id}/firewalls/list	cfw:instance:listInstance	-
PUT /v1/{project_id}/service-sets/{set_id}	cfw:serviceGroup:update	-
POST /v1/{project_id}/eip/protect	cfw:eip:updateProtectStatus	-
POST /v1/{project_id}/domain-set	cfw:domainGroup:create	-
GET /v1/{project_id}/firewall/exist	cfw:instance:getInstance	-
DELETE /v1/{project_id}/acl-rule	cfw:acl:deleteAclRule	-
GET /v1/{project_id}/domain/parse/{domain_name}	cfw:instance:listDomainParseServers	-
POST /v1/{project_id}/acl-rule/count	cfw:acl:listAclRules	-
DELETE /v1/{project_id}/address-sets/{set_id}	cfw:ipGroup:deleteIpGroup	-
POST /v1/{project_id}/domain-	cfw:domainGroup:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
set/domains/{set_id}		
GET /v1/{project_id}/service-sets	cfw:serviceGroup:list	-
GET /v2/{project_id}/cfw-acl/tags	cfw:acl:listAclTags	-
POST /v1/{project_id}/service-set	cfw:serviceGroup:create	-
DELETE /v1/{project_id}/service-items	cfw:serviceGroup:deleteServiceGroupMember	-
POST /v1/{project_id}/ips/switch	cfw:instance:updateIpsStatus	-
POST /v1/{project_id}/ips/protect	cfw:instance:updateIpsMode	-
GET /v1/{project_id}/service-sets/{set_id}	cfw:serviceGroup:get	-
DELETE /v1/{project_id}/acl-rule/count	cfw:acl:deleteHitCount	-
PUT /v1/{project_id}/address-sets/{set_id}	cfw:ipGroup:updateIpGroup	-
DELETE /v1/{project_id}/acl-rule/{acl_rule_id}	cfw:acl:deleteAclRule	-
PUT /v1/{project_id}/acl-rule/action	cfw:acl:updateAclRuleAction	-
POST /v1/{project_id}/address-set	cfw:ipGroup:createIpGroup	-
PUT /v1/{project_id}/black-white-list/{list_id}	cfw:blackWhiteList:update	-
DELETE /v1/{project_id}/address-items/{item_id}	cfw:ipGroup:deleteIpGroupMember	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/ips/switch	cfw:instance:getIpsStatus	-
PUT /v1/{project_id}/acl-rule/{acl_rule_id}	cfw:acl:updateAclRule	-
GET /v1/{project_id}/vpcs/protection	cfw:instance:listProtectedVpc	-
GET /v1/{project_id}/eip-count/{object_id}	cfw:eip:count	-
GET /v1/{project_id}/black-white-lists	cfw:blackWhiteList:list	-
GET /v1/{project_id}/eips/protect	cfw:eip:list	-
DELETE /v1/{project_id}/black-white-list/{list_id}	cfw:blackWhiteList:delete	-
GET /v1/{project_id}/acl-rules	cfw:acl:listAclRules	-
GET /v1/{project_id}/domain-set/domains/{domain_set_id}	cfw:domainGroup:list	-
POST /v1/{project_id}/acl-rule	cfw:acl:createAclRule	-
PUT /v1/{project_id}/acl-rule/order/{acl_rule_id}	cfw:acl:setPriority	-
POST /v1/{project_id}/address-items	cfw:ipGroup:createIpGroupMember	-
GET /v1/{project_id}/ips/protect	cfw:instance:getIpsMode	-
POST	cfw:serviceGroup:createServic	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/service-items	eGroupMember	
GET /v1/{project_id}/cfw/logs/configuration	cfw:instance:getLogConfig	-
POST /v1/{project_id}/cfw/logs/configuration	cfw:instance:updateLogConfig	-
POST /v2/{project_id}/firewall	cfw:instance:createInstance	-
GET /v3/{project_id}/jobs/{job_id}	cfw:instance:listInstance	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-138 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

CFW 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-138 CFW 支持的资源类型

资源类型	URN
blackWhiteList	cfw:<region>:<account-id>:blackWhiteList:<blackWhiteList-id>
acl	cfw:<region>:<account-id>:acl:<acl-id>
instance	cfw:<region>:<account-id>:instance:<fwInstance-id>
serviceGroup	cfw:<region>:<account-id>:serviceGroup:<serviceGroup-id>
domainGroup	cfw:<region>:<account-id>:domainGroup:<domainGroup-id>
ipGroup	cfw:<region>:<account-id>:ipGroup:<ipGroup-id>
eip	cfw:<region>:<account-id>:eip:<eip-id>

条件（Condition）

条件键概述

 版权所有 © 华为云计算技术有限公司

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 cfw:）仅适用于对应服务的操作，详情请参见表 3-139。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

CFW 支持的服务级条件键

CFW 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-139 CFW 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
cfw:LogGroupId	string	单值	根据请求参数中指定的 LTS 日志组 ID 过滤访问。

3.7.4 云堡垒机 CBH

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

 版权所有 © 华为云计算技术有限公司

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 CBH 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 CBH 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 CBH 的相关操作。

表3-140 CBH 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cbh::listAvailableZones	授予查询服务可用区的权限。	List	-	-	-
cbh::getEcsQuota	授予查询 ECS 资源配额的权限。	Read	-	-	-
cbh::getQuota	授予查询堡垒机实例配额的权限。	Read	-	-	-
cbh::listSpecifications	授予查询堡垒机规格的权	List	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
cbh:instance:listInstances	授予查询堡垒机列表的权限。	List	instance *	-	-
cbh:instance:getInstanceStatus	授予查询堡垒机状态的权限。	Read	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:startInstance	授予启动堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:stopInstance	授予关闭堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:rebootInstance	授予重启堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:upgradeInstance	授予升级堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:loginInstance	授予以 IAM 用户登录堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:resetInstancePassword	授予重置堡垒机密码的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:resetInstanceLoginMethod	授予重置堡垒机登录方式的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:deleteInstance	授予删除故障堡垒机的权	Write	instance *	• g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。			• g:ResourceTag/tag-key	
cbh:instance:alterInstance	授予变更堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:createInstance	授予创建堡垒机的权限。	Write	instance *	-	-
			-	• g:EnterpriseProjectId • g:RequestTag/tag-key • g:TagKeys • cbh:VpcId • cbh:SubnetId • cbh:AllowBindPublicIp	
cbh:instance:bindInstanceEip	授予为堡垒机绑定 EIP 的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:unbindInstanceEip	授予为堡垒机解绑 EIP 的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:updateInstanceSecurityGroup	授予更新堡垒机安全组的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh::operateAuthorization	授予创建或取消堡垒机服务委托授权的权限。	Write	-	-	-
cbh::getAuthorization	授予获取租户给堡垒机服务委托授权信息的权限。	Read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cbh::listTags	授予查询全部标签的权限。	List	-	-	-
cbh:instance:getInstanceTags	授予查询堡垒机实例资源的标签信息的权限。	Read	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:countInstancesByTag	授予统计符合标签条件的实例数量的权限。	List	instance *	-	-
cbh:instance:listInstancesByTag	授予使用标签过滤实例的权限。	List	-	-	-
cbh:instance:operateInstanceTags	授予操作堡垒机实例资源标签的权限。	Tagging	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
			-	• g:RequestTag/tag-key • g:TagKeys	
cbh:instance:getOmUrl	授予获取堡垒机内资产运维链接的权限。	Read	instance *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	cbh:instance:getOmUrl
cbh:instance:rollbackInstance	授予回滚堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	cbh:instance:upgrade

CBH 的 API 通常对应着一个或多个授权项。表 3-141 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-141 API 与授权项的关系

API	对应的授权项	依赖的授权项

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/cbs/available-zone	cbh::listAvailableZones	-
GET /v2/{project_id}/cbs/instance/specification	cbh::listSpecifications	-
GET /v2/{project_id}/cbs/instance/list	cbh:instance:listInstances	eps:enterpriseProjects:list
POST /v2/{project_id}/cbs/instance/start	cbh:instance:startInstance	-
POST /v2/{project_id}/cbs/instance/stop	cbh:instance:stopInstance	-
POST /v2/{project_id}/cbs/instance/upgrade	cbh:instance:upgradeInstance	-
POST /v2/{project_id}/cbs/instance/login	cbh:instance:loginInstance	-
PUT /v2/{project_id}/cbs/instance/password	cbh:instance:resetInstancePassword	-
PUT /v2/{project_id}/cbs/instance/login-method	cbh:instance:resetInstanceLoginMethod	-
DELETE /v2/{project_id}/cbs/instance	cbh:instance:deleteInstance	-
POST /v2/{project_id}/cbs/instance	cbh:instance:createInstance	• vpc:quotas:list • vpc:subnets:list • vpc:subnets:get • vpc:securityGroups:list • ecs:cloudServerFlavors:get
PUT /v2/{project_id}/cbs/instance/{server_id}/security-groups	cbh:instance:updateInstanceSecurityGroup	vpc:ports:update
GET /v2/{project_id}/cbs/agency/authorization	cbh::getAuthorization	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/cbs/instance/tags	cbh::listTags	-
GET /v2/{project_id}/cbs/instance/{resource_id}/tags	cbh:instance:getInstanceTags	-
POST /v2/{project_id}/cbs/instance/count	cbh:instance:countInstancesByTag	-
POST /v2/{project_id}/cbs/instance/filter	cbh:instance:listInstancesByTag	-
POST /v2/{project_id}/cbs/instance/{server_id}/eip/bind	cbh:instance:bindInstanceEip	• eip:publicIps:list • eip:publicIps:update
POST /v2/{project_id}/cbs/instance/{server_id}/eip/unbind	cbh:instance:unbindInstanceEip	• eip:publicIps:update • eip:publicIps:list
GET /v2/{project_id}/cbs/instance/ecs-quota	cbh::getEcsQuota	ecs:cloudServerFlavors:get
GET /v2/{project_id}/cbs/instance/quota	cbh::getQuota	-
GET /v2/{project_id}/cbs/instance/{server_id}/status	cbh:instance:getInstanceStatus	-
POST /v2/{project_id}/cbs/instance/reboot	cbh:instance:rebootInstance	-
PUT /v2/{project_id}/cbs/instance	cbh:instance:alterInstance	-
POST /v2/{project_id}/cbs/agency/authorization	cbh::operateAuthorization	-
POST /v2/{project_id}/cbs/instance/{resource_id}/tags/action	cbh:instance:operateInstanceTags	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/cbs/instance/get-om-url	cbh:instance:getOmUrl	-
POST /v2/{project_id}/cbs/instance/rollback	cbh:instance:rollbackInstance	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-142 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

CBH 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-142 CBH 支持的资源类型

资源类型	URN
instance	cbh:<region>:<account-id>:instance:<instance-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 cbh:）仅适用于对应服务的操作，详情请参见表 3-143。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

CBH 支持的服务级条件键

 版权所有 © 华为云计算技术有限公司

CBH 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-143 CBH 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
cbh:VpcId	string	单值	根据堡垒机实例通信的VPCID 开启过滤访问。
cbh:SubnetId	string	单值	根据堡垒机实例通信的子网 ID 开启过滤访问。
cbh:AllowBindPublicIp	boolean	单值	根据堡垒机实例是否可以绑定公网 IP 开启权限。

3.7.5 云证书管理服务 CCM

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “**访问级别**”列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “**资源类型**”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。

 版权所有 © 华为云计算技术有限公司

  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 PCA 定义的资源类型的详细信息请参见资源类型（Resource）。
- “**条件键**”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 PCA 定义的条件键的详细信息请参见条件（Condition）。
- “**别名**”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 PCA 的相关操作。

表3-144 PCA 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
pca:ca:create	授予权限创建私有 CA。	write	ca *	-	-
			-	g:EnterpriseProjectId	
pca:ca:delete	授予权限删除私有 CA。	write	ca *	g:ResourceTag/<tag-key>	-
			-	g:EnterpriseProjectId	
pca:ca:disable	授予权限禁用私有 CA。	write	ca *	g:ResourceTag/<tag-key>	-
			-	g:EnterpriseProjectId	
pca:ca:enable	授予权限启用私有 CA。	write	ca *	g:ResourceTag/<tag-key>	-
			-	g:EnterpriseProjectId	
pca:ca:export	授予权限导出私有 CA 证书。	read	ca *	g:ResourceTag/<tag-key>	-
			-	g:EnterpriseProjectId	
pca:ca:getCsr	授予权限导出私有 CA 的证	read	ca *	g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	书签名请求（CSR）。		-	g:EnterpriseProjectId	
pca:ca:import	授予权限导入证书作为私有CA 证书。	write	ca *	-	-
			-	g:EnterpriseProjectId	
pca:ca:activate	授予权限激活私有 CA。	write	ca *	g:ResourceTag/<tag-key>	pca:ca:active
			-	g:EnterpriseProjectId	
pca:ca:list	授予权限查询私有 CA 列表。	list	ca *	-	-
			-	g:EnterpriseProjectId	
pca:ca:restore	授予权限恢复私有 CA。	write	ca *	g:ResourceTag/<tag-key>	-
			-	g:EnterpriseProjectId	
pca:ca:revoke	授予权限吊销私有 CA。	write	ca *	g:ResourceTag/<tag-key>	-
			-	g:EnterpriseProjectId	
pca:ca:get	授予权限查询私有 CA 详情。	read	ca *	g:ResourceTag/<tag-key>	-
			-	g:EnterpriseProjectId	
pca:ca:quota	授予权限查询私有 CA 配额。	read	-	-	-
pca:ca:createTag	授予权限创建或更新私有 CA 标签。	tagging	ca *	g:ResourceTag/<tag-key>	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
pca:ca:deleteTa	授予权限删除	taggin	ca *	g:ResourceTag/	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
g	私有 CA 标签。	g		<tag-key>	
			-	• g:EnterpriseProjectId • g:TagKeys	
pca:ca:listTags	授予权限查询私有 CA 的标签列表。	list	ca *	g:ResourceTag/<tag-key>	-
			-	g:EnterpriseProjectId	
pca:ca:listAllTags	授予权限查询用户的私有 CA 标签列表。	list	ca *	-	-
pca:ca:listByTag	授予权限根据标签查询私有 CA 列表。	list	ca *	-	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
pca:ca:issueCert	授予权限签发私有证书。	write	ca *	-	-
			-	• g:EnterpriseProjectId • pca:CommonName	
pca:ca:issueCertByCsr	授予权限根据证书签名请求（CSR）签发私有证书。	write	ca *	-	pca:ca:issueCertThroughCSR
			-	• g:EnterpriseProjectId • pca:CommonName	
pca:cert:delete	授予权限删除私有证书。	write	-	g:EnterpriseProjectId	-
pca:cert:export	授予权限导出私有证书。	read	-	g:EnterpriseProjectId	-
pca:cert:list	授予权限查询私有证书列表。	list	-	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
pca:ca:revokeCert	授予权限吊销私有证书。	write	ca *	g:ResourceTag/<tag-key>	pca:cert:revoke
			-	g:EnterpriseProjectId	
pca:cert:get	授予权限查询私有证书详情。	read	-	g:EnterpriseProjectId	-
pca:cert:quota	授予权限查询私有证书配额。	read	-	-	-
pca:cert:createTag	授予权限创建或更新私有证书标签。	tagging	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	-
pca:cert:deleteTag	授予权限删除私有证书标签。	tagging	-	• g:EnterpriseProjectId • g:TagKeys	-
pca:cert:listTags	授予权限查询私有证书的标签列表。	list	-	g:EnterpriseProjectId	-
pca:cert:listAllTags	授予权限查询用户的私有证书标签列表。	list	-	-	-
pca:cert:listByTag	授予权限根据标签查询私有证书列表。	list	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	-
pca:ca:disableCrl	授予权限禁用CRL。	write	ca *	g:ResourceTag/<tag-key>	-
			-	g:EnterpriseProjectId	
pca:ca:enableCrl	授予权限启用CRL。	write	ca *	g:ResourceTag/<tag-key>	-
			-	g:EnterprisePro	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				jectId	

PCA 的 API 通常对应着一个或多个授权项。表 PCA API 与授权项的关系展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-145 PCA API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/private-certificate-authorities	pca:ca:create	-
POST /v1/private-certificate-authorities/order	pca:ca:create	-
DELETE /v1/private-certificate-authorities/{ca_id}	pca:ca:delete	-
POST /v1/private-certificate-authorities/{ca_id}/disable	pca:ca:disable	-
POST /v1/private-certificate-authorities/{ca_id}/enable	pca:ca:enable	-
POST /v1/private-certificate-authorities/{ca_id}/export	pca:ca:export	-
GET /v1/private-certificate-authorities/{ca_id}/csr	pca:ca:getCsr	-
POST /v1/private-certificate-authorities/{ca_id}/import	pca:ca:import	-
POST /v1/private-certificate-authorities/{ca_id}/activate	pca:ca:activate	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/private-certificate-authorities	pca:ca:list	-
POST /v1/private-certificate-authorities/{ca_id}/restore	pca:ca:restore	-
POST /v1/private-certificate-authorities/{ca_id}/revoke	pca:ca:revoke	-
GET /v1/private-certificate-authorities/{ca_id}	pca:ca:get	-
GET /v1/private-certificate-authorities/quotas	pca:ca:quota	-
POST /v1/private-certificate-authorities/{ca_id}/tags/create	pca:ca:createTag	-
DELETE /v1/private-certificate-authorities/{ca_id}/tags/delete	pca:ca:deleteTag	-
POST /v1/private-certificate-authorities/{ca_id}/tags	pca:ca:createTag	-
GET /v1/private-certificate-authorities/{ca_id}/tags	pca:ca:listTags	-
GET /v1/private-certificate-authorities/tags	pca:ca:listAllTags	-
POST /v1/private-certificate-authorities/resource-instances/filter	pca:ca:listByTag	-
POST /v1/private-certificates	pca:ca:issueCert	-
POST /v1/private-certificates/csr	pca:ca:issueCertByCsr	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /v1/private-certificates/{certificate_id}	pca:cert:delete	-
POST /v1/private-certificates/{certificate_id}/export	pca:cert:export	-
GET /v1/private-certificates	pca:cert:list	-
POST /v1/private-certificates/{certificate_id}/revoke	pca:ca:revokeCert	-
GET /v1/private-certificates/{certificate_id}	pca:cert:get	-
GET /v1/private-certificates/quotas	pca:cert:quota	-
POST /v1/private-certificates/{certificate_id}/tags/create	pca:cert:createTag	-
DELETE /v1/private-certificates/{certificate_id}/tags/delete	pca:cert:deleteTag	-
POST /v1/private-certificates/{certificate_id}/tags	pca:cert:createTag	-
GET /v1/private-certificates/{certificate_id}/tags	pca:cert:listTags	-
GET /v1/private-certificates/tags	pca:cert:listAllTags	-
POST /v1/private-certificates/resource-instances/filter	pca:cert:listByTag	-
POST /v1/private-certificate-authorities/{ca_id}/crl/disable	pca:ca:disableCrl	-
POST /v1/private-certificate-authorities/{ca_id}/crl/enable	pca:ca:enableCrl	-

 版权所有 © 华为云计算技术有限公司

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 PCA 支持的资源类型中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的 URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

PCA 定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-146 PCA 支持的资源类型

资源类型	URN
ca	pca:<region>:<account-id>:ca:<ca-id>

条件（Condition）

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 pca:）仅适用于对应服务的操作，详情请参见表 PCA 支持的服务级条件键。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

PCA 定义了以下可以在身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-147 PCA 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
pca:CommonName	string	单值	根据请求参数中的证书通用名称过滤访问。

 版权所有 © 华为云计算技术有限公司

3.7.6 数据库安全服务 DBSS

云服务在 IAM 预置了常用的权限，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 DBSS 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 DBSS 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 DBSS 的相关操作。

 版权所有 © 华为云计算技术有限公司

表3-148 DBSS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dbss:auditInstance:listSqlInjectRules	授予权限以查询 SQL 注入规则。	List	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:listSqls	授予权限以获取审计结果信息。	List	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:switchSqlInjectRule	授予权限以开启或关闭 sql 注入策略。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:addSqlInjectRule	授予权限以添加自定义 sql 注入规则。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:orderSqlInjectRule	授予权限以对 sql 规则优先级进行排序。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:createReporter	授予权限以立即生成报表。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:listReporters	授予权限以查询报表信息。	List	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:getRiskRuleDetail	授予权限以查询指定风险规则策略。	Read	auditInstance *	• g:ResourceTag/<tag-key> • g:Enterprise	dbss:auditInstance:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ProjectId	
dbss:auditInstance:listAlarmEmails	授予权限以查询告警邮件信息。	List	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:downloadReporter	授予权限以下载报表。	Read	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:listAuditScopeRules	授予权限以查询审计范围策略列表。	List	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:addSensitiveRule	授予权限以添加隐私数据保护规则。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:editSensitiveRule	授予权限以编辑隐私数据保护规则。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:deleteReporter	授予权限以删除报表。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:listOperateLog	授予权限以查询用户操作日志信息。	List	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:listMonitorInfos	授予权限以查询审计实例监控信息。	List	auditInstance *	• g:ResourceTag/<tag-key> • g:Enterprise	dbss:auditInstance:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ProjectId	
dbss:auditInstance:listSessionInfo	授予权限以查询审计实例会话信息。	List	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:switchBackup	授予权限以开启或关闭备份功能。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss::downloadLicense	授予权限以下载销售许可证。	Read	-	-	dbss:auditInstance:list
dbss::deleteAuditInstanceJob	授予权限以删除审计实例创建失败的任务。	Write	-	-	dbss:auditInstance:delete
dbss::listRdsDb	授予权限以查询 RDS 数据库。	List	-	-	dbss:auditInstance:list
dbss:auditInstance:instanceStart	授予权限以开启审计实例。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:start
dbss:auditInstance:reboot	授予权限以重启审计实例。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dbss:auditInstance:stop	授予权限以关闭审计实例。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dbss:auditInstance:upgrade	授予权限以升级审计实例。	Write	auditInstance *	• g:ResourceTag/<tag-key>	dbss:auditInstance:createOnOrder

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:EnterpriseProjectId	
dbss::queryUpgradeStatus	授予权限以查询审计实例升级状态。	List	-	-	dbss:auditInstance:createOnOrder
dbss:auditInstance:updateSecurityGroup	授予权限以修改审计实例安全组。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:modifyAttribute	授予权限以修改审计实例审计属性。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:downloadAgent	授予权限以下载 agent。	Read	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:switchAgent	授予权限以开启或关闭 Agent。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:listAgents	授予权限以获取 agent 列表。	List	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:deleteAgent	授予权限以删除 agent。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:addAgent	授予权限以添加 agent。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dbss:auditInstance:previewReporter	授予权限以预览报表。	Read	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:setAlarmConfig	授予权限以配置告警信息。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:configAlarmEmail	授予权限以配置告警邮件信息。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:getAlarmConfig	授予权限以查询告警配置信息。	Read	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:listRiskRules	授予权限以查询风险规则策略。	List	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:exportInstancesDatabaseConfig	授予权限以导出数据库配置。	List	auditInstance *	-	dbss:auditInstance:createOnOrder
dbss:auditInstance:createOnPeriod	授予权限以包年包月计费模式创建审计实例。	Write	auditInstance *	-	dbss:auditInstance:createOnOrder
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • dbss:VpcId • dbss:SubnetId	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dbss:auditInstance:editSqlInjectRule	授予权限以编辑自定义 sql 注入规则。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:deleteSqlInjectRule	授予权限以删除自定义 sql 注入规则。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:deleteSensitiveRule	授予权限以删除隐私数据保护规则。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:deleteAuditScopeRule	授予权限以删除审计范围规则。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:deleteRiskRule	授予权限以删除风险规则。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:deleteBackup	授予权限以删除本地备份信息。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:listBackups	授予权限以查询备份信息。	List	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:getBackupConfig	授予权限以获取备份配置信息。	Read	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dbss:auditInstance:editAuditScopeRule	授予权限以编辑审计范围规则。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:instanceList	授予权限以查询审计实例信息。	List	auditInstance *	-	dbss:auditInstance:list
dbss:auditInstance:createOnDemand	授予权限以按需模式创建审计实例。	Write	auditInstance *	-	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • dbss:VpcId • dbss:SubnetId	
dbss::listCommonInfo	授予权限以查询公共信息。	List	-	-	dbss:auditInstance:list
dbss:auditInstance:listInstancesSummaryInfo	授予权限以查询所有审计实例总览信息。	List	auditInstance *	-	dbss:auditInstance:list
dbss::getauditInstancesSummaryTaskStatus	授予权限以查询总览任务状态。	Read	-	-	dbss:auditInstance:list
dbss::updateAuditInstancesSummaryInfo	授予权限以更新所有审计实例总览信息。	Write	-	-	dbss:auditInstance:start
dbss:auditInstance:setReporterConfig	授予权限以更改报表的计划任务配置信息。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:getReporterConfig	授予权限以获取报表的计划任务配置信	Read	auditInstance *	• g:ResourceTag/<tag-key>	dbss:auditInstance:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	息。			• g:EnterpriseProjectId	
dbss:auditInstance:addBareDatabase	授予权限以添加自建数据库。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:listDatabases	授予权限以查询数据库列表。	List	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:switchDatabase	授予权限以开启关闭数据库审计功能。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:deleteDatabase	授予权限以删除数据库。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:addAuditScopeRule	授予权限以添加审计范围规则。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:switchAuditScopeRule	授予权限以开启关闭审计范围规则。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:addRiskRule	授予权限以添加风险规则。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:switchRiskRule	授予权限以开启或关闭风险规则。	Write	auditInstance *	• g:ResourceTag/<tag-key>	dbss:auditInstance:createOnOrder

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:EnterpriseProjectId	
dbss:auditInstance:editRiskRule	授予权限以编辑风险规则。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:setRiskRulePriority	授予权限以设置风险规则优先级。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:listStatistics	授予权限以查询审计实例概览信息。	List	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:listSensitiveRules	授予权限以查询隐私数据脱敏规则。	List	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:modifySensitiveRuleSaveResultSwitch	授予权限以开启关闭存储结果集开关。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:modifySensitiveRuleAnonymizeSwitch	授予权限以开启关闭隐私数据脱敏开关。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:switchSensitiveRule	授予权限以开启或关闭隐私数据保护规则。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:listAlarmItems	授予权限以查询告警信息。	List	auditInstance *	• g:ResourceTag/<tag-key>	dbss:auditInstance:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:EnterpriseProjectId	
dbss:auditInstance:markAlarm	授予权限以标记告警信息。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:deleteAlarm	授予权限以删除告警信息。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:restoreBackup	授予权限以恢复备份信息。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:retryBackup	授予权限以重试备份操作。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:getRiskBackupConfigInfo	授予权限以获取风险导出配置信息。	Read	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:switchRiskBackup	授予权限以开启关闭风险导出功能。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss:auditInstance:getRiskBackupBucketInfo	授予权限以获取风险导出obs 桶信息。	Read	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:list
dbss:auditInstance:setRiskBackupBucketInfo	授予权限以设置风险导出obs 桶信息。	Write	auditInstance *	• g:ResourceTag/<tag-key>	dbss:auditInstance:createOnOrder

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:EnterpriseProjectId	
dbss:auditInstance:addRdsDatabase	授予权限以添加 RDS 数据库。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:createOnOrder
dbss::getServerInfo	授予权限以获取 DBSS 服务信息。	Read	-	-	dbss:auditInstance:list
dbss::getAuditInstanceJob	授予权限以查看审计实例任务创建信息。	Read	-	-	dbss:auditInstance:list
dbss:auditInstance:listJobs	授予权限以列举审计实例任务创建信息。	List	auditInstance *	-	dbss:auditInstance:list
dbss::listObsBuckets	授予权限以查询 obs 桶列表。	List	-	-	dbss:auditInstance:list
dbss:auditInstance:instanceDelete	授予权限以删除审计实例。	Write	auditInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dbss:auditInstance:delete
dbss::listResourcesByTag	授予权限以根据标签信息查询审计实例。	List	-	• g:RequestTag/<tag-key> • g:TagKeys	dbss:auditInstance:list
dbss::tagResource	授予权限以批量添加实例标签。	Tagging	-	• g:RequestTag/<tag-key> • g:TagKeys	dbss:auditInstance:createOnOrder
dbss::unTagResource	授予权限以批量删除实例标签。	Tagging	-	• g:RequestTag/<tag-key> • g:TagKeys	dbss:auditInstance:delete
dbss::listTags	授予权限以查询项目下的所有标签。	List	-	-	dbss:auditInstance:list
dbss::listTagsF	授予权限以查	List	-	-	dbss:auditInstan

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
orResource	询实例标签信息。				ce:list

DBSS 的 API 通常对应着一个或多个授权项。表 3-149 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-149 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql-rules	dbss:auditInstance:listSqlInjectRules	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql/list-rules	dbss:auditInstance:listSqlInjectRules	-
POST /dbss/v1/{project_id}/{instance_id}/dbss/audit/rule/sql-injections	dbss:auditInstance:listSqlInjectRules	-
POST /dbss/v1/{project_id}/{instance_id}/audit/sqls	dbss:auditInstance:listSqls	-
POST /dbss/v1/{project_id}/{instance_id}/audit/sqls/list-sqls	dbss:auditInstance:listSqls	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql-rule/switch	dbss:auditInstance:switchSqlInjectRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql/switch	dbss:auditInstance:switchSqlInjectRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rul	dbss:auditInstance:addSqlInjectRule	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
e/sql-rule		
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql	dbss:auditInstance:addSqlInjectRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql-rules/rank	dbss:auditInstance:orderSqlInjectRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql/rank-sql	dbss:auditInstance:orderSqlInjectRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/reports	dbss:auditInstance:createReporter	-
POST /dbss/v1/{project_id}/{instance_id}/audit/reports/results/create-report	dbss:auditInstance:createReporter	-
POST /dbss/v1/{project_id}/{instance_id}/audit/reports/list	dbss:auditInstance:listReporters	-
POST /dbss/v1/{project_id}/{instance_id}/audit/reports/list-reports	dbss:auditInstance:listReporters	-
GET /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/{risk_id}	dbss:auditInstance:getRiskRuleDetail	-
GET /dbss/v1/{project_id}/{instance_id}/dbss/audit/rule/risk/{risk_id}	dbss:auditInstance:getRiskRuleDetail	-
GET /dbss/v1/{project_id}/{instance_id}/audit/operation/emails	dbss:auditInstance:listAlarmEmails	-
GET /dbss/v1/{project_id}/{instance_id}/audit/op	dbss:auditInstance:listAlarmEmails	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
eration/list-emails		
GET /dbss/v1/{project_id}/{instance_id}/audit/reports/{report_id}	dbss:auditInstance:downloadReporter	-
GET /dbss/v1/{project_id}/{instance_id}/audit/reports/results/{report_id}/download-report	dbss:auditInstance:downloadReporter	-
GET /dbss/v1/{project_id}/{instance_id}/audit/rule/scopes	dbss:auditInstance:listAuditScopeRules	-
GET /dbss/v1/{project_id}/{instance_id}/audit/rule/scope/list-scope	dbss:auditInstance:listAuditScopeRules	-
GET /dbss/v1/{project_id}/{instance_id}/dbss/audit/rule/scopes	dbss:auditInstance:listAuditScopeRules	-
GET /dbss/v1/{project_id}/{instance_id}/audit/sensitive/masks	dbss:auditInstance:listSensitiveRules	-
GET /dbss/v1/{project_id}/{instance_id}/audit/sensitive/mask/list-rules	dbss:auditInstance:listSensitiveRules	-
GET /dbss/v1/{project_id}/{instance_id}/dbss/audit/sensitive/masks	dbss:auditInstance:listSensitiveRules	-
POST /dbss/v1/{project_id}/{instance_id}/audit/sensitive/masks	dbss:auditInstance:addSensitiveRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/sensitive/mask/add-rule	dbss:auditInstance:addSensitiveRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/se	dbss:auditInstance:editSensitiveRule	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
nsitive/masks/{rule_id}		
POST /dbss/v1/{project_id}/{instance_id}/audit/sensitive/mask/{rule_id}/edit-rule	dbss:auditInstance:editSensitiveRule	-
GET /dbss/v1/{project_id}/{instance_id}/audit/reports/templates	dbss:auditInstance:listReporters	-
GET /dbss/v1/{project_id}/{instance_id}/audit/reports/list-templates	dbss:auditInstance:listReporters	-
GET /dbss/v1/{project_id}/{instance_id}/audit/rule/risk	dbss:auditInstance:listRiskRules	-
GET /dbss/v1/{project_id}/{instance_id}/dbss/audit/rule/risk	dbss:auditInstance:listRiskRules	-
DELETE /dbss/v1/{project_id}/{instance_id}/audit/reports/{report_id}	dbss:auditInstance:deleteReporter	-
DELETE /dbss/v1/{project_id}/{instance_id}/audit/reports/results/{report_id}/delete-report	dbss:auditInstance:deleteReporter	-
POST /dbss/v1/{project_id}/{instance_id}/audit/general/operate-log	dbss:auditInstance:listOperateLog	-
POST /dbss/v1/{project_id}/{instance_id}/dbss/audit/operate-log	dbss:auditInstance:listOperateLog	-
POST /dbss/v1/{project_id}/{instance_id}/audit/operation/monitorinfo	dbss:auditInstance:listMonitorInfos	-
POST	dbss:auditInstance:listMonitorI	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/dbss/v1/{project_id}/{instance_id}/audit/operation/get-monitorinfo	nfos	
POST /dbss/v1/{project_id}/{instance_id}/audit/sessionstatistics/clientsession	dbss:auditInstance:listSessionInfo	-
POST /dbss/v1/{project_id}/{instance_id}/audit/sessionstatistics/list-clientsession	dbss:auditInstance:listSessionInfo	-
POST /dbss/v1/{project_id}/{instance_id}/audit/sessionstatistics/accountsession	dbss:auditInstance:listSessionInfo	-
POST /dbss/v1/{project_id}/{instance_id}/audit/sessionstatistics/list-accountsession	dbss:auditInstance:listSessionInfo	-
POST /dbss/v1/{project_id}/{instance_id}/audit/backup/stop	dbss:auditInstance:switchBackup	dbss:auditInstance:getBackupConfig
POST /dbss/v1/{project_id}/{instance_id}/audit/backup/stop-backup	dbss:auditInstance:switchBackup	dbss:auditInstance:getBackupConfig
POST /dbss/v1/{project_id}/{instance_id}/audit/backup/start	dbss:auditInstance:switchBackup	dbss:auditInstance:getBackupConfig
POST /dbss/v1/{project_id}/{instance_id}/audit/backup/start-backup	dbss:auditInstance:switchBackup	dbss:auditInstance:getBackupConfig
GET /dbss/v1/{project_id}/dbss/saleslicense/download	dbss::downloadLicense	-
GET /dbss/v1/{project_id}/	dbss::downloadLicense	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
dbss/download-saleslicense		
DELETE /dbss/v1/{project_id}/dbss/audit/job/{failed_id}	dbss::deleteAuditInstanceJob	-
DELETE /dbss/v1/{project_id}/dbss/audit/delete-job/{failed_id}	dbss::deleteAuditInstanceJob	-
GET /dbss/v2/{project_id}/audit/databases/rds	dbss::listRdsDb	-
POST /dbss/v1/{project_id}/dbss/audit/rds-instance	dbss::listRdsDb	-
POST /dbss/v1/{project_id}/dbss/audit/guassDbInstance	dbss::listRdsDb	-
POST /dbss/v1/{project_id}/dbss/audit/instance/start	dbss:auditInstance:instanceStart	-
POST /dbss/v1/{project_id}/dbss/audit/start-instance	dbss:auditInstance:instanceStart	-
POST /dbss/v1/{project_id}/dbss/audit/instance/reboot	dbss:auditInstance:reboot	-
POST /dbss/v1/{project_id}/dbss/audit/reboot-instance	dbss:auditInstance:reboot	-
POST /dbss/v1/{project_id}/dbss/audit/instance/stop	dbss:auditInstance:stop	-
POST /dbss/v1/{project_id}/dbss/audit/stop-instance	dbss:auditInstance:stop	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /dbss/v1/{project_id}/dbss/{instance_id}/audit/upgrade	dbss:auditInstance:upgrade	-
GET /dbss/v1/{project_id}/dbss/audit/upgrade/status	dbss::queryUpgradeStatus	-
POST /dbss/v1/{project_id}/dbss/audit/securitygroup	dbss:auditInstance:updateSecurityGroup	-
POST /dbss/v1/{project_id}/dbss/audit/update-securitygroup	dbss:auditInstance:updateSecurityGroup	-
PUT /dbss/v1/{project_id}/dbss/audit/instances/{instance_id}	dbss:auditInstance:modifyAttribute	-
POST /dbss/v1/{project_id}/dbss/audit/update-instance/{instance_id}	dbss:auditInstance:modifyAttribute	-
GET /dbss/v1/{project_id}/{instance_id}/audit/operation/agent/{agent_id}/download	dbss:auditInstance:downloadAgent	-
GET /dbss/v1/{project_id}/{instance_id}/audit/operation/download-agent/{agent_id}	dbss:auditInstance:downloadAgent	-
GET /dbss/v2/{project_id}/{instance_id}/audit/agents/{agent_id}	dbss:auditInstance:downloadAgent	-
POST /dbss/v1/{project_id}/{instance_id}/audit/agent/switch	dbss:auditInstance:switchAgent	-
GET /dbss/v2/{project_id}/{instance_id}/audit/ag	dbss:auditInstance:listAgents	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ents		
GET /dbss/v1/{project_id}/{instance_id}/audit/agents/{db_id}	dbss:auditInstance:listAgents	-
DELETE /dbss/v1/{project_id}/{instance_id}/audit/agents/{db_id}/{agent_id}	dbss:auditInstance:deleteAgent	-
DELETE /dbss/v2/{project_id}/{instance_id}/audit/agents/{agent_id}	dbss:auditInstance:deleteAgent	-
POST /dbss/v2/{project_id}/{instance_id}/audit/agents	dbss:auditInstance:addAgent	-
POST /dbss/v1/{project_id}/{instance_id}/audit/agents	dbss:auditInstance:addAgent	-
POST /dbss/v1/{project_id}/{instance_id}/audit/agent/add-agent	dbss:auditInstance:addAgent	-
POST /dbss/v1/{project_id}/{instance_id}/audit/agent/{agent_id}	dbss:auditInstance:addAgent	-
GET /dbss/v1/{project_id}/{instance_id}/audit/reports/{report_id}/preview	dbss:auditInstance:previewReporter	-
GET /dbss/v1/{project_id}/{instance_id}/audit/reports/{report_id}/preview-report	dbss:auditInstance:previewReporter	-
POST /dbss/v1/{project_id}/{instance_id}/audit/general/alarm-config	dbss:auditInstance:setAlarmConfig	-
POST	dbss:auditInstance:configAlar	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/dbss/v1/{project_id}/{instance_id}/audit/operation/config-email	mEmail	
GET /dbss/v1/{project_id}/{instance_id}/audit/general/alarm-config	dbss:auditInstance:getAlarmConfig	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/search-rules	dbss:auditInstance:listRiskRules	-
POST /dbss/v1/{project_id}/obs/upload-config	dbss:auditInstance:exportInstancesDatabaseConfig	-
POST /dbss/v1/charge/{project_id}/audit/period/order	dbss:auditInstance:createOnPeriod	dbss::listCommonInfo
GET /dbss/v1/{project_id}/{instance_id}/audit/agent/get-agent	dbss:auditInstance:listAgents	-
POST /dbss/v1/{project_id}/{instance_id}/audit/agent/del-agent	dbss:auditInstance:deleteAgent	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql/{sql_id}	dbss:auditInstance:editSqlInjectRule	-
DELETE /dbss/v1/{project_id}/{instance_id}/audit/rule/sql/{sql_id}	dbss:auditInstance:deleteSqlInjectRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/sensitive/mask/delete-rules	dbss:auditInstance:deleteSensitiveRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/list-rules	dbss:auditInstance:listRiskRules	-
POST /dbss/v1/{project_id}/	dbss:auditInstance:deleteAuditScopeRule	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
{instance_id}/audit/rule/scope/delete-scope		
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/delete-risk	dbss:auditInstance:deleteRiskRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/backup/del-backup	dbss:auditInstance:deleteBackup	-
POST /dbss/v1/{project_id}/{instance_id}/audit/backup/status	dbss:auditInstance:listBackups	-
POST /dbss/v1/{project_id}/{instance_id}/audit/backup/auto-backup-template	dbss:auditInstance:getBackupConfig	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/scope/edit-rule/{scope-id}	dbss:auditInstance:editAuditScopeRule	-
GET /dbss/v1/{project_id}/dbss/audit/list-instances	dbss:auditInstance:instanceList	-
POST /dbss/v1/{project_id}/dbss/audit/create-instance	dbss:auditInstance:createOnDemand	dbss::listCommonInfo
POST /dbss/v2/{project_id}/dbss/audit/charge/period/order	dbss:auditInstance:createOnPeriod	dbss::listCommonInfo
GET /dbss/v2/{project_id}/dbss/audit/availability-zone	dbss::listCommonInfo	-
GET /dbss/v2/{project_id}/audit/summary/{busi_type}/taskstatus	dbss::getauditInstancesSummaryTaskStatus	-
GET	dbss:auditInstance:listInstances	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/dbss/v1/{project_id}/audit/summary/info	SummaryInfo	
GET /dbss/v1/{project_id}/audit/summary/{busi_type}/taskstatus	dbss::getauditInstancesSummaryTaskStatus	-
GET /dbss/v1/{project_id}/audit/risk/statistics	dbss:auditInstance:listInstancesSummaryInfo	-
POST /dbss/v1/{project_id}/audit/summary/{busi_type}/taskstatus	dbss::updateAuditInstancesSummaryInfo	-
POST /dbss/v1/{project_id}/{instance_id}/audit/reports/templates-topic/scheduler/config-task	dbss:auditInstance:setReporterConfig	-
GET /dbss/v1/{project_id}/{instance_id}/audit/reports/templates-topic/scheduler/{template_id}	dbss:auditInstance:getReporterConfig	-
POST /dbss/v1/{project_id}/{instance_id}/audit/general/alarm-config-topic	dbss:auditInstance:setAlarmConfig	-
GET /dbss/v1/{project_id}/{instance_id}/audit/general/alarm-config-topic	dbss:auditInstance:getAlarmConfig	-
POST /dbss/v1/{project_id}/{instance_id}/audit/databases	dbss:auditInstance:addBareDatabase	-
POST /dbss/v1/{project_id}/{instance_id}/audit/operation/databases	dbss:auditInstance:addBareDatabase	-
POST /dbss/v1/{project_id}/{instance_id}/audit/op	dbss:auditInstance:addBareDatabase	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
eration/create-database		
GET /dbss/v1/{project_id}/{instance_id}/dbss/audit/databases	dbss:auditInstance:listDatabases	-
GET /dbss/v1/{project_id}/{instance_id}/audit/operation/databases	dbss:auditInstance:listDatabases	-
GET /dbss/v1/{project_id}/{instance_id}/audit/operation/list-databases	dbss:auditInstance:listDatabases	-
POST /dbss/v1/{project_id}/{instance_id}/audit/operation/switch	dbss:auditInstance:switchDatabase	-
POST /dbss/v2/{project_id}/{instance_id}/audit/databases/switch	dbss:auditInstance:switchDatabase	-
DELETE /dbss/v2/{project_id}/{instance_id}/audit/databases/{db_id}	dbss:auditInstance:deleteDatabase	-
POST /dbss/v1/{project_id}/{instance_id}/audit/operation/database/delete	dbss:auditInstance:deleteDatabase	-
POST /dbss/v1/{project_id}/{instance_id}/audit/operation/delete-database	dbss:auditInstance:deleteDatabase	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/scopes	dbss:auditInstance:addAuditScopeRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/scope/add-rule	dbss:auditInstance:addAuditScopeRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/scope/switch	dbss:auditInstance:switchAuditScopeRule	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk	dbss:auditInstance:addRiskRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/add-rule	dbss:auditInstance:addRiskRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/switch	dbss:auditInstance:switchRiskRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/{risk_id}	dbss:auditInstance:editRiskRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/edit-risk/{risk_id}	dbss:auditInstance:editRiskRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/scopes/{scope_id}	dbss:auditInstance:editAuditScopeRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/operation/email/{email_id}	dbss:auditInstance:configAlarmEmail	-
POST /dbss/v1/{project_id}/{instance_id}/audit/operation/edit-email/{email_id}	dbss:auditInstance:configAlarmEmail	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/rank-risk	dbss:auditInstance:setRiskRulePriority	-
POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql-rule/{rule_id}	dbss:auditInstance:editSqlInjectRule	-
DELETE /dbss/v1/{project_id}/{instance_id}/audit/rul	dbss:auditInstance:deleteSqlInjectRule	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
e/sql-rule/{rule_id}		
POST /dbss/v1/{project_id}/{instance_id}/audit/reports/templates/scheduler/config-task	dbss:auditInstance:setReporterConfig	-
POST /dbss/v1/{project_id}/{instance_id}/audit/general/risk-statistics	dbss:auditInstance:listStatistics	-
POST /dbss/v1/{project_id}/{instance_id}/audit/general/session-statistics	dbss:auditInstance:listStatistics	-
POST /dbss/v1/{project_id}/{instance_id}/audit/general/sql-statistics	dbss:auditInstance:listStatistics	-
GET /dbss/v1/{project_id}/{instance_id}/audit/reports/templates/scheduler/{template_id}	dbss:auditInstance:getReporterConfig	-
GET /dbss/v1/{project_id}/{instance_id}/audit/sqls/{sql_statement_id}	dbss:auditInstance:listSqls	-
GET /dbss/v1/{project_id}/{instance_id}/audit/sensitive/result/switch	dbss:auditInstance:listSensitiveRules	-
GET /dbss/v1/{project_id}/{instance_id}/audit/sensitive/mask/switch	dbss:auditInstance:listSensitiveRules	-
POST /dbss/v1/{project_id}/{instance_id}/audit/sensitive/result/switch	dbss:auditInstance:modifySensitiveRuleSaveResultSwitch	-
POST /dbss/v1/{project_id}/{instance_id}/audit/sensitive/mask/switch	dbss:auditInstance:modifySensitiveRuleAnonymizeSwitch	-
DELETE /dbss/v1/{project_id}/	dbss:auditInstance:deleteSensitiveRule	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
{instance_id}/audit/sensitive/masks/{rule_id}		
POST /dbss/v1/{project_id}/{instance_id}/audit/sensitive/mask/rule/switch	dbss:auditInstance:switchSensitiveRule	-
DELETE /dbss/v1/{project_id}/{instance_id}/audit/rule/scopes/{scope_id}	dbss:auditInstance:deleteAuditScopeRule	-
DELETE /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/{risk_id}	dbss:auditInstance:deleteRiskRule	-
POST /dbss/v1/{project_id}/{instance_id}/audit/general/alarm-log	dbss:auditInstance:listAlarmItems	-
POST /dbss/v1/{project_id}/{instance_id}/audit/alarm-log	dbss:auditInstance:listAlarmItems	-
PUT /dbss/v1/{project_id}/{instance_id}/audit/general/alarm-log/{alarm_id}	dbss:auditInstance:markAlarm	-
DELETE /dbss/v1/{project_id}/{instance_id}/audit/general/alarm-log/{alarm_id}	dbss:auditInstance:deleteAlarm	-
POST /dbss/v1/{project_id}/{instance_id}/audit/general/mark-alarm-log	dbss:auditInstance:markAlarm	-
POST /dbss/v1/{project_id}/{instance_id}/audit/general/synopsis-statistics	dbss:auditInstance:listStatistics	-
POST /dbss/v1/{project_id}/{instance_id}/audit/ba	dbss:auditInstance:listBackups	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ckups		
POST /dbss/v1/{project_id}/{instance_id}/audit/backup/get-backup	dbss:auditInstance:listBackups	-
DELETE /dbss/v1/{project_id}/{instance_id}/audit/backups/{id}	dbss:auditInstance:deleteBackup	-
POST /dbss/v1/{project_id}/{instance_id}/audit/backup/restore	dbss:auditInstance:restoreBackup	-
POST /dbss/v1/{project_id}/{instance_id}/audit/backup/retry	dbss:auditInstance:retryBackup	-
GET /dbss/v1/{project_id}/{instance_id}/audit/backup/bucket-name	dbss:auditInstance:getBackupConfig	-
GET /dbss/v1/{project_id}/{instance_id}/audit/backup/status	dbss:auditInstance:listBackups	-
GET /dbss/v1/{project_id}/{instance_id}/audit/backup/auto-backup-template	dbss:auditInstance:getBackupConfig	-
GET /dbss/v1/{project_id}/{instance_id}/audit/backup/risk-templates	dbss:auditInstance:getRiskBackupConfigInfo	-
GET /dbss/v1/{project_id}/{instance_id}/audit/backup/risk-template/{db_id}	dbss:auditInstance:getRiskBackupConfigInfo	-
POST /dbss/v1/{project_id}/{instance_id}/audit/backup/risk/switch	dbss:auditInstance:switchRiskBackup	-
GET /dbss/v1/{project_id}/	dbss:auditInstance:getRiskBackupBucketInfo	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
{instance_id}/audit/backup/risk-bucket-path		
POST /dbss/v1/{project_id}/{instance_id}/audit/backup/risk-bucket-path	dbss:auditInstance:setRiskBackupBucketInfo	-
GET /dbss/v1/{project_id}/{instance_id}/audit/backup/bucket-path	dbss:auditInstance:getBackupConfig	-
POST /dbss/v1/{project_id}/{instance_id}/dbss/audit/databases/rds	dbss:auditInstance:addRdsDatabase	-
POST /dbss/v1/{project_id}/{instance_id}/audit/operation/rds	dbss:auditInstance:addRdsDatabase	-
POST /dbss/v1/{project_id}/{instance_id}/audit/operation/create-guassdb-rds	dbss:auditInstance:addRdsDatabase	-
POST /dbss/v2/{project_id}/{instance_id}/audit/databases/rds	dbss:auditInstance:addRdsDatabase	-
POST /dbss/v1/{domain_id}/{instance_id}/audit/backup/risk-bucket-path/global	dbss:auditInstance:setRiskBackupBucketInfo	-
POST /dbss/v1/{domain_id}/{instance_id}/audit/backup/global/switch	dbss:auditInstance:switchBackup	dbss:auditInstance:getBackupConfig
POST /dbss/v1/{domain_id}/{instance_id}/audit/backup/risk/global/switch	dbss:auditInstance:switchRiskBackup	-
GET /dbss/v1/{project_id}/dbss/server-info	dbss::getServerInfo	-
GET	dbss::getAuditInstanceJob	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/dbss/v1/{project_id}/dbss/audit/jobs/{resource_id}		
GET /dbss/v1/{project_id}/dbss/audit/list-jobs/{resource_id}	dbss::getAuditInstanceJob	-
GET /dbss/v1/{project_id}/dbss/audit/list-jobs	dbss:auditInstance:listJobs	-
GET /dbss/v1/{project_id}/dbss/audit/specification	dbss::listCommonInfo	-
GET /dbss/v1/{project_id}/dbss/audit/instances	dbss:auditInstance:instanceList	-
GET /dbss/v1/{project_id}/dbss/audit/quota	dbss::listCommonInfo	-
GET /dbss/v1/{project_id}/dbss/availability-zone	dbss::listCommonInfo	-
GET /dbss/v1/{project_id}/dbss/get-availability-zone	dbss::listCommonInfo	-
GET /dbss/v1/{project_id}/obs/audit/backup/obs-buckets	dbss::listObsBuckets	-
POST /dbss/v1/{project_id}/dbss/audit/security-group	dbss:auditInstance:updateSecurityGroup	-
POST /dbss/v1/{project_id}/dbss/audit/instances	dbss:auditInstance:createOnDemand	dbss::listCommonInfo
DELETE /dbss/v1/{project_id}/dbss/audit/delete-instance	dbss:auditInstance:instanceDelete	-
POST /dbss/v1/{project_id}/	dbss::listResourcesByTag	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
{resource_type}/resource-instances/filter		
POST /dbss/v1/{project_id}/{resource_type}/resource-instances/count	dbss::listResourcesByTag	-
POST /dbss/v1/{project_id}/{resource_type}/{resource_id}/tags/create	dbss::tagResource	-
DELETE /dbss/v1/{project_id}/{resource_type}/{resource_id}/tags/delete	dbss::unTagResource	-
GET /dbss/v1/{project_id}/{resource_type}/tags	dbss::listTags	-
GET /dbss/v1/{project_id}/{resource_type}/{resource_id}/tags	dbss::listTagsForResource	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-150 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

DBSS 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-150 DBSS 支持的资源类型

资源类型	URN
auditInstance	dbss:<region>:<account-id>:auditInstance:<instance-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。

 版权所有 © 华为云计算技术有限公司

  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 dbss:）仅适用于对应服务的操作，详情请参见表 3-151。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

DBSS 支持的服务级条件键

DBSS 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-151 DBSS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
dbss:VpcId	string	单值	根据请求参数中指定的网络 ID 过滤访问。
dbss:SubnetId	string	单值	根据请求参数中指定的子网 ID 过滤访问。

3.7.7 数据安全中心 DSC

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

 版权所有 © 华为云计算技术有限公司

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 DSC 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 DSC 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 DSC 的相关操作。

表3-152 DSC 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dsc:asset:delete	授予权限以删除数据资产。	write	asset *	-	-
dsc:asset:list	授予权限以查询数据资产列表。	list	asset *	-	-
dsc:asset:create	授予权限以添加数据资产。	write	asset *	-	-
dsc:asset:update	授予权限以更新数据资产信息。	write	asset *	-	-
dsc:common:operate	授予权限以操作 DSC 通用资源。	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dsc:common:list	授予权限以查询 DSC 通用资源列表。	list	-	-	-
dsc:maskTask:operate	授予权限以操作脱敏任务（启动、停止、开启、关闭等）。	write	maskTask *	-	-
dsc:maskTask:listSubTasks	授予权限以查询脱敏任务的子任务列表。	list	maskTask *	-	-
dsc:common:operate	授予权限以操作 DSC 通用资源。	write	-	-	-
dsc:common:list	授予权限以查询 DSC 通用资源列表。	list	-	-	-
dsc:scanTask:create	授予权限以创建敏感数据扫描任务。	write	scanTask *	-	-
dsc:scanTask:list	授予权限以查询敏感数据扫描任务列表或子任务列表。	list	scanTask *	-	-
dsc:scanRuleGroup:list	授予权限以查询扫描规则组列表。	list	-	-	-
dsc:scanRuleGroup:create	授予权限以创建扫描规则组。	write	-	-	-
dsc:scanRuleGroup:delete	授予权限以删除扫描规则组。	write	-	-	-
dsc:scanRule:list	授予权限以查询扫描规则列表。	list	scanRule *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dsc:scanRule:create	授予权限以创建扫描规则。	write	scanRule *	-	-
dsc:scanRule:update	授予权限以更新扫描规则。	write	scanRule *	-	-
dsc:scanRule:delete	授予权限以删除扫描规则。	write	scanRule *	-	-
dsc:scanTask:getResults	授予权限以查询单个扫描任务的扫描结果。	read	scanTask *	-	-
dsc:sensitiveData:mask	授予权限以对敏感数据进行动态脱敏。	write	-	-	-
dsc:watermark:embed	授予权限以对文档、图片或者数据库嵌入水印。	write	-	-	-
dsc:watermark:extract	授予权限以从文档、图片或者数据库中提取水印。	write	-	-	-
dsc:authorization:get	授予权限以查看云数据资产的授权情况。	permission_management	-	-	-

DSC 的 API 通常对应着一个或多个授权项。表 3-153 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-153 API 与授权项的关系

API	对应的授权项	依赖的授权项
DELETE/v1/{project_id}/sdg/asset/obs/bucket/{bucket_id}	dsc:asset:delete	obs:bucket:GetBucketLogging
		obs:bucket:PutBucketLogging
GET/v1/{project_id}/sdg/asset/obs/buckets	dsc:asset:list	obs:bucket:listAllMyBuckets

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST/v1/{project_id}/sdg/asset/obs/buckets	dsc:asset:create	obs:bucket:GetBucketStorage
		obs:bucket:listAllMyBuckets
PUT/v1/{project_id}/sdg/asset/{asset_id}/name	dsc:asset:update	-
POST/v1/{project_id}/period/order	dsc:common:operate	bss:renewal:update
		bss:order:update
GET/v1/{project_id}/period/product/specification	dsc:common:list	-
POST/v1/{project_id}/sdg/server/mask/dbs/templates/{template_id}/operation	dsc:maskTask:operate	-
GET/v1/{project_id}/sdg/server/mask/dbs/templates/{template_id}/tasks	dsc:maskTask:listSubTasks	-
PUT/v1/{project_id}/sdg/smn/topic	dsc:common:operate	-
GET/v1/{project_id}/sdg/smn/topics	dsc:common:list	smn:topic:list
GET/v1/{project_id}/openapi/called-records	dsc:common:list	-
POST/v1/{project_id}/sdg/scan/job	dsc:scanTask:create	-
GET/v1/{project_id}/sdg/scan/jobs	dsc:scanTask:list	-
GET/v1/{project_id}/sdg/server/scan/groups	dsc:scanRuleGroup:list	-
POST/v1/{project_id}/sdg/server/scan/groups	dsc:scanRuleGroup:create	-
DELETE/v1/{project_id}/sdg/server/scan/groups/{group_id}	dsc:scanRuleGroup:delete	-
GET/v1/{project_id}/sdg/server/scan/rules	dsc:scanRule:list	-
POST/v1/{project_id}/sdg/server/scan/rules	dsc:scanRule:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT/v1/{project_id}/sdg/server/scan/rules	dsc:scanRule:update	-
DELETE/v1/{project_id}/sdg/server/scan/rules/{rule_id}	dsc:scanRule:delete	-
GET/v1/{project_id}/sdg/scan/job/{job_id}/results	dsc:scanTask:getResults	-
GET/v1/{project_id}/sdg/server/relation/jobs/{job_id}/dbs	dsc:common:list	-
GET/v1/{project_id}/sdg/server/relation/jobs/{job_id}/dbs/{db_id}/tables	dsc:common:list	-
GET/v1/{project_id}/sdg/server/relation/jobs/{job_id}/dbs/{table_id}/columns	dsc:common:list	-
GET/v1/{project_id}/sdg/server/relation/jobs/{job_id}/obs/buckets	dsc:common:list	-
GET/v1/{project_id}/sdg/server/relation/jobs/{job_id}/obs/{bucket_id}/files	dsc:common:list	-
POST/v1/{project_id}/data/mask	dsc:sensitiveData:mask	-
POST/v1/{project_id}/doc-address/watermark/embed	dsc:watermark:embed	-
POST/v1/{project_id}/doc-address/watermark/extract	dsc:watermark:extract	-
POST/v1/{project_id}/image-address/watermark/embed	dsc:watermark:embed	-
POST/v1/{project_id}/image-address/watermark/extract	dsc:watermark:extract	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST/v1/{project_id}/image-address/watermark/extract-image	dsc:watermark:extract	-
POST/v1/{project_id}/image/watermark/embed	dsc:watermark:embed	-
POST/v1/{project_id}/image/watermark/extract	dsc:watermark:extract	-
POST/v1/{project_id}/image/watermark/extract-image	dsc:watermark:extract	-
POST/v1/{project_id}/sdg/database/watermark/embed	dsc:watermark:embed	-
POST/v1/{project_id}/sdg/database/watermark/extract	dsc:watermark:extract	-
POST/v1/{project_id}/sdg/doc/watermark/embed	dsc:watermark:embed	-
POST/v1/{project_id}/sdg/doc/watermark/extract	dsc:watermark:extract	-
GET/v1/{project_id}/sdg/asset/{asset_type}/{asset_id}/detail	dsc:common:list	-
GET /v1/{project_id}/sdg/asset/authorization	dsc:authorization:get	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-154 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

DSC 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

 版权所有 © 华为云计算技术有限公司

表3-154 DSC 支持的资源类型

资源类型	URN
scanTask	dsc:<region>:<account-id>:scanTask:<task-id>
scanRule	dsc:<region>:<account-id>:scanRule:<rule-id>
scanTemplate	dsc:<region>:<account-id>:scanTemplate:<template-id>
maskTask	dsc:<region>:<account-id>:maskTask:<task-id>
asset	dsc:<region>:<account-id>:asset:<asset-id>

条件（Condition）

DSC 服务不支持在身份策略中的条件键中配置服务级的条件键。DSC 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.7.8 Web 应用防火墙 WAF

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。

 版权所有 © 华为云计算技术有限公司

- 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
- 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

关于 WAF 定义的资源类型的详细信息请参见资源类型（Resource）。

- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 WAF 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 WAF 的相关操作。

表3-155 WAF 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
waf:host:list	授予查询防护域名列表的权限。	List	host *	-	waf:instance:list
			-	g:EnterpriseProjectId	
waf:host:create	授予创建防护域名的权限。	Write	host *	-	waf:instance:create
			policy	-	
			certificate	-	
			-	g:EnterpriseProjectId	
waf:host:get	授予查询防护域名的权限。	Read	host *	g:EnterpriseProjectId	waf:instance:get
waf:host:put	授予更新防护域名的权限。	Write	host *	g:EnterpriseProjectId	waf:instance:put
			certificate	-	
waf:host:delete	授予删除防护域名的权限。	Write	host *	g:EnterpriseProjectId	waf:instance:delete
waf:sourceIp:get	授予查询回源IP 信息的权限。	Read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
waf:policy:list	授予查询防护策略列表的权限。	List	policy *	-	-
			-	g:EnterpriseProjectId	
waf:policy:create	授予创建防护策略的权限。	Write	policy *	-	-
			-	g:EnterpriseProjectId	
waf:policy:get	授予查询防护策略的权限。	Read	policy *	g:EnterpriseProjectId	-
waf:policy:put	授予更新防护策略的权限。	Write	policy *	g:EnterpriseProjectId	-
			host	-	
waf:policy:delete	授予删除防护策略的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:ccRule:list	授予查询 cc 规则列表的权限。	List	policy *	-	waf:ccRuleRule:list
			-	g:EnterpriseProjectId	
waf:ccRule:create	授予创建 cc 规则的权限。	Write	policy *	-	-
			-	g:EnterpriseProjectId	
waf:ccRule:get	授予查询 cc 规则的权限。	Read	policy *	g:EnterpriseProjectId	-
waf:ccRule:put	授予更新 cc 规则的权限。	Write	policy *	g:EnterpriseProjectId	waf:ccRuleRule:put
waf:ccRule:delete	授予删除 cc 规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:preciseProtectionRule:list	授予查询精准防护规则列表的权限。	List	policy *	-	-
			-	g:EnterpriseProjectId	
waf:preciseProt	授予创建精准	Write	policy	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ectionRule:create	防护规则的权限。		*		
			-	g:EnterpriseProjectId	
waf:preciseProtectionRule:get	授予查询精准防护规则的权限。	Read	policy *	g:EnterpriseProjectId	-
waf:preciseProtectionRule:put	授予更新精准防护规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:preciseProtectionRule:delete	授予删除精准防护规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:whiteBlackIpRule:list	授予查询黑白名单规则列表的权限。	List	policy *	-	-
			-	g:EnterpriseProjectId	
waf:whiteBlackIpRule:create	授予创建黑白名单规则的权限。	Write	policy *	-	-
			-	g:EnterpriseProjectId	
waf:whiteBlackIpRule:get	授予查询黑白名单规则的权限。	Read	policy *	g:EnterpriseProjectId	-
waf:whiteBlackIpRule:put	授予更新黑白名单规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:whiteBlackIpRule:delete	授予删除黑白名单规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:privacyRule:list	授予查询隐私屏蔽规则列表的权限。	List	policy *	-	-
			-	g:EnterpriseProjectId	
waf:privacyRule:create	授予创建隐私屏蔽规则的权	Write	policy *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。		-	g:EnterpriseProjectId	
waf:privacyRule:get	授予查询隐私屏蔽规则的权限。	Read	policy *	g:EnterpriseProjectId	-
waf:privacyRule:put	授予更新隐私屏蔽规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:privacyRule:delete	授予删除隐私屏蔽规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:falseAlarmMaskRule:list	授予查询误报屏蔽规则列表的权限。	List	policy *	-	-
			-	g:EnterpriseProjectId	
waf:falseAlarmMaskRule:create	授予创建误报屏蔽规则的权限。	Write	policy *	-	-
			-	g:EnterpriseProjectId	
waf:falseAlarmMaskRule:get	授予查询误报屏蔽规则的权限。	Read	policy *	g:EnterpriseProjectId	-
waf:falseAlarmMaskRule:put	授予更新误报屏蔽规则的权限。	Write	policy *	g:EnterpriseProjectId	waf:falseAlarmMaskRule:recount
waf:falseAlarmMaskRule:delete	授予删除误报屏蔽规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:geoIpRule:list	授予查询地理位置封禁规则列表的权限。	List	policy *	-	-
			-	g:EnterpriseProjectId	
waf:geoIpRule:create	授予创建地理位置封禁规则的权限。	Write	policy *	-	-
			-	g:EnterpriseProjectId	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
waf:geoIpRule:get	授予查询地理位置封禁规则的权限。	Read	policy *	g:EnterpriseProjectId	-
waf:geoIpRule:put	授予更新地理位置封禁规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:geoIpRule:delete	授予删除地理位置封禁规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:antiTamperRule:list	授予查询网页防篡改规则列表的权限。	List	policy *	-	-
			-	g:EnterpriseProjectId	
waf:antiTamperRule:create	授予创建网页防篡改规则的权限。	Write	policy *	-	-
			-	g:EnterpriseProjectId	
waf:antiTamperRule:get	授予查询网页防篡改规则的权限。	Read	policy *	g:EnterpriseProjectId	-
waf:antiTamperRule:put	授予更新网页防篡改规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:antiTamperRule:delete	授予删除网页防篡改规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:antiLeakageRule:list	授予查询反敏感信息泄漏规则列表的权限。	List	policy *	-	-
			-	g:EnterpriseProjectId	
waf:antiLeakageRule:create	授予创建反敏感信息泄漏规则的权限。	Write	policy *	-	-
			-	g:EnterpriseProjectId	
waf:antiLeakageRule:get	授予查询反敏感信息泄漏规	Read	policy *	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	则的权限。				
waf:antiLeakageRule:put	授予更新反敏感信息泄漏规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:antiLeakageRule:delete	授予删除反敏感信息泄漏规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:anticrawlerRule:list	授予查询反爬虫规则列表的权限。	List	policy *	-	-
			-	g:EnterpriseProjectId	
waf:anticrawlerRule:create	授予创建反爬虫规则的权限。	Write	policy *	-	-
			-	g:EnterpriseProjectId	
waf:anticrawlerRule:get	授予查询反爬虫规则的权限。	Read	policy *	g:EnterpriseProjectId	-
waf:anticrawlerRule:put	授予更新反爬虫规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:anticrawlerRule:delete	授予删除反爬虫规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:punishmentRule:list	授予查询攻击惩罚规则列表的权限。	List	policy *	-	-
			-	g:EnterpriseProjectId	
waf:punishmentRule:create	授予创建攻击惩罚规则的权限。	Write	policy *	-	-
			-	g:EnterpriseProjectId	
waf:punishmentRule:get	授予查询攻击惩罚规则的权限。	Read	policy *	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
waf:punishmentRule:put	授予更新攻击惩罚规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:punishmentRule:delete	授予删除攻击惩罚规则的权限。	Write	policy *	g:EnterpriseProjectId	-
waf:valueList:list	授予查询引用表列表的权限。	List	-	g:EnterpriseProjectId	-
waf:valueList:create	授予创建引用表的权限。	Write	-	g:EnterpriseProjectId	-
waf:valueList:get	授予查询引用表的权限。	Read	-	g:EnterpriseProjectId	-
waf:valueList:put	授予更新引用表的权限。	Write	-	g:EnterpriseProjectId	-
waf:valueList:delete	授予删除引用表的权限。	Write	-	g:EnterpriseProjectId	-
waf:ipgroup:list	授予查询 IP 地址组列表的权限。	List	-	g:EnterpriseProjectId	-
waf:ipgroup:create	授予创建 IP 地址组的权限。	Write	-	g:EnterpriseProjectId	-
waf:ipgroup:get	授予查询 IP 地址组的权限。	Read	-	g:EnterpriseProjectId	-
waf:ipgroup:put	授予修改 IP 地址组的权限。	Write	-	g:EnterpriseProjectId	-
waf:ipgroup:delete	授予删除 IP 地址组的权限。	Write	-	g:EnterpriseProjectId	-
waf:certificate:list	授予查看证书列表的权限。	List	certificate *	-	-
			-	g:EnterpriseProjectId	
waf:certificate:create	授予创建证书	Write	certificate *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	的权限。		-	g:EnterpriseProjectId	
waf:certificate:get	授予查询证书的权限。	Read	certificate *	g:EnterpriseProjectId	-
waf:certificate:put	授予修改 WAF 证书的权限。	Write	certificate *	g:EnterpriseProjectId	-
waf:certificate:delete	授予删除证书的权限。	Write	certificate *	g:EnterpriseProjectId	-
waf:certificate:apply	授予应用证书到域名的权限。	Write	certificate *	g:EnterpriseProjectId	-
			host *	-	
waf:premiumInstance:list	授予查询独享引擎实例列表的权限。	List	premiumInstance *	-	-
			-	g:EnterpriseProjectId	
waf:premiumInstance:create	授予创建独享引擎实例的权限。	Write	premiumInstance *	-	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
waf:premiumInstance:get	授予查询独享引擎实例的权限。	Read	premiumInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
waf:premiumInstance:put	授予更新独享引擎实例的权限。	Write	premiumInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
waf:premiumIn	授予删除独享	Write	premiumIns	• g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
stance:delete	引擎实例的权限。		tance *	key> • g:EnterpriseProjectId	
waf:event:get	授予查询防护事件的权限。	Read	-	g:EnterpriseProjectId	-
waf:ltsConfig:get	授予查询对接云日志的配置的权限。	List	-	g:EnterpriseProjectId	-
waf:ltsConfig:put	授予更新对接云日志配置的权限。	Write	-	g:EnterpriseProjectId	-
waf:prepaid:create	授予创建包周期订单的权限。	Write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	-
waf:subscription:get	授予查询云模式订购信息的权限。	Read	-	-	-
waf:alert:get	授予查询告警通知的配置的权限。	List	-	-	-
waf:alert:put	授予更新告警通知配置的权限。	Write	-	-	-
waf:consoleConfig:get	授予查询页面配置信息的权限。	Read	-	-	-

WAF 的 API 通常对应着一个或多个授权项。表 3-156 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-156 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST	waf:host:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/waf/instance		
DELETE /v1/{project_id}/waf/instance/{instance_id}	waf:host:delete	-
GET /v1/{project_id}/waf/instance	waf:host:list	-
GET /v1/{project_id}/waf/instance/{instance_id}/route	waf:host:get	-
GET /v1/{project_id}/waf/instance/{instance_id}	waf:host:get	-
PATCH /v1/{project_id}/waf/instance/{instance_id}	waf:host:put	-
PUT /v1/{project_id}/waf/instance/{instance_id}/protect-status	waf:host:put	-
POST /v1/{project_id}/premium-waf/host	waf:host:create	-
DELETE /v1/{project_id}/premium-waf/host/{host_id}	waf:host:delete	-
GET /v1/{project_id}/premium-waf/host	waf:host:list	-
GET /v1/{project_id}/premium-waf/host/{host_id}	waf:host:get	-
PUT /v1/{project_id}/premium-waf/host/{host_id}	waf:host:put	-
PUT /v1/{project_id}/premium-waf/host/{host_id}/protect-status	waf:host:put	-
POST /v1/{project_id}/waf/p	waf:policy:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
olicy		
DELETE /v1/{project_id}/waf/policy/{policy_id}	waf:policy:delete	-
GET /v1/{project_id}/waf/policy	waf:policy:list	-
GET /v1/{project_id}/waf/policy/{policy_id}	waf:policy:get	-
PATCH /v1/{project_id}/waf/policy/{policy_id}	waf:policy:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}	waf:policy:put	-
POST /v1/{project_id}/waf/policy/{policy_id}/cc	waf:ccRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/custom	waf:preciseProtectionRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/antitamper	waf:antiTamperRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/antileakage	waf:antiLeakageRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/anticrawler	waf:anticrawlerRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/punishment	waf:punishmentRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/geoip	waf:geoIpRule:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/waf/policy/{policy_id}/ignore	waf:falseAlarmMaskRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/privacy	waf:privacyRule:create	-
POST /v1/{project_id}/waf/valuelist	waf:valueList:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/whiteblackip	waf:whiteBlackIpRule:create	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}	waf:ccRule:delete	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}	waf:preciseProtectionRule:delete	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}	waf:antiTamperRule:delete	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id}	waf:antiLeakageRule:delete	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/anticrawler/{rule_id}	waf:anticrawlerRule:delete	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/punishment/{rule_id}	waf:punishmentRule:delete	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}	waf:geoIpRule:delete	-
DELETE /v1/{project_id}/waf/p	waf:falseAlarmMaskRule:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
olicy/{policy_id}/ignore/{rule_id}		
DELETE /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}	waf:privacyRule:delete	-
DELETE /v1/{project_id}/waf/valuelist/{valuelistid}	waf:valueList:delete	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}	waf:whiteBlackIpRule:delete	-
GET /v1/{project_id}/waf/policy/{policy_id}/custom	waf:preciseProtectionRule:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/cc	waf:ccRule:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/antitamper	waf:antiTamperRule:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/antileakage	waf:antiLeakageRule:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/anticrawler	waf:anticrawlerRule:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/punishment	waf:punishmentRule:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/geoip	waf:geoIpRule:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/ignore	waf:falseAlarmMaskRule:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/waf/policy/{policy_id}/privacy	waf:privacyRule:list	-
GET /v1/{project_id}/waf/valuelist	waf:valueList:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip	waf:whiteBlackIpRule:list	-
PUT /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}	waf:ccRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}	waf:preciseProtectionRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}	waf:geoIpRule:put	-
POST /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}/refresh	waf:antiTamperRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id}	waf:antiLeakageRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/anticrawler/{rule_id}	waf:anticrawlerRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/anticrawler	waf:anticrawlerRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/punishment/{rule_id}	waf:punishmentRule:put	-
PUT	waf:whiteBlackIpRule:put	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/waf/policy/{policy_id}/{ruletype}/{rule_id}/status		
PUT /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}	waf:privacyRule:put	-
PUT /v1/{project_id}/waf/valuelist/{valuelistid}	waf:valueList:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}	waf:whiteBlackIpRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}	waf:falseAlarmMaskRule:put	-
GET /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}	waf:ccRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}	waf:preciseProtectionRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}	waf:whiteBlackIpRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}	waf:privacyRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}	waf:falseAlarmMaskRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}	waf:geoIpRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/antit	waf:antiTamperRule:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
amper/{rule_id}		
GET /v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id}	waf:antiLeakageRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/anticrawler/{rule_id}	waf:anticrawlerRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/punishment/{rule_id}	waf:punishmentRule:get	-
GET /v1/{project_id}/waf/valuelist/{valuelistid}	waf:valueList:get	-
POST /v1/{project_id}/waf/ip-groups	waf:ipgroup:create	-
DELETE /v1/{project_id}/waf/ip-group/{id}	waf:ipgroup:delete	-
GET /v1/{project_id}/waf/ip-groups	waf:ipgroup:list	-
GET /v1/{project_id}/waf/ip-group/{id}	waf:ipgroup:get	-
PUT /v1/{project_id}/waf/ip-group/{id}	waf:ipgroup:put	-
POST /v1/{project_id}/waf/certificate/{certificate_id}/apply-to-hosts	waf:certificate:apply	-
POST /v1/{project_id}/waf/certificate	waf:certificate:create	-
DELETE /v1/{project_id}/waf/certificate/{certificate_id}	waf:certificate:delete	-
GET /v1/{project_id}/waf/c	waf:certificate:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ertificate		
GET /v1/{project_id}/waf/certificate/{certificate_id}	waf:certificate:get	-
PUT /v1/{project_id}/waf/certificate/{certificate_id}	waf:certificate:put	-
GET /v1/{project_id}/waf/event	waf:event:get	-
GET /v1/{project_id}/waf/event/{eventid}	waf:event:get	-
GET /v1/{project_id}/waf/overviews/bandwidth/timeline	waf:event:get	-
GET /v1/{project_id}/waf/overviews/classification	waf:event:get	-
GET /v1/{project_id}/waf/overviews/qps/timeline	waf:event:get	-
GET /v1/{project_id}/waf/overviews/request/timeline	waf:event:get	-
GET /v1/{project_id}/waf/overviews/statistics	waf:event:get	-
GET /v1/{project_id}/waf/overviews/abnormal	waf:event:get	-
GET /v1/{project_id}/waf/config/console	waf:consoleConfig:get	-
POST /v1/{project_id}/premium-waf/instance	waf:premiumInstance:create	-
DELETE /v1/{project_id}/premium-	waf:premiumInstance:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
waf/instance/{instance_id}		
GET /v1/{project_id}/premium-waf/instance	waf:premiumInstance:list	-
PUT /v1/{project_id}/premium-waf/instance/{instance_id}	waf:premiumInstance:put	-
GET /v1/{project_id}/premium-waf/instance/{instance_id}	waf:premiumInstance:get	-
GET /v1/{project_id}/waf/config/lts	waf:ltsConfig:get	-
PUT /v1/{project_id}/waf/config/lts/{ltsconfig_id}	waf:ltsConfig:put	-
POST /v1/{project_id}/waf/subscription/batchalter/prepaid-cloud-waf	waf:prepaid:create	-
POST /v1/{project_id}/waf/subscription/purchase/prepaid-cloud-waf	waf:prepaid:create	-
GET /v1/{project_id}/waf/subscription	waf:subscription:get	-
GET /v2/{project_id}/waf/alerts	waf:alert:get	-
PUT /v2/{project_id}/waf/alert/{alert_id}	waf:alert:put	-
GET /v1/{project_id}/waf/config/source-ip	waf:sourceIp:get	-
POST /v1/{project_id}/comp	waf:host:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
osite-waf/hosts/migration		
GET /v1/{project_id}/composite-waf/host	waf:host:list	-
GET /v1/{project_id}/composite-waf/host/{host_id}	waf:host:get	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-157 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

WAF 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-157 WAF 支持的资源类型

资源类型	URN
policy	waf:<region>:<account-id>:policy:<policy-id>
host	waf:<region>:<account-id>:host:<host-id>
premiumInstance	waf:<region>:<account-id>:premiumInstance:<instance-id>
certificate	waf:<region>:<account-id>:certificate:<certificate-id>

条件（Condition）

WAF 服务不支持在身份策略中的条件键中配置服务级的条件键。WAF 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.7.9 企业主机安全 HSS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含

 版权所有 © 华为云计算技术有限公司

的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 HSS 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 HSS 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 HSS 的相关操作。

表3-158 HSS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:host:addHostsGroup	授予权限以创建服务器组。	write	host *	g:EnterpriseProjectId	hss:hostGroup:set
hss:ars:addPWLPolicyHost	授予权限以进行白名单策略	write	host *	g:EnterpriseProjectId	hss:ars:set

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	添加主机。				
hss:rasp:addRaspPolicy	授予权限以添加防护策略。	write	-	g:EnterpriseProjectId	hss:rasp:set
hss:safetyReport:addSecurityReport	授予权限以创建或复制新报告。	write	-	g:EnterpriseProjectId	hss:safetyReport:set
hss:wtp:addTimingOffConfigInfo	授予权限以添加定时关闭防护配置。	write	host *	g:EnterpriseProjectId	hss:wtpScheduledProtections:set
hss:wtp:addWtpHostProtectDirInfo	授予权限以增加防护目录。	write	host *	g:EnterpriseProjectId	hss:wtpDirectorys:set
hss:wtp:addWtpPrivilegedProcessInfo	授予权限以添加特权进程。	write	host *	g:EnterpriseProjectId	hss:wtpPrivilegedProcess:set
hss:setting:changeAutoKillVirusStatus	授予权限以开启或关闭程序自动隔离查杀。	write	-	g:EnterpriseProjectId	hss:automaticKillMp:set
hss:event:changeBlockedIp	授予权限以解除拦截。	write	host *	g:EnterpriseProjectId	hss:accountCracks:unblock
hss:setting:changeMalwareCollectStatus	授予权限以开启或关闭恶意软件云查样本收集配置。	write	-	g:EnterpriseProjectId	hss:automaticKillMp:set
hss:ars:changePWLPolicy	授予权限以修改白名单策略。	write	-	g:EnterpriseProjectId	hss:ars:set
hss:ars:changePWLPolicyProcessStatus	授予权限以标记进程白名单策略识别进程。	write	-	g:EnterpriseProjectId	hss:ars:set
hss:safetyReport:changeSecurityReport	授予权限以修改报告。	write	-	g:EnterpriseProjectId	hss:safetyReport:set
hss:ars:createP	授予权限以创	write	host *	-	hss:ars:set

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
WLPolicy	建白名单策略。		-	g:EnterpriseProjectId	
hss:ars:deletePWLPolicy	授予权限以删除白名单策略。	write	-	g:EnterpriseProjectId	hss:ars:set
hss:ars:deletePWLPolicyHost	授予权限以进行白名单策略删除主机。	write	host *	g:EnterpriseProjectId	hss:ars:set
hss:antiransomware:deleteRansomwareDuplicationInfo	授予权限以删除备份副本。	write	-	g:EnterpriseProjectId	hss:antiransomware:set
hss:antiransomware:deleteRansomwareProtectionPolicy	授予权限以删除防护策略。	write	-	g:EnterpriseProjectId	hss:antiransomware:set
hss:rasp:deleteRaspPolicy	授予权限以删除防护策略。	write	-	g:EnterpriseProjectId	hss:rasp:set
hss:safetyReport:deleteSecurityReport	授予权限以删除报告。	write	-	g:EnterpriseProjectId	hss:safetyReport:set
hss:wtp:deleteTimingOffConfigInfo	授予权限以删除定时关闭防护配置。	write	host *	g:EnterpriseProjectId	hss:wtpScheduledProtections:set
hss:wtp:deleteWtpBackupHostInfo	授予权限以删除远端备份服务器。	write	host *	g:EnterpriseProjectId	hss:wtpBackup:set
hss:wtp:deleteWtpHostProtectDirInfo	授予权限以删除防护目录。	write	host *	g:EnterpriseProjectId	hss:wtpDirectorys:set
hss:wtp:deleteWtpPrivilegedProcessInfo	授予权限以删除特权进程。	write	host *	g:EnterpriseProjectId	hss:wtpPrivilegedProcess:set
hss:setting:getAgentInstallScript	授予权限以查询 agent 安装脚本。	read	-	g:EnterpriseProjectId	hss:installAgent:get
hss:setting:getA	授予权限以查	read	-	g:EnterprisePro	hss:alertConfig:

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
larmConfig	询告警配置。			jectId	get
hss:rasp:getAppRaspSwitchStatus	授予权限以查询应用防护开启状态。	read	host *	g:EnterpriseProjectId	hss:rasp:list
hss:setting:getAutoKillVirusStatus	授予权限以查询程序自动隔离查杀状态。	read	-	g:EnterpriseProjectId	hss:automaticKillMp:get
hss:container:getContainerNodeStatistics	授予权限以查询容器节点防护总览数据。	read	-	g:EnterpriseProjectId	hss:containers:list
hss:keyfile:getFileStatistic	授予权限以获取服务器文件统计信息。	read	-	g:EnterpriseProjectId	hss:keyfiles:list
hss:setting:getMalwareCollectStatus	授予权限以查询恶意软件云查样本收集配置开关状态。	read	-	g:EnterpriseProjectId	hss:automaticKillMp:get
hss:setting:getMalwareReminders	授予权限以获取提示信息配置。	read	-	g:EnterpriseProjectId	hss:automaticKillMp:get
hss:securitycheck:getManualSecurityCheckStatus	授予权限以查询手动体检状态和进度。	read	-	g:EnterpriseProjectId	hss:securitycheck:list
hss:overview:getOverviewAssetGroupsStatistics	授予权限以获取业务组分布统计，并识别一般资产、重要资产、核心资产。	read	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:getOverviewAssetOsStatistics	授予权限以获取操作系统分布统计。	read	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:getOverviewAssetStatistics	授予权限以获取资产统计，包含主机、容器、镜像。	read	-	g:EnterpriseProjectId	hss:overview:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:overview:getOverviewAttckMitre	授予权限以调查响应-ATT&CK 攻击路径矩阵。	read	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:getOverviewDefenseStatistics	授予权限以获取主动防御统计。	read	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:getOverviewProtectionStatusStatistics	授予权限以查询当前云负载的防护状态。	read	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:getOverviewQuotaStatistics	授予权限以获取主机安全统计。	read	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:getOverviewRiskLists	授予权限以查询风险列表。	read	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:getOverviewRiskManageStatistics	授予权限以获取风险管理，包含风险趋势和类型统计。	read	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:getOverviewRiskScore	授予权限以查询风险评分结果。	read	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:getOverviewRiskStatistics	授予权限以查询风险统计，安全风险、安全告警、主动防御。	read	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:getOverviewTrialsStatistics	授予权限以试用主机风险统计。	read	-	g:EnterpriseProjectId	hss:overview:list
hss:antiransomware:getRansomwareBackupInfoByBackupId	授予权限以查询指定备份信息。	read	-	g:EnterpriseProjectId	hss:antiransomware:list
hss:antiransomware:getRanso	授予权限以查询备份策略信	read	-	g:EnterpriseProjectId	hss:antiransomware:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
mwareHSSBackupPolicyInfo	息。				
hss:antiransomware:getRansomwareBackupStatistics	授予权限以查询备份统计信息。	read	-	g:EnterpriseProjectId	hss:antiransomware:list
hss:antiransomware:getRansomwareProtectionStatistics	授予权限以查询防护统计信息。	read	-	g:EnterpriseProjectId	hss:antiransomware:list
hss:antiransomware:getRansomwareVaultInfo	授予权限以查询备份存储库信息。	read	-	g:EnterpriseProjectId	hss:antiransomware:list
hss:rasp:getRaspPolicyDetail	授予权限以查询防护策略详情。	read	-	g:EnterpriseProjectId	hss:rasp:list
hss:rasp:getRaspProtectStatistics	授予权限以获取防护数据统计。	read	-	g:EnterpriseProjectId	hss:rasp:list
hss:wtp:getRaspSwitchStatus	授予权限以查询动态网页防篡改开启状态。	read	host *	g:EnterpriseProjectId	hss:wtpHosts:list
hss:securitycheck:getSecurityCheckConfig	授予权限以查询安全体检定时配置信息。	read	-	g:EnterpriseProjectId	hss:securitycheck:list
hss:securitycheck:getSecurityCheckHostReport	授予权限以查询指定服务器的安全体检报告。	read	host *	g:EnterpriseProjectId	hss:securitycheck:list
hss:securitycheck:getSecurityCheckOverview	授予权限以查询安全体检概览信息。	read	-	g:EnterpriseProjectId	hss:securitycheck:list
hss:securitycheck:getSecurityCheckStatistic	授予权限以查询安全体检统计信息。	read	-	g:EnterpriseProjectId	hss:securitycheck:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:safetyReport:getSecurityReport	授予权限以查询安全报告内容。	read	-	g:EnterpriseProjectId	hss:safetyReport:list
hss:safetyReport:getSecurityReportSubscription	授予权限以查询报告订阅的内容。	read	-	g:EnterpriseProjectId	hss:safetyReport:list
hss:wtp:getTimingOffStatusInfo	授予权限以查询定时关闭防护开关状态。	read	host *	g:EnterpriseProjectId	hss:wtpScheduledProtections:get
hss:wtp:getWtpDashboardProtectStatistics	授予权限以查询防护数据统计。	read	-	g:EnterpriseProjectId	hss:wtpDashboard:get
hss:wtp:getWtpDirectory	授予权限以查询动态网页防篡改的 Tomcat bin 目录。	read	host *	g:EnterpriseProjectId	hss:wtpDirectorys:list
hss:wtp:getWtpDirectoryMonitorOnlyStatus	授予权限以查询只监控不修复开关状态。	read	host *	g:EnterpriseProjectId	hss:wtpDirectorys:list
hss:wtp:getWtpPrivilegedProcessesChildStatus	授予权限以展示特权进程子进程可信状态。	read	host *	g:EnterpriseProjectId	hss:wtpPrivilegedProcesses:list
hss:wtp:getWtpRemoteBackupHostInfo	授予权限以查询远端备份服务器信息。	read	host *	g:EnterpriseProjectId	hss:wtpProtectMode:get
hss:setting:listAgentVersion	授予权限以查询 agent 版本信息列表。	list	-	g:EnterpriseProjectId	hss:installAgent:get
hss:container:listContainerNodes	授予权限以查询容器节点列表。	list	-	g:EnterpriseProjectId	hss:containers:list
hss:keyfile:listFileEvents	授予权限以获取变更文件列表。	list	-	g:EnterpriseProjectId	hss:keyfiles:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:keyfile:listFileHostEventDetails	授予权限以获取某个服务器变更文件信息。	list	host *	g:EnterpriseProjectId	hss:keyfiles:list
hss:keyfile:listFileHosts	授予权限以获取云服务器变更列表。	list	-	g:EnterpriseProjectId	hss:keyfiles:list
hss:host:listHostGroups	授予权限以查询服务器组列表。	list	-	g:EnterpriseProjectId	hss:hostGroup:get
hss:setting:listLoginCommonIp	授予权限以查询常用登录 IP 信息。	list	-	g:EnterpriseProjectId	hss:commonIPs:list
hss:setting:listLoginCommonLocation	授予权限以查询常用登录地信息。	list	-	g:EnterpriseProjectId	hss:commonLocations:list
hss:setting:listLoginWhiteIp	授予权限以查询登录 IP 白名单。	list	-	g:EnterpriseProjectId	hss:whiteIps:list
hss:policy:listPolicyGroup	授予权限以查询策略组列表。	list	-	g:EnterpriseProjectId	hss:policy:get
hss:asset:listPortHost	授予权限以查询资产指纹-端口-服务器列表。	list	-	g:EnterpriseProjectId	hss:ports:list
hss:asset:listProcessesHost	授予权限以查询资产指纹-进程-服务器列表。	list	-	g:EnterpriseProjectId	hss:processes:list
hss:ars:listPWLEvent	授予权限以查询进程白名单事件。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:ars:listPwlPolicy	授予权限以查询进程白名单策略列表。	list	-	g:EnterpriseProjectId	hss:ars:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:ars:listPwlPolicyHost	授予权限以查询进程白名单策略关联主机列表。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:ars:listPwlPolicyProcess	授予权限以查询进程白名单策略识别进程。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:antiransomware:listRansomwareBackedupByHostId	授予权限以查询备份列表。	list	host *	g:EnterpriseProjectId	hss:antiransomware:list
hss:antiransomware:listRansomwareOperationLogsByVaultName	授予权限以查询备份恢复任务列表。	list	-	g:EnterpriseProjectId	hss:antiransomware:list
hss:antiransomware:listRansomwareProtectionOptionalServer	授予权限以查询可选防护服务器列表。	list	-	g:EnterpriseProjectId	hss:antiransomware:list
hss:antiransomware:listRansomwareProtectionPolicy	授予权限以查询防护策略列表。	list	-	g:EnterpriseProjectId	hss:antiransomware:list
hss:antiransomware:listRansomwareProtectionServer	授予权限以查询勒索防护服务器列表。	list	-	g:EnterpriseProjectId	hss:antiransomware:list
hss:rasp:listRaspCheckFeatureRule	授予权限以查询检测规则列表。	list	-	g:EnterpriseProjectId	hss:rasp:list
hss:rasp:listRaspEvents	授予权限以查询应用防护事件列表。	list	-	g:EnterpriseProjectId	hss:rasp:list
hss:rasp:listRaspPolicies	授予权限以查询防护策略列表。	list	-	g:EnterpriseProjectId	hss:rasp:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:rasp:listRaspProtectionServers	授予权限以查询防护服务器列表。	list	-	g:EnterpriseProjectId	hss:rasp:list
hss:securitycheck:listSecurityCheckHostReportHistory	授予权限以查询指定服务器的安全体检历史报告列表。	list	host *	g:EnterpriseProjectId	hss:securitycheck:list
hss:securitycheck:listSecurityCheckHostResult	授予权限以查询多服务器的安全体检结果列表。	list	-	g:EnterpriseProjectId	hss:securitycheck:list
hss:safetyReport:listSecurityReport	授予权限以查询报告总览页列表。	list	-	g:EnterpriseProjectId	hss:safetyReport:list
hss:safetyReport:listSecurityReportHistoryPeriod	授予权限以查询历史报告统计周期列表。	list	-	g:EnterpriseProjectId	hss:safetyReport:list
hss:safetyReport:listSecurityReportSendingRecord	授予权限以查询报告发送记录列表。	list	-	g:EnterpriseProjectId	hss:safetyReport:list
hss:wtp:listTimingOffConfigInfo	授予权限以查询定时关闭防护配置列表。	list	host *	g:EnterpriseProjectId	hss:wtpScheduledProtections:get
hss:setting:listTwoFactorLoginHost	授予权限以查询双因子主机列表。	list	-	g:EnterpriseProjectId	hss:twofactorAuth:list
hss:wtp:listWtpBackupHostsInfo	授予权限以查询远端备份服务器。	list	-	g:EnterpriseProjectId	hss:wtpBackup:get
hss:wtp:listWtpHostProtectDirInfo	授予权限以查询主机防护目录。	list	host *	g:EnterpriseProjectId	hss:wtpDirectorys:list
hss:wtp:listWtpHostProtectHistoryInfo	授予权限以查询主机静态网页防篡改防护	list	-	g:EnterpriseProjectId	hss:wtpReports:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	动态。				
hss:wtp:listWtpHostRaspProtectHistoryInfo	授予权限以查询主机动态网页防篡改防护动态。	list	-	g:EnterpriseProjectId	hss:wtpReports:list
hss:wtp:listWtpPrivilegedProcessesInfo	授予权限以查询特权进程配置。	list	host *	g:EnterpriseProjectId	hss:wtpPrivilegedProcesses:list
hss:wtp:listWtpProtectHost	授予权限以查询防护列表。	list	-	g:EnterpriseProjectId	hss:wtpHosts:list
hss:setting:modifyLoginCommonIp	授予权限以添加、编辑或删除常用登录 IP 地址。	write	host *	g:EnterpriseProjectId	hss:commonIPs:set
hss:setting:modifyLoginCommonLocation	授予权限以添加、编辑或删除常用登录地。	write	host *	g:EnterpriseProjectId	hss:commonLocations:set
hss:setting:modifyLoginWhiteIp	授予权限以添加、编辑或删除登录 IP 白名单。	write	host *	g:EnterpriseProjectId	hss:whiteIps:set
hss:ars:operatePWLEvent	授予权限以处理事件。	write	-	g:EnterpriseProjectId	hss:ars:set
hss:ars:relearnPWLPolicy	授予权限以进行白名单策略重新学习。	write	host *	g:EnterpriseProjectId	hss:ars:set
hss:overview:resetOverviewRiskScore	授予权限以重置风险评分，重新体检。	write	-	g:EnterpriseProjectId	hss:overview:set
hss:antiransomware:restoreRansomwareDuplicationInfo	授予权限以备份恢复。	write	-	g:EnterpriseProjectId	hss:antiransomware:set
hss:safetyReport:sendSecurityReport	授予权限以发送安全报告。	write	-	g:EnterpriseProjectId	hss:safetyReport:set

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:setting:setAlarmConfig	授予权限以设置提示信息配置。	write	-	g:EnterpriseProjectId	hss:alertConfig:get
hss:setting:setMalwareReminders	授予权限以设置提示信息配置。	write	-	g:EnterpriseProjectId	hss:automaticKillMp:set
hss:wtp:setRemoteWtpBackupInfo	授予权限以开启关闭远端备份。	write	host *	g:EnterpriseProjectId	hss:wtpBackup:set
hss:wtp:setTimingOffSwitchInfo	授予权限以设置定时关闭防护开关状态。	write	host *	g:EnterpriseProjectId	hss:wtpScheduledProtections:set
hss:setting:setTwoFactorLoginConfig	授予权限以设置双因子登录配置。	write	host *	g:EnterpriseProjectId	hss:twofactorAuth:set
hss:wtp:setWtpDirectoryMonitorOnlyStatus	授予权限以设置只监控不修复开关状态。	write	host *	g:EnterpriseProjectId	hss:wtpDirectorys:set
hss:wtp:setWtpPrivilegedProcessesChildStatus	授予权限以设置特权进程子进程可信状态。	write	host *	g:EnterpriseProjectId	hss:wtpPrivilegedProcesses:list
hss:wtp:setWtpProtectionStatusInfo	授予权限以开启关闭网页防篡改防护。	write	host *	g:EnterpriseProjectId	hss:wtpProtect:switch
hss:wtp:setWtpProtectSwitch	授予权限以开启/关闭动态网页防篡改防护。	write	host *	g:EnterpriseProjectId	hss:wtpProtect:switch
hss:wtp:setWtpScheduledProtectionDateOffConfigInfo	授予权限以设置自动关闭防护的频率周期。	write	host *	g:EnterpriseProjectId	hss:wtpScheduledProtections:set
hss:securitycheck:startManualSecurityCheck	授予权限以启动手动体检。	write	-	g:EnterpriseProjectId	hss:securitycheck:set

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:antiransomware:startRansomwareBackupSingle	授予权限以开启单台服务器备份功能。	write	host *	g:EnterpriseProjectId	hss:antiransomware:set
hss:antiransomware:startRansomwareProtection	授予权限以开启勒索病毒防护。	write	host *	g:EnterpriseProjectId	hss:antiransomware:set
hss:antiransomware:startRansomwareProtectionSingle	授予权限以开启单台服务器勒索防护。	write	host *	g:EnterpriseProjectId	hss:antiransomware:set
hss:securitycheck:stopManualSecurityCheck	授予权限以取消手动体检。	write	-	g:EnterpriseProjectId	hss:securitycheck:set
hss:antiransomware:stopRansomwareProtection	授予权限以关闭勒索病毒防护。	write	host *	g:EnterpriseProjectId	hss:antiransomware:set
hss:container:switchContainerProtectStatus	授予权限以切换防护状态。	write	host *	g:EnterpriseProjectId	hss:containers:set
hss:ars:switchPWLPolicyHost	授予权限以开启/关闭主机白名单策略。	write	host *	g:EnterpriseProjectId	hss:ars:set
hss:rasp:switchRasp	授予权限以开启/关闭应用防护。	write	host *	g:EnterpriseProjectId	hss:rasp:set
hss:safetyReport:switchSecurityReportStatus	授予权限以修改安全报告开关。	write	-	g:EnterpriseProjectId	hss:safetyReport:set
hss:wtp:switchWtpHostProtectDirInfo	授予权限以开启/关闭目录防护。	write	host *	g:EnterpriseProjectId	hss:wtpDirectorys:set
hss:host:uninstallAgents	授予权限以卸载 Agent。	write	host *	g:EnterpriseProjectId	hss:agent:uninstall
hss:setting:updateAlarmConfig	授予权限以设置告警配置。	write	-	g:EnterpriseProjectId	hss:alertConfig:set

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:antiransomware:updateRansomwareBackupPolicyInfo	授予权限以修改备份策略。	write	-	g:EnterpriseProjectId	hss:antiransomware:set
hss:antiransomware:updateRansomwareProtectionPolicy	授予权限以修改防护策略。	write	-	g:EnterpriseProjectId	hss:antiransomware:set
hss:rasp:updateRaspPolicy	授予权限以修改防护策略。	write	-	g:EnterpriseProjectId	hss:rasp:set
hss:securitycheck:updateSecurityCheckConfig	授予权限以修改安全体检定时配置信息。	write	-	g:EnterpriseProjectId	hss:securitycheck:set
hss:wtp:updateTimingOffConfigInfo	授予权限以修改定时关闭防护配置。	write	host *	g:EnterpriseProjectId	hss:wtpScheduledProtections:set
hss:wtp:updateWtpBackupHostInfo	授予权限以添加或修改远端备份服务器。	write	host *	g:EnterpriseProjectId	hss:wtpBackup:set
hss:wtp:updateWtpDirectoryInfo	授予权限以修改动态网页防篡改的 Tomcat bin 目录。	write	host *	g:EnterpriseProjectId	hss:wtpDirectorys:set
hss:wtp:updateWtpHostProtectDirInfo	授予权限以修改防护目录。	write	host *	g:EnterpriseProjectId	hss:wtpDirectorys:set
hss:wtp:updateWtpPrivilegedProcessInfo	授予权限以修改特权进程。	write	host *	g:EnterpriseProjectId	hss:wtpPrivilegedProcess:set
hss:asset:addValuesLevel	授予权限以关联资产管理-主机管理-资产重要性。	write	host *	g:EnterpriseProjectId	hss:assets:set
hss:asset:batchModifyPortStatus	授予权限以修改端口状态。	write	host *	g:EnterpriseProjectId	hss:ports:operate
hss:asset:deleteToolCondition	授予权限以清除工具的搜索	write	-	g:EnterpriseProjectId	hss:assets:set

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
History	记录（运营工具）。				
hss:asset:executeTool	授予权限以工具执行搜索（运营工具）。	write	-	g:EnterpriseProjectId	hss:assets:set
hss:asset:getAccountTop	授予权限以获取资产管理-概览-账户 Top。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getAgentStatisticsStatus	授予权限以获取资产管理-概览-资产状态-主机 Agent 状态。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getAssetStatistic	授予权限以获取资产统计信息，账号、端口、进程等。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getAssetType	授予权限以获取资产管理-概览-资产状态-资产分布。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getAutoLaunchTop	授予权限以获取资产管理-概览-自启动项 Top。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getCommonPort	授予权限以呈现某一端口详细信息。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getContainerProtectionStatus	授予权限以获取资产管理-概览-资产状态-容器节点防护状态。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getCoreConfFileTop	授予权限以获取资产管理-概览-关键配置 Top。	read	-	g:EnterpriseProjectId	hss:assets:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:asset:getEnvironmentTop	授予权限以获取资产管理-概览-环境变量Top。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getHostAssetManualCollectStatus	授予权限以获取单主机资产指纹立即采集接口的运行状态。	read	host *	g:EnterpriseProjectId	hss:assets:list
hss:asset:getHostProtectionStatus	授予权限以获取资产管理-概览-资产状态-Agent 状态。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getJarPackageTop	授予权限以获取资产管理-概览-jar 包 Top。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getKernelModuleTop	授予权限以获取资产管理-概览-内核模块Top。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getOsStatisticsInfo	授予权限以获取资产管理-概览-资产状态-操作系统统计信息。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getPorcessTop	授予权限以获取资产管理-概览-进程 Top。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getPortTop	授予权限以获取资产管理-概览-端口 Top。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getQuotaStatisticsInfo	授予权限以获取资产管理-概览-资产状态-防护配额统计信息。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getSof	授予权限以获	read	-	g:EnterprisePro	hss:assets:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
twareTop	取资产管理-概览-软件 Top。			jectId	
hss:asset:getWebAppAndServiceTop	授予权限以获取资产管理-概览-WebAppAndServiceTop。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getWebAppTop	授予权限以获取资产管理-概览-Web 应用 Top。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getWebFrameworkTop	授予权限以获取资产管理-概览-Web 框架 Top。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getWebServiceTop	授予权限以获取资产管理-概览-Web 服务 Top。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:getWebSiteTop	授予权限以获取资产管理-概览-Web 站点 Top。	read	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listAppChangeHistories	授予权限以获取资产指纹-软件信息-历史变动记录。	list	-	g:EnterpriseProjectId	hss:softwares:list
hss:asset:listApps	授予权限以获取单主机资产指纹-软件。	list	-	g:EnterpriseProjectId	hss:softwares:list
hss:asset:listAppStatistics	授予权限以获取资产指纹-软件信息。	list	-	g:EnterpriseProjectId	hss:softwares:list
hss:asset:listAutoLaunchChangeHistories	授予权限以获取资产指纹-自启动项-历史变动记录。	list	-	g:EnterpriseProjectId	hss:assets:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:asset:listAutoLaunchs	授予权限以获取单主机资产指纹-自启动项。	list	-	g:EnterpriseProjectId	hss:launch:list
hss:asset:listAutoLaunchStatistics	授予权限以获取资产指纹-自启动项信息。	list	-	g:EnterpriseProjectId	hss:launch:list
hss:asset:listCoreConfFileHostInfo	授予权限以获取资产管理-资产指纹-系统关键配置文件的服务器列表。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listCoreConfFileInfo	授予权限以获取资产管理-主机管理-指纹类型-关键配置。	list	host *	g:EnterpriseProjectId	hss:assets:list
hss:asset:listCoreConfFileStatistics	授予权限以获取资产管理-资产指纹-系统关键配置文件左侧树。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listEnvironmentHostInfo	授予权限以获取资产管理-资产指纹-环境变量的服务器列表（资产指纹右侧服务器列表）。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listEnvironmentInfo	授予权限以获取资产管理-主机管理-指纹类型-环境变量。	list	host *	g:EnterpriseProjectId	hss:assets:list
hss:asset:listEnvironmentStatistics	授予权限以获取资产管理-资产指纹-环境变量文件左侧树。	list	-	g:EnterpriseProjectId	hss:assets:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:asset:listJarPackageHostInfo	授予权限以获取资产管理-资产指纹-Jar 包的服务器列表。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listJarPackageInfo	授予权限以获取资产管理-主机管理-指纹类型-Jar 包。	list	host *	g:EnterpriseProjectId	hss:assets:list
hss:asset:listJarPackageStatistics	授予权限以获取资产管理-资产指纹-Jar 包左侧树。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listKernelModuleHostInfo	授予权限以获取资产管理-资产指纹-内核模块的服务器列表。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listKernelModuleInfo	授予权限以获取资产管理-主机管理-指纹类型-内核模块。	list	host *	g:EnterpriseProjectId	hss:assets:list
hss:asset:listKernelModuleStatistics	授予权限以获取资产管理-资产指纹-内核模块左侧树。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listPorts	授予权限以获取单主机资产指纹-开放端口信息。	list	host *	g:EnterpriseProjectId	hss:ports:list
hss:asset:listPortStatistics	授予权限以获取资产指纹-开放端口信息。	list	-	g:EnterpriseProjectId	hss:ports:list
hss:asset:listProcesses	授予权限以获取进程列表。	list	host *	g:EnterpriseProjectId	hss:processes:list
hss:asset:listProcessStatistics	授予权限以获取资产指纹-进	list	-	g:EnterpriseProjectId	hss:processes:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	程信息。				
hss:asset:listResult	授予权限以获取执行结果（运营工具）。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listTool	授予权限以获取工具列表（运营工具）。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listToolConditionHistory	授予权限以获取工具的搜索记录（运营工具）。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listUserChangeHistories	授予权限以获取账户变动历史记录信息。	list	-	g:EnterpriseProjectId	hss:accounts:list
hss:asset:listUserGroup	授予权限以获取用户组列表。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listUsers	授予权限以获取资产的账号列表。	list	-	g:EnterpriseProjectId	hss:accounts:list
hss:asset:listUserStatistics	授予权限以获取资产指纹-账号信息。	list	-	g:EnterpriseProjectId	hss:accounts:list
hss:asset:listWebAppAndServices	授予权限以获取资产管理-资产指纹-右侧WebAppAndService 资产信息。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listWebAppAndServiceStatistics	授予权限以获取资产管理-资产指纹-左侧WebAppAndService 名称树信息。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listWebAppHostInfo	授予权限以获取资产管理-资	list	-	g:EnterpriseProjectId	hss:assets:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	产指纹-Web 应用的服务器列表。				
hss:asset:listWebAppInfo	授予权限以获取资产管理-主机管理-指纹类型-Web 应用。	list	host *	g:EnterpriseProjectId	hss:assets:list
hss:asset:listWebAppStatistics	授予权限以获取资产管理-资产指纹-Web 应用左侧树。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listWebFrameworkHostInfo	授予权限以获取资产管理-资产指纹-Web 框架的服务器列表。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listWebFrameworkInfo	授予权限以获取资产管理-主机管理-指纹类型-Web 框架。	list	host *	g:EnterpriseProjectId	hss:assets:list
hss:asset:listWebFrameworkStatistics	授予权限以获取资产管理-资产指纹-Web 框架左侧树。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listWebServiceHostInfo	授予权限以获取资产管理-资产指纹-Web 服务的服务器列表。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listWebServiceInfo	授予权限以获取资产管理-主机管理-指纹类型-Web 服务。	list	host *	g:EnterpriseProjectId	hss:assets:list
hss:asset:listWebServiceStatistics	授予权限以获取资产管理-资产指纹-Web 服务左侧树。	list	-	g:EnterpriseProjectId	hss:assets:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:asset:listWebSiteHostInfo	授予权限以获取资产管理-资产指纹-Web 站点的服务器列表。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:listWebSiteInfo	授予权限以获取资产管理-主机管理-指纹类型-Web 站点。	list	host *	g:EnterpriseProjectId	hss:assets:list
hss:asset:listWebSiteStatistics	授予权限以获取资产管理-资产指纹-Web 站点左侧树。	list	-	g:EnterpriseProjectId	hss:assets:list
hss:asset:runHostAssetManualCollect	授予权限以立即采集单主机资产指纹。	write	host *	g:EnterpriseProjectId	hss:assets:set
hss:baseline:addSecurityCheckPolicyGroup	授予权限以新建配置检测策略信息。	write	-	g:EnterpriseProjectId	hss:baselines:set
hss:baseline:changeCheckRuleState	授予权限以对未通过的配置检查项进行忽略/取消忽略/修复/验证操作。	write	baseline *	g:EnterpriseProjectId	hss:configDetects:operate
hss:baseline:deleteSecurityCheckPolicyGroup	授予权限以删除指定配置检测策略信息。	write	-	g:EnterpriseProjectId	hss:baselines:set
hss:baseline:exportSecurityCheckReport	授予权限以按查询结果导出配置检测报告。	list	-	g:EnterpriseProjectId	hss:configDetects:list
hss:baseline:getBaselineOverview	授予权限以查询基线检查的统计数据信息。	read	-	g:EnterpriseProjectId	hss:baselines:list
hss:baseline:get	授予权限以查	read	-	g:EnterprisePro	hss:baselines:lis

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
BaselineScanStatus	询基线检查任务进度。			jectId	t
hss:baseline:getBaselineStatistic	授予权限以查询基线检查的统计数据信息，包括弱口令，口令复杂度，配置检测。	read	-	g:EnterpriseProjectId	hss:baselines:list
hss:baseline:getCheckRuleDetail	授予权限以查询配置检查项检测报告。	read	baseline *	g:EnterpriseProjectId	hss:configDetects:list
hss:baseline:getCheckRuleFixFailDetail	授予权限以查询检查项修复失败原因。	read	baseline *	g:EnterpriseProjectId	hss:baselines:list
hss:baseline:getDefaultSecurityCheckPolicy	授予权限以查询配置检测策略的默认基线信息。	read	-	g:EnterpriseProjectId	hss:baselines:list
hss:baseline:getDefaultSecurityCheckPolicyDetails	授予权限以查询基线的详细检查项。	read	-	g:EnterpriseProjectId	hss:baselines:list
hss:baseline:getRiskConfigDetail	授予权限以查询指定安全配置项的检查结果。	read	-	g:EnterpriseProjectId	hss:configDetects:list
hss:baseline:listCheckRuleHost	授予权限以查询配置检查项影响到的服务器列表。	list	baseline *	g:EnterpriseProjectId	hss:baselines:list
hss:baseline:listPasswordComplexity	授予权限以查询口令复杂度策略检测报告。	list	-	g:EnterpriseProjectId	hss:complexityPolicys:list
hss:baseline:listRiskConfigCheckRules	授予权限以查询指定安全配置项的检查项	list	-	g:EnterpriseProjectId	hss:configDetects:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	列表。				
hss:baseline:listRiskConfigHosts	授予权限以查询指定安全配置项的受影响服务器列表。	list	-	g:EnterpriseProjectId	hss:riskConfigHost:list
hss:baseline:listRiskConfigs	授予权限以查询租户的服务器安全配置检测结果列表。	list	-	g:EnterpriseProjectId	hss:configDetects:list
hss:baseline:listSecurityCheckPolicyGroup	授予权限以查询配置检测策略组列表。	list	-	g:EnterpriseProjectId	hss:baselines:list
hss:baseline:listWeakPasswordUsers	授予权限以查询弱口令检测结果列表。	list	-	g:EnterpriseProjectId	hss:weakPwds:list
hss:baseline:runBaselineDetect	授予权限以手动检测：对策略中选择的主机，进行配置检测和弱口令检测。	write	-	g:EnterpriseProjectId	hss:baselines:set
hss:baseline:updateSecurityCheckPolicyGroup	授予权限以修改指定配置检测策略信息。	write	-	g:EnterpriseProjectId	hss:baselines:set
hss:event:addLoginWhiteList	授予权限以添加登录白名单。	write	-	g:EnterpriseProjectId	hss:event:set
hss:event:batchChangeEvent	授予权限以批量处理告警事件。	write	-	g:EnterpriseProjectId	hss:event:set
hss:event:changeEvent	授予权限以处理告警事件。	write	event *	g:EnterpriseProjectId	hss:event:set
hss:event:changeIsolatedFile	授予权限以恢复已隔离文件。	write	host *	g:EnterpriseProjectId	hss:event:set
hss:event:expor	授予权限以导	list	-	g:EnterprisePro	hss:event:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
tAlarmWhiteList	出告警白名单。			jectId	
hss:event:exportEmergency	授予权限以导出应急恶意程序接口。	list	-	g:EnterpriseProjectId	hss:event:set
hss:event:getEmergencyStatistics	授予权限以获取应急事件统计信息。	read	-	g:EnterpriseProjectId	hss:event:get
hss:event:getEventAttackTag	授予权限以查询攻击标识分布统计列表。	read	-	g:EnterpriseProjectId	hss:event:get
hss:event:getEventSeverity	授予权限以查询威胁等级统计列表。	read	-	g:EnterpriseProjectId	hss:event:get
hss:event:getEventStatistics	授予权限以查询告警事件统计。	read	-	g:EnterpriseProjectId	hss:event:get
hss:event:getMalwareInfo	授予权限以获取突发恶意程序详情列表。	read	event *	g:EnterpriseProjectId	hss:event:get
hss:event:handleMalwareEvent	授予权限以处理恶意程序。	write	event *	g:EnterpriseProjectId	hss:event:set
hss:event:importAlarmWhiteList	授予权限以导入告警白名单。	write	-	g:EnterpriseProjectId	hss:event:set
hss:event:isolateOperateEmergency	授予权限以开启或关闭隔离箱。	write	-	g:EnterpriseProjectId	hss:event:set
hss:event:listAlarmWhiteList	授予权限以查询告警白名单列表。	list	-	g:EnterpriseProjectId	hss:event:get
hss:event:listBlockedIp	授予权限以查询已拦截 IP 列表。	list	-	g:EnterpriseProjectId	hss:accountCracks:list
hss:event:listEv	授予权限以查	list	-	g:EnterprisePro	hss:event:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
entOperates	询事件支持的处理类型。			jectId	
hss:event:listEventTopRisk	授予权限以查询 TOP10 事件类型统计列表。	list	-	g:EnterpriseProjectId	hss:event:get
hss:event:listEventType	授予权限以查询事件类型统计列表。	list	-	g:EnterpriseProjectId	hss:event:get
hss:event:listFileIsolateList	授予权限以获取突发恶意程序隔离文件列表。	list	-	g:EnterpriseProjectId	hss:event:get
hss:event:listIsolatedFile	授予权限以查询已隔离文件列表。	list	-	g:EnterpriseProjectId	hss:event:get
hss:event:listLoginWhiteList	授予权限以查询登录白名单列表。	list	-	g:EnterpriseProjectId	hss:event:get
hss:event:listMalware	授予权限以获取突发恶意程序事件列表。	list	-	g:EnterpriseProjectId	hss:event:get
hss:event:listSecurityEvents	授予权限以查入侵事件列表。	list	-	g:EnterpriseProjectId	hss:event:get
hss:event:recoverIsolateFile	授予权限以恢复文件隔离箱。	write	-	g:EnterpriseProjectId	hss:event:set
hss:event:removeAlarmWhiteList	授予权限以删除告警白名单。	write	-	g:EnterpriseProjectId	hss:event:set
hss:event:removeLoginWhiteList	授予权限以删除登录白名单。	write	-	g:EnterpriseProjectId	hss:event:set
hss:host:associateHostAssetVal	授予权限以关联资产重要	write	host *	g:EnterpriseProjectId	hss:hosts:set

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ue	性。				
hss:host:associateHostsGroup	授予权限以分配到组。	write	host *	g:EnterpriseProjectId	hss:hostGroup:set
hss:host:batchInstallAgent	授予权限以批量安装 agent。	write	host *	g:EnterpriseProjectId	hss:hosts:set
hss:host:changeHostsGroup	授予权限以编辑服务器组。	write	-	g:EnterpriseProjectId	hss:hostGroup:set
hss:host:deleteHostsGroup	授予权限以删除服务器组。	write	-	g:EnterpriseProjectId	hss:hostGroup:set
hss:host:getHostsStatistics	授予权限以统计服务器数据。	read	-	g:EnterpriseProjectId	hss:hosts:list
hss:host:listFirewallStatus	授予权限以查询主机是否开启防火墙。	read	host *	g:EnterpriseProjectId	hss:hosts:list
hss:host:listHostGroupAssetValue	授予权限以查询资产重要性的服务器组列表。	list	-	g:EnterpriseProjectId	hss:hosts:list
hss:host:listHostsRisk	授予权限以获取 ECS 风险状况。	read	host *	g:EnterpriseProjectId	hss:hosts:list
hss:host:listHostStatus	授予权限以查询云服务器列表。	list	-	g:EnterpriseProjectId	hss:hosts:list
hss:host:listHostsUpgrade	授予权限以获取主机的升级状态。	read	host *	-	hss:hosts:list
			-	g:EnterpriseProjectId	
hss:host:manualCheckVul	授予权限以手动检测漏洞。	write	-	g:EnterpriseProjectId	hss:hosts:manualDetect
hss:host:switchFirewallStatus	授予权限以修改防火墙授权状态。	write	host *	g:EnterpriseProjectId	hss:hosts:switchVersion
hss:host:switchHostsProtectSta	授予权限以切	write	host *	g:EnterprisePro	hss:hosts:switch

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
tus	换防护状态。			jectId	Version
hss:host:upgradeAgent	授予权限以升级 Agent1.0 到 2.0。	write	host * -	- g:EnterpriseProjectId	hss:hosts:switchVersion
hss:host:upgradeAgents	授予权限以升级 Agent。	write	host *	g:EnterpriseProjectId	hss:hosts:set
hss:image:batchScanLocalImage	授予权限以进行本地镜像扫描。	write	-	g:EnterpriseProjectId	hss:images:set
hss:image:batchScanPrivateImage	授予权限以批量扫描私有镜像仓库镜像。	write	-	g:EnterpriseProjectId	hss:images:set
hss:image:getImageFilesStat	授予权限以查询镜像文件统计信息。	read	-	g:EnterpriseProjectId	hss:images:list
hss:image:getImageLocalVulOverview	授予权限以查询本地漏洞概览信息。	read	-	g:EnterpriseProjectId	hss:images:list
hss:image:getImageVulOverview	授予权限以查询仓库漏洞概览信息。	read	-	g:EnterpriseProjectId	hss:images:list
hss:image:listCfgCheckAffectedImage	授予权限以查询租户镜像未通过基线项所影响的镜像列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listGlobalCfgCheck	授予权限以查询租户全量配置检测统计结果。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listGlobalMalware	授予权限以查询租户恶意文件列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listGlobalVul	授予权限以查询租户的漏洞	list	-	g:EnterpriseProjectId	hss:images:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	信息。				
hss:image:listImageApps	授予权限以查询镜像软件列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listImageAppVul	授予权限以查询软件漏洞列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listImageCfgCheck	授予权限以查询单个镜像的配置基线检测结果。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listImageFiles	授予权限以查询镜像无归属文件列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listImageLocal	授予权限以查询本地镜像列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listImageMalware	授予权限以查询镜像恶意文件列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listImageNamespace	授予权限以查询镜像 namespace 信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listImageRepository	授予权限以查询私有镜像仓库镜像列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listImageVul	授予权限以查询镜像的漏洞信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listInstanceImageVul	授予权限以查询企业镜像的漏洞信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listLocalImageApp	授予权限以查询本地镜像软件列表。	list	-	g:EnterpriseProjectId	hss:images:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:image:listLocalImageAppVuls	授予权限以查询本地镜像某软件的软件漏洞列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listLocalImageContainers	授予权限以查询本地镜像的容器信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listLocalImageHosts	授予权限以查询本地镜像的主机信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listLocalImageMalware	授予权限以查询本地镜像的恶意文件信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listLocalImageVuls	授予权限以查询本地镜像的漏洞信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listLocalVulRepoImage	授予权限以查询本地镜像漏洞影响的镜像和容器信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listPrivateImageRepository	授予权限以查询私有镜像仓库镜像列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listSharedImageRepository	授予权限以查询共享镜像仓库镜像列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listVulCve	授予权限以查询漏洞对应 cve 信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listVulRepoImage	授予权限以查询单个漏洞影响的镜像仓库中的镜像信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:runI	授予权限以扫	write	-	g:EnterprisePro	hss:images:set

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
mageScan	描镜像。			jectId	
hss:image:runImageSynchronizeTask	授予权限以从SWR服务同步自由镜像列表。	write	-	g:EnterpriseProjectId	hss:images:set
hss:image:runSwrImageScan	授予权限以更新并扫描SWR镜像,提供swr访问。	write	-	g:EnterpriseProjectId	hss:images:set
hss:image:sharedImageSynchronization	授予权限以从swr更新他人共享镜像。	write	-	g:EnterpriseProjectId	hss:images:set
hss:policy:addPolicyGroup	授予权限以复制主机策略组。	write	policy *	g:EnterpriseProjectId	hss:policy:set
hss:policy:associatePolicyGroup	授予权限以部署策略。	write	policy *	g:EnterpriseProjectId	hss:policy:set
			host *	g:EnterpriseProjectId	
hss:policy:changePolicyDetail	授予权限以修改策略内容。	write	policy *	g:EnterpriseProjectId	hss:policy:set
hss:policy:changePolicyGroup	授予权限以修改策略组相关内容。	write	policy *	g:EnterpriseProjectId	hss:policy:set
hss:policy:deletePolicyGroup	授予权限以删除策略组。	write	policy *	g:EnterpriseProjectId	hss:policy:set
hss:policy:getPolicyDetail	授予权限以查询指定策略详细信息。	read	policy *	g:EnterpriseProjectId	hss:policy:get
hss:policy:listPolicyGroupDetail	授予权限以查询策略组策略信息列表。	list	policy *	g:EnterpriseProjectId	hss:policy:get
hss:quota:addResourceInstanceTag	授予权限以单个资源添加资源标签。	tagging	-	• g:RequestTag/<tag-key> • g:TagKeys	hss:quotas:set

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:quota:batchCreateTags	授予权限以批量创建标签。	write	-	• g:RequestTag/<tag-key> • g:TagKeys	hss:quotas:set
hss:quota:batchDeleteTags	授予权限以批量删除标签。	write	-	• g:RequestTag/<tag-key> • g:TagKeys	hss:quotas:set
hss:quota:cancelHostsQuota	授予权限以解绑配额。	write	-	-	hss:quotas:set
hss:quota:changeTmsResourceTagInfo	授予权限以批量添加删除资源标签。	write	-	• g:RequestTag/<tag-key> • g:TagKeys	hss:quotas:set
hss:quota:countResourceInstances	授予权限以通过标签过滤购买的资源数量。	list	-	• g:RequestTag/<tag-key> • g:TagKeys	hss:quotas:set
hss:quota:dealOrder	授予权限以订购 HSS。	write	-	-	hss:quotas:set
hss:quota:deleteResourceInstanceTag	授予权限以删除单个资源下的标签。	tagging	-	• g:RequestTag/<tag-key> • g:TagKeys	hss:quotas:set
hss:quota:filterResourceInstanceList	授予权限以通过标签过滤购买的资源列表。	list	-	• g:RequestTag/<tag-key> • g:TagKeys	hss:quotas:set
hss:quota:getResourceInstanceTag	授予权限以查询单个资源的资源标签。	read	-	-	hss:quotas:get
hss:quota:getResourceQuotas	授予权限以查询配额信息。	read	-	-	hss:quotas:get
hss:quota:getTmsResourceTagsInfo	授予权限以查询资源标签。	read	-	-	hss:quotas:get
hss:quota:listProjectTags	授予权限以查询租户当前项目下所有用过的标签。	list	-	-	hss:quotas:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:quota:listQuotasDetail	授予权限以查询配额详情。	list	-	-	hss:quotas:get
hss:quota:listResourceIds	授予权限以批量查询配额 ID 信息。	list	-	-	hss:quotas:get
hss:quota:listTmsResourceInstancesInfo	授予权限以查询资源实例。	list	-	• g:RequestTag/<tag-key> • g:TagKeys	hss:quotas:get
hss:quota:upgradeOrder	授予权限以变更规格。	write	-	-	hss:quotas:set
hss:vulnerability:changeVulStatus	授予权限以修改漏洞的状态。	write	host *	g:EnterpriseProjectId	hss:vuls:set
hss:vulnerability:exportEmergencyVulnerabilities	授予权限以导出应急漏洞。	list	-	g:EnterpriseProjectId	hss:vuls:set
hss:vulnerability:exportVulsList	授予权限以导出漏洞及漏洞影响的主机的相关信息。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:getCmsVulDetail	授予权限以查询 webcms 漏洞基本信息。	read	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:getEmergencySummary	授予权限以查询应急事件总览。	read	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:getEmergencyVulDetail	授予权限以查询应急事件漏洞详情。	read	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:getLinuxVulDetail	授予权限以查询 linux 漏洞基本信息。	read	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:getVulCheckStatus	授予权限以查询主机漏洞的扫描状态。	read	-	g:EnterpriseProjectId	hss:manualDetectStatus:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:vulnerability:getVulSummary	授予权限以查询漏洞统计信息。	read	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:getWindosVulDetail	授予权限以查询 windows 漏洞基本信息。	read	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:getWindowsVulNum	授予权限以查询主机 windows 漏洞的数量。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listEmergencyVul	授予权限以查询应急事件漏洞。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listHostVuls	授予权限以查询单台服务器漏洞信息。	list	host *	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listHostVulSummary	授予权限以查询服务器统计信息和风险服务器 TOP5。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listTopVulSummary	授予权限以查询漏洞 TOP5。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listVulHosts	授予权限以查询单个漏洞影响的云服务器信息。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listVulnerabilities	授予权限以查询漏洞列表。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listVulRepairFailedDetail	授予权限以查询漏洞修复失败信息。	list	host *	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listVulTypeSummary	授予权限以查询漏洞类型分布。	list	-	g:EnterpriseProjectId	hss:vuls:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:vulnerability:operateEmergency	授予权限以操作应急事件漏洞。	write	-	g:EnterpriseProjectId	hss:vuls:set
hss:host:getScanStatus	授予权限以查询手动检测状态。	read	host *	g:EnterpriseProjectId	hss:hostGroup:get
hss:host:setManualDetect	授予权限以下发手动检测。	write	host *	g:EnterpriseProjectId	hss:hosts:manualDetect
hss::getTrustServiceStatus	授予权限以获取可信服务状态。	read	-	-	-
hss::enableTrustService	授予权限以开启可信服务。	permission_management	-	-	-
hss::validateAdmin	授予权限以校验当前账号是否是管理员账号（包含组织管理员和委托管理员）。	tagging	-	-	-
hss::listAccounts	授予权限以展示多账号列表。	list	-	-	-
hss::batchAddAccounts	授予权限以批量添加账号。	write	-	-	-
hss::deleteAccount	授予权限以删除账号。	write	-	-	-
hss::listOrganizationTree	授予权限以展示多账号树形结构。	list	-	-	-
hss::listDelegatedAccounts	授予权限以查询已委托账号树形结构。	list	-	-	-
hss:antiransomware:listBackup	授予权限以查询备份存储库	list	-	g:EnterpriseProjectId	hss:antiransomware:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
Vaults	列表。				
hss:antiransomware:listRansomwareProtectionNodes	授予权限以查询勒索防护服务器列表。	list	-	g:EnterpriseProjectId	hss:antiransomware:list
hss:antiransomware:getBackupsStatistics	授予权限以查询备份统计信息。	list	-	g:EnterpriseProjectId	hss:antiransomware:list
hss:antiransomware:startSingleBackup	授予权限以开启单台服务器备份功能。	write	host *	-	hss:antiransomware:set
			-	g:EnterpriseProjectId	
hss:antiransomware:getBackupPolicyInfo	授予权限以查询单个备份策略信息。	read	-	g:EnterpriseProjectId	hss:antiransomware:list
hss:hostGroup:getOutsideGroupStatus	授予权限以查询是否支持创建数据中心服务器组。	read	-	g:EnterpriseProjectId	hss:hostGroup:get
hss:hostGroup:getOutsideHostGroup	授予权限以查询线下数据中心服务器组。	read	-	g:EnterpriseProjectId	hss:hostGroup:get
hss:hostGroup:addOutsideHostGroup	授予权限以创建线下数据中心服务器组。	write	-	g:EnterpriseProjectId	hss:hostGroup:set
hss:hostGroup:changeOutsideHostGroup	授予权限以编辑线下数据中心服务器组。	write	-	g:EnterpriseProjectId	hss:hostGroup:set
hss:images:listImageTag	授予权限以查询镜像 tag 版本列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:images:listImageSensitive	授予权限以查询镜像的敏感信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:images:getFilePathWhiteDetail	授予权限以查询镜像的敏感信息文件路径	read	-	g:EnterpriseProjectId	hss:images:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	白名单。				
hss:images:changeFilePathWhiteDetail	授予权限以修改镜像的敏感信息文件路径白名单。	write	-	g:EnterpriseProjectId	hss:images:set
hss:images:changeSensitiveInfo	授予权限以操作处理敏感信息。	write	-	g:EnterpriseProjectId	hss:images:set
hss:event:listTopEventType	授予权限以查询 TOP5 事件类型统计列表。	list	-	g:EnterpriseProjectId	hss:event:get
hss:vulnerability:getVulScanPolicy	授予权限以查询漏洞扫描策略。	read	-	-	hss:vuls:list
hss:vulnerability:changeVulScanPolicy	授予权限以修改漏洞扫描策略。	write	host *	-	hss:vuls:set
hss:vulnerability:listVulWhiteList	授予权限以查询漏洞白名单列表。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:getVulWhiteListDetail	授予权限以查询漏洞白名单详情。	read	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:changeVulWhiteList	授予权限以修改漏洞白名单。	write	host *	-	hss:vuls:set
			-	g:EnterpriseProjectId	
hss:vulnerability:deleteVulWhiteList	授予权限以删除漏洞白名单。	write	-	-	hss:vuls:set
hss:vulnerability:addVulWhiteList	授予权限以添加漏洞白名单。	write	host *	-	hss:vuls:set
			-	g:EnterpriseProjectId	
hss:vulnerability:listVulWhite	授予权限以查询添加白名单	list	-	-	hss:vuls:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ListVulOptions	时的漏洞选项。				
hss:vulnerability:listVulScanTask	授予权限以查询漏洞扫描任务列表。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listVulScanTaskHost	授予权限以查询漏洞扫描任务对应的主机列表。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:rescanVulScanTask	授予权限以重新扫描之前漏洞扫描任务中的主机。	write	host *	-	hss:vuls:set
			-	g:EnterpriseProjectId	
hss:vulnerability:getVulScanTaskStatistics	授予权限以查询漏洞扫描任务的统计数据。	read	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listHostVulStatistics	授予权限以查询漏洞管理统计数据。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listVulHostApps	授予权限以查询漏洞受影响服务器详情-软件列表。	list	host *	-	hss:vuls:list
			-	g:EnterpriseProjectId	
hss:vulnerability:listVulHostProcess	授予权限以查询漏洞受影响服务器详情-进程列表。	list	host *	-	hss:vuls:list
			-	g:EnterpriseProjectId	
hss:vulnerability:listVulHandleHistory	授予权限以查询漏洞历史处置记录。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listVulHostHosts	授予权限以查询漏洞主机列表。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listVulHostVuls	授予权限以查询紧急修复/未完成修复漏	list	-	g:EnterpriseProjectId	hss:vuls:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	洞。				
hss:vulnerability:listVulHostHandleVuls	授予权限以查询今日处理漏洞/累计处理漏洞。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:image:listImageNonCompliantApp	授予权限以查询镜像的不合规软件信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:batchExportSWRVulList	授予权限以swr 镜像仓库漏洞批量导出。	write	-	g:EnterpriseProjectId	hss:images:set
hss:image:batchExportLocalVulList	授予权限以本地镜像漏洞批量导出。	write	-	g:EnterpriseProjectId	hss:images:set
hss:image:getExtendedWeakPassword	授予权限以查询镜像的自定义弱口令。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:changeExtendedWeakPassword	授予权限以修改镜像的自定义弱口令。	write	-	g:EnterpriseProjectId	hss:images:set
hss:image:listImageBasicImage	授予权限以查询镜像的基础镜像信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listImagePwdComplexity	授予权限以查询镜像口令复杂度策略检测报告。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listImageWeakPwdUsers	授予权限以查询镜像弱口令检测结果列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listImageRiskConfigs	授予权限以查询镜像安全配置检测结果列表。	list	-	g:EnterpriseProjectId	hss:images:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:image:listImageRiskConfigCheckRules	授予权限以查询镜像指定安全配置项的检查项列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:getImageRiskConfigDetail	授予权限以查询镜像指定安全配置项的检查结果。	read	-	g:EnterpriseProjectId	hss:images:list
hss:image:getImageCheckRuleDetail	授予权限以查询镜像配置检查项检测报告。	read	-	g:EnterpriseProjectId	hss:images:list
hss:image:getImageBaselineStatistic	授予权限以查询基线检查的统计数据信息，包括弱口令，口令复杂度，配置检测。	read	-	g:EnterpriseProjectId	hss:images:list
hss:event:addSystemUserWhiteList	授予权限以添加系统用户白名单。	write	-	g:EnterpriseProjectId	hss:event:set
hss:event:updateSystemUserWhiteList	授予权限以修改系统用户白名单。	write	-	g:EnterpriseProjectId	hss:event:set
hss:event:listSystemUserWhiteList	授予权限以查询系统用户白名单。	list	-	g:EnterpriseProjectId	hss:event:get
hss:event:removeSystemUserWhiteList	授予权限以删除系统用户白名单。	write	-	g:EnterpriseProjectId	hss:event:set
hss:container:saveClusters	授予权限以同步集群信息。	write	-	g:EnterpriseProjectId	hss:containers:set
hss:container:listClusterInfo	授予权限以查询 Kubernetes 集群列表。	list	-	g:EnterpriseProjectId	hss:containers:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:container:listPodInfo	授予权限以查询 pod 基本信息列表。	list	-	g:EnterpriseProjectId	hss:containers:list
hss:container:showPodDetail	授予权限以查询 pod 详细信息。	read	-	g:EnterpriseProjectId	hss:containers:list
hss:container:listContainerInfo	授予权限以查询容器基本信息列表。	list	-	g:EnterpriseProjectId	hss:containers:list
hss:container:showContainerDetail	授予权限以查询容器详细信息。	list	-	g:EnterpriseProjectId	hss:containers:list
hss:container:listServiceInfo	授予权限以查询 Kubernetes 服务列表。	list	-	g:EnterpriseProjectId	hss:containers:list
hss:container:showServiceDetail	授予权限以查询 Kubernetes 服务详情。	read	-	g:EnterpriseProjectId	hss:containers:list
hss:container:listEndpointInfo	授予权限以查询 kubernetes 端点列表。	list	-	g:EnterpriseProjectId	hss:containers:list
hss:container:showEndpointDetail	授予权限以查询 Kubernetes 端点详情。	read	-	g:EnterpriseProjectId	hss:containers:list
hss:container:listDeployments	授予权限以查询 Kubernetes 无状态负载列表。	list	-	g:EnterpriseProjectId	hss:containers:list
hss:container:listStatefulSets	授予权限以查询 Kubernetes 有状态负载列表。	list	-	g:EnterpriseProjectId	hss:containers:list
hss:container:listDaemonSets	授予权限以查询 Kubernetes 守护进程列表。	list	-	g:EnterpriseProjectId	hss:containers:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:container:listJobs	授予权限以查询 kubernetes 普通任务列表。	list	-	g:EnterpriseProjectId	hss:containers:list
hss:container:listCronJobs	授予权限以查询 Kubernetes 定时任务列表。	list	-	g:EnterpriseProjectId	hss:containers:list
hss:vulnerability:showVulAffectedStatics	授予权限以统计漏洞受影响服务器数量。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listVulHandleTask	授予权限以查询漏洞处置任务列表。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listVulHandleTaskDetail	授予权限以查询漏洞处置任务的详情列表。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:container:isolateK8sContainer	授予权限以修改容器的运行状态。	write	-	g:EnterpriseProjectId	hss:containers:set
hss:container:getNetworkStatistics	授予权限以查询容器防火墙统计状态。	list	-	g:EnterpriseProjectId	hss:container-network:list
hss:container:getClusters	授予权限以查询集群列表。	list	-	g:EnterpriseProjectId	hss:container-network:list
hss:container:getClusterNetworkInfo	授予权限以查询集群网络信息。	read	-	g:EnterpriseProjectId	hss:container-network:read
hss:container:getClusterPolicyList	授予权限以查询容器网络策略列表。	list	-	g:EnterpriseProjectId	hss:container-network:list
hss:container:deletePolicy	授予权限以删除容器网络策略。	write	-	g:EnterpriseProjectId	hss:clusterProtect:delete
hss:container:cr	授予权限以创	write	-	g:EnterprisePro	hss:container-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
eatePolicy	建容器网络策略。			jectId	network:set
hss:container:updatePolicy	授予权限以更新容器网络策略。	write	-	g:EnterpriseProjectId	hss:container-network:set
hss:container:syncClusterPolicyList	授予权限以同步容器网络策略。	read	-	g:EnterpriseProjectId	hss:container-network:read
hss:container:syncClusterList	授予权限以同步集群命名空间信息。	read	-	g:EnterpriseProjectId	hss:container-network:read
hss:container:getNamespaceList	授予权限以查询集群命名空间列表。	list	-	g:EnterpriseProjectId	hss:container-network:list
hss:container:getNodeList	授予权限以查询集群节点列表。	list	-	g:EnterpriseProjectId	hss:container-network:list
hss:container:syncClusterNodeList	授予权限以同步集群节点。	read	-	g:EnterpriseProjectId	hss:container-network:read
hss:vulnerability:getVulScanTaskEstimatedTime	授予权限以查询漏洞扫描的预估时间。	read	-	g:EnterpriseProjectId	hss:vuls:list
hss:antiransomware:addRansomwareProtectionPolicy	授予权限以添加勒索防护策略。	write	-	g:EnterpriseProjectId	hss:antiransomware:set
hss:antiransomware:associateBackupPolicy	授予权限以将备份策略绑定存储库。	write	-	g:EnterpriseProjectId	hss:antiransomware:set
hss:antiransomware:listBackupPolicy	授予权限以查询备份策略列表。	list	-	g:EnterpriseProjectId	hss:antiransomware:list
hss:antiransomware:associateProtectionPolicy	授予权限以切换勒索防护策略。	write	-	g:EnterpriseProjectId	hss:antiransomware:set

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:antiransomware:batchStartProtection	授予权限以开启勒索防护。	write	-	g:EnterpriseProjectId	hss:antiransomware:set
hss:event:getEventAttCk	授予权限以查询 ATT&CK 攻击阶段统计列表。	list	event *	-	hss:event:get
			-	g:EnterpriseProjectId	
hss:event:downloadEventSourceFile	授予权限以下载告警源文件。	list	event *	-	hss:event:get
			-	g:EnterpriseProjectId	
hss:overview:showSecurityScore	授予权限以查询安全评分。	list	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:listSecurityRisk	授予权限以查询安全风险列表。	list	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:showQuotaHostStatistics	授予权限以查询主机配额统计信息。	list	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:showAgentStatistics	授予权限以查询 agent 待升级，在线离线数量。	list	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:showHotInformation	授予权限以查询热点资讯。	list	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:showSecurityRisk	授予权限以查询安全风险信息。	list	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:showProtectStatistics	授予权限以查询守护天数，病毒库更新时间，漏洞库更新时间，各模块累计次数。	list	-	g:EnterpriseProjectId	hss:overview:list
hss:overview:sh	授予权限以查	list	-	g:EnterprisePro	hss:overview:lis

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
owStatistics	询勒索病毒防治开启数量，应用防护开启数量，网页防篡改开启数量，双因子认证开启数量，支持双因子认证开启数量，隔离文件数量。			jectId	t
hss:event:listEventHandleHistory	授予权限以查询历史事件处置列表。	list	event *	-	hss:event:get
			-	g:EnterpriseProjectId	
hss:image:listSwrImageRepository	授予权限以查询 swr 镜像仓库镜像列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:batchScanSwrImage	授予权限以镜像仓库镜像批量扫描。	write	-	g:EnterpriseProjectId	hss:images:set
hss:image:vulnerabilities	授予权限以查询镜像的漏洞信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listVulnerabilityCve	授予权限以漏洞对应 cve 信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listImageRiskConfigRules	授予权限以查询镜像指定安全配置项的检查项列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:runImageSynchronize	授予权限以从 SWR 服务同步镜像列表。	write	-	g:EnterpriseProjectId	hss:images:set
hss:event:listEventForensic	授予权限以查询事件取证信息。	list	event *	-	hss:event:get
			-	g:EnterprisePro	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				jectId	
hss:event:listSimilarHandledEvents	授予权限以查询相似已处置的告警记录。	list	event *	-	hss:event:get
			-	g:EnterpriseProjectId	
hss:event:listSameEvent	授予权限以查询相同告警。	list	event *	-	hss:event:get
			-	g:EnterpriseProjectId	
hss:container:getPolicies	授予权限以查询策略列表。	list	-	g:EnterpriseProjectId	hss:clusterProtect:list
hss:container:getPolicyDetail	授予权限以查询策略详情。	list	-	g:EnterpriseProjectId	hss:clusterProtect:list
hss:container:getOverview	授予权限以查询集群防护总览。	list	-	g:EnterpriseProjectId	hss:clusterProtect:list
hss:container:getProtectEvents	授予权限以查询集群防护事件。	list	-	g:EnterpriseProjectId	hss:clusterProtect:list
hss:container:getProtectClusters	授予权限以查询集群防护信息。	list	-	g:EnterpriseProjectId	hss:clusterProtect:list
hss:container:changeProtectStatus	授予权限以改变集群防护状态。	write	-	g:EnterpriseProjectId	hss:clusterProtect:list
hss:container:addWhiteImage	授予权限以加入镜像白名单。	write	-	g:EnterpriseProjectId	hss:clusterProtect:set
hss:container:listDefaultPolicy	授予权限以查询默认策略模板。	list	-	g:EnterpriseProjectId	hss:clusterProtect:list
hss:container:listProtectionItem	授予权限以查询防护范围。	list	-	g:EnterpriseProjectId	hss:clusterProtect:list
hss:vulnerability:getVulBacku	授予权限以查询漏洞处理对	read	-	g:EnterpriseProjectId	hss:vuls:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
pStatistics	应主机的备份相关统计信息。				
hss:vulnerability:ListVulHostVaults	授予权限以查询漏洞处理对应的主机存储库的列表。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:ListVulHostBackups	授予权限以查询可回滚的备份列表。	list	host *	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:RestoreVulHostBackup	授予权限以用备份进行回滚。	write	-	g:EnterpriseProjectId	hss:vuls:set
hss:event:exportEvent	授予权限以导出事件告警。	write	event *	-	hss:event:set
			-	g:EnterpriseProjectId	
hss:event:queryExportTask	授予权限以查询导出事件告警任务。	read	event *	-	hss:event:get
			-	g:EnterpriseProjectId	
hss:event:downloadEvent	授予权限以下载事件告警。	read	event *	-	hss:event:get
			-	g:EnterpriseProjectId	
hss:ars:createAppWhitelistPolicy	授予权限以创建应用进程白名单策略。	write	host *	-	hss:ars:set
			-	g:EnterpriseProjectId	
hss:ars:listAppWhitelistPolicy	授予权限以查询应用进程白名单策略列表。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:ars:changeAppWhitelistPolicy	授予权限以修改应用进程白名单策略。	write	host *	-	hss:ars:set
			-	g:EnterpriseProjectId	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:ars:deleteAppWhitelistPolicy	授予权限以删除应用进程白名单策略。	write	-	g:EnterpriseProjectId	hss:ars:set
hss:ars:showAppWhitelistPolicy	授予权限以查询应用进程白名单策略信息。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:ars:switchAppWhitelistPolicyHost	授予权限以修改应用进程白名单策略防护状态。	write	host *	-	hss:ars:set
			-	g:EnterpriseProjectId	
hss:ars:addAppWhitelistPolicyHost	授予权限以添加主机到应用进程白名单策略。	write	host *	-	hss:ars:set
			-	g:EnterpriseProjectId	
hss:ars:listAppWhitelistPolicyHost	授予权限以查询应用进程白名单策略的主机列表。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:ars:deleteAppWhitelistPolicyHost	授予权限以删除应用进程白名单策略的主机。	write	host *	-	hss:ars:set
			-	g:EnterpriseProjectId	
hss:ars:listAppWhitelistHostStatus	授予权限以查询应用进程白名单策略的可选服务器列表。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:ars:listAppWhitelistPolicyProcess	授予权限以查询应用进程白名单策略的进程列表。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:ars:changeAppWhitelistPolicyProcessStatus	授予权限以修改应用进程白名单策略的进程可信状态。	write	-	g:EnterpriseProjectId	hss:ars:set
hss:ars:addApp	授予权限以添	write	host *	-	hss:ars:set

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
WhitelistPolicyProcess	加进程到应用进程白名单策略。		-	g:EnterpriseProjectId	
hss:ars:listAppWhitelistPolicyProcessExtend	授予权限以查询应用进程白名单策略的进程扩展列表。	list	host *	-	hss:ars:list
			-	g:EnterpriseProjectId	
hss:ars:exportAppWhitelistPolicyProcess	授予权限以导出应用进程白名单策略的进程列表。	list	host *	-	hss:ars:list
			-	g:EnterpriseProjectId	
hss:ars:switchAppWhitelistPolicyLearnStatus	授予权限以修改应用进程白名单策略学习状态。	write	host *	-	hss:ars:set
			-	g:EnterpriseProjectId	
hss:ars:showAppWhitelistAgentStatics	授予权限以查询不支持应用进程控制功能的旗舰版主机数量。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:ars:listAppWhitelistEvent	授予权限以查询应用进程控制的可疑进程事件列表。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:container:deleteSelfBuildK8sClusterDaemonsetInfo	授予权限以删除询自建集群daemonset。	write	-	g:EnterpriseProjectId	hss:containers:set
hss:container:saveSelfBuildK8sClusterDaemonsetInfo	授予权限以保存自建集群daemonset。	write	-	g:EnterpriseProjectId	hss:containers:set
hss:container:showSelfBuildK8sClusterDaemonsetInfo	授予权限以查询自建集群daemonset。	read	-	g:EnterpriseProjectId	hss:containers:get
hss:container:listSelfBuildK8sClusterInfo	授予权限以查询自建Kubernetes 集	list	-	g:EnterpriseProjectId	hss:containers:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	群列表。				
hss:container:createDaemonset	授予权限以创建 CCE 集群 daemonset。	write	-	g:EnterpriseProjectId	hss:containers:set
hss:vulnerability:listVulRepairCmds	授予权限以查询漏洞修复命令。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:listUrgentVulnerabilities	授予权限以查询应急漏洞列表。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:antivirus:createAntivirusTask	授予权限以创建病毒查杀任务。	write	host *	-	hss:ars:set
			-	g:EnterpriseProjectId	
hss:antivirus:listAntivirusTask	授予权限以查询病毒查杀任务列表。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:antivirus:switchAntivirusTask	授予权限以取消病毒查杀任务。	write	host *	-	hss:ars:set
			-	g:EnterpriseProjectId	
hss:antivirus:listAntivirusHost	授予权限以查询病毒查杀可选服务器列表。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:antivirus:createAntivirusPolicy	授予权限以创建自定义查杀策略。	write	host *	-	hss:ars:set
			-	g:EnterpriseProjectId	
hss:antivirus:listAntivirusPolicy	授予权限以查询自定义查杀策略列表。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:antivirus:listAntivirusResult	授予权限以查询病毒查杀结果列表。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:antivirus:operateAntivirusResult	授予权限以处置病毒查杀结果。	write	-	g:EnterpriseProjectId	hss:ars:set

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
hss:antivirus:exportAntivirusResult	授予权限以导出病毒查杀结果。	write	-	g:EnterpriseProjectId	hss:ars:set
hss:antivirus:showAntivirusStatistic	授予权限以查询病毒查杀统计信息。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:image:showImageFullScanProgress	授予权限以查询镜像全量扫描进展。	list	-	g:EnterpriseProjectId	hss:images:list
hss:host:changeHostIgnoreStatus	授予权限以忽略或取消忽略主机。	write	host *	-	hss:hosts:set
			-	g:EnterpriseProjectId	
hss:host:listIgnoreHosts	授予权限以查询已忽略主机。	list	host *	-	hss:hosts:list
			-	g:EnterpriseProjectId	
hss:image:batchExportBaselineTask	授予权限以导出镜像基线检查结果。	write	-	g:EnterpriseProjectId	hss:images:set
hss:image:showImageSecurityReportStatistic	授予权限以查询镜像安全报告导出统计。	write	-	g:EnterpriseProjectId	hss:images:set
hss:vulnerability:exportVuls	授予权限以创建漏洞导出任务。	write	-	g:EnterpriseProjectId	hss:vuls:set
hss:exportTask:queryExportTask	授予权限以查询导出任务。	list	-	g:EnterpriseProjectId	hss:keyfiles:list
hss:file:downloadExportedFile	授予权限以下载文件。	list	-	g:EnterpriseProjectId	hss:keyfiles:list
hss:image:listGlobalVulnerabilities	授予权限以查询租户的漏洞信息。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listVulnerabilityImages	授予权限以查询单个漏洞影响的镜像仓库	list	-	g:EnterpriseProjectId	hss:images:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	中的镜像信息。				
hss:setting:getPluginInstallScript	授予权限以查询服务器安装的插件信息。	list	-	g:EnterpriseProjectId	hss:installAgent:get
hss:setting:getPluginList	授予权限以查询插件安装指南信息。	list	-	g:EnterpriseProjectId	hss:installAgent:get
hss:setting:getAutoOpenQuotaStatus	授予权限以查询自动绑定配额开关状态。	read	-	g:EnterpriseProjectId	hss:hosts:list
hss:setting:changeAutoOpenQuotaStatus	授予权限以修改自动绑定配额开关状态。	write	-	g:EnterpriseProjectId	hss:hosts:list
hss:image:batchExportSWRVulTask	授予权限以导出 swr 镜像漏洞结果。	write	-	g:EnterpriseProjectId	hss:images:list
hss:image:batchExportLocalVulTask	授予权限以导出本地镜像漏洞结果。	write	-	g:EnterpriseProjectId	hss:images:list
hss:vulnerability:exportVulReport	授予权限以导出 html 格式的漏洞报告。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:getVulReportData	授予权限以获取 pdf 漏洞报告的数据。	list	-	g:EnterpriseProjectId	hss:vuls:list
hss:setting:getAgentAutoUpgradeStatus	授予权限以查询 agent 自动升级开关状态。	read	-	g:EnterpriseProjectId	hss:hosts:list
hss:setting:changeAgentAutoUpgradeStatus	授予权限以修改 agent 自动升级开关状态。	write	-	g:EnterpriseProjectId	hss:hosts:list
hss:quota:showProductdataOff	授予权限以查询商品信息。	list	-	g:EnterpriseProjectId	hss:quotas:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
eringInfos					
hss:image:listLocalImageAppInfo	授予权限以查询本地镜像软件列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:image:listLocalImageAppVulnerabilities	授予权限以查询本地镜像单个软件漏洞列表。	list	-	g:EnterpriseProjectId	hss:images:list
hss:antiransomware:getRansomwareProtectionStatus	授予权限以查询勒索防护状态。	list	-	g:EnterpriseProjectId	hss:antiransomware:list
hss:antiransomware:getAutoDeployAgentList	授予权限以查询自动开启勒索防护的主机。	list	-	-	hss:antiransomware:list
hss:antiransomware:updateAutoDeployAgent	授予权限以更新自动开启勒索防护的主机。	write	-	-	hss:antiransomware:set
hss:vulnerability:getVulIndividualStatistics	授予权限以查询漏洞指定统计数据。	read	-	g:EnterpriseProjectId	hss:vuls:list
hss:vulnerability:getVulAffectInfo	授予权限以查询漏洞影响的主机信息或主机下的漏洞信息。	read	-	g:EnterpriseProjectId	hss:vuls:list
hss:event:deleteIsolatedFile	授予权限以删除隔离箱文件。	write	host *	-	hss:event:set
			-	g:EnterpriseProjectId	
hss:antivirus:listAntivirusHandleHistory	授予权限以查询病毒查杀历史处置记录。	list	-	g:EnterpriseProjectId	hss:ars:list
hss:decoyport:showStatistics	授予权限以查看端口蜜罐防护的统计信	read	-	g:EnterpriseProjectId	hss:decoyport:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	息。				
hss:decoyport:showAutoBind	授予权限以查看端口蜜罐的自动绑定状态。	read	-	g:EnterpriseProjectId	hss:decoyport:get
hss:decoyport:switchAutoBind	授予权限以修改端口蜜罐的自动绑定状态。	write	-	g:EnterpriseProjectId	hss:decoyport:set
hss:decoyport:showHostList	授予权限以查看端口蜜罐策略的防护主机列表。	list	-	g:EnterpriseProjectId	hss:decoyport:get
hss:decoyport:listPolicy	授予权限以查看端口蜜罐的策略列表。	list	-	g:EnterpriseProjectId	hss:decoyport:get
hss:decoyport:listAvailableHost	授予权限以查看支持开启端口蜜罐的主机列表。	list	-	g:EnterpriseProjectId	hss:decoyport:get
hss:decoyport:switchHostPolicy	授予权限以切换主机的端口蜜罐防护策略。	write	-	g:EnterpriseProjectId	hss:decoyport:set
hss:decoyport:deleteHostPolicy	授予权限以关闭主机的端口蜜罐防护策略。	write	-	g:EnterpriseProjectId	hss:decoyport:set
hss:decoyport:createPolicy	授予权限以新增端口蜜罐策略。	write	-	g:EnterpriseProjectId	hss:decoyport:set
hss:decoyport:modifyPolicy	授予权限以编辑端口蜜罐防护策略。	write	-	g:EnterpriseProjectId	hss:decoyport:set
hss:decoyport:showPolicyDetails	授予权限以查看端口蜜罐策	read	-	g:EnterpriseProjectId	hss:decoyport:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	略详情。				
hss:decoyport:deletePolicy	授予权限以删除端口蜜罐策略。	write	-	g:EnterpriseProjectId	hss:decoyport:set
hss:decoyport:switchPolicy	授予权限以启用或关闭端口蜜罐策略。	write	-	g:EnterpriseProjectId	hss:decoyport:set
hss:exportTask:queryLatestExportTaskByType	授予权限以查询最近导出任务。	read	-	g:EnterpriseProjectId	hss:keyfiles:list
hss:container:createSecurityGroupPolicy	授予权限以创建安全组策略。	write	-	g:EnterpriseProjectId	hss:container-network:set
hss:container:updateSecurityGroupPolicy	授予权限以更新安全组策略。	write	-	g:EnterpriseProjectId	hss:container-network:set
hss:container:getSecurityGroupPolicyList	授予权限以查询安全组策略列表。	list	-	g:EnterpriseProjectId	hss:container-network:list
hss:container:deleteSecurityGroupPolicy	授予权限以删除安全组策略。	write	-	g:EnterpriseProjectId	hss:container-network:set
hss:container:syncSecurityGroupPolicy	授予权限以同步集群下安全组策略。	read	-	g:EnterpriseProjectId	hss:container-network:read
hss:container:getWorkloadList	授予权限以查询工作负载列表。	list	-	g:EnterpriseProjectId	hss:container-network:list
hss:container:getSecurityGroupList	授予权限以查询安全组列表。	list	-	g:EnterpriseProjectId	hss:container-network:list

HSS 的 API 通常对应着一个或多个授权项。表 3-159 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

 版权所有 © 华为云计算技术有限公司

表3-159 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v5/{project_id}/host-management/groups	hss:host:addHostsGroup	eps:enterpriseProjects:list
PUT /v5/{project_id}/pwl/{policy_id}/host	hss:ars:addPWLPolicyHost	eps:enterpriseProjects:list
POST /v5/{project_id}/rasp/policy	hss:rasp:addRaspPolicy	eps:enterpriseProjects:list
POST /v5/{project_id}/report/security-report	hss:safetyReport:addSecurityReport	eps:enterpriseProjects:list
POST /v5/{project_id}/wtp/{host_id}/timing-off-config	hss:wtp:addTimingOffConfigInfo	eps:enterpriseProjects:list
POST /v5/{project_id}/wtp/{host_id}/protect-directories	hss:wtp:addWtpHostProtectDirInfo	eps:enterpriseProjects:list
POST /v5/{project_id}/wtp/{host_id}/privileged-process	hss:wtp:addWtpPrivilegedProcessInfo	eps:enterpriseProjects:list
POST /v5/{project_id}/setting/virus-kill	hss:setting:changeAutoKillVirusStatus	eps:enterpriseProjects:list
PUT /v5/{project_id}/event/blocked-ip	hss:event:changeBlockedIp	eps:enterpriseProjects:list
PUT /v5/{project_id}/setting/malware/collect	hss:setting:changeMalwareCollectStatus	eps:enterpriseProjects:list
POST /v5/{project_id}/pwl/policy	hss:ars:changePWLPolicy	eps:enterpriseProjects:list
POST /v5/{project_id}/pwl/{policy_id}/process	hss:ars:changePWLPolicyProcessStatus	eps:enterpriseProjects:list
PUT /v5/{project_id}/report/security-report	hss:safetyReport:changeSecurityReport	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v5/{project_id}/pwl/policy	hss:ars:createPWLPolicy	eps:enterpriseProjects:list
DELETE /v5/{project_id}/pwl/policy	hss:ars:deletePWLPolicy	eps:enterpriseProjects:list
DELETE /v5/{project_id}/pwl/{policy_id}/host	hss:ars:deletePWLPolicyHost	eps:enterpriseProjects:list
DELETE /v5/{project_id}/ransomware/duplication/{backup_id}	hss:antiransomware:deleteRansomwareDuplicationInfo	eps:enterpriseProjects:list
DELETE /v5/{project_id}/ransomware/protection/policy	hss:antiransomware:deleteRansomwareProtectionPolicy	eps:enterpriseProjects:list
DELETE /v5/{project_id}/rasp/policy	hss:rasp:deleteRaspPolicy	eps:enterpriseProjects:list
DELETE /v5/{project_id}/report/security-report	hss:safetyReport:deleteSecurityReport	eps:enterpriseProjects:list
DELETE /v5/{project_id}/wtp/{host_id}/timing-off-config	hss:wtp:deleteTimingOffConfigInfo	eps:enterpriseProjects:list
DELETE /v5/{project_id}/wtp/{host_id}/protect-directories	hss:wtp:deleteWtpHostProtectDirInfo	eps:enterpriseProjects:list
DELETE /v5/{project_id}/wtp/{host_id}/privileged-process	hss:wtp:deleteWtpPrivilegedProcessInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/setting/agent-install-script	hss:setting:getAgentInstallScript	eps:enterpriseProjects:list
GET /v5/{project_id}/setting/alarm-config	hss:setting:getAlarmConfig	eps:enterpriseProjects:list
GET /v5/{project_id}/rasp/{host_id}/status	hss:rasp:getAppRaspSwitchStatus	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/setting/virus-kill	hss:setting:getAutoKillVirusStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/container/node-statistics	hss:container:getContainerNodeStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/files/statistic	hss:keyfile:getFileStatistic	eps:enterpriseProjects:list
GET /v5/{project_id}/setting/malware/collect	hss:setting:getMalwareCollectStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/setting/malware/reminders	hss:setting:getMalwareReminders	eps:enterpriseProjects:list
GET /v5/{project_id}/security-check/manual-check/status	hss:securitycheck:getManualSecurityCheckStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/overview/asset/groups/statistics	hss:overview:getOverviewAssetGroupsStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/overview/asset/os/statistics	hss:overview:getOverviewAssetOsStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/overview/asset/statistics	hss:overview:getOverviewAssetStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/overview/risk/attck-mitre	hss:overview:getOverviewAttckMitre	eps:enterpriseProjects:list
GET /v5/{project_id}/overview/risk/defense/statistics	hss:overview:getOverviewDefenseStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/overview/risk/protection/statistics	hss:overview:getOverviewProtectionStatusStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/overview/quota/statistics	hss:overview:getOverviewQuotaStatistics	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/overview/risk/lists	hss:overview:getOverviewRiskLists	eps:enterpriseProjects:list
GET /v5/{project_id}/overview/risk/manage/statistics	hss:overview:getOverviewRiskManageStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/overview/risk/score	hss:overview:getOverviewRiskScore	eps:enterpriseProjects:list
GET /v5/{project_id}/overview/risk/event/statistics	hss:overview:getOverviewRiskStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/overview/trial/statistic	hss:overview:getOverviewTrialsStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/ransomware/backup/{backup_id}/detail	hss:antiransomware:getRansomwareBackupInfoByBackupId	eps:enterpriseProjects:list
GET /v5/{project_id}/backup/policy	hss:antiransomware:getRansomwareHSSBackupPolicyInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/ransomware/statistics/backup	hss:antiransomware:getRansomwareBackupStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/ransomware/statistics/protection	hss:antiransomware:getRansomwareProtectionStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/ransomware/backup/vault	hss:antiransomware:getRansomwareVaultInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/rasp/policy/detail	hss:rasp:getRaspPolicyDetail	eps:enterpriseProjects:list
GET /v5/{project_id}/rasp/statistics	hss:rasp:getRaspProtectStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/wtp/{host_id}/rasp/status	hss:wtp:getRaspSwitchStatus	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/security-check/config	hss:securitycheck:getSecurityCheckConfig	eps:enterpriseProjects:list
GET /v5/{project_id}/security-check/host-report/{host_id}	hss:securitycheck:getSecurityCheckHostReport	eps:enterpriseProjects:list
GET /v5/{project_id}/security-check/overview	hss:securitycheck:getSecurityCheckOverview	eps:enterpriseProjects:list
GET /v5/{project_id}/security-check/statistic	hss:securitycheck:getSecurityCheckStatistic	eps:enterpriseProjects:list
GET /v5/{project_id}/report/security-report	hss:safetyReport:getSecurityReport	eps:enterpriseProjects:list
GET /v5/{project_id}/report/report-subscription	hss:safetyReport:getSecurityReportSubscription	eps:enterpriseProjects:list
GET /v5/{project_id}/wtp/{host_id}/timing-off/status	hss:wtp:getTimingOffStatusInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/wtp/statistics	hss:wtp:getWtpDashboardProtectStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/wtp/{host_id}/rasp_path	hss:wtp:getWtpDirectory	eps:enterpriseProjects:list
GET /v5/{project_id}/wtp/{host_id}/monitor-only/status	hss:wtp:getWtpDirectoryMonitorOnlyStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/webtamper/static/{host_id}/privileged-child/status	hss:wtp:getWtpPrivilegedProcessesChildStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/wtp/{host_id}/backup-host	hss:wtp:getWtpRemoteBackupHostInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/setting/agent-version	hss:setting:listAgentVersion	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/container/nodes	hss:container:listContainerNodes	eps:enterpriseProjects:list
GET /v5/{project_id}/files/change-files	hss:keyfile:listFileEvents	eps:enterpriseProjects:list
GET /v5/{project_id}/{host_id}/files/change-files	hss:keyfile:listFileHostEventDetails	eps:enterpriseProjects:list
GET /v5/{project_id}/files/change-host	hss:keyfile:listFileHosts	eps:enterpriseProjects:list
GET /v5/{project_id}/host-management/groups	hss:host:listHostGroups	eps:enterpriseProjects:list
GET /v5/{project_id}/setting/login-common-ip	hss:setting:listLoginCommonIp	eps:enterpriseProjects:list
GET /v5/{project_id}/setting/login-common-location	hss:setting:listLoginCommonLocation	eps:enterpriseProjects:list
GET /v5/{project_id}/setting/login-white-ip	hss:setting:listLoginWhiteIp	eps:enterpriseProjects:list
GET /v5/{project_id}/policy/groups	hss:policy:listPolicyGroup	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/ports/detail	hss:asset:listPortHost	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/processes/detail	hss:asset:listProcessesHost	eps:enterpriseProjects:list
GET /v5/{project_id}/pwl/event	hss:ars:listPWLEvent	eps:enterpriseProjects:list
GET /v5/{project_id}/pwl/policy	hss:ars:listPwlPolicy	eps:enterpriseProjects:list
GET /v5/{project_id}/pwl/{policy_id}/host	hss:ars:listPwlPolicyHost	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/pwl/{policy_id}/process	hss:ars:listPwlPolicyProcess	eps:enterpriseProjects:list
GET /v5/{project_id}/ransomware/backup/{host_id}	hss:antiransomware:listRansomwareBackedupByHostId	eps:enterpriseProjects:list
GET /v5/{project_id}/ransomware/backup/operation-logs	hss:antiransomware:listRansomwareOperationLogsByVaultName	eps:enterpriseProjects:list
GET /v5/{project_id}/ransomware/optional/server	hss:antiransomware:listRansomwareProtectionOptionalServer	eps:enterpriseProjects:list
GET /v5/{project_id}/ransomware/protection/policy	hss:antiransomware:listRansomwareProtectionPolicy	eps:enterpriseProjects:list
GET /v5/{project_id}/ransomware/server	hss:antiransomware:listRansomwareProtectionServer	eps:enterpriseProjects:list
GET /v5/{project_id}/rasp/rule	hss:rasp:listRaspCheckFeatureRule	eps:enterpriseProjects:list
GET /v5/{project_id}/rasp/events	hss:rasp:listRaspEvents	eps:enterpriseProjects:list
GET /v5/{project_id}/rasp/policies	hss:rasp:listRaspPolicies	eps:enterpriseProjects:list
GET /v5/{project_id}/rasp/servers	hss:rasp:listRaspProtectionServers	eps:enterpriseProjects:list
GET /v5/{project_id}/security-check/host-report/history/{host_id}	hss:securitycheck:listSecurityCheckHostReportHistory	eps:enterpriseProjects:list
GET /v5/{project_id}/security-check/host-results	hss:securitycheck:listSecurityCheckHostResult	eps:enterpriseProjects:list
GET /v5/{project_id}/report/report-list	hss:safetyReport:listSecurityReport	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/report/period-list	hss:safetyReport:listSecurityReportHistoryPeriod	eps:enterpriseProjects:list
GET /v5/{project_id}/report/sending-list	hss:safetyReport:listSecurityReportSendingRecord	eps:enterpriseProjects:list
GET /v5/{project_id}/wtp/{host_id}/timing-off-config	hss:wtp:listTimingOffConfigInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/setting/two-factor-login/hosts	hss:setting:listTwoFactorLoginHost	eps:enterpriseProjects:list
GET /v5/{project_id}/wtp/backup-hosts	hss:wtp:listWtpBackupHostsInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/wtp/{host_id}/protect-directories	hss:wtp:listWtpHostProtectDirInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/webtamper/static/protect-history	hss:wtp:listWtpHostProtectHistoryInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/webtamper/rasp/protect-history	hss:wtp:listWtpHostRaspProtectHistoryInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/wtp/{host_id}/privileged-process	hss:wtp:listWtpPrivilegedProcessesInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/webtamper/hosts	hss:wtp:listWtpProtectHost	• eps:enterpriseProjects:list • vpc:ports:list
POST /v5/{project_id}/setting/login-common-ip	hss:setting:modifyLoginCommonIp	eps:enterpriseProjects:list
POST /v5/{project_id}/setting/login-common-location	hss:setting:modifyLoginCommonLocation	eps:enterpriseProjects:list
POST	hss:setting:modifyLoginWhiteI	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v5/{project_id}/setting/login-white-ip	p	
POST /v5/{project_id}/pwl/event/operate	hss:ars:operatePWLEvent	eps:enterpriseProjects:list
POST /v5/{project_id}/pwl/{policy_id}/relearn	hss:ars:relearnPWLPolicy	eps:enterpriseProjects:list
PUT /v5/{project_id}/overview/risk/score	hss:overview:resetOverviewRiskScore	eps:enterpriseProjects:list
POST /v5/{project_id}/ransomware/duplication/{backup_id}/restore	hss:antiransomware:restoreRansomwareDuplicationInfo	eps:enterpriseProjects:list
POST /v5/{project_id}/report/sending	hss:safetyReport:sendSecurityReport	eps:enterpriseProjects:list
PUT /v5/{project_id}/setting/reminders-config	hss:setting:setAlarmConfig	eps:enterpriseProjects:list
PUT /v5/{project_id}/setting/malware/reminders	hss:setting:setMalwareReminders	eps:enterpriseProjects:list
POST /v5/{project_id}/wtp/{host_id}/set-remote-backup	hss:wtp:setRemoteWtpBackupInfo	eps:enterpriseProjects:list
POST /v5/{project_id}/wtp/{host_id}/timing-off/status	hss:wtp:setTimingOffSwitchInfo	eps:enterpriseProjects:list
PUT /v5/{project_id}/setting/two-factor-login/config	hss:setting:setTwoFactorLoginConfig	eps:enterpriseProjects:list
POST /v5/{project_id}/wtp/{host_id}/monitor-only/status	hss:wtp:setWtpDirectoryMonitorOnlyStatus	eps:enterpriseProjects:list
POST /v5/{project_id}/webtamper/static/{host_id}/privileged-child/status	hss:wtp:setWtpPrivilegedProcessesChildStatus	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v5/{project_id}/webtamper/static/status	hss:wtp:setWtpProtectionStatusInfo	eps:enterpriseProjects:list
POST /v5/{project_id}/webtamper/rasp/status	hss:wtp:setWtpProtectSwitch	eps:enterpriseProjects:list
PUT /v5/{project_id}/wtp/{host_id}/date-off-config	hss:wtp:setWtpScheduledProtectionDateOffConfigInfo	eps:enterpriseProjects:list
POST /v5/{project_id}/security-check/manual-check/start	hss:securitycheck:startManualSecurityCheck	eps:enterpriseProjects:list
POST /v5/{project_id}/ransomware/backup/open/{host_id}	hss:antiransomware:startRansomwareBackupSingle	eps:enterpriseProjects:list
POST /v5/{project_id}/ransomware/protection/open	hss:antiransomware:startRansomwareProtection	eps:enterpriseProjects:list
POST /v5/{project_id}/ransomware/protection/open/{host_id}	hss:antiransomware:startRansomwareProtectionSingle	eps:enterpriseProjects:list
POST /v5/{project_id}/security-check/manual-check/stop	hss:securitycheck:stopManualSecurityCheck	eps:enterpriseProjects:list
POST /v5/{project_id}/ransomware/protection/close	hss:antiransomware:stopRansomwareProtection	eps:enterpriseProjects:list
POST /v5/{project_id}/container/switch-version	hss:container:switchContainerProtectStatus	eps:enterpriseProjects:list
POST /v5/{project_id}/pwl/{policy_id}/host	hss:ars:switchPWLPolicyHost	eps:enterpriseProjects:list
PUT /v5/{project_id}/rasp/status	hss:rasp:switchRasp	eps:enterpriseProjects:list
POST /v5/{project_id}/report	hss:safetyReport:switchSecurityReportStatus	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/report-status		
POST /v5/{project_id}/wtp/{host_id}/protect-directories/status	hss:wtp:switchWtpHostProtectDirInfo	eps:enterpriseProjects:list
POST /v5/{project_id}/host-management/uninstall	hss:host:uninstallAgents	eps:enterpriseProjects:list
PUT /v5/{project_id}/setting/alarm-config	hss:setting:updateAlarmConfig	eps:enterpriseProjects:list
PUT /v5/{project_id}/backup/policy	hss:antiransomware:updateRansomwareBackupPolicyInfo	eps:enterpriseProjects:list
PUT /v5/{project_id}/ransomware/protection/policy	hss:antiransomware:updateRansomwareProtectionPolicy	eps:enterpriseProjects:list
PUT /v5/{project_id}/rasp/policy	hss:rasp:updateRaspPolicy	eps:enterpriseProjects:list
POST /v5/{project_id}/security-check/config	hss:securitycheck:updateSecurityCheckConfig	eps:enterpriseProjects:list
PUT /v5/{project_id}/wtp/{host_id}/timing-off-config	hss:wtp:updateTimingOffConfigInfo	eps:enterpriseProjects:list
PUT /v5/{project_id}/wtp/backup-hosts	hss:wtp:updateWtpBackupHostInfo	eps:enterpriseProjects:list
PUT /v5/{project_id}/wtp/{host_id}/rasp_path	hss:wtp:updateWtpDirectoryInfo	eps:enterpriseProjects:list
PUT /v5/{project_id}/wtp/{host_id}/protect-directories	hss:wtp:updateWtpHostProtectDirInfo	eps:enterpriseProjects:list
PUT /v5/{project_id}/wtp/{host_id}/privileged-process	hss:wtp:updateWtpPrivilegedProcessInfo	eps:enterpriseProjects:list
POST /v5/{project_id}/asset/	hss:asset:addValuesLevel	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
values/host		
POST /v5/{project_id}/asset/batch-modify-port-status	hss:asset:batchModifyPortStatus	eps:enterpriseProjects:list
DELETE /v5/{project_id}/investigation/tool/condition-history	hss:asset:deleteToolConditionHistory	eps:enterpriseProjects:list
POST /v5/{project_id}/investigation/tool/execute	hss:asset:executeTool	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/statistics/top/account	hss:asset:getAccountTop	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/status/agent	hss:asset:getAgentStatisticsStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/statistics	hss:asset:getAssetStatistic	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/status/type	hss:asset:getAssetType	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/statistics/top/auto-launch	hss:asset:getAutoLaunchTop	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/common-port-info	hss:asset:getCommonPort	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/status/container/protection	hss:asset:getContainerProtectionStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/statistics/top/core-conf-file	hss:asset:getCoreConfFileTop	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/statistics/top/environment	hss:asset:getEnvironmentTop	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/asset/manual-collect/{type}	hss:asset:getHostAssetManualCollectStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/status/host/protection	hss:asset:getHostProtectionStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/statistics/top/jar-package	hss:asset:getJarPackageTop	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/statistics/top/kernel-module	hss:asset:getKernelModuleTop	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/status/os	hss:asset:getOsStatisticsInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/statistics/top/process	hss:asset:getPorcessTop	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/statistics/top/port	hss:asset:getPortTop	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/status/quota	hss:asset:getQuotaStatisticsInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/statistics/top/software	hss:asset:getSoftwareTop	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/statistics/top/web-app-and-service	hss:asset:getWebAppAndServiceTop	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/statistics/top/web-app	hss:asset:getWebAppTop	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/statistics/top/web-framework	hss:asset:getWebFrameworkTop	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/asset/overview/statistics/top/web-service	hss:asset:getWebServiceTop	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/overview/statistics/top/web-site	hss:asset:getWebSiteTop	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/app/change-history	hss:asset:listAppChangeHistories	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/apps	hss:asset:listApps	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/app/statistics	hss:asset:listAppStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/auto-launch/change-history	hss:asset:listAutoLaunchChangeHistories	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/auto-launchs	hss:asset:listAutoLaunchs	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/auto-launch/statistics	hss:asset:listAutoLaunchStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/host/core-conf-file	hss:asset:listCoreConfFileHostInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/{host_id}/core-conf-file	hss:asset:listCoreConfFileInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/statistics/core-conf-file	hss:asset:listCoreConfFileStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/host/environment	hss:asset:listEnvironmentHostInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/{host_id}/environment	hss:asset:listEnvironmentInfo	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/asset/statistics/environment	hss:asset:listEnvironmentStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/midwares/detail	hss:asset:listJarPackageHostInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/{host_id}/jar-package	hss:asset:listJarPackageInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/midwares	hss:asset:listJarPackageStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/host/kernel-module	hss:asset:listKernelModuleHostInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/{host_id}/kernel-module	hss:asset:listKernelModuleInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/statistics/kernel-module	hss:asset:listKernelModuleStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/ports	hss:asset:listPorts	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/port/statistics	hss:asset:listPortStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/processes	hss:asset:listProcesses	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/process/statistics	hss:asset:listProcessStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/investigation/tool/result	hss:asset:listResult	eps:enterpriseProjects:list
GET /v5/{project_id}/investigation/tool/list	hss:asset:listTool	eps:enterpriseProjects:list
GET /v5/{project_id}/invest	hss:asset:listToolConditionHistory	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
igation/tool/condition-history		
GET /v5/{project_id}/asset/user/change-history	hss:asset:listUserChangeHistories	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/userGroup	hss:asset:listUserGroup	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/users	hss:asset:listUsers	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/user/statistics	hss:asset:listUserStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/web-app-and-services	hss:asset:listWebAppAndServices	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/web-app-and-service-statistics	hss:asset:listWebAppAndServiceStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/host/web-app	hss:asset:listWebAppHostInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/{host_id}/web-app	hss:asset:listWebAppInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/statistics/web-app	hss:asset:listWebAppStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/host/web-framework	hss:asset:listWebFrameworkHostInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/{host_id}/web-framework	hss:asset:listWebFrameworkInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/statistics/web-framework	hss:asset:listWebFrameworkStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/	hss:asset:listWebServiceHostInfo	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
host/web-service		
GET /v5/{project_id}/asset/{host_id}/web-service	hss:asset:listWebServiceInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/statistics/web-service	hss:asset:listWebServiceStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/host/web-site	hss:asset:listWebSiteHostInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/{host_id}/web-site	hss:asset:listWebSiteInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/statistics/web-site	hss:asset:listWebSiteStatistics	eps:enterpriseProjects:list
POST /v5/{project_id}/asset/manual-collect/{type}	hss:asset:runHostAssetManualCollect	eps:enterpriseProjects:list
POST /v5/{project_id}/baseline/security-checks/policy-group/add	hss:baseline:addSecurityCheckPolicyGroup	eps:enterpriseProjects:list
PUT /v5/{project_id}/baseline/check-rule/action	hss:baseline:changeCheckRuleState	eps:enterpriseProjects:list
DELETE /v5/{project_id}/baseline/security-checks/policy-group/{group_id}	hss:baseline:deleteSecurityCheckPolicyGroup	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/risk-config/export	hss:baseline:exportSecurityCheckReport	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/overview	hss:baseline:getBaselineOverview	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/scan-status	hss:baseline:getBaselineScanStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/baseli	hss:baseline:getBaselineStatistic	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ne/statistic		
GET /v5/{project_id}/baseline/check-rule/detail	hss:baseline:getCheckRuleDetail	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/check-rule/fail-detail	hss:baseline:getCheckRuleFixFailDetail	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/security-checks/default-policy	hss:baseline:getDefaultSecurityCheckPolicy	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/security-checks/default-policy/details	hss:baseline:getDefaultSecurityCheckPolicyDetails	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/risk-config/{check_name}/detail	hss:baseline:getRiskConfigDetail	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/check-rule/hosts	hss:baseline:listCheckRuleHost	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/password-complexity	hss:baseline:listPasswordComplexity	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/risk-config/{check_name}/check-rules	hss:baseline:listRiskConfigCheckRules	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/risk-config/{check_name}/hosts	hss:baseline:listRiskConfigHosts	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/risk-configs	hss:baseline:listRiskConfigs	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/security-	hss:baseline:listSecurityCheckPolicyGroup	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
checks/policy-groups		
GET /v5/{project_id}/baseline/weak-password-users	hss:baseline:listWeakPasswordUsers	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/detection/{group_id}	hss:baseline:runBaselineDetect	eps:enterpriseProjects:list
POST /v5/{project_id}/baseline/security-checks/policy-group/{group_id}	hss:baseline:updateSecurityCheckPolicyGroup	eps:enterpriseProjects:list
POST /v5/{project_id}/event/white-list/login	hss:event:addLoginWhiteList	eps:enterpriseProjects:list
POST /v5/{project_id}/event/batch-operate	hss:event:batchChangeEvent	eps:enterpriseProjects:list
POST /v5/{project_id}/event/operate	hss:event:changeEvent	eps:enterpriseProjects:list
PUT /v5/{project_id}/event/isolated-file	hss:event:changeIsolatedFile	eps:enterpriseProjects:list
GET /v5/{project_id}/event/white-list/export	hss:event:exportAlarmWhiteList	eps:enterpriseProjects:list
POST /v5/{project_id}/emergency/event/export	hss:event:exportEmergency	eps:enterpriseProjects:list
GET /v5/{project_id}/emergency/event/emergency-statistics	hss:event:getEmergencyStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/event/attack-tag	hss:event:getEventAttackTag	eps:enterpriseProjects:list
GET /v5/{project_id}/event/severity	hss:event:getEventSeverity	eps:enterpriseProjects:list
GET /v5/{project_id}/event	hss:event:getEventStatistics	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/statistics		
GET /v5/{project_id}/emergency/event/event-detail	hss:event:getMalwareInfo	eps:enterpriseProjects:list
POST /v5/{project_id}/emergency/event/handle-malware-event	hss:event:handleMalwareEvent	eps:enterpriseProjects:list
POST /v5/{project_id}/event/white-list/import	hss:event:importAlarmWhiteList	eps:enterpriseProjects:list
POST /v5/{project_id}/emergency/event/isolate-operate	hss:event:isolateOperateEmergency	eps:enterpriseProjects:list
GET /v5/{project_id}/event/white-list/alarm	hss:event:listAlarmWhiteList	eps:enterpriseProjects:list
GET /v5/{project_id}/event/blocked-ip	hss:event:listBlockedIp	eps:enterpriseProjects:list
GET /v5/{project_id}/event/batch-operate	hss:event:listEventOperates	eps:enterpriseProjects:list
GET /v5/{project_id}/event/top-risk	hss:event:listEventTopRisk	eps:enterpriseProjects:list
GET /v5/{project_id}/event/event-type	hss:event:listEventType	eps:enterpriseProjects:list
GET /v5/{project_id}/emergency/event/file-isolate-list	hss:event:listFileIsolateList	eps:enterpriseProjects:list
GET /v5/{project_id}/event/isolated-file	hss:event:listIsolatedFile	eps:enterpriseProjects:list
GET /v5/{project_id}/event/white-list/login	hss:event:listLoginWhiteList	eps:enterpriseProjects:list
GET /v5/{project_id}/emer	hss:event:listMalware	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
gency/event/event-list		
GET /v5/{project_id}/event/events	hss:event:listSecurityEvents	eps:enterpriseProjects:list
POST /v5/{project_id}/emergency/event/recover-isolate-file	hss:event:recoverIsolateFile	eps:enterpriseProjects:list
DELETE /v5/{project_id}/event/white-list/alarm	hss:event:removeAlarmWhiteList	eps:enterpriseProjects:list
DELETE /v5/{project_id}/event/white-list/login	hss:event:removeLoginWhiteList	eps:enterpriseProjects:list
PUT /v5/{project_id}/host-management/asset-value/associate	hss:host:associateHostAssetValue	eps:enterpriseProjects:list
POST /v5/{project_id}/host-management/group/associate	hss:host:associateHostsGroup	eps:enterpriseProjects:list
POST /v5/{project_id}/setting/batch-install-agent	hss:host:batchInstallAgent	• eps:enterpriseProjects:list • ecs:cloudServers:listServersDetails
PUT /v5/{project_id}/host-management/groups	hss:host:changeHostsGroup	eps:enterpriseProjects:list
DELETE /v5/{project_id}/host-management/groups	hss:host:deleteHostsGroup	eps:enterpriseProjects:list
GET /v5/{project_id}/host-management/host-statistics	hss:host:getHostsStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/host-management/firewall	hss:host:listFirewallStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/host-management/asset-value	hss:host:listHostGroupAssetValue	eps:enterpriseProjects:list
GET	hss:host:listHostsRisk	• eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v5/{project_id}/host-management/hosts-risk		• vpc:ports:list • eip:publicIps:list
GET /v5/{project_id}/host-management/hosts	hss:host:listHostStatus	• eps:enterpriseProjects:list • vpc:ports:list • eip:publicIps:list
GET /v5/{project_id}/upgrade/agent-upgrade	hss:host:listHostsUpgrade	eps:enterpriseProjects:list
POST /v5/{project_id}/vulnerability/scan-task	hss:host:manualCheckVul	eps:enterpriseProjects:list
POST /v5/{project_id}/host-management/firewall	hss:host:switchFirewallStatus	eps:enterpriseProjects:list
POST /v5/{project_id}/host-management/protection	hss:host:switchHostsProtectStatus	eps:enterpriseProjects:list
POST /v5/{project_id}/upgrade/agent-upgrade	hss:host:upgradeAgent	eps:enterpriseProjects:list
POST /v5/{project_id}/host-management/upgrade	hss:host:upgradeAgents	eps:enterpriseProjects:list
POST /v5/{project_id}/image/local/batch-scan	hss:image:batchScanLocalImage	eps:enterpriseProjects:list
GET /v5/{project_id}/image/{image_id}/files-statistics	hss:image:getImageFilesStat	eps:enterpriseProjects:list
GET /v5/{project_id}/image/local/vul/overview	hss:image:getImageLocalVulOverview	eps:enterpriseProjects:list
GET /v5/{project_id}/image/vul/overview	hss:image:getImageVulOverview	eps:enterpriseProjects:list
GET /v5/{project_id}/image/baseline/affected	hss:image:listCfgCheckAffectedImage	eps:enterpriseProjects:list
GET /v5/{project_id}/imag	hss:image:listGlobalCfgCheck	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
e/baseline		
GET /v5/{project_id}/image/malwares	hss:image:listGlobalMalware	eps:enterpriseProjects:list
GET /v5/{project_id}/image/vuls	hss:image:listGlobalVul	eps:enterpriseProjects:list
GET /v5/{project_id}/image/{image_id}/apps	hss:image:listImageApps	eps:enterpriseProjects:list
GET /v5/{project_id}/image/{image_id}/app/vuls	hss:image:listImageAppVul	eps:enterpriseProjects:list
GET /v5/{project_id}/image/{image_id}/baseline	hss:image:listImageCfgCheck	eps:enterpriseProjects:list
GET /v5/{project_id}/image/{image_id}/files	hss:image:listImageFiles	eps:enterpriseProjects:list
GET /v5/{project_id}/image/local-repository	hss:image:listImageLocal	eps:enterpriseProjects:list
GET /v5/{project_id}/image/{image_id}/malwares	hss:image:listImageMalware	eps:enterpriseProjects:list
GET /v5/{project_id}/image/namespace	hss:image:listImageNamespace	eps:enterpriseProjects:list
GET /v5/{project_id}/image/repos	hss:image:listImageRepository	eps:enterpriseProjects:list
GET /v5/{project_id}/instance/{instance_id}/image/vuls	hss:image:listInstanceImageVul	eps:enterpriseProjects:list
GET /v5/{project_id}/image/local/containers	hss:image:listLocalImageContainers	eps:enterpriseProjects:list
GET /v5/{project_id}/image/local/hosts	hss:image:listLocalImageHosts	eps:enterpriseProjects:list
GET	hss:image:listLocalImageMalw	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v5/{project_id}/image/local/malware	are	
GET /v5/{project_id}/image/local/vuls	hss:image:listLocalImageVuls	eps:enterpriseProjects:list
GET /v5/{project_id}/image/local/{vul_id}/images	hss:image:listLocalVulRepoImage	eps:enterpriseProjects:list
GET /v5/{project_id}/image/shared-repository	hss:image:listSharedImageRepository	eps:enterpriseProjects:list
GET /v5/{project_id}/image/{vul_id}/images	hss:image:listVulRepoImage	eps:enterpriseProjects:list
POST /v5/{project_id}/image/vul-task	hss:image:runImageScan	eps:enterpriseProjects:list
POST /v5/{project_id}/image/swr/vul-task	hss:image:runSwrImageScan	eps:enterpriseProjects:list
POST /v5/{project_id}/image/shared-synchronize-task	hss:image:sharedImageSynchronization	eps:enterpriseProjects:list
PUT /v5/{project_id}/policy/group	hss:policy:addPolicyGroup	eps:enterpriseProjects:list
POST /v5/{project_id}/policy/deploy	hss:policy:associatePolicyGroup	eps:enterpriseProjects:list
POST /v5/{project_id}/policy/{policy_id}	hss:policy:changePolicyDetail	eps:enterpriseProjects:list
POST /v5/{project_id}/policy/group	hss:policy:changePolicyGroup	eps:enterpriseProjects:list
DELETE /v5/{project_id}/policy/group	hss:policy:deletePolicyGroup	eps:enterpriseProjects:list
GET /v5/{project_id}/policy/{policy_id}	hss:policy:getPolicyDetail	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/policy/group/{group_id}	hss:policy:listPolicyGroupDetail	eps:enterpriseProjects:list
POST /v5/{project_id}/{resource_type}/{resource_id}/tags	hss:quota:addResourceInstanceTag	eps:enterpriseProjects:list
POST /v5/{project_id}/{resource_type}/{resource_id}/tags/create	hss:quota:batchCreateTags	eps:enterpriseProjects:list
DELETE /v5/{project_id}/{resource_type}/{resource_id}/tags/delete	hss:quota:batchDeleteTags	eps:enterpriseProjects:list
PUT /v5/{project_id}/billing/quotas	hss:quota:cancelHostsQuota	eps:enterpriseProjects:list
POST /v1/{project_id}/hss/{resource_id}/tags/action	hss:quota:changeTmsResourceTagInfo	eps:enterpriseProjects:list
POST /v5/{project_id}/{resource_type}/resource-instances/count	hss:quota:countResourceInstances	eps:enterpriseProjects:list
DELETE /v5/{project_id}/{resource_type}/{resource_id}/tags/{key}	hss:quota:deleteResourceInstanceTag	eps:enterpriseProjects:list
POST /v5/{project_id}/{resource_type}/resource-instances/filter	hss:quota:filterResourceInstanceList	eps:enterpriseProjects:list
GET /v5/{project_id}/{resource_type}/{resource_id}/tags	hss:quota:getResourceInstanceTag	eps:enterpriseProjects:list
GET /v5/{project_id}/billing/quotas	hss:quota:getResourceQuotas	eps:enterpriseProjects:list
GET /v1/{project_id}/hss/{resource_id}/tags	hss:quota:getTmsResourceTagsInfo	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/{resource_type}/tags	hss:quota:listProjectTags	eps:enterpriseProjects:list
GET /v5/{project_id}/billing/quotas-detail	hss:quota:listQuotasDetail	eps:enterpriseProjects:list
POST /v5/{project_id}/billing/resource-id-list	hss:quota:listResourceIds	eps:enterpriseProjects:list
POST /v1/{project_id}/hss/resource_instances/action	hss:quota:listTmsResourceInstancesInfo	eps:enterpriseProjects:list
POST /v5/{project_id}/hss/upgrade_orders/{order_id}	hss:quota:upgradeOrder	eps:enterpriseProjects:list
PUT /v5/{project_id}/vulnerability/status	hss:vulnerability:changeVulStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/vul/emergency/list	hss:vulnerability:exportEmergencyVulnerabilities	eps:enterpriseProjects:list
GET /v5/{project_id}/vul/export-vuls-list	hss:vulnerability:exportVulsList	eps:enterpriseProjects:list
GET /v5/{project_id}/vul/cms-detail	hss:vulnerability:getCmsVulDetail	eps:enterpriseProjects:list
GET /v5/{project_id}/vul/emergency/summary	hss:vulnerability:getEmergencySummary	eps:enterpriseProjects:list
GET /v5/{project_id}/vul/emergency/detail	hss:vulnerability:getEmergencyVulDetail	eps:enterpriseProjects:list
GET /v5/{project_id}/vul/linux-detail	hss:vulnerability:getLinuxVulDetail	eps:enterpriseProjects:list
GET /v5/{project_id}/vul/manual/scan/status	hss:vulnerability:getVulCheckStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/vul/v	hss:vulnerability:getVulSummary	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ul-summary		
GET /v5/{project_id}/vul/windows-detail	hss:vulnerability:getWindosVulDetail	eps:enterpriseProjects:list
GET /v5/{project_id}/windows/vul/num	hss:vulnerability:getWindowsVulNum	eps:enterpriseProjects:list
GET /v5/{project_id}/vulnerability/host/{host_id}	hss:vulnerability:listHostVuls	eps:enterpriseProjects:list
GET /v5/{project_id}/vul/host-summary	hss:vulnerability:listHostVulSummary	eps:enterpriseProjects:list
GET /v5/{project_id}/vul/top-vul	hss:vulnerability:listTopVulSummary	eps:enterpriseProjects:list
GET /v5/{project_id}/vulnerability/hosts	hss:vulnerability:listVulHosts	eps:enterpriseProjects:list
GET /v5/{project_id}/vulnerability/vulnerabilities	hss:vulnerability:listVulnerabilities	eps:enterpriseProjects:list
GET /v5/{project_id}/vul/{host_id}/fail_detail	hss:vulnerability:listVulRepairFailedDetail	eps:enterpriseProjects:list
GET /v5/{project_id}/vul/vul-type-summary	hss:vulnerability:listVulTypeSummary	eps:enterpriseProjects:list
POST /v5/{project_id}/vul/emergency/operate	hss:vulnerability:operateEmergency	eps:enterpriseProjects:list
GET /v5/{project_id}/host-management/{host_id}/scan_status	hss:host:getScanStatus	eps:enterpriseProjects:list
POST /v5/{project_id}/host-management/{host_id}/manual_detect	hss:host:setManualDetect	eps:enterpriseProjects:list
GET /v5/setting/account/trusted-services	hss::getTrustServiceStatus	eps:enterpriseProjects:list
POST	hss::enableTrustService	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v5/setting/account/trusted-services		
GET /v5/setting/account/admin	hss::validateAdmin	eps:enterpriseProjects:list
GET /v5/setting/account/accounts	hss::listAccounts	eps:enterpriseProjects:list
POST /v5/setting/account/accounts	hss::batchAddAccounts	eps:enterpriseProjects:list
DELETE /v5/setting/account/accounts	hss::deleteAccount	eps:enterpriseProjects:list
GET /v5/setting/account/organization-tree	hss::listOrganizationTree	eps:enterpriseProjects:list
GET /v5/setting/account/delegated-accounts	hss::listDelegatedAccounts	eps:enterpriseProjects:list
GET /v5/{project_id}/ransomware/optional/vaults	hss:antiransomware:listBackupVaults	eps:enterpriseProjects:list
GET /v5/{project_id}/ransomware/servers	hss:antiransomware:listRansomwareProtectionNodes	eps:enterpriseProjects:list
GET /v5/{project_id}/ransomware/statistics/backups	hss:antiransomware:getBackupsStatistics	eps:enterpriseProjects:list
POST /v5/{project_id}/ransomware/backup/single_open	hss:antiransomware:startSingleBackup	eps:enterpriseProjects:list
GET /v5/{project_id}/backup/{policy_id}	hss:antiransomware:getBackupPolicyInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/host-management/outside-group/status	hss:hostGroup:getOutsideGroupStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/host-management/outside-	hss:hostGroup:getOutsideHostGroup	eps:enterpriseProjects:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
group		
POST /v5/{project_id}/host-management/outside-group	hss:hostGroup:addOutsideHostGroup	eps:enterpriseProjects:list
PUT /v5/{project_id}/host-management/outside-group	hss:hostGroup:changeOutsideHostGroup	eps:enterpriseProjects:list
GET /v5/{project_id}/image/tags	hss:images:listImageTag	eps:enterpriseProjects:list
GET /v5/{project_id}/image/{image_digest}/sensitive	hss:images:listImageSensitive	eps:enterpriseProjects:list
GET /v5/{project_id}/image/sensitive/filepath_whitelist	hss:images:getFilePathWhiteDetail	eps:enterpriseProjects:list
POST /v5/{project_id}/image/sensitive/filepath_whitelist	hss:images:changeFilePathWhiteDetail	eps:enterpriseProjects:list
POST /v5/{project_id}/image/sensitive/operate	hss:images:changeSensitiveInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/event/top-event-type	hss:event:listTopEventType	eps:enterpriseProjects:list
GET /v5/{project_id}/vulnerability/scan-policy	hss:vulnerability:getVulScanPolicy	-
PUT /v5/{project_id}/vulnerability/scan-policy	hss:vulnerability:changeVulScanPolicy	-
GET /v5/{project_id}/vulnerability/white-lists	hss:vulnerability:listVulWhiteList	-
GET /v5/{project_id}/vulnerability/white-list/{id}	hss:vulnerability:getVulWhiteListDetail	-
PUT /v5/{project_id}/vulne	hss:vulnerability:changeVulW	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
rability/white-list/{id}	hiteList	
DELETE /v5/{project_id}/vulnerability/white-list/{id}	hss:vulnerability:deleteVulWhiteList	-
POST /v5/{project_id}/vulnerability/white-list	hss:vulnerability:addVulWhiteList	-
GET /v5/{project_id}/vulnerability/white-list/vulnerability-options	hss:vulnerability:listVulWhiteListVulOptions	-
GET /v5/{project_id}/vulnerability/scan-tasks	hss:vulnerability:listVulScanTask	-
GET /v5/{project_id}/vulnerability/scan-task/{task_id}/hosts	hss:vulnerability:listVulScanTaskHost	-
PUT /v5/{project_id}/vulnerability/scan/task/{task_id}/rescan	hss:vulnerability:rescanVulScanTask	-
GET /v5/{project_id}/vulnerability/scan/task/statistics	hss:vulnerability:getVulScanTaskStatistics	-
GET /v5/{project_id}/vulnerability/statistics	hss:vulnerability:listHostVulStatistics	-
GET /v5/{project_id}/vulnerability/{host_id}/apps	hss:vulnerability:listVulHostApps	-
GET /v5/{project_id}/vulnerability/{host_id}/process	hss:vulnerability:listVulHostProcess	-
GET /v5/{project_id}/vulnerability/handle-history	hss:vulnerability:listVulHandleHistory	-
GET /v5/{project_id}/vulnerability/host/hosts	hss:vulnerability:listVulHostHosts	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/vulnerability/host-vulnerability/vulnerabilities	hss:vulnerability:listVulHostVuls	-
GET /v5/{project_id}/vulnerability/handle/vulnerabilities	hss:vulnerability:listVulHostHandleVuls	-
GET /v5/{project_id}/image/{image_digest}/non-compliant-app	hss:image:listImageNonCompliantApp	-
POST /v5/{project_id}/image/swr/vul/batch-export-vul	hss:image:batchExportSWRVulList	-
POST /v5/{project_id}/image/local/vul/batch-export-vul	hss:image:batchExportLocalVulList	-
GET /v5/{project_id}/image/baseline/extended-weak-password	hss:image:getExtendedWeakPassword	-
POST /v5/{project_id}/image/baseline/extended-weak-password	hss:image:changeExtendedWeakPassword	-
GET /v5/{project_id}/image/{image_digest}/basic-image	hss:image:listImageBasicImage	-
GET /v5/{project_id}/image/baseline/password-complexity	hss:image:listImagePwdComplexity	-
GET /v5/{project_id}/image/baseline/weak-password-users	hss:image:listImageWeakPwdUsers	-
GET /v5/{project_id}/image/baseline/risk-configs	hss:image:listImageRiskConfigs	-
GET	hss:image:getImageRiskConfig	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v5/{project_id}/image/baseline/risk-configs/{check_name}/detail	Detail	
GET /v5/{project_id}/image/baseline/check-rule/detail	hss:image:getImageCheckRuleDetail	-
GET /v5/{project_id}/image/baseline/statistic	hss:image:getImageBaselineStatistic	-
POST /v5/{project_id}/event/white-list/userlist	hss:event:addSystemUserWhiteList	-
PUT /v5/{project_id}/event/white-list/userlist	hss:event:updateSystemUserWhiteList	-
GET /v5/{project_id}/event/white-list/userlist	hss:event:listSystemUserWhiteList	-
DELETE /v5/{project_id}/event/white-list/userlist	hss:event:removeSystemUserWhiteList	-
POST /v5/{project_id}/kubernetes/save-clusters	hss:container:saveClusters	-
GET /v5/{project_id}/kubernetes/clusters	hss:container:listClusterInfo	-
GET /v5/{project_id}/kubernetes/pods	hss:container:listPodInfo	-
GET /v5/{project_id}/kubernetes/{pod_name}/pod/detail	hss:container:showPodDetail	-
GET /v5/{project_id}/kubernetes/containers	hss:container:listContainerInfo	-
GET /v5/{project_id}/kubernetes/container/detail	hss:container:showContainerDetail	-
GET /v5/{project_id}/kuber	hss:container:listServiceInfo	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
netes/services		
GET /v5/{project_id}/kubernetes/service/detail	hss:container:showServiceDetail	-
GET /v5/{project_id}/kubernetes/endpoints	hss:container:listEndpointInfo	-
GET /v5/{project_id}/kubernetes/endpoint/detail	hss:container:showEndpointDetail	-
GET /v5/{project_id}/kubernetes/deployments	hss:container:listDeployments	-
GET /v5/{project_id}/kubernetes/statefulsets	hss:container:listStatefulSets	-
GET /v5/{project_id}/kubernetes/daemonsets	hss:container:listDaemonSets	-
GET /v5/{project_id}/kubernetes/jobs	hss:container:listJobs	-
GET /v5/{project_id}/kubernetes/cronjobs	hss:container:listCronJobs	-
GET /v5/{project_id}/vulnerability/statistics/affected	hss:vulnerability:showVulAffectedStatics	-
PUT /v5/{project_id}/kubernetes/{container_name}/container/isolate	hss:container:isolateK8sContainer	-
GET /v5/{project_id}/container-network/network-statistics	hss:container:getNetworkStatistics	-
GET /v5/{project_id}/container-network/cluster-list	hss:container:getClusters	-
GET /v5/{project_id}/container-	hss:container:getClusterNetworkInfo	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
network/{cluster_id}/network-info		
GET /v5/{project_id}/container-network/{cluster_id}/policy-list	hss:container:getClusterPolicyList	-
DELETE /v5/{project_id}/container-network/{cluster_id}/policy	hss:container:deletePolicy	-
POST /v5/{project_id}/container-network/{cluster_id}/policy	hss:container:createPolicy	-
PUT /v5/{project_id}/container-network/{cluster_id}/policy	hss:container:updatePolicy	-
GET /v5/{project_id}/container-network/{cluster_id}/policy-sync	hss:container:syncClusterPolicyList	-
GET /v5/{project_id}/container-network/cluster-sync	hss:container:syncClusterList	-
GET /v5/{project_id}/container-network/{cluster_id}/namespace-list	hss:container:getNamespaceList	-
GET /v5/{project_id}/container-network/{cluster_id}/node-list	hss:container:getNodeList	-
GET /v5/{project_id}/container-network/{cluster_id}/node-sync	hss:container:syncClusterNodeList	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v5/{project_id}/ransomware/protection/policy	hss:antiransomware:addRansomwareProtectionPolicy	-
POST /v5/{project_id}/ransomware/backup/associate-policy	hss:antiransomware:associateBackupPolicy	-
GET /v5/{project_id}/ransomware/backup/policies	hss:antiransomware:listBackupPolicy	-
POST /v5/{project_id}/ransomware/protection/policy/deploy	hss:antiransomware:associateProtectionPolicy	-
POST /v5/{project_id}/ransomware/protection/batch-open	hss:antiransomware:batchStartProtection	-
GET /v5/{project_id}/event/att-ck	hss:event:getEventAttCk	-
GET /v5/{project_id}/event/download-file	hss:event:downloadEventSourceFile	-
GET /v5/{project_id}/overview/security/score	hss:overview:showSecurityScore	-
GET /v5/{project_id}/overview/security/risk/list	hss:overview:listSecurityRisk	-
GET /v5/{project_id}/overview/quotas/host/statistics	hss:overview:showQuotaHostStatistics	-
GET /v5/{project_id}/overview/agent/statistics	hss:overview:showAgentStatistics	-
GET /v5/{project_id}/overview/hot/information	hss:overview:showHotInformation	-
GET /v5/{project_id}/overview/security/risk	hss:overview:showSecurityRisk	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/overview/protection/statistics	hss:overview:showProtectStatistics	-
GET /v5/{project_id}/overview/statistics	hss:overview:showStatistics	-
GET /v5/{project_id}/image/swr-repository	hss:image:listSwrImageRepository	-
POST /v5/{project_id}/image/batch-scan	hss:image:batchScanSwrImage	-
GET /v5/{project_id}/image/{image_id}/vulnerabilities	hss:image:vulnerabilities	-
GET /v5/{project_id}/image/vulnerability/{vul_id}/cve	hss:image:listVulnerabilityCve	-
GET /v5/{project_id}/image/baseline/risk-configs/{check_name}/rules	hss:image:listImageRiskConfigRules	-
POST /v5/{project_id}/image/synchronize	hss:image:runImageSynchronize	-
GET /v5/{project_id}/event/forensic	hss:event:listEventForensic	-
GET /v5/{project_id}/event/similar-handled-events	hss:event:listSimilarHandledEvents	-
GET /v5/{project_id}/cluster-protect/policy	hss:container:getPolicies	-
GET /v5/{project_id}/cluster-protect/policy/{policy_id}	hss:container:getPolicyDetail	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/cluster-protect/events	hss:container:getProtectEvents	-
GET /v5/{project_id}/cluster-protect/clusters	hss:container:getProtectClusters	-
GET /v5/{project_id}/cluster-protect/switch-mode	hss:container:changeProtectStatus	-
GET /v5/{project_id}/cluster-protect/whiteimage	hss:container:addWhiteImage	-
GET /v5/{project_id}/cluster-protect/default-policy	hss:container:listDefaultPolicy	-
GET /v5/{project_id}/cluster-protect/protection-item	hss:container:listProtectionItem	-
POST /v5/{project_id}/vulnerability/backup-statistics	hss:vulnerability:getVulBackupStatistics	-
GET /v5/{project_id}/vulnerability/backup/host-vaults	hss:vulnerability:ListVulHostVaults	-
GET /v5/{project_id}/vulnerability/backup/backups	hss:vulnerability:ListVulHostBackups	-
PUT /v5/{project_id}/vulnerability/backup/{backup_id}/restore	hss:vulnerability:RestoreVulHostBackup	-
POST /v5/{project_id}/event/export	hss:event:exportEvent	-
GET /v5/{project_id}/event/export-task/{task_id}	hss:event:queryExportTask	-
GET /v5/{project_id}/event	hss:event:downloadEvent	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/download/{file_id}		
POST /v5/{project_id}/app/policy	hss:ars:createAppWhitelistPolicy	-
GET /v5/{project_id}/app/policy	hss:ars:listAppWhitelistPolicy	-
PUT /v5/{project_id}/app/policy	hss:ars:changeAppWhitelistPolicy	-
DELETE /v5/{project_id}/app/policy	hss:ars:deleteAppWhitelistPolicy	-
GET /v5/{project_id}/app/{policy_id}/detail	hss:ars:showAppWhitelistPolicy	-
PUT /v5/{project_id}/app/host	hss:ars:switchAppWhitelistPolicyHost	-
POST /v5/{project_id}/app/{policy_id}/host	hss:ars:addAppWhitelistPolicyHost	-
GET /v5/{project_id}/app/host	hss:ars:listAppWhitelistPolicyHost	-
DELETE /v5/{project_id}/app/{policy_id}/host	hss:ars:deleteAppWhitelistPolicyHost	-
GET /v5/{project_id}/app/host-management/hosts	hss:ars:listAppWhitelistHostStatus	-
GET /v5/{project_id}/app/{policy_id}/process	hss:ars:listAppWhitelistPolicyProcess	-
PUT /v5/{project_id}/app/{policy_id}/process	hss:ars:changeAppWhitelistPolicyProcessStatus	-
POST /v5/{project_id}/app/{policy_id}/process	hss:ars:addAppWhitelistPolicyProcess	-
GET /v5/{project_id}/app/{policy_id}/process-	hss:ars:listAppWhitelistPolicyProcessExtend	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
extend		
GET /v5/{project_id}/app/{policy_id}/process/export	hss:ars:exportAppWhitelistPolicyProcess	-
POST /v5/{project_id}/app/{policy_id}/learn	hss:ars:switchAppWhitelistPolicyLearnStatus	-
GET /v5/{project_id}/app/agent/statistics	hss:ars:showAppWhitelistAgentStatics	-
GET /v5/{project_id}/app/event	hss:ars:listAppWhitelistEvent	-
DELETE /v5/{project_id}/selfbuilt/kubernetes/cluster/daemonset	hss:container:deleteSelfBuildK8sClusterDaemonsetInfo	-
POST /v5/{project_id}/selfbuilt/kubernetes/cluster/daemonset	hss:container:saveSelfBuildK8sClusterDaemonsetInfo	-
GET /v5/{project_id}/selfbuilt/kubernetes/cluster/daemonset	hss:container:showSelfBuildK8sClusterDaemonsetInfo	-
GET /v5/{project_id}/selfbuilt/kubernetes/clusters	hss:container:listSelfBuildK8sClusterInfo	-
POST /v5/{project_id}/namespaces/{namespace}/daemonsets	hss:container:createDaemonset	-
POST /v5/{project_id}/vulnerability/repair-cmds	hss:vulnerability:listVulRepairCmds	-
GET /v5/{project_id}/vulnerability/urgent-vulnerabilities	hss:vulnerability:listUrgentVulnerabilities	-
PUT /v5/{project_id}/antivirus/task	hss:antivirus:switchAntivirusTask	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/antivirus/statistic	hss:antivirus:showAntivirusStatistic	-
GET /v5/{project_id}/image/full-scan-progress	hss:image:showImageFullScanProgress	-
PUT /v5/{project_id}/host/operate	hss:host:changeHostIgnoreStatus	-
POST /v5/{project_id}/image/baseline/export	hss:image:batchExportBaselineTask	-
POST /v5/{project_id}/image/security-report/statistic	hss:image:showImageSecurityReportStatistic	-
POST /v5/{project_id}/vul/export	hss:vulnerability:exportVuls	-
GET /v5/{project_id}/export-task/{task_id}	hss:exportTask:queryExportTask	-
GET /v5/{project_id}/download/{file_id}	hss:file:downloadExportedFile	-
GET /v5/{project_id}/image/vulnerabilities	hss:image:listGlobalVulnerabilities	-
GET /v5/{project_id}/image/vulnerability/images	hss:image:listVulnerabilityImages	-
GET /v5/{project_id}/setting/docker-plugin-install-script	hss:setting:getPluginInstallScript	-
GET /v5/{project_id}/setting/plugins	hss:setting:getPluginList	-
GET /v5/{project_id}/setting/config/auto-open-quota	hss:setting:getAutoOpenQuotaStatus	-
PUT	hss:setting:changeAutoOpenQ	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v5/{project_id}/setting/config/auto-open-quota	uotaStatus	
POST /v5/{project_id}/image/swr-vulnerability/export	hss:image:batchExportSWRVulTask	-
POST /v5/{project_id}/image/local-vulnerability/export	hss:image:batchExportLocalVulTask	-
GET /v5/{project_id}/setting/config/agent-auto-upgrade	hss:setting:getAgentAutoUpgradeStatus	-
PUT /v5/{project_id}/setting/config/agent-auto-upgrade	hss:setting:changeAgentAutoUpgradeStatus	-
GET /v5/{project_id}/product/productdata/offering-infos	hss:quota:showProductdataOfferingInfos	-
GET /v5/{project_id}/image/local/apps	hss:image:listLocalImageAppInfo	-
GET /v5/{project_id}/image/local/app/vulnerabilities	hss:image:listLocalImageAppVulnerabilities	-
GET /v5/{project_id}/ransomware/protection/status	hss:antiransomware:getRansomwareProtectionStatus	-
GET /v5/{project_id}/ransomware/protection/auto-deploy-policy	hss:antiransomware:getAutoDeployAgentList	-
PUT /v5/{project_id}/ransomware/protection/auto-deploy-policy	hss:antiransomware:updateAutoDeployAgent	-
GET /v5/{project_id}/vulnerability/individual-	hss:vulnerability:getVulIndividualStatistics	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
statistics		
DELETE /v5/{project_id}/event/isolated-file	hss:event:deleteIsolatedFile	-
GET /v5/{project_id}/antivirus/handle-history	hss:antivirus:listAntivirusHandleHistory	-
GET /v5/{project_id}/honeypot-port/host-statistics	hss:decoyport:showStatistics	-
GET /v5/{project_id}/honeypot-port/default-config	hss:decoyport:showAutoBind	-
PUT /v5/{project_id}/honeypot-port/default-config	hss:decoyport:switchAutoBind	-
GET /v5/{project_id}/honeypot-port/host-list	hss:decoyport:showHostList	-
GET /v5/{project_id}/honeypot-port/policy-list	hss:decoyport:listPolicy	-
GET /v5/{project_id}/honeypot-port/support-list	hss:decoyport:listAvailableHost	-
PUT /v5/{project_id}/honeypot-port/host-policy/{policy_id}	hss:decoyport:switchHostPolicy	-
DELETE /v5/{project_id}/honeypot-port/host-policy/{policy_id}	hss:decoyport:deleteHostPolicy	-
POST /v5/{project_id}/honeypot-port/policy	hss:decoyport:createPolicy	-
PUT /v5/{project_id}/honeypot-port/policy/{policy_id}	hss:decoyport:modifyPolicy	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/honeypot-port/policy/{policy_id}	hss:decoyport:showPolicyDetails	-
DELETE /v5/{project_id}/honeypot-port/policy/{policy_id}	hss:decoyport:deletePolicy	-
PUT /v5/{project_id}/honeypot-port/policy-enable/{policy_id}	hss:decoyport:switchPolicy	-
GET /v5/{project_id}/export-task	hss:exportTask:queryLatestExportTaskByType	-
POST /v5/{project_id}/container-network/{cluster_id}/{namespace}/security-group-policy	hss:container:createSecurityGroupPolicy	-
PUT /v5/{project_id}/container-network/{cluster_id}/{namespace}/security-group-policy	hss:container:updateSecurityGroupPolicy	-
GET /v5/{project_id}/container-network/{cluster_id}/security-group-policies	hss:container:getSecurityGroupPolicyList	-
DELETE /v5/{project_id}/container-network/{cluster_id}/security-group-policy	hss:container:deleteSecurityGroupPolicy	-
GET /v5/{project_id}/container-network/{cluster_id}/security-group-policy-sync	hss:container:syncSecurityGroupPolicy	-
GET	hss:container:getWorkloadList	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v5/{project_id}/container-network/{cluster_id}/{namespace}/workloads		
GET /v5/{project_id}/container-network/security-groups	hss:container:getSecurityGroupList	-

资源类型（Resource）

HSS 服务不支持在身份策略中的资源中指定资源进行权限控制。如需允许访问 HSS 服务，请在身份策略的 Resource 元素中使用通配符号*，表示身份策略将应用到所有资源。

条件（Condition）

HSS 服务不支持在身份策略中的条件键中配置服务级的条件键。HSS 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.7.10 安全云脑 SecMaster

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为 SCP 中支持的授权项。

 版权所有 © 华为云计算技术有限公司

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在 SCP 中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在 SCP 语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 SecMaster 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在 SCP 语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

  关于 SecMaster 定义的条件键的详细信息请参见条件（Condition）。
- **“别名”**列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 SecMaster 的相关操作。

表3-160 SecMaster 支持的授权项 Part1

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:playbook:get	授予权限获取剧本详情。	read	playbook *	-	-
secmaster:playbook:create	授予权限创建剧本。	write	playbook *	-	-
secmaster:playbook:delete	授予权限删除剧本。	write	playbook *	-	-
secmaster:playbook:update	授予权限更新剧本。	write	playbook *	-	-
secmaster:playbook:list	授予权限获取剧本列表。	list	playbook *	-	-
secmaster:playbook:getStatistics	授予权限获取剧本统计数据。	read	playbook *	-	-
secmaster:playbook:getMonitor	授予权限获取剧本运行监控数据。	read	playbook *	-	-
secmaster:playbook:copyVersion	授予权限克隆剧本。	write	playbook *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:playbook:approve	授予权限审核剧本。	write	playbook *	-	-
secmaster:playbook:listApproves	授予权限查询审核列表。	list	playbook *	-	-
secmaster:playbook:listInstances	授予权限查询实例列表。	list	playbook *	-	-
secmaster:playbook:getInstanceAuditlog	授予权限查询实例审计日志列表。	list	playbook *	-	-
secmaster:playbook:createVersion	授予权限创建剧本版本。	write	playbook *	-	-
secmaster:playbook:getVersion	授予权限获取剧本版本。	read	playbook *	-	-
secmaster:playbook:deleteVersion	授予权限删除剧本版本。	write	playbook *	-	-
secmaster:playbook:updateVersion	授予权限更新剧本版本。	write	playbook *	-	-
secmaster:playbook:listVersions	授予权限获取剧本版本列表。	list	playbook *	-	-
secmaster:playbook:getInstance	授予权限查询实例详情。	read	playbook *	-	-
secmaster:playbook:getInstanceTopology	授予权限查询实例拓扑详情。	read	playbook *	-	-
secmaster:playbook:operateInstance	授予权限操作剧本实例。	write	playbook *	-	-
secmaster:workflow:list	授予权限查询流程列表。	list	workflow *	-	-
secmaster:workflow:get	授予权限获取流程的详情。	read	workflow *	-	-
secmaster:workflow:delete	授予权限删除流程。	write	workflow *	-	-
secmaster:workflow:create	授予权限创建流程。	write	workflow *	-	-
secmaster:workflow:	授予权限更新流	write	workflo	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
update	程。		w *		
secmaster:workflow:listVersions	授予权限获取流程版本的列表。	list	workflow *	-	-
secmaster:workflow:getVersion	授予权限获取流程的版本详情。	read	workflow *	-	-
secmaster:workflow:deleteVersion	授予权限删除流程的版本。	write	workflow *	-	-
secmaster:workflow:createVersion	授予权限创建流程版本。	write	workflow *	-	-
secmaster:workflow:updateVersion	授予权限更新流程的版本。	write	workflow *	-	-
secmaster:workflow:approveVersion	授予权限审核流程版本。	write	workflow *	-	-
secmaster:workflow:validate	授予权限校验流程的版本。	write	workflow *	-	-
secmaster:workflow:simulate	授予权限更新流程版本调试结果。	write	workflow *	-	-
secmaster:workflow:getInstance	授予权限流程实例拓扑图。	read	workflow *	-	-
secmaster:workflow:operateInstance	授予权限更新或创建流程实例。	write	workflow *	-	-
secmaster:connection:list	授予权限查询资产连接列表。	list	connection *	-	-
secmaster:connection:create	授予权限创建资产连接。	write	connection *	-	-
secmaster:connection:get	授予权限获取资产连接详情。	read	connection *	-	-
secmaster:connection:delete	授予权限删除资产连接。	write	connection *	-	-
secmaster:connection:update	授予权限更新资产连接。	write	connection *	-	-
secmaster:workspace:listWorkspace	授予权限查询工作空间列表。	list	workspace *	-	secmaster:workspace:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:workspace:createWorkspace	授予权限创建工作空间。	write	workspace *	-	secmaster:workspace:create
secmaster:workspace:updateWorkspace	授予权限更新工作空间。	write	workspace *	-	secmaster:workspace:update
secmaster:workspace:getWorkspace	授予权限获取工作空间详情。	read	workspace *	-	secmaster:workspace:get
secmaster:workspace:deleteWorkspace	授予权限删除工作空间。	write	workspace *	-	secmaster:workspace:delete
secmaster:workspace:listAgency	授予权限查询空间托管列表。	list	workspace *	-	secmaster:workspace:list
secmaster:workspace:createAgency	授予权限创建空间托管。	write	workspace *	secmaster:TargetRegion	secmaster:workspace:create
secmaster:workspace:updateAgency	授予权限更新空间托管。	write	workspace *	-	secmaster:workspace:update
secmaster:workspace:getAgency	授予权限获取空间托管详情。	read	workspace *	-	secmaster:workspace:get
secmaster:workspace:deleteAgency	授予权限删除空间托管。	write	workspace *	-	secmaster:workspace:delete
secmaster:task:list	授予权限查询待办列表。	list	task *	-	-
secmaster:task:create	授予权限创建待办。	write	task *	-	-
secmaster:task:update	授予权限更新待办。	write	task *	-	-
secmaster:task:get	授予权限获取待办详情。	read	task *	-	-
secmaster:indicator:get	授予权限获取情报详情。	read	indicator *	-	-
secmaster:indicator:create	授予权限创建情报。	write	indicator *	-	-
secmaster:indicator:u	授予权限更新情	write	indicato	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
pdate	报。		r *		
secmaster:indicator:delete	授予权限删除情报。	write	indicator *	-	-
secmaster:indicator:list	授予权限查询情报列表。	read	indicator *	-	-
secmaster:indicator:listTypes	授予权限查询情报类型列表。	list	indicator *	-	-
secmaster:indicator:bindLayout	授予权限绑定情报类型与布局关联。	write	indicator *	-	-
secmaster:alert:get	授予权限获取告警详情。	read	alert *	-	-
secmaster:alert:create	授予权限创建告警。	write	alert *	-	-
secmaster:alert:update	授予权限更新告警。	write	alert *	-	-
secmaster:alert:list	授予权限搜索告警列表。	list	alert *	-	-
secmaster:alert:delete	授予权限删除告警。	write	alert *	-	-
secmaster:alert:batchOrders	授予权限告警转事件。	list	alert *	-	-
secmaster:alert:listTypes	授予权限查询告警类型列表。	list	alert *	-	-
secmaster:alert:listCategories	授予权限查询告警类别列表。	list	alert *	-	-
secmaster:alert:createType	授予权限创建告警类型。	write	alert *	-	-
secmaster:alert:updateType	授予权限修改告警类型。	write	alert *	-	-
secmaster:alert:deleteType	授予权限删除告警类型。	write	alert *	-	-
secmaster:alert:enableType	授予权限启用/禁用告警类型。	write	alert *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:alert:bindLayout	授予权限绑定告警类型与布局关联。	write	alert *	-	-
secmaster:incident:get	授予权限获取事件详情。	read	incident *	-	-
secmaster:incident:create	授予权限创建事件。	write	incident *	-	-
secmaster:incident:update	授予权限更新事件。	write	incident *	-	-
secmaster:incident:list	授予权限搜索事件列表。	list	incident *	-	-
secmaster:incident:listTypes	授予权限获取事件的类型列表。	list	incident *	-	-
secmaster:incident:delete	授予权限删除事件。	write	incident *	-	-
secmaster:incident:listCategories	授予权限查询事件类别列表。	list	incident *	-	-
secmaster:incident:createType	授予权限创建事件类型。	write	incident *	-	-
secmaster:incident:updateType	授予权限修改事件类型。	write	incident *	-	-
secmaster:incident:deleteType	授予权限删除事件类型。	write	incident *	-	-
secmaster:incident:enableType	授予权限启用/禁用事件类型。	write	incident *	-	-
secmaster:incident:bindLayout	授予权限绑定事件类型与布局的关联。	write	incident *	-	-
secmaster:dataobject:createRelation	授予权限创建对象关系。	write	dataobject *	-	-
secmaster:dataobject:deleteRelation	授予权限删除对象关系。	write	dataobject *	-	-
secmaster:dataobject:listRelation	授予权限搜索对象关系列表。	list	dataobject *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:vulnerability:listGroup	授予权限查询漏洞组列表。	list	vulnerability *	-	-
secmaster:vulnerability:getGroup	授予权限获取漏洞组详情。	read	vulnerability *	-	-
secmaster:vulnerability:exportGroup	授予权限导出漏洞组列表。	list	vulnerability *	-	-
secmaster:vulnerability:listType	授予权限查询漏洞类型列表。	list	vulnerability *	-	-
secmaster:vulnerability:bindLayout	授予权限绑定漏洞类型与布局关联。	write	vulnerability *	-	-
secmaster:vulnerability:createType	授予权限创建漏洞类型。	write	vulnerability *	-	-
secmaster:vulnerability:updateType	授予权限修改漏洞类型。	write	vulnerability *	-	-
secmaster:vulnerability:deleteType	授予权限删除漏洞类型。	write	vulnerability *	-	-
secmaster:vulnerability:enableType	授予权限启用/禁用漏洞类型。	write	vulnerability *	-	-
secmaster:subscription:deletePostPaidOrder	授予权限删除按需订单。	write	-	-	-
secmaster:subscription:createPostPaidOrder	授予权限创建按需订单。	write	-	-	-
secmaster:subscription:createPrePaidOrder	授予权限创建包周期订单。	write	-	-	-
secmaster:subscription:getVersion	授予权限查看订购版本。	read	-	-	-
secmaster:metric:getResult	授予权限查看指标结果。	read	metric *	-	-
secmaster:metric:listResults	授予权限列出指标结果。	list	metric *	-	-
secmaster:metric:listHits	授予权限列出指标 Hits 结果。	list	metric *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:agency:get	授予权限查看委托。	read	-	-	-
secmaster:agency:create	授予权限创建委托。	write	-	-	-
secmaster:resource:getStatistics	授予权限查看资源统计。	read	resource *	-	-
secmaster:resource:list	授予权限列出资源。	list	resource *	-	-
secmaster:resource:import	授予权限导入资源。	write	resource *	-	-
secmaster:resource:getTemplate	授予权限获取资源导入模板。	read	resource *	-	-
secmaster:report:list	授予权限列出报告。	list	report *	-	-
secmaster:report:get	授予权限查看报告。	read	report *	-	-
secmaster:report:create	授予权限创建报告。	write	report *	-	-
secmaster:report:update	授予权限更新报告。	write	report *	-	-
secmaster:report:delete	授予权限删除报告。	write	report *	-	-
secmaster:emergencyVulnerability:updateReadStatus	授予权限设置应急漏洞读取状态。	write	emergencyVulnerability *	-	-
secmaster:emergencyVulnerability:list	授予权限列出应急漏洞。	list	emergencyVulnerability *	-	-
secmaster:emergencyVulnerability:export	授予权限导出应急漏洞。	read	emergencyVulnerability *	-	-
secmaster:dataspace:list	授予权限查询数据空间列表。	list	dataspace *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:dataspace:create	授予权限创建数据空间。	write	dataspace *	-	-
secmaster:dataspace:get	授予权限查询数据空间详情。	read	dataspace *	-	-
secmaster:dataspace:update	授予权限更新数据空间。	write	dataspace *	-	-
secmaster:dataspace:delete	授予权限删除数据空间。	write	dataspace *	-	-
secmaster:pipe:list	授予权限查询数据管道列表。	list	pipe *	-	-
secmaster:pipe:create	授予权限创建数据管道。	write	pipe *	-	-
secmaster:pipe:get	授予权限查询数据管道详情。	read	pipe *	-	-
secmaster:pipe:update	授予权限更新数据管道。	write	pipe *	-	-
secmaster:pipe:delete	授予权限删除数据管道。	write	pipe *	-	-
secmaster:pipe:getIndex	授予权限查询数据管道索引。	read	pipe *	-	-
secmaster:pipe:updateIndex	授予权限更新数据管道索引。	write	pipe *	-	-
secmaster:pipe:getConsumption	授予权限查询数据管道消费。	read	pipe *	-	-
secmaster:pipe:createConsumption	授予权限创建数据管道消费。	write	pipe *	-	-
secmaster:pipe:deleteConsumption	授予权限删除数据管道消费。	write	pipe *	-	-
secmaster:search:listLogs	授予权限查询数据。	list	workspace *	-	-
secmaster:search:listHistograms	授予权限查询数据分布直方图。	list	workspace *	-	-
secmaster:search:createAnalysis	授予权限执行分析。	write	workspace *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:searchCondition:list	授予权限查询检索条件列表。	list	searchCondition *	-	-
secmaster:searchCondition:create	授予权限创建检索条件。	write	searchCondition *	-	-
secmaster:searchCondition:get	授予权限查询检索条件详情。	read	searchCondition *	-	-
secmaster:searchCondition:update	授予权限更新检索条件。	write	searchCondition *	-	-
secmaster:searchCondition:delete	授予权限删除检索条件。	write	searchCondition *	-	-
secmaster:alertRule:list	授予权限查询告警模型。	list	alertRule *	-	-
secmaster:alertRule:create	授予权限创建告警模型。	write	alertRule *	-	-
secmaster:alertRule:get	授予权限查询告警模型详情。	read	alertRule *	-	-
secmaster:alertRule:update	授予权限修改告警模型。	write	alertRule *	-	-
secmaster:alertRule:delete	授予权限删除告警模型。	write	alertRule *	-	-
secmaster:alertRule:enable	授予权限启用告警模型。	write	alertRule *	-	-
secmaster:alertRule:disable	授予权限停用告警模型。	write	alertRule *	-	-
secmaster:alertRule:listMetrics	授予权限查询告警模型总览。	list	alertRule *	-	-
secmaster:alertRule:createSimulation	授予权限模拟告警模型。	write	alertRule *	-	-
secmaster:alertRuleTemplate:list	授予权限查询告警模板。	list	alertRuleTemplate *	-	-
secmaster:alertRuleT	授予权限查询告	read	alertRul	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
emplate:get	警模板详情。		eTemplate *		
secmaster:alertRuleTemplate:listMetrics	授予权限查询告警模板总览。	list	alertRuleTemplate *	-	-
secmaster:dataclass:create	授予权限创建数据类。	write	dataclass *	-	-
secmaster:dataclass:update	授予权限更新数据类。	write	dataclass *	-	-
secmaster:dataclass:delete	授予权限删除数据类。	write	dataclass *	-	-
secmaster:dataclass:get	授予权限获取数据类详情。	read	dataclass *	-	-
secmaster:dataclass:list	授予权限查询数据类列表。	list	dataclass *	-	-
secmaster:dataclass:createField	授予权限创建字段。	write	dataclass *	-	-
secmaster:dataclass:updateField	授予权限更新字段。	write	dataclass *	-	-
secmaster:dataclass:deleteField	授予权限删除字段。	write	dataclass *	-	-
secmaster:dataclass:getField	授予权限获取字段详情。	read	dataclass *	-	-
secmaster:dataclass:listFields	授予权限查询字段列表。	list	dataclass *	-	-
secmaster:dataclass:getType	授予权限获取类型详情。	read	dataclass *	-	-
secmaster:dataclass:listTypes	授予权限查询类型列表。	list	dataclass *	-	-
secmaster:mapping:update	授予权限更新分类映射状态。	write	mapping *	-	-
secmaster:mapping:list	授予权限搜索分类映射列表。	list	mapping *	-	-
secmaster:mapping:getDatasource	授予权限获取分类映射数据源。	read	mapping *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:mapping:listFunctions	授予权限获取分类映射函数。	list	mapping *	-	-
secmaster:mapping:delete	授予权限删除分类映射。	write	mapping *	-	-
secmaster:mapping:copy	授予权限复制分类映射。	write	mapping *	-	-
secmaster:mapping:createClassifier	授予权限创建分类。	write	mapping *	-	-
secmaster:mapping:updateClassifier	授予权限更新分类。	write	mapping *	-	-
secmaster:mapping:getClassifier	授予权限获取分类信息。	read	mapping *	-	-
secmaster:mapping:deleteClassifier	授予权限删除分类。	write	mapping *	-	-
secmaster:mapping:createMapper	授予权限创建映射。	write	mapping *	-	-
secmaster:mapping:updateMapper	授予权限更新映射。	write	mapping *	-	-
secmaster:mapping:listMappers	授予权限查询映射列表。	list	mapping *	-	-
secmaster:mapping:getMapper	授予权限获取映射信息。	read	mapping *	-	-
secmaster:mapping:deleteMapper	授予权限删除映射。	write	mapping *	-	-
secmaster:layout:listBusinessTypes	授予权限获取布局类型列表。	list	layout *	-	-
secmaster:layout:list	授予权限查询布局列表。	list	layout *	-	-
secmaster:layout:create	授予权限创建布局。	write	layout *	-	-
secmaster:layout:delete	授予权限删除布局。	write	layout *	-	-
secmaster:layout:update	授予权限更新布局。	write	layout *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:layout:get	授予权限查询布局。	read	layout *	-	-
secmaster:layout:createTemplate	授予权限另存为模板。	write	layout *	-	-
secmaster:layout:createField	授予权限创建布局字段。	write	layout *	-	-
secmaster:layout:listFields	授予权限获取布局字段列表。	list	layout *	-	-
secmaster:layout:getField	授予权限获取布局字段详情。	read	layout *	-	-
secmaster:layout:updateField	授予权限更新布局字段。	write	layout *	-	-
secmaster:layout:deleteField	授予权限删除布局字段。	write	layout *	-	-
secmaster:layout:listWizards	授予权限获取页面。	list	layout *	-	-
secmaster:layout:createWizard	授予权限创建页面。	write	layout *	-	-
secmaster:layout:getWizard	授予权限获取页面详情。	read	layout *	-	-
secmaster:layout:deleteWizard	授予权限删除页面。	write	layout *	-	-
secmaster:layout:updateWizard	授予权限更新页面。	write	layout *	-	-
secmaster:catalogue:list	授予权限目录列表查询。	list	catalogue *	-	-
secmaster:catalogue:update	授予权限更新目录。	write	catalogue *	-	-
secmaster:playbook:export	授予权限导出剧本。	read	playbook *	-	-
secmaster:playbook:import	授予权限导入剧本。	write	playbook *	-	-
secmaster:indicator:downloadTemplate	授予权限下载指标模板。	read	indicator *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:indicator:export	授予权限导出指标。	read	indicator *	-	-
secmaster:indicator:import	授予权限导入指标。	write	indicator *	-	-
secmaster:table:list	授予权限查询表。	list	table *	-	-
secmaster:table:create	授予权限创建表。	write	table *	-	-
secmaster:table:get	授予权限查询表详情。	read	table *	-	-
secmaster:table:update	授予权限修改表。	write	table *	-	-
secmaster:table:delete	授予权限删除表。	write	table *	-	-
secmaster:table:createLock	授予权限锁止表。	write	table *	-	-
secmaster:table:deleteLock	授予权限解锁表。	write	table *	-	-
secmaster:table:listMetrics	授予权限查询表总览。	list	table *	-	-
secmaster:table:updateSchema	授予权限设计表。	write	table *	-	-
secmaster:workspace:listTags	授予权限查询资源标签。	list	workspace *	-	-
secmaster:workspace:listResourcesByTag	授予权限查询资源实例列表。	list	workspace *	-	-
secmaster:workspace:listTagsForResource	授予权限查询资源标签。	list	workspace *	-	-
secmaster:workspace:createTags	授予权限批量添加资源标签。	write	workspace *	-	-
secmaster:workspace:deleteTags	授予权限批量删除资源标签。	write	workspace *	-	-
secmaster:workspace:updateTag	授予权限更新标签值。	write	workspace *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:workflow:export	授予权限导出流程。	read	workflow *	-	-
secmaster:workflow:import	授予权限导入流程。	write	workflow *	-	-
secmaster:alert:import	授予权限导入告警。	write	alert *	-	-
secmaster:alert:export	授予权限导出告警。	read	alert *	-	-
secmaster:alert:downloadTemplate	授予权限下载告警模板。	read	alert *	-	-
secmaster:incident:import	授予权限导入事件。	write	incident *	-	-
secmaster:incident:export	授予权限导出事件。	read	incident *	-	-
secmaster:incident:downloadTemplate	授予权限下载事件模板。	read	incident *	-	-
secmaster:dataclass:bindLayout	授予权限绑定数据类类型与布局关联。	write	dataclass *	-	-
secmaster:dataclass:createType	授予权限创建自定义数据类型。	write	dataclass *	-	-
secmaster:dataclass:updateType	授予权限更新自定义数据类型。	write	dataclass *	-	-
secmaster:dataclass:deleteType	授予权限删除自定义数据类型。	write	dataclass *	-	-
secmaster:dataclass:enableType	授予权限启用数据类类型。	write	dataclass *	-	-
secmaster:preference:create	授予权限设置用户偏好。	write	-	-	-
secmaster:preference:get	授予权限获取用户偏好。	read	-	-	-
secmaster:preference:delete	授予权限删除用户偏好。	write	-	-	-
secmaster:preference:	授予权限更新用	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
update	户偏好。				
secmaster:preference:list	授予权限搜索用户偏好。	list	-	-	-
secmaster:metric:list	授予权限获取指标列表。	list	metric *	-	-
secmaster:metric:create	授予权限创建指标。	write	metric *	-	-
secmaster:metric:get	授予权限获取指标详情。	read	metric *	-	-
secmaster:metric:delete	授予权限删除指标。	write	metric *	-	-
secmaster:metric:update	授予权限更新指标。	write	metric *	-	-
secmaster:module:list	授予权限获取模块列表。	list	-	-	-
secmaster:module:create	授予权限创建模块。	write	-	-	-
secmaster:module:get	授予权限获取模块详情。	read	-	-	-
secmaster:module:delete	授予权限删除模块。	write	-	-	-
secmaster:module:update	授予权限更新模块。	write	-	-	-
secmaster:vulnerability:downloadTemplate	授予权限下载漏洞模板。	read	vulnerability *	-	-
secmaster:vulnerability:import	授予权限导入漏洞数据。	write	vulnerability *	-	-
secmaster:policy:list	授予权限查询策略列表。	list	policy *	-	-
secmaster:policy:create	授予权限创建策略。	write	policy *	-	-
secmaster:policy:get	授予权限查询策略详情。	read	policy *	-	-
secmaster:policy:upd	授予权限更新策	write	policy *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
ate	略。				
secmaster:policy:delete	授予权限删除策略。	write	policy *	-	-
secmaster:policy:batchDelete	授予权限批量删除策略。	write	policy *	-	-
secmaster:note:list	授予权限查询评论列表。	list	-	-	-
secmaster:note:create	授予权限创建评论。	write	-	-	-
secmaster:note:delete	授予权限删除评论。	write	-	-	-
secmaster:secureScore:update	授予权限更新安全评分。	write	-	-	-
secmaster:baseline:list	授予权限查看基线检查结果。	list	baseline *	-	-
secmaster:baseline:export	授予权限导出基线检查结果。	read	baseline *	-	-
secmaster:baseline:import	授予权限导入基线检查结果。	write	baseline *	-	-
secmaster:baseline:downloadTemplate	授予权限下载基线检查模板。	read	baseline *	-	-
secmaster:resource:get	授予权限获取资源详情。	read	resource *	-	-
secmaster:resource:getRelations	授予权限获取资源拓扑。	read	resource *	-	-
secmaster:resource:update	授予权限更新资源。	write	resource *	-	-
secmaster:resource:batchUpdate	授予权限批量更新资源。	write	resource *	-	-
secmaster:resource:batchDelete	授予权限批量删除资源。	write	resource *	-	-
secmaster:resource:export	授予权限导出资源。	read	resource *	-	-
secmaster:resource:ge	授予权限查看资	read	resource	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
tSyncStatus	源同步状态。		*		
secmaster:resource:sync	授予权限同步资源。	write	resource *	-	-
secmaster:guide:get	授予权限查询用户指引。	read	-	-	-
secmaster:guide:create	授予权限创建用户指引。	write	-	-	-
secmaster:shipper:list	授予权限获取投递信息列表。	list	shipper *	-	-
secmaster:shipper:create	授予权限创建数据投递。	write	shipper *	-	-
secmaster:shipper:delete	授予权限删除投递信息。	write	shipper *	-	-
secmaster:shipper:createAuthorization	授予权限投递授权。	write	shipper *	-	-
secmaster:shipper:listAuthorizations	授予权限获取投递授权信息列表。	list	shipper *	-	-
secmaster:shipper:handleAuthorization	授予权限授权处理。	write	shipper *	-	-
secmaster:shipper:get	授予权限获取投递规则详情。	read	shipper *	-	-
secmaster:shipper:resume	授予权限启动投递。	write	shipper *	-	-
secmaster:shipper:pause	授予权限投递挂起。	write	shipper *	-	-
secmaster:shipper:getDelegateAuth	授予权限获取委托权限。	read	shipper *	-	-
secmaster:shipper:createDelegateAuth	授予权限创建委托权限。	write	shipper *	-	-
secmaster:shipper:retryAuthorization	授予权限重新授权。	write	shipper *	-	-
secmaster:shipper:retry	授予权限重新投递。	write	shipper *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:adHocQuery:create	授予权限执行analysis 语句。	write	-	-	-
secmaster:adHocQuery:get	授予权限查询语句结果。	read	-	-	-
secmaster:adHocQuery:delete	授予权限关闭查询操作。	write	-	-	-
secmaster:dataTransformation:list	授予权限查询数据转移任务。	list	-	-	-
secmaster:dataTransformation:get	授予权限查询数据转移任务详情。	read	-	-	-
secmaster:dataTransformation:enable	授予权限启用数据转移任务。	write	-	-	-
secmaster:dataTransformation:create	授予权限创建数据转移任务。	write	-	-	-
secmaster:dataTransformation:delete	授予权限删除数据转移任务。	write	-	-	-
secmaster:dataTransformation:update	授予权限更新数据转移任务。	write	-	-	-

表3-161 SecMaster 支持的授权项 Part2

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:dataTransformation:listMetrics	授予权限查询数据转移任务指标。	read	-	-	-
secmaster:dataTransformation:disable	授予权限停用数据转移任务。	write	-	-	-
secmaster:analysisScript:list	授予权限查询分析脚本。	list	-	-	-
secmaster:analysisScript:create	授予权限创建分析脚本。	write	-	-	-
secmaster:analysisScri	授予权限查询分析	rea	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
pt:get	脚本详情。	d			
secmaster:analysisScript:update	授予权限更新分析脚本。	write	-	-	-
secmaster:analysisScript:delete	授予权限删除分析脚本。	write	-	-	-
secmaster:codeSegment:list	授予权限查询代码片段。	list	-	-	-
secmaster:codeSegment:create	授予权限创建代码片段。	write	-	-	-
secmaster:codeSegment:get	授予权限查询代码片段详情。	read	-	-	-
secmaster:codeSegment:update	授予权限更新代码片段。	write	-	-	-
secmaster:codeSegment:delete	授予权限删除代码片段。	write	-	-	-
secmaster:retrieveScript:list	授予权限查询检索脚本。	list	-	-	-
secmaster:retrieveScript:create	授予权限创建检索脚本。	write	-	-	-
secmaster:retrieveScript:get	授予权限查询检索脚本详情。	read	-	-	-
secmaster:retrieveScript:update	授予权限更新检索脚本。	write	-	-	-
secmaster:retrieveScript:delete	授予权限删除检索脚本。	write	-	-	-
secmaster:pipe:updateSchema	授予权限修改管道字段。	write	pipe *	-	-
secmaster:node:create	授予权限新建节点。	write	-	-	-
secmaster:node:monitor	授予权限监控节点信息。	write	-	-	-
secmaster:node:updateTaskNodeStatus	授予权限修改节点任务状态。	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:node:taskQueueDetail	授予权限查询节点任务详情。	read	-	-	-
secmaster:analysisScript:export	授予权限导出分析脚本。	read	analysisScript *	-	-
secmaster:analysisScript:import	授予权限导入分析脚本。	write	analysisScript *	-	-
secmaster:cloudLog:create	授予权限保存云服务日志订阅配置。	write	-	-	-
secmaster:cloudLog:delete	授予权限删除云服务日志订阅配置。	write	-	-	-
secmaster:cloudLog:list	授予权限获取云服务日志订阅配置。	list	-	-	-
secmaster:cloudLog:listResourceConfig	授予权限查询资产订阅配置。	list	workspace *	-	-
secmaster:collector:createConfig	授予权限保存云服务日志订阅配置。	write	-	-	-
secmaster:collector:listConfig	授予权限获取云服务日志订阅配置。	list	-	-	-
secmaster:collectorChannel:create	授予权限创建采集通道。	write	collectorChannel *	-	-
secmaster:collectorChannel:createOperation	授予权限控制采集通道。	write	collectorChannel *	-	-
secmaster:collectorChannel:delete	授予权限删除采集通道。	write	collectorChannel *	-	-
secmaster:collectorChannel:get	授予权限获取采集通道详情。	read	collectorChannel *	-	-
secmaster:collectorChannel:list	授予权限获取采集通道列表。	list	collectorChannel *	-	-
secmaster:collectorChannel:listInstances	授予权限获取采集通道实例列表。	list	collectorChannel *	-	-
secmaster:collectorChannel:listNodes	授予权限获取采集通道节点列表。	list	collectorChannel *	-	-
secmaster:collectorCh	授予权限更新采集	wri	collectorC	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
annel:update	通道。	te	hannel *		
secmaster:collectorChannelGroup:create	授予权限创建采集通道分组。	write	collectorChannelGroup *	-	-
secmaster:collectorChannelGroup:delete	授予权限删除采集通道分组。	write	collectorChannelGroup *	-	-
secmaster:collectorChannelGroup:list	授予权限获取采集通道分组列表。	list	collectorChannelGroup *	-	-
secmaster:collectorChannelGroup:update	授予权限更新采集通道分组列表。	write	collectorChannelGroup *	-	-
secmaster:collectorConnection:create	授予权限创建采集器连接。	write	collectorConnection *	-	-
secmaster:collectorConnection:delete	授予权限删除采集器连接。	write	collectorConnection *	-	-
secmaster:collectorConnection:get	授予权限获取采集器连接详情。	read	collectorConnection *	-	-
secmaster:collectorConnection:list	授予权限获取采集器连接列表。	list	collectorConnection *	-	-
secmaster:collectorConnection:update	授予权限更新采集器连接。	write	collectorConnection *	-	-
secmaster:collectorNode:list	授予权限获取采集节点列表。	list	workspace *	-	-
secmaster:collectorParser:create	授予权限创建采集解析器。	write	collectorParser *	-	-
secmaster:collectorParser:delete	授予权限删除采集解析器。	write	collectorParser *	-	-
secmaster:collectorParser:export	授予权限导出采集解析器。	read	collectorParser *	-	-
secmaster:collectorParser:get	授予权限获取采集解析器详情。	read	collectorParser *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:collectorParser:list	授予权限获取采集解析器列表。	list	collectorParser *	-	-
secmaster:collectorParser:listTemplates	授予权限获取采集解析器模板列表。	list	collectorParser *	-	-
secmaster:component:get	授予权限获取组件详情。	read	component *	-	-
secmaster:component:list	授予权限获取组件列表。	list	component *	-	-
secmaster:component:listConfigurationVersions	授予权限获取组件历史版本的配置数据。	list	component *	-	-
secmaster:component:listConfigurations	授予权限获取组件配置列表。	list	component *	-	-
secmaster:component:listRunningNodes	授予权限获取组件运行节点列表。	list	component *	-	-
secmaster:component:listTemplates	授予权限获取组件模板列表。	list	component *	-	-
secmaster:component:updateConfigurations	授予权限更新组件配置。	write	component *	-	-
secmaster:node:delete	授予权限删除节点信息。	write	node *	-	-
secmaster:node:list	授予权限查询节点信息列表。	list	node *	-	-
secmaster:node:update	授予权限更新节点信息。	write	node *	-	-
secmaster:table:createConsumption	授予权限创建表数据消费。	write	table *	-	-
secmaster:table:deleteConsumption	授予权限删除表数据消费。	write	table *	-	-
secmaster:table:getConsumption	授予权限获取表数据消费信息。	read	table *	-	-
secmaster:accountAgency:list	授予权限查询账号纳管信息。	read	accountAgency *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必要）	条件键	别名
secmaster:accountAgency:create	授予权限创建账号纳管。	write	accountAgency *	-	-
secmaster:accountAgency:get	授予权限获取账号纳管信息。	read	accountAgency *	-	-
secmaster:accountAgency:update	授予权限更新账号纳管。	write	accountAgency *	-	-
secmaster:accountAgency:delete	授予权限批量解除账号纳管。	write	accountAgency *	-	-

SecMaster 的 API 通常对应着一个或多个授权项。表 3-162 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-162 API 与操作项的关系

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}	secmaster:playbook:get	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks	secmaster:playbook:create	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}	secmaster:playbook:delete	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}	secmaster:playbook:update	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks	secmaster:playbook:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/statistics	secmaster:playbook:getStatistics	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}/monitor	secmaster:playbook:getMonitor	-
POST	secmaster:playbook:copyVers	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/clone	ion	
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/approve	secmaster:playbook:approve	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/approval	secmaster:playbook:listApproves	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances	secmaster:playbook:listInstances	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/auditlogs	secmaster:playbook:getInstanceAuditlog	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions	secmaster:playbook:createVersion	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/rules	secmaster:playbook:createVersionRule	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/actions	secmaster:playbook:createVersionAction	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}	secmaster:playbook:getVersion	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/rules/{rule_id}	secmaster:playbook:getVersionRule	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}	secmaster:playbook:deleteVersion	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/rules/{rule_id}	secmaster:playbook:deleteVersionRule	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/actions/{action_id}	secmaster:playbook:deleteVersionAction	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}	secmaster:playbook:updateVersion	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/rules/{rule_id}	secmaster:playbook:updateVersionRule	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/actions/{action_id}	secmaster:playbook:updateVersionAction	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}/versions	secmaster:playbook:listVersions	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/actions	secmaster:playbook:listVersionActions	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}	secmaster:playbook:getInstance	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}/topology	secmaster:playbook:getInstanceTopology	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}/operation	secmaster:playbook:operateInstance	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows	secmaster:workflow:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}	secmaster:workflow:get	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}	secmaster:workflow:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/workspacesPOST /v1/{project_id}/workspaces/{workspace_id}/soc/workflows	secmaster:workflow:create	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}	secmaster:workflow:update	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions	secmaster:workflow:listVersions	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions/{version_id}	secmaster:workflow:getVersion	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions/{version_id}	secmaster:workflow:deleteVersion	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions	secmaster:workflow:createVersion	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions/{version_id}	secmaster:workflow:updateVersion	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions/{version_id}/approval	secmaster:workflow:approveVersion	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/validation	secmaster:workflow:validate	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions/{version_id}/debug/result	secmaster:workflow:simulate	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/instances/{instance_id}/topology	secmaster:workflow:getInstance	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/instances	secmaster:workflow:operateInstance	-
GET	secmaster:connection:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/workspaces/{workspace_id}/soc/assetcredentials		
POST /v1/{project_id}/workspaces/{workspace_id}/soc/assetcredentials	secmaster:connection:create	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/assetcredentials/{asset_id}	secmaster:connection:get	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/assetcredentials/{asset_id}	secmaster:connection:delete	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/assetcredentials/{asset_id}	secmaster:connection:update	-
GET /v1/{project_id}/workspaces	secmaster:workspace:list	-
POST /v1/{project_id}/workspaces	secmaster:workspace:create	-
PUT /v1/{project_id}/workspaces/{workspace_id}	secmaster:workspace:update	-
GET /v1/{project_id}/workspaces/v1/{project_id}/workspaces/{workspace_id}	secmaster:workspace:get	-
DELETE /v1/{project_id}/workspaces/{workspace_id}	secmaster:workspace:delete	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/tasks	secmaster:task:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/tasks	secmaster:task:create	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/tasks/{task_id}	secmaster:task:update	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/tasks/{task_id}	secmaster:task:get	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/{indicator_id}	secmaster:indicator:get	-
POST	secmaster:indicator:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/workspaces/{workspace_id}/soc/indicators		
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/{indicator_id}	secmaster:indicator:update	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/{indicator_id}	secmaster:indicator:delete	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/search	secmaster:indicator:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/types	secmaster:indicator:listTypes	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/types/layout	secmaster:indicator:bindLayout	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/{alert_id}	secmaster:alert:get	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts	secmaster:alert:create	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/{alert_id}	secmaster:alert:update	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/search	secmaster:alert:list	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/alerts	secmaster:alert:delete	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/batch-order	secmaster:alert:batchOrders	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types	secmaster:alert:listTypes	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types/category	secmaster:alert:listCategories	-
POST	secmaster:alert:createType	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types		
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types/{dataclass_type_id}	secmaster:alert:updateType	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types	secmaster:alert:deleteType	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types/enable	secmaster:alert:enableType	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types/layout	secmaster:alert:bindLayout	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/{incident_id}	secmaster:incident:get	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents	secmaster:incident:create	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/{incident_id}	secmaster:incident:update	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/search	secmaster:incident:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types	secmaster:incident:listTypes	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/incidents	secmaster:incident:delete	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types/category	secmaster:incident:listCategories	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types	secmaster:incident:createType	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types/{dataclass_type_id}	secmaster:incident:updateType	-
DELETE	secmaster:incident:deleteType	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types		
POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/incidents/enable	secmaster:incident:enableType	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types/layout	secmaster:incident:bindLayout	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}	secmaster:dataobject:createRelation	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}	secmaster:dataobject:deleteRelation	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}/search	secmaster:dataobject:listRelation	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerability/search	secmaster:vulnerability:listGroup	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerability/{vul_id}	secmaster:vulnerability:getGroup	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerability/export	secmaster:vulnerability:exportGroup	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types	secmaster:vulnerability:listType	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types/layout	secmaster:vulnerability:bindLayout	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types	secmaster:vulnerability:createType	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types/{dataclass_type_id}	secmaster:vulnerability:updateType	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types	secmaster:vulnerability:deleteType	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types/enable	secmaster:vulnerability:enableType	-
DELETE /v1/{project_id}/subscriptions/orders	secmaster:subscription:deletePostPaidOrder	-
POST /v1/{project_id}/subscriptions/orders	secmaster:subscription:createPostPaidOrder	-
POST /v1/{project_id}/subscriptions/orders/{order_id}	secmaster:subscription:createPrePaidOrder	-
GET /v1/{project_id}/subscriptions/version	secmaster:subscription:getVersion	-
GET /v1/{project_id}/workspaces/{workspace_id}/sa/metrics/{metric_id}/result	secmaster:metric:getResult	-
POST /v1/{project_id}/workspaces/{workspace_id}/sa/metrics/results	secmaster:metric:listResults	-
POST /v1/{project_id}/workspaces/{workspace_id}/sa/metrics/hits	secmaster:metric:listHits	-
GET /v1/{project_id}/agency	secmaster:agency:get	-
POST /v1/{project_id}/agency	secmaster:agency:create	-
GET /v1/{project_id}/workspaces/{workspace_id}/resource-statistics	secmaster:resource:getStatistics	-
GET /v1/{project_id}/workspaces/{workspace_id}/resources	secmaster:resource:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/sa/resources/import	secmaster:resource:import	-
GET /v1/{project_id}/workspaces/{workspace_id}/sa/resource/template	secmaster:resource:getTemplate	-
GET /v1/{project_id}/workspaces/{workspace_id}/sa/reports	secmaster:report:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/workspaces/{workspace_id}/sa/reports/{report_id}	secmaster:report:get	-
POST /v1/{project_id}/workspaces/{workspace_id}/sa/reports	secmaster:report:create	-
PUT /v1/{project_id}/workspaces/{workspace_id}/sa/reports/{report_id}	secmaster:report:update	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/sa/reports/{report_id}	secmaster:report:delete	-
POST /v1/{project_id}/workspaces/{workspace_id}/sa/vulnerability/read-status	secmaster:emergencyVulnerability:updateReadStatus	-
GET /v1/{project_id}/workspaces/{workspace_id}/sa/vulnerability/list	secmaster:emergencyVulnerability:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/sa/vulnerability/export	secmaster:emergencyVulnerability:export	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces	secmaster:dataspace:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces	secmaster:dataspace:create	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces/{dataspace_id}	secmaster:dataspace:get	-
PUT /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces/{dataspace_id}	secmaster:dataspace:update	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces/{dataspace_id}	secmaster:dataspace:delete	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/pipes	secmaster:pipe:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/pipes	secmaster:pipe:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}	secmaster:pipe:get	-
PUT /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}	secmaster:pipe:update	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}	secmaster:pipe:delete	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}/index	secmaster:pipe:getIndex	-
PUT /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}/index	secmaster:pipe:updateIndex	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}/consumption	secmaster:pipe:getConsumption	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}/consumption	secmaster:pipe:createConsumption	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}/consumption	secmaster:pipe:deleteConsumption	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/search/logs	secmaster:search:listLogs	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/search/histograms	secmaster:search:listHistograms	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/search/analysis	secmaster:search:createAnalysis	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/search/conditions	secmaster:searchCondition:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/search/conditions	secmaster:searchCondition:create	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/search/conditions/{condition_id}	secmaster:searchCondition:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/workspaces/{workspace_id}/siem/search/conditions/{condition_id}	secmaster:searchCondition:update	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/search/conditions/{condition_id}	secmaster:searchCondition:delete	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules	secmaster:alertRule:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules	secmaster:alertRule:create	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/{rule_id}	secmaster:alertRule:get	-
PUT /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/{rule_id}	secmaster:alertRule:update	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules	secmaster:alertRule:delete	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/enable	secmaster:alertRule:enable	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/disable	secmaster:alertRule:disable	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/metrics	secmaster:alertRule:listMetrics	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/simulation	secmaster:alertRule:createSimulation	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/templates	secmaster:alertRuleTemplate:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/templates/{template_id}	secmaster:alertRuleTemplate:get	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/templates/metrics	secmaster:alertRuleTemplate:listMetrics	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses	secmaster:dataclass:create	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}	secmaster:dataclass:update	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}	secmaster:dataclass:delete	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}	secmaster:dataclass:get	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses	secmaster:dataclass:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields	secmaster:dataclass:createField	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields/{field_id}	secmaster:dataclass:updateField	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields	secmaster:dataclass:deleteField	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields/{field_id}	secmaster:dataclass:getField	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields	secmaster:dataclass:listFields	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/types/{dataclass_type_id}	secmaster:dataclass:getType	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/types	secmaster:dataclass:listTypes	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/{mapping_id}/status	secmaster:mapping:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/search	secmaster:mapping:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/data-source	secmaster:mapping:getDatasource	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/functions	secmaster:mapping:listFunctions	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/{mapping_id}	secmaster:mapping:delete	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/{mapping_id}/clone	secmaster:mapping:copy	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/classifiers	secmaster:mapping:createClassifier	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/classifiers/{classifier_id}	secmaster:mapping:updateClassifier	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/classifiers/{classifier_id}	secmaster:mapping:getClassifier	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/classifiers/{classifier_id}	secmaster:mapping:deleteClassifier	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/mappers	secmaster:mapping:createMapper	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/mappers/{mapper_id}	secmaster:mapping:updateMapper	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/mappers/search	secmaster:mapping:listMappers	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/mappers/{mapper_id}	secmaster:mapping:getMapper	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/mappers/{mapper_id}	secmaster:mapping:deleteMapper	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/business-type	secmaster:layout:listBusinessTypes	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/search	secmaster:layout:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/layouts	secmaster:layout:create	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/layouts	secmaster:layout:delete	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}	secmaster:layout:update	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}	secmaster:layout:get	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/template	secmaster:layout:createTemplate	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/fields	secmaster:layout:createField	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/fields	secmaster:layout:listFields	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/fields/{field_id}	secmaster:layout:getField	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/fields/{field_id}	secmaster:layout:updateFiled	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/fields	secmaster:layout:deleteField	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/wizards	secmaster:layout:listWizards	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/wizards	secmaster:layout:createWizard	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/wizards/{wizard_id};/v1/{project_id}/workspaces/{workspace_id}/soc/layouts/wizards	secmaster:layout:getWizard	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/wizards/{wizard_id}	secmaster:layout:deleteWizard	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/wizards	secmaster:layout:updateWizard	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/catalogues/search;/v1/{project_id}/workspaces/{workspace_id}/soc/catalogues	secmaster:catalogue:list	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/catalogues/{catalogue_id}	secmaster:catalogue:update	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/export	secmaster:playbook:export	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/import	secmaster:playbook:import	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/template/download	secmaster:indicator:downloadTemplate	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/export	secmaster:indicator:export	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/import	secmaster:indicator:import	-
GET /v2/{project_id}/workspaces/{workspace_id}/siem/tables	secmaster:table:list	-
-POST /v2/{project_id}/workspaces/{workspace_id}/siem/tables	secmaster:table:create	-
GET /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}	secmaster:table:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}	secmaster:table:update	-
DELETE /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}	secmaster:table:delete	-
POST /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}/lock	secmaster:table:createLock	-
DELETE /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}/lock	secmaster:table:deleteLock	-
GET /v2/{project_id}/workspaces/{workspace_id}/siem/tables/metrics	secmaster:table:listMetrics	-
PUT /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}/schema	secmaster:table:updateSchema	-

资源类型（Resource）

资源类型（Resource）表示 SCP 所作用的资源。某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的 SCP 语句中指定该资源的 URN，SCP 仅作用于此资源；如未指定，Resource 默认为“*”，则 SCP 将应用到所有资源。您也可以在 SCP 中设置条件，从而指定资源类型。

SecMaster 定义了以下可以在 SCP 的 Resource 元素中使用的资源类型。

表3-163 SecMaster 支持的资源类型

资源类型	URN
workspace	secmaster:<region>:<account-id>:workspace:<workspace-id>
playbook	secmaster:<region>:<account-id>:playbook:<workspace-id>/<playbook-id>
workflow	secmaster:<region>:<account-id>:workflow:<workspace-id>/<workflow-id>
connection	secmaster:<region>:<account-id>:connection:<workspace-id>/<connection-id>
task	secmaster:<region>:<account-id>:task:<workspace-id>/<task-id>
indicator	secmaster:<region>:<account-id>:indicator:<workspace-

 版权所有 © 华为云计算技术有限公司

资源类型	URN
	id>/<indicator-id>
alert	secmaster:<region>:<account-id>:alert:<workspace-id>/<alert-id>
incident	secmaster:<region>:<account-id>:incident:<workspace-id>/<incident-id>
dataobject	secmaster:<region>:<account-id>:dataobject:<workspace-id>/<dataobject-id>
metric	secmaster:<region>:<account-id>:metric:<workspace-id>/<metric-id>
resource	secmaster:<region>:<account-id>:resource:<workspace-id>/<resource-id>
report	secmaster:<region>:<account-id>:report:<workspace-id>/<report-id>
emergencyVulnerability	secmaster:<region>:<account-id>:emergencyVulnerability:<workspace-id>/<emergency-vulnerability-id>
dataspace	secmaster:<region>:<account-id>:dataspace:<workspace-id>/<dataspace-id>
pipe	secmaster:<region>:<account-id>:pipe:<workspace-id>/<pipe-id>
alertRule	secmaster:<region>:<account-id>:alertRule:<workspace-id>/<alertRule-id>
vulnerability	secmaster:<region>:<account-id>:vulnerability:<workspace-id>/<vulnerability-id>
alertRuleTemplate	secmaster:<region>:<account-id>:alertRuleTemplate:<workspace-id>/<alertRuleTemplate-id>
searchCondition	secmaster:<region>:<account-id>:searchCondition:<workspace-id>/<searchCondition-id>
dataclass	secmaster:<region>:<account-id>:dataclass:<workspace-id>/<dataclass-id>
mapping	secmaster:<region>:<account-id>:mapping:<workspace-id>/<mapping-id>
layout	secmaster:<region>:<account-id>:layout:<workspace-id>/<layout-id>
catalogue	secmaster:<region>:<account-id>:catalogue:<workspace-id>/<catalogue-id>
table	secmaster:<region>:<account-id>:table:<workspace-id>/<table-id>
policy	secmaster:<region>:<account-id>:policy:<workspace-id>/<policy-id>

 版权所有 © 华为云计算技术有限公司

资源类型	URN
baseline	secmaster:<region>:<account-id>:baseline:<workspace-id>/<baseline-id>
shipper	secmaster:<region>:<account-id>:shipper:<workspace-id>/<shipper-id>
analysisScript	secmaster:<region>:<account-id>:analysisScript:<workspace-id>/<analysisScript-id>
collectorChannel	secmaster:<region>:<account-id>:collectorChannel:<workspace-id>/<collectorChannel-id>
collectorChannelGroup	secmaster:<region>:<account-id>:collectorChannelGroup:<workspace-id>/<collectorChannelGroup-id>
collectorConnection	secmaster:<region>:<account-id>:collectorConnection:<workspace-id>/<collectorConnection-id>
collectorParser	secmaster:<region>:<account-id>:collectorParser:<workspace-id>/<collectorParser-id>
component	secmaster:<region>:<account-id>:component:<workspace-id>/<component-id>
node	secmaster:<region>:<account-id>:node:<workspace-id>/<node-id>
accountAgency	secmaster:<region>:<account-id>:accountAgency:<accountAgency-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 *secmaster*）仅适用于对应服务的操作，详情请参见表 3-164。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。

 版权所有 © 华为云计算技术有限公司

- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

SecMaster 支持的服务级条件键

SecMaster 定义了以下可以在身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

SecMaster 服务不支持在 SCP 中的条件键中配置服务级的条件键。

表3-164 SecMaster 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
secmaster:TargetRegion	字符串	多值	仅 Action secmaster:workspace:createAgency 支持该服务级条件键。根据请求中的托管空间的 region 属性过滤条件键 secmaster:TargetRegion 指定的目标区域（Region）。

条件键示例

- secmaster:TargetRegion

  示例：表示不允许 region id 为 1 的 region 创建空间托管。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "secmaster:workspace:createAgency"
      ],
      "Condition": {
        "ForAllValues:StringEquals": {
          "secmaster:TargetRegion": [
            "region_id_1"
          ]
        }
      }
    }
  ]
}
```

 版权所有 © 华为云计算技术有限公司

3.8 大数据

3.8.1 云搜索服务 CSS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “**访问级别**”列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “**资源类型**”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 CSS 定义的资源类型的详细信息请参见资源类型（Resource）。
- “**条件键**”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 CSS 定义的条件键的详细信息请参见条件（Condition）。
- “**别名**”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 CSS 的相关操作。

 版权所有 © 华为云计算技术有限公司

表3-165 CSS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
css:VPCEndpoint:updateWhitelist	授予权限更新已存在的终端节点白名单。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:log:updateBackupPolicy	授予权限日志备份修改或删除。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:snapshot:setSnapshotPolicy	授予权限操作备份策略。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:snapshot:getSnapshotPolicy	授予权限查询备份策略。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:snapshot:restore	授予权限恢复快照。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:snapshot:create	授予权限创建快照。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:publicIPAddress:associates	授予权限开启或关闭公网访问。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:publicIPAddress:setAccessControl	授予权限对白名单列表进行操作。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				key>	
css:tag:get	授予权限查询资源标签。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:publicIPAddress:modifyBandwidth	授予权限修改带宽大小。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:VPCEndpoint:enableOrDisable	授予权限创建或删除VPCEP。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:log:getBasicConfigurations	授予权限日志基础配置查询。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:snapshot:list	授予权限查看快照列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:log:list	授予权限查看日志。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:snapshot:setSnapshotContiguration	授予权限设置快照基础配置。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:listFlavors	授予权限查询规格 ID 列表。	list	-	-	css:cluster:showFlavor

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
css:cluster:listDiskType	授予权限列举可用磁盘类型。	list	-	-	-
css:tag:list	授予权限查询项目标签。	list	cluster *	-	-
css:VPCEndpoint:manageConnection	授予权限操作终端节点的连接。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:log:listJob	授予权限查询作业列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:downloadCert	授予权限获取证书内容。	read	-	-	-
css:cluster:get	授予权限查询集群详情。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	css:cluster:getInstance
css:snapshot:enableAtomaticSnapsot	授予权限设置快照自动备份的基础配置。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:snapshot:delete	授予权限删除指定快照。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:IKThesaurus:get	授予权限查看自定义词库配置。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:restart	授予权限重启ElasticSearch	write	cluster *	• g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	集群。			• g:ResourceTag/<tag-key>	
css:cluster:modifySecurityGroup	授予权限修改集群安全组。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:configurations:list	授予权限查询获取参数配置的任务操作列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:delete	授予权限删除集群。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:modifySpecifications	授予权限修改集群规格。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:list	授予权限列举集群信息。	list	cluster *	-	css:cluster:getInstances
css:cluster:scaleOut	授予权限扩容集群。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:IKThesaurus:load	授予权限加载自定义词库。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:configurations:modify	授予权限更新参数配置。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
css:configurations:get	授予权限列举参数配置列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:IKThesaurus:delete	授予权限删除词库。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:expand	授予权限扩容实例的数量和存储容量。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:snapshot:disableSnapshotFuction	授予权限关闭集群快照功能。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:upgradeCluster	授予权限升级集群或节点替换。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:VPCEndpoint:listConnection	授予权限查询VPCEP的连接。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:scaleIn	授予权限对集群缩容。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:log:setBasicConfigurations	授予权限日志基础配置设置。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
css:tag:addOrDelete	授予权限批量添加删除资源标签。	tagging	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
css:publicKibana:close	授予权限关闭公网访问。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:tag:edit	授予权限修改集群标签。	tagging	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
css:cluster:create	授予权限创建集群。	write	cluster *	-	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
css:cluster:toPeriod	授予权限对集群转包周期。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:modifyName	授予权限修改集群名称。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
css:log:backup	授予权限对日志备份。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:closeLogSetting	授予权限关闭日志功能。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	css:log:enableOrDisableLogFunction
css:cluster:openLogSetting	授予权限开启日志功能。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	css:log:enableOrDisableLogFunction
css:cluster:modifyPassword	授予权限修改集群密码。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:publicIPAddress:disassociates	授予权限解绑公网。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:publicKibana:open	授予权限绑定公网。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:tag:delete	授予权限删除标签。	tagging	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	g:TagKeys	
css:cluster:shrinkNodes	授予权限指定节点缩容。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				key>	
css:cluster:changeMode	授予权限修改安全模式。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:addIndependenceNodes	授予权限添加独立master,client。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:rollingReboot	授予权限滚动重启ElasticSearch集群。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	css:cluster:rollingRestart
css:logstash:listActions	授予权限查询操作记录。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:uploadCerts	授予权限上传证书。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:deleteCerts	授予权限删除证书。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:listCerts	授予权限查询证书列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	css:cluster:getCertsList
css:cluster:getCertsDetail	授予权限查询证书详情。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				key>	
css:logstash:deleteConfTemplate	授予权限删除自定义模板。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:logstash:listConfigTemplate	授予权限查询模板列表。	list	-	-	css:logstash:configListTemplate
css:logstash:confStop	授予权限停止或热停止pipeline 迁移数据。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:logstash:checkConnection	授予权限连通性测试。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:logstash:confDelete	授予权限删除配置文件。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:logstash:confStart	授予权限启动或热启动pipeline 迁移数据。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:logstash:getConfDetail	授予权限用于查询配置文件内容。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:azmigrate	授予权限进行可用区切换。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
css:logstash:confUpdate	授予权限更新配置文件。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:logstash:listPipelines	授予权限查询pipeline 列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:retryAction	授予权限重试该任务或终止该任务的影响。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:logstash:listConfs	授予权限查询配置文件列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:logstash:configFavorites	授予权限添加到自定义模板。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:listUpgradeCluster	授予权限获取升级镜像 id 及升级详情。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:logstash:submitConf	授予权限创建配置文件。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:plugin:list	授予权限查询集群插件列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
css:plugin:getOperationRecords	授予权限查询插件的操作记录。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:plugin:delete	授予权限删除插件。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:plugin:installOrUninstall	授予权限安装或卸载插件。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:plugin:upload	授予权限上传插件。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:plugin:getDefault	授予权限查询默认插件。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:getAgencies	授予权限获取代理。	read	-	-	-
css:cluster:modifyRoute	授予权限修改集群路由。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:getRoutes	授予权限获取集群路由。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:logstash:actionList	授予权限查询集群任务列	list	cluster *	• g:EnterpriseProjectId • g:ResourceT	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	表。			ag/<tag-key>	
css:cluster:createUserInfo	授予权限查创建用户信息。	write	cluster *	-	-
css:VPCEndpoint:modifyConnections	授予权限修改连接大小。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:queryNeedDeleteInstances	授予权限查询需要删除的节点。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:queryKey	授予权限获得密钥。	read	-	-	-
css:cluster:queryKeys	授予权限获得密钥列表。	list	-	-	-
css:cluster:getPubliczonePice	授予权限获取带宽价格。	read	cluster *	-	-
css:datastore:get	授予权限获取数据引擎。	read	cluster *	-	-
css:datastore:list	授予权限获取数据引擎列表。	list	cluster *	-	-
css:cluster:getDiskUsage	授予权限获取集群存储容量状态。	read	cluster *	-	-
css:snapshot:showDetail	授予权限获得快照详情。	read	cluster *	-	-
css:cluster:getAvailableBuckets	授予权限获取可用 OBS 桶。	list	-	-	-
css:cluster:checkCssName	授予权限检查集群名称。	write	cluster *	-	-
css:snapshot:deleteAllFailedTas	授予权限删除所有的失败任	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
k	务。				
css:snapshot:deleteSingleFailedTask	授予权限删除指定失败任务。	write	-	-	-
css:snapshot:getAllFailedTask	授予权限查看备份失败任务。	list	-	-	-
css::createServiceAgency	授予权限创建委托。	write	-	-	-
css:cluster:createAiOps	授予权限创建检测任务。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:listAiOps	授予权限获取检测任务列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:deleteAiOps	授予权限删除检测任务。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:listSmnTopics	授予权限获取SMN主题列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:listElbs	授予权限下获取当前集群可用的负载均衡器列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:elbSwitch	授予权限打开或关闭负载均衡功能。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
css:cluster:createElbListener	授予权限为当前集群创建监听器。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:updateElbListener	授予权限修改当前集群的监听器。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:getElbDetail	授予权限查询当前集群使用的负载均衡器信息。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
css:cluster:listElbCerts	授予权限获取负载均衡器证书列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-

CSS 的 API 通常对应着一个或多个授权项。表 3-170 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-166 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/clusters	css:cluster:create	• ecs:cloudServerFlavors:get • evs:types:get • vpc:vpcs:list • vpc:securityGroups:list • vpc:securityGroups:get • vpc:subnets:list • vpc:subnets:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:ports:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
		• css:cluster:getAgencies • iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject • iam:agencies:pass
POST /v2.0/{project_id}/clusters	css:cluster:create	• ecs:cloudServerFlavors:get • evs:types:get • vpc:vpcs:list • vpc:securityGroups:list • vpc:securityGroups:get • vpc:subnets:list • vpc:subnets:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:ports:get • css:cluster:getAgencies • iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject • iam:agencies:pass
POST /v1.0/{project_id}/clusters/{cluster_id}/sg/change	css:cluster:modifySecurityGroup	• vpc:securityGroups:list • vpc:ports:update
GET /v1.0/{project_id}/clusters	css:cluster:list	-
GET /v1.0/{project_id}/clusters/{cluster_id}	css:cluster:get	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}	css:cluster:delete	-
POST /v1.0/{project_id}/cluster/{cluster_id}/period	css:cluster:toPeriod	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/clusters/{cluster_id}/changename	css:cluster:modifyName	-
POST /v1.0/{project_id}/clusters/{cluster_id}/password/reset	css:cluster:modifyPassword	-
POST /v1.0/{project_id}/clusters/{cluster_id}/restart	css:cluster:restart	-
POST /v2.0/{project_id}/clusters/{cluster_id}/restart	css:cluster:restart	-
POST /v1.0/{project_id}/clusters/{cluster_id}/extend	css:cluster:scaleOut	• ecs:cloudServerFlavors:get • evs:types:get • vpc:vpcs:list • vpc:subnets:list • vpc:subnets:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:ports:get
POST /v1.0/{project_id}/clusters/{cluster_id}/role_extend	css:cluster:expand	• ecs:cloudServerFlavors:get • evs:types:get • vpc:vpcs:list • vpc:subnets:list • vpc:subnets:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:ports:get
POST /v1.0/{project_id}/clusters/{cluster_id}/flavor	css:cluster:modifySpecifications	ecs:cloudServerFlavors:get
GET /v1.0/{project_id}/es-flavors	css:cluster:listFlavors	ecs:cloudServerFlavors:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1.0/{project_id}/{resource_type}/tags	css:tag:list	-
GET /v1.0/{project_id}/{resource_type}/{cluster_id}/tags	css:tag:get	-
POST /v1.0/{project_id}/{resource_type}/{cluster_id}/tags	css:tag:edit	-
DELETE /v1.0/{project_id}/{resource_type}/{cluster_id}/tags/{key}	css:tag:delete	-
POST /v1.0/{project_id}/{resource_type}/{cluster_id}/tags/action	css:tag:addOrDelete	-
POST /v1.0/{project_id}/clusters/{cluster_id}/{types}/flavor	css:cluster:modifySpecifications	ecs:cloudServerFlavors:get
POST /v1.0/extend/{project_id}/clusters/{cluster_id}/role/shrink	css:cluster:scaleIn	• iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject
GET /v1.0/{project_id}/cer/download	css:cluster:downloadCert	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/instance/{instance_id}/replace	css:cluster:upgradeCluster	• iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject
POST /v1.0/{project_id}/clusters/{cluster_id}/node/offline	css:cluster:shrinkNodes	• iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject
POST /v1.0/{project_id}/clusters/{cluster_id}/mode	css:cluster:changeMode	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/change		
POST /v1.0/{project_id}/clusters/{cluster_id}/type/{type}/independent	css:cluster:addIndependenceNodes	• ecs:cloudServerFlavors:get • evs:types:get • vpc:vpcs:list • vpc:subnets:list • vpc:subnets:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:ports:get
POST /v1.0/{project_id}/clusters/{cluster_id}/inst-type/{inst_type}/image/upgrade	css:cluster:upgradeCluster	-
POST /v1.0/{project_id}/clusters/{cluster_id}/inst-type/{inst_type}/azmigrate	css:cluster:azmigrate	• iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject
GET /v1.0/{project_id}/clusters/{cluster_id}/upgrade/detail	css:cluster:listUpgradeCluster	-
GET /v1.0/{project_id}/clusters/{cluster_id}/target/{upgrade_type}/images	css:cluster:listUpgradeCluster	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/upgrade/{action_id}/retry	css:cluster:retryAction	-
POST /v1.0/{project_id}/clusters/{cluster_id}/thesaurus	css:IKThesaurus:load	• obs:bucket:listAllMyBuckets • obs:bucket:getBucketLocation • obs:bucket:getBucketStoragePolicy • obs:object:getObject
GET /v1.0/{project_id}/clusters/{cluster_id}/thesa	css:IKThesaurus:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
urus		
DELETE /v1.0/{project_id}/clusters/{cluster_id}/thesaurus	css:IKThesaurus:delete	-
POST /v1.0/{project_id}/clusters/{cluster_id}/publickibana/open	css:publicKibana:open	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/publickibana/close	css:publicKibana:close	-
POST /v1.0/{project_id}/clusters/{cluster_id}/publickibana/bandwidth	css:publicIPAddress:modifyBandwidth	-
POST /v1.0/{project_id}/clusters/{cluster_id}/publickibana/whitelist/update	css:publicIPAddress:setAccessControl	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/publickibana/whitelist/close	css:publicIPAddress:setAccessControl	-
POST /v1.0/{project_id}/clusters/{cluster_id}/logs/open	css:cluster:openLogSetting	• iam:agencies:pass • obs:bucket:listAllMyBuckets • obs:bucket:getBucketLocation • obs:bucket:getBucketStoragePolicy • iam:agencies:listAgencies
PUT /v1.0/{project_id}/clusters/{cluster_id}/logs/close	css:cluster:closeLogSetting	-
GET /v1.0/{project_id}/clusters/{cluster_id}/logs/records	css:log:listJob	-
GET /v1.0/{project_id}/clusters/{cluster_id}/logs/s	css:log:getBasicConfigurations	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ettings		
POST /v1.0/{project_id}/clusters/{cluster_id}/logs/settings	css:log:setBasicConfigurations	• obs:bucket:listAllMyBuckets • obs:bucket:getBucketLocation • obs:bucket:getBucketStoragePolicy • iam:agencies:listAgencies • iam:agencies:pass
POST /v1.0/{project_id}/clusters/{cluster_id}/logs/policy/update	css:log:updateBackupPolicy	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/logs/policy/close	css:log:updateBackupPolicy	-
POST /v1.0/{project_id}/clusters/{cluster_id}/logs/collect	css:log:backup	-
POST /v1.0/{project_id}/clusters/{cluster_id}/logs/search	css:log:list	-
POST /v1.0/{project_id}/clusters/{cluster_id}/public/open	css:publicIPAddress:associates	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/public/close	css:publicIPAddress:disassociates	-
POST /v1.0/{project_id}/clusters/{cluster_id}/public/bandwidth	css:publicIPAddress:modifyBandwidth	-
POST /v1.0/{project_id}/clusters/{cluster_id}/public/whitelist/update	css:publicIPAddress:setAccessControl	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/publi	css:publicIPAddress:setAccessControl	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
c/whitelist/close		
POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/auto_setting	css:snapshot:enableAtomaticSnapsot	• obs:bucket:createBucket • obs:bucket:headBucket • iam:agencies:listAgencies • iam:agencies:createAgency • iam:permissions:grantRoleToAgency
POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/setting	css:snapshot:setSnapshotConfiguration	• obs:bucket:listAllMyBuckets • obs:bucket:getBucketLocation • obs:bucket:getBucketStoragePolicy • iam:agencies:listAgencies • iam:agencies:pass
POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot	css:snapshot:create	iam:agencies:pass
POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/{snapshot_id}/restore	css:snapshot:restore	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/{snapshot_id}	css:snapshot:delete	-
POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/policy	css:snapshot:setSnapshotPolicy	-
GET /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/policy	css:snapshot:getSnapshotPolicy	-
GET /v1.0/{project_id}/clusters/{cluster_id}/index_snapshots	css:snapshot:list	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/index	css:snapshot:disableSnapshotFuction	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
_snapshots		
POST /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/open	css:VPCEndpoint:enableOrDisable	• vpcep:endpoints:create • vpcep:endpoints:list • vpcep:endpoints:get • vpcep:endpoints:delete • vpcep:endpoints:update
PUT /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/close	css:VPCEndpoint:enableOrDisable	• vpcep::listQuotas • vpcep:endpoints:create • vpcep:endpoints:list • vpcep:endpoints:get • vpcep:endpoints:delete • vpcep:endpoints:update
GET /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/connections	css:VPCEndpoint:listConnection	vpcep:endpoints:get
POST /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/connections	css:VPCEndpoint:manageConnection	-
POST /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/permissions	css:VPCEndpoint:updateWhitelist	-
POST /v1.0/{project_id}/clusters/{cluster_id}/ymls/update	css:configurations:modify	-
GET /v1.0/{project_id}/clusters/{cluster_id}/ymls/joblists	css:configurations:list	-
GET /v1.0/{project_id}/clusters/{cluster_id}/ymls/template	css:configurations:get	-
POST /v2.0/{project_id}/clusters/{cluster_id}/snapshots/policy/open	css:snapshot:setSnapshotPolicy	-
PUT /v2.0/{project_id}/clusters/{cluster_id}/snaps	css:snapshot:setSnapshotPolicy	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
hots/policy/close		
POST /v2.0/{project_id}/clusters/{cluster_id}/rolling_restart	css:cluster:rollingReboot	-
GET /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/listactions	css:logstash:listActions	-
DELETE /v1.0/{project_id}/lgsconf/deletetemplate	css:logstash:deleteConfTemplate	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/stop	css:logstash:confStop	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/hot-stop	css:logstash:confStop	-
POST /v1.0/{project_id}/clusters/{cluster_id}/checkconnection	css:logstash:checkConnection	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/delete	css:logstash:confDelete	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/start	css:logstash:confStart	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/hot-start	css:logstash:confStart	-
GET /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/confdetail	css:logstash:getConfDetail	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/update	css:logstash:confUpdate	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/listpipelines	css:logstash:listPipelines	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/submit	css:logstash:submitConf	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/favorite	css:logstash:configFavorites	-
GET /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/listconfs	css:logstash:listConfs	-
GET /v1.0/{project_id}/lgsconf/template	css:logstash:listConfigTemplate	-
POST /v1.0/{project_id}/clusters/{cluster_id}/certs/upload	css:cluster:uploadCerts	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/certs/{cert_id}/delete	css:cluster:deleteCerts	-
GET /v1.0/{project_id}/clusters/{cluster_id}/certs	css:cluster:listCerts	-
GET /v1.0/{project_id}/clusters/{cluster_id}/certs/{cert_id}	css:cluster:getCertsDetail	-
POST /v1.0/{project_id}/clusters/{cluster_id}/route	css:cluster:modifyRoute	-
GET /v1.0/{project_id}/clusters/{cluster_id}/route	css:cluster:getRoutes	-
POST /v1.0/{project_id}/clusters/{cluster_id}/ai-ops	css:cluster:createAiOps	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1.0/{project_id}/clusters/{cluster_id}/ai-ops	css:cluster:listAiOps	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/ai-ops/{aiops_id}	css:cluster:deleteAiOps	-
GET /v1.0/{project_id}/domains/{domain_id}/ai-ops/smn-topics	css:cluster:listSmnTopics	• css:cluster:getAgencies • iam:agencies:list • iam:agencies:listAgencies • iam:agencies:listAttachedPolicies • iam:agencies:pass
GET /v1.0/{project_id}/clusters/{cluster_id}/loadbalancers	css:cluster:listElbs	elb:loadbalancers:list
POST /v1.0/{project_id}/clusters/{cluster_id}/loadbalancers/es-switch	css:cluster:elbSwitch	• elb:loadbalancers:list • iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject • iam:agencies:pass
POST /v1.0/{project_id}/clusters/{cluster_id}/es-listeners	css:cluster:createElbListener	-
GET /v1.0/{project_id}/clusters/{cluster_id}/es-listeners	css:cluster:getElbDetail	-
GET /v1.0/{project_id}/clusters/{cluster_id}/elb/certificates	css:cluster:listElbCerts	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/es-listeners/{listener_id}	css:cluster:updateElbListener	-

 版权所有 © 华为云计算技术有限公司

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-171 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

CSS 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-167 CSS 支持的资源类型

资源类型	URN
cluster	css:<region>:<account-id>:cluster:<cluster-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 css:）仅适用于对应服务的操作，详情请参见表 3-172。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

CSS 支持的服务级条件键

CSS 定义了以下可以在身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-168 CSS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
css:AssociatePublicIp	boolean	单值	是否允许实例开启公网访问。

 版权所有 © 华为云计算技术有限公司

条件键示例

- css:AssociatePublicIp

  示例：禁止创建带 EIP 的 CSS 集群

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "css:cluster:create"
      ],
      "Condition": {
        "Bool": {
          "css:AssociatePublicIp": [
            "true"
          ]
        }
      }
    }
  ]
}
```

  示例：禁止给 CSS 集群绑定 EIP

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "css:publicIPAddress:associates",
        "css:publicKibana:open"
      ]
    }
  ]
}
```

3.8.2 数据治理中心 DataArts Studio

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

 版权所有 © 华为云计算技术有限公司

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中 SCP 支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 DataArts Studio 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

  关于 DataArts Studio 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在自定义身份策略语句的 Action 元素中指定以下 DataArts Studio 的相关操作。

说明

由于当前接口限制，自定义身份策略指定资源类型时，由于部分操作不支持指定具体的 workspace 或 instance 资源，会导致权限配置不符合预期。如允许（allow）某个不支持指定资源的操作，但又为其指定了具体资源时，会导致所有资源操作均被拒绝；拒绝（deny）某个不支持指定资源的操作，但又为其指定了具体资源时，会导致所有资源操作均被允许。

因此，在自定义身份策略需要指定资源类型时，需要剔除这类操作，然后将这类操作独立为不指定资源或指定全局资源的身份策略，使用多个身份策略一起为用户赋权。不指定资源或指定全局资源的身份策略，即 JSON 策略内容中不带 Resource 元素，或者 Resource 内容如下所示：

```
"Resource": [
    "DataArtsStudio:*:*:workspace:*",
    "DataArtsStudio:*:*:instance:*"
]
```

当前 DataArts Studio 不支持指定具体资源的操作汇总如下：

- 不支持指定 workspace 资源，仅支持指定 instance 资源：
  - DataArtsStudio:workspace:create

 版权所有 © 华为云计算技术有限公司

  - DataArtsStudio:workspace:list
- **不支持指定** instance 资源或 workspace 资源：
  - DataArtsStudio:instance:create
  - DataArtsStudio:instance:get
  - DataArtsStudio:instance:list
  - DataArtsStudio:instance:resize
  - DataArtsStudio:instance:getAgency
  - DataArtsStudio:instance:createAgency
  - DataArtsStudio:instance:uploadDriver
  - DataArtsStudio:instance:deleteDriver
  - DataArtsStudio:instance:listDrivers
  - DataArtsStudio:instance:listTags
  - DataArtsStudio:workspace:listTags

表3-169 DataArts Studio 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
DataArtsStudio:workspace:list	授予权限以列举所有工作空间。	list	workspace *	g:ResourceTag/<tag-key>	dgc:workspace:list
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:workspace:create	授予权限以创建工作空间。	write	workspace *	-	-
			instance *	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
DataArtsStudio:workspace:get	授予权限以查询工作空间信息。	read	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:workspace:frozen	授予权限以冻结工作空间。	write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:workspace:unfrozen	授予权限以解除工作空间冻结。	write	workspace *	g:ResourceTag/<tag-key>	-
			instan	g:ResourceTag/	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			ce *	<tag-key>	
DataArtsStudio:workspace:update	授予权限以更新工作空间信息。	write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:instance:list	授予权限以列举所有实例。	list	instance *	g:ResourceTag/<tag-key>	dgc:workspace:list
DataArtsStudio:instance:create	授予权限以创建实例。	write	instance *	-	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
DataArtsStudio:instance:get	授予权限以查询实例。	read	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:resize	授予权限以变更实例规格。	write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:listDrivers	授予权限以查询所有驱动文件。	list	-	-	-
DataArtsStudio:instance:uploadDriver	授予权限以上传驱动文件。	write	-	-	-
DataArtsStudio:instance:deleteDriver	授予权限以删除驱动文件。	write	-	-	-
DataArtsStudio:workspace:delete	授予权限以删除工作空间。	write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:instance:getAgency	授予权限以查询云服务访问授权委托。	read	-	-	-
DataArtsStudio:instance:createAgency	授予权限以创建云服务访问授权委托。	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
DataArtsStudio:instance:delete	授予权限以删除实例。	write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:migrateBusinessModel	授予权限以迁移实例商业模式。	write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:operate	授予权限以操作实例上的资源。	write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:workspace:operate	授予权限以操作工作空间上的资源。	write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:instance:createRole	授予权限以创建自定义角色。	write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:listRoles	授予权限以查询自定义角色列表。	list	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:getRoleType	授予权限以查询自定义角色类型。	read	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:getRole	授予权限以查询自定义角色。	read	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:updateRole	授予权限以更新自定义角色。	write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:deleteRole	授予权限以删除自定义角色。	write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:tagResource	授予权限以增加实例标签。	write	instance *	g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
DataArtsStudio:instance:unTagResource	授予权限以删除实例标签。	write	instance *	g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
DataArtsStudio:instance:listIncrementalPackages	授予权限以列举所有增量包。	list	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:workspace:createIncrementalPackage	授予权限以创建工作空间增量包。	write	workspace *	• g:ResourceTag/<tag-key> • DataArtsStudio:EnablePublicAccess	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:workspace:tagResource	授予权限以增加工作空间标签。	write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
DataArtsStudio:workspace:unTagResource	授予权限以删除工作空间标签。	write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
DataArtsStudio:instance:createIncrementalPackage	授予权限以创建实例增量包。	write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:listTags	授予权限以获取所有实例标签列表。	list	instance *	g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
DataArtsStudio:workspace:listTags	授予权限以获取所有工作空间标签列表。	list	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:instance:listTagsForResource	授予权限以获取某个实例标签列表。	list	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:workspace:listTagsForResource	授予权限以获取某个工作空间标签列表。	list	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:workspace:updateDataServiceApiQuota	授予权限以更新工作空间数据服务 API 配额。	write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:workspace:executeDataServiceInstanceAction	授予权限以执行数据服务集群操作命令。	write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:instance:configureDataSecurityAdministrator	授予权限以配置数据安全管理员。	write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:listResourcesByTag	授予权限以根据标签筛选实例列表。	list	instance *	-	-
			-	g:TagKeys	
DataArtsStudio:workspace:listResourcesByTag	授予权限以根据标签筛选空间列表。	list	workspace *	-	-
			instance *	-	
			-	g:TagKeys	

DataArts Studio 的 API 通常对应着一个或多个授权项。表 3-174 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

 版权所有 © 华为云计算技术有限公司

表3-170 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/workspaces/{instance_id}	DataArtsStudio:workspace:list	-
POST /v1/{project_id}/workspaces/{instance_id}	DataArtsStudio:workspace:create	-
GET /v1/{project_id}/workspaces/{instance_id}/{workspace_id}	DataArtsStudio:workspace:get	-
POST /v1/{project_id}/change-resource	DataArtsStudio:instance:resize	-
GET /v1/{project_id}/instances	DataArtsStudio:instance:list	-
POST /v1/{project_id}/instances/onekey-purchase	DataArtsStudio:instance:create	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-175 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

DataArts Studio 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-171 DataArts Studio 支持的资源类型

资源类型	URN
workspace	DataArtsStudio:<region>:<account-id>:workspace:<instance-id>/<workspace-id>
instance	DataArtsStudio:<region>:<account-id>:instance:<instance-id>

条件（Condition）

条件键概述

条件（Condition）是自定义身份策略生效的特定条件，包括条件键和运算符。

 版权所有 © 华为云计算技术有限公司

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀为服务缩写，如 DataArtsStudio:）仅适用于对应服务的操作，详情请参见表 3-176。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：。

DataArts Studio 支持的服务级条件键

DataArts Studio 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-172 DataArts Studio 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
DataArtsStudio:EnablePublicAccess	boolean	单值	是否开启公网访问。

3.8.3 数据湖探索 DLI

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

 版权所有 © 华为云计算技术有限公司

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必须资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 DLI 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

  关于 DLI 定义的条件键的详细信息请参见条件（Condition）。
- **“别名”**列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。

您可以在自定义身份策略语句的 Action 元素中指定以下 DLI 的相关操作。

表3-173 DLI 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dli::operateAuth	授予数据湖探索权限管理权限。	permission_management	-	-	
dli::listAuth	授予数据湖探索权限信息查询权限。	list	-	-	
dli:variable:list	授予全局变量列表查询权限。	list	variable *	-	
dli:variable:create	授予全局变量创建权限。	write	variable *	-	
dli:variable:update	授予全局变量更新权限。	write	variable *	-	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dli:variable:delete	授予全局变量删除权限。	write	variable *	-	
dli:catalog:list	授予数据目录列表查询权限。	list	-	-	
dli:catalog:bind	授予数据目录绑定权限。	write	-	-	
dli:catalog:get	授予数据目录详情查询权限。	read	-	-	
dli:queue:list	授予队列列表查询权限。	list	queue *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
dli:queue:create	授予队列创建权限。	write	queue *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	
dli:queue:get	授予队列详情查询权限。	read	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:queue:update	授予队列更新权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:queue:delete	授予队列删除权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:queue:scal	授予队列扩	write	queue *	• g:Resourc	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
e	缩容权限。			eTag/<tag-key> • g:EnterpriseProjectId	
dli:queue:checkConnection	授予地址连通性测试权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:queue:getConnection	授予连通性结果查询权限。	read	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:queue:listPlans	授予查询队列定时扩缩容计划列表权限。	list	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:queue:createPlan	授予创建队列定时扩缩容计划权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:queue:deletePlan	授予删除队列定时扩缩容计划权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:queue:updatePlan	授予更新队列定时扩缩容计划权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:queue:createProperty	授予新增队列配置权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:queue:listProperties	授予查询队列配置列表权限。	list	queue *	• g:ResourceTag/<tag-key> • g:Enterpris	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				eProjectId	
dli:queue:updateProperty	授予更新队列配置权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:queue:deleteProperty	授予删除队列配置权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:jobs:list	授予作业列表查询权限。	list	jobs *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
dli:queue:submitJob	授予队列作业提交权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:jobs:get	授予作业详情查询权限。	read	jobs *	g:ResourceTag/<tag-key>	
dli:table:select	授予表查询权限。	read	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:table:insertInto	授予表数据插入权限。	write	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:queue:cancelJob	授予队列作业取消权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:jobs:exportResult	授予作业导出结果权	read	jobs *	g:ResourceTag/<tag-key>	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
dli::checkSql	授予校验SQL 语法权限。	write	-	-	
dli:database:list	授予数据库列表查询权限。	list	database *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
dli:database:create	授予数据库创建权限。	write	database *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	
dli:database:update	授予数据库更新权限。	write	database *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:database:delete	授予数据库删除权限。	write	database *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:database:displayAllTables	授予数据库显示所有表权限。	list	database *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:database:createTable	授予数据库创建表权限。	write	database *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:table:update	授予表更新权限。	write	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dli:table:describe	授予表结构显示权限。	read	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:table:delete	授予表删除权限。	write	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:table:showPartitions	授予表所有分区显示权限。	read	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:sqldefendrule:create	授予创建SQL 防御规则权限。	write	-	-	
dli:sqldefendrule:list	授予查询SQL 防御规则列表权限。	list	-	-	
dli:sqldefendrule:update	授予更新SQL 防御规则权限。	write	-	-	
dli:sqldefendrule:delete	授予删除SQL 防御规则权限。	write	-	-	
dli:sqldefendrule:get	授予查询SQL 防御规则详情权限。	read	-	-	
dli:resource:create	授予资源包创建权限。	write	resource *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
dli:resource:get	授予资源包详情查询权限。	read	resource *	g:ResourceTag/<tag-key>	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dli:resource:delete	授予资源包删除权限。	write	resource *	g:ResourceTag/<tag-key>	
dli:resource:list	授予资源包列表查询权限。	list	resource *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
dli:resource:update	授予资源包更新权限。	write	resource *	g:ResourceTag/<tag-key>	
dli:jobs:update	授予作业更新权限。	write	jobs *	g:ResourceTag/<tag-key>	
dli:jobs:delete	授予作业删除权限。	write	jobs *	g:ResourceTag/<tag-key>	
dli:jobs:create	授予作业创建权限。	write	jobs *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
dli:jobs:startFlinkJob	授予作业启动权限。	write	jobs *	g:ResourceTag/<tag-key>	
dli:jobs:stopFlinkJob	授予作业停止权限。	write	jobs *	g:ResourceTag/<tag-key>	
dli:jobs:export	授予作业导出权限。	write	jobs *	g:ResourceTag/<tag-key>	
dli::createEdgeChannel	授予创建 IEF 消息通道权限。	write	-	-	
dli::reportEdgeJob	授予边缘 Flink 作业状态信息上报权限。	write	-	-	
dli::callbackEdgeJobAction	授予边缘 Flink 作业 Action 状态回调权限。	write	-	-	
dli::createEdgeSystemEvent	授予 IEF 系统事件上报	write	-	-	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	权限。				
dli:template:list	授予模板列表查询权限。	list	template *	-	
dli:template:create	授予模板创建权限。	write	template *	-	
dli:template:update	授予模板更新权限。	write	template *	-	
dli:template:delete	授予模板删除权限。	write	template *	-	
dli:template:get	授予模板详情查询权限。	read	template *	-	
dli:elasticresourcepool:resourceManagement	授予弹性资源池管理资源权限。	write	elasticresourcepool *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:elasticresourcepool:list	授予弹性资源池列表查询权限。	list	elasticresourcepool *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
dli:elasticresourcepool:create	授予弹性资源池创建权限。	write	elasticresourcepool *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	
dli:elasticresourcepool:update	授予弹性资源池更新权限。	write	elasticresourcepool *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:elasticresourcepool:delete	授予弹性资源池删除权	write	elasticresourcepool *	• g:ResourceTag/<tag-key>	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。			• g:EnterpriseProjectId	
dli:elasticresourcepool:scale	授予弹性资源池扩缩容权限。	list	elasticresourcepool *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli::createLakehouse	授予lakehouse 创建权限。	write	-	-	
dli::getLakehouse	授予lakehouse 查询权限。	read	-	-	
dli:connection:list	授予查询经典型跨源连接列表权限。	list	-	• g:RequestTag/<tag-key> • g:TagKeys	
dli:connection:create	授予创建经典型跨源连接权限。	write	-	• g:RequestTag/<tag-key> • g:TagKeys	
dli:connection:get	授予查询经典型跨源连接权限。	read	-	-	
dli:connection:delete	授予删除经典型跨源连接权限。	write	-	-	
dli:edsconnection:get	授予增强型跨源详情查询权限。	read	edsconnection *	g:ResourceTag/<tag-key>	
dli:edsconnection:update	授予增强型跨源更新权限。	write	edsconnection *	g:ResourceTag/<tag-key>	
dli:edsconnection:delete	授予增强型跨源删除权限。	write	edsconnection *	g:ResourceTag/<tag-key>	
dli:edsconnection:list	授予增强型跨源列表查询权限。	list	edsconnection *	-	
			-	• g:RequestTag/<tag-	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				key> • g:TagKeys	
dli:edsconnection:create	授予增强型跨源创建权限。	write	edsconnection *	-	
			-	• g:RequestTag/<tag-key> • g:TagKeys • dli:VpcId	
dli:edsconnection:unbindQueue	授予增强型跨源解绑队列权限。	write	edsconnection *	g:ResourceTag/<tag-key>	
dli:edsconnection:bindQueue	授予增强型跨源绑定队列权限。	write	edsconnection *	g:ResourceTag/<tag-key>	
dli:datasourceauth:list	授予跨源认证列表查询权限。	list	datasourceauth *	-	
dli:datasourceauth:update	授予安全认证信息更新权限。	write	datasourceauth *	-	
dli:datasourceauth:create	授予安全认证信息创建权限。	write	datasourceauth *	-	
dli:datasourceauth:delete	授予安全认证信息删除权限。	write	datasourceauth *	-	
dli:edsconnection:deleteRoute	授予增强型跨源删除路由权限。	write	edsconnection *	g:ResourceTag/<tag-key>	
dli:edsconnection:createRoute	授予增强型跨源创建路由权限。	write	edsconnection *	g:ResourceTag/<tag-key>	
dli::getQuota	授予查询配额权限。	read	-	-	
dli:queue:restart	授予队列重启权限。	write	queue *	• g:ResourceTag/<tag-key> • g:Enterpris	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				eProjectId	
dli:table:insertOverwriteTable	授予表重写表数据权限。	write	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
dli:catalog:unbind	授予数据目录解绑权限。	write	-	-	
dli::listTags	授予标签获取列表权限。	list	-	-	
dli::listResourcesByTag	授予标签查询资源列表权限。	list	-	• g:RequestTag/<tag-key> • g:TagKeys	
dli::unTagResource	授予删除标签权限。	tagging	queue	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			resource	g:ResourceTag/<tag-key>	
			database	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			elasticresourcepool	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			edsconnection	g:ResourceTag/<tag-key>	
			jobs	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dli::listTagsForResource	授予查询指定资源标签的权限。	list	queue	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			resource	g:ResourceTag/<tag-key>	
			database	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			elasticresourcepool	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	
			edsconnection	g:ResourceTag/<tag-key>	
			jobs	g:ResourceTag/<tag-key>	
dli::createDownloader	授予创建下载任务权限。	write	-	-	

DLI 的 API 通常对应着一个或多个授权项。表 3-178 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-174 API 与授权项的关系（OpenAPI）

API	对应的授权项	依赖的授权项
PUT /v1.0/{project_id}/queues/user-authorization	dli::operateAuth	-
PUT /v1.0/{project_id}/user-authorization	dli::operateAuth	-
GET /v1.0/{project_id}/databases/{database_name}/tables/{table_name}/users	dli::listAuth	-
GET /v1.0/{project_id}/databases/{database_name}/tables/{table_name}/users/{user_nam	dli::listAuth	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
e}		
GET /v1.0/{project_id}/databases/{database_name}/users	dli::listAuth	-
GET /v1.0/{project_id}/queues/{queue_name}/users	dli::listAuth	-
GET /v1.0/{project_id}/authorization/privileges	dli::listAuth	-
PUT /v1.0/{project_id}/authorization	dli::operateAuth	-
GET /v1.0/{project_id}/variables	dli:variable:list	-
POST /v1.0/{project_id}/variables	dli:variable:create	-
PUT /v1.0/{project_id}/variables/{var_name}	dli:variable:update	-
DELETE /v1.0/{project_id}/variables/{var_name}	dli:variable:delete	-
GET /v3/{project_id}/catalogs	dli:catalog:list	-
POST /v3/{project_id}/catalogs/action	dli:catalog:bind	dli:catalog:unbind
GET /v3/{project_id}/catalogs/{catalog_name}	dli:catalog:get	-
GET /v1.0/{project_id}/queues	dli:queue:list	-
POST /v1.0/{project_id}/queues	dli:queue:create	-
GET /v1.0/{project_id}/queues/{queue_name}	dli:queue:get	-
PUT /v1.0/{project_id}/queues/{queue_name}	dli:queue:update	-
DELETE /v1.0/{project_id}/queues/{queue_name}	dli:queue:delete	-
PUT /v1.0/{project_id}/queues/{queue_name}/action	dli:queue:scale	dli:queue:restart
POST /v1.0/{project_id}/queues/{queue_name}/connection-test	dli:queue:checkConnection	-
GET /v1.0/{project_id}/queues/{queue_name}/connection-test/{task_id}	dli:queue:getConnection	-
GET /v1/{project_id}/queues/{queue_name}/pl	dli:queue:listPlans	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ans		
POST /v1/{project_id}/queues/{queue_name}/plans	dli:queue:createPlan	-
POST /v1/{project_id}/queues/{queue_name}/plans/batch-delete	dli:queue:deletePlan	-
PUT /v1.0/{project_id}/queues/{queue_name}	dli:queue:updatePlan	-
DELETE /v1/{project_id}/queues/{queue_name}/plans/{plan_id}	dli:queue:deletePlan	-
POST /v3/{project_id}/queues/{queue_name}/properties	dli:queue:createProperty	-
GET /v3/{project_id}/queues/{queue_name}/properties	dli:queue:listProperties	-
PUT /v3/{project_id}/queues/{queue_name}/properties	dli:queue:updateProperty	-
DELETE /v3/{project_id}/queues/{queue_name}/properties	dli:queue:deleteProperty	-
GET /v1.0/{project_id}/jobs	dli:jobs:list	-
POST /v1.0/{project_id}/jobs/submit-job	dli:queue:submitJob	-
GET /v1.0/{project_id}/jobs/{job_id}/status	dli:jobs:get	-
GET /v1.0/{project_id}/jobs/{job_id}/detail	dli:jobs:get	-
DELETE /v1.0/{project_id}/jobs/{job_id}	dli:queue:cancelJob	-
GET /v1.0/{project_id}/jobs/{job_id}/preview	dli:jobs:get	-
POST /v1.0/{project_id}/jobs/check-sql	dli::checkSql	-
GET /v1/{project_id}/jobs/{job_id}/progress	dli:jobs:get	-
POST /v1/{project_id}/sql-defend-rules	dli:sqldefendrule:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/sql-defend-rules	dli:sqldefendrule:list	-
PUT /v1/{project_id}/sql-defend-rules/{rule_id}	dli:sqldefendrule:update	-
DELETE /v1/{project_id}/sql-defend-rules/{rule_id}	dli:sqldefendrule:delete	-
GET /v1/{project_id}/sql-defend-rules/{rule_id}	dli:sqldefendrule:get	-
POST /v1.0/{project_id}/streaming/jobs/{job_id}/import-savepoint	dli:jobs:update	-
POST /v1.0/{project_id}/streaming/jobs/{job_id}/savepoint	dli:jobs:update	-
GET /v1.0/{project_id}/streaming/jobs/{job_id}	dli:jobs:get	-
DELETE /v1.0/{project_id}/streaming/jobs/{job_id}	dli:jobs:delete	-
GET /v1.0/{project_id}/streaming/jobs	dli:jobs:list	-
POST /v1.0/{project_id}/streaming/sql-jobs	dli:jobs:create	-
PUT /v1.0/{project_id}/streaming/sql-jobs/{job_id}	dli:jobs:update	-
POST /v1.0/{project_id}/streaming/flink-jobs	dli:jobs:create	-
PUT /v1.0/{project_id}/streaming/flink-jobs/{job_id}	dli:jobs:update	-
POST /v1.0/{project_id}/streaming/jobs/run	dli:jobs:startFlinkJob	dli:queue:submitJob
POST /v1.0/{project_id}/streaming/jobs/stop	dli:jobs:stopFlinkJob	dli:queue:cancelJob
POST /v1.0/{project_id}/streaming/jobs/delete	dli:jobs:delete	-
GET /v1.0/{project_id}/streaming/jobs/{job_id}/execute-graph	dli:jobs:get	-
POST /v1.0/{project_id}/streaming/jobs/export	dli:jobs:export	-
POST	dli:jobs:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1.0/{project_id}/streaming/jobs/import		
POST /v3/{project_id}/streaming/jobs/{job_id}/gen-graph	dli:jobs:get	-
GET /v1.0/{project_id}/streaming/job-templates	dli:template:list	-
POST /v1.0/{project_id}/streaming/job-templates	dli:template:create	-
PUT /v1.0/{project_id}/streaming/job-templates/{template_id}	dli:template:update	-
DELETE /v1.0/{project_id}/streaming/job-templates/{template_id}	dli:template:delete	-
POST /v1.0/{project_id}/sqls	dli:template:create	-
GET /v1.0/{project_id}/sqls	dli:template:list	-
GET /v1.0/{project_id}/sqls/sample	dli:template:list	-
PUT /v1.0/{project_id}/sqls/{template_id}	dli:template:update	-
POST /v1.0/{project_id}/sqls-deletion	dli:template:delete	-
POST /v3/{project_id}/templates	dli:template:create	-
GET /v3/{project_id}/templates	dli:template:list	-
PUT /v3/{project_id}/templates/{template_id}	dli:template:update	-
GET /v3/{project_id}/templates/{template_id}	dli:template:get	-
GET /v2.0/{project_id}/batches	dli:jobs:list	-
POST /v2.0/{project_id}/batches	dli:queue:submitJob	-
GET /v2.0/{project_id}/batches/{batch_id}	dli:jobs:get	-
DELETE /v2.0/{project_id}/batches/{batch_id}	dli:queue:cancelJob	-
GET /v2.0/{project_id}/batches/{batch_id}/log	dli:jobs:get	-
GET /v2.0/{project_id}/batches/{batch_id}/state	dli:jobs:get	-
POST /v3/{project_id}/elastic-resource-	dli:elasticresourcepool:resourceManagemen	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
pools/{elastic_resource_pool_name}/notebook/action	t	
POST /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/notebook/instances	dli:elasticresourcepool:resourceManagement	-
GET /v3/{project_id}/elastic-resource-pools	dli:elasticresourcepool:list	-
POST /v3/{project_id}/elastic-resource-pools	dli:elasticresourcepool:create	-
PUT /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}	dli:elasticresourcepool:update	-
DELETE /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}	dli:elasticresourcepool:delete	-
GET /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/queues	dli:elasticresourcepool:resourceManagement	-
POST /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/queues	dli:elasticresourcepool:resourceManagement	• dli:queue:create • dli:queue:delete
PUT /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/queues/{queue_name}	dli:elasticresourcepool:resourceManagement	-
GET /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/scale-records	dli:elasticresourcepool:scale	-
POST /v3/{project_id}/orders/elastic-resource-pools	dli:elasticresourcepool:create	-
POST /v3/{project_id}/orders/elastic-resource-pools/specification-change	dli:elasticresourcepool:scale	-
POST /v3/{project_id}/lakehouse	dli::createLakehouse	-
GET /v3/{project_id}/lakehouse	dli::getLakehouse	-
GET /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}	dli:edsconnection:get	-
PUT /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}	dli:edsconnection:update	-
DELETE /v2.0/{project_id}/datasource/enhanced-	dli:edsconnection:dele	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
connections/{connection_id}	te	
GET /v2.0/{project_id}/datasource/enhanced-connections	dli:edsconnection:list	-
POST /v2.0/{project_id}/datasource/enhanced-connections	dli:edsconnection:create	-
POST /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}/disassociate-queue	dli:edsconnection:unbindQueue	-
POST /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}/associate-queue	dli:edsconnection:bindQueue	-
GET /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}/privileges	dli::listAuth	-
GET /v3/{project_id}/datasource/auth-infos	dli:datasourceauth:list	-
PUT /v3/{project_id}/datasource/auth-infos	dli:datasourceauth:update	-
POST /v3/{project_id}/datasource/auth-infos	dli:datasourceauth:create	-
DELETE /v3/{project_id}/datasource/auth-infos/{auth_info_name}	dli:datasourceauth:delete	-
POST /v3/{project_id}/datasource/enhanced-connections/{connection_id}/routes	dli:edsconnection:deleteRoute	-
DELETE /v3/{project_id}/datasource/enhanced-connections/{connection_id}/routes/{name}	dli:edsconnection:createRoute	-
GET /v3/{project_id}/quotas	dli::getQuota	-
GET /v3/{project_id}/datasource/auth-infos	dli:datasourceauth:list	-
PUT /v3/{project_id}/datasource/auth-infos	dli:datasourceauth:update	-
POST /v3/{project_id}/datasource/auth-infos	dli:datasourceauth:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /v3/{project_id}/datasource/auth-infos/{auth_info_name}	dli:datasourceauth:delete	-
POST /v3/{project_id}/datasource/enhanced-connections/{connection_id}/routes	dli:edsconnection:createRoute	-
DELETE /v3/{project_id}/datasource/enhanced-connections/{connection_id}/routes/{name}	dli:edsconnection:deleteRoute	-
GET /v3/{project_id}/{resource_type}/tags	dli::listTags	-
POST /v3/{project_id}/{resource_type}/resource-instances/filter	dli::listResourcesByTag	-
POST /v3/{project_id}/{resource_type}/resource-instances/count	dli::listResourcesByTag	-
POST /v3/{project_id}/{resource_type}/{resource_id}/tags/delete	dli::unTagResource	-
GET /v3/{project_id}/{resource_type}/{resource_id}/tags	dli::listTagsForResource	-

表3-175 API 与授权项的关系（控制台操作相关）

API	对应的授权项	依赖的授权项
GET /v1.0/{project_id}/logs/transfer	dli::getLogTransfer	-
POST /v1.0/{project_id}/logs/history	dli::getLog	-
POST /v1.0/{project_id}/logs/runtime	dli::getLog	-
GET /v1.0/{project_id}/logs/pods	dli::getLog	-
GET /v1.0/{project_id}/logs/pods/{pod_name}	dli::getLog	-
PUT /v1.0/{project_id}/databases/{database_name}/name	dli:database:update	-
POST /v1/{project_id}/streaming/jobs/check	dli:jobs:check	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/streaming/sql/validate	dli::checkSql	-
GET /v1/{project_id}/streaming/jobs/{job_id}/log	dli:jobs:get	-
GET /v1/{project_id}/streaming/jobs/{job_id}/log/{tm_id}	dli:jobs:get	-
GET /v1/{project_id}/streaming/jobs/{job_id}/submitlog	dli:jobs:get	-
POST /v1/{project_id}/streaming/templates/check	dli:template:check	-
GET /v1.0/{project_id}/databases/{database_name}/projects	dli::listAuth	-
GET /v1.0/{project_id}/databases/{database_name}/tables/{table_name}/projects	dli::listAuth	-
GET /v1.0/{project_id}/databases/{database_name}/tables/{table_name}/projects/{projectId}	dli::listAuth	-
GET /v1.0/{project_id}/databases/{database_name}/projects/{projectId}	dli::listAuth	-
GET /v1.0/{project_id}/databases/{database_name}/tables/{table_name}/columns/{column_name}/projects/{projectId}	dli::listAuth	-
POST /v1.0/{project_id}/logs/transfer	dli::createLogTransfer	-
POST /v1.0/{project_id}/orders/queues	dli:queue:create	-
PUT /v1.0/{project_id}/orders/queues	dli:queue:scale	-
PUT /v3/{project_id}/queues/{queue_name}/scale-range	dli:queue:scale	-

 版权所有 © 华为云计算技术有限公司

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-180 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

DLI 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-176 DLI 支持的资源类型

资源类型	URN
variable	dli:<region>:<account-id>:variable:<variable-name-with-prefix>
queue	dli:<region>:<account-id>:queue:<queue-name-with-prefix>
jobs	dli:<region>:<account-id>:jobs:<job-id-with-prefix>
table	dli:<region>:<account-id>:table:<table-name-with-prefix>
database	dli:<region>:<account-id>:database:<database-name-with-prefix>
resource	dli:<region>:<account-id>:resource:<resource-name-with-prefix>
template	dli:<region>:<account-id>:template:<template-name-with-prefix>
elasticresourcepool	dli:<region>:<account-id>:elasticresourcepool:<elasticresourcepool-name-with-prefix>
edsconnection	dli:<region>:<account-id>:edsconnection:<edsconnection-id-with-prefix>
datasourceauth	dli:<region>:<account-id>:datasourceauth:<datasourceauth-name-with-prefix>

条件（Condition）

条件（Condition）是自定义身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀为服务缩写，如 dli:）仅适用于对应服务的操作，详情请参见表 3-181。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。

 版权所有 © 华为云计算技术有限公司

例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。

- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

DLI 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-177 DLI 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
dli:VpcId	string	单值	根据虚拟网络 ID 筛选访问权限。

3.8.4 MapReduce 服务 MRS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务基于策略授权场景中自定义策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在策略语句的 Resource 元素中指定所有资源类型（“*”）。

 版权所有 © 华为云计算技术有限公司

- 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
- 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

关于 MRS 服务定义的资源类型的详细信息请参见资源类型（Resource）。

- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅队列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 MRS 定义的条件键的详细信息请参见条件（Condition）。
- **“别名”**列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在策略语句的 Action 元素中指定以下 MapReduce 服务（MRS）的相关操作。

表3-178 MapReduce 服务（MRS）支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
mrs:cluster:createCluster	授予权限以创建集群。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:RequestTag/<tag-key>,g:TagKeys,g:EnterpriseProjectId	mrs:cluster:create
mrs:cluster:deleteCluster	授予权限以删除集群。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	mrs:cluster:delete
mrs:cluster:listHosts	授予权限以查询集群中的节点。	list	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	mrs:host:list
mrs:cluster:listFiles	授予权限以查询集群中的文件列表。	list	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	mrs:file:list
mrs:cluster:createJob	授予权限以在集群中执行作业。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	mrs:job:submit
mrs:cluster:list	授予权限以查询集群列表。	list	-	g:RequestTag/<tag-key>,g:TagKeys,g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
mrs:cluster:listJobs	授予权限以查询集群的作业列表。	list	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	mrs:job:list
mrs:cluster:getJob	授予权限以查询集群的作业详情。	read	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	mrs:job:get
mrs:cluster:getCluster	授予权限以查询集群详情。	read	mrs:<region>:<account-id>:cluster:<cluster-id>	-	mrs:cluster:get
mrs:cluster:resizeNodes	授予权限以调整集群节点。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	mrs:cluster:resize
mrs:cluster:updateClusterName	授予权限以重命名集群。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	-
mrs:cluster:listTags	授予权限以查询集群标签。	list	-	g:EnterpriseProjectId	mrs:tag:list
mrs:cluster:updateTags	授予权限以增删集群标签。	tagging	-	g:RequestTag/<tag-key>,g:TagKeys,g:EnterpriseProjectId	mrs:tag:create mrs:tag:delete mrs:tag:batchOperate
mrs:cluster:listClustersByTag	授予权限以查询特定标签的集群列表。	list	-	g:RequestTag/<tag-key>,g:TagKeys	mrs:tag:listResource
mrs:cluster:stopJob	授予权限以停止集群作业。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	mrs:job:stop
mrs:cluster:deleteJobs	授予权限以批量删除集群作业。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	mrs:job:batchDelete
mrs:cluster:stopSql	授予权限以取消 sql 执	write	mrs:<region>:<account-	g:EnterpriseProjectId	mrs:sql:cancel

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	行。		id>:cluster:<cluster-id>		
mrs:cluster:createSql	授予权限以提交 sql 执行。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	mrs:sql:execute mrs:job:checkSql
mrs:cluster:listPolicies	授予权限以获取集群内所有的弹性伸缩策略。	list	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	mrs:cluster:policy
mrs:cluster:updatePolicies	授予权限以修改集群的弹性伸缩策略。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	mrs:cluster:policy
mrs:cluster:getAgencyMapping	授予权限以获取用户代理信息。	read	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	-
mrs:cluster:updateAgencyMapping	授予权限以更新用户代理信息。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	mrs:cluster:syncUser
mrs:cluster:getSql	授予权限以获取 sql 执行结果。	read	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId	mrs:sql:get

资源类型（Resource）

资源类型（Resource）表示策略所作用的资源。如表 3 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的策略语句中指定该资源的 URN，策略仅作用于此资源；如未指定，Resource 默认为“*”，则策略将应用到所有资源。您也可以在策略中设置条件，从而指定资源类型。

MapReduce 服务（MRS）定义了以下可以在策略的 Resource 元素中使用的资源类型。

表3-179 MapReduce 服务（MRS）支持的资源类型

资源类型	URN
cluster	mrs:<region>:<account-id>:cluster:<cluster-id>

 版权所有 © 华为云计算技术有限公司

条件（Condition）

MRS 服务不支持在身份策略中的条件键中配置服务级的条件键。MRS 服务可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.8.5 数据仓库服务 GaussDB(DWS)

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 GaussDB(DWS)定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 GaussDB(DWS)定义的条件键的详细信息请参见条件（Condition）。
- **“别名”**列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

 版权所有 © 华为云计算技术有限公司

您可以在身份策略语句的 Action 元素中指定以下 GaussDB(DWS)的相关操作。

表3-180 GaussDB(DWS)支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:cluster:list	授予集群列表查询权限。	list	-	-	-
dws:cluster:getDetail	授予集群详情查看权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:openAPICluster:getDetail
dws:cluster:create	授予 DWS 集群创建权限。	write	-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	dws:openAPICluster:create
dws:cluster:delete	授予 DWS 集群删除权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:openAPICluster:delete
dws:cluster:scaleIn	授予 DWS 集群缩容权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:cluster:shrink
dws:cluster:listRing	授予获得合适的缩容环列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:ring:list
dws:cluster:restore	授予就地恢复集群权限。	write	cluster *	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	-
dws:cluster:scaleOut	授予集群扩容权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:Enterprise	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ProjectId	
dws:cluster:resize	授予集群扩容和调整大小权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:cluster:scaleOutOrOpenAPIResize
dws:cluster:expandDisk	授予 DWS 集群磁盘扩容权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:disk:expand
dws:cluster:restart	授予 DWS 集群重启权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:openAPICluster:restart
dws:cluster:resetPassword	授予 DWS 集群重置密码权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:openAPICluster:resetPassword
dws:cluster:listAuditLog	授予查看审计日志列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:setMaintainceWindow	授予维护时间窗修改权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:switchover	授予集群主备恢复权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:cancelReadonly	授予集群解除只读权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:Enterprise	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ProjectId	
dws:cluster:addCN	授予集群增加CN节点权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:module:install
dws:cluster:listCN	授予获取集群CN列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:deleteCN	授予删除CN节点权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:module:uninstall
dws:cluster:redistribution	授予集群数据重分布权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:redistribution:operate
dws:cluster:createDataSource	授予创建MRS数据源权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:MRSConnection:create
dws:cluster:updateDataSource	授予更新MRS数据源权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:MRSConnection:update
dws:cluster:deleteDataSource	授予删除MRS数据源权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:MRSConnection:delete
dws:alarm:listConfig	授予查询告警配置权限。	list	-	-	dws:alarmConfig:list
dws:alarm:listD	授予查询告警	list	-	-	dws:alarmDetai

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
etail	详情列表权限。				l:list
dws:alarm:listStatistics	授予查询告警统计列表权限。	list	-	-	dws:alarmStatistic:list
dws:alarm:createSubscription	授予创建告警订阅权限。	write	-	-	dws:alarmSub:create
dws:alarm:listSubscription	授予查询订阅告警权限。	list	-	-	dws:alarmSub:list
dws:alarm:updateSubscription	授予更新订阅告警权限。	write	-	-	dws:alarmSub:update
dws:alarm:deleteSubscription	授予删除订阅的告警权限。	write	-	-	dws:alarmSub:delete
dws:alarm:report	授予上报告警权限。	write	-	-	-
dws:event:list	授予查询事件列表权限。	list	-	-	-
dws:event:listSpec	授予查询事件配置权限。	list	-	-	dws:eventSpec:list
dws:event:listSubscription	授予查询订阅事件权限。	read	-	-	dws:eventSub:list
dws:event:createSpec	授予创建事件配置权限。	write	-	-	-
dws:event:deleteSpec	授予删除事件配置权限。	write	-	-	-
dws:event:createSubscription	授予创建订阅事件权限。	write	-	-	dws:eventSub:create
dws:event:updateSubscription	授予更新订阅事件权限。	write	-	-	dws:eventSub:update
dws:event:deleteSubscription	授予删除订阅的事件权限。	write	-	-	dws:eventSub:delete
dws:event:report	授予上报事件权限。	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:cluster:createConnection	授予创建 DWS 集群连接权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:dns:create
dws:cluster:deleteConnection	授予删除 DWS 集群连接权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:dns:release
dws:cluster:updateConnection	授予更新 DWS 集群连接权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:dns:edit
dws:cluster:bindEIP	授予公网 IP 绑定权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:eip:operate
dws:cluster:unbindEIP	授予公网 IP 解绑权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:eip:operate
dws:cluster:listELB	授予获得弹性负载均衡列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:elb:list
dws:cluster:bindELB	授予绑定弹性负载均衡权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:elb:bind
dws:cluster:unbindELB	授予解绑弹性负载均衡权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:elb:unbind

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:cluster:createSnapshotPolicy	授予设置自动快照策略权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:cluster:setAutomatedSnapshot
dws:cluster:listSnapshotStatistics	授予查询快照空间容量权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listSnapshot	授予查看集群快照列表权限。	list	cluster	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:openAPISnapshot:list
dws:cluster:getSnapshotDetail	授予查看集群快照详情权限。	list	cluster	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:openAPISnapshot:detail
dws:cluster:createSnapshot	授予使用 API 创建快照权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:openAPISnapshot:create
dws:cluster:deleteSnapshotPolicy	授予删除快照策略权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:backupPolicy:delete
dws:cluster:listSnapshotPolicy	授予查询快照策略权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:copySnapshot	授予复制快照权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:snapshot:copy

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:cluster:deleteSnapshot	授予删除快照权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:openAPISnapshot:delete
dws:cluster:restoreSnapshot	授予恢复快照权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:openAPISnapshot:restore
dws:cluster:deleteDisasterRecovery	授予删除容灾权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:disasterRecovery:delete
dws:cluster:createDisasterRecovery	授予创建备份容灾权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:disasterRecovery:create
dws:cluster:startDisasterRecovery	授予容灾启动权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:disasterRecovery:otherOperate
dws:cluster:pauseDisasterRecovery	授予容灾暂停权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:disasterRecovery:otherOperate
dws:cluster:switchoverDisasterRecovery	授予容灾切换权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:disasterRecovery:otherOperate
dws:cluster:switchFailoverDisaster	授予容灾切换权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:disasterRecovery:otherOperate

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:cluster:restoreDisaster	授予容灾恢复权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:disasterRecovery:otherOperate
dws:cluster:getDisasterRecovery	授予容灾查询操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:disasterRecovery:get
dws::listTagsForProject	授予查询该项目下的标签列表权限。	list	-	-	dws:openAPITag:list
dws::listTagsForResource	授予查询集群标签列表权限。	list	cluster *	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	dws:openAPITag:getResourceTag
dws::tagResource	授予添加标签权限。	tagging	cluster *	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	dws:openAPITag:add
dws::unTagResource	授予删除标签权限。	tagging	cluster *	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	dws:openAPITag:delete
dws:monitor:listHostDisk	授予 DMS-查询主机磁盘信息权限。	list	-	-	-
dws:monitor:listHostNet	授予 DMS-查询主机网络监控权限。	list	-	-	-
dws:monitor:listMonitorIndicatorData	授予 DMS-查询主机历史监控信息权限。	list	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:monitor:listMonitorIndicators	授予 DMS-查询性能监控指标权限。	list	-	-	-
dws:cluster:listConfig	授予查看集群配置参数权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:service:listSpec	授予查看服务规格列表权限。	list	-	-	dws:specProduct:list
dws:cluster:listDataSource	授予查看集群数据源权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:MRSSource:list
dws:service:listJobDetail	授予查看任务进度详情权限。	list	-	-	-
dws:service:listStatistics	授予查看当前可用资源数量权限。	list	-	-	-
dws:service:listQuotas	授予查看用户配额权限。	list	-	-	-
dws:cluster:updateConfig	授予更新集群配置参数权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:cluster:setSecuritySettings
dws:service:listAZ	授予查看服务可用区列表权限。	list	-	-	-
dws:service:listDssPools	授予查看专属存储池列表权限。	list	-	-	-
dws:service:listEps	授予查看 eps 列表权限。	list	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:service:authorize	授予获取用户授权权限。	write	-	-	dws:authorize:operate
dws:service:checkAuthorize	授予检查用户授权权限。	read	-	-	dws:checkAuthorize:operate
dws::updateTag	授予更新标签权限。	tagging	cluster *	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	dws:tag:edit
dws:cluster:getSnapshotPolicy	授予查看快照策略权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:backupPolicy:list
dws:cluster:bindOrUnbindELB	授予绑定或解绑弹性负载均衡权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:elb:bind
dws:cluster:bindOrUnbindEIP	授予绑定或解绑弹性 IP 权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:eip:operate
dws:cluster:deleteNode	授予删除节点权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:clusterNodes:operate
dws:cluster:listConnection	授予查询 DWS 集群连接列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:dns:list
dws:cluster:checkConnection	授予检查 DWS 集群连接权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:cluster:listDN	授予获取集群DN 列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listBucket	授予获取桶列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listScaleInNode	授予获取缩容待删除节点列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listFlavorForResize	授予查询支持变更的规格列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listFlavorForRestore	授予查询支持恢复的规格列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws::countResourceByTag	授予使用标签查询集群权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:updateSnapshotPolicy	授予更新快照策略权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:backupPolicyDetail:update
dws::listResourceByTag	授予根据标签查询集群列表权限。	list	cluster *	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	dws:openAPITag:getResourceByTag

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:cluster:assessRisk	授予评估调整大小风险权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:checkRestoreTable	授予恢复表检查权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:tableRestoreCheck:operate
dws:cluster:checkSupportFineGrainedBackup	授予检测集群是否支持细粒度备份权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:checkSupport:operate
dws:cluster:configureNetwork	授予配置集群网络权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:expandWithExistedNodes	授予集群从空闲节点扩容权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:expandWithExistedNodes:update
dws:cluster:getAntiAffinity	授予查询反亲和性状态权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getCnCount	授予查询集群CN 数量权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getCredential	授予获取集群JDBC 连接凭证权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:cluster:getDiskExpandScope	授予获取磁盘扩容范围权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getEncryptInfo	授予查看集群加密信息权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listHistoryConfig	授予查询参数修改历史权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getHistoryConfigDetail	授予查询参数修改历史详情权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getInstanceDetail	授予实例详情查看权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getProcessTopo	授予查询集群节点进程拓扑权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:processTopo:list
dws:cluster:getRedistribution	授予查询重分布详情权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:redistributionInfo:list
dws:cluster:getRestoreDatabase	授予获取用户恢复数据库权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:cluster:getRoachConfig	授予获取 roach 参数配置权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:roachConfig:get
dws:cluster:getSnapshotEncryptInfo	授予查看快照加密信息权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:clusterEncryptInfo:list
dws:cluster:getSnapshotStorage	授予查询快照空间容量使用情况权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getTaskDetail	授予查询集群任务详情权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getVolumeInfo	授予查询磁盘信息权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listNode	授予查询节点列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listSchema	授予获取用户结构列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:schemas:list
dws:cluster:listTable	授予获取用户表列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:tables:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:cluster:listDatabase	授予获取用户数据库列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:userDatabase:list
dws:cluster:recoverRedistribution	授予恢复重分布权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:redistribution:recover
dws:cluster:resizeFlavor	授予执行规格变更权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:specResize:operate
dws:cluster:resizeRetry	授予调整大小重试权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:cluster:submitResizeRetry
dws:cluster:restoreTable	授予表恢复权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:tableRestore:operate
dws:cluster:retryELBSwitch	授予重试 ELB 切换任务权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listRingForScaleIn	授予获得缩容环列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:saveDescriptionInfo	授予保存集群描述信息权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:cluster:stopSnapshot	授予停止快照权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:snapshot:stop
dws:cluster:suspendRedistribution	授予暂停重分布权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:redistribution:suspend
dws:cluster:updateInstanceAliasName	授予更新节点别名权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:instanceAliasName:update
dws:cluster:updateRoachConfig	授予更新 roach 参数配置权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:roachConfig:update
dws:cluster:updateScheduleConfig	授予更新调度配置权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:roachConfig:update
dws:service:getClusterSum	授予查询集群数量权限。	read	-	-	-
dws:service:getResourceStatistics	授予查询资源统计权限。	read	-	-	-
dws:service:getStorageStatistics	授予查询存储统计信息权限。	read	-	-	-
dws:cluster:listDisasterRecovery	授予容灾列表查询操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:disasterRecovery:get
dws:cluster:che	授予容灾名称	read	cluster	• g:ResourceT	dws:disasterRec

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ckDisasterRecoveryName	检查操作权限。		*	ag/<tag-key> • g:EnterpriseProjectId	overy:get
dws:cluster:updateDisasterRecoveryConfig	授予更新容灾配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:disasterRecovery:otherOperate
dws:cluster:addOperationalTask	授予新增调度任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:operationalTask:operate
dws:cluster:bindManageIp	授予绑定管理面 IP 操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:bindManageIp:operate
dws:cluster:checkAccessLts	授予检查 LTS 服务是否正常操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:ltsAccess:get
dws:cluster:checkLogicalClusterData	授予逻辑集群-检查集群有无业务数据操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:logicalCluster:get
dws:cluster:closeAccessLts	授予关闭云服务日志操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:ltsAccess:operate
dws:cluster:createLogicalCluster	授予逻辑集群-创建逻辑集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:logicalCluster:operate
dws:cluster:crea	授予数据迁移-	write	cluster	• g:ResourceT	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
teApplicationForDM	增加作业任务操作权限。		*	ag/<tag-key> • g:EnterpriseProjectId	
dws:cluster:createClusterForDM	授予数据迁移-创建集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:createConnectionForDM	授予数据迁移-增加指定连接信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:createMappingForDM	授予数据迁移-增加指定映射信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:deleteApplicationForDM	授予数据迁移-删除作业任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:deleteClusterForDM	授予数据迁移-删除集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:deleteConnectionForDM	授予数据迁移-删除指定连接信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:deleteMappingForDM	授予数据迁移-删除指定映射信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:dial	授予数据迁移-	read	cluster	• g:ResourceT	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
sConnectionForDM	连接信息探活操作权限。		*	ag/<tag-key> • g:EnterpriseProjectId	
dws:cluster:getApplicationForDM	授予数据迁移-查询作业任务详情操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listApplicationConfigForDM	授予数据迁移-作业任务参数配置信息操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listApplicationForDM	授予数据迁移-查询集群内所有作业任务操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getClusterForDM	授予数据迁移-查询集群信息详情操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listClusterForDM	授予数据迁移-查询集群信息列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listConfigurationTemplateForDM	授予数据迁移-查询参数模板操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getConnectionForDM	授予数据迁移-查询连接信息详情操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:list	授予数据迁移-	list	cluster	• g:ResourceT	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ConnectionForDM	查询所有连接信息操作权限。		*	ag/<tag-key> • g:EnterpriseProjectId	
dws:cluster:listDependApplicationForDM	授予数据迁移-查询所有依赖作业任务操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getMappingForDM	授予数据迁移-查询映射信息详情操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listMappingForDM	授予数据迁移-查询所有映射信息操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listProductForDM	授予 GDS-Kafka-查询产品信息操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:updateConnectionForDM	授予数据迁移-修改指定连接信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:updateMappingForDM	授予数据迁移-修改指定映射信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:startApplicationForDM	授予数据迁移-启动作业任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:stop	授予数据迁移-	write	cluster	• g:ResourceT	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ApplicationForDM	停止作业任务操作权限。		*	ag/<tag-key> • g:EnterpriseProjectId	
dws:cluster:deleteCrossRegionSnapshotPolicy	授予删除跨区域备份配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:crossRegionBackupConfig:delete
dws:cluster:deleteLogicalCluster	授予逻辑集群-删除逻辑集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:logicalCluster:operate
dws:cluster:deleteOperationalTask	授予调度器-删除调度任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:operationalTask:operate
dws:cluster:operateDisasterRecovery	授予容灾-容灾操作，启/停/切换等操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:disasterRecovery:otherOperate
dws:cluster:updateLogicalCluster	授予逻辑集群-更新逻辑集群权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:logicalCluster:operate
dws:cluster:listAllCrossRegionSnapshotConfig	授予查询所有跨区域快照配置操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getDisasterRecoveryProject	授予容灾-查询可用 project 操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:disasterRecovery:get
dws:cluster:get	授予容灾-查询	read	cluster	• g:ResourceT	dws:disasterRec

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
DisasterRecoveryRegion	可用 region 操作权限。		*	ag/<tag-key> • g:EnterpriseProjectId	overy:get
dws:cluster:getLastOperationalTask	授予调度器-查询上次构建任务操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:operationalTask:get
dws:cluster:getLogicalClusterRings	授予逻辑集群-查询集群环信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:logicalCluster:get
dws:cluster:getLogicalClusterVolume	授予逻辑集群-查询集群磁盘信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:logicalCluster:get
dws:cluster:getOperationalTaskConfig	授予调度器-获取调度器运维任务公共配置操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:operationalTask:get
dws:cluster:getOperationalTaskDetail	授予调度器-获取运维任务详情列表操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:operationalTask:get
dws:cluster:getOperationalTaskStatus	授予调度器-获取调度器状态操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:operationalTask:get
dws:cluster:listSnapshotRegion	授予获取跨区域快照可用 region 操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:get	授予查询所有	read	cluster	• g:ResourceT	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
TargetAllCrossRegionSnapshotConfig	跨区域快照配置操作权限。		*	ag/<tag-key> • g:EnterpriseProjectId	
dws:cluster:initLogicalClusterSwitch	授予逻辑集群-切换逻辑集群开关操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:logicalCluster:operate
dws:cluster:listAccessLts	授予查询 LTS 列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listLogicalCluster	授予逻辑集群-查询逻辑集群列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:logicalCluster:get
dws:cluster:listLogicalClusterTask	授予逻辑集群-查询任务信息操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:logicalCluster:get
dws:cluster:listOperationalTask	授予调度器-获取运维任务列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:operationalTask:get
dws:cluster:openAccessLts	授予开启云服务日志操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:ltsAccess:operate
dws:cluster:pauseOperationalTask	授予调度器-暂停调度任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:operationalTask:operate
dws:cluster:get	授予容灾-查询	write	cluster	• g:ResourceT	dws:disasterRec

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
DisasterRecoveryDetail	容灾详情操作权限。		*	ag/<tag-key> • g:EnterpriseProjectId	overy:get
dws:cluster:refreshOperationalTask	授予调度器-远程刷新当前集群运维任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:operationalTask:get
dws:cluster:restartLogicalCluster	授予逻辑集群-重启逻辑集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:logicalCluster:operate
dws:cluster:resumeOperationalTask	授予调度器-恢复调度任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:operationalTask:operate
dws:cluster:setCrossRegionSnapshotPolicy	授予设置跨区域备份配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:crossRegionBackupConfig:update
dws:cluster:startOperationalTask	授予调度器-打开调度器操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:operationalTask:operate
dws:cluster:stopOperationalTask	授予调度器-关闭调度器操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:operationalTask:operate
dws:cluster:switchLogicalCluster	授予逻辑集群-转换到逻辑集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:logicalCluster:operate
dws:cluster:syn	授予同步跨	write	cluster	• g:ResourceT	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cCrossRegionBackupClusterInfo	region 备份集群信息操作权限。		*	ag/<tag-key> • g:EnterpriseProjectId	
dws:cluster:syncCrossRegionBackupConfig	授予同步跨区域快照配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:syncCrossRegionBackupInfo	授予同步跨region 快照信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:syncLogicalCluster	授予逻辑集群-逻辑集群从后台同步操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:logicalCluster:get
dws:cluster:updateOperationalTaskConfig	授予调度器-修改调度器运维任务公共配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:operationalTask:get
dws:cluster:updateOperationalTask	授予调度器-修改调度任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:operationalTask:operate
dws:cluster:addPlanForWLM	授予工作负载管理-添加工作负载计划操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:addPlanStageForWLM	授予工作负载管理-添加工作负载计划阶段操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:add	授予工作负载	write	cluster	• g:ResourceT	dws:workLoad

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
QueueForWLM	管理-添加工作负载队列操作权限。		*	ag/<tag-key> • g:EnterpriseProjectId	Manager:operate
dws:cluster:addQueueUserForWLM	授予工作负载管理-添加工作负载队列的绑定用户操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:deletePlanForWLM	授予工作负载管理-删除工作负载计划操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:deletePlanStageForWLM	授予工作负载管理-删除工作负载计划阶段操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:deleteQueueForWLM	授予工作负载管理-删除工作负载队列操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:deleteQueueUserForWLM	授予工作负载管理-删除工作负载队列的绑定用户操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:exportPlanForWLM	授予工作负载管理-导出工作负载计划操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:getPlanDetailForWLM	授予工作负载管理-查询某个工作负载计划详细信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:cluster:getPlanLogForWLM	授予工作负载管理-查看计划执行日志操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:get
dws:cluster:getPlanQueueForWLM	授予工作负载管理-查询某个队列是否在计划中操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:get
dws:cluster:getPlanStageForWLM	授予工作负载管理-查询工作负载计划阶段操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:get
dws:cluster:listQueueForWLM	授予工作负载管理-获得当前集群的工作负载队列的名称列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:get
dws:cluster:getQueueDetailForWLM	授予工作负载管理-获得工作负载队列信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:get
dws:cluster:getQueueRuleForWLM	授予工作负载管理-获得工作负载队列异常规则信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:get
dws:cluster:importPlanForWLM	授予工作负载管理-导入工作负载计划操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:listPlanQueueForWLM	授予工作负载管理-查询所有工作负载计划	list	cluster *	• g:ResourceTag/<tag-key> • g:Enterprise	dws:workLoadManager:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	可用的队列信息操作权限。			ProjectId	
dws:cluster:listPlanForWLM	授予工作负载管理-查询工作负载计划操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:get
dws:cluster:listQueueUserForWLM	授予工作负载管理-获得工作负载队列的绑定用户列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:get
dws:cluster:listUserForWLM	授予工作负载管理-获得集群中所有未绑定工作负载队列的用户列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:get
dws:cluster:getClusterDBInfoForWLM	授予工作负载管理-查询集群数据库信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:get
dws:cluster:listClusterPlanForWLM	授予工作负载管理-查询集群中所有工作负载计划操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:get
dws:cluster:getClusterSchemaInfoForWLM	授予工作负载管理-查询集群模式空间信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:get
dws:cluster:getClusterVersionForWLM	授予工作负载管理-获得当前集群后台数据库的版本操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:get
dws:cluster:get	授予工作负载	read	cluster	• g:ResourceT	dws:workLoad

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
FunctionStatusForWLM	管理-获得工作负载功能开关状态操作权限。		*	ag/<tag-key> • g:EnterpriseProjectId	Manager:get
dws:cluster:setFunctionStatusForWLM	授予工作负载管理-设置工作负载功能开关状态操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:startPlanForWLM	授予工作负载管理-启动工作负载计划操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:stopPlanForWLM	授予工作负载管理-停止工作负载计划操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:switchPlanStageForWLM	授予工作负载管理-切换工作负载阶段操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:updatePlanStageForWLM	授予工作负载管理-修改工作负载计划阶段操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:updateQueueBaseForWLM	授予工作负载管理-更新工作负载队列基础信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:updateQueueResourceForWLM	授予工作负载管理-更新工作负载队列资源配置信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:cluster:updateQueueRuleForWLM	授予工作负载管理-更新工作负载队列异常规则信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:updateSchemaLimitForWLM	授予工作负载管理-更新模式空间限额操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:workLoadManager:operate
dws:cluster:getMonitorConfigForDMS	授予 DMS-查询采集配置或存储配置额操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:monitor:listClusterOverview	授予 DMS-获取集群概览操作权限。	list	-	-	-
dws:cluster:listClusterInstanceForDMS	授予 DMS-获取集群实例列表操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getDDLExamineDetailForDMS	授予 DMS-查询审核结果详细信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getClusterDnStreamForDMS	授予 DMS-查询 dn 数据流监控信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listClusterAlarmRuleForDMS	授予 DMS-查询租户侧告警规则列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getClusterInstance	授予 DMS-查	read	cluster	• g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ForDMS	询实例信息操作权限。		*	key> • g:EnterpriseProjectId	
dws:cluster:getHostNetMetricsForDMS	授予 DMS-查询网络状态操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:monitor:getHistoryMetrics	授予 DMS-查询历史监控数据操作权限。	read	-	-	-
dws:cluster:getMonitoringInfoForDMS	授予 DMS-查询监控数据操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listAlarmRuleForDMS	授予 DMS-租户侧根据告警 id 查询告警规则操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:updateCollectionItemForDMS	授予 DMS-更新采集配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:doDDLExamineActionForDMS	授予 DMS-手动触发审核操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:downloadDDLExamineDetailForDMS	授予 DMS-DDL 审核详情下载操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listInstanceDiskIOForDMS	授予 DMS-查询磁盘 IO 操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:Enterprise	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ProjectId	
dws:cluster:resetCollectionItemForDMS	授予 DMS-重置采集配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getQueryRangeForDMS	授予 DMS-查询时间句柄操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:monitor:getAlarmConfig	授予 DMS-租户侧查询所有集群和告警配置信息操作权限。	read	-	-	-
dws:cluster:switchoverCollectionItemForDMS	授予 DMS-切换采集开关操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:monitor:getOSMetrics	授予 DMS-查询 DWS 硬件资源使用情况操作权限。	read	-	-	-
dws:cluster:listPerfDashboardForDMS	授予 DMS-查询当前用户所有性能监控面板操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:disableCollectionItemForDMS	授予 DMS-关闭采集开关操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:monitor:getAggregationOSMetrics	授予 DMS-查询 DWS 集群硬件资源使用情况操作权	read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
dws:cluster:terminateSessionForDMS	授予 DMS-终止会话操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getPerfDashboardDetailForDMS	授予 DMS-通过面板 id 获取面板信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:monitor:createAlarmRule	授予 DMS-租户侧添加告警规则操作权限。	write	-	-	-
dws:cluster:enableCollectionItemForDMS	授予 DMS-开启采集开关操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listInstanceNetworkMetricsForDMS	授予 DMS-查询 DWS 集群节点各网卡流量操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:createPerfDashboardForDMS	授予 DMS-创建用户面板操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getMonitorMetricsForDMS	授予 DMS-获取首页监控项操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:createSQLProbeForDMS	授予 DMS-新增 SQL 探针操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:cluster:listInstanceIOStatusForDMS	授予 DMS-查询 DWS 集群各节点磁盘 IO 使用情况操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getMonitorMetricsByDimensionForDMS	授予 DMS-按维度获取指标操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:updateStorageConfigForDMS	授予 DMS-更新存储配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:monitor:updateAlarmRule	授予 DMS-租户侧修改告警规则操作权限。	write	-	-	-
dws:cluster:getInstanceIOAggResultForDMS	授予 DMS-查询 DWS 集群各节点磁盘 IO 汇聚使用情况操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:updatePerfDashboardForDMS	授予 DMS-修改用户面板操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getMonitorHistoryMetricsCost	授予 DMS-查询队列历史消耗操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:monitor:deleteAlarmRule	授予 DMS-租户侧删除规则操作权限。	write	-	-	-
dws:cluster:updateSQLProbeFo	授予 DMS-修改 SQL 探针操	write	cluster *	• g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rDMS	作权限。			key> • g:EnterpriseProjectId	
dws:cluster:startMonitorMetricsCollectionForDMS	授予 DMS-开始采集操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listInstanceStorageForDMS	授予 DMS-查询 DWS 集群各节点文件系统使用情况操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:deletePerfDashboardForDMS	授予 DMS-删除用户监控面板操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getMonitorMetricsDetailForDMS	授予 DMS-查询指标数据操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:deleteSQLProbeForDMS	授予 DMS-删除 SQL 探针操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:monitor:stopAlarmRule	授予 DMS-租户侧停用规则操作权限。	write	-	-	-
dws:cluster:stopMonitorMetricsCollectionForDMS	授予 DMS-停止采集操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listExceptionTableForDMS	授予 DMS-查询表倾斜或脏页率信息操作	list	cluster *	• g:ResourceTag/<tag-key> • g:Enterprise	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	权限。			ProjectId	
dws:cluster:getInstanceStorageAggForDMS	授予 DMS-查询 DWS 集群各节点文件系统使用情况操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getWDRSnapShotForDMS	授予 DMS-获取快照记录操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getPerfMetricsDataForDMS	授予 DMS-获取所有监控指标操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listQueryForDMS	授予 DMS-获取当前所有的查询操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getInstanceIOMetricsForDMS	授予 DMS-查询网卡 IO 数据操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getSQLProbeDetailForDMS	授予 DMS-查询 SQL 探针详情操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:switchoverMonitorMetricStatusForDMS	授予 DMS-切换采集开关操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:monitor:startAlarmRule	授予 DMS-租户侧启用规则操作权限。	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:monitor:getClusterStatus	授予 DMS-查询 DWS 集群状态操作权限。	read	-	-	-
dws:cluster:getPerfMetricsDetailForDMS	授予 DMS-通过 pmid 获取监控项操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listSlowInstanceForDMS	授予 DMS-查询慢节点操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getDDLExamineConfigForDMS	授予 DMS-查询采集配置操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getMonitoringViewStatusForDMS	授予 DMS-获取 DMS 视图状态操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:monitor:enableAlarm	授予 DMS-租户侧集群启用告警功能操作权限。	write	-	-	-
dws:cluster:createWDRSnapShotForDMS	授予 DMS-新增快照操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listExecuteStatusForDMS	授予 DMS-查询 DWS 集群查询执行情况操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getSlowInstanceD	授予 DMS-查	read	cluster	• g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
etailForDMS	询慢节点详情操作权限。		*	key> • g:EnterpriseProjectId	
dws:cluster:enableSQLProbeForDMS	授予 DMS-更新 SQL 探针启用状态操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getWDRConfigForDMS	授予 DMS-查询集群 WDR 配置操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:monitor:disableAlarm	授予 DMS-租户侧集群停用告警功能操作权限。	write	-	-	-
dws:cluster:getMonitoringViewForDMS	授予 DMS-获取可用菜单操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getDatabaseUsageForDMS	授予 DMS-查询 DWS 集群中数据库使用情况操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listSQLProbeForDMS	授予 DMS-分页查询 SQL 探针操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:monitor:getAlarmMetrics	授予 DMS-租户侧查询告警指标操作权限。	read	-	-	-
dws:monitor:listMetricStatus	授予 DMS-获取功能状态操作权限。	list	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dws:cluster:listSessionStatusForDMS	授予 DMS-查询 DWS 集群会话执行情况操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:downloadPerfHistoryForDMS	授予 DMS-下载历史监控趋势操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:addPerfItemForDMS	授予 DMS-添加监控项操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listClusterSessionForDMS	授予 DMS-获取当前所有的会话操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getSQLDiagnosticsForDMS	授予 DMS-查询 SQL 诊断详情操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:updateWDRSnapShotForDMS	授予 DMS-更新集群 WDR 配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:monitor:clearAlarm	授予 DMS-租户侧告警清除操作权限。	write	-	-	-
dws:cluster:executeSQLProbeForDMS	授予 DMS-执行 SQL 探针操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listQueryStatusFor	授予 DMS-获取查询的当前	list	cluster	• g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
DMS	状态操作权限。		*	key> • g:EnterpriseProjectId	
dws:cluster:getWDRReportForDMS	授予 DMS-获取报告记录操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listWLMQueueForDMS	授予 DMS-查询当前的工作负载队列操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:updatePerfItemForDMS	授予 DMS-更新监控项操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getQueryCostForDMS	授予 DMS-获取历史资源消耗操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:createWDRReportForDMS	授予 DMS-新增 WDR 报告操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:downloadWDRReportForDMS	授予 DMS-WDR 报告下载操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listDatabaseForDMS	授予 DMS-查询当前集群所有数据库操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listUserWLMQueu	授予 DMS-查询用户工作负	list	cluster *	• g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
eForDMS	载队列操作权限。			key> • g:EnterpriseProjectId	
dws:cluster:deletePerfItemForDMS	授予 DMS-删除监控项操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:monitor:getExceptionAlarmRule	授予 DMS-查询异常告警规则操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getWDRHostForDMS	授予 DMS-查询节点信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getHistoryPerfDataForDMS	授予 DMS-查询历史监控数据操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:deleteWDRReportForDMS	授予 DMS-删除 WDR 报告操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getPerfDetailByDimensionForDMS	授予 DMS-通过集群 id，维度获取监控对象操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:downloadPerfHistoryByIdForDMS	授予 DMS-下载历史监控趋势操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listWaitingWLMF	授予 DMS-获取当前等待的	list	cluster *	• g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
orDMS	查询操作权限。			key> • g:EnterpriseProjectId	
dws:cluster:getQueryPropertyForDMS	授予 DMS-获取查询属性操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listBucketForDMS	授予 DMS-获取 OBS 桶列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getHistoryQueryPropertyForDMS	授予 DMS-获取历史查询属性操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listExceptionWLMForDMS	授予 DMS-查询当前异常任务操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:terminateQueryForDMS	授予 DMS-终止查询操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:updateTaskForDMS	授予 DMS-更新任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:retryTaskForDMS	授予 DMS-重试任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listTaskForDMS	授予 DMS-任务查询操作权	list	cluster *	• g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。			key> • g:EnterpriseProjectId	
dws:cluster:syncIamUser	授予同步 IAM 用户到 DWS 数据库操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listDatabaseUser	授予查询用户/角色列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getDatabaseUser	授予查询用户基本信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:updateDatabaseUserInfo	授予修改用户基本信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:updateDatabaseAuthority	授予设置数据库对象权限操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getDatabaseAuthority	授予查询数据库对象权限操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getDisasterProgress	授予获取容灾进程接口操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getDatabaseOmUs	授予获取运维用户状态操作	read	cluster *	• g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
erStatus	权限。			key> • g:EnterpriseProjectId	
dws:cluster:executeDatabaseOmUserAction	授予执行运维用户操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getClusterInstancesInfo	授予查询集群实例逻辑集群详情操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getMetadataSyncStatus	授予 dataArts 元数据同步开启状态查询操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:startMetadataSync	授予开启 dataArts 元数据同步操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:stopMetadataSync	授予关闭 dataArts 元数据同步操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:updatePeriodCluster	授予更新包周期集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:periodCluster:modify
dws:cluster:createPeriodCluster	授予创建包周期集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:periodCluster:create
dws:cluster:deleteConfigTempl	授予删除配置模板操作权	write	cluster *	• g:ResourceTag/<tag-	dws:parameterGroup:delete

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ate	限。			key> • g:EnterpriseProjectId	
dws:cluster:getCountDown	授予获取倒计时信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getObsHotStorage	授予查询存算分离集群 OBS 数据使用情况操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listConfigTemplate	授予查询配置参数模板操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listDwsResource	授予获取集群实例资源列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:resources:list
dws:cluster:listDiscountNode	授予查询折扣套餐包节点操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:changeToPeriod	授予按需转包周期操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:ondemandToPeriod:operate
dws:cluster:rotateKey	授予密钥轮转操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:operateCluster	授予集群操作，修复集	write	cluster *	• g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	群、解除只读等操作权限。			key> • g:EnterpriseProjectId	
dws:cluster:doUpgrade	授予升级集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:cluster:doUpdate
dws:cluster:listUpgradePath	授予获取集群升级路径操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:cluster:getUpgradePaths
dws:cluster:listUpgradeRecord	授予获取集群升级记录操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dws:cluster:getUpgradeRecords
dws:cluster:createDatabaseUser	授予创建用户并授权权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:deleteDatabaseUser	授予删除用户权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getUserRoles	授予获取用户拥有角色列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getUserAuthority	授予查询用户权限列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:getDatabaseObject	授予查询数据库对象列表权	list	cluster *	• g:ResourceTag/<tag-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
s	限。			key> • g:EnterpriseProjectId	
dws:cluster:listLogicalClusterPlans	授予查询定时增删计划权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:createLogicalClusterPlan	授予添加定时增删计划权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:deleteLogicalClusterPlan	授予删除定时增删计划权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:listDatabaseUsers	授予查询所有数据库用户权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:switchLogicalClusterPlan	授予启停定时增删计划权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dws:cluster:updateLogicalClusterPlan	授予编辑定时增删计划权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

GaussDB(DWS)的 API 通常对应着一个或多个授权项。表 3-185 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

 版权所有 © 华为云计算技术有限公司

表3-181 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/alarm-subs	dws:alarm:createSubscription	-
DELETE /v2/{project_id}/alarm-subs/{alarm_sub_id}	dws:alarm:deleteSubscription	-
GET /v2/{project_id}/alarm-configs	dws:alarm:listConfig	-
GET /v2/{project_id}/alarms	dws:alarm:listDetail	-
GET /v2/{project_id}/alarm-statistic	dws:alarm:listStatistics	-
GET /v2/{project_id}/alarm-subs	dws:alarm:listSubscription	-
	dws:alarm:report	-
PUT /v2/{project_id}/alarm-subs/{alarm_sub_id}	dws:alarm:updateSubscription	-
POST /v1.0/{project_id}/clusters/{cluster_id}/cns/batch-create	dws:cluster:addCN	-
PUT /v2/{project_id}/clusters/{cluster_id}/workload/queues	dws:cluster:addQueueForWLM	-
	dws:cluster:assessRisk	-
POST /v2/{project_id}/clusters/{cluster_id}/eips/{eip_id}	dws:cluster:bindEIP	-
	dws:cluster:bindOrUnbindEIP	
POST /v2/{project_id}/clusters/{cluster_id}/elbs/{elb_id}	dws:cluster:bindELB	-
	dws:cluster:bindOrUnbindELB	-
POST /v1.0/{project_id}/clusters/{cluster_id}/cancel-readonly	dws:cluster:cancelReadonly	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/disaster-recovery/check-name	dws:cluster:checkConnection	-
	dws:cluster:checkDisasterRecoveryName	-
POST /v1/{project_id}/clusters/{cluster_id}/check-instance-storage	dws:cluster:expandDisk	-
	dws:cluster:resize	-
	dws:cluster:checkRestoreTable	-
	dws:cluster:scaleIn	-
	dws:cluster:checkSupportFineGrainedBackup	-
	dws:cluster:configureNetwork	-
POST /v1.0/{project_id}/snapshots/{snapshot_id}/linked-copy	dws:cluster:copySnapshot	-
POST /v1.0/{project_id}/clusters	dws:cluster:create	• ecs:cloudServerQuotas:get • ecs:cloudServerFlavors:get • bms:serverQuotas:get • bms:serverFlavors:get • vpc:subnets:get • vpc:vpcs:list • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:securityGroups:get • vpc:securityGroups:create • vpc:securityGroups:delete • vpc:securityGroupRules:create • vpc:securityGroupRules:delete • vpc:quotas:list • eip:publicIps:list • eip:publicIps:get • eip:publicIps:create • evs:quotas:get
POST /v2/{project_id}/clusters	dws:cluster:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/cluster-precheck	dws:cluster:create	-
POST /v1.0/{project_id}/clusters/{cluster_id}/dns	dws:cluster:createConnection	-
	dws:cluster:createDataSource	-
POST /v2/{project_id}/disaster-recoveries	dws:cluster:createDisasterRecovery	-
POST /v2/{project_id}/clusters/{cluster_id}/workload	dws:cluster:setFunctionStatusForWLM	-
POST /v1.0/{project_id}/snapshots	dws:cluster:createSnapshot	-
PUT /v2/{project_id}/clusters/{cluster_id}/snapshot-policies	dws:cluster:createSnapshotPolicy	-
POST /v2/{project_id}/clusters/{cluster_id}/workload/plans	dws:cluster:addPlanForWLM	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}	dws:cluster:delete	-
POST /v1.0/{project_id}/clusters/{cluster_id}/cns/batch-delete	dws:cluster:deleteCN	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/dns	dws:cluster:deleteConnection	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/ext-data-sources/{ext_data_source_id}	dws:cluster:deleteDataSource	-
DELETE /v2/{project_id}/disaster-	dws:cluster:deleteDisasterRecovery	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
recovery/{disaster_recovery_id}		
POST /v2/{project_id}/clusters/{cluster_id}/nodes/delete	dws:cluster:deleteNode	-
DELETE /v1.0/{project_id}/snapshots/{snapshot_id}	dws:cluster:deleteSnapshot	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/snapshot-policies/{id}	dws:cluster:deleteSnapshotPolicy	-
DELETE /v2/{project_id}/clusters/{cluster_id}/workload/queues	dws:cluster:deleteQueueForWLM	-
POST /v1.0/{project_id}/clusters/{cluster_id}/expand-instance-storage	dws:cluster:expandDisk	-
	dws:cluster:expandWithExistedNodes	-
	dws:cluster:getAntiAffinity	-
	dws:cluster:getCnCount	-
	dws:cluster:listConfig	-
	dws:cluster:getCredential	-
GET /v1.0/{project_id}/clusters/{cluster_id}	dws:cluster:getDetail	-
GET /v2/{project_id}/disaster-recoveries	dws:cluster:getDisasterRecovery	-
	dws:cluster:getDiskExpandScope	-
	dws:cluster:getEncryptInfo	-
	dws:cluster:getHistoryConfigDetail	-
	dws:cluster:getInstanceDetail	-
GET /v2/{project_id}/disaster-recovery/{disaster_re	dws:cluster:getDisasterRecovery	-
	dws:cluster:getInstanceDetail	-
	dws:cluster:getProcessTopo	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
covery_id}	dws:cluster:getRedistribution	-
	dws::listResourceByTag	-
	dws::countResourceByTag	-
	dws:cluster:getRestoreDatabase	-
	dws:cluster:getRoachConfig	-
	dws:cluster:getSnapshotEncryptInfo	-
	dws:cluster:getSnapshotPolicy	-
	dws:cluster:getSnapshotStorage	-
	dws:cluster:getTaskDetail	-
	dws:cluster:getVolumeInfo	-
GET /v1.0/{project_id}/clusters	dws:cluster:list	-
GET /v1.0/{project_id}/clusters/{cluster_id}/audit-log-records	dws:cluster:listAuditLog	-
	dws:cluster:listBucket	-
GET /v1.0/{project_id}/clusters/{cluster_id}/cns	dws:cluster:listCN	-
GET /v1.0/{project_id}/clusters/{cluster_id}/configurations	dws:cluster:listConfig	-
GET /v1.0/{project_id}/clusters/{cluster_id}/configurations/{configuration_id}	dws:cluster:listConfig	-
	dws:cluster:listConnection	-
	dws:cluster:listDatabase	-
GET /v1.0/{project_id}/clusters/{cluster_id}/ext-data-sources	dws:cluster:listDataSource	-
GET /v2/{project_id}/clusters/{cluster_id}/elbs	dws:cluster:listDN	-
	dws:cluster:listELB	-
	dws:cluster:listFlavorForResize	-
	dws:cluster:listFlavorForRestore	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	dws:cluster:listHistoryConfig	-
	dws:cluster:listNode	-
	dws::listResourceByTag	-
	dws:cluster:listRing	-
GET /v2/{project_id}/disaster-recovery-clusters	dws:cluster:listDisasterRecovery	-
GET /v1.0/{project_id}/clusters/{cluster_id}/shrink-numbers	dws:cluster:listRingForScaleIn	-
	dws:cluster:listSchema	-
	dws:cluster:listScaleInNode	-
GET /v1.0/{project_id}/clusters/{cluster_id}/snapshots	dws:cluster:listSnapshot	-
GET /v1.0/{project_id}/snapshots	dws:cluster:listSnapshot	-
GET /v1.0/{project_id}/snapshots/{snapshot_id}	dws:cluster:getSnapshotDetail	-
GET /v2/{project_id}/clusters/{cluster_id}/snapshot-policies	dws:cluster:listSnapshotPolicy	-
GET /v1.0/{project_id}/clusters/{cluster_id}/snapshots/statistics	dws:cluster:listSnapshotStatistics	-
	dws:cluster:listTable	-
GET /v1.0/{project_id}/clusters/{cluster_id}/tags	dws::listTagsForResource	-
GET /v2/{project_id}/clusters/{cluster_id}/workload	dws:cluster:getFunctionStatusForWLM	-
GET /v2/{project_id}/clusters/{cluster_id}/workload/queues	dws:cluster:listQueueForWLM	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/disaster-recovery/{disaster_recovery_id}/pause	dws:cluster:pauseDisasterRecovery	-
	dws:cluster:recoverRedistribution	-
POST /v2/{project_id}/clusters/{cluster_id}/redistribution	dws:cluster:redistribution	-
POST /v1.0/{project_id}/clusters/{cluster_id}/reset-password	dws:cluster:resetPassword	-
POST /v1.0/{project_id}/clusters/{cluster_id}/resize	dws:cluster:resize	-
	dws:cluster:resizeFlavor	-
	dws:cluster:resizeRetry	-
POST /v1.0/{project_id}/clusters/{cluster_id}/restart	dws:cluster:restart	-
POST /v2/{project_id}/disaster-recovery/{disaster_recovery_id}/recovery	dws:cluster:restore	-
	dws:cluster:restoreDisaster	-
POST /v1.0/{project_id}/snapshots/{snapshot_id}/actions	dws:cluster:restoreSnapshot	-
	dws:cluster:restoreTable	-
	dws:cluster:retryELBSwitch	-
POST /v1/{project_id}/clusters/{cluster_id}/description	dws:cluster:saveDescriptionInfo	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/maintenance-window	dws:cluster:scaleOut	-
	dws:cluster:setMaintainceWindow	-
POST /v1.0/{project_id}/clusters/{cluster_id}/cluster-shrink	dws:cluster:scaleIn	-
POST /v2/{project_id}/disaster-	dws:cluster:startDisasterRecovery	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
recovery/{disaster_recovery_id}/start		
POST /v1/{project_id}/snapshots/{snapshot_id}/stop	dws:cluster:stopSnapshot	-
	dws:cluster:suspendRedistribution	-
POST /v2/{project_id}/disaster-recovery/{disaster_recovery_id}/failover	dws:cluster:switchFailoverDisaster	-
POST /v1.0/{project_id}/clusters/{cluster_id}/switchover	dws:cluster:switchover	-
POST /v2/{project_id}/disaster-recovery/{disaster_recovery_id}/switchover	dws:cluster:switchoverDisasterRecovery	-
POST /v1.0/{project_id}/clusters/{cluster_id}/tags/batch-create	dws::tagResource	-
DELETE /v2/{project_id}/clusters/{cluster_id}/eips/{eip_id}	dws:cluster:unbindEIP	-
DELETE /v2/{project_id}/clusters/{cluster_id}/elbs/{elb_id}	dws:cluster:unbindELB	-
POST /v1.0/{project_id}/clusters/{cluster_id}/tags/batch-delete	dws::unTagResource	-
PUT /v2/{project_id}/clusters/{cluster_id}/configurations/{configuration_id}	dws:cluster:updateConfig	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/dns	dws:cluster:updateConnection	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v1.0/{project_id}/clusters/{cluster_id}/ext-data-sources/{ext_data_source_id}	dws:cluster:updateDataSource	-
	dws:cluster:updateInstanceAliasName	-
	dws:cluster:updateRoachConfig	-
	dws:cluster:updateScheduleConfig	-
	dws:cluster:updateSnapshotPolicy	-
	dws::updateTag	-
PUT /v2/{project_id}/disaster-recovery/{disaster_recovery_id}	dws:cluster:updateDisasterRecoveryConfig	-
POST /v2/{project_id}/event-subs	dws::updateTag	-
	dws:event:createSpec	-
	dws:event:createSubscription	-
DELETE /v2/{project_id}/event-subs/{event_sub_id}	dws:event:deleteSpec	-
	dws:event:deleteSubscription	-
GET /v2/{project_id}/events	dws:event:list	-
GET /v2/{project_id}/event-specs	dws:event:listSpec	-
GET /v2/{project_id}/event-subs	dws:event:listSubscription	-
	dws:event:report	-
PUT /v2/{project_id}/event-subs/{event_sub_id}	dws:event:updateSubscription	-
	dws:service:authorize	-
	dws:service:checkAuthorize	-
	dws:service:getClusterSum	-
	dws:service:getResourceStatistics	-
	dws:service:getStorageStatistics	-
GET	dws:service:listAZ	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1.0/{project_id}/availability-zones		
GET /v1.0/{project_id}/dss-pools	dws:service:listDssPools	-
	dws:service:listEps	-
GET /v1.0/{project_id}/dms/disk	dws:monitor:listHostDisk	-
GET /v1.0/{project_id}/dms/net	dws:monitor:listHostNet	-
GET /v1.0/{project_id}/dms/host-overview	dws:monitor:listClusterOverview	-
GET /v1.0/{project_id}/job/{job_id}	dws:service:listJobDetail	-
GET /v1.0/{project_id}/dms/metric-data	dws:monitor:listMonitorIndicatorData	-
GET /v1.0/{project_id}/dms/metric-data/indicators	dws:monitor:listMonitorIndicators	-
GET /v1.0/{project_id}/quotas	dws:service:listQuotas	-
GET /v2/{project_id}/node-types	dws:service:listSpec	-
GET /v1.0/{project_id}/statistics	dws:service:listStatistics	-
GET /v1.0/{project_id}/tags	dws::listTagsForProject	-
	dws:cluster:addOperationalTask	-
	dws:cluster:bindManageIp	-
	dws:cluster:checkAccessLts	-
	dws:cluster:checkDisasterRecoveryName	-
	dws:cluster:checkLogicalClusterData	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	dws:cluster:closeAccessLts	-
	dws:cluster:createDisasterRecovery	-
POST /v2/{project_id}/clusters/{cluster_id}/logical-clusters	dws:cluster:createLogicalCluster	-
	dws:cluster:createApplicationForDM	-
	dws:cluster:createClusterForDM	-
	dws:cluster:createConnectionForDM	-
	dws:cluster:createMappingForDM	-
	dws:cluster:deleteApplicationForDM	-
	dws:cluster:deleteClusterForDM	-
	dws:cluster:deleteConnectionForDM	-
	dws:cluster:deleteMappingForDM	-
	dws:cluster:dialsConnectionForDM	-
	dws:cluster:getApplicationForDM	-
	dws:cluster:listApplicationConfigForDM	-
	dws:cluster:listApplicationForDM	-
	dws:cluster:getClusterForDM	-
	dws:cluster:listClusterForDM	-
	dws:cluster:listConfigurationTemplateForDM	-
	dws:cluster:getConnectionForDM	-
	dws:cluster:listConnectionForDM	-
	dws:cluster:listDependApplicationForDM	-
	dws:cluster:getMappingForDM	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	dws:cluster:listMappingForDM	-
	dws:cluster:listProductForDM	-
	dws:cluster:updateConnectionForDM	-
	dws:cluster:updateMappingForDM	-
	dws:cluster:startApplicationForDM	-
	dws:cluster:stopApplicationForDM	-
	dws:cluster:deleteCrossRegionSnapshotPolicy	-
	dws:cluster:deleteDisasterRecovery	-
DELETE /v2/{project_id}/clusters/{cluster_id}/logical-clusters/{logical_cluster_id}	dws:cluster:deleteLogicalCluster	-
	dws:cluster:deleteOperationalTask	-
	dws:cluster:operateDisasterRecovery	-
PUT /v2/{project_id}/clusters/{cluster_id}/logical-clusters/{logical_cluster_id}	dws:cluster:updateLogicalCluster	-
	dws:cluster:listAllCrossRegionSnapshotConfig	-
	dws:cluster:getDisasterRecoveryProject	-
	dws:cluster:getDisasterRecoveryRegion	-
	dws:cluster:getLastOperationalTask	-
	dws:cluster:getLogicalClusterRings	-
	dws:cluster:getLogicalClusterVolume	-
	dws:cluster:getOperationalTaskConfig	-
	dws:cluster:getOperationalTaskDetail	-
	dws:cluster:getOperationalTask	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	Status	
	dws:cluster:listSnapshotRegion	-
	dws:cluster:getTargetAllCrossRegionSnapshotConfig	-
	dws:cluster:initLogicalClusterSwitch	-
	dws:cluster:listAccessLts	-
	dws:cluster:listDisasterRecovery	-
	dws:cluster:listLogicalCluster	-
	dws:cluster:listLogicalClusterTask	-
	dws:cluster:listOperationalTask	-
	dws:cluster:openAccessLts	-
	dws:cluster:pauseOperationalTask	-
	dws:cluster:getDisasterRecoveryDetail	-
	dws:cluster:refreshOperationalTask	-
POST /v2/{project_id}/clusters/{cluster_id}/logical-clusters/{logical_cluster_id}/restart	dws:cluster:restartLogicalCluster	-
	dws:cluster:resumeOperationalTask	-
	dws:cluster:setCrossRegionSnapshotPolicy	-
	dws:cluster:startOperationalTask	-
	dws:cluster:stopOperationalTask	-
	dws:cluster:switchLogicalCluster	-
	dws:cluster:syncCrossRegionBackupClusterInfo	-
	dws:cluster:syncCrossRegionBackupConfig	-
	dws:cluster:syncCrossRegionBackupInfo	-
	dws:cluster:syncLogicalCluster	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	dws:cluster:updateDisasterRecoveryConfig	-
	dws:cluster:updateOperationalTaskConfig	-
	dws:cluster:updateOperationalTask	-
	dws:cluster:addPlanForWLM	-
	dws:cluster:addPlanStageForWLM	-
	dws:cluster:addQueueForWLM	-
	dws:cluster:addQueueUserForWLM	-
	dws:cluster:deletePlanForWLM	-
	dws:cluster:deletePlanStageForWLM	-
	dws:cluster:deleteQueueForWLM	-
	dws:cluster:deleteQueueUserForWLM	-
	dws:cluster:exportPlanForWLM	-
	dws:cluster:getPlanDetailForWLM	-
	dws:cluster:getPlanDetailForWLM	-
	dws:cluster:getPlanLogForWLM	-
	dws:cluster:getPlanQueueForWLM	-
	dws:cluster:getPlanStageForWLM	-
	dws:cluster:listQueueForWLM	-
	dws:cluster:getQueueDetailForWLM	-
	dws:cluster:getQueueRuleForWLM	-
	dws:cluster:importPlanForWLM	-
	dws:cluster:listPlanQueueForW	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	LM	
	dws:cluster:listPlanForWLM	-
	dws:cluster:listQueueUserForWLM	-
	dws:cluster:listUserForWLM	-
	dws:cluster:getClusterDBInfoForWLM	-
	dws:cluster:listClusterPlanForWLM	-
	dws:cluster:getClusterSchemaInfoForWLM	-
	dws:cluster:getClusterVersionForWLM	-
	dws:cluster:getFunctionStatusForWLM	-
	dws:cluster:setFunctionStatusForWLM	-
	dws:cluster:startPlanForWLM	-
	dws:cluster:startPlanForWLM	-
	dws:cluster:stopPlanForWLM	-
	dws:cluster:stopPlanForWLM	-
	dws:cluster:switchPlanStageForWLM	-
	dws:cluster:switchPlanStageForWLM	-
	dws:cluster:updatePlanStageForWLM	-
	dws:cluster:updateQueueBaseForWLM	-
	dws:cluster:updateQueueResourceForWLM	-
	dws:cluster:updateQueueRuleForWLM	-
	dws:cluster:updateSchemaLimitForWLM	-
	dws:cluster:getMonitorConfigForDMS	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	dws:monitor:listClusterOverview	-
	dws:cluster:listClusterInstanceForDMS	-
	dws:cluster:getDDLExamineDetailForDMS	-
	dws:cluster:getClusterDnStreamForDMS	-
	dws:cluster:listClusterAlarmRuleForDMS	-
	dws:cluster:getClusterInstanceForDMS	-
	dws:cluster:getDDLExamineDetailForDMS	-
	dws:cluster:getHostNetMetricsForDMS	-
	dws:monitor:getHistoryMetrics	-
	dws:cluster:getMonitoringInfoForDMS	-
	dws:cluster:listAlarmRuleForDMS	-
	dws:cluster:updateCollectionItemForDMS	-
	dws:cluster:doDDLExamineActionForDMS	-
	dws:cluster:downloadDDLExamineDetailForDMS	-
	dws:cluster:listInstanceDiskIOForDMS	-
	dws:cluster:resetCollectionItemForDMS	-
	dws:monitor:listClusterOverview	-
	dws:monitor:listClusterOverview	-
	dws:cluster:getQueryRangeForDMS	-
	dws:monitor:getAlarmConfig	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	dws:cluster:switchoverCollectionItemForDMS	-
	dws:monitor:listClusterOverview	-
	dws:monitor:listClusterOverview	-
	dws:monitor:getOSMetrics	-
	dws:cluster:listPerfDashboardForDMS	-
	dws:cluster:disableCollectionItemForDMS	-
	dws:monitor:listClusterOverview	-
	dws:monitor:getAggregationOSMetrics	-
	dws:cluster:terminateSessionForDMS	-
	dws:cluster:getPerfDashboardDetailForDMS	-
	dws:monitor:createAlarmRule	-
	dws:cluster:enableCollectionItemForDMS	-
	dws:monitor:listClusterOverview	-
	dws:cluster:listInstanceNetworkMetricsForDMS	-
	dws:cluster:createPerfDashboardForDMS	-
	dws:cluster:getMonitorMetricsForDMS	-
	dws:monitor:listClusterOverview	-
	dws:cluster:createSQLProbeForDMS	-
	dws:cluster:listInstanceIOStatusForDMS	-
	dws:cluster:getMonitorMetricsByDimensionForDMS	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	dws:cluster:updateStorageConfigForDMS	-
	dws:monitor:listClusterOverview	-
	dws:monitor:updateAlarmRule	-
	dws:cluster:getInstanceIOAggResultForDMS	-
	dws:cluster:updatePerfDashboardForDMS	-
	dws:cluster:getMonitorHistoryMetricsCost	-
	dws:monitor:deleteAlarmRule	-
	dws:cluster:updateSQLProbeForDMS	-
	dws:cluster:startMonitorMetricsCollectionForDMS	-
	dws:cluster:listInstanceStorageForDMS	-
	dws:cluster:deletePerfDashboardForDMS	-
	dws:cluster:getMonitorMetricsDetailForDMS	-
	dws:cluster:deleteSQLProbeForDMS	-
	dws:monitor:stopAlarmRule	-
	dws:cluster:stopMonitorMetricsCollectionForDMS	-
	dws:cluster:listExceptionTableForDMS	-
	dws:cluster:getInstanceStorageAggForDMS	-
	dws:cluster:getWDRSnapShotForDMS	-
	dws:cluster:getPerfMetricsDataForDMS	-
	dws:cluster:listQueryForDMS	-
	dws:cluster:getInstanceIOMetricsForDMS	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	dws:cluster:getSQLProbeDetailForDMS	-
	dws:cluster:switchoverMonitorMetricStatusForDMS	-
	dws:monitor:startAlarmRule	-
	dws:monitor:getClusterStatus	-
	dws:cluster:getPerfMetricsDetailForDMS	-
	dws:cluster:listSlowInstanceForDMS	-
	dws:cluster:getDDLExamineConfigForDMS	-
	dws:cluster:getMonitoringViewStatusForDMS	-
	dws:monitor:enableAlarm	-
	dws:cluster:createWDRSnapShotForDMS	-
	dws:cluster:listExecuteStatusForDMS	-
	dws:cluster:listQueryForDMS	-
	dws:cluster:getSlowInstanceDetailForDMS	-
	dws:cluster:enableSQLProbeForDMS	-
	dws:cluster:getWDRConfigForDMS	-
	dws:monitor:disableAlarm	-
	dws:cluster:getMonitoringViewForDMS	-
	dws:cluster:createWDRSnapShotForDMS	-
	dws:cluster:getDatabaseUsageForDMS	-
	dws:cluster:listSQLProbeForDMS	-
	dws:monitor:getAlarmMetrics	-
	dws:monitor:listMetricStatus	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	dws:cluster:listSessionStatusForDMS	-
	dws:cluster:downloadPerfHistoryForDMS	-
	dws:cluster:addPerfItemForDMS	-
	dws:cluster:listClusterSessionForDMS	-
	dws:cluster:getSQLDiagnosticsForDMS	-
	dws:cluster:updateWDRSnapShotForDMS	-
	dws:monitor:clearAlarm	-
	dws:cluster:executeSQLProbeForDMS	-
	dws:cluster:listQueryStatusForDMS	-
	dws:cluster:getWDRReportForDMS	-
	dws:cluster:listWLMQueueForDMS	-
	dws:cluster:updatePerfItemForDMS	-
	dws:cluster:executeSQLProbeForDMS	-
	dws:cluster:getQueryCostForDMS	-
	dws:cluster:createWDRReportForDMS	-
	dws:cluster:downloadWDRReportForDMS	-
	dws:cluster:listDatabaseForDMS	-
	dws:cluster:listUserWLMQueueForDMS	-
	dws:cluster:deletePerfItemForDMS	-
	dws:cluster:createWDRReportForDMS	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	dws:cluster:getQueryCostForDMS	-
	dws:monitor:getExceptionAlarmRule	-
	dws:cluster:getWDRHostForDMS	-
	dws:cluster:getHistoryPerfDataForDMS	-
	dws:cluster:deleteWDRReportForDMS	-
	dws:cluster:getQueryCostForDMS	-
	dws:cluster:getPerfDetailByDimensionForDMS	-
	dws:cluster:downloadPerfHistoryByIdForDMS	-
	dws:cluster:listWaitingWLMForDMS	-
	dws:cluster:downloadWDRReportForDMS	-
	dws:cluster:getQueryPropertyForDMS	-
	dws:cluster:listBucketForDMS	-
	dws:cluster:getHistoryQueryPropertyForDMS	-
	dws:cluster:listExceptionWLMForDMS	-
	dws:cluster:addPerfItemForDMS	-
	dws:cluster:terminateQueryForDMS	-
	dws:cluster:updateTaskForDMS	-
	dws:cluster:retryTaskForDMS	-
	dws:cluster:listTaskForDMS	-
POST /v1/{project_id}/clusters/{cluster_id}/db-manager/sync-iam-user	dws:cluster:syncIamUser	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/clusters/{cluster_id}/db-manager/users	dws:cluster:listDatabaseUser	-
GET /v1/{project_id}/clusters/{cluster_id}/db-manager/users/{name}	dws:cluster:getDatabaseUser	-
POST /v1/{project_id}/clusters/{cluster_id}/db-manager/users/{name}	dws:cluster:updateDatabaseUserInfo	-
POST /v1/{project_id}/clusters/{cluster_id}/db-manager/authority	dws:cluster:updateDatabaseAuthority	-
GET /v1/{project_id}/clusters/{cluster_id}/db-manager/authority	dws:cluster:getDatabaseAuthority	-
GET /v1/{project_id}/disaster-recovery/{disaster_recovery_id}/show-progress	dws:cluster:getDisasterProgress	-
GET /v1/{project_id}/clusters/{cluster_id}/db-manager/om-user/status	dws:cluster:getDatabaseOmUserStatus	-
POST /v1/{project_id}/clusters/{cluster_id}/db-manager/om-user/action	dws:cluster:executeDatabaseOmUserAction	-
GET /v2/{project_id}/clusters/{cluster_id}/instances	dws:cluster:getClusterInstancesInfo	-
	dws:cluster:getMetadataSyncStatus	-
	dws:cluster:startMetadataSync	-
	dws:cluster:stopMetadataSync	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	dws:cluster:updatePeriodCluster	-
	dws:cluster:createPeriodCluster	-
	dws:cluster:deleteConfigTemplate	-
	dws:cluster:getCountDown	-
	dws:cluster:getObsHotStorage	-
	dws:cluster:listConfigTemplate	-
	dws:cluster:listDwsResource	-
	dws:cluster:listDiscountNode	-
	dws:cluster:changeToPeriod	-
	dws:cluster:rotateKey	-
	dws:cluster:operateCluster	-
	dws:cluster:setMaintainceWindow	-
	dws:cluster:doUpgrade	-
	dws:cluster:listUpgradePath	-
	dws:cluster:listUpgradeRecord	-
	dws:cluster:delete	-
POST /v1/{project_id}/clusters/{cluster_id}/db-manager/users	dws:cluster:createDatabaseUser	-
DELETE /v1/{project_id}/clusters/{cluster_id}/db-manager/users/{name}	dws:cluster:deleteDatabaseUser	-
GET /v1/{project_id}/clusters/{cluster_id}/db-manager/users/{name}/roles	dws:cluster:getUserRoles	-
GET /v1/{project_id}/clusters/{cluster_id}/db-manager/users/{name}/authority	dws:cluster:getUserAuthority	-
GET	dws:cluster:getDatabaseObjects	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/clusters/{cluster_id}/db-manager/objects	dws:cluster:listLogicalClusterPlans	-
	dws:cluster:createLogicalClusterPlan	-
	dws:cluster:deleteLogicalClusterPlan	-
	dws:cluster:listDatabaseUsers	-
	dws:cluster:switchLogicalClusterPlan	-
	dws:cluster:updateLogicalClusterPlan	-
	dws:cluster:getAccessWhitelistStatus	-
PUT /v1/{project_id}/clusters/{cluster_id}/access-whitelist/enable	dws:cluster:enableAccessWhitelist	-
PUT /v1/{project_id}/clusters/{cluster_id}/access-whitelist/disable	dws:cluster:disableAccessWhitelist	-
POST /v1/{project_id}/clusters/{cluster_id}/access-whitelist	dws:cluster:addAccessWhitelist	-
	dws:cluster:getAccessWhitelist	-
DELETE /v1/{project_id}/clusters/{cluster_id}/access-whitelist/{whitelist_id}	dws:cluster:deleteAccessWhitelist	-
PUT /v1/{project_id}/clusters/{cluster_id}/access-whitelist/{whitelist_id}	dws:cluster:getAccessWhitelistDetail	-
	dws:cluster:setAccessWhitelistDetail	-
DELETE /v2/{project_id}/clusters/{cluster_id}	dws:cluster:delete	-

 版权所有 © 华为云计算技术有限公司

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-186 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

GaussDB(DWS)定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-182 GaussDB(DWS)支持的资源类型

资源类型	URN
cluster	dws:<region>:<account-id>:cluster:<cluster-id>

说明

GaussDB(DWS)服务不支持在 IAM 自定义策略中的资源中指定资源进行授权。如需允许访问GaussDB(DWS)服务，请在 IAM 自定义策略的 Resource 元素中使用通配符号*，表示获得所有资源的该操作项权限。

条件（Condition）

GaussDB(DWS)服务不支持在身份策略中的条件键中配置服务级的条件键。
GaussDB(DWS)可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.9 应用中间件

3.9.1 微服务引擎 CSE

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。

 版权所有 © 华为云计算技术有限公司

- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 CSE 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 CSE 定义的条件键的详细信息请参见条件（Condition）。
- **“别名”**列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问，详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 CSE 的相关操作。

表3-183 CSE 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cse:config:upload	授予上传微服务配置权限	write	-	g:EnterpriseProjectId	cse:config:modify
cse:config:download	授予下载微服务配置权限	write	-	g:EnterpriseProjectId	cse:config:modify
cse:namespace:list	授予查看命名空间资源列表权限	list	-	-	cse:namespace:read
cse:namespace:get	授予查看命名空间资源权限	read	engine	• *g:ResourceTag/<tag-key>* • g:EnterpriseProjectId	cse:namespace:read
cse:namespa	授予创建命	write	engine	• *g:ResourceT*	cse:na

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ce:create	名空间资源权限			*ag/<tag-key>* • g:EnterpriseProjectId • g:TagKeys	mespace:write
cse:namespace:update	授予修改命名空间资源权限	write	engine	• *g:ResourceTag/<tag-key>* • g:EnterpriseProjectId	cse:namespace:write
cse:namespace:delete	授予删除命名空间资源权限	write	engine	• *g:ResourceTag/<tag-key>* • g:EnterpriseProjectId	cse:namespace:write
cse:policy:list	授予查看治理策略列表权限	list	-	-	cse:governance:get
cse:policy:get	授予查看治理策略信息权限	read	-	-	-
cse:policy:create	授予创建治理策略权限	write	-	-	cse:governance:modify
cse:policy:update	授予修改治理策略权限	write	-	-	cse:governance:modify
cse:policy:delete	授予删除治理策略权限	write	-	-	cse:governance:modify
cse:engine:get	授予查看引擎信息权限	read	engine	• *g:ResourceTag/<tag-key>* • g:EnterpriseProjectId	-
cse:engine:list	授予查询引擎信息列表权限	list	-	-	-
cse:engine:backupRecover	授予备份、恢复ServiceComb引擎数据和	write	engine	• *g:ResourceTag/<tag-key>* • g:Enterprise	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	变更备份策略权限。			ProjectId	
cse:engine:associatePublicips	授予绑定和解绑ServiceComb引擎公网访问权限。	write	engine	• *g:ResourceTag/<tag-key>* • g:EnterpriseProjectId	-
cse:engine:update	授予修改ServiceComb引擎配置和系统管理权限。	write	engine	• *g:ResourceTag/<tag-key>* • g:EnterpriseProjectId	-
cse:engine:resize	授予变更ServiceComb引擎规格权限	write	engine	• *g:ResourceTag/<tag-key>* • g:EnterpriseProjectId	-
cse:engine:create	授予创建引擎权限	write	-	• *g:ResourceTag/<tag-key>* • g:EnterpriseProjectId • g:TagKeys	-
cse:engine:upgrade	授予升级引擎权限	write	engine	• *g:ResourceTag/<tag-key>* • g:EnterpriseProjectId	-
cse:engine:delete	授予删除引擎权限	write	engine	• *g:ResourceTag/<tag-key>* • g:EnterpriseProjectId	-
cse:engine:tagResource	授予添加引擎标签的权限	write	engine	• *g:ResourceTag/<tag-key>* • g:EnterpriseProjectId	cse:engine:modify
cse:engine:unTagResource	授予删除引擎标签的权限	write	engine	• *g:ResourceTag/<tag-key>* • g:Enterprise	cse:engine:modify

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ProjectId	
cse:engine:listTags	授予查询项目下所有引擎标签的权限	list	-	-	cse:engine:list
cse:engine:listTagsForResource	授予查询引擎标签的权限	list	engine	• *g:ResourceTag/<tag-key>* • g:EnterpriseProjectId	cse:engine:get
cse:engine:listResourcesByTag	授予通过标签查询引擎列表的权限	list	-	g:TagKeys	cse:engine:list

CSE 的 API 通常对应着一个或多个授权项。表 3-188 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-184 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/enginemgr/engines/{engine_id}	cse:engine:get	-
PUT /v2/{project_id}/enginemgr/engines/{engine_id}/actions	cse:engine:modify	-
GET /v2/{project_id}/enginemgr/engines/{engine_id}/jobs/{job_id}	cse:engine:get	-
GET /v2/{project_id}/enginemgr/engines	cse:engine:list	-
POST /v1/{project_id}/kie/download	cse:config:download	-
POST /v1/{project_id}/kie/file	cse:config:upload	-
GET /v1/{project_id}/kie/kv	cse:namespace:get	-
POST	cse:namespace:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/kie/kv		
DELETE /v1/{project_id}/kie/kv	cse:namespace:update	-
PUT /v1/{project_id}/kie/kv/{kv_id}	cse:namespace:update	-
DELETE /v1/{project_id}/kie/kv/{kv_id}	cse:namespace:update	-
GET /v1/{project_id}/nacos/v1/console/namespaces	cse:namespace:get	-
DELETE /v1/{project_id}/nacos/v1/console/namespaces	cse:namespace:delete	-
POST /v1/{project_id}/nacos/v1/console/namespaces	cse:namespace:create	-
PUT /v1/{project_id}/nacos/v1/console/namespaces	cse:namespace:update	-
POST /v2/{project_id}/enginemgr/engines	cse:engine:create	-
GET /v2/{project_id}/enginemgr/engines/{engine_id}	cse:engine:get	-
DELETE /v2/{project_id}/enginemgr/engines/{engine_id}	cse:engine:delete	-
PUT /v2/{project_id}/enginemgr/engines/{engine_id}/resize	cse:engine:modify	-
PUT /v2/{project_id}/enginemgr/engines/{engine_id}/config	cse:engine:modify	-
PUT /v2/{project_id}/enginemgr/engines/{engine_id}/upgrade	cse:engine:upgrade	-
GET /v3/{project_id}/govern/governance/{kind}	cse:policy:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/govern/governance/{kind}	cse:policy:create	-
DELETE /v3/{project_id}/govern/governance/{kind}/{policy_id}	cse:policy:delete	-
GET /v3/{project_id}/govern/governance/{kind}/{policy_id}	cse:policy:get	-
PUT /v3/{project_id}/govern/governance/{kind}/{policy_id}	cse:policy:update	-
GET /v3/{project_id}/govern/governance/display	cse:policy:list	-
DELETE /v3/{project_id}/govern/route-rule/microservices/{service_name}	cse:policy:delete	-
PUT /v3/{project_id}/govern/route-rule/microservices/{service_name}	cse:policy:update	-
GET /v3/{project_id}/govern/route-rule/microservices/{service_name}	cse:policy:get	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的策略语句中指定该资源的 URN，策略仅作用于此资源；如未指定，Resource 默认为“*”，则策略将应用到所有资源。您也可以在策略中设置条件，从而指定资源类型。

CSE 定义了以下可以在策略的 Resource 元素中使用的资源类型。

表3-185 CSE 支持的资源类型

资源类型	URN
namespace	cse:<region>:<account-

 版权所有 © 华为云计算技术有限公司

资源类型	URN
	id>:namespace:<engine-id>/<namespace-id>
policy	cse:<region>:<account-id>:policy:<namespace-id>/<policy-name>
engine	cse:<region>:<account-id>:engine:<engine-id>

条件（Condition）

CSE 服务不支持在策略中的条件键中配置服务级的条件键。

CSE 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.9.2 分布式消息服务 Kafka 版 Kafka

云服务在 IAM 预置了常用的权限，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。

 版权所有 © 华为云计算技术有限公司

- 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

关于 DMS for Kafka 定义的资源类型的详细信息请参见资源类型（Resource）。

- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 DMS for Kafka 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 DMS for Kafka 的相关操作。

表3-186 DMS for Kafka 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dms:instance:connector	授予开启实例Smart Connect功能的权限。	Write	kafka *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:list	授予查看实例列表的权限。	List	kafka *	g:EnterpriseProjectId	-
dms:instance:scale	授予实例扩容权限。	Write	kafka *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:listConnectorSinkTask	授予查看Smart Connect任务列表的权限。	List	kafka *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:getBackgroundTask	授予查看实例后台任务详情权限。	Read	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:deleteBackgroundTask	授予删除实例后台任务的权	Write	kafka	• g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。			• g:EnterpriseProjectId	
dms:instance:create	授予创建实例的权限。	Write	kafka *	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • dms:ssl • dms:publicIp • dms:connector	-
dms:instance:update	授予修改实例的权限。	Write	kafka *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	• dms:instance:modify
dms:instance:getDetail	授予查看实例详情的权限。	Read	kafka *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
dms:instance:closeManager	授予关闭Kafka Manager的权限。	Write	kafka *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:deleteConnectorSinkTask	授予删除Smart Connect任务的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:modifyAuthInfo	授予修改实例访问密码的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dms:instance:modifyStatus	授予重启实例的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:delete	授予删除实例的权限。	Write	kafka *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:getConnectorSinkTask	授予查看Smart Connect任务详情的权限。	Read	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:createConnectorSinkTask	授予创建Smart Connect任务的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:updateConnectorSinkTask	授予更新Smart Connect任务的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:createConnectorSinkTask
dms:instance:resetAuthInfo	授予重置实例访问密码的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:message:get	授予查询消息详情的权限。	Read	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
			topic	-	
dms:message:send	授予发送消息的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:Enterprise	• dms:instance:modify

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ProjectId	
dms:topic:list	授予获取主题列表的权限。	List	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
			topic *	-	
dms:topic:modify	授予修改主题的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
			topic *	-	
dms:topic:create	授予创建主题的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
			topic	-	
dms:instance:getTopicDiskUsage	授予查询主题磁盘使用率的权限。	Read	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:topic:delete	授予删除主题的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
			topic *	-	
dms:topic:getAccessPolicy	授予获取主题授权策略的权限。	Read	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
			topic *	-	
dms:topic:autoCreate	授予开启或关闭自动创建主	Write	kafka	• g:ResourceTag/<tag-	• dms:instance:modify

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	题的权限。			key> • g:EnterpriseProjectId	
dms:topic:get	授予查询主题信息的权限。	Read	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
			topic *	-	
dms:topic:updateReplica	授予修改主题分区的副本的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
			topic *	-	
dms:topic:setAccessPolicy	授予为主题设置访问策略的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
			topic *	-	
dms:user:list	授予获取实例用户列表的权限。	List	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
dms:user:modify	授予修改实例用户信息的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
dms:user:delete	授予删除实例用户的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
dms:user:create	授予新增实例用户的权限。	Write	kafka	• g:ResourceTag/<tag-key>	• dms:instance:modify

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:EnterpriseProjectId	
dms:group:get	授予获取消费组的详情的权限。	Read	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
			consumerGroup *	-	
dms:group:list	授予获取消费组列表的权限。	List	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
			consumerGroup *	-	
dms:group:modify	授予修改消费组的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
			consumerGroup *	-	
dms:group:create	授予创建消费组的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
			consumerGroup *	-	
dms:group:delete	授予删除消费组的权限。	Write	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			consumerGroup *	-	
dms:coordinator:list	授予获取实例的协调器列表的权限。	List	kafka	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:reassignTopic	授予 Topic 分区平衡的权限。	Write	kafka *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

DMS for Kafka 的 API 通常对应着一个或多个授权项。表 3-191 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-187 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/instances/{instance_id}/messages	dms:message:get	-
PUT /v2/{project_id}/instances/{instance_id}/kafka-manager-password	dms:instance:modifyAuthInfo	-
PUT /v2/{project_id}/instances/{instance_id}/restart-kafka-manager	dms:instance:modifyStatus	-
DELETE /v2/{project_id}/kafka/instances/{instance_id}/management	dms:instance:closeManager	-
POST /v2/{project_id}/instances/action	dms:instance:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/instances	dms:instance:list	-
POST /v2/{project_id}/kafka/instances/{instance_id}/extend	dms:instance:scale	-
GET /v2/{project_id}/kafka/instances/{instance_id}/extend	dms:instance:getDetail	-
POST /v2/{project_id}/instances/{instance_id}/connector	dms:instance:connector	• vpc:vpcs:get • vpc:vpcs:list • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:securityGroups:get • vpc:subnets:get • eip:publicIps:get • eip:publicIps:list • eip:publicIps:update
GET /v2/{project_id}/instances/{instance_id}	dms:instance:getDetail	• vpc:vpcs:get • vpc:ports:get • vpc:securityGroups:get • vpc:subnets:get • eip:publicIps:get
PUT /v2/{project_id}/instances/{instance_id}	dms:instance:update	• vpc:vpcs:get • vpc:subnets:get • eip:publicIps:get • eip:publicIps:update • vpc:ports:get • vpc:securityGroups:get • vpc:securityGroups:update
DELETE /v2/{project_id}/instances/{instance_id}	dms:instance:delete	-
POST /v2/{project_id}/instances/{instance_id}/connector/tasks	dms:instance:createConnectorSinkTask	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/instances/{instance_id}/connector/tasks	dms:instance:listConnectorSinkTask	-
PUT /v2/{project_id}/instances/{instance_id}/connector/tasks/{task_id}/pause	dms:instance:updateConnectorSinkTask	-
PUT /v2/{project_id}/instances/{instance_id}/connector/tasks/{task_id}/resume	dms:instance:updateConnectorSinkTask	-
GET /v2/{project_id}/instances/{instance_id}/connector/tasks/{task_id}	dms:instance:getConnectorSinkTask	-
DELETE /v2/{project_id}/instances/{instance_id}/connector/tasks/{task_id}	dms:instance:deleteConnectorSinkTask	-
POST /v2/{project_id}/instances/{instance_id}/password	dms:instance:resetAuthInfo	-
GET /v2/{project_id}/instances/{instance_id}/tasks	dms:instance:getBackgroundTask	-
GET /v2/{project_id}/instances/{instance_id}/tasks/{task_id}	dms:instance:getBackgroundTask	-
DELETE /v2/{project_id}/instances/{instance_id}/tasks/{task_id}	dms:instance:deleteBackgroundTask	-
GET /v2/{project_id}/instances/{instance_id}/topics	dms:topic:list	-
PUT /v2/{project_id}/instances/{instance_id}/topi	dms:topic:modify	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
cs		
POST /v2/{project_id}/instances/{instance_id}/topics	dms:topic:create	-
GET /v2/{project_id}/instances/{instance_id}/topics/diskusage	dms:instance:getTopicDiskUsage	-
POST /v2/{project_id}/instances/{instance_id}/topics/delete	dms:topic:delete	-
POST /v2/{project_id}/instances/{instance_id}/crossvpc/modify	dms:instance:update	-
GET /v2/{project_id}/instances/{instance_id}/users	dms:user:list	-
PUT /v2/{project_id}/instances/{instance_id}/users	dms:user:delete	-
POST /v2/{project_id}/instances/{instance_id}/users	dms:user:create	-
PUT /v2/{project_id}/instances/{instance_id}/users/{user_name}	dms:user:modify	-
POST /v2/{project_id}/instances/{instance_id}/autotopic	dms:topic:autoCreate	-
GET /v2/{project_id}/instances/{instance_id}/management/topics/{topic}/partitions/{partition}/beginning-message	dms:message:get	-
GET /v2/{project_id}/instan	dms:message:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ces/{instance_id}/management/topics/{topic}/partitions/{partition}/end-message		
GET /v2/{project_id}/instances/{instance_id}/management/cluster	dms:instance:getDetail	-
GET /v2/{project_id}/instances/{instance_id}/management/groups/{group}	dms:group:get	-
GET /v2/{project_id}/instances/{instance_id}/management/topics/{topic}/partitions/{partition}/message	dms:message:get	-
GET /v2/{project_id}/instances/{instance_id}/management/topics/{topic}/messages	dms:message:get	-
GET /v2/{project_id}/instances/{instance_id}/management/coordinators	dms:coordinator:list	-
GET /v2/{project_id}/instances/{instance_id}/management/topics/{topic}	dms:topic:get	-
POST /v2/{project_id}/instances/{instance_id}/management/topics/{topic}/replicas-reassignment	dms:topic:updateReplica	-
GET /v2/{project_id}/instances/{instance_id}/groups	dms:group:list	-
POST /v2/{project_id}/kafka/instances	dms:instance:create	• vpc:vpcs:get • vpc:vpcs:list • vpc:ports:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
		• vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:securityGroups:get • vpc:subnets:get • eip:publicIps:get • eip:publicIps:list • eip:publicIps:update
GET /v1/{project_id}/instances/{instance_id}/topics/{topic_name}/accesspolicy	dms:topic:getAccessPolicy	-
POST /v1/{project_id}/instances/{instance_id}/topics/accesspolicy	dms:topic:setAccessPolicy	-
GET /v2/{project_id}/instances/{instance_id}/ces-hierarchy	dms:instance:getDetail	-
GET /v2/{project_id}/kafka/{instance_id}/tags	dms:instance:getDetail	-
GET /v2/{project_id}/kafka/tags	dms:instance:getDetail	-
POST /v2/{project_id}/kafka/{instance_id}/tags/action	dms:instance:update	-
POST /v2/{project_id}/kafka/instances/{instance_id}/reassign	dms:instance:reassignTopic	-
POST /v2/{project_id}/instances/{instance_id}/groups/batch-delete	dms:group:delete	-
POST /v2/{project_id}/kafka/instances/{instance_id}/group	dms:group:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v2/{engine}/{project_id}/instances/{instance_id}/groups/{group}	dms:group:modify	-
POST /v2/{project_id}/kafka/instances/{instance_id}/delete-connector	dms:instance:connector	-
POST /v2/{project_id}/instances/{instance_id}/messages/action	dms:message:send	-
GET /v2/{project_id}/kafka/instances/{instance_id}/topics/{topic}/partitions	dms:topic:get	-
GET /v2/{project_id}/kafka/instances/{instance_id}/topics/{topic}/producers	dms:topic:get	-
PUT /v2/{engine}/{project_id}/instances/{instance_id}/users/{user_name}	dms:user:modify	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-192 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

DMS for Kafka 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-188 DMS for Kafka 支持的资源类型

资源类型	URN
kafka	dms:<region>:<account-id>:kafka:<instance-id>
topic	dms:<region>:<account-id>:topic:<instance-id>/<topic-name>
consumerGroup	dms:<region>:<account-id>:consumerGroup:<instance-id>/<consumerGroup-name>

 版权所有 © 华为云计算技术有限公司

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 dms:）仅适用于对应服务的操作，详情请参见表 3-193。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

DMS for Kafka 支持的服务级条件键

DMS for Kafka 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-189 DMS for Kafka 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
dms:ssl	boolean	单值	根据实例是否开启 SSL 筛选访问权限。
dms:publicIp	boolean	单值	根据实例是否开启公网访问筛选访问权限。
dms:connector	boolean	单值	根据实例是否开启 Smart Connect 功能筛选访问权限。

3.9.3 分布式消息服务 RabbitMQ 版 RabbitMQ

云服务在 IAM 预置了常用的权限，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

 版权所有 © 华为云计算技术有限公司

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 DMS for RabbitMQ 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 DMS for RabbitMQ 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 DMS for RabbitMQ 的相关操作。

表3-190 DMS for RabbitMQ 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dms:instance:list	授予查看实例列表的权限。	List	rabbitmq *	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dms:instance:scale	授予实例扩容权限。	Write	rabbitmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:getBackgroundTask	授予查看实例后台任务详情权限。	Read	rabbitmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:deleteBackgroundTask	授予删除实例后台任务的权限。	Write	rabbitmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:create	授予创建实例的权限。	Write	rabbitmq *	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • dms:ssl • dms:publicIp	-
dms:instance:update	授予修改实例的权限。	Write	rabbitmq *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	• dms:instance:modify
dms:instance:getDetail	授予查看实例详情的权限。	Read	rabbitmq *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
dms:instance:delete	授予删除实例的权限。	Write	rabbitmq	• g:ResourceTag/<tag-key> • g:Enterprise	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ProjectId	
dms:instance:resetAuthInfo	授予重置实例访问密码的权限。	Write	rabbitmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:plugin:list	授予获取实例插件列表的权限。	List	rabbitmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:list
dms:plugin:modifyStatus	授予开启或关闭实例插件的权限。	Write	rabbitmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify

DMS for RabbitMQ 的 API 通常对应着一个或多个授权项。表 3-195 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-191 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/instances/action	dms:instance:delete	-
GET /v2/{project_id}/instances	dms:instance:list	-
POST /v2/{engine}/{project_id}/instances/{instance_id}/extend	dms:instance:scale	-
GET /v2/{engine}/{project_id}/instances/{instance_id}/extend	dms:instance:getDetail	-
GET /v2/{project_id}/instan	dms:instance:getDetail	• vpc:vpcs:get • vpc:ports:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ces/{instance_id}		• vpc:securityGroups:get • vpc:subnets:get • eip:publicIps:get
PUT /v2/{project_id}/instances/{instance_id}	dms:instance:update	• vpc:vpcs:get • vpc:subnets:get • eip:publicIps:get • eip:publicIps:update • vpc:ports:get • vpc:securityGroups:get • vpc:securityGroups:update
DELETE /v2/{project_id}/instances/{instance_id}	dms:instance:delete	-
POST /v2/{project_id}/instances/{instance_id}/password	dms:instance:resetAuthInfo	-
GET /v2/{project_id}/instances/{instance_id}/tasks	dms:instance:getBackgroundTask	-
GET /v2/{project_id}/instances/{instance_id}/tasks/{task_id}	dms:instance:getBackgroundTask	-
DELETE /v2/{project_id}/instances/{instance_id}/tasks/{task_id}	dms:instance:deleteBackgroundTask	-
GET /v2/{project_id}/instances/{instance_id}/rabbitmq/plugins	dms:plugin:list	-
PUT /v2/{project_id}/instances/{instance_id}/rabbitmq/plugins	dms:plugin:modifyStatus	-
POST /v2/{engine}/{project_id}/instances	dms:instance:create	• vpc:vpcs:get • vpc:vpcs:list • vpc:ports:get • vpc:ports:create • vpc:ports:update

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
		• vpc:ports:delete • vpc:securityGroups:get • vpc:subnets:get • eip:publicIps:get • eip:publicIps:list • eip:publicIps:update
GET /v2/{project_id}/rabbitmq/{instance_id}/tags	dms:instance:getDetail	-
GET /v2/{project_id}/rabbitmq/tags	dms:instance:getDetail	-
POST /v2/{project_id}/rabbitmq/{instance_id}/tags/action	dms:instance:update	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-196 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

DMS for RabbitMQ 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-192 DMS for RabbitMQ 支持的资源类型

资源类型	URN
rabbitmq	dms:<region>:<account-id>:rabbitmq:<instance-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。

 版权所有 © 华为云计算技术有限公司

- 服务级条件键（前缀通常为服务缩写，如 dms:）仅适用于对应服务的操作，详情请参见表 3-197。
- 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。

- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

DMS for RabbitMQ 支持的服务级条件键

DMS for RabbitMQ 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-193 DMS for RabbitMQ 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
dms:ssl	boolean	单值	根据实例是否开启 SSL 筛选访问权限。
dms:publicIp	boolean	单值	根据实例是否开启公网访问筛选访问权限。

3.9.4 分布式消息服务 RocketMQ 版 RocketMQ

云服务在 IAM 预置了常用的权限，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

 版权所有 © 华为云计算技术有限公司

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 DMS for RocketMQ 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 DMS for RocketMQ 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 DMS for RocketMQ 的相关操作。

表3-194 DMS for RocketMQ 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dms:instance:list	授予查看实例列表的权限。	List	rocketmq *	g:EnterpriseProjectId	-
dms:instance:create	授予创建实例的权限。	Write	rocketmq *	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • dms:ssl • dms:publicIp	-
dms:instance:update	授予修改实例的权限。	Write	rocketmq *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:RequestTag/<tag-key> • g:TagKeys	
dms:instance:getDetail	授予查看实例详情的权限。	Read	rocketmq *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
dms:instance:modifyConfig	授予修改实例配置的权限。	Write	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:delete	授予删除实例的权限。	Write	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:message:export	授予导出消息列表的权限。	Write	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
			topic	-	
dms:message:get	授予查询消息详情的权限。	Read	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
			topic	-	
dms:message:getTrace	授予查询消息轨迹的权限。	Read	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
dms:message:send	授予发送消息的权限。	Write	rocketmq	• g:ResourceTag/<tag-key> • g:Enterprise	• dms:instance:modify

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ProjectId	
dms:topic:list	授予获取主题列表的权限。	List	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
			topic *	-	
dms:topic:modify	授予修改主题的权限。	Write	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
			topic *	-	
dms:topic:create	授予创建主题的权限。	Write	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
			topic	-	
dms:topic:delete	授予删除主题的权限。	Write	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
			topic *	-	
dms:topic:getAccessPolicy	授予获取主题授权策略的权限。	Read	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
			topic *	-	
dms:topic:get	授予查询主题信息的权限。	Read	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
			topic *	-	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dms:user:list	授予获取实例用户列表的权限。	List	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
dms:user:get	授予获取实例用户详情的权限。	Read	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
dms:user:modify	授予修改实例用户信息的权限。	Write	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
dms:user:delete	授予删除实例用户的权限。	Write	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
dms:user:create	授予新增实例用户的权限。	Write	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
dms:group:get	授予获取消费组的详情的权限。	Read	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
			consumerGroup *	-	
dms:group:getAccessPolicy	授予获取消费组的访问策略的权限。	Read	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
			consumerGr	-	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			oup *		
dms:group:resetConsumeOffset	授予重置消费组的消费进度的权限。	Write	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
			consumerGroup *	-	
dms:group:list	授予获取消费组列表的权限。	List	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
			consumerGroup *	-	
dms:group:modify	授予修改消费组的权限。	Write	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
			consumerGroup *	-	
dms:group:create	授予创建消费组的权限。	Write	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
			consumerGroup *	-	
dms:group:delete	授予删除消费组的权限。	Write	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:modify
			consumerGr	-	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			oup *		
dms:broker:list	授予获取实例代理列表的权限。	List	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• dms:instance:get
dms:instance:createMetadataMigrationTask	授予创建实例元数据迁移任务的权限。	Write	rocketmq *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:listMetadataMigrationTasks	授予查询实例元数据迁移任务列表的权限。	Write	rocketmq *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:deleteMetadataMigrationTask	授予删除实例元数据迁移任务的权限。	Write	rocketmq *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dms:instance:resendDlqMsg	授予重发死信消息的权限。	Write	rocketmq	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

DMS for RocketMQ 的 API 通常对应着一个或多个授权项。表 3-199 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-195 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v2/{engine}/{project_id}/instances/{instance_id}/messages	dms:message:get	-
POST /v2/{project_id}/instances/{instance_id}/mes	dms:message:export	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
sages/export		
POST /v2/{project_id}/instances/action	dms:instance:delete	-
GET /v2/{project_id}/instances	dms:instance:list	-
GET /v2/{project_id}/instances/{instance_id}	dms:instance:getDetail	• vpc:vpcs:get • vpc:ports:get • vpc:securityGroups:get • vpc:subnets:get • eip:publicIps:get
PUT /v2/{project_id}/instances/{instance_id}	dms:instance:update	• vpc:vpcs:get • vpc:subnets:get • eip:publicIps:get • eip:publicIps:update • vpc:ports:get • vpc:securityGroups:get • vpc:securityGroups:update
DELETE /v2/{project_id}/instances/{instance_id}	dms:instance:delete	-
GET /v2/{engine}/{project_id}/instances/{instance_id}/trace	dms:message:getTrace	-
GET /v2/{project_id}/instances/{instance_id}/topics	dms:topic:list	-
POST /v2/{project_id}/instances/{instance_id}/topics	dms:topic:create	dms:topic:delete
GET /v2/{project_id}/instances/{instance_id}/users	dms:user:list	-
POST /v2/{project_id}/instances/{instance_id}/users	dms:user:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/instances/{instance_id}/users/{user_name}	dms:user:get	-
DELETE /v2/{project_id}/instances/{instance_id}/users/{user_name}	dms:user:delete	-
PUT /v2/{project_id}/instances/{instance_id}/users/{user_name}	dms:user:modify	-
GET /v2/{project_id}/instances/{instance_id}/topics/{topic}/accesspolicy	dms:topic:getAccessPolicy	-
GET /v2/{engine}/{project_id}/instances/{instance_id}/groups/{group_id}/accesspolicy	dms:group:getAccessPolicy	-
GET /v2/{project_id}/instances/{instance_id}/topics/{topic}/status	dms:topic:get	-
GET /v2/{project_id}/instances/{instance_id}/topics/{topic}/groups	dms:topic:get	-
GET /v2/{project_id}/instances/{instance_id}/groups/{group}/topics	dms:group:get	-
POST /v2/{engine}/{project_id}/instances/{instance_id}/groups/{group_id}/reset-message-offset	dms:group:resetConsumeOffset	-
GET /v2/{project_id}/instances/{instance_id}/brokers	dms:broker:list	-
GET /v2/{project_id}/instances/{instance_id}/grou	dms:group:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ps		
PUT /v2/{project_id}/instances/{instance_id}/groups	dms:group:modify	-
POST /v2/{project_id}/instances/{instance_id}/groups	dms:group:create	dms:group:delete
GET /v2/{project_id}/instances/{instance_id}/groups/{group}	dms:group:get	-
PUT /v2/{project_id}/instances/{instance_id}/groups/{group}	dms:group:modify	-
DELETE /v2/{project_id}/instances/{instance_id}/groups/{group}	dms:group:delete	-
GET /v2/{project_id}/instances/{instance_id}/topics/{topic}	dms:topic:get	-
PUT /v2/{project_id}/instances/{instance_id}/topics/{topic}	dms:topic:modify	-
DELETE /v2/{project_id}/instances/{instance_id}/topics/{topic}	dms:topic:delete	-
POST /v2/{engine}/{project_id}/instances	dms:instance:create	• vpc:vpcs:get • vpc:vpcs:list • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:securityGroups:get • vpc:subnets:get • eip:publicIps:get • eip:publicIps:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
		• eip:publicIps:update
POST /v2/{project_id}/rocketmq/{instance_id}/tags/action	dms:instance:update	-
GET /v2/{project_id}/rocketmq/{instance_id}/tags	dms:instance:getDetail	-
GET /v2/{project_id}/rocketmq/tags	dms:instance:getDetail	-
GET /v2/rocketmq/{project_id}/instances/{instance_id}/groups/{group}/clients	dms:group:get	-
POST /v2/{engine}/{project_id}/instances/{instance_id}/messages/deadletter-resend	dms:instance:resendDlqMsg	-
POST /v2/{engine}/{project_id}/instances/{instance_id}/messages/resend	dms:message:send	-
POST /v2/{project_id}/instances/{instance_id}/metadata	dms:instance:createMetadataMigrationTask	-
GET /v2/{project_id}/instances/{instance_id}/metadata	dms:instance:listMetadataMigrationTasks	-
DELETE /v2/{project_id}/instances/{instance_id}/metadata	dms:instance:deleteMetadataMigrationTask	-
GET /v2/{project_id}/rocketmq/instances/{instance_id}/configs	dms:instance:getDetail	-
PUT /v2/{project_id}/rocketmq/instances/{instance_id}/configs	dms:instance:modifyConfig	-

 版权所有 © 华为云计算技术有限公司

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-200 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

DMS for RocketMQ 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-196 DMS for RocketMQ 支持的资源类型

资源类型	URN
topic	dms:<region>:<account-id>:topic:<instance-id>/<topic-name>
consumerGroup	dms:<region>:<account-id>:consumerGroup:<instance-id>/<consumerGroup-name>
rocketmq	dms:<region>:<account-id>:rocketmq:<instance-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 dms:）仅适用于对应服务的操作，详情请参见表 3-201。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

DMS for RocketMQ 支持的服务级条件键

DMS for RocketMQ 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

 版权所有 © 华为云计算技术有限公司

表3-197 DMS for RocketMQ 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
dms:ssl	boolean	单值	根据实例是否开启 SSL 筛选访问权限。
dms:publicIp	boolean	单值	根据实例是否开启公网访问筛选访问权限。

3.9.5 API 网关 APIG

云服务在 IAM 预置了常用的权限，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 apig 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。

 版权所有 © 华为云计算技术有限公司

- 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
- 如果此列条件键没有值（-），表示此操作不支持指定条件键。

关于 apig 定义的条件键的详细信息请参见条件（Condition）。

- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 apig 的相关操作。

表3-198 apig 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:acl:list	授予权限以查看 ACL 策略列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:acls:list
apig:acl:create	授予权限以创建 ACL 策略。	Write	instance *	g:ResourceTag/<tag-key>	• apig:acls:create
apig:acl:batchDelete	授予权限以批量删除 ACL 策略。	Write	instance *	g:ResourceTag/<tag-key>	• apig:acls:delete
apig:acl:delete	授予权限以删除 ACL 策略。	Write	instance *	g:ResourceTag/<tag-key>	• apig:acls:delete
apig:acl:get	授予权限以查看 ACL 策略详情。	Read	instance *	g:ResourceTag/<tag-key>	• apig:acls:get
apig:acl:update	授予权限以修改 ACL 策略。	Write	instance *	g:ResourceTag/<tag-key>	• apig:acls:update
apig:api:bindAcl	授予权限以绑定 API 和 ACL 策略。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:bindAcls
apig:api:batchUnbindAcl	授予权限以批量解除 API 和 ACL 策略的绑定关系。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:unbindAcls
apig:api:unbindAcl	授予权限以解除 API 和 ACL 策略的绑定关系。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:unbindAcls
apig:api:listBou	授予权限以获	List	instan	g:ResourceTag/	• apig:apis:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ndAcl	取 API 绑定的 ACL 策略列表。		ce *	<tag-key>	BindedAcls
apig:acl:listBoundApi	授予权限以获取 ACL 策略绑定的 API 列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:acls:listBindedApis
apig:acl:listUnboundApi	授予权限以获取 ACL 策略未绑定的 API 列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:acls:listUnbindedApis
apig:api:bindRequestThrottling	授予权限以绑定 API 和流控策略。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:bindThrottles
apig:api:batchUnbindRequestThrottling	授予权限以批量解除 API 和流控策略的绑定关系。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:unbindThrottles
apig:api:unbindRequestThrottling	授予权限以解除 API 和流控策略的绑定关系。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:unbindThrottles
apig:requestThrottling:listBoundApi	授予权限以获取流控策略绑定的 API 列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:throttles:listBindedApis
apig:api:listBoundRequestThrottling	授予权限以获取 API 绑定的流控策略列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:apis:listBindedThrottles
apig:requestThrottling:listUnboundApi	授予权限以获取流控策略未绑定的 API 列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:throttles:listUnbindedApis
apig:apiGroup:list	授予权限以获取 API 分组列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:groups:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:apiGroup:create	授予权限以创建 API 分组。	Write	instance *	g:ResourceTag/<tag-key>	• apig:groups:create
apig:apiGroup:delete	授予权限以删除 API 分组。	Write	instance *	g:ResourceTag/<tag-key>	• apig:groups:delete
apig:apiGroup:get	授予权限以查询 API 分组详情。	Read	instance *	g:ResourceTag/<tag-key>	• apig:groups:get
apig:apiGroup:update	授予权限以修改 API 分组。	Write	instance *	g:ResourceTag/<tag-key>	• apig:groups:update
apig:apiGroup:checkApiGroupNameExistOrNot	授予权限以校验 API 分组名称是否存在。	Read	instance *	g:ResourceTag/<tag-key>	• apig:groups:get
apig:api:list	授予权限以获取 API 列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:apis:list
apig:api:create	授予权限以创建 API。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:create
apig:api:delete	授予权限以删除 API。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:delete
apig:api:get	授予权限以查询 API 详情。	Read	instance *	g:ResourceTag/<tag-key>	• apig:apis:get
apig:api:update	授予权限以修改 API。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:update
apig:api:onlineOrOffline	授予权限以发布或下线 API。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:publish • apig:apis:offline
apig:api:batchDelete	授予权限以批量删除 API。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:delete
apig:api:checkApiPathOrApiNameExistOrNot	授予权限以校验 API 定义。	Read	instance *	g:ResourceTag/<tag-key>	• apig:apis:get
apig:api:debug	授予权限以调试 API。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:debug

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:api:batchOnlineOrOffline	授予权限以批量发布或下线API。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:publish • apig:apis:offline
apig:api:listHistoryVersion	授予权限以查询 API 历史版本列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:apis:get
apig:api:switchVersion	授予权限以切换 API 版本。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:publish
apig:api:getRuntimeDefinition	授予权限以查询 API 运行时定义。	Read	instance *	g:ResourceTag/<tag-key>	• apig:apis:get
apig:api:deleteHistoryVersion	授予权限以根据版本编号下线 API。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:offline
apig:api:getHistoryVersion	授予权限以获取版本详情。	Read	instance *	g:ResourceTag/<tag-key>	• apig:apis:get
apig:app:list	授予权限以获取 APP 列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:apps:list
apig:app:create	授予权限以创建 APP。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apps:create
apig:app:delete	授予权限以删除 APP。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apps:delete
apig:app:get	授予权限以查看 APP 详情。	Read	instance *	g:ResourceTag/<tag-key>	• apig:apps:get
apig:app:update	授予权限以修改 APP 信息。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:update
apig:app:listAppCode	授予权限以查询 APP Code 列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:appCodes:list
apig:app:createAppCode	授予权限以创建 APP Code。	Write	instance *	g:ResourceTag/<tag-key>	• apig:appCodes:create
apig:app:generateAppCode	授予权限以自动生成 APP	Write	instance *	g:ResourceTag/<tag-key>	• apig:appCodes:update

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	Code。				
apig:app:deleteAppCode	授予权限以删除 APP Code。	Write	instance *	g:ResourceTag/<tag-key>	• apig:appCodes:delete
apig:app:getAppCode	授予权限以获取 APP Code 详情。	Read	instance *	g:ResourceTag/<tag-key>	• apig:appCodes:get
apig:app:resetSecret	授予权限以重置 APP 的密钥。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apps:update
apig:app:validate	授予权限以校验 APP 是否存在。	Read	instance *	g:ResourceTag/<tag-key>	• apig:apps:get
apig:app:getBoundQuota	授予权限以查询 APP 关联的凭据配额策略。	Read	instance *	g:ResourceTag/<tag-key>	• apig:apps:get
apig:app:bindApi	授予权限以绑定 API 和 APP。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:grantAppAccess
apig:app:unbindApi	授予权限以解除 API 和 APP 的绑定关系。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:relieveAppAccess
apig:app:listBoundApi	授予权限以查看 APP 已绑定的 API 列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:apps:listBindedApis
apig:api:listBoundApp	授予权限以查看 API 已绑定的 APP 列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:apis:listBindedApps
apig:app:listUnboundApi	授予权限以查看 APP 未绑定的 API 列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:apps:listUnbindedApis
apig:api:export	授予权限以导出 API。	Read	instance *	g:ResourceTag/<tag-key>	• apig:apis:export
apig:api:import	授予权限以导入 API。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:import

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:asyncTask:get	授予权限以查看异步任务结果详情。	Read	instance *	g:ResourceTag/<tag-key>	• apig:apis:export • apig:apis:import
apig:certificate:list	授予权限以获取 SSL 证书列表。	List	instance	g:ResourceTag/<tag-key>	-
apig:certificate:create	授予权限以创建 SSL 证书。	Write	instance	g:ResourceTag/<tag-key>	-
apig:certificate:delete	授予权限以删除 SSL 证书。	Write	instance	g:ResourceTag/<tag-key>	-
apig:certificate:get	授予权限以获取 SSL 证书详情。	Read	instance	g:ResourceTag/<tag-key>	-
apig:certificate:update	授予权限以修改 SSL 证书。	Write	instance	g:ResourceTag/<tag-key>	-
apig:certificate:listBoundDomain	授予权限以获取 SSL 证书已绑定的域名列表。	List	instance	g:ResourceTag/<tag-key>	-
apig:certificate:batchBindDomain	授予权限以绑定域名到 SSL 证书。	Write	instance	g:ResourceTag/<tag-key>	-
apig:certificate:batchUnbindDomain	授予权限以解绑 SSL 证书绑定的域名。	Write	instance	g:ResourceTag/<tag-key>	-
apig:apiGroup:batchBindCertificateToDomain	授予权限以绑定 SSL 证书到域名。	Write	instance *	g:ResourceTag/<tag-key>	• apig:domains:bindCertificate
apig:apiGroup:batchUnbindCertificateFromDomain	授予权限以解绑域名绑定的证书。	Write	instance *	g:ResourceTag/<tag-key>	• apig:domains:unbindCertificate
apig:loadBalanceChannel:list	授予权限以获取负载通道列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:loadBalanceChannel:create	授予权限以创建负载通道。	Write	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:create
apig:loadBalanceChannel:delete	授予权限以删除负载通道。	Write	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:delete
apig:loadBalanceChannel:get	授予权限以获取负载通道详情。	Read	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:get
apig:loadBalanceChannel:update	授予权限以更新负载通道。	Write	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:update
apig:loadBalanceChannel:updateHealthCheckConfig	授予权限以修改负载通道健康检查配置。	Write	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:update
apig:loadBalanceChannel:listServerGroup	授予权限以查询负载通道后端服务器组列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:get
apig:loadBalanceChannel:createServerGroup	授予权限以添加或更新 VPC 通道后端服务器组。	Write	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:addOrUpdateMemberGroups
apig:loadBalanceChannel:deleteServerGroup	授予权限以删除 VPC 通道后端服务器组。	Write	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:deleteMemberGroup
apig:loadBalanceChannel:getServerGroup	授予权限以查看指定的 VPC 通道后端服务器组详情。	Read	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:get
apig:loadBalanceChannel:updateServerGroup	授予权限以更新 VPC 通道后端服务器组。	Write	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:updateMemberGroup
apig:loadBalanceChannel:listBackendServerAddress	授予权限以获取负载通道后端实例列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:loadBalanceChannel:createBackendServerAddress	授予权限以添加或更新负载通道后端实例。	Write	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:addInstance
apig:loadBalanceChannel:updateBackendServerAddress	授予权限以更新负载通道后端实例。	Write	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:addInstance
apig:loadBalanceChannel:deleteBackendServerAddress	授予权限以删除负载通道后端实例。	Write	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:deleteInstance
apig:loadBalanceChannel:batchDisableBackendServerAddress	授予权限以批量修改后端服务器状态不可用。	Write	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:batchDisableInstance
apig:loadBalanceChannel:batchEnableBackendServerAddress	授予权限以批量修改后端服务器状态可用。	Write	instance *	g:ResourceTag/<tag-key>	• apig:vpcChannels:batchEnableInstance
apig:instance:listTag	授予权限以获取标签列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:tags:list
apig:api:listUnboundPlugin	授予权限以获取 API 可绑定的插件列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:apis:listBindedPlugins
apig:api:listBoundPlugin	授予权限以获取 API 已绑定的插件列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:apis:listBindedPlugins
apig:api:bindPlugin	授予权限以绑定插件到API。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:bindPlugins
apig:api:unbindPlugin	授予权限以解绑 API 绑定的插件。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:unbindPlugins
apig:plugin:list	授予权限以获取插件列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:plugins:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:plugin:create	授予权限以创建插件。	Write	instance *	g:ResourceTag/<tag-key>	• apig:plugins:create
apig:plugin:delete	授予权限以删除插件。	Write	instance *	g:ResourceTag/<tag-key>	• apig:plugins:delete
apig:plugin:get	授予权限以获取插件详情。	Read	instance *	g:ResourceTag/<tag-key>	• apig:plugins:get
apig:plugin:update	授予权限以修改插件。	Write	instance *	g:ResourceTag/<tag-key>	• apig:plugins:update
apig:plugin:bindApi	授予权限以绑定 API 到插件。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:bindPlugins
apig:plugin:listUnbindApi	授予权限以获取插件可绑定的 API 列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:plugins:listUnbindedApis
apig:plugin:listBoundApi	授予权限以获取插件已绑定的 API 列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:plugins:listBindedApis
apig:plugin:unbindApi	授予权限以解绑插件绑定的API。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:unbindPlugins
apig:apiGroup:listGatewayResponse	授予权限以获取分组自定义响应列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:gatewayResponses:list
apig:apiGroup:createGatewayResponse	授予权限以创建分组自定义响应。	Write	instance *	g:ResourceTag/<tag-key>	• apig:gatewayResponses:create
apig:apiGroup:deleteGatewayResponse	授予权限以删除分组自定义响应。	Write	instance *	g:ResourceTag/<tag-key>	• apig:gatewayResponses:delete
apig:apiGroup:getGatewayResponse	授予权限以获取分组自定义响应详情。	Read	instance *	g:ResourceTag/<tag-key>	• apig:gatewayResponses:get
apig:apiGroup:updateGatewayResponse	授予权限以修改分组自定义响应。	Write	instance *	g:ResourceTag/<tag-key>	• apig:gatewayResponses:updat

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:apiGroup:deleteGatewayResponseType	授予权限以删除分组指定错误类型的自定义响应配置。	Write	instance *	g:ResourceTag/<tag-key>	• apig:gatewayResponses:update
apig:apiGroup:getGatewayResponseType	授予权限以获取分组下指定错误类型的自定义响应。	Read	instance *	g:ResourceTag/<tag-key>	• apig:gatewayResponses:get
apig:apiGroup:updateGatewayResponseType	授予权限以修改分组下指定错误类型的自定义响应。	Write	instance *	g:ResourceTag/<tag-key>	• apig:gatewayResponses:update
apig:instance:listApiOutline	授予权限以获取 API 概况。	List	instance *	g:ResourceTag/<tag-key>	• apig:apis:get
apig:instance:listAppOutline	授予权限以获取 APP 概况。	List	instance *	g:ResourceTag/<tag-key>	• apig:apps:get
apig:instance:listApiGroupOutline	授予权限以获取 API 分组概况。	List	instance *	g:ResourceTag/<tag-key>	• apig:groups:get
apig:environmentVariable:list	授予权限以查询环境变量列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:variables:list
apig:environmentVariable:create	授予权限以新建环境变量。	Write	instance *	g:ResourceTag/<tag-key>	• apig:variables:create
apig:environmentVariable:delete	授予权限以删除环境变量。	Write	instance *	g:ResourceTag/<tag-key>	• apig:variables:delete
apig:environmentVariable:get	授予权限以获取环境变量详情。	Read	instance *	g:ResourceTag/<tag-key>	• apig:variables:get
apig:environmentVariable:update	授予权限以修改环境变量。	Write	instance *	g:ResourceTag/<tag-key>	• apig:variables:update
apig:environment:list	授予权限以获取环境列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:envs:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:environment:create	授予权限以创建环境。	Write	instance *	g:ResourceTag/<tag-key>	• apig:envs:create
apig:environment:delete	授予权限以删除环境。	Write	instance *	g:ResourceTag/<tag-key>	• apig:envs:delete
apig:environment:update	授予权限以修改环境。	Write	instance *	g:ResourceTag/<tag-key>	• apig:envs:update
apig:instance:listMetricData	授予权限以查询实例监控数据。	List	instance *	g:ResourceTag/<tag-key>	• apig:metricData:get
apig:instance:listApiMonitoring	授予权限以查询最近一段时间 API 的统计信息。	List	instance *	g:ResourceTag/<tag-key>	• apig:apis:get
apig:instance:listApiGroupMonitoring	授予权限以查询最近一小时内 API 分组的统计信息。	List	instance *	g:ResourceTag/<tag-key>	• apig:groups:get
apig:requestThrottling:list	授予权限以获取流控策略列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:throttles:list
apig:requestThrottling:create	授予权限以创建流控策略。	Write	instance *	g:ResourceTag/<tag-key>	• apig:throttles:create
apig:requestThrottling:delete	授予权限以删除流控策略。	Write	instance *	g:ResourceTag/<tag-key>	• apig:throttles:delete
apig:requestThrottling:get	授予权限以获取流控策略详情。	Read	instance *	g:ResourceTag/<tag-key>	• apig:throttles:get
apig:requestThrottling:update	授予权限以修改流控策略。	Write	instance *	g:ResourceTag/<tag-key>	• apig:throttles:update
apig:requestThrottling:batchDelete	授予权限以批量删除流控策略。	Write	instance *	g:ResourceTag/<tag-key>	• apig:throttles:delete
apig:api:bindSignatureKey	授予权限以绑定签名密钥和 API。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:bindSigns

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:api:unbindSignatureKey	授予权限以解除签名密钥和API的绑定关系。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:unbindSigns
apig:signatureKey:listBoundApi	授予权限以获取签名密钥绑定的API列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:signs:listBindedApis
apig:api:listBoundSignatureKey	授予权限以获取API绑定的签名密钥列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:apis:listBindedSigns
apig:signatureKey:listUnboundApi	授予权限以查询所有未绑定到该签名密钥上的API列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:signs:listUnbindedApis
apig:signatureKey:list	授予权限以获取签名密钥列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:signs:list
apig:signatureKey:create	授予权限以创建签名密钥。	Write	instance *	g:ResourceTag/<tag-key>	• apig:signs:create
apig:signatureKey:delete	授予权限以删除签名密钥。	Write	instance *	g:ResourceTag/<tag-key>	• apig:signs:delete
apig:signatureKey:update	授予权限以修改签名密钥。	Write	instance *	g:ResourceTag/<tag-key>	• apig:signs:update
apig:requestThrottling:listSpecial	授予权限以获取流控特殊设置列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:specialThrottles:get
apig:requestThrottling:createSpecial	授予权限以创建流控特殊设置。	Write	instance *	g:ResourceTag/<tag-key>	• apig:specialThrottles:create
apig:requestThrottling:deleteSpecial	授予权限以删除流控特殊设置。	Write	instance *	g:ResourceTag/<tag-key>	• apig:specialThrottles:delete
apig:requestThr	授予权限以修	Write	instan	g:ResourceTag/	• apig:special

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ottling:updateSpecial	改某个流控策略下的某个特殊设置。		ce *	<tag-key>	Throttles:update
apig:instance:listSingleInstanceTag	授予权限以查询指定的实例标签列表。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:instanceTags:list
apig:instance:batchCreateOrDeleteTag	授予权限以实现批量添加或删除实例标签的功能。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:instanceTags:create • apig:instanceTags:delete
			-	• g:RequestTag/<tag-key> • g:TagKeys	
apig::listTag	授予权限以获取项目下所有实例标签。	List	-	-	• apig:instanceTags:list
apig:instance:getNumByTags	授予权限以实现通过标签查询实例数量的功能。	Read	instance *	-	-
			-	g:TagKeys	
apig:instance:listByTags	授予权限以实现通过标签查询实例列表的功能。	List	instance *	-	-
			-	g:TagKeys	
apig:instance:list	授予权限以获取专享版实例列表。	List	-	-	• apig:instances:list
apig:instance:create	授予权限以创建专享版实例。	Write	-	• g:RequestTag/<tag-key> • g:TagKeys	• apig:instances:create
apig:instance:delete	授予权限以删除专享版实例。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:instances:delete

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:instance:get	授予权限以查看专享版实例详情。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:instances:get
apig:instance:update	授予权限以更新专享版实例。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:instances:update
apig:instance:unbindEip	授予权限以解绑专享版实例的 EIP。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:instances:update
apig:instance:bindOrChangeEip	授予权限以添加或更换专享版实例的 EIP。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:instances:update
apig:instance:deleteOutboundEip	授予权限以关闭专享版实例的公网出口。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:instances:update
apig:instance:createOutboundEip	授予权限以开启专享版实例的公网出口。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:instances:update
apig:instance:changeOutboundEipBandwidth	授予权限以修改专享版实例公网出口的带宽。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:instances:update
apig:instance:getCreateProgress	授予权限以获取专享版实例的创建进度。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:instance:deleteIngressEip	授予权限以关闭专享版实例的公网入口。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:instances:update
apig:instance:createIngressEip	授予权限以开启专享版实例的公网入口。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:instances:update
apig:instance:changeIngressEipBindwidth	授予权限以更新专享版实例的入公网带宽。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:instances:update
apig::createPrepayOrder	授予权限以创建包周期专享版实例订单。	Write	-	• g:RequestTag/<tag-key> • g:TagKeys	• apig:instances:create
apig:instance:createPrepayResizeOrder	授予权限以创建包周期专享版实例规格变更订单。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:instances:update
apig:instance:resize	授予权限以创建按需专享版实例规格变更订单。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:getRestriction	授予权限以获取实例约束信息。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:instances:get
apig:instance:listParameter	授予权限以获取实例参数列表。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	• apig:features:list
apig:instance:u	授予权限以编	Write	instan	• g:ResourceTag/<tag-	• apig:features

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
pdateParameter	辑实例参数。		ce *	key> • g:EnterpriseProjectId	:create
apig:instance:listFeature	授予权限以获取实例支持的特性列表。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:importMicroservice	授予权限以导入微服务到专享版实例。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apis:import
apig:apiGroup:bindDomain	授予权限以绑定独立域名。	Write	instance *	g:ResourceTag/<tag-key>	• apig:domains:create
apig:apiGroup:unbindDomain	授予权限以解绑独立域名。	Write	instance *	g:ResourceTag/<tag-key>	• apig:domains:delete
apig:apiGroup:updateDomainConfig	授予权限以修改独立域名。	Write	instance *	g:ResourceTag/<tag-key>	• apig:domains:update
apig:apiGroup:createAndBindCertificateToDomain	授予权限以创建并绑定证书到独立域名。	Write	instance *	g:ResourceTag/<tag-key>	• apig:domains:bindCertificate
apig:apiGroup:unbindAndDeleteCertificateFromDomain	授予权限以解绑并删除独立域名的证书。	Write	instance *	g:ResourceTag/<tag-key>	• apig:domains:unbindCertificate
apig:apiGroup:getCertificateOfDomain	授予权限以查看独立域名的证书。	Read	instance *	g:ResourceTag/<tag-key>	• apig:domains:getCertificate
apig:apiGroup:updateSLDomainSetting	授予权限以设置调试域名是否可以访问。	Write	instance *	g:ResourceTag/<tag-key>	• apig:domains:updateSLDomainSetting
apig:customAuthorizer:list	授予权限以获取自定义认证列表。	List	instance *	g:ResourceTag/<tag-key>	• apig:authorizers:list
apig:customAuthorizer:create	授予权限以创建自定义认	Write	instance *	g:ResourceTag/<tag-key>	• apig:authorizers:create

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	证。				
apig:customAuthorizer:delete	授予权限以删除自定义认证。	Write	instance *	g:ResourceTag/<tag-key>	• apig:authorizers:delete
apig:customAuthorizer:get	授予权限以获取自定义认证详情。	Read	instance *	g:ResourceTag/<tag-key>	• apig:authorizers:get
apig:customAuthorizer:update	授予权限以修改自定义认证。	Write	instance *	g:ResourceTag/<tag-key>	• apig:authorizers:update
apig:instance:listVpcEndpoint	授予权限以获取实例终端节点列表。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:acceptOrRejectVpcEndpointConnection	授予权限以接受或拒绝终端节点连接。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:listVpcEndpointPermission	授予权限以获取实例终端节点服务的白名单列表。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:batchAddVpcEndpointPermission	授予权限以批量添加实例终端节点连接白名单。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:batchDeleteVpcEndpointPermission	授予权限以批量删除实例终端节点连接白名单。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:app:deleteAcl	授予权限以删除凭据的访问控制规则。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apps:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:app:getAcl	授予权限以获取凭据的访问控制规则。	Read	instance *	g:ResourceTag/<tag-key>	• apig:apps:get
apig:app:updateAcl	授予权限以设置凭据的访问控制规则。	Write	instance *	g:ResourceTag/<tag-key>	• apig:apps:get
apig:clientQuota:list	授予权限以获取凭据配额策略列表。	List	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:create	授予权限以创建凭据配额策略。	Write	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:delete	授予权限以删除凭据配额策略。	Write	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:get	授予权限以获取凭据配额策略详情。	Read	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:update	授予权限以修改凭据配额策略。	Write	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:listBoundApp	授予权限以查询凭据配额策略已绑定的凭据列表。	List	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:bindApp	授予权限以绑定凭据配额和凭据。	Write	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:unbindApp	授予权限以解除凭据配额和凭据的绑定关系。	Write	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:listUnboundApp	授予权限以查询凭据配额可绑定的凭据列表。	List	instance *	g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:instance:listFeatureHistory	授予权限以查询特性的历史记录列表。	List	instance *	g:ResourceTag/<tag-key>	-
apig:instance:addCustomIngressPort	授予权限以新增实例自定义入方向端口。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:listCustomIngressPort	授予权限以获取实例自定义入方向端口列表。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:deleteCustomIngressPort	授予权限以删除实例自定义入方向端口。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:listCustomIngressPortDomain	授予权限以获取实例自定义入方向端口绑定的域名信息列表。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

apig 的 API 通常对应着一个或多个授权项。表 3-203 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-199 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /{project_id}/apigw/instances/{instance_id}/acls	apig:acl:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/acls	apig:acl:create	apig:instance:get
PUT	apig:acl:batchDelete	apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/{project_id}/apigw/instances/{instance_id}/acls		
DELETE /{project_id}/apigw/instances/{instance_id}/acls/{acl_id}	apig:acl:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/acls/{acl_id}	apig:acl:get	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/acls/{acl_id}	apig:acl:update	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/acl-bindings	apig:api:bindAcl	• apig:instance:get • apig:api:get • apig:acl:get
PUT /{project_id}/apigw/instances/{instance_id}/acl-bindings	apig:api:batchUnbindAcl	• apig:instance:get • apig:api:get • apig:acl:get
DELETE /{project_id}/apigw/instances/{instance_id}/acl-bindings/{acl_bindings_id}	apig:api:unbindAcl	• apig:instance:get • apig:api:get • apig:acl:get
GET /{project_id}/apigw/instances/{instance_id}/acl-bindings/binded-acls	apig:api:listBoundAcl	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/acl-bindings/binded-apis	apig:acl:listBoundApi	• apig:instance:get • apig:acl:get
GET /{project_id}/apigw/instances/{instance_id}/acl-bindings/unbinded-apis	apig:acl:listUnboundApi	• apig:instance:get • apig:acl:get
POST /{project_id}/apigw/in	apig:api:bindRequestThrottling	• apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
stances/{instance_id}/throttle-bindings		• apig:api:get • apig:requestThrottling:get
PUT /{project_id}/apigw/instances/{instance_id}/throttle-bindings	apig:api:batchUnbindRequestThrottling	• apig:instance:get • apig:api:get • apig:requestThrottling:get
DELETE /{project_id}/apigw/instances/{instance_id}/throttle-bindings/{throttle_binding_id}	apig:api:unbindRequestThrottling	• apig:instance:get • apig:api:get • apig:requestThrottling:get
GET /{project_id}/apigw/instances/{instance_id}/throttle-bindings/binded-apis	apig:requestThrottling:listBoundApi	• apig:instance:get • apig:requestThrottling:get
GET /{project_id}/apigw/instances/{instance_id}/throttle-bindings/binded-throttles	apig:api:listBoundRequestThrottling	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/throttle-bindings/unbinded-apis	apig:requestThrottling:listUnboundApi	• apig:instance:get • apig:requestThrottling:get
GET /{project_id}/apigw/instances/{instance_id}/api-groups	apig:apiGroup:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups	apig:apiGroup:create	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}	apig:apiGroup:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}	apig:apiGroup:get	apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}	apig:apiGroup:update	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups/check	apig:apiGroup:checkApiGroupNameExistOrNot	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/apis	apig:api:list	• apig:instance:get • apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/apis	apig:api:create	• apig:instance:get • apig:apiGroup:get • apig:loadBalanceChannel:get • apig:customAuthorizer:get • functiongraph:function:getFunctionConfig
DELETE /{project_id}/apigw/instances/{instance_id}/apis/{api_id}	apig:api:delete	• apig:instance:get • apig:apiGroup:get
GET /{project_id}/apigw/instances/{instance_id}/apis/{api_id}	apig:api:get	• apig:instance:get • apig:apiGroup:get
PUT /{project_id}/apigw/instances/{instance_id}/apis/{api_id}	apig:api:update	• apig:instance:get • apig:apiGroup:get • apig:loadBalanceChannel:get • apig:customAuthorizer:get • functiongraph:function:getFunctionConfig
POST /{project_id}/apigw/instances/{instance_id}/apis/action	apig:api:onlineOrOffline	• apig:instance:get • apig:apiGroup:get • apig:environment:list
POST /{project_id}/apigw/instances/{instance_id}/apis/check	apig:api:checkApiPathOrApiNameExistOrNot	• apig:instance:get • apig:apiGroup:get
POST /{project_id}/apigw/in	apig:api:debug	• apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
stances/{instance_id}/apis/debug/{api_id}		• apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/apis/publish	apig:api:batchOnlineOrOffline	• apig:instance:get • apig:apiGroup:get • apig:environment:list
GET /{project_id}/apigw/instances/{instance_id}/apis/publish/{api_id}	apig:api:listHistoryVersion	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/apis/publish/{api_id}	apig:api:switchVersion	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/apis/runtime/{api_id}	apig:api:getRuntimeDefinition	• apig:instance:get • apig:environment:list
DELETE /{project_id}/apigw/instances/{instance_id}/apis/versions/{version_id}	apig:api:deleteHistoryVersion	• apig:instance:get • apig:apiGroup:get • apig:environment:list
GET /{project_id}/apigw/instances/{instance_id}/apis/versions/{version_id}	apig:api:getHistoryVersion	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/apps	apig:app:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/apps	apig:app:create	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/apps/{app_id}	apig:app:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}	apig:app:get	apig:instance:get
PUT	apig:app:update	apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/{project_id}/apigw/instances/{instance_id}/apps/{app_id}		
GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes	apig:app:listAppCode	• apig:instance:get • apig:app:get
POST /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes	apig:app:createAppCode	• apig:instance:get • apig:app:get
PUT /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes	apig:app:generateAppCode	• apig:instance:get • apig:app:get
DELETE /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes/{app_code_id}	apig:app:deleteAppCode	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes/{app_code_id}	apig:app:getAppCode	• apig:instance:get • apig:app:get
PUT /{project_id}/apigw/instances/{instance_id}/apps/secret/{app_id}	apig:app:resetSecret	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/apps/validation/{app_id}	apig:app:validate	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/bound-quota	apig:app:getBoundQuota	• apig:instance:get • apig:app:get
POST /{project_id}/apigw/instances/{instance_id}/app-auths	apig:app:bindApi	• apig:instance:get • apig:app:get • apig:api:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /{project_id}/apigw/instances/{instance_id}/app-auths/{app_auth_id}	apig:app:unbindApi	• apig:instance:get • apig:app:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/app-auths/binded-apis	apig:app:listBoundApi	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/app-auths/binded-apps	apig:api:listBoundApp	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/app-auths/unbinded-apis	apig:app:listUnboundApi	• apig:instance:get • apig:app:get
POST /{project_id}/apigw/instances/{instance_id}/openapi/export	apig:api:export	• apig:instance:get • apig:api:list • apig:api:get • apig:api:listBoundAcl • apig:acl:get • apig:api:listBoundRequestThrottling • apig:requestThrottling:get • apig:apiGroup:get • apig:apiGroup:getGatewayResponse • apig:environment:list • apig:api:listBoundPlugin • apig:plugin:get
POST /{project_id}/apigw/instances/{instance_id}/openapi/async-export	apig:api:export	• apig:instance:get • apig:api:list • apig:api:get • apig:api:listBoundAcl • apig:acl:get • apig:api:listBoundRequestThrottling • apig:requestThrottling:get • apig:apiGroup:get • apig:apiGroup:getGatewayResponse

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
		• apig:environment:list • apig:api:listBoundPlugin • apig:plugin:get
POST /{project_id}/apigw/instances/{instance_id}/openapi/import	apig:api:import	• apig:instance:get • apig:api:get • apig:acl:get • apig:requestThrottling:get • apig:apiGroup:get • apig:apiGroup:getGatewayResponse • apig:environment:list • apig:plugin:get
POST /{project_id}/apigw/instances/{instance_id}/openapi/async-import	apig:api:import	• apig:instance:get • apig:api:get • apig:acl:get • apig:requestThrottling:get • apig:apiGroup:get • apig:apiGroup:getGatewayResponse • apig:environment:list • apig:plugin:get
GET /{project_id}/apigw/instances/{instance_id}/async-tasks/{task_id}	apig:asyncTask:get	apig:instance:get
GET /{project_id}/apigw/certificates	apig:certificate:list	-
POST /{project_id}/apigw/certificates	apig:certificate:create	apig:instance:get
DELETE /{project_id}/apigw/certificates/{certificate_id}	apig:certificate:delete	-
GET /{project_id}/apigw/certificates/{certificate_id}	apig:certificate:get	-
PUT /{project_id}/apigw/certificates/{certificate_i	apig:certificate:update	apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
d}		
GET /{project_id}/apigw/certificates/{certificate_id}/attached-domains	apig:certificate:listBoundDomain	-
POST /{project_id}/apigw/certificates/{certificate_id}/domains/attach	apig:certificate:batchBindDomain	• apig:certificate:get • apig:apiGroup:get
POST /{project_id}/apigw/certificates/{certificate_id}/domains/detach	apig:certificate:batchUnbindDomain	• apig:certificate:get • apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificates/attach	apig:apiGroup:batchBindCertificateToDomain	• apig:instance:get • apig:apiGroup:get • apig:certificate:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificates/detach	apig:apiGroup:batchUnbindCertificateFromDomain	• apig:instance:get • apig:apiGroup:get • apig:certificate:get
GET /{project_id}/apigw/instances/{instance_id}/vpc-channels	apig:loadBalanceChannel:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-channels	apig:loadBalanceChannel:create	• apig:instance:get • cce:cluster:getCluster • ecs:cloudServers:showServer • cce:cluster:generateClientCredential
DELETE /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}	apig:loadBalanceChannel:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/	apig:loadBalanceChannel:get	apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
vpc-channels/{vpc_channel_id}		
PUT /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}	apig:loadBalanceChannel:update	• apig:instance:get • cce:cluster:getCluster • ecs:cloudServers:showServer • cce:cluster:generateClientCredential
PUT /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/health-config	apig:loadBalanceChannel:updateHealthCheckConfig	• apig:instance:get • apig:loadBalanceChannel:get
GET /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups	apig:loadBalanceChannel:listServerGroup	• apig:instance:get • apig:loadBalanceChannel:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups	apig:loadBalanceChannel:createServerGroup	• apig:instance:get • apig:loadBalanceChannel:get
DELETE /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id}	apig:loadBalanceChannel:deleteServerGroup	• apig:instance:get • apig:loadBalanceChannel:get
GET /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id}	apig:loadBalanceChannel:getServerGroup	• apig:instance:get • apig:loadBalanceChannel:get
PUT /{project_id}/apigw/instances/{instance_id}/vpc-	apig:loadBalanceChannel:updateServerGroup	• apig:instance:get • apig:loadBalanceChannel:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
channels/{vpc_channel_id}/member-groups/{member_group_id}		
GET /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members	apig:loadBalanceChannel:listBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members	apig:loadBalanceChannel:createBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get • ecs:cloudServers:showServer
PUT /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members	apig:loadBalanceChannel:updateBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get • ecs:cloudServers:showServer
DELETE /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/{member_id}	apig:loadBalanceChannel:deleteBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/batch-disable	apig:loadBalanceChannel:batchDisableBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/batch-enable	apig:loadBalanceChannel:batchEnableBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get
GET /{project_id}/apigw/instances/{instance_id}/tags	apig:instance:listTag	apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /{project_id}/apigw/instances/{instance_id}/apis/{api_id}/attachable-plugins	apig:api:listUnboundPlugin	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/apis/{api_id}/attached-plugins	apig:api:listBoundPlugin	• apig:instance:get • apig:api:get
POST /{project_id}/apigw/instances/{instance_id}/apis/{api_id}/plugins/attach	apig:api:bindPlugin	• apig:instance:get • apig:api:get • apig:plugin:get
PUT /{project_id}/apigw/instances/{instance_id}/apis/{api_id}/plugins/detach	apig:api:unbindPlugin	• apig:instance:get • apig:api:get • apig:plugin:get
GET /{project_id}/apigw/instances/{instance_id}/plugins	apig:plugin:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/plugins	apig:plugin:create	• apig:instance:get • apig:loadBalanceChannel:get • functiongraph:function:getFunctionConfig
DELETE /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}	apig:plugin:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}	apig:plugin:get	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}	apig:plugin:update	• apig:instance:get • apig:loadBalanceChannel:get • functiongraph:function:getFunctionConfig
POST /{project_id}/apigw/instances/{instance_id}/	apig:plugin:bindApi	• apig:instance:get • apig:api:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
plugins/{plugin_id}/attach		• apig:plugin:get
GET /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attachable-apis	apig:plugin:listUnbindApi	• apig:instance:get • apig:plugin:get
GET /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attached-apis	apig:plugin:listBoundApi	• apig:instance:get • apig:plugin:get
PUT /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/detach	apig:plugin:unbindApi	• apig:instance:get • apig:api:get • apig:plugin:get
GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses	apig:apiGroup:listGatewayResponse	• apig:instance:get • apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses	apig:apiGroup:createGatewayResponse	• apig:instance:get • apig:apiGroup:get
DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}	apig:apiGroup:deleteGatewayResponse	• apig:instance:get • apig:apiGroup:get
GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}	apig:apiGroup:getGatewayResponse	• apig:instance:get • apig:apiGroup:get
PUT /{project_id}/apigw/in	apig:apiGroup:updateGatewayResponse	• apig:instance:get • apig:apiGroup:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
stances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}		
DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}/{response_type}	apig:apiGroup:deleteGatewayResponseType	• apig:instance:get • apig:apiGroup:get
GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}/{response_type}	apig:apiGroup:getGatewayResponseType	• apig:instance:get • apig:apiGroup:get
PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}/{response_type}	apig:apiGroup:updateGatewayResponseType	• apig:instance:get • apig:apiGroup:get
GET /{project_id}/apigw/instances/{instance_id}/resources/outline/apis	apig:instance:listApiOutline	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/resources/outline/apps	apig:instance:listAppOutline	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/resources/outline/groups	apig:instance:listApiGroupOutline	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/env-variables	apig:environmentVariable:list	• apig:instance:get • apig:apiGroup:get • apig:environment:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /{project_id}/apigw/instances/{instance_id}/env-variables	apig:environmentVariable:create	• apig:instance:get • apig:apiGroup:get • apig:environment:list
DELETE /{project_id}/apigw/instances/{instance_id}/env-variables/{env_variable_id}	apig:environmentVariable:delete	• apig:instance:get • apig:apiGroup:get • apig:environment:list
GET /{project_id}/apigw/instances/{instance_id}/env-variables/{env_variable_id}	apig:environmentVariable:get	• apig:instance:get • apig:apiGroup:get • apig:environment:list
PUT /{project_id}/apigw/instances/{instance_id}/env-variables/{env_variable_id}	apig:environmentVariable:update	• apig:instance:get • apig:apiGroup:get • apig:environment:list
GET /{project_id}/apigw/instances/{instance_id}/envs	apig:environment:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/envs	apig:environment:create	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/envs/{env_id}	apig:environment:delete	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/envs/{env_id}	apig:environment:update	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/metric-data	apig:instance:listMetricData	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/statistics/api/latest	apig:instance:listApiMonitoring	apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /{project_id}/apigw/instances/{instance_id}/statistics/group/latest	apig:instance:listApiGroupMonitoring	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/throttles	apig:requestThrottling:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/throttles	apig:requestThrottling:create	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}	apig:requestThrottling:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}	apig:requestThrottling:get	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}	apig:requestThrottling:update	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/sign-bindings	apig:api:bindSignatureKey	• apig:instance:get • apig:api:get • apig:signatureKey:list
DELETE /{project_id}/apigw/instances/{instance_id}/sign-bindings/{sign_bindings_id}	apig:api:unbindSignatureKey	• apig:instance:get • apig:api:get • apig:signatureKey:list
GET /{project_id}/apigw/instances/{instance_id}/sign-bindings/binded-apis	apig:signatureKey:listBoundApi	• apig:instance:get • apig:signatureKey:list
GET /{project_id}/apigw/instances/{instance_id}/sign-bindings/binded-signs	apig:api:listBoundSignatureKey	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/in	apig:signatureKey:listUnbound	• apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
stances/{instance_id}/sign-bindings/unbinded-apis	Api	• apig:signatureKey:list
GET /{project_id}/apigw/instances/{instance_id}/signs	apig:signatureKey:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/signs	apig:signatureKey:create	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/signs/{sign_id}	apig:signatureKey:delete	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/signs/{sign_id}	apig:signatureKey:update	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials	apig:requestThrottling:listSpecial	• apig:instance:get • apig:requestThrottling:get
POST /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials	apig:requestThrottling:createSpecial	• apig:instance:get • apig:requestThrottling:get
DELETE /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials/{strategy_id}	apig:requestThrottling:deleteSpecial	• apig:instance:get • apig:requestThrottling:get
PUT /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials/{strategy_id}	apig:requestThrottling:updateSpecial	• apig:instance:get • apig:requestThrottling:get
GET /{project_id}/apigw/instances/{instance_id}/instance-tags	apig:instance:listSingleInstanceTag	apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /{project_id}/apigw/instances/{instance_id}/instance-tags/action	apig:instance:batchCreateOrDeleteTag	apig:instance:get
GET /{project_id}/apigw/instance-tags	apig::listTag	apig:instance:get
POST /{project_id}/apigw/resource-instances/count	apig:instance:getNumByTags	-
POST /{project_id}/apigw/resource-instances/filter	apig:instance:listByTags	-
GET /{project_id}/apigw/instances	apig:instance:list	-
POST /{project_id}/apigw/instances	apig:instance:create	• vpc:securityGroups:get • vpc:ports:create • vpc:ports:update • eip:publicIps:get • eip:publicIps:update • eps:enterpriseProjects:list
DELETE /{project_id}/apigw/instances/{instance_id}	apig:instance:delete	• eip:publicIps:get • eip:publicIps:update • vpc:ports:delete
GET /{project_id}/apigw/instances/{instance_id}	apig:instance:get	-
PUT /{project_id}/apigw/instances/{instance_id}	apig:instance:update	• vpc:securityGroups:get • vpc:ports:update
DELETE /{project_id}/apigw/instances/{instance_id}/eip	apig:instance:unbindEip	• apig:instance:get • eip:publicIps:update
PUT /{project_id}/apigw/instances/{instance_id}/eip	apig:instance:bindOrChangeEip	• apig:instance:get • eip:publicIps:update
DELETE /{project_id}/apigw/instances/{instance_id}/	apig:instance:deleteOutboundEip	apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
nat-eip		
POST /{project_id}/apigw/instances/{instance_id}/nat-eip	apig:instance:createOutboundEip	• apig:instance:get • vpc:ports:get
PUT /{project_id}/apigw/instances/{instance_id}/nat-eip	apig:instance:changeOutboundEipBandwidth	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/progress	apig:instance:getCreateProgress	-
DELETE /{project_id}/apigw/instances/{instance_id}/ingress-eip	apig:instance:deleteIngressEip	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/ingress-eip	apig:instance:createIngressEip	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/ingress-eip	apig:instance:changeIngressEipBindwidth	apig:instance:get
POST /{project_id}/apigw/prepay-instances	apig::createPrepayOrder	bss:order:update
POST /{project_id}/apigw/instances/{instance_id}/prepay-resize	apig:instance:createPrepayResizeOrder	• apig:instance:get • bss:order:update
POST /{project_id}/apigw/instances/{instance_id}/postpaid-resize	apig:instance:resize	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/restriction	apig:instance:getRestriction	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/features	apig:instance:listParameter	apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /{project_id}/apigw/instances/{instance_id}/features	apig:instance:updateParameter	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/instance-features	apig:instance:listFeature	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/microservice/import	apig:instance:importMicroservice	• apig:instance:get • apig:api:create • apig:apiGroup:get • apig:apiGroup:create • apig:loadBalanceChannel:get • apig:loadBalanceChannel:create • cce:cluster:getCluster • cce:cluster:generateClientCredential
POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains	apig:apiGroup:bindDomain	• apig:instance:get • apig:apiGroup:get
DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}	apig:apiGroup:unbindDomain	• apig:instance:get • apig:apiGroup:get
PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}	apig:apiGroup:updateDomainConfig	• apig:instance:get • apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate	apig:apiGroup:createAndBindCertificateToDomain	• apig:instance:get • apig:apiGroup:get • apig:certificate:get
DELETE	apig:apiGroup:unbindAndDele	• apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate/{certificate_id}	teCertificateFromDomain	• apig:apiGroup:get • apig:certificate:get
GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate/{certificate_id}	apig:apiGroup:getCertificateOfDomain	• apig:instance:get • apig:apiGroup:get • apig:certificate:get
PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/sl-domain-access-settings	apig:apiGroup:updateSLDomainSetting	• apig:instance:get • apig:apiGroup:get
GET /{project_id}/apigw/instances/{instance_id}/authorizers	apig:customAuthorizer:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/authorizers	apig:customAuthorizer:create	• apig:instance:get • functiongraph:function:getFunctionConfig
DELETE /{project_id}/apigw/instances/{instance_id}/authorizers/{authorizer_id}	apig:customAuthorizer:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/authorizers/{authorizer_id}	apig:customAuthorizer:get	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/authorizers/{authorizer_id}	apig:customAuthorizer:update	• apig:instance:get • functiongraph:function:getFunctionConfig
GET /{project_id}/apigw/instances/{instance_id}/	apig:instance:listVpcEndpoint	apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
vpc-endpoint/connections		
POST /{project_id}/apigw/instances/{instance_id}/vpc-endpoint/connections/action	apig:instance:acceptOrRejectVpcEndpointConnection	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/vpc-endpoint/permissions	apig:instance:listVpcEndpointPermission	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-endpoint/permissions/batch-add	apig:instance:batchAddVpcEndpointPermission	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-endpoint/permissions/batch-delete	apig:instance:batchDeleteVpcEndpointPermission	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-acl	apig:app:deleteAcl	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-acl	apig:app:getAcl	• apig:instance:get • apig:app:get
PUT /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-acl	apig:app:updateAcl	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/app-quotas	apig:clientQuota:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/app-quotas	apig:clientQuota:create	apig:instance:get
DELETE	apig:clientQuota:delete	apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}		
GET /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}	apig:clientQuota:get	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}	apig:clientQuota:update	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/bound-apps	apig:clientQuota:listBoundApp	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/binding-apps	apig:clientQuota:bindApp	• apig:instance:get • apig:clientQuota:get
DELETE /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/bound-apps/{app_id}	apig:clientQuota:unbindApp	• apig:instance:get • apig:app:get • apig:clientQuota:get
GET /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/bindable-apps	apig:clientQuota:listUnboundApp	• apig:instance:get • apig:clientQuota:get
POST /{project_id}/apigw/instances/{instance_id}/custom-ingress-ports	apig:instance:addCustomIngressPort	apig:instance:get
GET	apig:instance:listCustomIngres	apig:instance:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/{project_id}/apigw/instances/{instance_id}/custom-ingress-ports	sPort	
DELETE /{project_id}/apigw/instances/{instance_id}/custom-ingress-ports/{ingress_port_id}	apig:instance:deleteCustomIngressPort	• apig:instance:get • apig:instance:listCustomIngressPort
GET /{project_id}/apigw/instances/{instance_id}/custom-ingress-ports/{ingress_port_id}/domains	apig:instance:listCustomIngressPortDomain	• apig:instance:get • apig:apiGroup:get • apig:instance:listCustomIngressPort

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-204 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

apig 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-200 apig 支持的资源类型

资源类型	URN
instance	apig:<region>:<account-id>:instance:<instance-id>

条件（Condition）

apig 服务不支持在身份策略中的条件键中配置服务级的条件键。apig 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.9.6 分布式缓存服务 DCS

云服务在 IAM 预置了常用的权限，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

 版权所有 © 华为云计算技术有限公司

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 DCS 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 DCS 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 DCS 的相关操作。

表3-201 DCS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dcs:instance:create	授予权限以创建缓存实例。	Write	-	• g:EnterpriseProjectId • g:RequestTa	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				g/<tag-key> • g:TagKeys • dcs:backupEnabled	
dcs:instance:list	授予权限以查询缓存列表。	List	-	g:EnterpriseProjectId	-
dcs:instance:exportListFile	授予权限以下载导出的缓存实例列表文件。	List	-	-	• dcs:instance:list
dcs:instance:delete	授予权限以删除缓存实例。	Write	instance	g:EnterpriseProjectId	-
dcs:instance:get	授予权限以查询缓存实例。	Read	instance *	g:EnterpriseProjectId	-
dcs:instance:modify	授予权限以修改缓存实例。	Write	instance *	• g:EnterpriseProjectId • dcs:backupEnabled	-
dcs:instance:scale	授予权限以扩容缓存实例。	Write	instance *	g:EnterpriseProjectId	-
dcs:instance:swap	授予权限以执行缓存实例主备倒换。	Write	instance *	g:EnterpriseProjectId	-
dcs:instance:modifyAuthInfo	授予权限以修改缓存实例密码。	Write	instance *	g:EnterpriseProjectId	• dcs:instance:resetAuthInfo
dcs:instance:modifyStatus	授予权限以重启缓存实例或清空缓存实例数据。	Write	instance *	g:EnterpriseProjectId	-
dcs:instance:getConfiguration	授予权限以查询实例配置参数。	Read	instance *	g:EnterpriseProjectId	-
dcs:instance:modifyConfiguration	授予权限以修改缓存实例配置参数。	Write	instance *	g:EnterpriseProjectId	• dcs:instance:modifyConfigureation

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dcs:instance:deleteDataBackupFile	授予权限以删除缓存实例备份数据。	Write	instance *	g:EnterpriseProjectId	-
dcs:instance:restoreData	授予权限以恢复缓存实例数据。	Write	instance *	g:EnterpriseProjectId	-
dcs:instance:getDataRestoreLog	授予权限以查询实例恢复记录。	Read	instance *	g:EnterpriseProjectId	-
dcs:instance:downloadBackupData	授予权限以获取实例备份文件下载链接。	Read	instance *	g:EnterpriseProjectId	-
dcs:instance:backupData	授予权限以备份缓存实例数据。	Write	instance *	g:EnterpriseProjectId	-
dcs:instance:getDataBackupLog	授予权限以查询实例备份记录。	Read	instance *	g:EnterpriseProjectId	-
dcs:migrationTask:create	授予权限以创建数据迁移任务。	Write	-	-	-
dcs:migrationTask:list	授予权限以查询数据迁移任务列表。	List	-	-	-
dcs:migrationTask:delete	授予权限以删除数据迁移任务。	Write	migrationTask	-	-
dcs:migrationTask:get	授予权限以查询数据迁移任务。	Read	migrationTask *	-	-
dcs:migrationTask:modify	授予权限以配置、停止数据迁移任务。	Write	migrationTask *	-	• dcs:migrationTask:exchangeIp • dcs:migrationTask:rollbackIp

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dcs:instance:listBigKey	授予权限以查询实例大 key 列表。	List	instance *	g:EnterpriseProjectId	• dcs:instance:analyze
dcs:instance:getBigKey	授予权限以查询实例大 key 详情。	Read	instance *	g:EnterpriseProjectId	• dcs:instance:analyze
dcs:instance:deleteBigKeyScanTask	授予权限以删除实例大 key 扫描任务。	Write	instance	g:EnterpriseProjectId	• dcs:instance:analyze
dcs:instance:updateBigKeyAutoScanConfig	授予权限以修改实例大 key 扫描任务配置。	Write	instance *	g:EnterpriseProjectId	• dcs:instance:analyze
dcs:instance:getBigKeyAutoScanConfig	授予权限以查询实例大 key 扫描任务配置。	Read	instance *	g:EnterpriseProjectId	• dcs:instance:analyze
dcs:instance:analyzeHotKey	授予权限以执行实例热 key 分析。	Write	instance *	g:EnterpriseProjectId	• dcs:instance:analyze
dcs:instance:listHotKey	授予权限以查询实例热 key 列表。	List	instance *	g:EnterpriseProjectId	• dcs:instance:analyze
dcs:instance:getHotKey	授予权限以查询实例热 key 详情。	Read	instance *	g:EnterpriseProjectId	• dcs:instance:analyze
dcs:instance:deleteHotKeyScanTask	授予权限以删除实例热 key 扫描任务。	Write	instance	g:EnterpriseProjectId	• dcs:instance:analyze
dcs:instance:updateHotKeyAutoScanConfig	授予权限以修改实例热 key 扫描任务配置。	Write	instance *	g:EnterpriseProjectId	• dcs:instance:analyze
dcs:instance:getHotKeyAutoScanConfig	授予权限以查询实例热 key 扫描任务配	Read	instance *	g:EnterpriseProjectId	• dcs:instance:analyze

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	置。				
dcs:instance:analyzeExpiredKey	授予权限以执行实例过期 key 分析。	Write	instance *	g:EnterpriseProjectId	• dcs:instance:analyze
dcs:instance:getAutoExpiredKeyScanTask	授予权限以查询过期 key 扫描任务。	Read	instance *	-	• dcs:instance:analyze
dcs:instance:updateExpiredKeyScanConfig	授予权限以修改实例过期 key 扫描任务配置。	Write	instance *	g:EnterpriseProjectId	• dcs:instance:analyze
dcs:instance:getExpiredKeyScanConfig	授予权限以查询实例过期 key 扫描任务配置。	Read	instance *	g:EnterpriseProjectId	• dcs:instance:analyze
dcs:slowlog:list	授予权限以查询慢日志列表。	List	instance *	g:EnterpriseProjectId	-
dcs:aclaccount:create	授予权限以创建 ACL 账号。	Write	instance *	-	-
dcs:aclaccount:list	授予权限以查询 ACL 账户列表。	List	instance *	-	-
dcs:aclaccount:modify	授予权限以修改 ACL 账号密码。	Write	instance *	-	-
dcs:aclaccount:delete	授予权限以删除 ACL 账号。	Write	instance *	-	-
dcs:whitelist:modify	授予权限以设置 IP 白名单分组。	Write	instance *	-	-
dcs:whitelist:list	授予权限以查询指定实例的 IP 白名单。	List	instance *	-	-
dcs:instance:getBackgroundTas	授予权限以查	Read	instan	g:EnterprisePro	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
k	询后台任务列表。		ce *	jectId	
dcs:instance:deleteBackgroundTask	授予权限以删除后台任务。	Write	instance *	g:EnterpriseProjectId	-
dcs:instance:createDiagnosisTask	授予权限以诊断实例。	Write	instance *	g:EnterpriseProjectId	• dcs:instance:diagnosis
dcs:instance:listDiagnosisTask	授予权限以查询实例诊断任务列表。	List	instance *	g:EnterpriseProjectId	• dcs:instance:diagnosis
dcs:instance:getDiagnosisTask	授予权限以查询实例诊断详情。	Read	instance *	g:EnterpriseProjectId	• dcs:instance:diagnosis
dcs:instance:deleteDiagnosisTask	授予权限以删除诊断记录。	Write	instance *	g:EnterpriseProjectId	• dcs:instance:diagnosis
dcs:template:list	授予权限以查询参数模板列表。	List	-	-	-
dcs:template:create	授予权限以创建自定义模板。	Write	-	-	-
dcs:template:get	授予权限以查询参数模板。	Read	-	-	-
dcs:template:modify	授予权限以修改自定义参数模板。	Write	-	-	-
dcs:template:delete	授予权限以删除自定义参数模板。	Write	-	-	-
dcs:tag:list	授予权限以查询租户所有标签。	List	-	-	-
dcs:tag:modify	授予权限以批量添加或删除	Write	instance *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	标签。		-	• g:RequestTag/<tag-key> • g:TagKeys	
dcs:tag:get	授予权限以查询单个实例标签。	Read	instance *	-	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
dcs:redisLog:get	授予权限以获取日志下载链接。	Read	instance *	-	-
dcs:quota:get	授予权限以查询租户配额。	Read	-	-	-
dcs:instance:webcli	授予权限以使用 WebCli 连接 Redis 实例。	Write	instance *	-	-
dcs:clientIpTrans:modify	授予权限以开启或关闭客户端 ip 透传。	Write	instance *	-	• dcs:clientiptrans:modify
dcs:clients:list	授予权限以查询 Redis 会话列表。	Read	instance *	-	-
dcs:clients:kill	授予权限以 Kill Redis 会话。	Write	instance *	-	-
dcs:ssl:get	授予权限以获取 SSL 证书信息。	Read	instance *	-	-
dcs:ssl:modify	授予权限以修改 SSL 开关配置。	Write	instance *	-	-
dcs:job:get	授予权限以获取前置任务检查结果。	Read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dcs:task:list	授予权限以获取后台任务列表。	List	-	-	-
dcs:task:delete	授予权限以删除后台任务记录。	Write	-	-	-

DCS 的 API 通常对应着一个或多个授权项。表 3-206 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-202 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/instances	dcs:instance:create	• vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:subnets:get • vpc:securityGroupRules:get • vpc:securityGroups:get
GET /v2/{project_id}/instances	dcs:instance:list	-
DELETE /v2/{project_id}/instances	dcs:instance:delete	• vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:subnets:get
GET /v2/{project_id}/instances/{instance_id}	dcs:instance:get	-
DELETE /v2/{project_id}/instances/{instance_id}	dcs:instance:delete	• vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:subnets:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/instances/{instance_id}	dcs:instance:modify	• vpc:ports:get • vpc:ports:update
POST /v2/{project_id}/instances/{instance_id}/resize	dcs:instance:scale	• vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:subnets:get • vpc:securityGroupRules:get • vpc:securityGroups:get
POST /v2/{project_id}/instances/{instance_id}/resize/check-job	dcs:instance:scale	-
POST /v2/{project_id}/instances/{instance_id}/swap	dcs:instance:swap	-
PUT /v2/{project_id}/instances/{instance_id}/password	dcs:instance:modifyAuthInfo	-
POST /v2/{project_id}/instances/{instance_id}/password/reset	dcs:instance:modifyAuthInfo	-
GET /v2/{project_id}/instances/status	dcs:instance:list	-
PUT /v2/{project_id}/instances/status	dcs:instance:modifyStatus	-
GET /v2/{project_id}/instances/statistic	dcs:instance:list	-
POST /v2/{project_id}/instances/{instance_id}/groups/{group_id}/replications/{node_id}/slave-priority	dcs:instance:modify	-
DELETE /v2/{project_id}/instances/{instance_id}/grou	dcs:instance:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ps/{group_id}/replications/{node_id}/remove-ip		
GET /v2/{project_id}/instance/{instance_id}/groups	dcs:instance:get	-
GET /v2/{project_id}/instances/{instance_id}/configs	dcs:instance:getConfiguration	-
PUT /v2/{project_id}/instances/{instance_id}/configs	dcs:instance:modifyConfiguration	-
PUT /v2/{project_id}/instances/{instance_id}/async-configs	dcs:instance:modifyConfiguration	-
DELETE /v2/{project_id}/instances/{instance_id}/backups/{backup_id}	dcs:instance:deleteDataBackupFile	-
POST /v2/{project_id}/instances/{instance_id}/restores	dcs:instance:restoreData	-
GET /v2/{project_id}/instances/{instance_id}/restores	dcs:instance:getDataRestoreLog	-
POST /v2/{project_id}/instances/{instance_id}/backups/{backup_id}/links	dcs:instance:downloadBackupData	-
POST /v2/{project_id}/instances/{instance_id}/backups	dcs:instance:backupData	-
GET /v2/{project_id}/instances/{instance_id}/backups	dcs:instance:getDataBackupLog	-
POST /v2/{project_id}/migra	dcs:migrationTask:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
tion-task		
GET /v2/{project_id}/migration-tasks	dcs:migrationTask:list	-
DELETE /v2/{project_id}/migration-tasks/delete	dcs:migrationTask:delete	-
GET /v2/{project_id}/migration-task/{task_id}	dcs:migrationTask:get	-
POST /v2/{project_id}/migration-task/{task_id}/stop	dcs:migrationTask:modify	-
GET /v2/{project_id}/migration-task/{task_id}/stats	dcs:migrationTask:get	-
POST /v2/{project_id}/migration/instance	dcs:migrationTask:create	-
POST /v2/{project_id}/migration/{task_id}/task	dcs:migrationTask:modify	-
POST /v2/{project_id}/migration-task/batch-stop	dcs:migrationTask:modify	-
POST /v2/{project_id}/migration-task/{task_id}/sync-stop	dcs:migrationTask:modify	-
GET /v2/{project_id}/dcs/tags	dcs:tag:list	-
POST /v2/{project_id}/dcs/{instance_id}/tags/action	dcs:tag:modify	-
GET /v2/{project_id}/instances/{instance_id}/tags	dcs:tag:get	-
GET /v2/{project_id}/instan	dcs:instance:listBigKey	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ces/{instance_id}/bigkey-tasks		
PUT /v2/{project_id}/instances/{instance_id}/bigkey/autoscan	dcs:instance:updateBigKeyAutoScanConfig	-
GET /v2/{project_id}/instances/{instance_id}/bigkey/autoscan	dcs:instance:getBigKeyAutoScanConfig	-
POST /v2/{project_id}/instances/{instance_id}/hotkey-task	dcs:instance:analyzeHotKey	-
GET /v2/{project_id}/instances/{instance_id}/hotkey-tasks	dcs:instance:listHotKey	-
GET /v2/{project_id}/instances/{instance_id}/hotkey-task/{hotkey_id}	dcs:instance:getHotKey	-
DELETE /v2/{project_id}/instances/{instance_id}/hotkey-task/{hotkey_id}	dcs:instance:deleteHotKeyScanTask	-
PUT /v2/{project_id}/instances/{instance_id}/hotkey/autoscan	dcs:instance:updateHotKeyAutoScanConfig	-
GET /v2/{project_id}/instances/{instance_id}/hotkey/autoscan	dcs:instance:getHotKeyAutoScanConfig	-
POST /v2/{project_id}/instances/{instance_id}/scan-expire-keys-task	dcs:instance:analyzeExpiredKey	-
GET /v2/{project_id}/instances/{instance_id}/auto-expire/histories	dcs:instance:getAutoExpiredKeyScanTask	-
POST /v2/{project_id}/instances/{instance_id}/auto	dcs:instance:analyzeExpiredKey	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
-expire/scan		
GET /v2/{project_id}/instances/{instance_id}/scan-expire-keys/autoscan-config	dcs:instance:getExpiredKeyScanConfig	-
PUT /v2/{project_id}/instances/{instance_id}/scan-expire-keys/autoscan-config	dcs:instance:updateExpiredKeyScanConfig	-
GET /v2/{project_id}/instances/{instance_id}/slowlog	dcs:slowlog:list	-
GET /v2/{project_id}/instances/{instance_id}/redislog	dcs:redisLog:get	-
POST /v2/{project_id}/instances/{instance_id}/redislog	dcs:redisLog:get	-
POST /v2/{project_id}/instances/{instance_id}/redislog/{id}/links	dcs:redisLog:get	-
POST /v2/{project_id}/instances/{instance_id}/accounts	dcs:aclaccount:create	-
GET /v2/{project_id}/instances/{instance_id}/accounts	dcs:aclaccount:list	-
PUT /v2/{project_id}/instances/{instance_id}/accounts/{account_id}/password/modify	dcs:aclaccount:modify	-
PUT /v2/{project_id}/instances/{instance_id}/accounts/{account_id}/password/reset	dcs:aclaccount:modify	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/instances/{instance_id}/accounts/{account_id}	dcs:aclaccount:modify	-
PUT /v2/{project_id}/instances/{instance_id}/accounts/{account_id}/role	dcs:aclaccount:modify	-
DELETE /v2/{project_id}/instances/{instance_id}/accounts/{account_id}	dcs:aclaccount:delete	-
PUT /v2/{project_id}/instance/{instance_id}/whitelist	dcs:whitelist:modify	-
GET /v2/{project_id}/instance/{instance_id}/whitelist	dcs:whitelist:list	-
GET /v2/{project_id}/instances/{instance_id}/tasks	dcs:instance:getBackgroundTask	-
DELETE /v2/{project_id}/instances/{instance_id}/tasks/{task_id}	dcs:instance:deleteBackgroundTask	-
GET /v2/{project_id}/quota	dcs:quota:get	-
GET /v2/{project_id}/dims/monitored-objects/{instance_id}	dcs:instance:get	-
GET /v2/{project_id}/dims/monitored-objects	dcs:instance:list	-
POST /v2/{project_id}/instances/{instance_id}/diagnosis	dcs:instance:createDiagnosisTask	-
GET /v2/{project_id}/instances/{instance_id}/diagnosis	dcs:instance:listDiagnosisTask	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/diagnosis/{report_id}	dcs:instance:getDiagnosisTask	-
DELETE /v2/{project_id}/instances/{instance_id}/diagnosis	dcs:instance:deleteDiagnosisTask	-
GET /v2/{project_id}/config-templates	dcs:template:list	-
POST /v2/{project_id}/config-templates	dcs:template:create	-
GET /v2/{project_id}/config-templates/{template_id}	dcs:template:get	-
DELETE /v2/{project_id}/config-templates/{template_id}	dcs:template:delete	-
PUT /v2/{project_id}/config-templates/{template_id}	dcs:template:modify	-
GET /v2/{project_id}/instances-logical-nodes	dcs:instance:list	-
GET /v2/{project_id}/instances/{instance_id}/config-histories	dcs:instance:get	-
PUT /v2/{project_id}/instances/{instance_id}/bandwidth	dcs:instance:modify	-
PUT /v2/{project_id}/instances/{instance_id}/async-swap	dcs:instance:swap	-
GET /v2/{project_id}/instan	dcs:instance:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ces/{instance_id}/operations		
POST /v2/{project_id}/instances/{instance_id}/webcli/auth	dcs:instance:webcli	-
POST /v2/{project_id}/instances/{instance_id}/webcli/command	dcs:instance:webcli	-
POST /v2/{project_id}/instances/{instance_id}/webcli/logout	dcs:instance:webcli	-
PUT /v2/{project_id}/{instance_id}/client-ip-transparent-transmission	dcs:clientIpTrans:modify	-
GET /v2/{project_id}/instances/{instance_id}/bigkey-task/{bigkey_id}	dcs:instance:getBigKey	-
DELETE /v2/{project_id}/instances/{instance_id}/bigkey-task/{bigkey_id}	dcs:instance:deleteBigKeyScanTask	-
POST /v2/{project_id}/instances/{instance_id}/clients	dcs:clients:list	-
GET /v2/{project_id}/instances/{instance_id}/clients	dcs:clients:list	-
POST /v2/{project_id}/instances/{instance_id}/clients/kill	dcs:clients:kill	-
POST /v2/{project_id}/instances/{instance_id}/clients/kill-all	dcs:clients:kill	-
GET /v2/{project_id}/instan	dcs:instance:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ces/{instance_id}/config-histories/{history_id}		
GET /v2/{project_id}/instances/{instance_id}/deletable-replication	dcs:instance:scale	-
POST /v2/{project_id}/instances/export	dcs:instance:list	-
GET /v2/{project_id}/instance/{instance_id}/groups/{group_id}/group-nodes-state	dcs:instance:get	-
POST /v2/{project_id}/instance/{instance_id}/groups/{group_id}/replications/{node_id}/async-switchover	dcs:instance:swap	-
GET /v2/{project_id}/instances/{instance_id}/ssl	dcs:ssl:get	-
PUT /v2/{project_id}/instances/{instance_id}/ssl	dcs:ssl:modify	-
POST /v2/{project_id}/instances/{instance_id}/ssl-certs/download	dcs:ssl:modify	-
GET /v2/{project_id}/instances/{instance_id}/tasks/{task_id}/progress	dcs:instance:getBackgroundTask	-
GET /v2/{project_id}/instances/export-job	dcs:instance:exportListFile	-
GET /v2/{project_id}/jobs/{job_id}	dcs:job:get	-
PUT /v2/{project_id}/migration-task/{task_id}	dcs:migrationTask:modify	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/migration-task/{task_id}/exchange-ip	dcs:migrationTask:modify	-
POST /v2/{project_id}/orders/instances/{instance_id}/resize	dcs:instance:scale	-
GET /v2/{project_id}/tasks	dcs:task:list	-
DELETE /v2/{project_id}/tasks/{task_id}	dcs:task:delete	-
GET /v2/{project_id}/migration-task/{task_id}/logs	dcs:migrationTask:get	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-207 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

DCS 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-203 DCS 支持的资源类型

资源类型	URN
instance	dcs:<region>:<account-id>:instance:<instance-id>
migrationTask	dcs:<region>:<account-id>:migrationTask:<task-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。

 版权所有 © 华为云计算技术有限公司

  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 dcs:）仅适用于对应服务的操作，详情请参见表 3-208。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

DCS 支持的服务级条件键

DCS 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-204 DCS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
dcs:backupEnabled	boolean	单值	对 DCS 实例开启自动备份进行权限控制。

3.10 开发与运维

3.10.1 应用管理与运维平台 ServiceStage

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参考 IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义策略，请参考考创建自定义身份策略。

 版权所有 © 华为云计算技术有限公司

- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 ServiceStage 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 ServiceStage 定义的条件键的详细信息请参见条件（Condition）。
- **“别名”**列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 ServiceStage 的相关操作。

表3-205 ServiceStage 支持的授权项

授权项	描述	访问级别	资源类型	条件键	别名
servicestage:app:getApplication	授予用户查看指定应用权限	read	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	servicestage:app:get
servicestage:app:createApplication	授予用户创建应用权限	write	app	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	servicestage:app:create
servicestage:app:modifyApplication	授予用户更新应用权限	write	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	servicestage:app:modify

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型	条件键	别名
				• g:RequestTag/<tag-key> • g:TagKeys	
servicestage:app:deleteApplication	授予用户删除应用权限	write	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	servicestage:app:delete
servicestage:app:listApplication	授予用户查看应用列表权限	list	-	-	servicestage:app:list
servicestage:app:getConfiguration	授予用户查看应用配置权限	read	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	servicestage:app:get
servicestage:app:deleteConfiguration	授予用户删除应用配置权限	write	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	servicestage:app:modify
servicestage:app:modifyConfiguration	授予用户更新应用配置权限	write	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	servicestage:app:modify
servicestage:app:getComponent	授予用户查看指定应用组件权限	read	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	servicestage:app:get
servicestage:app:createComponent	授予用户创建应用组件权限	write	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	servicestage:app:create
servicestage:app:modifyComponent	授予用户更新应用组件权限	write	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	servicestage:app:modify

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型	条件键	别名
servicestage:app:deleteComponent	授予用户删除应用组件权限	write	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	servicestage:app:delete
servicestage:app:listComponent	授予用户查看应用组件列表权限	list	-	-	servicestage:app:list
servicestage:environment:create	授予用户创建环境权限	write	environment	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	-
servicestage:environment:get	授予用户查看环境信息权限	read	environment	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
servicestage:environment:list	授予用户查看环境列表权限	list	-	-	servicestage:app:list
servicestage:environment:modify	授予用户更新环境权限	write	environment	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	-
servicestage:environment:delete	授予用户删除环境权限	write	environment	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
servicestage:environment:tag	授予 TMS 用户创建环境标签权限	tagging	environment	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-	servicestage:environment:modify

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型	条件键	别名
				key> • g:TagKeys	
servicestage:app:tag	授予 TMS 用户创建应用标签权限	tagging	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	servicestage:app:modify
servicestage:environment:listResourcesByTag	授予 TMS 用户通过标签查询环境资源权限	read	environment	• g:RequestTag/<tag-key> • g:TagKeys	servicestage:environment:list
servicestage:app:listResourcesByTag	授予 TMS 用户通过标签查询应用资源权限	read	app	• g:RequestTag/<tag-key> • g:TagKeys	servicestage:app:list
servicestage:environment:unTagResource	授予 TMS 用户删除环境资源标签权限	tagging	environment	• g:ResourceTag/<tag-key> • g:RequestTag/<tag-key> • g:EnterpriseProjectId • g:TagKeys	servicestage:environment:modify
servicestage:app:unTagResource	授予 TMS 用户删除应用资源标签权限	tagging	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	servicestage:app:modify
servicestage:environment:listTags	授予 TMS 用户查询环境资源标签列表权限	read	-	-	servicestage:environment:list
servicestage:	授予 TMS 用	read	-	-	servicesta

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型	条件键	别名
app:listTags	户查询应用资源标签列表权限				ge:app:list
servicestage:pipeline:get	授予用户查看流水线权限	read	pipeline	-	-
servicestage:pipeline:create	授予用户创建流水线权限	write	pipeline	-	-
servicestage:pipeline:modify	授予用户更新流水线权限	write	pipeline	-	-
servicestage:pipeline:delete	授予用户删除流水线权限	write	pipeline	-	-
servicestage:pipeline:list	授予用户查看流水线列表权限	list	-	-	-
servicestage:assembling:runtimeList	授予用户查看技术栈列表权限	read	-	-	servicestage:assembling:get
servicestage:assembling:getInfo	授予用户查看构建信息权限	list	-	-	-
servicestage:assembling:create	授予用户创建构建任务权限	write	assembling	-	-
servicestage:assembling:modify	授予用户更新构建任务权限	write	assembling	-	-
servicestage:assembling:delete	授予用户删除构建任务权限	write	assembling	-	-
servicestage:assembling:list	授予用户查看构建任务列表权限	list	-	-	-
servicestage:repositoryA	授予用户获取仓库授权	list	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型	条件键	别名
uth:list	列表权限				
servicestage:repositoryAuth:get	授予用户获取仓库授权权限	read	repositoryAuth	-	-
servicestage:repositoryAuth:create	授予用户创建仓库授权权限	write	repositoryAuth	-	-
servicestage:repositoryAuth:delete	授予用户删除仓库授权权限	write	repositoryAuth	-	-
servicestage:environment:listTagsForResource	授予 eps 用户查询环境资源标签列表权限	read	environment	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	servicestage:app:list
servicestage:app:listTagsForResource	授予 eps 用户查询应用资源标签列表权限	read	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	servicestage:app:list

ServiceStage 的 API 通常对应着一个或多个授权项。表 3-210 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-206 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/cas/metadata/runtimes	servicestage:app:listApplication	-
GET /v2/{project_id}/cas/metadata/flavors	servicestage:app:listApplication	-
POST /v2/{project_id}/cas/environments	servicestage:environment:create	-
GET /v2/{project_id}/cas/environments	servicestage:environment:list	-
PUT /v2/{project_id}/cas/environ	servicestage:environment:m	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ments/{environment_id}	odify	
DELETE /v2/{project_id}/cas/environments/{environment_id}	servicestage:environment:delete	-
GET /v2/{project_id}/cas/environments/{environment_id}	servicestage:environment:get	-
PATCH /v2/{project_id}/cas/environments/{environment_id}/resources	servicestage:environment:modify	-
POST /v2/{project_id}/cas/applications	servicestage:app:createApplication	-
GET /v2/{project_id}/cas/applications	servicestage:app:listApplication	-
PUT /v2/{project_id}/cas/applications/{application_id}	servicestage:app:modifyApplication	-
DELETE /v2/{project_id}/cas/applications/{application_id}	servicestage:app:deleteApplication	-
GET /v2/{project_id}/cas/applications/{application_id}	servicestage:app:getApplication	-
PUT /v2/{project_id}/cas/applications/{application_id}/configuration	servicestage:app:modifyConfiguration	-
DELETE /v2/{project_id}/cas/applications/{application_id}/configuration	servicestage:app:deleteConfiguration	-
GET /v2/{project_id}/cas/applications/{application_id}/configuration	servicestage:app:getConfiguration	-
POST /v2/{project_id}/cas/applications/{application_id}/components	servicestage:app:createComponent	servicestage:assembling:getInfo servicestage:assembling:create
GET	servicestage:app:listCompon	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v2/{project_id}/cas/applications/{application_id}/components	ent	
PUT /v2/{project_id}/cas/applications/{application_id}/components/{component_id}	servicestage:app:modifyComponent	-
DELETE /v2/{project_id}/cas/applications/{application_id}/components/{component_id}	servicestage:app:deleteComponent	-
GET /v2/{project_id}/cas/applications/{application_id}/components/{component_id}	servicestage:app:getComponent	-
POST /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances	servicestage:app:createComponent	servicestage:assembling:getInfo servicestage:assembling:create
GET /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances	servicestage:app:listComponent	-
POST /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}/action	servicestage:app:modifyComponent	-
PUT /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}	servicestage:app:modifyComponent	-
DELETE /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}	servicestage:app:deleteComponent	-
GET /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}	servicestage:app:getComponent	-
GET	servicestage:app:getCompon	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}/snapshots	ent	
GET /v2/{project_id}/cas/jobs/{job_id}	servicestage:app:listApplication	-
POST /v3/{project_id}/cas/environments	servicestage:environment:create	-
GET /v3/{project_id}/cas/environments	servicestage:environment:list	-
PUT /v3/{project_id}/cas/environments/{environment_id}	servicestage:environment:modify	-
DELETE /v3/{project_id}/cas/environments/{environment_id}	servicestage:environment:delete	-
GET /v3/{project_id}/cas/environments/{environment_id}	servicestage:environment:get	-
PUT /v3/{project_id}/cas/environments/{environment_id}/resources	servicestage:environment:modify	-
GET /v3/{project_id}/cas/environments/{environment_id}/resources	servicestage:environment:list	-
POST /v3/{project_id}/cas/applications	servicestage:app:createApplication	-
GET /v3/{project_id}/cas/applications	servicestage:app:listApplication	-
PUT /v3/{project_id}/cas/applications/{application_id}	servicestage:app:modifyApplication	-
GET /v3/{project_id}/cas/applications/{application_id}	servicestage:app:getApplication	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/cas/applications/{application_id}/configuration	servicestage:app:getConfiguration	-
PUT /v3/{project_id}/cas/applications/{application_id}/configuration	servicestage:app:modifyConfiguration	-
DELETE /v3/{project_id}/cas/applications/{application_id}/configuration	servicestage:app:deleteConfiguration	-
POST /v3/{project_id}/cas/applications/{application_id}/components	servicestage:app:createComponent	servicestage:assembling:getInfo servicestage:assembling:create
GET /v3/{project_id}/cas/applications/{application_id}/components	servicestage:app:listComponent	-
GET /v3/{project_id}/cas/components	servicestage:app:listComponent	-
PUT /v3/{project_id}/cas/applications/{application_id}/components/{component_id}	servicestage:app:modifyComponent	-
DELETE /v3/{project_id}/cas/applications/{application_id}/components/{component_id}	servicestage:app:deleteComponent	-
GET /v3/{project_id}/cas/applications/{application_id}/components/{component_id}	servicestage:app:getComponent	-
POST /v3/{project_id}/cas/applications/{application_id}/components/{component_id}/action	servicestage:app:modifyComponent	-
GET /v3/{project_id}/cas/applications/{application_id}/components/{component_id}/records	servicestage:app:listComponent	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/cas/runtime stacks	servicestage:app:listApplication	-
GET /v1/{project_id}/git/auths	servicestage:repositoryAuth:list	-
GET /v1/{project_id}/git/auths/{repo_type}/redirect	servicestage:repositoryAuth:get	-
POST /v1/{project_id}/git/auths/{repo_type}/oauth	servicestage:repositoryAuth:create	-
POST /v1/{project_id}/git/auths/{repo_type}/personal	servicestage:repositoryAuth:create	-
POST /v1/{project_id}/git/auths/{repo_type}/password	servicestage:repositoryAuth:create	-
DELETE /v1/{project_id}/git/auths/{name}	servicestage:repositoryAuth:delete	-
GET /v2/{project_id}/servicestage-environment/{environment_id}/tags	servicestage:environment:listTagsForResource	-
GET /v2/{project_id}/servicestage-application/{app_id}/tags	servicestage:app:listTagsForResource	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-211 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，策略仅作用于此资源；如未指定，Resource 默认为“*”，则策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

ServiceStage 定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-207 ServiceStage 支持的资源类型

资源类型	URN
app	servicestage:<region>:<account-id>:app:<app-id>

 版权所有 © 华为云计算技术有限公司

资源类型	URN
environment	servicestage:<region>:<account-id>:environment:<environment-id>
pipeline	servicestage:<region>:<account-id>:pipeline:<pipeline-id>
assembling	servicestage:<region>:<account-id>:assembling:<assembling-id>
repositoryAuth	servicestage:<region>:<account-id>:repositoryAuth:<repositoryAuth-id>

条件（Condition）

ServiceStage 服务不支持在身份策略中的条件键中配置服务级的条件键。

ServiceStage 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.10.2 软件开发生产线 CodeArts

Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）可以使用以下授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。

本章节介绍组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为 SCP 中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在 SCP 中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在 SCP 语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 CodeArts 控制台定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在 SCP 语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。

 版权所有 © 华为云计算技术有限公司

- 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
- 如果此列条件键没有值（-），表示此操作不支持指定条件键。

关于 CodeArts 控制台定义的条件键的详细信息请参见条件（Condition）。

您可以在 SCP 语句的 Action 元素中指定以下 CodeArts 控制台的相关操作。

表3-208 CodeArts 控制台支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
codearts:projectman:viewUsage	授予权限以在控制台查询项目管理服务资源用量。	read	-	-
codearts:codehub:viewUsage	授予权限以在控制台查询代码托管服务资源用量。	read	-	-
codearts:cloudbuild:viewUsage	授予权限以在控制台查询编译构建服务资源用量。	read	-	-
codearts:codecheck:viewUsage	授予权限以在控制台查询代码检查服务资源用量。	read	-	-
codearts:cloudtest:viewUsage	授予权限以在控制台查询云测-测试管理服务资源用量。	read	-	-
codearts:apitest:viewUsage	授予权限以在控制台查询云测-接口测试服务资源用量。	read	-	-
codearts:cloudrelease:viewUsage	授予权限以在控制台查询发布服务资源用量。	read	-	-
codearts:cloudide:viewUsage	授予权限以在控制台查询CloudIDE 服务资源用量。	read	-	-
codearts:classro	授予权限以在	read	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
om:viewUsage	控制台查询Classroom服务资源用量。			
codearts:monthlyPackage:changeSpecification	授予权限以在控制台变更软件开发平台套餐规格。	write	-	-
codearts:monthlyPackage:subscribe	授予权限以在控制台订购软件开发平台套餐。	write	-	-
codearts:projectman:subscribeService	授予权限以在控制台开通按需项目管理服务。	write	-	-
codearts:codehub:subscribeService	授予权限以在控制台开通按需代码托管服务。	write	-	-
codearts:cloudbuild:subscribeService	授予权限以在控制台开通按需编译构建服务。	write	-	-
codearts:codecheck:subscribeService	授予权限以在控制台开通按需代码检查服务。	write	-	-
codearts:cloudtest:subscribeService	授予权限以在控制台开通按需云测-测试管理服务。	write	-	-
codearts:apitest:subscribeService	授予权限以在控制台开通按需云测-接口测试服务。	write	-	-
codearts:cloudrelease:subscribeService	授予权限以在控制台开通按需发布服务。	write	-	-
codearts:package:subscribeServ	授予权限以在控制台开通按	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
ice	需服务组合。			
codearts:cloudide:subscribeService	授予权限以在控制台开通按需 CloudIDE 服务。	write	-	-
codearts:classroom:subscribeService	授予权限以在控制台开通按需 Classroom 服务。	write	-	-
codearts:projectman:unsubscribeService	授予权限以在控制台取消开通按需项目管理服务。	write	-	-
codearts:codehub:unsubscribeService	授予权限以在控制台取消开通按需代码托管服务。	write	-	-
codearts:cloudbuild:unsubscribeService	授予权限以在控制台取消开通按需编译构建服务。	write	-	-
codearts:codecheck:unsubscribeService	授予权限以在控制台取消开通按需代码检查服务。	write	-	-
codearts:cloudtest:unsubscribeService	授予权限以在控制台取消开通按需云测-测试管理服务。	write	-	-
codearts:apitest:unsubscribeService	授予权限以在控制台取消开通按需云测-接口测试服务。	write	-	-
codearts:cloudrelease:unsubscribeService	授予权限以在控制台取消开通按需发布服务。	write	-	-
codearts:package:unsubscribeService	授予权限以在控制台取消开通按需服务组	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
	合。			
codearts:cloudide:unsubscribeService	授予权限以在控制台取消开通按需CloudIDE 服务。	write	-	-
codearts:classroom:unsubscribeService	授予权限以在控制台取消开通按需Classroom 服务。	write	-	-
codearts:authorization:list	授予权限以在控制台查看租户授权列表。	list	-	-
codearts:payPerUsePackage:listResourceDetail	授予权限以在控制台查看按需套餐包资源详情。	list	-	-
codearts:monthlyPackage:listResourceDetail	授予权限以在控制台查看软件开发平台套餐资源详情。	list	-	-
codearts:projectman:listResourceDetail	授予权限以在控制台查看项目管理资源列表详情。	list	-	-
codearts:codehub:listResourceDetail	授予权限以在控制台查看仓库托管资源列表详情。	list	-	-
codearts:cloudbuild:listResourceDetail	授予权限以在控制台查看构建资源列表详情。	list	-	-
codearts:codecheck:listResourceDetail	授予权限以在控制台查看代码检查资源列表详情。	list	-	-
codearts:cloudtest:listResource	授予权限以在控制台查看云	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
Detail	测-测试管理资源列表详情。			
codearts:cloudrelease:listResourceDetail	授予权限以在控制台查看发布资源列表详情。	list	-	-
codearts:cloudide:listResourceDetail	授予权限以在控制台查看CloudIDE 资源列表详情。	list	-	-
codearts:classroom:listResourceDetail	授予权限以在控制台查看Classroom 资源列表详情。	list	-	-
codearts:agileDevopsTrainingServices:listResourceDetail	授予权限以在控制台查看敏捷与 DevOps 培训服务资源列表详情。	list	-	-
codearts:projectman:listSubscriptionHistory	授予权限以在控制台查看项目管理服务开通记录。	list	-	-
codearts:codehub:listSubscriptionHistory	授予权限以在控制台查看代码托管服务开通记录。	list	-	-
codearts:cloudbuild:listSubscriptionHistory	授予权限以在控制台查看编译构建服务开通记录。	list	-	-
codearts:codecheck:listSubscriptionHistory	授予权限以在控制台查看代码检查服务开通记录。	list	-	-
codearts:cloudtest:listSubscriptionHistory	授予权限以在控制台查看云测-测试管理服务开通记录。	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
codearts:apitest:listSubscriptionHistory	授予权限以在控制台查看云测-接口测试服务开通记录。	list	-	-
codearts:cloudrelease:listSubscriptionHistory	授予权限以在控制台查看发布服务开通记录。	list	-	-
codearts:package:listSubscriptionHistory	授予权限以在控制台查看按需服务组合开通记录。	list	-	-
codearts:cloudide:listSubscriptionHistory	授予权限以在控制台查看CloudIDE服务开通记录。	list	-	-
codearts:classroom:listSubscriptionHistory	授予权限以在控制台查看Classroom服务开通记录。	list	-	-
codearts:authorization:create	授予权限以在控制台新增企业账户授权。	permissions	-	-
codearts:authorization:cancel	授予权限以在控制台取消企业账户授权。	permissions	-	-
codearts:authorization:update	授予权限以在控制台同意或拒绝企业账户授权。	permissions	-	-

资源类型（Resource）

CodeArts控制台不支持在SCP中的资源中指定资源进行权限控制。如需允许访问CodeArts控制台，请在SCP的Resource元素中使用通配符号*，表示SCP将应用到所有资源。

条件（Condition）

CodeArts控制台不支持在SCP中的条件键中配置服务级的条件键。

 版权所有 © 华为云计算技术有限公司

CodeArts 控制台可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.10.3 流水线 CodeArts Pipeline

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 CodeartsPipeline 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 CodeartsPipeline 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 CodeartsPipeline 的相关操作。

 版权所有 © 华为云计算技术有限公司

表3-209 CodeartsPipeline 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
codeartspipeline:pipelinetemplate:create	授予权限以创建流水线模板。	write	-	-	-
codeartspipeline:pipelinetemplate:update	授予权限以更新流水线模板。	write	-	-	cloudpipeline:pipelinetemplate:update
codeartspipeline:pipelinetemplate:delete	授予权限以删除流水线模板。	write	-	-	cloudpipeline:pipelinetemplate:update
codeartspipeline:pipelinetemplate:get	授予权限以查看流水线模板。	read	-	-	-
codeartspipeline:pipelinetemplate:list	授予权限以查看流水线模板列表。	list	-	-	-
codeartspipeline:rule:create	授予权限以创建规则。	write	-	-	cloudpipeline:rule:update
codeartspipeline:rule:update	授予权限以更新规则。	write	-	-	cloudpipeline:rule:update
codeartspipeline:rule:delete	授予权限以删除规则。	write	-	-	cloudpipeline:rule:update
codeartspipeline:rule:get	授予权限以查看规则。	read	-	-	-
codeartspipeline:rule:list	授予权限以查看规则列表。	list	-	-	-
codeartspipeline:strategy:create	授予权限以创建策略。	write	-	-	cloudpipeline:ruletemplate:update
codeartspipeline:strategy:update	授予权限以更新策略。	write	-	-	cloudpipeline:ruletemplate:update
codeartspipeline:strategy:delete	授予权限以删除策略。	write	-	-	cloudpipeline:ruletemplate:update

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
codeartspipeline:strategy:get	授予权限以查看策略。	read	-	-	-
codeartspipeline:strategy:list	授予权限以查看策略列表。	list	-	-	-
codeartspipeline:extension:create	授予权限以创建插件。	write	-	-	cloudpipeline:extensions:update
codeartspipeline:extension:update	授予权限以更新插件。	write	-	-	cloudpipeline:extensions:update
codeartspipeline:extension:delete	授予权限以删除插件。	write	-	-	cloudpipeline:extensions:update
codeartspipeline:extension:get	授予权限以查看插件。	read	-	-	-
codeartspipeline:extension:list	授予权限以查看插件列表。	list	-	-	-

资源类型（Resource）

CodeartsPipeline 服务不支持在身份策略中的资源中指定资源进行权限控制。如需允许访问 CodeartsPipeline 服务，请在身份策略的 Resource 元素中使用通配符号*，表示身份策略将应用到所有资源。

条件（Condition）

CodeartsPipeline 服务不支持在身份策略中的条件键中配置服务级的条件键。
CodeartsPipeline 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.10.4 云应用引擎 CAE

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

 版权所有 © 华为云计算技术有限公司

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 cae 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 cae 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 cae 的相关操作。

表3-210 cae 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cae:environment:listEnvironments	授予查询所有环境的权限。	List	environment *	-	cae:environment:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cae:environment:createEnvironment	授予创建环境的权限。	Write	environment *	-	cae:environment:create
			-	g:EnterpriseProjectId	
cae:environment:deleteEnvironment	授予删除环境的权限。	Write	environment *	-	cae:environment:delete
			-	g:EnterpriseProjectId	
cae:environment:getEnvironment	授予查询环境的权限。	Read	environment *	-	cae:environment:get
			-	g:EnterpriseProjectId	
cae:environment:listCloudVolumes	授予查询所有云存储的权限。	List	environment *	-	cae:environment:list
			-	g:EnterpriseProjectId	
cae:environment:createCloudVolume	授予授权云存储的权限。	Write	environment *	-	cae:environment:create
			-	g:EnterpriseProjectId	
cae:environment:deleteCloudVolume	授予解绑云存储的权限。	Write	environment *	-	cae:environment:delete
			-	g:EnterpriseProjectId	
cae:environment:listDomains	授予查询所有域名的权限。	List	environment *	-	cae:environment:get
			-	g:EnterpriseProjectId	
cae:environment:createDomain	授予创建域名的权限。	Write	environment *	-	cae:environment:create

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	g:EnterpriseProjectId	
cae:environment:deleteDomain	授予删除域名的权限。	Write	environment *	-	cae:environment:delete
			-	g:EnterpriseProjectId	
cae:environment:listCertificates	授予查询所有证书的权限。	List	environment *	-	cae:environment:get
			-	g:EnterpriseProjectId	
cae:environment:createCertificate	授予创建证书的权限。	Write	environment *	-	cae:environment:create
			-	g:EnterpriseProjectId	
cae:environment:deleteCertificate	授予删除证书的权限。	Write	environment *	-	cae:environment:delete
			-	g:EnterpriseProjectId	
cae:environment:updateCertificate	授予更新证书的权限。	Write	environment *	-	cae:environment:update
			-	g:EnterpriseProjectId	
cae:environment:listTimerRules	授予查询所有启停规则的权限。	List	environment *	-	cae:environment:get
			-	g:EnterpriseProjectId	
cae:environment:createTimerRule	授予创建启停规则的权限。	Write	environment *	-	cae:environment:create
			-	g:EnterpriseProjectId	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cae:environment:deleteTimerRule	授予删除启停规则的权限。	Write	environment *	-	cae:environment:delete
			-	g:EnterpriseProjectId	
cae:environment:updateTimerRule	授予更新启停规则的权限。	Write	environment *	-	cae:environment:update
			-	g:EnterpriseProjectId	
cae:environment:getTimerRule	授予查询启停规则的权限。	Read	environment *	-	cae:environment:get
			-	g:EnterpriseProjectId	
cae:environment:listEips	授予查看所有EIP(环境与公网互相访问)的权限。	List	environment *	-	cae:environment:get
			-	g:EnterpriseProjectId	
cae:environment:updateEip	授予更新EIP(环境与公网互相访问)的权限。	Write	environment *	-	cae:environment:update
			-	g:EnterpriseProjectId	
cae:environment:listVpcEgresses	授予查看所有VpcEgress(环境访问 VPC)的权限。	List	environment *	-	cae:environment:get
			-	g:EnterpriseProjectId	
cae:environment:createVpcEgress	授予创建VpcEgress(环境访问 VPC)的权限。	Write	environment *	-	cae:environment:create
			-	g:EnterpriseProjectId	
cae:environment:deleteVpcEgress	授予删除VpcEgress(环	Write	environment *	-	cae:environment:delete

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	境访问 VPC)的权限。		-	g:EnterpriseProjectId	
cae:environment:listVpcIngresses	授予查看所有VpcIngress(VPC 访问环境)的权限。	List	environment *	-	cae:environment:get
			-	g:EnterpriseProjectId	
cae:environment:createVpcIngress	授予创建VpcIngress(VPC 访问环境)的权限。	Write	environment *	-	cae:environment:create
			-	g:EnterpriseProjectId	
cae:environment:deleteVpcIngress	授予删除VpcIngress(VPC 访问环境)的权限。	Write	environment *	-	cae:environment:delete
			-	g:EnterpriseProjectId	
cae:environment:createMonitorSystem	授予创建监控系统的权限。	Write	environment *	-	cae:environment:create
			-	g:EnterpriseProjectId	
cae:environment:updateMonitorSystem	授予更新监控系统的权限。	Write	environment *	-	cae:environment:update
			-	g:EnterpriseProjectId	
cae:environment:getMonitorSystem	授予查询监控系统的权限。	Read	environment *	-	cae:environment:get
			-	g:EnterpriseProjectId	
cae:application:listApplications	授予查询所有应用的权限。	List	application *	-	cae:application:list
cae:application:createApplication	授予创建应用的权限。	Write	application *	-	cae:application:create
			-	g:EnterprisePro	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				jectId	
cae:application:deleteApplication	授予删除应用的权限。	Write	application *	-	cae:application:delete
			-	g:EnterpriseProjectId	
cae:component:listComponents	授予查询所有组件的权限。	List	component *	-	cae:application:list
			-	g:EnterpriseProjectId	
cae:component:createComponent	授予创建组件的权限。	Write	component *	-	cae:application:create
			-	g:EnterpriseProjectId	
cae:component:deleteComponent	授予删除组件的权限。	Write	component *	-	cae:application:delete
			-	g:EnterpriseProjectId	
cae:component:updateComponent	授予更新组件的权限。	Write	component *	-	cae:application:modify
			-	g:EnterpriseProjectId	
cae:component:getComponent	授予查询组件的权限。	Read	component *	-	cae:application:get
			-	g:EnterpriseProjectId	
cae:component:createWithConfigComponent	授予创建、生效配置并部署组件的权限。	Write	component *	-	cae:application:create
			-	g:EnterpriseProjectId	
cae:component:operateComponent	授予操作(deploy|scale|upgrade|rollback|start|stop|restart|configure)组件的权限。	Write	component *	-	cae:application:modify
			-	g:EnterpriseProjectId	
cae:component:	授予查询组件	List	compo	-	cae:application:

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
listConfigurations	所有配置的权限。		nent *		get
			-	g:EnterpriseProjectId	
cae:component:createConfiguration	授予创建(更新)组件配置的权限。	Write	component *	-	cae:application:create
			-	g:EnterpriseProjectId	
cae:component:deleteConfiguration	授予删除(取消)组件配置的权限。	Write	component *	-	cae:application:delete
			-	g:EnterpriseProjectId	
cae:component:getConfiguration	授予查询组件配置的权限。	Read	component *	-	cae:application:list
			-	g:EnterpriseProjectId	
cae:component:createInstanceWebShell	授予创建远程登录的权限。	Write	component *	-	cae:application:createConsole
			-	g:EnterpriseProjectId	
cae::listNoticeRules	授予查询所有事件通知规则的权限。	List	-	g:EnterpriseProjectId	cae:environment:get
cae::createNoticeRule	授予创建事件通知规则的权限。	Write	-	g:EnterpriseProjectId	cae:environment:create
cae::deleteNoticeRule	授予删除事件通知规则的权限。	Write	-	g:EnterpriseProjectId	cae:environment:delete
cae::updateNoticeRule	授予更新事件通知规则的权限。	Write	-	g:EnterpriseProjectId	cae:environment:update
cae::getNoticeRule	授予查询事件通知规则的权限。	Read	-	g:EnterpriseProjectId	cae:environment:get
cae::listDewSecrets	授予查询所有	List	-	g:EnterpriseProjectId	cae:environment:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	凭据的权限。				
cae::createDewSecret	授予创建凭据的权限。	Write	-	g:EnterpriseProjectId	cae:environment:create
cae::deleteDewSecret	授予删除凭据的权限。	Write	-	g:EnterpriseProjectId	cae:environment:delete
cae::updateDewSecret	授予更新凭据的权限。	Write	-	g:EnterpriseProjectId	cae:environment:update
cae::getDewSecret	授予查询凭据的权限。	Read	-	g:EnterpriseProjectId	cae:environment:get
cae::buyPackage	授予购买按需套餐包的权限。	Write	-	g:EnterpriseProjectId	cae:environment:create

cae 的 API 通常对应着一个或多个授权项。表 3-215 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-211 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/cae/environments	cae:environment:listEnvironments	-
POST /v1/{project_id}/cae/environments	cae:environment:createEnvironment	-
DELETE /v1/{project_id}/cae/environments/{environment_id}	cae:environment:deleteEnvironment	-
POST /v1/{project_id}/cae/environments/{environment_id}/wakeup	cae:environment:createEnvironment	-
GET /v1/{project_id}/cae/collections	cae:environment:getEnvironment	-
GET	cae:environment:getEnvironme	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/{project_id}/cae/applications/comb	nt	
GET /v1/{project_id}/cae/volumes	cae:environment:listCloudVolumes	-
POST /v1/{project_id}/cae/volumes	cae:environment:createCloudVolume	-
DELETE /v1/{project_id}/cae/volumes/{id}	cae:environment:deleteCloudVolume	-
GET /v1/{project_id}/cae/domains	cae:environment:listDomains	-
POST /v1/{project_id}/cae/domains	cae:environment:createDomain	-
DELETE /v1/{project_id}/cae/domains/{domain_id}	cae:environment:deleteDomain	-
GET /v1/{project_id}/cae/certificates	cae:environment:listCertificates	-
POST /v1/{project_id}/cae/certificates	cae:environment:createCertificate	-
PUT /v1/{project_id}/cae/certificates/{certificate_id}	cae:environment:updateCertificate	-
DELETE /v1/{project_id}/cae/certificates/{certificate_id}	cae:environment:deleteCertificate	-
GET /v1/{project_id}/cae/timer-rules	cae:environment:listTimerRules	-
POST /v1/{project_id}/cae/timer-rules	cae:environment:createTimerRule	-
DELETE /v1/{project_id}/cae/timer-	cae:environment:deleteTimerRule	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
rules/{timer_rule_id}		
PUT /v1/{project_id}/cae/timer-rules/{timer_rule_id}	cae:environment:updateTimerRule	-
GET /v1/{project_id}/cae/timer-rules/{timer_rule_id}/execution-results	cae:environment:getTimerRule	-
GET /v1/{project_id}/cae/eips	cae:environment:listEips	-
PUT /v1/{project_id}/cae/eips	cae:environment:updateEip	-
GET /v1/{project_id}/cae/vpc-egress	cae:environment:listVpcEgresses	-
POST /v1/{project_id}/cae/vpc-egress	cae:environment:createVpcEgress	-
DELETE /v1/{project_id}/cae/vpc-egress/{vpc_egress_id}	cae:environment:deleteVpcEgress	-
GET /v1/{project_id}/cae/vpc-ingress	cae:environment:listVpcIngresses	-
POST /v1/{project_id}/cae/vpc-ingress	cae:environment:createVpcIngress	-
DELETE /v1/{project_id}/cae/vpc-ingress/{vpc_ingress_id}	cae:environment:deleteVpcIngress	-
GET /v1/{project_id}/cae/monitor-system	cae:environment:getMonitorSystem	-
POST /v1/{project_id}/cae/monitor-system	cae:environment:createMonitorSystem	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/cae/monitor-system/{monitor_system_id}	cae:environment:updateMonitorSystem	-
GET /v1/{project_id}/cae/applications	cae:application:listApplications	-
POST /v1/{project_id}/cae/applications	cae:application:createApplication	-
DELETE /v1/{project_id}/cae/applications/{application_id}	cae:application:deleteApplication	-
GET /v1/{project_id}/cae/applications/{application_id}	cae:application:listApplications	-
POST /v1/{project_id}/cae/applications/{application_id}/components	cae:component:createComponent	-
GET /v1/{project_id}/cae/applications/{application_id}/components	cae:component:listComponents	-
GET /v1/{project_id}/cae/applications/{application_id}/components/{component_id}	cae:component:getComponent	-
PUT /v1/{project_id}/cae/applications/{application_id}/components/{component_id}	cae:component:updateComponent	-
DELETE /v1/{project_id}/cae/applications/{application_id}/components/{component_id}	cae:component:deleteComponent	-
POST /v1/{project_id}/cae/applications/{application_id}/components/{co	cae:component:operateComponent	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
mponent_id}/action		
GET /v1/{project_id}/cae/applications/{application_id}/components/{component_id}/configurations	cae:component:listConfigurations	-
POST /v1/{project_id}/cae/applications/{application_id}/components/{component_id}/configurations	cae:component:createConfiguration	-
DELETE /v1/{project_id}/cae/applications/{application_id}/components/{component_id}/configurations	cae:component:deleteConfiguration	-
GET /v1/{project_id}/cae/applications/{application_id}/components/{component_id}/configuration-history-time	cae:component:getConfiguration	-
GET /v1/{project_id}/cae/applications/{application_id}/components/{component_id}/configuration-history	cae:component:getConfiguration	-
GET /v1/{project_id}/cae/applications/{application_id}/components/{component_id}/instances	cae:component:getComponent	-
DELETE /v1/{project_id}/cae/applications/{application_id}/components/{component_id}/instances/{instance_name}	cae:component:deleteComponent	-
POST /v1/{project_id}/cae/remote-console/{instance_id}	cae:component:createInstanceWebShell	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/cae/jobs/{job_id}	cae:environment:getEnvironment	-
POST /v1/{project_id}/cae/jobs/{job_id}	cae:environment:createEnvironment	-
POST /v1/{project_id}/cae/notice-rules	cae::createNoticeRule	-
GET /v1/{project_id}/cae/notice-rules	cae::listNoticeRules	-
PUT /v1/{project_id}/cae/notice-rules/{rule_id}	cae::updateNoticeRule	-
GET /v1/{project_id}/cae/notice-rules/{rule_id}	cae::getNoticeRule	-
DELETE /v1/{project_id}/cae/notice-rules/{rule_id}	cae::deleteNoticeRule	-
POST /v1/{project_id}/cae/dew-secrets	cae::createDewSecret	-
GET /v1/{project_id}/cae/dew-secrets	cae::listDewSecrets	-
PUT /v1/{project_id}/cae/dew-secrets/{secret_id}	cae::updateDewSecret	-
DELETE /v1/{project_id}/cae/dew-secrets/{secret_id}	cae::deleteDewSecret	-
GET /v1/{project_id}/cae/dew-secrets/{secret_id}/effective-components	cae::getDewSecret	-
GET /v1/{project_id}/cae/demo	cae:component:getComponent	-
POST /v1/{project_id}/cae/d	cae:component:createComponent	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
emo/install		
POST /v1/{project_id}/cae/orders	cae::buyPackage	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-216 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

cae 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-212 cae 支持的资源类型

资源类型	URN
component	cae:<region>:<account-id>:component:<application-id>/<component-id>
environment	cae:<region>:<account-id>:environment:<environment-id>
application	cae:<region>:<account-id>:application:<application-id>

条件（Condition）

cae 服务不支持在身份策略中的条件键中配置服务级的条件键。cae 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.11 企业应用

3.11.1 云解析服务 DNS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

 版权所有 © 华为云计算技术有限公司

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 DNS 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 DNS 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 DNS 的相关操作。

表3-213 DNS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dns:zone:list	授予列出域名的权限。	List	zone *	-	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dns:zone:create	授予创建域名的权限。	Write	zone *	-	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	
dns:zone:createBatchPublicZonesByName	授予根据 Zone Name 批量创建域名的权限。	Write	zone *	-	-
			-	g:EnterpriseProjectId	
dns:zone:get	授予获取域名的权限。	Read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dns:zone:update	授予更新域名的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dns:zone:delete	授予删除域名的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dns:zone:associaterouter	授予将内网域名与 VPC 关联的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dns:zone:disassociaterouter	授予取消内网域名与 VPC 关联的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dns:zone:setProxyPattern	授予设置内网域名递归解析代理的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:Enterprise	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				ProjectId	
dns:zone:transfer	授予创建公网域名转移任务的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dns:recordset:list	授予列出记录集的权限。	List	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dns:recordset:create	授予创建记录集的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
			-	• dns:RecordSetNames • dns:RecordSetTypes	
dns:recordset:get	授予获取记录集的权限。	Read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dns:recordset:update	授予更新记录集的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
			-	• dns:RecordSetNames • dns:RecordSetTypes	
dns:recordset:delete	授予删除记录集的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	• dns:RecordSetNames • dns:RecordSetTypes	
dns:zone:setStatus	授予设置域名状态的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dns:recordset:setStatus	授予设置记录集状态的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
			-	• dns:RecordSetNames • dns:RecordSetTypes	
dns:recordset:associatehealthcheck	授予 Record Set 关联健康检查的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
			-	• dns:RecordSetNames • dns:RecordSetTypes	
dns:recordset:disassociatehealthcheck	授予 Record Set 解关联健康检查的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
			-	• dns:RecordSetNames • dns:RecordSetTypes	
dns:ptr:list	授予列出 PTR 记录的权限。	List	ptr *	-	-
			-	• g:RequestTag/<tag-key>	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:TagKeys • g:EnterpriseProjectId	
dns:ptr:get	授予获取单个PTR 记录的权限。	Read	ptr *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dns:ptr:create	授予创建 PTR 记录的权限。	Write	ptr *	-	dns:ptr:set
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId	
dns:ptr:update	授予更新 PTR 记录的权限。	Write	ptr *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dns:ptr:set
dns:ptr:delete	授予删除 PTR 记录的权限。	Write	ptr *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dns:ptr:set
dns:tag:get	授予查询域名标签的权限。	Read	zone	-	-
			ptr	-	
dns:tag:set	授予为域名设置标签的权限。	Tagging	zone	g:ResourceTag/<tag-key>	-
			ptr	g:ResourceTag/<tag-key>	
dns:zone:createRetrieval	授予找回域名的权限。	Write	-	-	-
dns:zone:getRetrieval	授予查询域名找回状态的权限。	Read	-	-	-
dns:customLine:create	授予创建自定义线路的权	Write	customLine	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。		*		
dns:customLine:list	授予列出自定义线路的权限。	List	customLine *	-	-
dns:customLine:delete	授予删除自定义线路的权限。	Write	customLine *	-	-
dns:customLine:update	授予更新自定义线路的权限。	Write	customLine *	-	-
dns:nameserver:list	授予列出名称服务器的权限。	List	-	-	dns:zone:get
dns:nameserver:getZoneNameServer	授予查询公网域名的 DNS 服务器的权限。	Read	-	-	-
dns:quota:list	授予列出租户配额的权限。	List	-	-	dns:zone:get
dns:recordset:getPrivateRecordSetImport	授予查询内网 RecordSet 导入任务的权限。	Read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dns:privateRecordset:getImport
dns:recordset:getPrivateRecordSetImportTemplate	授予下载内网 RecordSet 导入模板的权限。	Read	-	-	dns:privateRecordset:getImport
dns:recordset:createPrivateRecordSetImport	授予创建内网 RecordSet 导入任务的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dns:privateRecordset:createImport
dns:recordset:deletePrivateRecordSetImportTask	授予删除内网 RecordSet 导入任务的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dns:privateRecordset:deleteImport

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dns:recordset:createPublicRecordSetImport	授予创建公网RecordSet 导入任务的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dns:publicRecordset:createImport
dns:recordset:getPublicRecordSetImport	授予查询公网RecordSet 导入任务的权限。	Read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dns:publicRecordset:getImport
dns:recordset:getPublicRecordSetImportTemplate	授予下载公网RecordSet 导入模板的权限。	Read	-	-	dns:publicRecordset:getImport
dns:recordset:deletePublicRecordSetImportTask	授予删除公网RecordSet 导入任务的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	dns:publicRecordset:deleteImport
dns:zone:getExport	授予导出 zone 的权限。	Read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dns:lineGroup:create	授予创建线路分组的权限。	Write	lineGroup *	-	-
dns:lineGroup:list	授予列出线路分组的权限。	List	lineGroup *	-	-
dns:lineGroup:get	授予查询单个线路分组的权限。	Read	lineGroup *	-	-
dns:lineGroup:delete	授予删除线路分组的权限。	Write	lineGroup *	-	-
dns:lineGroup:update	授予更新线路分组的权限。	Write	lineGroup *	-	-
dns:endpoint:create	授予创建终端节点的权限。	Write	endpoint *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dns:endpoint:list	授予列出终端节点的权限。	List	endpoint *	-	-
dns:endpoint:get	授予查询单个终端节点的权限。	Read	endpoint *	-	-
dns:endpoint:update	授予更新终端节点的权限。	Write	endpoint *	-	-
dns:endpoint:delete	授予删除终端节点的权限。	Write	endpoint *	-	-
dns:endpoint:createIpaddress	授予为终端节点绑定 ip 地址的权限。	Write	endpoint *	-	-
dns:endpoint:deleteIpaddress	授予为终端节点解绑 ip 地址的权限。	Write	endpoint *	-	-
dns:endpoint:listIpaddresses	授予列出终端节点 ip 地址的权限。	List	endpoint *	-	-
dns:endpoint:listVpcs	授予列出终端节点关联的 VPC 的权限。	List	endpoint *	-	-
dns:resolverRule:create	授予创建解析规则的权限，定义如何将来自 VPC 的查询路由给目标 VPC。	Write	resolverRule *	-	-
dns:resolverRule:list	授予列出解析规则的权限。	List	resolverRule *	-	-
dns:resolverRule:get	授予查询单个解析规则的权限。	Read	resolverRule *	-	-
dns:resolverRule:update	授予更新解析规则的权限。	Write	resolverRule *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dns:resolverRule:delete	授予删除解析规则的权限。	Write	resolverRule *	-	-
dns:resolverRule:associaterouter	授予在解析规则上关联 VPC 的权限。	Write	resolverRule *	-	-
dns:resolverRule:disassociaterouter	授予在解析规则上解关联 VPC 的权限。	Write	resolverRule *	-	-
dns:zone:enableDnssecConfig	授予在 zone 上打开 dnssec 的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dns:zone:disableDnssecConfig	授予在 zone 上关闭 dnssec 的权限。	Write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dns:zone:getDnssecConfig	授予在 zone 上查询 dnssec 的权限。	Read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
dns:zone:listPublicZoneBatchOperationRecords	授予列出公网域名批量操作记录的权限。	List	-	-	dns:recordset:get
dns:zone:getPublicZoneBatchOperationResult	授予下载公网域名批量操作失败结果的权限。	Read	-	-	dns:recordset:get
dns:recordset:batchImportPublicRecordSet	授予批量导入公网 RecordSet 的权限。	Write	-	-	-
dns:zone:createAuthorizeTxtRecord	授予授权域名的权限。	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dns:zone:getAuthorizeTxtRecord	授予查询域名授权状态的权限。	Read	-	-	-
dns:zone:getDomainDetection	授予查询公网域名解析诊断结果的权限。	Read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

DNS 的 API 通常对应着一个或多个授权项。表 3-218 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-214 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET 01 /v2/zones	dns:zone:list	-
POST 05 /v2/zones	dns:zone:create	• dns:tag:set • dns:quota:list
GET 01 /v2/zones/{zone_id}	dns:zone:get	-
PATCH 03 /v2/zones/{zone_id}	dns:zone:update	-
DELETE 02 /v2/zones/{zone_id}	dns:zone:delete	• ces:siteMonitorRule:showHealthCheck • ces:siteMonitorRule:put • ces:siteMonitorRule:delete • ces:siteMonitorRule:list
GET 01 /v2/zones/{zone_id}/nameservers	dns:zone:get	-
GET /v2/zones	dns:zone:list	-
POST 02 /v2/zones	dns:zone:create	• vpc:vpcs:get • dns:tag:set • dns:quota:list
GET 04 /v2/zones/{zone_id}	dns:zone:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PATCH 06 /v2/zones/{zone_id}	dns:zone:update	-
DELETE 05 /v2/zones/{zone_id}	dns:zone:delete	-
GET /v2/zones/{zone_id}/nameservers	dns:zone:get	-
POST /v2/zones/{zone_id}/associaterouter	dns:zone:associaterouter	vpc:vpcs:get
POST /v2/zones/{zone_id}/disassociaterouter	dns:zone:disassociaterouter	vpc:vpcs:get
GET /v2/zones/{zone_id}/recordsets	dns:recordset:list	-
POST /v2/zones/{zone_id}/recordsets	dns:recordset:create	• dns:recordset:associatehealthcheck • ces:siteMonitorRule:showHealthCheck • ces:siteMonitorRule:put • ces:siteMonitorRule:delete • ces:siteMonitorRule:list • dns:quota:list
GET /v2/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:get	-
PUT 02 /v2/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:update	-
DELETE 01 /v2/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:delete	• dns:recordset:disassociatehealthcheck • ces:siteMonitorRule:showHealthCheck • ces:siteMonitorRule:put • ces:siteMonitorRule:delete • ces:siteMonitorRule:list
GET /v2/recordsets	dns:recordset:list	-
PUT /v2/zones/{zone_id}/st	dns:zone:setStatus	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
atuses		
GET /v2.1/recordsets	dns:recordset:list	-
POST /v2.1/zones/{zone_id}/recordsets	dns:recordset:create	• dns:recordset:associatehealthcheck • ces:siteMonitorRule:showHealthCheck • ces:siteMonitorRule:put • ces:siteMonitorRule:delete • ces:siteMonitorRule:list • dns:quota:list
GET 03 /v2.1/zones/{zone_id}/recordsets	dns:recordset:list	-
GET 01 /v2.1/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:get	-
PUT 03 /v2.1/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:update	-
DELETE 02 /v2.1/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:delete	• dns:recordset:disassociatehealthcheck • ces:siteMonitorRule:showHealthCheck • ces:siteMonitorRule:put • ces:siteMonitorRule:delete • ces:siteMonitorRule:list
PUT /v2.1/recordsets/{recordset_id}/statuses/set	dns:recordset:setStatus	-
POST /v2.1/zones/{zone_id}/recordsets/batch/lines	dns:recordset:create	• dns:recordset:associatehealthcheck • ces:siteMonitorRule:showHealthCheck • ces:siteMonitorRule:put • ces:siteMonitorRule:delete • ces:siteMonitorRule:list • dns:quota:list
PUT /v2.1/zones/{zone_id}/recordsets	dns:recordset:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /v2.1/zones/{zone_id}/recordsets	dns:recordset:delete	• dns:recordset:disassociatehealthcheck • ces:siteMonitorRule:showHealthCheck • ces:siteMonitorRule:put • ces:siteMonitorRule:delete • ces:siteMonitorRule:list
GET /v2/reverse/floatingips	dns:ptr:list	-
GET 02 /v2/reverse/floatingips/{region}:{floatingip_id}	dns:ptr:get	-
PATCH 01 /v2/reverse/floatingips/{region}:{floatingip_id}	dns:ptr:create	• eip:publicIps:get • dns:tag:set • dns:quota:list
PATCH 04 /v2/reverse/floatingips/{region}:{floatingip_id}	dns:ptr:update	-
PATCH 03 /v2/reverse/floatingips/{region}:{floatingip_id}	dns:ptr:delete	-
GET /v2/{project_id}/{resource_type}/tags	dns:tag:get	-
GET 02 /v2/{project_id}/{resource_type}/{resource_id}/tags	dns:tag:get	-
POST /v2/{project_id}/{resource_type}/{resource_id}/tags	dns:tag:set	-
DELETE /v2/{project_id}/{resource_type}/{resource_id}/tags/{key}	dns:tag:set	-
POST /v2/{project_id}/{resource_type}/{resource_id}/tags/action	dns:tag:set	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/{resource_type}/resource_instances/action	dns:tag:get	-
POST /v2.1/customlines	dns:customLine:create	dns:quota:list
GET /v2.1/customlines	dns:customLine:list	-
DELETE /v2.1/customlines/{line_id}	dns:customLine:delete	-
PUT /v2.1/customlines/{line_id}	dns:customLine:update	-
GET /v2/nameservers	dns:nameserver:list	-
GET /v2/quotamg/dns/quotas	dns:quota:list	-
POST /v2.1/linegroups	dns:lineGroup:create	dns:quota:list
GET /v2.1/linegroups	dns:lineGroup:list	-
GET /v2.1/linegroups/{linegroup_id}	dns:lineGroup:get	-
PUT /v2.1/linegroups/{linegroup_id}	dns:lineGroup:update	-
DELETE /v2.1/linegroups/{linegroup_id}	dns:lineGroup:delete	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-219 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

DNS 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-215 DNS 支持的资源类型

资源类型	URN

 版权所有 © 华为云计算技术有限公司

资源类型	URN
resolverRule	dns:<region>:<account-id>:resolverRule:<resolver-rule-id>
lineGroup	dns::<account-id>:lineGroup:<line-group-id>
customLine	dns::<account-id>:customLine:<custom-line-id>
zone	dns::<account-id>:zone:<zone-id>
endpoint	dns:<region>:<account-id>:endpoint:<endpoint-id>
ptr	dns:<region>:<account-id>:ptr:<ptr-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 dns:）仅适用于对应服务的操作，详情请参见表 3-220。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

DNS 支持的服务级条件键

DNS 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-216 DNS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
dns:RecordSetNames	string	多值	根据指定的记录集名称过滤访问。记录集名称所有字母必须为小写形式，不得带有结尾圆点。
dns:RecordSetTypes	string	多值	根据指定的记录集类型

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
			过滤访问。取值范围：A、AAAA、MX、CNAME、TXT、NS、SRV、CAA。

3.11.2 身份策略授权参考

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 ECS 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

 版权所有 © 华为云计算技术有限公司

关于 Workspace 定义的条件键的详细信息请参见条件（Condition）。

- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下云桌面的相关操作。

表3-217 workspace 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:authConfigs:get	授予查询认证登录方式配置信息的权限。	read	-	-
workspace:authConfigs:update	授予更新认证策略配置信息的权限。	write	-	-
workspace:assistAuthConfigs:get	授予查询辅助认证的配置信息的权限。	read	-	-
workspace:assistAuthConfigs:update	授予更新辅助认证配置的权限。	write	-	-
workspace:jobs:retry	授予重试任务的权限。	write	-	-
workspace:quotas:get	授予查询租户配额的权限。	read	-	-
workspace:tenants:getRoles	授予查询租户角色的权限。	read	-	-
workspace:tenants:ListConfig	授予查询租户个性配置列表的权限。	list	-	-
workspace:tenants:updateConfig	授予修改租户个性配置的权限。	write	-	-
workspace:natMappings:getConfig	授予查询租户的 NAT 映射配置项的权限。	read	-	-
workspace:natMappings:updateConfig	授予修改租户的 NAT 映射配置项的权限。	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:tenants:get	授予查询云办公服务详情的权限。	read	-	-
workspace:tenants:open	授予开通云办公服务的权限。	write	-	workspace:AccessMode
workspace:tenants:delete	授予注销云办公服务的权限。	write	-	-
workspace:tenants:update	授予修改云办公服务属性的权限。	write	-	workspace:AccessMode
workspace:tenants:getLockStatus	授予查询云办公服务是否被锁定的权限。	read	-	-
workspace:tenants:unlock	授予解除云办公服务锁定状态的权限。	write	-	-
workspace:agencies:create	授予创建委托的权限。	write	-	-
workspace:agencies:get	授予查询委托的权限。	read	-	-
workspace:desktops:createAiAccelerateJob	授予创建渲染加速任务的权限。	write	-	-
workspace:desktops:getAiAccelerateJob	授予查询渲染加速任务的权限。	read	-	-
workspace:desktops:getSysPrepInfo	授予查询 sysprep 详情的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:checkBatchChangeImage	授予校验批量切换镜像的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:tenants:listDesktop	授予查询桌面名称策略列表	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
NamePolicies	的权限。			
workspace:tenants:createDesktopNamePolicy	授予创建桌面名称策略的权限。	write	-	-
workspace:tenants:updateDesktopNamePolicy	授予更新桌面名称策略的权限。	write	-	-
workspace:tenants:batchDeleteDesktopNamePolicies	授予批量删除桌面名称策略的权限。	write	-	-
workspace:desktopPools:create	授予创建桌面池的权限。	write	desktopPool *	-
			user	-
			userGroup	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktopPools:list	授予查询桌面池列表的权限。	list	desktopPool *	-
workspace:desktopPools:update	授予修改桌面池属性的权限。	write	desktopPool *	-
workspace:desktopPools:delete	授予删除桌面池的权限。	write	desktopPool *	-
workspace:desktopPools:get	授予查询桌面池详情的权限。	read	desktopPool *	-
workspace:desktopPools:expand	授予扩容桌面池的权限。	write	desktopPool *	-
workspace:desktopPools:resize	授予桌面池变更规格的权限。	write	desktopPool *	-
workspace:desktopPools:rebuil	授予桌面池重建系统盘的权	write	desktopPool *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
d	限。			
workspace:desktopPools:batchAddVolumes	授予桌面池批量添加磁盘的权限。	write	desktopPool *	-
workspace:desktopPools:batchDeleteVolumes	授予桌面池批量删除磁盘的权限。	write	desktopPool *	-
workspace:desktopPools:batchExpandVolumes	授予桌面池批量扩容磁盘的权限。	write	desktopPool *	-
workspace:desktopPools:operate	授予操作桌面池的权限。	write	desktopPool *	-
workspace:desktopPools:listUsers	授予查询桌面池授权的用户、用户组的权限。	list	desktopPool *	-
workspace:desktopPools:authorizeUsers	授予桌面池授权用户、用户组的权限。	write	desktopPool *	-
			user	-
			userGroup	-
workspace:desktopPools:listDesktops	授予查询桌面池桌面信息的权限。	list	desktopPool *	-
workspace:desktopPools:listScriptTasks	授予查询桌面池的脚本执行任务列表的权限。	list	desktopPool *	-
workspace:desktopPools:executeScripts	授予桌面池批量执行脚本的权限。	write	desktopPool *	-
			script	-
workspace:desktopPools:sendNotifications	授予发送消息通知的权限。	write	desktopPool *	-
workspace:desktops:export	授予导出桌面列表的权限。	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProje

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
				ctId
workspace:desktops:create	授予创建桌面的权限。	write	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • workspace:AssociatePublicIp • workspace:AccessMode
workspace:desktops:list	授予查询桌面列表的权限。	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:update	授予更新桌面信息的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:delete	授予删除桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:get	授予查询桌面详情的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDelete	授予批量删除桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:logoff	授予批量注销桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDetail	授予查询桌面详情列表的权限。	list	desktop *	-
			-	• g:RequestTag/<tag-key>

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
				• g:TagKeys • g:EnterpriseProjectId
workspace:desktops:operate	授予操作桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:resize	授予变更规格的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getConnectStatus	授予查询桌面登录状态统计数据的权限。	read	-	-
workspace:desktops:ListStatus	授予查询桌面登录状态的权限。	list	-	-
workspace:desktops:rebuild	授予重建桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getActions	授予查询桌面开关机信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createConsole	授予获取远程登录控制台地址的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:updateSids	授予更新桌面SID 的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:rejoinDomain	授予重新加入AD 域的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createImage	授予桌面转镜像的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:desktops:batchDetach	授予批量解绑用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:detach	授予解绑用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:attach	授予分配用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getNetwork	授予查询桌面网络信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:changeNetwork	授予切换桌面网络的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:exclusiveHosts:listDesktops	授予查询专享桌面详情列表的权限。	list	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:desktops:listAll	授予查询普通桌面和渲染桌面列表的权限。	list	desktop *	-
workspace:desktopAssociate:listDiscoverVmInfo	授予查询可纳管的虚拟机列表的权限。	list	-	-
workspace:desktopAssociate:startTask	授予启动纳管虚拟机任务的权限。	write	-	-
workspace:desktopAssociate:switchScanTask	授予开启纳管扫描任务的权限。	write	-	-
workspace:desktopAssociate:getScanTaskSwitc	授予查询纳管扫描任务开关的权限。	read	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
h				
workspace:desktops:setMaintenanceMode	授予批量设置桌面管理员维护模式的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:prepAttachUsers	授予预批量分配用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchAttachUsers	授予批量分配用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:changeUsername	授予在Windows AD场景下，修改与桌面关联的用户名的权限。	write	-	-
workspace:desktops:sendNotifications	授予发送消息通知的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:migrate	授予迁移桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listAgents	授予查询桌面安装 agent 列表的权限。	list	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchInstallAgents	授予批量为桌面安装 agent 的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listTags	授予查询桌面标签的权限。	list	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:tag	授予创建桌面	tagging	desktop *	• g:ResourceTag/<tag-key>

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
	标签的权限。			• g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:untag	授予删除桌面标签的权限。	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:listProjectTags	授予查询项目标签的权限。	list	-	-
workspace:desktops:operateTags	授予批量添加删除标签的权限。	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:listByTags	授予使用标签过滤桌面的权限。	list	-	-
workspace:exclusiveHosts:create	授予创建专享主机的权限。	write	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:exclusiveHosts:list	授予查询专享主机列表的权限。	list	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:exclusiveHosts:check	授予校验是否能创建专享主机的权限。	write	-	-
workspace:exclusiveHosts:get	授予查询专享主机详情的权限。	read	exclusiveHost *	g:EnterpriseProjectId
workspace:exclusiveHosts:upd	授予更新专享主机信息的权	write	exclusiveHost *	g:EnterpriseProjectId

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
ate	限。			
workspace:exclusiveHosts:delete	授予删除专享主机的权限。	write	exclusiveHost *	g:EnterpriseProjectId
workspace:mkp:listImages	授予查询云市场镜像列表的权限。	list	-	-
workspace:mkp:listCommodityInfos	授予查询云市场商品信息的权限。	list	-	-
workspace:mkp:createOrder	授予创建云市场产品订单的权限。	write	-	-
workspace:mkp:listListProductReserve	授予查询云市场库存信息的权限。	list	-	-
workspace:mkp:listCommodityDetails	授予查询云市场商品详情的权限。	list	-	-
workspace:mkp:listRelationCommodityDetails	授予查询商品的关联商品的权限。	list	-	-
workspace:mkp:listCommodityAgreements	授予查询云市场商品协议的权限。	list	-	-
workspace:networks:listEips	授予查询 EIP 列表的权限。	list	-	-
workspace:networks:createEips	授予创建 EIP 的权限。	write	-	-
workspace:networks:bindEips	授予绑定 EIP 的权限。	write	-	-
workspace:networks:unbindEips	授予解绑 EIP 的权限。	write	-	-
workspace:networks:getEipQuota	授予查询 EIP 配额的权限。	read	-	-
workspace:netw	授予查询 Nat	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
orks:ListNatGateways	网关列表的权限。			
workspace:orders:create	授予包周期下单的权限。	write	-	• workspace:CreateOrderType • workspace:AssociatePublicIp • workspace:AccessMode
workspace:orders:change	授予创建变更订单的权限。	write	-	workspace:ChangeOrderType
workspace:orders:batchInquiry	授予批量询价的权限。	write	-	-
workspace:quotas:check	授予校验配额的权限。	write	-	-
workspace:rendererDesktops:create	授予创建渲染桌面的权限。	write	-	-
workspace:rendererDesktops:delete	授予删除渲染桌面的权限。	write	-	-
workspace:rendererDesktops:list	授予查询渲染桌面列表的权限。	list	-	-
workspace:rendererDesktops:action	授予操作渲染桌面的权限。	write	-	-
workspace:scheduledTasks:list	授予查询定时任务列表的权限。	list	scheduledTask *	-
workspace:scheduledTasks:create	授予创建定时任务的权限。	write	scheduledTask *	-
			desktop	-
			desktopPool	-
			server	-
			serverGroup	-
workspace:scheduledTasks:get	授予查询定时任务详情的权限。	read	scheduledTask *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:scheduledTasks:update	授予更新定时任务的权限。	write	scheduledTask *	-
			desktop	-
			desktopPool	-
			server	-
			serverGroup	-
workspace:scheduledTasks:delete	授予删除定时任务的权限。	write	scheduledTask *	-
workspace:scheduledTasks:getFuture	授予查询定时任务未来执行时间的权限。	read	-	-
workspace:scheduledTasks:batchDelete	授予批量删除定时任务的权限。	write	scheduledTask *	-
workspace:scheduledTasks:listRecords	授予查询定时任务执行记录的权限。	list	scheduledTask *	-
workspace:scheduledTasks:getRecord	授予查询定时任务执行记录详情的权限。	read	scheduledTask *	-
workspace:scheduledTasks:exportRecords	授予导出定时任务记录及执行详情的权限。	list	scheduledTask *	-
workspace:users:subscribeSharer	授予订阅协同资源的权限。	write	user *	-
workspace:desktops:addSubResources	授予购买桌面附属资源的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:deleteSubResources	授予删除桌面附属资源的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createSnapshots	授予创建桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProje

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
				ctId
workspace:desktops:getSnapshots	授予查询桌面快照的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:deleteSnapshots	授予删除桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:restoreBySnapshot	授予使用桌面快照恢复桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:statistics:listDesktopStatus	授予统计桌面状态的权限。	list	-	-
workspace:statistics:getUnused	授予查询在指定时间段未使用的桌面的权限。	read	-	-
workspace:statistics:getUsed	授予查询使用桌面的时长的权限。	read	-	-
workspace:bindingPolicies:export	授予导出终端与桌面绑定配置 excel 的权限。	list	-	-
workspace:bindingPolicies:getConfig	授予查询终端与桌面绑定的开关配置信息的权限。	read	-	-
workspace:bindingPolicies:createConfig	授予设置终端与桌面绑定的开关配置的权限。	write	-	-
workspace:bindingPolicies:get	授予查询终端与桌面绑定配置列表的权限。	read	-	-
workspace:bind	授予增加终端	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
ingPolicies:add	与桌面绑定配置的权限。			
workspace:bindingPolicies:update	授予修改终端与桌面绑定配置的权限。	write	-	-
workspace:bindingPolicies:delete	授予删除终端与桌面绑定配置的权限。	write	-	-
workspace:volumes:delete	授予删除桌面数据盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:batchAdd	授予增加桌面磁盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:batchExpand	授予扩容桌面磁盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:wdh:getType	授予查询云办公主机类型的权限。	read	wdh *	g:EnterpriseProjectId
workspace:wdh:get	授予查询云办公主机列表的权限。	read	wdh *	g:EnterpriseProjectId
workspace:desktops:getRemoteAssistance	授予查询远程协助信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createRemoteAssistance	授予创建远程协助的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:cancelRemoteAssistance	授予取消远程协助的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:add	授予单个桌面增加磁盘的权	write	desktop	• g:ResourceTag/<tag-key>

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
	限。			• g:EnterpriseProjectId
workspace:volumes:expand	授予扩容磁盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:listDssPoolsDetail	授予获取专属分布式存储池详情列表的权限。	list	-	-
workspace:common:listTimezones	授予查询时区配置的权限。	list	-	-
workspace:connections:securityExport	授予导出连接记录的权限。	list	-	-
workspace:images:list	授予查询支持的镜像列表的权限。	list	-	-
workspace:policyGroups:import	授予导入策略组的权限。	write	-	-
workspace:accessPolicies:create	授予创建接入策略的权限。	write	-	-
workspace:accessPolicies:get	授予查询接入策略的权限。	read	-	-
workspace:accessPolicies:delete	授予删除指定接入策略的权限。	write	-	-
workspace:accessPolicies:getTarget	授予查询指定接入策略的应用对象的权限。	read	-	-
workspace:accessPolicies:updateTarget	授予更新指定接入策略的应用对象的权限。	write	-	-
workspace:products:listDesktop	授予查询支持的产品套餐列	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
Products	表的权限。			
workspace:products:listSharerProducts	授予查询协同套餐列表的权限。	list	-	-
workspace:products:listInternetProducts	授予查询上网套餐列表的权限。	list	-	-
workspace:availabilityZones:list	授予查询支持的可用分区列表的权限。	list	-	-
workspace:userGroups:export	授予导出用户组的权限。	list	userGroup *	-
workspace:users:export	授予导出用户的权限。	list	user *	-
workspace:users:import	授予导入用户的权限。	write	user *	-
workspace:userGroups:exportUsers	授予导出用户组用户的权限。	list	userGroup *	-
workspace:users:operate	授予操作用户（锁定、解锁和重置密码）的权限。	write	user *	-
workspace:users:randomPassword	授予给用户重置随机密码的权限。	write	user *	-
workspace:users:deleteOtps	授予解绑 OTP 设备的权限。	write	user *	-
workspace:users:resendEmail	授予重新发送邮件的权限。	write	user *	-
workspace:connections:securityList	授予查询连接信息的权限。	list	-	-
workspace:connections:listOnlineUsers	授予查询登录人数的权限。	list	-	-
workspace:userGroups:list	授予查询用户组列表的权	list	userGroup *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
	限。			
workspace:userGroups:create	授予创建用户组的权限。	write	userGroup *	-
workspace:userGroups:batchDelete	授予批量删除用户组的权限。	write	userGroup *	-
workspace:userGroups:delete	授予删除桌面用户组的权限。	write	userGroup *	-
workspace:userGroups:update	授予修改用户组信息的权限。	write	userGroup *	-
workspace:userGroups:operate	授予操作用户组的权限。	write	userGroup *	-
			user *	-
workspace:userGroups:getUsers	授予查询用户组中的用户的权限。	list	userGroup *	-
workspace:jobs:listSubJobs	授予查询子任务列表的权限。	list	-	-
workspace:jobs:deleteSubJobRecords	授予删除子任务记录的权限。	write	-	-
workspace:ou:get	授予查询 OU 信息的权限。	list	-	-
workspace:ou:create	授予新增 OU 信息的权限。	write	-	-
workspace:ou:delete	授予删除 OU 信息的权限。	write	-	-
workspace:ou:update	授予更新 OU 信息的权限。	write	-	-
workspace:policyGroups:list	授予查询策略组列表的权限。	list	policyGroup *	-
workspace:policyGroups:creat	授予新增策略组的权限。	write	policyGroup *	-
			desktop	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
e			desktopPool	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:delete	授予删除策略组的权限。	write	policyGroup *	-
workspace:policyGroups:get	授予查询策略组的权限。	read	policyGroup *	-
workspace:policyGroups:update	授予修改策略组的权限。	write	policyGroup *	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:export	授予导出策略组的权限。	list	policyGroup *	-
workspace:policyGroups:listPolicies	授予查询策略组中的策略项的权限。	list	policyGroup *	-
workspace:policyGroups:updatePolicies	授予修改策略组中的策略项的权限。	write	policyGroup *	-
workspace:policyGroups:listTargets	授予查询策略组应用对象的权限。	list	policyGroup *	-
workspace:policyGroups:updateTargets	授予修改策略组应用对象的权限。	write	policyGroup *	-
			desktop	-
			desktopPool	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:listDetail	授予查询策略组详情列表的权限。	list	policyGroup *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:policyGroups:getOriginalPolicies	授予查询初始策略项的权限。	read	policyGroup *	-
workspace:users:list	授予查询用户列表的权限。	list	user *	-
workspace:users:create	授予创建用户的权限。	write	user *	-
workspace:users:delete	授予删除指定用户的权限。	write	user *	-
workspace:users:get	授予查询用户详情信息的权限。	read	user *	-
workspace:users:update	授予修改用户信息的权限。	write	user *	-
workspace:users:batchDelete	授予批量删除用户的权限。	write	user *	-
workspace:users:resetPassword	授予重置用户密码的权限。	write	user *	-
workspace:users:checkResetPasswordToken	授予校验重置域用户密码 Token 的权限。	write	user *	-
workspace:users:getTemplate	授予用户模板下载的权限。	read	-	-
workspace:users:checkExist	授予校验用户是否存在的权限。	write	user *	-
workspace:users:listOtps	授予查询 OTP 设备的权限。	list	user *	-
workspace:users:getImportTemplate	授予创建用户模板下载的权限。	read	-	-
workspace:users:batchCreate	授予批量创建用户的权限。	write	user *	-
workspace:products:listVolumeProducts	授予查询磁盘产品列表的权限。	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:tenants:listExportTasks	授予查询导出任务列表的权限。	list	-	-
workspace:tenants:deleteExportTasks	授予批量删除导出任务记录的权限。	write	-	-
workspace:tenants:exportData	授予下载导出的文件的权限。	read	-	-
workspace:statistics:listAlarm	授予查询告警列表的权限。	list	-	-
workspace:statistics:getAlarm	授予查询告警数的权限。	read	-	-
workspace:statistics:getGrowthRate	授予查询指标环比值的权限。	read	-	-
workspace:statistics:getMetric	授予查询指标的权限。	read	-	-
workspace:statistics:getMetricTrend	授予查询指标趋势的权限。	read	-	-
workspace:statistics:updateNotificationRules	授予更新指标的通知规则的权限。	write	-	-
workspace:statistics:deleteNotificationRules	授予删除指标的通知规则的权限。	write	-	-
workspace:statistics:createNotifyRules	授予新增指标的通知规则的权限。	write	-	-
workspace:statistics:listNotificationRules	授予查询指标的通知规则的权限。	list	-	-
workspace:statistics:listNotificationRecords	授予查询指标通知记录的权限。	list	-	-
workspace:statistics:listDeskto	授予查询桌面使用统计信息	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
pMetrics	的权限。			
workspace:statistics:exportDesktopMetrics	授予导出桌面使用统计信息的权限。	list	-	-
workspace:statistics:listUserMetrics	授予查询用户使用统计信息的权限。	list	-	-
workspace:statistics:exportUserMetrics	授予导出用户使用统计信息;的权限。	list	-	-
workspace:appcenter:createBucketCredential	授予生成 OBS 桶凭证信息信息的权限。	write	-	-
workspace:appcenter:createAndAuthorizeBucket	授予添加并授权默认 OBS 桶的权限。	write	-	-
workspace:appcenter:listApps	授予按照名称分页查询应用的权限。	list	-	-
workspace:appcenter:createApp	授予上传应用的权限。	write	-	-
workspace:appcenter:updateApp	授予修改应用的权限。	write	-	-
workspace:appcenter:deleteApp	授予删除应用的权限。	write	-	-
workspace:appcenter:installApp	授予自动安装应用的权限。	write	-	-
workspace:appcenter:listAppAuthorizations	授予查询应用授权信息的权限。	list	-	-
workspace:appcenter:batchUpdateAppAuthorizations	授予设置应用授权的权限。	write	-	-
workspace:appcenter:batchDeleteApps	授予批量删除应用的权限。	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:appcenter:batchDisableApps	授予批量设置应用不可见的权限。	write	-	-
workspace:appcenter:batchEnableApps	授予批量设置应用可见的权限。	write	-	-
workspace:appcenter:batchInstallApps	授予批量自动安装安装应用的权限。	write	-	-
workspace:appcenter:listAppCatalogs	授予查询应用分类信息的权限。	list	-	-
workspace:appcenter:listJobs	授予查询应用安装 job 信息的权限。	list	-	-
workspace:appcenter:batchDeleteJobs	授予批量删除 job 的权限。	write	-	-
workspace:appcenter:retryJobs	授予重试失败 job 的权限。	write	-	-
workspace:appcenter:createAppRule	授予创建应用规则的权限。	write	-	-
workspace:appcenter:listAppRule	授予查询应用规则的权限。	list	-	-
workspace:appcenter:updateAppRule	授予修改应用规则的权限。	write	-	-
workspace:appcenter:deleteAppRule	授予删除应用规则的权限。	write	-	-
workspace:appcenter:batchDeleteAppRules	授予批量删除应用规则的权限。	write	-	-
workspace:appcenter:enableRuleRestriction	授予启用规则管控的权限。	write	-	-
workspace:appcenter:disableRu	授予禁用规则	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
leRestriction	管控的权限。			
workspace:appcenter:addRestrictedRule	授予增加管控规则的权限。	write	-	-
workspace:appcenter:listRestrictedRule	授予查询管控规则列表的权限。	list	-	-
workspace:appcenter:deleteRestrictedRule	授予批量删除管控规则列表的权限。	write	-	-
workspace:appcenter:updateTenantProfile	授予启禁用租户功能的权限。	write	-	-
workspace:appcenter:listTenantProfiles	授予查询租户功能状态的权限。	list	-	-
workspace:scripts:create	授予创建脚本的权限。	write	script *	-
workspace:scripts:list	授予查询脚本列表的权限。	list	script *	-
workspace:scripts:get	授予查询脚本详情的权限。	read	script *	-
workspace:scripts:put	授予更新脚本的权限。	write	script *	-
workspace:scripts:delete	授予删除脚本的权限。	write	script *	-
workspace:scripts:execute	授予批量执行脚本或命令的权限。	write	script *	-
			desktop *	-
workspace:scripts:getRecordDetail	授予查询脚本或命令执行记录详情的权限。	read	script *	-
workspace:scripts:listRecords	授予查询脚本执行记录列表的权限。	list	script *	-
workspace:scrip	授予查询脚本	list	script *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
ts:listTasks	任务列表的权限。			
workspace:scripts:retry	授予重试脚本的权限。	write	script *	-
workspace:scripts:stop	授予停止脚本或命令执行任务的权限。	write	script *	-
workspace:scripts:download	授予下载脚本输出记录的权限。	write	script *	-
workspace:tenants:getShareSpaceConfig	授予查询协同配置的权限。	read	-	-
workspace:tenants:updateShareSpaceConfig	授予修改协同配置的权限。	write	-	-
workspace:authConfigs:getStatus	授予查询认证状态的权限。	read	-	-
workspace:privacystatements:sign	授予签署隐私声明的权限。	write	-	-
workspace:sites:get	授予查询站点信息的权限。	read	-	-
workspace:sites:add	授予新增站点的权限。	write	-	workspace:AccessMode
workspace:sites:delete	授予删除站点的权限。	write	-	-
workspace:sites:updateAccessMode	授予修改站点接入方式的权限。	write	-	workspace:AccessMode
workspace:sites:updateSubnets	授予修改站点业务子网的权限。	write	-	-
workspace:tenants:checkEnterpriseIds	授予检查企业ID是否已被使用的权限。	write	-	-
workspace:tenants:updateEnter	授予修改企业	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
priseId	ID 的权限。			
workspace:bandwidth:create	授予开通云办公带宽的权限。	write	-	-
workspace:bandwidth:list	授予查询云办公带宽列表的权限。	list	-	-
workspace:bandwidth:update	授予修改云办公带宽的权限。	write	-	-
workspace:bandwidth:delete	授予取消云办公带宽的权限。	write	-	-
workspace:bandwidth:getControlConfig	授予查询云办公带宽的控制配置的权限。	read	-	-
workspace:bandwidth:updateControlConfig	授予修改云办公带宽的控制配置的权限。	write	-	-
workspace:bandwidth:createChangeOrder	授予创建云办公带宽变更订单的权限。	write	-	-
workspace:desktops:batchCreateSnapshots	授予批量创建桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDeleteSnapshots	授予批量删除桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchRestoreSnapshots	授予批量恢复桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listSnapshots	授予查询桌面快照列表的权限。	list	-	-
workspace:desktops:verifyDesk	授予校验桌面名称的权限。	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
topName				
workspace:networks:getAvailableIp	授予根据子网id查询该子网下可用的ip的权限。	read	-	-
workspace:desktops:getAdStatus	授予查询AD网络状态的权限。	read	-	-
workspace:networks:checkIpIfExist	授予检查IP是否存在的权限。	write	-	-
workspace:images:checkIfExist	授予检查镜像是否存在的权限。	write	-	-
workspace:wdh:listDesktops	授予查询云办公主机包含桌面信息的权限。	list	wdh *	-
			-	g:EnterpriseProjectId
workspace:wdh:update	授予更新云办公主机信息的权限。	write	wdh *	g:EnterpriseProjectId
workspace:bindingPolicies:getTemplate	授予下载终端与桌面绑定模板的权限。	read	-	-
workspace:bindingPolicies:import	授予批量导入终端与桌面绑定的权限。	write	-	-
workspace:statistics:getRunState	授予运行状态统计的权限。	read	-	-
workspace:statistics:getLoginState	授予登录状态统计的权限。	read	-	-
workspace:networks:getUsingSubnets	授予查询正在被使用的子网列表的权限。	read	-	-
workspace:networks:listPorts	授予查询端口列表的权限。	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:rendererDesktops:createConsole	授予获取远程登录控制台地址的权限。	write	-	-
workspace:rendererDesktops:resize	授予变更渲染桌面规格的权限。	write	-	-
workspace:exclusiveHosts:resizeLites	授予变更专享主机规格的权限。	write	exclusiveHost *	g:EnterpriseProjectId
workspace:desktops:getMonitor	授予查询桌面监控信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDetachInfo	授予查询桌面历史解绑用户信息的权限。	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:getSysprepVersion	授予查询 sysprep 版本信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:networks:createNat	授予开通 NAT 网关上网功能的权限。	write	-	-
workspace:networks:listNats	授予查询 NAT 网关上网功能的权限。	list	-	-
workspace:networks:listSubnets	授予查询子网列表的权限。	list	-	-
workspace:networks:listVpcs	授予查询查询 vpc 的权限。	list	-	-
workspace:policyGroups:createTemplate	授予创建策略模板的权限。	write	-	-
workspace:policyGroups:listTemplate	授予查询策略模板列表的权限。	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:policyGroups:updateTemplate	授予更新策略模板的权限。	write	-	-
workspace:networks:listSecurityGroups	授予查询安全组列表的权限。	list	-	-
workspace:availabilityZones:getSummary	授予查询可用分区列表概要的权限。	read	-	-
workspace:availabilityZones:get	授予查询可用分区详情的权限。	read	-	-
workspace:users:importUser	授予导入用户列表的权限。	write	user *	-
workspace:users:uploadTemplate	授予导入桌面用户列表的权限。	write	user *	-
workspace:accessPolicies:update	授予更新指定接入策略的权限。	write	-	-
workspace:desktops:verifySource	授予校验桌面来源的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDesktopNetworks	授予批量查询桌面网络信息的权限。	list	desktop *	-
workspace:desktops:batchChangeNetwork	授予批量切换桌面网络的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:jobs:get	授予查询任务详情的权限。	read	-	-
workspace:accessPolicies:importIp	授予导入 IP 列表的权限。	write	-	-
workspace:accessPolicies:getIpImportTemplate	授予下载 IP 导入模板的权限。	read	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:sites:listEdgeSites	授予查询边缘站点的权限。	list	-	-
workspace:sites:checkEdgeSiteResources	授予校验边缘站点资源的权限。	write	-	-
workspace:ou:listAdOus	授予查询 AD 域下 OU 信息的权限。	list	-	-
workspace:ou:listOuUsers	授予查询 OU 下用户信息的权限。	list	-	-
workspace:ou:importUsersByOU	授予导入 OU 用户的权限。	write	-	-
workspace:appGroup:list	授予查询应用组的权限。	list	appGroup *	-
workspace:appGroup:create	授予创建应用组的权限。	write	appGroup *	-
			serverGroup	-
workspace:appGroup:delete	授予应用组删除的权限。	write	appGroup *	-
workspace:appGroup:get	授予查询应用组详情的权限。	read	appGroup *	-
workspace:appGroup:update	授予修改应用组的权限。	write	appGroup *	-
			serverGroup	-
workspace:app:listPublishedApp	授予查询已发布应用的权限。	list	app *	-
			appGroup *	-
workspace:app:publish	授予发布应用的权限。	write	app *	-
			appGroup *	-
workspace:app:get	授予查询应用详细信息的权限。	read	app *	-
			appGroup *	-
workspace:app:update	授予修改应用信息的权限。	write	app *	-
			appGroup *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:app:deleteIcon	授予删除自定义应用图标的权限。	write	app *	-
			appGroup *	-
workspace:app:uploadIcon	授予修改自定义应用图标的权限。	write	app *	-
			appGroup *	-
workspace:app:check	授予校验应用的权限。	write	app *	-
			appGroup *	-
workspace:app:batchDisable	授予批量禁用应用的权限。	write	app *	-
			appGroup *	-
workspace:app:batchEnable	授予批量启用应用的权限。	write	app *	-
			appGroup *	-
workspace:app:unpublish	授予批量取消应用发布的权限。	write	app *	-
			appGroup *	-
workspace:appGroup:listPublishableApp	授予可发布应用列表的权限。	list	appGroup *	-
workspace:appGroup:batchDeleteAuthorization	授予移除应用组授权的权限。	write	appGroup *	-
			user	-
			userGroup	-
workspace:appGroup:disassociate	授予解除服务组关联的所有应用组的权限。	write	-	-
workspace:appGroup:listAuthorization	授予查询应用组授权记录的权限。	list	appGroup *	-
workspace:appGroup:addAuthorization	授予增加应用组授权的权限。	write	appGroup *	-
			user	-
			userGroup	-
workspace:appGroup:batchDelete	授予批量删除应用组的权限。	write	appGroup *	-
workspace:app	授予校验应用	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
Group:check	组的权限。			
workspace:serverGroup:list	授予查询服务器组列表的权限。	list	serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:serverGroup:create	授予创建服务器组的权限。	write	serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:serverGroup:delete	授予删除服务器组的权限。	write	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:get	授予查询指定服务器组的权限。	read	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:update	授予修改服务器组的权限。	write	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:getServerState	授予查询指定服务器组内服务器状态的权限。	read	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:listDetail	授予查询租户服务器组基础信息列表的权限。	list	serverGroup *	-
workspace:serverGroup:getRestrict	授予指定租户服务器组限制查询的权限。	read	serverGroup *	-
workspace:serverGroup:validate	授予校验服务器组的权限。	write	serverGroup *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:serverGroup:tagResource	授予服务器组添加标签的权限。	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:unTagResource	授予服务器组删除标签的权限。	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:listTagsForResource	授予查询服务器组标签的权限。	list	serverGroup *	-
			-	g:EnterpriseProjectId
workspace:serverGroup:listTags	授予查询租户所有服务器上标签的权限。	list	serverGroup *	-
workspace:serverGroup:batchCreateTags	授予批量添加服务器组标签的权限。	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:batchDeleteTags	授予批量删除服务器组标签的权限。	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:server:list	授予查询服务器列表的权限。	list	server *	-
workspace:server:delete	授予删除服务器的权限。	write	server *	• g:ResourceTag/<tag-key>

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
				• g:EnterpriseProjectId
workspace:server:get	授予查询指定服务器的权限。	read	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:update	授予修改服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:changeImage	授予修改服务器的镜像的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:reinstall	授予重装服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:getVncUrl	授予获取 VNC 远程登录地址的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:accessAgent:list	授予查询租户的所有 HDA 最新版本的权限。	list	-	-
workspace:accessAgent:batchUpgrade	授予批量升级服务器 HDA 版本的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:accessAgent:listLatestVersion	授予查询租户的 HDA 最新版本的权限。	list	-	-
workspace:server:listAccessAgentDetails	授予查询服务器的 HDA 相关信息的权限。	list	server *	-
workspace:accessAgent:getUpgradeFlag	授予查询 HDA 升级提醒标识的权限。	read	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:accessAgent:updateUpgradeFlag	授予更新 HDA 升级通知标识的权限。	write	-	-
workspace:accessAgent:listUpgradeRecords	授予查询服务器的 HDA 升级跟踪记录的权限。	list	-	-
workspace:server:batchDelete	授予批量删除服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchChangeMaintainMode	授予标记服务器维护状态的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchReboot	授予重启服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchRejoinDomain	授予批量服务器重新加域的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchStart	授予启动服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchStop	授予关闭服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchUpdateTsvi	授予批量更新服务器虚拟会话 IP 配置的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:create	授予创建应用服务器的权限。	write	server *	-
			serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
				• g:EnterpriseProjectId
workspace:server:batchMigrateHosts	授予迁移云办公主机下面的服务器到目标云办公主机的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			wdh *	-
workspace:server:getMetricData	授予查询云应用服务器监控信息的权限。	read	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:jobs:batchDeleteSubJobs	授予批量删除子任务的权限。	write	-	-
workspace:jobs:countSubJobs	授予子任务数量查询的权限。	list	-	-
workspace:appWarehouse:authorizeObs	授予获取上传至 OBS 桶的 ak/sk 的权限。	write	-	-
workspace:appWarehouse:batchDeleteApp	授予批量删除应用仓库中的指定应用的权限。	write	-	-
workspace:appWarehouse:ListWarehouseApps	授予查询租户应用仓库中的应用列表的权限。	list	-	-
workspace:appWarehouse:createApp	授予在应用仓库中新增应用的权限。	write	-	-
workspace:appWarehouse:deleteApp	授予删除应用仓库中的指定应用的权限。	write	-	-
workspace:appWarehouse:uploadAppIcon	授予在应用仓库中上传图标文件的权限。	write	-	-
workspace:appWarehouse:crea	授予添加桶或者桶授权的权	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
teBucketOrAcl	限。			
workspace:images:listImageJobs	授予查询租户的任务列表的权限。	list	-	-
workspace:images:getImageJob	授予查询任务详情的权限。	read	-	-
workspace:imageServer:list	授予查询镜像实例列表的权限。	list	imageServer *	-
			-	g:EnterpriseProjectId
workspace:imageServer:create	授予创建镜像实例的权限。	write	imageServer *	-
			-	g:EnterpriseProjectId
workspace:imageServer:get	授予查询指定镜像实例的权限。	read	imageServer *	g:EnterpriseProjectId
workspace:imageServer:update	授予修改镜像实例的权限。	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:attachApp	授予分发软件信息至镜像实例的权限。	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:listLatestAttachedApp	授予查询最近一次分发软件信息列表的权限。	list	imageServer *	-
workspace:imageServer:recreate	授予构建云应用镜像的权限。	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:batchDelete	授予批量删除镜像实例的权限。	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:listImageSubJobs	授予子任务查询的权限。	list	-	-
workspace:imageServer:batchDeleteImageSubJobs	授予批量删除子任务的权限。	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:imageServer:countImageSubJobs	授予子任务数量查询的权限。	read	-	-
workspace:appGroup:listMailRecord	授予查询应用组授权邮件发送记录的权限。	list	-	-
workspace:appGroup:resendMail	授予重发应用组授权邮件（根据授权邮件记录）的权限。	write	-	-
workspace:storage:listPersistentStorage	授予查询 WKS 存储的权限。	list	storage *	-
workspace:storage:createPersistentStorage	授予创建 WKS 存储的权限。	write	storage *	-
workspace:storage:deletePersistentStorage	授予删除 WKS 存储的权限。	write	storage *	-
workspace:storage:updateUserFolderAssignment	授予创建个人存储目录的权限。	write	storage *	-
workspace:storage:updateShareFolderAssignment	授予修改共享目录成员的权限。	write	storage *	-
workspace:storage:createShareFolder	授予创建共享存储目录的权限。	write	storage *	-
workspace:storage:deleteStorageClaim	授予删除共享目录的权限。	write	storage *	-
workspace:storage:deleteUserStorageAttachment	授予删除个人存储目录的权限。	write	storage *	-
workspace:storage:batchDeletePersistentStorag	授予批量删除 WKS 存储的权	write	storage *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
e	限。			
workspace:storage:listStorageAssignment	授予查询个人存储目录的权限。	list	storage *	-
workspace:storage:listShareFolder	授予查询共享存储目录的权限。	list	storage *	-
workspace:policyGroups:deleteTemplate	授予删除策略模板的权限。	write	-	-
workspace:privacystatements:get	授予查询最新版本的隐私声明的权限。	read	-	-
workspace:scalingPolicy:delete	授予删除弹性伸缩策略的权限。	write	-	-
workspace:scalingPolicy:list	授予查询服务器组弹性伸缩策略的权限。	read	-	-
workspace:scalingPolicy:create	授予新增/修改弹性伸缩策略的权限。	write	-	-
workspace:session:listAppConnection	授予查询应用使用记录的权限。	write	-	-
workspace:session:logoffUserSession	授予用户会话注销的权限。	write	-	-
workspace:session:listUserConnection	授予查询用户登录记录的权限。	write	-	-
workspace:session:listSessionByUserName	授予根据用户名查询当前会话的权限。	list	-	-
workspace:storagePolicy:create	授予新增或更新存储目录访问权限自定义策略的权限。	write	storage *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:storagePolicy:list	授予查询存储目录访问权限策略的权限。	list	storage *	-
workspace:storage:listSfs3Storage	授予查询SFS3.0 存储的权限。	list	storage *	-
workspace:baseResource:list	授予查询可用分区列表的权限。	list	-	-
workspace:tenants:listConfigInfo	授予查询企业系统配置的权限。	list	-	-
workspace:tenants:active	授予租户服务激活、初始化的权限。	write	-	-
workspace:tenants:listTenantProfile	授予查询租户信息的权限。	list	-	-
workspace:server:listServerMetricData	授予查询服务器的监控数据的权限。	list	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:session:listSessions	授予查询企业会话列表的权限。	list	-	-
workspace:appWarehouse:updateApp	授予更新应用仓库中的应用的权限。	write	-	-
workspace:server:batchChangeImage	授予批量切换服务器镜像的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchReinstall	授予批量重装服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:authConfigs:get	授予查询认证登录方式配置信息的权限。	read	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:authConfigs:update	授予更新认证策略配置信息的权限。	write	-	-
workspace:assistAuthConfigs:get	授予查询辅助认证的配置信息的权限。	read	-	-
workspace:assistAuthConfigs:update	授予更新辅助认证配置的权限。	write	-	-
workspace:jobs:retry	授予重试任务的权限。	write	-	-
workspace:quotas:get	授予查询租户配额的权限。	read	-	-
workspace:tenants:getRoles	授予查询租户角色的权限。	read	-	-
workspace:tenants:ListConfig	授予查询租户个性配置列表的权限。	list	-	-
workspace:tenants:updateConfig	授予修改租户个性配置的权限。	write	-	-
workspace:natMappings:getConfig	授予查询租户的 NAT 映射配置项的权限。	read	-	-
workspace:natMappings:updateConfig	授予修改租户的 NAT 映射配置项的权限。	write	-	-
workspace:tenants:get	授予查询云办公服务详情的权限。	read	-	-
workspace:tenants:open	授予开通云办公服务的权限。	write	-	workspace:AccessMode
workspace:tenants:delete	授予注销云办公服务的权限。	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:tenants:update	授予修改云办公服务属性的权限。	write	-	workspace:AccessMode
workspace:tenants:getLockStatus	授予查询云办公服务是否被锁定的权限。	read	-	-
workspace:tenants:unlock	授予解除云办公服务锁定状态的权限。	write	-	-
workspace:agencies:create	授予创建委托的权限。	write	-	-
workspace:agencies:get	授予查询委托的权限。	read	-	-
workspace:desktops:commitAiAccelerateJob	授予创建渲染加速任务的权限。	write	-	-
workspace:desktops:getAiAccelerateJob	授予查询渲染加速任务的权限。	read	-	-
workspace:desktops:getSysPrepInfo	授予查询 sysprep 详情的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:checkBatchChangeImage	授予校验批量切换镜像的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:tenants:listDesktopNamePolicies	授予查询桌面名称策略列表的权限。	list	-	-
workspace:tenants:createDesktopNamePolicy	授予创建桌面名称策略的权限。	write	-	-
workspace:tenants:updateDesktopNamePolicy	授予更新桌面名称策略的权限。	write	-	-
workspace:tenants:batchDeleteDesktopNameP	授予批量删除桌面名称策略	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
olicies	的权限。			
workspace:desktopPools:create	授予创建桌面池的权限。	write	desktopPool *	-
			user	-
			userGroup	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktopPools:list	授予查询桌面池列表的权限。	list	desktopPool *	-
workspace:desktopPools:update	授予修改桌面池属性的权限。	write	desktopPool *	-
workspace:desktopPools:delete	授予删除桌面池的权限。	write	desktopPool *	-
workspace:desktopPools:get	授予查询桌面池详情的权限。	read	desktopPool *	-
workspace:desktopPools:expand	授予扩容桌面池的权限。	write	desktopPool *	-
workspace:desktopPools:resize	授予桌面池变更规格的权限。	write	desktopPool *	-
workspace:desktopPools:rebuild	授予桌面池重建系统盘的权限。	write	desktopPool *	-
workspace:desktopPools:batchAddVolumes	授予桌面池批量添加磁盘的权限。	write	desktopPool *	-
workspace:desktopPools:batchDeleteVolumes	授予桌面池批量删除磁盘的权限。	write	desktopPool *	-
workspace:desktopPools:batchExpandVolume	授予桌面池批量扩容磁盘的	write	desktopPool *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
s	权限。			
workspace:desktopPools:operate	授予操作桌面池的权限。	write	desktopPool *	-
workspace:desktopPools:listUsers	授予查询桌面池授权的用户、用户组的权限。	list	desktopPool *	-
workspace:desktopPools:authorizeUsers	授予桌面池授权用户、用户组的权限。	write	desktopPool *	-
			user	-
			userGroup	-
workspace:desktopPools:listDesktops	授予查询桌面池桌面信息的权限。	list	desktopPool *	-
workspace:desktopPools:listScriptTasks	授予查询桌面池的脚本执行任务列表的权限。	list	desktopPool *	-
workspace:desktopPools:executeScripts	授予桌面池批量执行脚本的权限。	write	desktopPool *	-
			script	-
workspace:desktopPools:sendNotifications	授予发送消息通知的权限。	write	desktopPool *	-
workspace:desktops:export	授予导出桌面列表的权限。	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:create	授予创建桌面的权限。	write	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • workspace:AssociatePublicIp • workspace:Acces

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
				sMode
workspace:desktops:list	授予查询桌面列表的权限。	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:update	授予更新桌面信息的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:delete	授予删除桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:get	授予查询桌面详情的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDelete	授予批量删除桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:logoff	授予批量注销桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDetail	授予查询桌面详情列表的权限。	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:operate	授予操作桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:resize	授予变更规格的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProje

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
				ctId
workspace:desktops:getConnectStatus	授予查询桌面登录状态统计数据的权限。	read	-	-
workspace:desktops:ListStatus	授予查询桌面登录状态的权限。	list	-	-
workspace:desktops:rebuild	授予重建桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getActions	授予查询桌面开关机信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createConsole	授予获取远程登录控制台地址的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:updateSids	授予更新桌面SID 的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:rejoinDomain	授予重新加入AD 域的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createImage	授予桌面转镜像的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDetach	授予批量解绑用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:detach	授予解绑用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desk	授予分配用户	write	desktop *	• g:ResourceTag/<

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
tops:attach	的权限。			tag-key> • g:EnterpriseProjectId
workspace:desktops:getNetwork	授予查询桌面网络信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:changeNetwork	授予切换桌面网络的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:exclusiveHosts:listDesktops	授予查询专享桌面详情列表的权限。	list	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:desktops:listAll	授予查询普通桌面和渲染桌面列表的权限。	list	desktop *	-
workspace:desktopAssociate:listDiscoverVmInfo	授予查询可纳管的虚拟机列表的权限。	list	-	-
workspace:desktopAssociate:startTask	授予启动纳管虚拟机任务的权限。	write	-	-
workspace:desktopAssociate:switchScanTask	授予开启纳管扫描任务的权限。	write	-	-
workspace:desktopAssociate:getScanTaskSwitch	授予查询纳管扫描任务开关的权限。	read	-	-
workspace:desktops:setMaintenanceMode	授予批量设置桌面管理员维护模式的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:prepAttachUsers	授予预批量分配用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:desktops:batchAttachUsers	授予批量分配用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:changeUsername	授予在Windows AD场景下，修改与桌面关联的用户名的权限。	write	-	-
workspace:desktops:sendNotifications	授予发送消息通知的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:migrate	授予迁移桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listAgents	授予查询桌面安装 agent 列表的权限。	list	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchInstallAgents	授予批量为桌面安装 agent 的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listTags	授予查询桌面标签的权限。	list	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:tag	授予创建桌面标签的权限。	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:untag	授予删除桌面标签的权限。	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:listProjectTags	授予查询项目标签的权限。	list	-	-
workspace:desktops:operateTags	授予批量添加删除标签的权限。	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:listByTags	授予使用标签过滤桌面的权限。	list	-	-
workspace:exclusiveHosts:create	授予创建专享主机的权限。	write	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:exclusiveHosts:list	授予查询专享主机列表的权限。	list	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:exclusiveHosts:check	授予校验是否能创建专享主机的权限。	write	-	-
workspace:exclusiveHosts:get	授予查询专享主机详情的权限。	read	exclusiveHost *	g:EnterpriseProjectId
workspace:exclusiveHosts:update	授予更新专享主机信息的权限。	write	exclusiveHost *	g:EnterpriseProjectId
workspace:exclusiveHosts:delete	授予删除专享主机的权限。	write	exclusiveHost *	g:EnterpriseProjectId
workspace:mkp:listImages	授予查询云市场镜像列表的权限。	list	-	-
workspace:mkp:listCommodity	授予查询云市	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
Infos	场商品信息的权限。			
workspace:mkp:createOrder	授予创建云市场产品订单的权限。	write	-	-
workspace:mkp:listListProductReserve	授予查询云市场库存信息的权限。	list	-	-
workspace:mkp:listCommodityDetails	授予查询云市场商品详情的权限。	list	-	-
workspace:mkp:listRelationCommodityDetails	授予查询商品的关联商品的权限。	list	-	-
workspace:mkp:listCommodityAgreements	授予查询云市场商品协议的权限。	list	-	-
workspace:networks:listEips	授予查询 EIP 列表的权限。	list	-	-
workspace:networks:createEips	授予创建 EIP 的权限。	write	-	-
workspace:networks:bindEips	授予绑定 EIP 的权限。	write	-	-
workspace:networks:unbindEips	授予解绑 EIP 的权限。	write	-	-
workspace:networks:getEipQuota	授予查询 EIP 配额的权限。	read	-	-
workspace:networks:ListNatGateways	授予查询 Nat 网关列表的权限。	list	-	-
workspace:orders:create	授予包周期下单的权限。	write	-	• workspace:CreateOrderType • workspace:AssociatePublicIp • workspace:AccessMode

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:orders:change	授予创建变更订单的权限。	write	-	workspace:ChangeOrderType
workspace:orders:batchInquiry	授予批量询价的权限。	write	-	-
workspace:quotas:check	授予校验配额的权限。	write	-	-
workspace:rendererDesktops:create	授予创建渲染桌面的权限。	write	-	-
workspace:rendererDesktops:delete	授予删除渲染桌面的权限。	write	-	-
workspace:rendererDesktops:list	授予查询渲染桌面列表的权限。	list	-	-
workspace:rendererDesktops:action	授予操作渲染桌面的权限。	write	-	-
workspace:scheduledTasks:list	授予查询定时任务列表的权限。	list	scheduledTask *	-
workspace:scheduledTasks:create	授予创建定时任务的权限。	write	scheduledTask *	-
			desktop	-
			desktopPool	-
			server	-
			serverGroup	-
workspace:scheduledTasks:get	授予查询定时任务详情的权限。	read	scheduledTask *	-
workspace:scheduledTasks:update	授予更新定时任务的权限。	write	scheduledTask *	-
			desktop	-
			desktopPool	-
			server	-
			serverGroup	-
workspace:scheduledTasks:dele	授予删除定时	write	scheduledTask *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
te	任务的权限。			
workspace:scheduledTasks:getFuture	授予查询定时任务未来执行时间的权限。	read	-	-
workspace:scheduledTasks:batchDelete	授予批量删除定时任务的权限。	write	scheduledTask *	-
workspace:scheduledTasks:listRecords	授予查询定时任务执行记录的权限。	list	scheduledTask *	-
workspace:scheduledTasks:getRecord	授予查询定时任务执行记录详情的权限。	read	scheduledTask *	-
workspace:scheduledTasks:exportRecords	授予导出定时任务记录及执行详情的权限。	list	scheduledTask *	-
workspace:users:subscribeSharer	授予订阅协同资源的权限。	write	user *	-
workspace:desktops:addSubResources	授予购买桌面附属资源的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:deleteSubResources	授予删除桌面附属资源的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createSnapshots	授予创建桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getSnapshots	授予查询桌面快照的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:deleteSnapshots	授予删除桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:desktops:restoreBySnapshot	授予使用桌面快照恢复桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:statistics:listDesktopStatus	授予统计桌面状态的权限。	list	-	-
workspace:statistics:getUnused	授予查询在指定时间段未使用的桌面的权限。	read	-	-
workspace:statistics:getUsed	授予查询使用桌面的时长的权限。	read	-	-
workspace:bindingPolicies:export	授予导出终端与桌面绑定配置 excel 的权限。	list	-	-
workspace:bindingPolicies:getConfig	授予查询终端与桌面绑定的开关配置信息的权限。	read	-	-
workspace:bindingPolicies:createConfig	授予设置终端与桌面绑定的开关配置的权限。	write	-	-
workspace:bindingPolicies:get	授予查询终端与桌面绑定配置列表的权限。	read	-	-
workspace:bindingPolicies:add	授予增加终端与桌面绑定配置的权限。	write	-	-
workspace:bindingPolicies:update	授予修改终端与桌面绑定配置的权限。	write	-	-
workspace:bindingPolicies:delete	授予删除终端与桌面绑定配置的权限。	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:volumes:delete	授予删除桌面数据盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:batchAdd	授予增加桌面磁盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:batchExpand	授予扩容桌面磁盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:wdh:getType	授予查询云办公主机类型的权限。	read	wdh *	g:EnterpriseProjectId
workspace:wdh:get	授予查询云办公主机列表的权限。	read	wdh *	g:EnterpriseProjectId
workspace:desktops:getRemoteAssistance	授予查询远程协助信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createRemoteAssistance	授予创建远程协助的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:cancelRemoteAssistance	授予取消远程协助的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:add	授予单个桌面增加磁盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:expand	授予扩容磁盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:listDssPoolsDetail	授予获取专属分布式存储池详情列表的权	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
	限。			
workspace:common:listTimezones	授予查询时区配置的权限。	list	-	-
workspace:connections:securityExport	授予导出连接记录的权限。	list	-	-
workspace:images:list	授予查询支持的镜像列表的权限。	list	-	-
workspace:policyGroups:import	授予导入策略组的权限。	write	-	-
workspace:accessPolicies:create	授予创建接入策略的权限。	write	-	-
workspace:accessPolicies:get	授予查询接入策略的权限。	read	-	-
workspace:accessPolicies:delete	授予删除指定接入策略的权限。	write	-	-
workspace:accessPolicies:getTarget	授予查询指定接入策略的应用对象的权限。	read	-	-
workspace:accessPolicies:updateTarget	授予更新指定接入策略的应用对象的权限。	write	-	-
workspace:products:listDesktopProducts	授予查询支持的产品套餐列表的权限。	list	-	-
workspace:products:listSharerProducts	授予查询协同套餐列表的权限。	list	-	-
workspace:products:listInternetProducts	授予查询上网套餐列表的权限。	list	-	-
workspace:avail	授予查询支持	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
abilityZones:list	的可用分区列表的权限。			
workspace:userGroups:export	授予导出用户组的权限。	list	userGroup *	-
workspace:users:export	授予导出用户的权限。	list	user *	-
workspace:users:import	授予导入用户的权限。	write	user *	-
workspace:userGroups:exportUsers	授予导出用户组用户的权限。	list	userGroup *	-
workspace:users:operate	授予操作用户（锁定、解锁和重置密码）的权限。	write	user *	-
workspace:users:randomPassword	授予给用户重置随机密码的权限。	write	user *	-
workspace:users:deleteOtps	授予解绑 OTP 设备的权限。	write	user *	-
workspace:users:resendEmail	授予重新发送邮件的权限。	write	user *	-
workspace:connections:securityList	授予查询连接信息的权限。	list	-	-
workspace:connections:listOnlineUsers	授予查询登录人数的权限。	list	-	-
workspace:userGroups:list	授予查询用户组列表的权限。	list	userGroup *	-
workspace:userGroups:create	授予创建用户组的权限。	write	userGroup *	-
workspace:userGroups:batchDelete	授予批量删除用户组的权限。	write	userGroup *	-
workspace:userGroups:delete	授予删除桌面用户组的权	write	userGroup *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
	限。			
workspace:userGroups:update	授予修改用户组信息的权限。	write	userGroup *	-
workspace:userGroups:operate	授予操作用户组的权限。	write	userGroup *	-
			user *	-
workspace:userGroups:getUsers	授予查询用户组中的用户的权限。	list	userGroup *	-
workspace:jobs:listSubJobs	授予查询子任务列表的权限。	list	-	-
workspace:jobs:deleteSubJobRecords	授予删除子任务记录的权限。	write	-	-
workspace:ou:get	授予查询 OU 信息的权限。	list	-	-
workspace:ou:create	授予新增 OU 信息的权限。	write	-	-
workspace:ou:delete	授予删除 OU 信息的权限。	write	-	-
workspace:ou:update	授予更新 OU 信息的权限。	write	-	-
workspace:policyGroups:list	授予查询策略组列表的权限。	list	policyGroup *	-
workspace:policyGroups:create	授予新增策略组的权限。	write	policyGroup *	-
			desktop	-
			desktopPool	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:delete	授予删除策略组的权限。	write	policyGroup *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:policyGroups:get	授予查询策略组的权限。	read	policyGroup *	-
workspace:policyGroups:update	授予修改策略组的权限。	write	policyGroup *	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:export	授予导出策略组的权限。	list	policyGroup *	-
workspace:policyGroups:listPolicies	授予查询策略组中的策略项的权限。	list	policyGroup *	-
workspace:policyGroups:updatePolicies	授予修改策略组中的策略项的权限。	write	policyGroup *	-
workspace:policyGroups:listTargets	授予查询策略组应用对象的权限。	list	policyGroup *	-
workspace:policyGroups:updateTargets	授予修改策略组应用对象的权限。	write	policyGroup *	-
			desktop	-
			desktopPool	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:listDetail	授予查询策略组详情列表的权限。	list	policyGroup *	-
workspace:policyGroups:getOriginalPolicies	授予查询初始策略项的权限。	read	policyGroup *	-
workspace:users:list	授予查询用户列表的权限。	list	user *	-
workspace:users:create	授予创建用户的权限。	write	user *	-
workspace:user	授予删除指定	write	user *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
s:delete	用户的权限。			
workspace:users:get	授予查询用户详情信息的权限。	read	user *	-
workspace:users:update	授予修改用户信息的权限。	write	user *	-
workspace:users:batchDelete	授予批量删除用户的权限。	write	user *	-
workspace:users:resetPassword	授予重置用户密码的权限。	write	user *	-
workspace:users:checkResetPasswordToken	授予校验重置域用户密码 Token 的权限。	write	user *	-
workspace:users:getTemplate	授予用户模板下载的权限。	read	-	-
workspace:users:checkExist	授予校验用户是否存在的权限。	write	user *	-
workspace:users:listOtps	授予查询 OTP 设备的权限。	list	user *	-
workspace:users:getImportTemplate	授予创建用户模板下载的权限。	read	-	-
workspace:users:batchCreate	授予批量创建用户的权限。	write	user *	-
workspace:products:listVolumeProducts	授予查询磁盘产品列表的权限。	list	-	-
workspace:tenants:listExportTasks	授予查询导出任务列表的权限。	list	-	-
workspace:tenants:deleteExportTasks	授予批量删除导出任务记录的权限。	write	-	-
workspace:tenants:exportData	授予下载导出的文件的权	read	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
	限。			
workspace:statistics:listAlarm	授予查询告警列表的权限。	list	-	-
workspace:statistics:getAlarm	授予查询告警数的权限。	read	-	-
workspace:statistics:getGrowthRate	授予查询指标环比值的权限。	read	-	-
workspace:statistics:getMetric	授予查询指标的权限。	read	-	-
workspace:statistics:getMetricTrend	授予查询指标趋势的权限。	read	-	-
workspace:statistics:updateNotificationRules	授予更新指标的通知规则的权限。	write	-	-
workspace:statistics:deleteNotificationRules	授予删除指标的通知规则的权限。	write	-	-
workspace:statistics:createNotifyRules	授予新增指标的通知规则的权限。	write	-	-
workspace:statistics:listNotificationRules	授予查询指标的通知规则的权限。	list	-	-
workspace:statistics:listNotificationRecords	授予查询指标通知记录的权限。	list	-	-
workspace:statistics:listDesktopMetrics	授予查询桌面使用统计信息的权限。	list	-	-
workspace:statistics:exportDesktopMetrics	授予导出桌面使用统计信息的权限。	list	-	-
workspace:statistics:listUserMetrics	授予查询用户使用统计信息的权限。	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:statistics:exportUserMetrics	授予导出用户使用统计信息;的权限。	list	-	-
workspace:appcenter:createBucketCredential	授予生成 OBS 桶凭证信息信息的权限。	write	-	-
workspace:appcenter:createAndAuthorizeBucket	授予添加并授权默认 OBS 桶的权限。	write	-	-
workspace:appcenter:listApps	授予按照名称分页查询应用的权限。	list	-	-
workspace:appcenter:createApp	授予上传应用的权限。	write	-	-
workspace:appcenter:updateApp	授予修改应用的权限。	write	-	-
workspace:appcenter:deleteApp	授予删除应用的权限。	write	-	-
workspace:appcenter:installApp	授予自动安装应用的权限。	write	-	-
workspace:appcenter:listAppAuthorizations	授予查询应用授权信息的权限。	list	-	-
workspace:appcenter:batchUpdateAppAuthorizations	授予设置应用授权的权限。	write	-	-
workspace:appcenter:batchDeleteApps	授予批量删除应用的权限。	write	-	-
workspace:appcenter:batchDisableApps	授予批量设置应用不可见的权限。	write	-	-
workspace:appcenter:batchEnableApps	授予批量设置应用可见的权限。	write	-	-
workspace:appc	授予批量自动	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
enter:batchInstallApps	安装安装应用的权限。			
workspace:appcenter:listAppCatalogs	授予查询应用分类信息的权限。	list	-	-
workspace:appcenter:listJobs	授予查询应用安装 job 信息的权限。	list	-	-
workspace:appcenter:batchDeleteJobs	授予批量删除 job 的权限。	write	-	-
workspace:appcenter:retryJobs	授予重试失败 job 的权限。	write	-	-
workspace:appcenter:createAppRule	授予创建应用规则的权限。	write	-	-
workspace:appcenter:listAppRule	授予查询应用规则的权限。	list	-	-
workspace:appcenter:updateAppRule	授予修改应用规则的权限。	write	-	-
workspace:appcenter:deleteAppRule	授予删除应用规则的权限。	write	-	-
workspace:appcenter:batchDeleteAppRules	授予批量删除应用规则的权限。	write	-	-
workspace:appcenter:enableRuleRestriction	授予启用规则管控的权限。	write	-	-
workspace:appcenter:disableRuleRestriction	授予禁用规则管控的权限。	write	-	-
workspace:appcenter:addRestrictedRule	授予增加管控规则的权限。	write	-	-
workspace:appcenter:listRestrictedRule	授予查询管控规则列表的权限。	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:appcenter:deleteRestrictedRule	授予批量删除管控规则列表的权限。	write	-	-
workspace:appcenter:updateTenantProfile	授予启禁用租户功能的权限。	write	-	-
workspace:appcenter:listTenantProfiles	授予查询租户功能状态的权限。	list	-	-
workspace:scripts:create	授予创建脚本的权限。	write	script *	-
workspace:scripts:list	授予查询脚本列表的权限。	list	script *	-
workspace:scripts:get	授予查询脚本详情的权限。	read	script *	-
workspace:scripts:put	授予更新脚本的权限。	write	script *	-
workspace:scripts:delete	授予删除脚本的权限。	write	script *	-
workspace:scripts:execute	授予批量执行脚本或命令的权限。	write	script *	-
			desktop *	-
workspace:scripts:getRecordDetail	授予查询脚本或命令执行记录详情的权限。	read	script *	-
workspace:scripts:listRecords	授予查询脚本执行记录列表的权限。	list	script *	-
workspace:scripts:listTasks	授予查询脚本任务列表的权限。	list	script *	-
workspace:scripts:retry	授予重试脚本的权限。	write	script *	-
workspace:scripts:stop	授予停止脚本或命令执行任务的权限。	write	script *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:scripts:download	授予下载脚本输出记录的权限。	write	script *	-
workspace:tenants:getShareSpaceConfig	授予查询协同配置的权限。	read	-	-
workspace:tenants:updateShareSpaceConfig	授予修改协同配置的权限。	write	-	-
workspace:authConfigs:getStatus	授予查询认证状态的权限。	read	-	-
workspace:privacystatements:sign	授予签署隐私声明的权限。	write	-	-
workspace:sites:get	授予查询站点信息的权限。	read	-	-
workspace:sites:add	授予新增站点的权限。	write	-	workspace:AccessMode
workspace:sites:delete	授予删除站点的权限。	write	-	-
workspace:sites:updateAccessMode	授予修改站点接入方式的权限。	write	-	workspace:AccessMode
workspace:sites:updateSubnets	授予修改站点业务子网的权限。	write	-	-
workspace:tenants:checkEnterpriseIds	授予检查企业ID是否已被使用的权限。	write	-	-
workspace:tenants:updateEnterpriseId	授予修改企业ID的权限。	write	-	-
workspace:bandwidth:create	授予开通云办公带宽的权限。	write	-	-
workspace:bandwidth:list	授予查询云办公带宽列表的权限。	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:bandwidth:update	授予修改云办公带宽的权限。	write	-	-
workspace:bandwidth:delete	授予取消云办公带宽的权限。	write	-	-
workspace:bandwidth:getControlConfig	授予查询云办公带宽的控制配置的权限。	read	-	-
workspace:bandwidth:updateControlConfig	授予修改云办公带宽的控制配置的权限。	write	-	-
workspace:bandwidth:createChangeOrder	授予创建云办公带宽变更订单的权限。	write	-	-
workspace:desktops:batchCreateSnapshots	授予批量创建桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDeleteSnapshots	授予批量删除桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchRestoreSnapshots	授予批量恢复桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listSnapshots	授予查询桌面快照列表的权限。	list	-	-
workspace:desktops:verifyDesktopName	授予校验桌面名称的权限。	write	-	-
workspace:networks:getAvailableIp	授予根据子网 id 查询该子网下可用的 ip 的权限。	read	-	-
workspace:desktops:getAdStatus	授予查询 AD 网络状态的权	read	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
	限。			
workspace:networks:checkIpIfExist	授予检查 IP 是否存在的权限。	write	-	-
workspace:images:checkIfExist	授予检查镜像是否存在的权限。	write	-	-
workspace:wdh:listDesktops	授予查询云办公主机包含桌面信息的权限。	list	wdh *	-
			-	g:EnterpriseProjectId
workspace:wdh:update	授予更新云办公主机信息的权限。	write	wdh *	g:EnterpriseProjectId
workspace:bindingPolicies:getTemplate	授予下载终端与桌面绑定模板的权限。	read	-	-
workspace:bindingPolicies:import	授予批量导入终端与桌面绑定的权限。	write	-	-
workspace:statistics:getRunState	授予运行状态统计的权限。	read	-	-
workspace:statistics:getLoginState	授予登录状态统计的权限。	read	-	-
workspace:networks:getUsingSubnets	授予查询正在被使用的子网列表的权限。	read	-	-
workspace:networks:listPorts	授予查询端口列表的权限。	list	-	-
workspace:rendererDesktops:createConsole	授予获取远程登录控制台地址的权限。	write	-	-
workspace:rendererDesktops:resize	授予变更渲染桌面规格的权限。	write	-	-
workspace:exclusiveHosts:resi	授予变更专享	write	exclusiveHost *	g:EnterpriseProjectI

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
zeLites	主机规格的权限。			d
workspace:desktops:getMonitor	授予查询桌面监控信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDetachInfo	授予查询桌面历史解绑用户信息的权限。	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:getSysprepVersion	授予查询 sysprep 版本信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:networks:createNat	授予开通 NAT 网关上网功能的权限。	write	-	-
workspace:networks:listNats	授予查询 NAT 网关上网功能的权限。	list	-	-
workspace:networks:listSubnets	授予查询子网列表的权限。	list	-	-
workspace:networks:listVpcs	授予查询查询 vpc 的权限。	list	-	-
workspace:policyGroups:createTemplate	授予创建策略模板的权限。	write	-	-
workspace:policyGroups:listTemplate	授予查询策略模板列表的权限。	list	-	-
workspace:policyGroups:updateTemplate	授予更新策略模板的权限。	write	-	-
workspace:networks:listSecurityGroups	授予查询安全组列表的权限。	list	-	-
workspace:avail	授予查询可用	read	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
abilityZones:getSummary	分区列表概要的权限。			
workspace:availabilityZones:get	授予查询可用分区详情的权限。	read	-	-
workspace:users:importUser	授予导入用户列表的权限。	write	user *	-
workspace:users:uploadTemplate	授予导入桌面用户列表的权限。	write	user *	-
workspace:accessPolicies:update	授予更新指定接入策略的权限。	write	-	-
workspace:desktops:verifySource	授予校验桌面来源的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDesktopNetworks	授予批量查询桌面网络信息的权限。	list	desktop *	-
workspace:desktops:batchChangeNetwork	授予批量切换桌面网络的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:jobs:get	授予查询任务详情的权限。	read	-	-
workspace:accessPolicies:importIp	授予导入 IP 列表的权限。	write	-	-
workspace:accessPolicies:getIpImportTemplate	授予下载 IP 导入模板的权限。	read	-	-
workspace:sites:listEdgeSites	授予查询边缘站点的权限。	list	-	-
workspace:sites:checkEdgeSiteResources	授予校验边缘站点资源的权限。	write	-	-
workspace:ou:li	授予查询 AD	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
stAdOus	域下 OU 信息的权限。			
workspace:ou:listOuUsers	授予查询 OU 下用户信息的权限。	list	-	-
workspace:ou:importUsersByOU	授予导入 OU 用户的权限。	write	-	-
workspace:appGroup:list	授予查询应用组的权限。	list	appGroup *	-
workspace:appGroup:create	授予创建应用组的权限。	write	appGroup *	-
			serverGroup	-
workspace:appGroup:delete	授予应用组删除的权限。	write	appGroup *	-
workspace:appGroup:get	授予查询应用组详情的权限。	read	appGroup *	-
workspace:appGroup:update	授予修改应用组的权限。	write	appGroup *	-
			serverGroup	-
workspace:app:listPublishedApp	授予查询已发布应用的权限。	list	app *	-
			appGroup *	-
workspace:app:publish	授予发布应用的权限。	write	app *	-
			appGroup *	-
workspace:app:get	授予查询应用详细信息的权限。	read	app *	-
			appGroup *	-
workspace:app:update	授予修改应用信息的权限。	write	app *	-
			appGroup *	-
workspace:app:deleteIcon	授予删除自定义应用图标的权限。	write	app *	-
			appGroup *	-
workspace:app:uploadIcon	授予修改自定义应用图标的权限。	write	app *	-
			appGroup *	-
workspace:app:	授予校验应用	write	app *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
check	的权限。		appGroup *	-
workspace:app:batchDisable	授予批量禁用应用的权限。	write	app *	-
			appGroup *	-
workspace:app:batchEnable	授予批量启用应用的权限。	write	app *	-
			appGroup *	-
workspace:app:unpublish	授予批量取消应用发布的权限。	write	app *	-
			appGroup *	-
workspace:appGroup:listPublishableApp	授予可发布应用列表的权限。	list	appGroup *	-
workspace:appGroup:batchDeleteAuthorization	授予移除应用组授权的权限。	write	appGroup *	-
			user	-
			userGroup	-
workspace:appGroup:disassociate	授予解除服务组关联的所有应用组的权限。	write	-	-
workspace:appGroup:listAuthorization	授予查询应用组授权记录的权限。	list	appGroup *	-
workspace:appGroup:addAuthorization	授予增加应用组授权的权限。	write	appGroup *	-
			user	-
			userGroup	-
workspace:appGroup:batchDelete	授予批量删除应用组的权限。	write	appGroup *	-
workspace:appGroup:check	授予校验应用组的权限。	write	-	-
workspace:serverGroup:list	授予查询服务器组列表的权限。	list	serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:serverGroup:create	授予创建服务器组的权限。	write	serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:serverGroup:delete	授予删除服务器组的权限。	write	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:get	授予查询指定服务器组的权限。	read	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:update	授予修改服务器组的权限。	write	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:getServerState	授予查询指定服务器组内服务器状态的权限。	read	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:listDetail	授予查询租户服务器组基础信息列表的权限。	list	serverGroup *	-
workspace:serverGroup:getRestrict	授予指定租户服务器组限制查询的权限。	read	serverGroup *	-
workspace:serverGroup:validate	授予校验服务器组的权限。	write	serverGroup *	-
workspace:serverGroup:tagResource	授予服务器组添加标签的权限。	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serv	授予服务器组	taggin	serverGroup *	• g:ResourceTag/<

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
erGroup:unTagResource	删除标签的权限。	g		tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:listTagsForResource	授予查询服务器组标签的权限。	list	serverGroup *	-
			-	g:EnterpriseProjectId
workspace:serverGroup:listTags	授予查询租户所有服务器上标签的权限。	list	serverGroup *	-
workspace:serverGroup:batchCreateTags	授予批量添加服务器组标签的权限。	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:batchDeleteTags	授予批量删除服务器组标签的权限。	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:server:list	授予查询服务器列表的权限。	list	server *	-
workspace:server:delete	授予删除服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:get	授予查询指定服务器的权限。	read	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:update	授予修改服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProje

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
				ctId
workspace:server:changeImage	授予修改服务器的镜像的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:reinstall	授予重装服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:getVncUrl	授予获取 VNC 远程登录地址的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:accessAgent:list	授予查询租户的所有 HDA 最新版本的权限。	list	-	-
workspace:accessAgent:batchUpgrade	授予批量升级服务器 HDA 版本的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:accessAgent:listLatestVersion	授予查询租户的 HDA 最新版本的权限。	list	-	-
workspace:server:listAccessAgentDetails	授予查询服务器的 HDA 相关信息的权限。	list	server *	-
workspace:accessAgent:getUpgradeFlag	授予查询 HDA 升级提醒标识的权限。	read	-	-
workspace:accessAgent:updateUpgradeFlag	授予更新 HDA 升级通知标识的权限。	write	-	-
workspace:accessAgent:listUpgradeRecords	授予查询服务器的 HDA 升级跟踪记录的权限。	list	-	-
workspace:server:batchDelete	授予批量删除服务器的权	write	server *	• g:ResourceTag/<tag-key>

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
	限。			• g:EnterpriseProjectId
workspace:server:batchChangeMaintainMode	授予标记服务器维护状态的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchReboot	授予重启服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchRejoinDomain	授予批量服务器重新加域的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchStart	授予启动服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchStop	授予关闭服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchUpdateTsvi	授予批量更新服务器虚拟会话 IP 配置的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:create	授予创建应用服务器的权限。	write	server *	-
			serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:server:batchMigrateHosts	授予迁移云办公主机下面的服务器到目标云办公主机的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			wdh *	-
workspace:server:getMetricDat	授予查询云应用服务器监控	read	server *	• g:ResourceTag/<tag-key>

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
a	信息的权限。			• g:EnterpriseProjectId
workspace:jobs:batchDeleteSubJobs	授予批量删除子任务的权限。	write	-	-
workspace:jobs:countSubJobs	授予子任务数量查询的权限。	list	-	-
workspace:appWarehouse:authorizeObs	授予获取上传至 OBS 桶的 ak/sk 的权限。	write	-	-
workspace:appWarehouse:batchDeleteApp	授予批量删除应用仓库中的指定应用的权限。	write	-	-
workspace:appWarehouse:ListWarehouseApps	授予查询租户应用仓库中的应用列表的权限。	list	-	-
workspace:appWarehouse:createApp	授予在应用仓库中新增应用的权限。	write	-	-
workspace:appWarehouse:deleteApp	授予删除应用仓库中的指定应用的权限。	write	-	-
workspace:appWarehouse:uploadAppIcon	授予在应用仓库中上传图标文件的权限。	write	-	-
workspace:appWarehouse:createBucketOrAcl	授予添加桶或者桶授权的权限。	write	-	-
workspace:images:listImageJobs	授予查询租户的任务列表的权限。	list	-	-
workspace:images:getImageJob	授予查询任务详情的权限。	read	-	-
workspace:ima	授予查询镜像	list	imageServer *	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
geServer:list	实例列表的权限。		-	g:EnterpriseProjectId
workspace:imageServer:create	授予创建镜像实例的权限。	write	imageServer *	-
			-	g:EnterpriseProjectId
workspace:imageServer:get	授予查询指定镜像实例的权限。	read	imageServer *	g:EnterpriseProjectId
workspace:imageServer:update	授予修改镜像实例的权限。	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:attachApp	授予分发软件信息至镜像实例的权限。	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:listLatestAttachedApp	授予查询最近一次分发软件信息列表的权限。	list	imageServer *	-
workspace:imageServer:recreate	授予构建云应用镜像的权限。	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:batchDelete	授予批量删除镜像实例的权限。	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:listImageSubJobs	授予子任务查询的权限。	list	-	-
workspace:imageServer:batchDeleteImageSubJobs	授予批量删除子任务的权限。	write	-	-
workspace:imageServer:countImageSubJobs	授予子任务数量查询的权限。	read	-	-
workspace:appGroup:listMailRecord	授予查询应用组授权邮件发送记录的权限。	list	-	-
workspace:appGroup:resendM	授予重发应用组授权邮件	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
ail	（根据授权邮件记录）的权限。			
workspace:storage:listPersistentStorage	授予查询 WKS 存储的权限。	list	storage *	-
workspace:storage:createPersistentStorage	授予创建 WKS 存储的权限。	write	storage *	-
workspace:storage:deletePersistentStorage	授予删除 WKS 存储的权限。	write	storage *	-
workspace:storage:updateUserFolderAssignment	授予创建个人存储目录的权限。	write	storage *	-
workspace:storage:updateShareFolderAssignment	授予修改共享目录成员的权限。	write	storage *	-
workspace:storage:createShareFolder	授予创建共享存储目录的权限。	write	storage *	-
workspace:storage:deleteStorageClaim	授予删除共享目录的权限。	write	storage *	-
workspace:storage:deleteUserStorageAttachment	授予删除个人存储目录的权限。	write	storage *	-
workspace:storage:batchDeletePersistentStorage	授予批量删除 WKS 存储的权限。	write	storage *	-
workspace:storage:listStorageAssignment	授予查询个人存储目录的权限。	list	storage *	-
workspace:storage:listShareFolder	授予查询共享存储目录的权限。	list	storage *	-
workspace:policyGroups:delet	授予删除策略	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
eTemplate	模板的权限。			
workspace:privacystatements:get	授予查询最新版本的隐私声明的权限。	read	-	-
workspace:scalingPolicy:delete	授予删除弹性伸缩策略的权限。	write	-	-
workspace:scalingPolicy:list	授予查询服务器组弹性伸缩策略的权限。	read	-	-
workspace:scalingPolicy:create	授予新增/修改弹性伸缩策略的权限。	write	-	-
workspace:session:listAppConnection	授予查询应用使用记录的权限。	write	-	-
workspace:session:logoffUserSession	授予用户会话注销的权限。	write	-	-
workspace:session:listUserConnection	授予查询用户登录记录的权限。	write	-	-
workspace:session:listSessionByUserName	授予根据用户名查询当前会话的权限。	list	-	-
workspace:storagePolicy:create	授予新增或更新存储目录访问权限自定义策略的权限。	write	storage *	-
workspace:storagePolicy:list	授予查询存储目录访问权限策略的权限。	list	storage *	-
workspace:storage:listSfs3Storage	授予查询SFS3.0 存储的权限。	list	storage *	-
workspace:baseResource:list	授予查询可用分区列表的权限。	list	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:tenants:listConfigInfo	授予查询企业系统配置的权限。	list	-	-
workspace:tenants:active	授予租户服务激活、初始化的权限。	write	-	-
workspace:tenants:listTenantProfile	授予查询租户信息的权限。	list	-	-
workspace:server:listServerMetricData	授予查询服务器的监控数据的权限。	list	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:session:listSessions	授予查询企业会话列表的权限。	list	-	-
workspace:appWarehouse:updateApp	授予更新应用仓库中的应用的权限。	write	-	-
workspace:server:batchChangeImage	授予批量切换服务器镜像的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchReinstall	授予批量重装服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:tenants:updateAccessAddressBackupConfig	授予修改云办公服务接入地址备份配置的权限	write	-	-
workspace:tenants:listAccessAddressBackupConfig	授予获取云办公服务接入地址备份配置的权限	list	-	-
workspace:desktops:listWithConnectStatus	授予查询桌面连接状态列表的权限	list	-	-
workspace:orders:createDeskto	授予创建桌面	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
pOrder	订单的权限			
workspace:products:listHourPackageProducts	授予查询可订购小时包套餐的权限	list	-	-

Workspace 的 API 通常对应着一个或多个授权项。表 3-222 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-218 API 与操作项的关系

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/auth-config/method-config	workspace:authConfigs:get	-
PUT /v2/{project_id}/auth-config/method-config	workspace:authConfigs:update	-
GET /v2/{project_id}/assist-auth-config/method-config	workspace:assistAuthConfigs:get	-
PUT /v2/{project_id}/assist-auth-config/method-config	workspace:assistAuthConfigs:update	-
POST /v2/{project_id}/workspace-jobs/{job_id}/actions	workspace:jobs:retry	-
GET /v2/{project_id}/quotas	workspace:quotas:get	-
GET /v2/{project_id}/tenants/roles	workspace:tenants:getRoles	-
GET /v2/{project_id}/tenant-configs	workspace:tenants:ListConfig	-
PUT /v2/{project_id}/tenant-configs	workspace:tenants:updateConfig	-
GET /v2/{project_id}/nat-mapping-configs	workspace:natMappings:getConfig	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
PUT /v2/{project_id}/nat-mapping-configs	workspace:natMappings:updateConfig	-
GET /v2/{project_id}/workspaces	workspace:tenants:get	• vpc:vpcs:get • vpc:subnets:get • vpc:securityGroups:get
POST /v2/{project_id}/workspaces	workspace:tenants:open	• eip:bandwidths:create • eip:publicIps:create • elb:healthmonitors:create • elb:healthmonitors:show • elb:listeners:create • elb:listeners:update • elb:listeners:show • elb:listeners:list • elb:loadbalancers:create • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:list • elb:members:update • elb:pools:create • elb:pools:update • elb:pools:show • vpc:ports:create • vpc:ports:delete • vpc:securityGroupRules:create • vpc:securityGroupRules:delete • vpc:securityGroupRules:get • vpc:securityGroups:create • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:get
DELETE /v2/{project_id}/workspaces	workspace:tenants:delete	• elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:delete • elb:listeners:show • elb:loadbalancers:delete

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
		• elb:loadbalancers:show • elb:members:delete • elb:members:list • elb:pools:delete • elb:pools:show • vpc:ports:delete • vpc:securityGroups:delete • vpcep:endpoints:delete • vpcep:endpoints:get • eip:publicIps:disassociateInstance • eip:bandwidths:delete • eip:publicIps:delete
PUT /v2/{project_id}/workspaces	workspace:tenants:update	• eip:bandwidths:create • eip:bandwidths:delete • eip:publicIps:create • eip:publicIps:delete • eip:publicIps:disassociateInstance • elb:healthmonitors:create • elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:create • elb:listeners:delete • elb:listeners:update • elb:listeners:show • elb:loadbalancers:create • elb:loadbalancers:delete • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:delete • elb:members:list • elb:members:update • elb:pools:create • elb:pools:delete • elb:pools:update • elb:pools:show • vpc:subnets:get • vpc:subnets:update

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
		• vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:delete • vpcep:endpoints:get
GET /v2/{project_id}/workspaces/lock-status	workspace:tenants:getLockStatus	-
PUT /v2/{project_id}/workspaces/lock-status	workspace:tenants:unlock	-
POST /v2/{project_id}/agencies	workspace:agencies:create	• iam:agencies:listV5 • iam:agencies:getV5 • iam:agencies:createServiceLinkedAgencyV5 • iam:roles:getRole • iam:roles:listRoles • iam:agencies:getAgency • iam:agencies:listAgencies • iam:agencies:createAgency • iam:permissions:listRolesForAgencyOnProject • iam:permissions:grantRoleToAgencyOnProject
GET /v2/{project_id}/agencies	workspace:agencies:get	• iam:agencies:listV5 • iam:agencies:getV5 • iam:agencies:getAgency • iam:agencies:listAgencies • iam:permissions:listRolesForAgencyOnProject
POST /v3/{project_id}/desktops/{desktop_id}/ai-accelerate-job	workspace:desktops:commitAiAccelerateJob	-
POST /v2/{project_id}/desktops/{desktop_id}/ai-accelerate-job	workspace:desktops:createAiAccelerateJob	-
GET /v2/{project_id}/ai-accelerate-job/{job_id}	workspace:desktops:getAiAccelerateJob	-
POST /v2/{project_id}/sysprep	workspace:desktops:getSysPrepInfo	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/verification/batch-change-image	workspace:desktops:checkBatchChangeImage	ims:images:list
GET /v2/{project_id}/desktop-name-policies	workspace:tenants:listDesktopNamePolicies	-
POST /v2/{project_id}/desktop-name-policies	workspace:tenants:createDesktopNamePolicy	-
PUT /v2/{project_id}/desktop-name-policies/{policy_id}	workspace:tenants:updateDesktopNamePolicy	-
POST /v2/{project_id}/desktop-name-policies/batch-delete	workspace:tenants:batchDeleteDesktopNamePolicies	-
POST /v2/{project_id}/desktop-pools	workspace:desktopPools:create	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
GET /v2/{project_id}/desktop-pools	workspace:desktopPools:list	ims:images:list
PUT /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:update	-
DELETE /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:delete	-
GET /v2/{project_id}/desktop-	workspace:desktopPool	ims:images:list

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
pools/{pool_id}	s:get	
POST /v2/{project_id}/desktop-pools/{pool_id}/expand	workspace:desktopPools:expand	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
POST /v2/{project_id}/desktop-pools/{pool_id}/resize	workspace:desktopPools:resize	• vpc:subnets:get • ims:images:list
POST /v2/{project_id}/desktop-pools/{pool_id}/rebuild	workspace:desktopPools:rebuild	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-add	workspace:desktopPools:batchAddVolumes	-
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-delete	workspace:desktopPools:batchDeleteVolumes	-
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-expand	workspace:desktopPools:batchExpandVolumes	-
POST	workspace:desktopPool	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
/v2/{project_id}/desktop-pools/{pool_id}/action	s:operate	
GET /v2/{project_id}/desktop-pools/{pool_id}/users	workspace:desktopPools:listUsers	-
POST /v2/{project_id}/desktop-pools/{pool_id}/users	workspace:desktopPools:authorizeUsers	ims:images:list
GET /v2/{project_id}/desktop-pools/{pool_id}/desktops	workspace:desktopPools:listDesktops	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktop-pools/script-execution-tasks/detail	workspace:desktopPools:listScriptTasks	-
POST /v2/{project_id}/desktop-pools/{pool_id}/script-executions	workspace:desktopPools:executeScripts	-
POST /v2/{project_id}/desktop-pools/{pool_id}/notifications	workspace:desktopPools:sendNotifications	-
GET /v3/{project_id}/desktops/export	workspace:desktops:export	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
POST /v2/{project_id}/desktops	workspace:desktops:create	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
		• vpc:ports:update • eip:publicIps:get • eip:publicIps:list • eip:publicIps:create • eip:publicIps:associateInstance • eip:publicIps:delete • eip:publicIps:createTags • vpc:quotas:list • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
GET /v2/{project_id}/desktops	workspace:desktops:list	-
PUT /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:update	-
DELETE /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:delete	• vpc:ports:get • vpc:ports:delete
GET /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:get	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
POST /v2/{project_id}/desktops/batch-delete	workspace:desktops:batchDelete	• vpc:ports:get • vpc:ports:delete
POST /v2/{project_id}/desktops/logoff	workspace:desktops:logoff	-
GET /v2/{project_id}/desktops/detail	workspace:desktops:listDetail	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
POST /v2/{project_id}/desktops/action	workspace:desktops:operate	-
POST	workspace:desktops:res	• vpc:subnets:get

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
/v2/{project_id}/desktops/resize	ize	• ims:images:list
GET /v2/{project_id}/connections/status	workspace:desktops:getConnectStatus	-
GET /v2/{project_id}/desktops/status	workspace:desktops:ListStatus	-
POST /v2/{project_id}/desktops/rebuild	workspace:desktops:rebuild	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
GET /v2/{project_id}/desktops/{desktop_id}/actions	workspace:desktops:getActions	-
GET /v2/{project_id}/desktops/{desktop_id}/remote-consoles	workspace:desktops:createConsole	-
PUT /v2/{project_id}/desktops/sids	workspace:desktops:updateSids	-
POST /v2/{project_id}/desktops/{desktop_id}/rejoin-domain	workspace:desktops:rejoinDomain	-
POST /v2/{project_id}/desktops/desktop-to-image	workspace:desktops:createImage	• ims:quotas:get • ims:images:get • ims:images:list • ims:images:setTags • ims:images:setOrDeleteTags • ims:images:updateMemberStatus • ims:images:copyInRegion • ims:serverImages:create
POST /v2/{project_id}/desktops/batch-detach	workspace:desktops:batchDetach	vpc:ports:get

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktops/detach	workspace:desktops:detach	vpc:ports:get
POST /v2/{project_id}/desktops/attach	workspace:desktops:attach	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
GET /v2/{project_id}/desktops/{desktop_id}/networks	workspace:desktops:getNetwork	• vpc:vpcs:get • vpc:networks:get • vpc:subnets:get • vpc:ports:get • vpc:securityGroups:get • eip:publicIps:list
PUT /v2/{project_id}/desktops/{desktop_id}/networks	workspace:desktops:changeNetwork	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:securityGroups:get • eip:publicIps:list • eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
GET /v2/{project_id}/exclusive-hosts/{host_id}/desktops	workspace:exclusiveHosts:listDesktops	-
GET /v2/{project_id}/all-desktops	workspace:desktops:listAll	-
GET /v2/{project_id}/desktop-associate/discover-vm/infos	workspace:desktopAssociate:listDiscoverVmInfo	-
POST /v2/{project_id}/desktop-	workspace:desktopAsso	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
associate/tasks	ciate:startTask	
POST /v2/{project_id}/desktop-associate/discover-vm/switch	workspace:desktopAssociate:switchScanTask	-
GET /v2/{project_id}/desktop-associate/discover-vm/switch	workspace:desktopAssociate:getScanTaskSwitch	-
PUT /v2/{project_id}/desktops/maintenance-mode	workspace:desktops:setMaintenanceMode	-
POST /v2/{project_id}/desktops/pre-batch-attach	workspace:desktops:prepAttachUsers	-
POST /v2/{project_id}/desktops/batch-attach	workspace:desktops:batchAttachUsers	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
PUT /v2/{project_id}/desktops/change-username	workspace:desktops:changeUsername	-
POST /v2/{project_id}/desktops/notifications	workspace:desktops:sendNotifications	-
POST /v2/{project_id}/desktops/{desktop_id}/migrate	workspace:desktops:migrate	• vpc:networks:get • vpc:subnets:get • vpc:ports:create • vpc:ports:delete • vpc:ports:update • vpc:ports:get
GET /v2/{project_id}/desktops/agents	workspace:desktops:listAgents	-
POST /v2/{project_id}/desktops/agents	workspace:desktops:batchInstallAgents	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/desktops/{desktop_id}/tags	workspace:desktops:listTags	-
POST /v2/{project_id}/desktops/{desktop_id}/tags	workspace:desktops:tag	-
DELETE /v2/{project_id}/desktops/{desktop_id}/tags/{key}	workspace:desktops:untag	-
GET /v2/{project_id}/desktops/tags	workspace:desktops:listProjectTags	-
POST /v2/{project_id}/desktops/{desktop_id}/tags/action	workspace:desktops:operateTags	-
POST /v2/{project_id}/desktops/resource_instances/action	workspace:desktops:listByTags	-
POST /v2/{project_id}/desktops/batch-tags	workspace:desktops:tag	-
DELETE /v2/{project_id}/desktops/batch-tags	workspace:desktops:untag	-
POST /v2/{project_id}/exclusive-hosts	workspace:exclusiveHosts:create	• vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:subnets:get • vpc:vpcs:get
GET /v2/{project_id}/exclusive-hosts	workspace:exclusiveHosts:list	-
POST /v2/{project_id}/exclusive-hosts/check-limits	workspace:exclusiveHosts:check	-
GET /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:get	• nat:snatRules:list • eip:publicIps:list
PUT /v2/{project_id}/exclusive-	workspace:exclusiveHosts:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
hosts/{host_id}		
DELETE /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:delete	-
GET /v2/{project_id}/market-images	workspace:mkp:listImages	ims:images:list
GET /v2/{project_id}/mkp/commodities/commodity-ids	workspace:mkp:listCommodityInfos	-
POST /v2/{project_id}/mkp/order	workspace:mkp:createOrder	-
POST /v2/{project_id}/mkp/product-reserve	workspace:mkp:listListProductReserve	-
GET /v2/{project_id}/mkp/commodities	workspace:mkp:listCommodityDetails	-
GET /v2/{project_id}/mkp/commodities/{commodity_id}/relation-commodities	workspace:mkp:listRelationCommodityDetails	-
GET /v2/{project_id}/mkp/commodities/agreements	workspace:mkp:listCommodityAgreements	-
GET /v2/{project_id}/eips	workspace:networks:listEips	• eip:publicIps:list • eip:bandwidths:list
POST /v2/{project_id}/eips	workspace:networks:createEips	• vpc:quotas:list • eip:publicIps:create • eip:publicIps:associateInstance
POST /v2/{project_id}/eips/binding	workspace:networks:bindEips	• eip:publicIps:associateInstance • eip:publicIps:get
POST /v2/{project_id}/eips/unbinding	workspace:networks:unbindEips	• eip:publicIps:list • eip:publicIps:disassociateInstance
GET /v2/{project_id}/eips/quotas	workspace:networks:getEipQuota	vpc:quotas:list
GET /v2/{project_id}/nat-	workspace:networks:ListNatGateways	• vpc:subnets:get • vpc:vpcs:get

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
gateways		• nat:snatRules:list • nat:natGateways:list
POST /v2/{project_id}/periodic/subscribe/order	workspace:orders:create	• ims:images:list • vpc:vpcs:get • vpc:networks:get • vpc:subnets:get • vpc:ports:get • bss:order:update
POST /v2/{project_id}/periodic/{desktop_id}/change/order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/periodic/change/batch-order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/periodic/inquiry/change-image	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/change/order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/desktop-pool/periodic/inquiry/add-volume	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/change-image	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/extend-volume	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/resize	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/periodic/inquiry/add-resources	workspace:orders:batchInquiry	ims:images:list
GET /v2/{project_id}/checkOrderLimits	workspace:quotas:check	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/render-desktops	workspace:renderDesktops:create	• ims:images:list • ims:images:share • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get
DELETE /v2/{project_id}/render-desktops	workspace:renderDesktops:delete	• vpc:ports:get • vpc:ports:delete
GET /v2/{project_id}/render-desktops	workspace:renderDesktops:list	-
POST /v2/{project_id}/render-desktops/action	workspace:renderDesktops:action	-
GET /v2/{project_id}/scheduled-tasks	workspace:scheduledTasks:list	-
POST /v2/{project_id}/scheduled-tasks	workspace:scheduledTasks:create	-
GET /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:get	-
PUT /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:update	-
DELETE /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:delete	-
POST /v2/{project_id}/scheduled-tasks/future-executions	workspace:scheduledTasks:getFuture	-
POST /v2/{project_id}/scheduled-tasks/batch-delete	workspace:scheduledTasks:batchDelete	-
GET /v2/{project_id}/scheduled	workspace:scheduledTasks:listRecords	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
-tasks/{task_id}/records		
GET /v2/{project_id}/scheduled-tasks/{task_id}/records/{record_id}	workspace:scheduledTasks:getRecord	-
POST /v2/{project_id}/scheduled-tasks/{task_id}/records/export	workspace:scheduledTasks:exportRecords	-
POST /v2/{project_id}/user/share-resources	workspace:users:subscribeSharer	-
POST /v2/{project_id}/desktop/sub-resources	workspace:desktops:addSubResources	-
POST /v2/{project_id}/desktop/delete-sub-resources	workspace:desktops:deleteSubResources	-
POST /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:createSnapshots	-
GET /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:getSnapshots	-
DELETE /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:deleteSnapshots	-
POST /v2/{project_id}/desktops/{desktop_id}/snapshots/restore	workspace:desktops:restoreBySnapshot	-
GET /v2/{project_id}/statistics	workspace:statistics:listDesktopStatus	-
GET /v2/{project_id}/desktops/statistics/unused	workspace:statistics:getUnused	-
POST /v2/{project_id}/desktops/statistics/used	workspace:statistics:getUsed	-
GET /v3/{project_id}/terminals/binding-	workspace:bindingPolicies:export	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
desktops/template/export		
GET /v2/{project_id}/terminals/binding-desktops/config	workspace:bindingPolicies:getConfig	-
POST /v2/{project_id}/terminals/binding-desktops/config	workspace:bindingPolicies:createConfig	-
GET /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:get	-
POST /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:add	-
PUT /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:update	-
POST /v2/{project_id}/terminals/binding-desktops/batch-delete	workspace:bindingPolicies:delete	-
POST /v2/{project_id}/desktops/{desktop_id}/volumes/batch-delete	workspace:volumes:delete	-
POST /v2/{project_id}/volumes	workspace:volumes:batchAdd	-
POST /v2/{project_id}/volumes/expand	workspace:volumes:batchExpand	-
GET /v2/{project_id}/hosts/types	workspace:wdh:getType	-
GET /v2/{project_id}/hosts	workspace:wdh:get	-
GET /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:getRemoteAssistance	-
POST /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:createRemoteAssistance	-
DELETE	workspace:desktops:ca	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
/v2/{project_id}/desktops/{desktop_id}/remote-assistance	ncelRemoteAssistance	
POST /v2/{project_id}/desktops/{desktop_id}/volumes	workspace:volumes:add	-
POST /v2/{project_id}/desktops/{desktop_id}/volumes/{volume_id}/expand	workspace:volumes:expand	-
GET /v2/{project_id}/dss-pools/detail	workspace:volumes:listDssPoolsDetail	dss:pools:list
GET /v2/{project_id}/common/timezones	workspace:common:listTimezones	-
GET /v3/{project_id}/desktops/connections/export	workspace:connections:securityExport	-
GET /v2/{project_id}/images	workspace:images:list	ims:images:list
POST /v2/{project_id}/policy-groups/import	workspace:policyGroups:import	-
POST /v2/{project_id}/access-policy	workspace:accessPolicies:create	-
GET /v2/{project_id}/access-policy	workspace:accessPolicies:get	-
DELETE /v2/{project_id}/access-policy	workspace:accessPolicies:delete	-
GET /v2/{project_id}/access-policy/{access_policy_id}/objects	workspace:accessPolicies:getTarget	-
PUT /v2/{project_id}/access-policy/{access_policy_id}/objects	workspace:accessPolicies:updateTarget	-
GET /v2/{project_id}/products	workspace:products:listDesktopProducts	ecs:cloudServerFlavors:get

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/products/sharer	workspace:products:listSharerProducts	-
GET /v2/{project_id}/products/adninternet	workspace:products:listInternetProducts	-
GET /v2/{project_id}/availability-zones	workspace:availabilityZones:list	-
GET /v2/{project_id}/groups/export	workspace:userGroups:export	-
POST /v3/{project_id}/users/export	workspace:users:export	-
POST /v2/{project_id}/users/import	workspace:users:import	-
GET /v3/{project_id}/groups/{group_id}/users/export	workspace:userGroups:exportUsers	-
GET /v2/{project_id}/groups/{group_id}/users/export	workspace:userGroups:exportUsers	-
POST /v2/{project_id}/users/{user_id}/actions	workspace:users:operate	-
GET /v2/{project_id}/users/{user_id}/random-password	workspace:users:randomPassword	-
DELETE /v2/{project_id}/users/{user_id}/otp-devices	workspace:users:deleteOtps	-
POST /v2/{project_id}/users/{user_id}/resend-email	workspace:users:resendEmail	-
GET /v2/{project_id}/connections/desktops	workspace:connections:securityList	-
GET /v2/{project_id}/connections/desktops/export	workspace:connections:securityExport	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/connections/online-users	workspace:connections:listOnlineUsers	-
GET /v2/{project_id}/desktops/connections	workspace:connections:securityList	-
GET /v2/{project_id}/desktops/connections/export	workspace:connections:securityExport	-
GET /v2/{project_id}/desktops/online-users	workspace:connections:listOnlineUsers	-
GET /v2/{project_id}/groups	workspace:userGroups:list	-
POST /v2/{project_id}/groups	workspace:userGroups:create	-
POST /v2/{project_id}/groups/batch-delete	workspace:userGroups:batchDelete	-
DELETE /v2/{project_id}/groups/{group_id}	workspace:userGroups:delete	-
PUT /v2/{project_id}/groups/{group_id}	workspace:userGroups:update	-
POST /v2/{project_id}/groups/{group_id}/actions	workspace:userGroups:operate	-
GET /v2/{project_id}/groups/{group_id}/users	workspace:userGroups:getUsers	-
GET /v2/{project_id}/workspace-sub-jobs	workspace:jobs:listSubJobs	-
POST /v2/{project_id}/workspace-sub-jobs/batch-delete	workspace:jobs:deleteSubJobRecords	-
GET /v2/{project_id}/ous	workspace:ou:get	-
POST /v2/{project_id}/ous	workspace:ou:create	-
DELETE	workspace:ou:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
/v2/{project_id}/ous/{ou_id}		
PUT /v2/{project_id}/ous/{ou_id}	workspace:ou:update	-
GET /v2/{project_id}/policy-groups	workspace:policyGroups:list	-
POST /v2/{project_id}/policy-groups	workspace:policyGroups:create	-
DELETE /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:delete	-
GET /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:get	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:update	-
POST /v2/{project_id}/policy-groups/export	workspace:policyGroups:export	-
GET /v2/{project_id}/policy-groups/{policy_group_id}/policies	workspace:policyGroups:listPolicies	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}/policies	workspace:policyGroups:updatePolicies	-
GET /v2/{project_id}/policy-groups/{policy_group_id}/targets	workspace:policyGroups:listTargets	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}/targets	workspace:policyGroups:updateTargets	-
GET /v2/{project_id}/policy-groups/detail	workspace:policyGroups:listDetail	-
GET /v2/{project_id}/policy-	workspace:policyGroup	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
groups/original-policies	s:getOriginalPolicies	
GET /v2/{project_id}/users	workspace:users:list	-
POST /v2/{project_id}/users	workspace:users:create	-
DELETE /v2/{project_id}/users/{user_id}	workspace:users:delete	-
GET /v2/{project_id}/users/{user_id}	workspace:users:get	-
PUT /v2/{project_id}/users/{user_id}	workspace:users:update	-
POST /v2/{project_id}/users/batch-delete	workspace:users:batchDelete	-
POST /v2/{project_id}/users/password	workspace:users:resetPassword	-
POST /v2/{project_id}/users/password-token	workspace:users:checkResetPasswordToken	-
GET /v2/{project_id}/users/desktop-users/template	workspace:users:getTemplate	-
POST /v2/{project_id}/users/exist	workspace:users:checkExist	-
GET /v2/{project_id}/users/{user_id}/otp-devices	workspace:users:listOtps	-
GET /v2/{project_id}/users/template/download	workspace:users:getImportTemplate	-
POST /v2/{project_id}/users/export	workspace:users:export	-
POST /v2/{project_id}/users/batch-create	workspace:users:batchCreate	-
GET	workspace:products:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
/v2/{project_id}/volume/products	VolumeProducts	
GET /v2/{project_id}/export-tasks	workspace:tenants:listExportTasks	-
POST /v2/{project_id}/export-tasks/batch-delete	workspace:tenants:deleteExportTasks	-
GET /v2/{project_id}/export-tasks/{task_id}/download	workspace:tenants:exportData	-
GET /v2/{project_id}/alarms	workspace:statistics:listAlarm	ces:alarmHistory:list
GET /v2/{project_id}/statistics/alarms	workspace:statistics:getAlarm	ces:alarmHistory:list
GET /v2/{project_id}/statistics/growth-rate	workspace:statistics:getGrowthRate	-
GET /v2/{project_id}/statistics/metrics	workspace:statistics:getMetric	-
GET /v2/{project_id}/statistics/metrics/trend	workspace:statistics:getMetricTrend	-
PUT /v2/{project_id}/statistics/notify-rules/{rule_id}	workspace:statistics:updateNotificationRules	smn:topic:get
DELETE /v2/{project_id}/statistics/notify-rules/{rule_id}	workspace:statistics:deleteNotificationRules	-
POST /v2/{project_id}/statistics/notify-rules	workspace:statistics:createNotifyRules	smn:topic:get
GET /v2/{project_id}/statistics/notify-rules	workspace:statistics:listNotificationRules	-
GET /v2/{project_id}/statistics/notification-records	workspace:statistics:listNotificationRecords	-
GET /v2/{project_id}/statistics/metrics/desktops	workspace:statistics:listDesktopMetrics	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/statistics/metrics/desktops/export	workspace:statistics:exportDesktopMetrics	-
GET /v2/{project_id}/statistics/metrics/users	workspace:statistics:listUserMetrics	-
GET /v2/{project_id}/statistics/metrics/users/export	workspace:statistics:exportUserMetrics	-
GET /v3/{project_id}/statistics/metrics/desktops/export	workspace:statistics:exportDesktopMetrics	-
GET /v3/{project_id}/statistics/metrics/users/export	workspace:statistics:exportUserMetrics	-
POST /v1/{project_id}/app-center/buckets/actions/create-credential	workspace:appcenter:createBucketCredential	• obs:bucket:GetBucketAcl • obs:object:PutObject • obs:object:DeleteObject
POST /v1/{project_id}/app-center/buckets	workspace:appcenter:createAndAuthorizeBucket	• obs:bucket:HeadBucket • obs:bucket:PutBucketAcl • obs:bucket:PutReplicationConfiguration • obs:bucket:CreateBucket • obs:bucket:PutBucketCORS
GET /v1/{project_id}/app-center/apps	workspace:appcenter:listApps	-
POST /v1/{project_id}/app-center/apps	workspace:appcenter:createApp	-
PATCH /v1/{project_id}/app-center/apps/{app_id}	workspace:appcenter:updateApp	-
DELETE /v1/{project_id}/app-center/apps/{app_id}	workspace:appcenter:deleteApp	-
POST /v1/{project_id}/app-center/apps/{app_id}/actions/auto-install	workspace:appcenter:installApp	-
GET /v1/{project_id}/app-	workspace:appcenter:lis	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
center/apps/{app_id}/authorizations	tAppAuthorizations	
POST /v1/{project_id}/app-center/apps/{app_id}/actions/assign-authorizations	workspace:appcenter:batchUpdateAppAuthorizations	-
POST /v1/{project_id}/app-center/apps/actions/batch-delete	workspace:appcenter:batchDeleteApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-disable	workspace:appcenter:batchDisableApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-enable	workspace:appcenter:batchEnableApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-assign-authorization	workspace:appcenter:batchUpdateAppAuthorizations	-
POST /v1/{project_id}/app-center/apps/actions/batch-auto-install	workspace:appcenter:batchInstallApps	-
GET /v1/{project_id}/app-center/app-catalogs	workspace:appcenter:listAppCatalogs	-
GET /v1/{project_id}/app-center/jobs	workspace:appcenter:listJobs	-
POST /v1/{project_id}/app-center/jobs/actions/batch-delete	workspace:appcenter:batchDeleteJobs	-
POST /v1/{project_id}/app-center/jobs/actions/retry	workspace:appcenter:retryJobs	-
POST /v1/{project_id}/app-center/app-rules	workspace:appcenter:createAppRule	-
GET /v1/{project_id}/app-	workspace:appcenter:listAppRule	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
center/app-rules		
PATCH /v1/{project_id}/app-center/app-rules/{rule_id}	workspace:appcenter:updateAppRule	-
DELETE /v1/{project_id}/app-center/app-rules/{rule_id}	workspace:appcenter:deleteAppRule	-
POST /v1/{project_id}/app-center/app-rules/batch-delete	workspace:appcenter:batchDeleteAppRules	-
POST /v1/{project_id}/app-center/app-rules/actions/enable-rule-restriction	workspace:appcenter:enableRuleRestriction	-
POST /v1/{project_id}/app-center/app-rules/actions/disable-rule-restriction	workspace:appcenter:disableRuleRestriction	-
POST /v1/{project_id}/app-center/app-restricted-rules	workspace:appcenter:addRestrictedRule	-
GET /v1/{project_id}/app-center/app-restricted-rules	workspace:appcenter:listRestrictedRule	-
POST /v1/{project_id}/app-center/app-restricted-rules/actions/batch-delete	workspace:appcenter:deleteRestrictedRule	-
PATCH /v1/{project_id}/app-center/profiles	workspace:appcenter:updateTenantProfile	-
GET /v1/{project_id}/app-center/profiles	workspace:appcenter:listTenantProfiles	-
POST /v2/{project_id}/scripts	workspace:scripts:create	-
GET /v2/{project_id}/scripts	workspace:scripts:list	-
GET /v2/{project_id}/scripts/{sc	workspace:scripts:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
ript_id}		
PUT /v2/{project_id}/scripts/{script_id}	workspace:scripts:put	-
DELETE /v2/{project_id}/scripts/{script_id}	workspace:scripts:delete	-
POST /v2/{project_id}/script-executions	workspace:scripts:execute	-
GET /v2/{project_id}/script-execution-records/{record_id}	workspace:scripts:getRecordDetail	-
GET /v2/{project_id}/script-execution-records	workspace:scripts:listRecords	-
GET /v2/{project_id}/script-execution-tasks	workspace:scripts:listTasks	-
POST /v2/{project_id}/script-executions/retry	workspace:scripts:retry	-
POST /v2/{project_id}/script-executions/stop	workspace:scripts:stop	-
POST /v2/{project_id}/script-execution-records/{record_id}/download	workspace:scripts:download	-
GET /v2/{project_id}/share-space/configuration	workspace:tenants:getShareSpaceConfig	-
PUT /v2/{project_id}/share-space/configuration	workspace:tenants:updateShareSpaceConfig	-
GET /v2/{project_id}/auth-config/status	workspace:authConfigs:getStatus	-
POST /v2/{project_id}/privacystatement	workspace:privacystatements:sign	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/quotas/detail	workspace:quotas:get	-
GET /v2/{project_id}/sites	workspace:sites:get	-
POST /v2/{project_id}/sites	workspace:sites:add	• eip:bandwidths:create • eip:publicIps:create • elb:healthmonitors:create • elb:healthmonitors:show • elb:listeners:create • elb:listeners:update • elb:listeners:show • elb:listeners:list • elb:loadbalancers:create • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:list • elb:members:update • elb:pools:create • elb:pools:update • elb:pools:show • vpc:ports:create • vpc:ports:delete • vpc:securityGroupRules:create • vpc:securityGroupRules:delete • vpc:securityGroupRules:get • vpc:securityGroups:create • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:get
DELETE /v2/{project_id}/sites/{site_id}	workspace:sites:delete	• elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:delete • elb:listeners:show • elb:loadbalancers:delete • elb:loadbalancers:show

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
		• elb:members:delete • elb:members:list • elb:pools:delete • elb:pools:show • vpc:ports:delete • vpc:securityGroups:delete • vpcep:endpoints:delete • vpcep:endpoints:get • eip:publicIps:disassociateInstance • eip:bandwidths:delete • eip:publicIps:delete
PUT /v2/{project_id}/sites/{site_id}/access-mode	workspace:sites:updateAccessMode	• eip:bandwidths:create • eip:bandwidths:delete • eip:publicIps:create • eip:publicIps:delete • eip:publicIps:disassociateInstance • elb:healthmonitors:create • elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:create • elb:listeners:delete • elb:listeners:update • elb:listeners:show • elb:loadbalancers:create • elb:loadbalancers:delete • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:delete • elb:members:list • elb:members:update • elb:pools:create • elb:pools:delete • elb:pools:update • elb:pools:show • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
		• vpcep:endpoints:create • vpcep:endpoints:delete • vpcep:endpoints:get
PUT /v2/{project_id}/sites/{site_id}/subnet-ids	workspace:sites:updateSubnets	• vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get
GET /v2/{project_id}/tenants/lock-status	workspace:tenants:getLockStatus	-
PUT /v2/{project_id}/tenants/lock-status	workspace:tenants:unlock	-
POST /v2/{project_id}/workspaces/enterprise-ids/check	workspace:tenants:checkEnterpriseIds	-
PUT /v2/{project_id}/workspaces/enterprise-id	workspace:tenants:updateEnterpriseId	-
POST /v2/{project_id}/bandwidths	workspace:bandwidth:create	-
GET /v2/{project_id}/bandwidths	workspace:bandwidth:list	-
POST /v2/{project_id}/bandwidths/{bandwidth_id}/update	workspace:bandwidth:update	-
DELETE /v2/{project_id}/bandwidths/{bandwidth_id}	workspace:bandwidth:delete	-
GET /v2/{project_id}/bandwidths/{bandwidth_id}/control-list	workspace:bandwidth:getControlConfig	-
PUT /v2/{project_id}/bandwidths/{bandwidth_id}/control-list	workspace:bandwidth:updateControlConfig	-
POST /v2/{project_id}/bandwidths/{bandwidth_id}/periodic/change/order	workspace:bandwidth:createChangeOrder	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/adns	workspace:bandwidth:create	-
GET /v2/{project_id}/adns	workspace:bandwidth:list	-
POST /v2/{project_id}/desktops-adn/batch-delete	workspace:bandwidth:delete	-
POST /v2/{project_id}/snapshots/batch-create	workspace:desktops:batchCreateSnapshots	-
POST /v2/{project_id}/snapshots/batch-delete	workspace:desktops:batchDeleteSnapshots	-
POST /v2/{project_id}/snapshots/batch-restore	workspace:desktops:batchRestoreSnapshots	-
GET /v2/{project_id}/snapshots	workspace:desktops:listSnapshots	-
POST /v2/{project_id}/verification/desktop-name	workspace:desktops:verifyDesktopName	-
GET /v2/{project_id}/subnets/{subnet_id}/available-ip	workspace:networks:getAvailableIp	-
GET /v2/{project_id}/ad/status	workspace:desktops:getAdStatus	-
GET /v2/{project_id}/ip-exist	workspace:networks:checkIpIfExist	-
POST /v2/{project_id}/desktops/check-images	workspace:images:checkIfExist	ims:images:list
GET /v2/{project_id}/hosts/{host_id}/servers	workspace:wdh:listDesktops	-
PUT /v2/{project_id}/hosts	workspace:wdh:update	-
GET /v2/{project_id}/terminals/binding-desktops/template	workspace:bindingPolicies:getTemplate	-
POST /v2/{project_id}/terminals/binding-	workspace:bindingPolicies:import	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
desktops/template/import		
GET /v2/{project_id}/terminals/binding-desktops/template/export	workspace:bindingPolicies:export	-
GET /v2/{project_id}/desktops/statistics/run-state	workspace:statistics:getRunState	-
GET /v2/{project_id}/desktops/statistics/login-state	workspace:statistics:getLoginState	-
GET /v2/{project_id}/subnets/using-subnets	workspace:networks:getUsingSubnets	-
GET /v2/{project_id}/ports	workspace:networks:listPorts	-
GET /v2/{project_id}/render-desktops/{desktop_id}/remote-consoles	workspace:renderDesktops:createConsole	-
PUT /v2/{project_id}/render-desktops/resize	workspace:renderDesktops:resize	-
POST /v2/{project_id}/exclusive-hosts/{host_id}/resize-lites	workspace:exclusiveHosts:resizeLites	-
GET /services/v2/{project_id}/desktops/{desktop_id}	workspace:desktops:get	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktop-monitor/{desktop_id}	workspace:desktops:getMonitor	ces:metricData:get
GET /v2/{project_id}/desktops/export	workspace:desktops:export	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktops/	workspace:desktops:listDetachInfo	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
{desktop_id}/detach-info		
GET /v2/{project_id}/desktops/{desktop_id}/sysprep	workspace:desktops:getSysprepVersion	-
POST /v2/{project_id}/internet	workspace:networks:createNat	• vpc:ports:delete • vpc:ports:get • vpc:networks:get • eip:publicIps:create • eip:publicIps:update • eip:publicIps:delete • nat:snatRules:list • nat:snatRules:create • nat:natGateways:list • nat:natGateways:create
GET /v2/{project_id}/internet	workspace:networks:listNats	• vpc:subnets:get • vpc:vpcs:get • nat:snatRules:list • nat:natGateways:list
POST /v2/{project_id}/quotas/check	workspace:quotas:check	-
GET /v2/{project_id}/subnets	workspace:networks:listSubnets	• vpc:subnets:list • vpc:subnets:get
GET /v2/{project_id}/vpcs	workspace:networks:listVpcs	vpc:vpcs:list
POST /v2/{project_id}/policy-groups/policy-template	workspace:policyGroups:createTemplate	-
GET /v1/{project_id}/policy-templates	workspace:policyGroups:listTemplate	-
PUT /v2/{project_id}/policy-groups/policy-template/{policy_group_id}	workspace:policyGroups:updateTemplate	-
GET /v2/{project_id}/security-groups	workspace:networks:listSecurityGroups	-
GET /v2/{project_id}/availabilit	workspace:availabilityZones:getSummary	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
y-zones/summary		
GET /v2/{project_id}/availability-zones/detail	workspace:availabilityZones:get	-
POST /v2/{project_id}/users/desktop-users/action/import	workspace:users:importUser	-
POST /v2/{project_id}/users/template-upload	workspace:users:uploadTemplate	-
PUT /v2/{project_id}/access-policy/{access_policy_id}	workspace:accessPolicies:update	-
POST /v2/{project_id}/desktops/{desktop_id}/verify-source	workspace:desktops:verifySource	-
GET /v2/{project_id}/desktops/networks	workspace:desktops:listDesktopNetworks	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:securityGroups:get • eip:publicIps:list
POST /v2/{project_id}/desktops/networks/batch-change	workspace:desktops:batchChangeNetwork	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:securityGroups:get • eip:publicIps:list • eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
GET /v2/{project_id}/workspace-jobs/{job_id}	workspace:jobs:get	-
POST /v2/{project_id}/ip/import	workspace:accessPolicies:importIp	-
GET /v2/{project_id}/ip/templat	workspace:accessPolicies:getIpImportTemplate	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
e/download		
GET /v2/{project_id}/wks-edge-sites	workspace:sites:listEdgeSites	• ies:edgeSite:list • ies:edgeSite:getMetricData
POST /v2/{project_id}/check-edge-site-resources	workspace:sites:checkEdgeSiteResources	• ies:edgeSite:list • ies:edgeSite:getMetricData
GET /v2/{project_id}/ad-ous	workspace:ou:listAdOus	-
GET /v2/{project_id}/ou-users	workspace:ou:listOuUsers	-
POST /v2/{project_id}/ou-users/import	workspace:ou:importUsersByOU	-
GET /v1/{project_id}/app-groups	workspace:appGroup:list	-
POST /v1/{project_id}/app-groups	workspace:appGroup:create	-
DELETE /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:delete	-
GET /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:get	-
PATCH /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:update	-
GET /v1/{project_id}/app-groups/{app_group_id}/apps	workspace:app:listPublishedApp	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps	workspace:app:publish	-
GET /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}	workspace:app:get	-
PATCH /v1/{project_id}/app-groups/{app_group_id}/ap	workspace:app:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
ps/{app_id}		
DELETE /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}/icon	workspace:app:deleteIcon	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}/icon	workspace:app:uploadIcon	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/check	workspace:app:check	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/disable	workspace:app:batchDisable	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/enable	workspace:app:batchEnable	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/batch-unpublish	workspace:app:unpublish	-
GET /v1/{project_id}/app-groups/{app_group_id}/publishable-app	workspace:appGroup:listPublishableApp	-
POST /v1/{project_id}/app-groups/actions/batch-delete-authorization	workspace:appGroup:batchDeleteAuthorization	-
POST /v1/{project_id}/app-groups/actions/disassociate-app-group	workspace:appGroup:disassociate	-
GET /v1/{project_id}/app-groups/actions/list-authorizations	workspace:appGroup:listAuthorization	-
POST /v1/{project_id}/app-groups/authorizations	workspace:appGroup:addAuthorization	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/app-groups/batch-delete	workspace:appGroup:batchDelete	-
POST /v1/{project_id}/app-groups/rules/validate	workspace:appGroup:check	-
GET /v1/{project_id}/app-server-groups	workspace:serverGroup:list	-
POST /v1/{project_id}/app-server-groups	workspace:serverGroup:create	• ims:images:list • vpc:ports:get • vpc:subnets:get
DELETE /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:delete	-
GET /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:get	-
PATCH /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:update	ims:images:list
GET /v1/{project_id}/app-server-groups/{server_group_id}/state	workspace:serverGroup:getServerState	-
GET /v1/{project_id}/app-server-groups/actions/list	workspace:serverGroup:listDetail	-
GET /v1/{project_id}/app-server-groups/resources/restrict	workspace:serverGroup:getRestrict	-
POST /v1/{project_id}/app-server-groups/rules/validate	workspace:serverGroup:validate	-
POST /v1/{project_id}/server-group/{server_group_id}/tags/create	workspace:serverGroup:tagResource	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
DELETE /v1/{project_id}/server-group/{server_group_id}/tags/delete	workspace:serverGroup:unTagResource	-
GET /v1/{project_id}/server-group/{server_group_id}/tags	workspace:serverGroup:listTagsForResource	-
GET /v1/{project_id}/server-group/tags	workspace:serverGroup:listTags	-
POST /v1/{project_id}/server-group/tags/batch-create	workspace:serverGroup:batchCreateTags	-
DELETE /v1/{project_id}/server-group/tags/batch-delete	workspace:serverGroup:batchDeleteTags	-
GET /v1/{project_id}/app-servers	workspace:server:list	-
DELETE /v1/{project_id}/app-servers/{server_id}	workspace:server:delete	• iam:roles:listRoles • vpc:ports:delete • vpc:ports:get
GET /v1/{project_id}/app-servers/{server_id}	workspace:server:get	-
PATCH /v1/{project_id}/app-servers/{server_id}	workspace:server:update	-
POST /v1/{project_id}/app-servers/{server_id}/actions/change-image	workspace:server:changeImage	• ims:images:list • vpc:ports:get • vpc:subnets:get
POST /v1/{project_id}/app-servers/{server_id}/actions/reinstall	workspace:server:reinstall	• ims:images:list • vpc:ports:get • vpc:subnets:get
GET /v1/{project_id}/app-servers/{server_id}/actions/vnc	workspace:server:getVncUrl	-
GET /v1/{project_id}/app-servers/access-agent/latest-	workspace:accessAgent:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
version		
PATCH /v1/{project_id}/app-servers/access-agent/actions/upgrade	workspace:accessAgent:batchUpgrade	-
GET /v1/{project_id}/app-servers/access-agent/latest-version	workspace:accessAgent:listLatestVersion	-
GET /v1/{project_id}/app-servers/access-agent/list	workspace:server:listAccessAgentDetails	-
GET /v1/{project_id}/app-servers/access-agent/upgrade-flag	workspace:accessAgent:getUpgradeFlag	-
PATCH /v1/{project_id}/app-servers/access-agent/upgrade-flag	workspace:accessAgent:updateUpgradeFlag	-
GET /v1/{project_id}/app-servers/access-agent/upgrade-record	workspace:accessAgent:listUpgradeRecords	-
POST /v1/{project_id}/app-servers/actions/batch-delete	workspace:server:batchDelete	• iam:roles:listRoles • vpc:ports:delete • vpc:ports:get
PATCH /v1/{project_id}/app-servers/actions/batch-maint	workspace:server:batchChangeMaintainMode	-
PATCH /v1/{project_id}/app-servers/actions/batch-reboot	workspace:server:batchReboot	-
PATCH /v1/{project_id}/app-servers/actions/batch-rejoin-domain	workspace:server:batchRejoinDomain	-
PATCH /v1/{project_id}/app-servers/actions/batch-start	workspace:server:batchStart	-
PATCH /v1/{project_id}/app-	workspace:server:batchStop	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
servers/actions/batch-stop		
PATCH /v1/{project_id}/app-servers/actions/batch-update-tsvi	workspace:server:batchUpdateTsvi	• vpc:subnets:get • vpc:ports:update
POST /v1/{project_id}/app-servers/actions/create	workspace:server:create	• ims:images:list • ims:images:updateMemberStatus • ims:images:share • ims:images:get • vpc:securityGroups:get • vpc:securityGroupRules:get • vpc:networks:get • vpc:subnets:get • vpc:ports:create • vpc:ports:get • vpc:ports:delete • vpc:vpcs:get • dss:pools:list
PATCH /v1/{project_id}/app-servers/hosts/batch-migrate	workspace:server:batchMigrateHosts	-
GET /v1/{project_id}/app-servers/metric-data/{server_id}	workspace:server:getMetricData	-
GET /v1/{project_id}/app-server-sub-jobs	workspace:jobs:listSubJobs	-
POST /v1/{project_id}/app-server-sub-jobs/actions/batch-delete	workspace:jobs:batchDeleteSubJobs	-
GET /v1/{project_id}/app-server-sub-jobs/actions/count	workspace:jobs:countSubJobs	-
POST /v1/{project_id}/app-warehouse/action/authorize	workspace:appWarehouse:authorizeObs	• obs:bucket:GetBucketAcl • obs:object:PutObject • obs:object:DeleteObject
POST /v1/{project_id}/app-warehouse/actions/batch-	workspace:appWarehouse:batchDeleteApp	• obs:bucket:HeadBucket • obs:object:DeleteObject

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
delete		
GET /v1/{project_id}/app-warehouse/apps	workspace:appWarehouse:ListWarehouseApps	-
POST /v1/{project_id}/app-warehouse/apps	workspace:appWarehouse:createApp	-
DELETE /v1/{project_id}/app-warehouse/apps/{id}	workspace:appWarehouse:deleteApp	• obs:bucket:HeadBucket • obs:object:DeleteObject
POST /v1/{project_id}/app-warehouse/apps/icon	workspace:appWarehouse:uploadAppIcon	obs:object:PutObject
POST /v1/{project_id}/app-warehouse/bucket-and-acl/create	workspace:appWarehouse:createBucketOrAcl	• obs:bucket:GetBucketAcl • obs:bucket:HeadBucket • obs:bucket:PutBucketAcl • obs:bucket:PutReplicationConfiguration • obs:bucket:CreateBucket • obs:bucket:PutBucketCORS
GET /v1/{project_id}/check/quota	workspace:quotas:get	-
GET /v1/{project_id}/image-server-jobs	workspace:images:listImageJobs	-
GET /v1/{project_id}/image-server-jobs/{job_id}	workspace:images:getImageJob	-
GET /v1/{project_id}/image-servers	workspace:imageServer:list	-
POST /v1/{project_id}/image-servers	workspace:imageServer:create	• ims:images:list • vpc:ports:get • vpc:subnets:get
GET /v1/{project_id}/image-servers/{server_id}	workspace:imageServer:get	-
PATCH /v1/{project_id}/image-servers/{server_id}	workspace:imageServer:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/image-servers/{server_id}/actions/attach-app	workspace:imageServer:attachApp	-
GET /v1/{project_id}/image-servers/{server_id}/actions/latest-attached-app	workspace:imageServer:listLatestAttachedApp	-
POST /v1/{project_id}/image-servers/{server_id}/actions/recreate-image	workspace:imageServer:recreate	• vpc:ports:get • vpc:subnets:get • ims:quotas:get • ims:images:get • ims:images:list • ims:images:setTags • ims:images:setOrDeleteTags • ims:images:updateMemberStatus • ims:images:copyInRegion • ims:serverImages:create
PATCH /v1/{project_id}/image-servers/actions/batch-delete	workspace:imageServer:batchDelete	-
GET /v1/{project_id}/image-server-sub-jobs	workspace:imageServer:listImageSubJobs	-
PATCH /v1/{project_id}/image-server-sub-jobs/actions/batch-delete	workspace:imageServer:batchDeleteImageSubJobs	-
GET /v1/{project_id}/image-server-sub-jobs/actions/count	workspace:imageServer:countImageSubJobs	-
GET /v2/{project_id}/job/{job_id}	workspace:jobs:get	-
GET /v1/{project_id}/mails	workspace:appGroup:listMailRecord	-
POST /v1/{project_id}/mails/actions/send	workspace:appGroup:resendMail	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/mails/actions/send-by-authorization	workspace:appGroup:resendMail	-
GET /v1/{project_id}/persistent-storages	workspace:storage:listPersistentStorage	-
POST /v1/{project_id}/persistent-storages	workspace:storage:createPersistentStorage	• obs:bucket:HeadBucket • obs:bucket:PutBucketPolicy • obs:bucket:PutBucketAcl • obs:bucket:PutBucketCORS
DELETE /v1/{project_id}/persistent-storages/{storage_id}	workspace:storage:deletePersistentStorage	• obs:object:GetObject • obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/assign-folder	workspace:storage:updateUserFolderAssignment	-
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/assign-share-folder	workspace:storage:updateShareFolderAssignment	-
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/create-share-folder	workspace:storage:createShareFolder	• obs:object:GetObject • obs:object:PutObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/delete-storage-claim	workspace:storage:deleteStorageClaim	obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/delete-user-attachment	workspace:storage:deleteUserStorageAttachment	obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/actions/batch-delete	workspace:storage:batchDeletePersistentStorage	-
GET /v1/{project_id}/persistent-storages/actions/list-attachments	workspace:storage:listStorageAssignment	-
GET /v1/{project_id}/persistent-storages/actions/list-share-	workspace:storage:listShareFolder	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
folders		
GET /v1/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:get	-
GET /v1/{project_id}/policy-groups/{policy_group_id}/policy	workspace:policyGroups:listPolicies	-
GET /v1/{project_id}/policy-groups/{policy_group_id}/target	workspace:policyGroups:listTargets	-
GET /v1/{project_id}/policy-groups/show/detail	workspace:policyGroups:listDetail	-
GET /v1/{project_id}/policy-templates	workspace:policyGroups:listTemplate	-
DELETE /v1/{project_id}/policy-templates/{policy_template_id}	workspace:policyGroups:deleteTemplate	-
PATCH /v1/{project_id}/policy-templates/{policy_template_id}	workspace:policyGroups:updateTemplate	-
GET /v1/{project_id}/privacy-statement	workspace:privacystatements:get	-
DELETE /v1/{project_id}/scaling-policy	workspace:scalingPolicy:delete	-
GET /v1/{project_id}/scaling-policy	workspace:scalingPolicy:list	-
PUT /v1/{project_id}/scaling-policy	workspace:scalingPolicy:create	-
GET /v1/{project_id}/schedule-task/{task_id}/execute-history	workspace:scheduledTasks:list	-
POST /v1/{project_id}/schedule-	workspace:scheduledTa	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
task	sks:create	
GET /v1/{project_id}/schedule-task/{execute_history_id}/execute-detail	workspace:scheduledTasks:getRecord	-
DELETE /v1/{project_id}/schedule-task/{task_id}	workspace:scheduledTasks:delete	-
POST /v1/{project_id}/schedule-task/future-executions	workspace:scheduledTasks:get	-
PATCH /v1/{project_id}/schedule-task/{task_id}	workspace:scheduledTasks:update	-
GET /v1/{project_id}/schedule-task/{task_id}/execute-history	workspace:scheduledTasks:listRecords	-
POST /v1/{project_id}/schedule-task/actions/batch-delete	workspace:scheduledTasks:batchDelete	-
POST /v1/{project_id}/session/app-connection	workspace:session:listAppConnection	-
POST /v1/{project_id}/session/logoff	workspace:session:logoffUserSession	-
POST /v1/{project_id}/session/user-connection	workspace:session:listUserConnection	-
GET /v1/{project_id}/session/user-session-info	workspace:session:listSessionByUserName	-
PUT /v1/{project_id}/storages-policy/actions/create-statements	workspace:storagePolicy:create	-
GET /v1/{project_id}/storages-policy/actions/list-statements	workspace:storagePolicy:list	-
GET /v1/{project_id}/users	workspace:users:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
GET /v1/persistent-storages/actions/list-sfs-storages	workspace:storage:listSfs3Storage	• obs:bucket:ListBucket • obs:bucket:GetBucketStorage • obs:bucket:ListAllMyBuckets
GET /v1/{project_id}/product	workspace:baseResource:list	ecs:availabilityZones:list
POST /v1/{project_id}/bundles/batch-query-config-info	workspace:tenants:listConfigInfo	-
GET /v1/{project_id}/product	workspace:baseResource:list	-
GET /v1/{project_id}/volume-type	workspace:baseResource:list	-
POST /v1/{project_id}/tenant/action/active	workspace:tenants:active	-
GET /v1/{project_id}/tenant/profile	workspace:tenants:listTenantProfile	-
GET /v1/{project_id}/volume-type	workspace:baseResource:list	-
GET /v1/{project_id}/app-servers/server-metric-data/{server_id}	workspace:server:listServerMetricData	-
GET /v1/{project_id}/session/list-sessions	workspace:session:listSessions	-
PATCH /v1/{project_id}/app-warehouse/apps/{id}	workspace:appWarehouse:updateApp	-
POST /v1/{project_id}/app-servers/actions/batch-change-image	workspace:server:batchChangeImage	• ims:images:list • vpc:ports:get • vpc:subnets:get
POST /v1/{project_id}/app-servers/actions/batch-reinstall	workspace:server:batchReinstall	• ims:images:list • vpc:ports:get • vpc:subnets:get
GET /v2/{project_id}/auth-	workspace:authConfigs:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
config/method-config		
PUT /v2/{project_id}/auth-config/method-config	workspace:authConfigs:update	-
GET /v2/{project_id}/assist-auth-config/method-config	workspace:assistAuthConfigs:get	-
PUT /v2/{project_id}/assist-auth-config/method-config	workspace:assistAuthConfigs:update	-
POST /v2/{project_id}/workspace-jobs/{job_id}/actions	workspace:jobs:retry	-
GET /v2/{project_id}/quotas	workspace:quotas:get	-
GET /v2/{project_id}/tenants/roles	workspace:tenants:getRoles	-
GET /v2/{project_id}/tenant-configs	workspace:tenants:ListConfig	-
PUT /v2/{project_id}/tenant-configs	workspace:tenants:updateConfig	-
GET /v2/{project_id}/nat-mapping-configs	workspace:natMappings:getConfig	-
PUT /v2/{project_id}/nat-mapping-configs	workspace:natMappings:updateConfig	-
GET /v2/{project_id}/workspaces	workspace:tenants:get	• vpc:vpcs:get • vpc:subnets:get • vpc:securityGroups:get
POST /v2/{project_id}/workspaces	workspace:tenants:open	• eip:bandwidths:create • eip:publicIps:create • elb:healthmonitors:create • elb:healthmonitors:show • elb:listeners:create • elb:listeners:update • elb:listeners:show • elb:listeners:list

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
		• elb:loadbalancers:create • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:list • elb:members:update • elb:pools:create • elb:pools:update • elb:pools:show • vpc:ports:create • vpc:ports:delete • vpc:securityGroupRules:create • vpc:securityGroupRules:delete • vpc:securityGroupRules:get • vpc:securityGroups:create • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:get
DELETE /v2/{project_id}/workspaces	workspace:tenants:delete	• elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:delete • elb:listeners:show • elb:loadbalancers:delete • elb:loadbalancers:show • elb:members:delete • elb:members:list • elb:pools:delete • elb:pools:show • vpc:ports:delete • vpc:securityGroups:delete • vpcep:endpoints:delete • vpcep:endpoints:get • eip:publicIps:disassociateInstance • eip:bandwidths:delete • eip:publicIps:delete
PUT /v2/{project_id}/workspac	workspace:tenants:update	• eip:bandwidths:create

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
es		• eip:bandwidths:delete • eip:publicIps:create • eip:publicIps:delete • eip:publicIps:disassociateInstance • elb:healthmonitors:create • elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:create • elb:listeners:delete • elb:listeners:update • elb:listeners:show • elb:loadbalancers:create • elb:loadbalancers:delete • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:delete • elb:members:list • elb:members:update • elb:pools:create • elb:pools:delete • elb:pools:update • elb:pools:show • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:delete • vpcep:endpoints:get
GET /v2/{project_id}/workspaces/lock-status	workspace:tenants:getLockStatus	-
PUT /v2/{project_id}/workspaces/lock-status	workspace:tenants:unlock	-
POST /v2/{project_id}/agencies	workspace:agencies:create	• iam:agencies:listV5 • iam:agencies:getV5 • iam:agencies:createServiceLinkedAgencyV5

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
		• iam:roles:getRole • iam:roles:listRoles • iam:agencies:getAgency • iam:agencies:listAgencies • iam:agencies:createAgency • iam:permissions:listRolesForAgencyOnProject • iam:permissions:grantRoleToAgencyOnProject
GET /v2/{project_id}/agencies	workspace:agencies:get	• iam:agencies:listV5 • iam:agencies:getV5 • iam:agencies:getAgency • iam:agencies:listAgencies • iam:permissions:listRolesForAgencyOnProject
POST /v3/{project_id}/desktops/{desktop_id}/ai-accelerate-job	workspace:desktops:commitAiAccelerateJob	-
POST /v2/{project_id}/desktops/{desktop_id}/ai-accelerate-job	workspace:desktops:createAiAccelerateJob	-
GET /v2/{project_id}/ai-accelerate-job/{job_id}	workspace:desktops:getAiAccelerateJob	-
POST /v2/{project_id}/sysprep	workspace:desktops:getSysPrepInfo	-
POST /v2/{project_id}/verification/batch-change-image	workspace:desktops:checkBatchChangeImage	ims:images:list
GET /v2/{project_id}/desktop-name-policies	workspace:tenants:listDesktopNamePolicies	-
POST /v2/{project_id}/desktop-name-policies	workspace:tenants:createDesktopNamePolicy	-
PUT /v2/{project_id}/desktop-name-policies/{policy_id}	workspace:tenants:updateDesktopNamePolicy	-
POST /v2/{project_id}/desktop-	workspace:tenants:batchDeleteDesktopNameP	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
name-policies/batch-delete	olicies	
POST /v2/{project_id}/desktop-pools	workspace:desktopPools:create	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
GET /v2/{project_id}/desktop-pools	workspace:desktopPools:list	ims:images:list
PUT /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:update	-
DELETE /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:delete	-
GET /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:get	ims:images:list
POST /v2/{project_id}/desktop-pools/{pool_id}/expand	workspace:desktopPools:expand	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
		• vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
POST /v2/{project_id}/desktop-pools/{pool_id}/resize	workspace:desktopPools:resize	• vpc:subnets:get • ims:images:list
POST /v2/{project_id}/desktop-pools/{pool_id}/rebuild	workspace:desktopPools:rebuild	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-add	workspace:desktopPools:batchAddVolumes	-
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-delete	workspace:desktopPools:batchDeleteVolumes	-
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-expand	workspace:desktopPools:batchExpandVolumes	-
POST /v2/{project_id}/desktop-pools/{pool_id}/action	workspace:desktopPools:operate	-
GET /v2/{project_id}/desktop-pools/{pool_id}/users	workspace:desktopPools:listUsers	-
POST /v2/{project_id}/desktop-pools/{pool_id}/users	workspace:desktopPools:authorizeUsers	ims:images:list
GET /v2/{project_id}/desktop-pools/{pool_id}/desktops	workspace:desktopPools:listDesktops	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/desktop-pools/script-execution-tasks/detail	workspace:desktopPools:listScriptTasks	-
POST /v2/{project_id}/desktop-pools/{pool_id}/script-executions	workspace:desktopPools:executeScripts	-
POST /v2/{project_id}/desktop-pools/{pool_id}/notifications	workspace:desktopPools:sendNotifications	-
GET /v3/{project_id}/desktops/export	workspace:desktops:export	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
POST /v2/{project_id}/desktops	workspace:desktops:create	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • eip:publicIps:get • eip:publicIps:list • eip:publicIps:create • eip:publicIps:associateInstance • eip:publicIps:delete • eip:publicIps:createTags • vpc:quotas:list • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
GET	workspace:desktops:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
/v2/{project_id}/desktops		
PUT /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:update	-
DELETE /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:delete	• vpc:ports:get • vpc:ports:delete
GET /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:get	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
POST /v2/{project_id}/desktops/batch-delete	workspace:desktops:batchDelete	• vpc:ports:get • vpc:ports:delete
POST /v2/{project_id}/desktops/logoff	workspace:desktops:logoff	-
GET /v2/{project_id}/desktops/detail	workspace:desktops:listDetail	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
POST /v2/{project_id}/desktops/action	workspace:desktops:operate	-
POST /v2/{project_id}/desktops/resize	workspace:desktops:resize	• vpc:subnets:get • ims:images:list
GET /v2/{project_id}/connections/status	workspace:desktops:getConnectStatus	-
GET /v2/{project_id}/desktops/status	workspace:desktops:ListStatus	-
POST /v2/{project_id}/desktops/rebuild	workspace:desktops:rebuild	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
		• ims:images:deleteMember • ims:images:addMember
GET /v2/{project_id}/desktops/{desktop_id}/actions	workspace:desktops:getActions	-
GET /v2/{project_id}/desktops/{desktop_id}/remote-consoles	workspace:desktops:createConsole	-
PUT /v2/{project_id}/desktops/sids	workspace:desktops:updateSids	-
POST /v2/{project_id}/desktops/{desktop_id}/rejoin-domain	workspace:desktops:rejoinDomain	-
POST /v2/{project_id}/desktops/desktop-to-image	workspace:desktops:createImage	• ims:quotas:get • ims:images:get • ims:images:list • ims:images:setTags • ims:images:setOrDeleteTags • ims:images:updateMemberStatus • ims:images:copyInRegion • ims:serverImages:create
POST /v2/{project_id}/desktops/batch-detach	workspace:desktops:batchDetach	vpc:ports:get
POST /v2/{project_id}/desktops/detach	workspace:desktops:detach	vpc:ports:get
POST /v2/{project_id}/desktops/attach	workspace:desktops:attach	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
GET /v2/{project_id}/desktops/{desktop_id}/networks	workspace:desktops:getNetwork	• vpc:vpcs:get • vpc:networks:get

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
		• vpc:subnets:get • vpc:ports:get • vpc:securityGroups:get • eip:publicIps:list
PUT /v2/{project_id}/desktops/{desktop_id}/networks	workspace:desktops:changeNetwork	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:securityGroups:get • eip:publicIps:list • eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
GET /v2/{project_id}/exclusive-hosts/{host_id}/desktops	workspace:exclusiveHosts:listDesktops	-
GET /v2/{project_id}/all-desktops	workspace:desktops:listAll	-
GET /v2/{project_id}/desktop-associate/discover-vm/infos	workspace:desktopAssociate:listDiscoverVmInfo	-
POST /v2/{project_id}/desktop-associate/tasks	workspace:desktopAssociate:startTask	-
POST /v2/{project_id}/desktop-associate/discover-vm/switch	workspace:desktopAssociate:switchScanTask	-
GET /v2/{project_id}/desktop-associate/discover-vm/switch	workspace:desktopAssociate:getScanTaskSwitch	-
PUT /v2/{project_id}/desktops/maintenance-mode	workspace:desktops:setMaintenanceMode	-
POST /v2/{project_id}/desktops/	workspace:desktops:prepAttachUsers	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
pre-batch-attach		
POST /v2/{project_id}/desktops/batch-attach	workspace:desktops:batchAttachUsers	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
PUT /v2/{project_id}/desktops/change-username	workspace:desktops:changeUsername	-
POST /v2/{project_id}/desktops/notifications	workspace:desktops:sendNotifications	-
POST /v2/{project_id}/desktops/{desktop_id}/migrate	workspace:desktops:migrate	• vpc:networks:get • vpc:subnets:get • vpc:ports:create • vpc:ports:delete • vpc:ports:update • vpc:ports:get
GET /v2/{project_id}/desktops/agents	workspace:desktops:listAgents	-
POST /v2/{project_id}/desktops/agents	workspace:desktops:batchInstallAgents	-
GET /v2/{project_id}/desktops/{desktop_id}/tags	workspace:desktops:listTags	-
POST /v2/{project_id}/desktops/{desktop_id}/tags	workspace:desktops:tag	-
DELETE /v2/{project_id}/desktops/{desktop_id}/tags/{key}	workspace:desktops:untag	-
GET /v2/{project_id}/desktops/tags	workspace:desktops:listProjectTags	-
POST /v2/{project_id}/desktops/	workspace:desktops:operateTags	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
{desktop_id}/tags/action		
POST /v2/{project_id}/desktops/resource_instances/action	workspace:desktops:listByTags	-
POST /v2/{project_id}/desktops/batch-tags	workspace:desktops:tag	-
DELETE /v2/{project_id}/desktops/batch-tags	workspace:desktops:untag	-
POST /v2/{project_id}/exclusive-hosts	workspace:exclusiveHosts:create	• vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:subnets:get • vpc:vpcs:get
GET /v2/{project_id}/exclusive-hosts	workspace:exclusiveHosts:list	-
POST /v2/{project_id}/exclusive-hosts/check-limits	workspace:exclusiveHosts:check	-
GET /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:get	• nat:snatRules:list • eip:publicIps:list
PUT /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:update	-
DELETE /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:delete	-
GET /v2/{project_id}/market-images	workspace:mkp:listImages	ims:images:list
GET /v2/{project_id}/mkp/commodities/commodity-ids	workspace:mkp:listCommodityInfos	-
POST /v2/{project_id}/mkp/order	workspace:mkp:createOrder	-
POST /v2/{project_id}/mkp/prod	workspace:mkp:listList	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
uct-reserve	ProductReserve	
GET /v2/{project_id}/mkp/commodities	workspace:mkp:listCommodityDetails	-
GET /v2/{project_id}/mkp/commodities/{commodity_id}/relation-commodities	workspace:mkp:listRelationCommodityDetails	-
GET /v2/{project_id}/mkp/commodities/agreements	workspace:mkp:listCommodityAgreements	-
GET /v2/{project_id}/eips	workspace:networks:listEips	• eip:publicIps:list • eip:bandwidths:list
POST /v2/{project_id}/eips	workspace:networks:createEips	• vpc:quotas:list • eip:publicIps:create • eip:publicIps:associateInstance
POST /v2/{project_id}/eips/binding	workspace:networks:bindEips	• eip:publicIps:associateInstance • eip:publicIps:get
POST /v2/{project_id}/eips/unbinding	workspace:networks:unbindEips	• eip:publicIps:list • eip:publicIps:disassociateInstance
GET /v2/{project_id}/eips/quotas	workspace:networks:getEipQuota	vpc:quotas:list
GET /v2/{project_id}/nat-gateways	workspace:networks:ListNatGateways	• vpc:subnets:get • vpc:vpcs:get • nat:snatRules:list • nat:natGateways:list
POST /v2/{project_id}/periodic/subscribe/order	workspace:orders:create	• ims:images:list • vpc:vpcs:get • vpc:networks:get • vpc:subnets:get • vpc:ports:get • bss:order:update
POST /v2/{project_id}/periodic/{desktop_id}/change/order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/periodic/c	workspace:orders:change	• ims:images:list • bss:order:update

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
hange/batch-order		
POST /v2/{project_id}/periodic/inquiry/change-image	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/change/order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/desktop-pool/periodic/inquiry/add-volume	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/change-image	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/extend-volume	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/resize	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/periodic/inquiry/add-resources	workspace:orders:batchInquiry	ims:images:list
GET /v2/{project_id}/checkOrderLimits	workspace:quotas:check	-
POST /v2/{project_id}/render-desktops	workspace:renderDesktops:create	• ims:images:list • ims:images:share • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get
DELETE /v2/{project_id}/render-desktops	workspace:renderDesktops:delete	• vpc:ports:get • vpc:ports:delete

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/render-desktops	workspace:renderDesktops:list	-
POST /v2/{project_id}/render-desktops/action	workspace:renderDesktops:action	-
GET /v2/{project_id}/scheduled-tasks	workspace:scheduledTasks:list	-
POST /v2/{project_id}/scheduled-tasks	workspace:scheduledTasks:create	-
GET /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:get	-
PUT /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:update	-
DELETE /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:delete	-
POST /v2/{project_id}/scheduled-tasks/future-executions	workspace:scheduledTasks:getFuture	-
POST /v2/{project_id}/scheduled-tasks/batch-delete	workspace:scheduledTasks:batchDelete	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records	workspace:scheduledTasks:listRecords	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records/{record_id}	workspace:scheduledTasks:getRecord	-
POST /v2/{project_id}/scheduled-tasks/{task_id}/records/export	workspace:scheduledTasks:exportRecords	-
POST /v2/{project_id}/user/share-resources	workspace:users:subscribeSharer	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktop/sub-resources	workspace:desktops:addSubResources	-
POST /v2/{project_id}/desktop/delete-sub-resources	workspace:desktops:deleteSubResources	-
POST /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:createSnapshots	-
GET /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:getSnapshots	-
DELETE /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:deleteSnapshots	-
POST /v2/{project_id}/desktops/{desktop_id}/snapshots/restore	workspace:desktops:restoreBySnapshot	-
GET /v2/{project_id}/statistics	workspace:statistics:listDesktopStatus	-
GET /v2/{project_id}/desktops/statistics/unused	workspace:statistics:getUnused	-
POST /v2/{project_id}/desktops/statistics/used	workspace:statistics:getUsed	-
GET /v3/{project_id}/terminals/binding-desktops/template/export	workspace:bindingPolicies:export	-
GET /v2/{project_id}/terminals/binding-desktops/config	workspace:bindingPolicies:getConfig	-
POST /v2/{project_id}/terminals/binding-desktops/config	workspace:bindingPolicies:createConfig	-
GET /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:get	-
POST /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:add	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
PUT /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:update	-
POST /v2/{project_id}/terminals/binding-desktops/batch-delete	workspace:bindingPolicies:delete	-
POST /v2/{project_id}/desktops/{desktop_id}/volumes/batch-delete	workspace:volumes:delete	-
POST /v2/{project_id}/volumes	workspace:volumes:batchAdd	-
POST /v2/{project_id}/volumes/expand	workspace:volumes:batchExpand	-
GET /v2/{project_id}/hosts/types	workspace:wdh:getType	-
GET /v2/{project_id}/hosts	workspace:wdh:get	-
GET /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:getRemoteAssistance	-
POST /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:createRemoteAssistance	-
DELETE /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:cancelRemoteAssistance	-
POST /v2/{project_id}/desktops/{desktop_id}/volumes	workspace:volumes:add	-
POST /v2/{project_id}/desktops/{desktop_id}/volumes/{volume_id}/expand	workspace:volumes:expand	-
GET /v2/{project_id}/dss-pools/detail	workspace:volumes:listDssPoolsDetail	dss:pools:list

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/common/timezones	workspace:common:listTimezones	-
GET /v3/{project_id}/desktops/connections/export	workspace:connections:securityExport	-
GET /v2/{project_id}/images	workspace:images:list	ims:images:list
POST /v2/{project_id}/policy-groups/import	workspace:policyGroups:import	-
POST /v2/{project_id}/access-policy	workspace:accessPolicies:create	-
GET /v2/{project_id}/access-policy	workspace:accessPolicies:get	-
DELETE /v2/{project_id}/access-policy	workspace:accessPolicies:delete	-
GET /v2/{project_id}/access-policy/{access_policy_id}/objects	workspace:accessPolicies:getTarget	-
PUT /v2/{project_id}/access-policy/{access_policy_id}/objects	workspace:accessPolicies:updateTarget	-
GET /v2/{project_id}/products	workspace:products:listDesktopProducts	ecs:cloudServerFlavors:get
GET /v2/{project_id}/products/sharer	workspace:products:listSharerProducts	-
GET /v2/{project_id}/products/adninternet	workspace:products:listInternetProducts	-
GET /v2/{project_id}/availability-zones	workspace:availabilityZones:list	-
GET /v2/{project_id}/groups/export	workspace:userGroups:export	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
POST /v3/{project_id}/users/export	workspace:users:export	-
POST /v2/{project_id}/users/import	workspace:users:import	-
GET /v3/{project_id}/groups/{group_id}/users/export	workspace:userGroups:exportUsers	-
GET /v2/{project_id}/groups/{group_id}/users/export	workspace:userGroups:exportUsers	-
POST /v2/{project_id}/users/{user_id}/actions	workspace:users:operate	-
GET /v2/{project_id}/users/{user_id}/random-password	workspace:users:randomPassword	-
DELETE /v2/{project_id}/users/{user_id}/otp-devices	workspace:users:deleteOtps	-
POST /v2/{project_id}/users/{user_id}/resend-email	workspace:users:resendEmail	-
GET /v2/{project_id}/connections/desktops	workspace:connections:securityList	-
GET /v2/{project_id}/connections/desktops/export	workspace:connections:securityExport	-
GET /v2/{project_id}/connections/online-users	workspace:connections:listOnlineUsers	-
GET /v2/{project_id}/desktops/connections	workspace:connections:securityList	-
GET /v2/{project_id}/desktops/connections/export	workspace:connections:securityExport	-
GET /v2/{project_id}/desktops/online-users	workspace:connections:listOnlineUsers	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/groups	workspace:userGroups:list	-
POST /v2/{project_id}/groups	workspace:userGroups:create	-
POST /v2/{project_id}/groups/batch-delete	workspace:userGroups:batchDelete	-
DELETE /v2/{project_id}/groups/{group_id}	workspace:userGroups:delete	-
PUT /v2/{project_id}/groups/{group_id}	workspace:userGroups:update	-
POST /v2/{project_id}/groups/{group_id}/actions	workspace:userGroups:operate	-
GET /v2/{project_id}/groups/{group_id}/users	workspace:userGroups:getUsers	-
GET /v2/{project_id}/workspace-sub-jobs	workspace:jobs:listSubJobs	-
POST /v2/{project_id}/workspace-sub-jobs/batch-delete	workspace:jobs:deleteSubJobRecords	-
GET /v2/{project_id}/ous	workspace:ou:get	-
POST /v2/{project_id}/ous	workspace:ou:create	-
DELETE /v2/{project_id}/ous/{ou_id}	workspace:ou:delete	-
PUT /v2/{project_id}/ous/{ou_id}	workspace:ou:update	-
GET /v2/{project_id}/policy-groups	workspace:policyGroups:list	-
POST /v2/{project_id}/policy-groups	workspace:policyGroups:create	-
DELETE	workspace:policyGroup	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
/v2/{project_id}/policy-groups/{policy_group_id}	s:delete	
GET /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:get	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:update	-
POST /v2/{project_id}/policy-groups/export	workspace:policyGroups:export	-
GET /v2/{project_id}/policy-groups/{policy_group_id}/policies	workspace:policyGroups:listPolicies	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}/policies	workspace:policyGroups:updatePolicies	-
GET /v2/{project_id}/policy-groups/{policy_group_id}/targets	workspace:policyGroups:listTargets	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}/targets	workspace:policyGroups:updateTargets	-
GET /v2/{project_id}/policy-groups/detail	workspace:policyGroups:listDetail	-
GET /v2/{project_id}/policy-groups/original-policies	workspace:policyGroups:getOriginalPolicies	-
GET /v2/{project_id}/users	workspace:users:list	-
POST /v2/{project_id}/users	workspace:users:create	-
DELETE /v2/{project_id}/users/{user_id}	workspace:users:delete	-
GET /v2/{project_id}/users/{user_id}	workspace:users:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
PUT /v2/{project_id}/users/{user_id}	workspace:users:update	-
POST /v2/{project_id}/users/batch-delete	workspace:users:batchDelete	-
POST /v2/{project_id}/users/password	workspace:users:resetPassword	-
POST /v2/{project_id}/users/password-token	workspace:users:checkResetPasswordToken	-
GET /v2/{project_id}/users/desktop-users/template	workspace:users:getTemplate	-
POST /v2/{project_id}/users/exist	workspace:users:checkExist	-
GET /v2/{project_id}/users/{user_id}/otp-devices	workspace:users:listOtps	-
GET /v2/{project_id}/users/template/download	workspace:users:getImportTemplate	-
POST /v2/{project_id}/users/export	workspace:users:export	-
POST /v2/{project_id}/users/batch-create	workspace:users:batchCreate	-
GET /v2/{project_id}/volume/products	workspace:products:listVolumeProducts	-
GET /v2/{project_id}/export-tasks	workspace:tenants:listExportTasks	-
POST /v2/{project_id}/export-tasks/batch-delete	workspace:tenants:deleteExportTasks	-
GET /v2/{project_id}/export-tasks/{task_id}/download	workspace:tenants:exportData	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/alarms	workspace:statistics:listAlarm	ces:alarmHistory:list
GET /v2/{project_id}/statistics/alarms	workspace:statistics:getAlarm	ces:alarmHistory:list
GET /v2/{project_id}/statistics/growth-rate	workspace:statistics:getGrowthRate	-
GET /v2/{project_id}/statistics/metrics	workspace:statistics:getMetric	-
GET /v2/{project_id}/statistics/metrics/trend	workspace:statistics:getMetricTrend	-
PUT /v2/{project_id}/statistics/notify-rules/{rule_id}	workspace:statistics:updateNotificationRules	smn:topic:get
DELETE /v2/{project_id}/statistics/notify-rules/{rule_id}	workspace:statistics:deleteNotificationRules	-
POST /v2/{project_id}/statistics/notify-rules	workspace:statistics:createNotifyRules	smn:topic:get
GET /v2/{project_id}/statistics/notify-rules	workspace:statistics:listNotificationRules	-
GET /v2/{project_id}/statistics/notification-records	workspace:statistics:listNotificationRecords	-
GET /v2/{project_id}/statistics/metrics/desktops	workspace:statistics:listDesktopMetrics	-
GET /v2/{project_id}/statistics/metrics/desktops/export	workspace:statistics:exportDesktopMetrics	-
GET /v2/{project_id}/statistics/metrics/users	workspace:statistics:listUserMetrics	-
GET /v2/{project_id}/statistics/metrics/users/export	workspace:statistics:exportUserMetrics	-
GET /v3/{project_id}/statistics/	workspace:statistics:ex	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
metrics/desktops/export	portDesktopMetrics	
GET /v3/{project_id}/statistics/metrics/users/export	workspace:statistics:exportUserMetrics	-
POST /v1/{project_id}/app-center/buckets/actions/create-credential	workspace:appcenter:createBucketCredential	• obs:bucket:GetBucketAcl • obs:object:PutObject • obs:object:DeleteObject
POST /v1/{project_id}/app-center/buckets	workspace:appcenter:createAndAuthorizeBucket	• obs:bucket:HeadBucket • obs:bucket:PutBucketAcl • obs:bucket:PutReplicationConfiguration • obs:bucket:CreateBucket • obs:bucket:PutBucketCORS
GET /v1/{project_id}/app-center/apps	workspace:appcenter:listApps	-
POST /v1/{project_id}/app-center/apps	workspace:appcenter:createApp	-
PATCH /v1/{project_id}/app-center/apps/{app_id}	workspace:appcenter:updateApp	-
DELETE /v1/{project_id}/app-center/apps/{app_id}	workspace:appcenter:deleteApp	-
POST /v1/{project_id}/app-center/apps/{app_id}/actions/auto-install	workspace:appcenter:installApp	-
GET /v1/{project_id}/app-center/apps/{app_id}/authorizations	workspace:appcenter:listAppAuthorizations	-
POST /v1/{project_id}/app-center/apps/{app_id}/actions/assign-authorizations	workspace:appcenter:batchUpdateAppAuthorizations	-
POST /v1/{project_id}/app-center/apps/actions/batch-delete	workspace:appcenter:batchDeleteApps	-
POST	workspace:appcenter:ba	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
/v1/{project_id}/app-center/apps/actions/batch-disable	tchDisableApps	
POST /v1/{project_id}/app-center/apps/actions/batch-enable	workspace:appcenter:batchEnableApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-assign-authorization	workspace:appcenter:batchUpdateAppAuthorizations	-
POST /v1/{project_id}/app-center/apps/actions/batch-auto-install	workspace:appcenter:batchInstallApps	-
GET /v1/{project_id}/app-center/app-catalogs	workspace:appcenter:listAppCatalogs	-
GET /v1/{project_id}/app-center/jobs	workspace:appcenter:listJobs	-
POST /v1/{project_id}/app-center/jobs/actions/batch-delete	workspace:appcenter:batchDeleteJobs	-
POST /v1/{project_id}/app-center/jobs/actions/retry	workspace:appcenter:retryJobs	-
POST /v1/{project_id}/app-center/app-rules	workspace:appcenter:createAppRule	-
GET /v1/{project_id}/app-center/app-rules	workspace:appcenter:listAppRule	-
PATCH /v1/{project_id}/app-center/app-rules/{rule_id}	workspace:appcenter:updateAppRule	-
DELETE /v1/{project_id}/app-center/app-rules/{rule_id}	workspace:appcenter:deleteAppRule	-
POST /v1/{project_id}/app-center/app-rules/batch-delete	workspace:appcenter:batchDeleteAppRules	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/app-center/app-rules/actions/enable-rule-restriction	workspace:appcenter:enableRuleRestriction	-
POST /v1/{project_id}/app-center/app-rules/actions/disable-rule-restriction	workspace:appcenter:disableRuleRestriction	-
POST /v1/{project_id}/app-center/app-restricted-rules	workspace:appcenter:addRestrictedRule	-
GET /v1/{project_id}/app-center/app-restricted-rules	workspace:appcenter:listRestrictedRule	-
POST /v1/{project_id}/app-center/app-restricted-rules/actions/batch-delete	workspace:appcenter:deleteRestrictedRule	-
PATCH /v1/{project_id}/app-center/profiles	workspace:appcenter:updateTenantProfile	-
GET /v1/{project_id}/app-center/profiles	workspace:appcenter:listTenantProfiles	-
POST /v2/{project_id}/scripts	workspace:scripts:create	-
GET /v2/{project_id}/scripts	workspace:scripts:list	-
GET /v2/{project_id}/scripts/{script_id}	workspace:scripts:get	-
PUT /v2/{project_id}/scripts/{script_id}	workspace:scripts:put	-
DELETE /v2/{project_id}/scripts/{script_id}	workspace:scripts:delete	-
POST /v2/{project_id}/script-executions	workspace:scripts:execute	-
GET	workspace:scripts:getR	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
/v2/{project_id}/script-execution-records/{record_id}	ecordDetail	
GET /v2/{project_id}/script-execution-records	workspace:scripts:listRecords	-
GET /v2/{project_id}/script-execution-tasks	workspace:scripts:listTasks	-
POST /v2/{project_id}/script-executions/retry	workspace:scripts:retry	-
POST /v2/{project_id}/script-executions/stop	workspace:scripts:stop	-
POST /v2/{project_id}/script-execution-records/{record_id}/download	workspace:scripts:download	-
GET /v2/{project_id}/share-space/configuration	workspace:tenants:getShareSpaceConfig	-
PUT /v2/{project_id}/share-space/configuration	workspace:tenants:updateShareSpaceConfig	-
GET /v2/{project_id}/auth-config/status	workspace:authConfigs:getStatus	-
POST /v2/{project_id}/privacystatement	workspace:privacystatements:sign	-
GET /v2/{project_id}/quotas/detail	workspace:quotas:get	-
GET /v2/{project_id}/sites	workspace:sites:get	-
POST /v2/{project_id}/sites	workspace:sites:add	• eip:bandwidths:create • eip:publicIps:create • elb:healthmonitors:create • elb:healthmonitors:show • elb:listeners:create

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
		• elb:listeners:update • elb:listeners:show • elb:listeners:list • elb:loadbalancers:create • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:list • elb:members:update • elb:pools:create • elb:pools:update • elb:pools:show • vpc:ports:create • vpc:ports:delete • vpc:securityGroupRules:create • vpc:securityGroupRules:delete • vpc:securityGroupRules:get • vpc:securityGroups:create • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:get
DELETE /v2/{project_id}/sites/{site_id}	workspace:sites:delete	• elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:delete • elb:listeners:show • elb:loadbalancers:delete • elb:loadbalancers:show • elb:members:delete • elb:members:list • elb:pools:delete • elb:pools:show • vpc:ports:delete • vpc:securityGroups:delete • vpcep:endpoints:delete • vpcep:endpoints:get • eip:publicIps:disassociateInstance • eip:bandwidths:delete

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
		• eip:publicIps:delete
PUT /v2/{project_id}/sites/{site_id}/access-mode	workspace:sites:updateAccessMode	• eip:bandwidths:create • eip:bandwidths:delete • eip:publicIps:create • eip:publicIps:delete • eip:publicIps:disassociateInstance • elb:healthmonitors:create • elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:create • elb:listeners:delete • elb:listeners:update • elb:listeners:show • elb:loadbalancers:create • elb:loadbalancers:delete • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:delete • elb:members:list • elb:members:update • elb:pools:create • elb:pools:delete • elb:pools:update • elb:pools:show • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:delete • vpcep:endpoints:get
PUT /v2/{project_id}/sites/{site_id}/subnet-ids	workspace:sites:updateSubnets	• vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get
GET /v2/{project_id}/tenants/lock-status	workspace:tenants:getLockStatus	-
PUT /v2/{project_id}/tenants/lo	workspace:tenants:unlock	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
ck-status		
POST /v2/{project_id}/workspaces/enterprise-ids/check	workspace:tenants:checkEnterpriseIds	-
PUT /v2/{project_id}/workspaces/enterprise-id	workspace:tenants:updateEnterpriseId	-
POST /v2/{project_id}/bandwidths	workspace:bandwidth:create	-
GET /v2/{project_id}/bandwidths	workspace:bandwidth:list	-
POST /v2/{project_id}/bandwidths/{bandwidth_id}/update	workspace:bandwidth:update	-
DELETE /v2/{project_id}/bandwidths/{bandwidth_id}	workspace:bandwidth:delete	-
GET /v2/{project_id}/bandwidths/{bandwidth_id}/control-list	workspace:bandwidth:getControlConfig	-
PUT /v2/{project_id}/bandwidths/{bandwidth_id}/control-list	workspace:bandwidth:updateControlConfig	-
POST /v2/{project_id}/bandwidths/{bandwidth_id}/periodic/change/order	workspace:bandwidth:createChangeOrder	-
POST /v2/{project_id}/adns	workspace:bandwidth:create	-
GET /v2/{project_id}/adns	workspace:bandwidth:list	-
POST /v2/{project_id}/desktops-adn/batch-delete	workspace:bandwidth:delete	-
POST /v2/{project_id}/snapshots/batch-create	workspace:desktops:batchCreateSnapshots	-
POST /v2/{project_id}/snapshots/	workspace:desktops:batchDeleteSnapshots	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
batch-delete		
POST /v2/{project_id}/snapshots/batch-restore	workspace:desktops:batchRestoreSnapshots	-
GET /v2/{project_id}/snapshots	workspace:desktops:listSnapshots	-
POST /v2/{project_id}/verification/desktop-name	workspace:desktops:verifyDesktopName	-
GET /v2/{project_id}/subnets/{subnet_id}/available-ip	workspace:networks:getAvailableIp	-
GET /v2/{project_id}/ad/status	workspace:desktops:getAdStatus	-
GET /v2/{project_id}/ip-exist	workspace:networks:checkIpIfExist	-
POST /v2/{project_id}/desktops/check-images	workspace:images:checkIfExist	ims:images:list
GET /v2/{project_id}/hosts/{host_id}/servers	workspace:wdh:listDesktops	-
PUT /v2/{project_id}/hosts	workspace:wdh:update	-
GET /v2/{project_id}/terminals/binding-desktops/template	workspace:bindingPolicies:getTemplate	-
POST /v2/{project_id}/terminals/binding-desktops/template/import	workspace:bindingPolicies:import	-
GET /v2/{project_id}/terminals/binding-desktops/template/export	workspace:bindingPolicies:export	-
GET /v2/{project_id}/desktops/statistics/run-state	workspace:statistics:getRunState	-
GET /v2/{project_id}/desktops/statistics/login-state	workspace:statistics:getLoginState	-
GET	workspace:networks:ge	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
/v2/{project_id}/subnets/using-subnets	tUsingSubnets	
GET /v2/{project_id}/ports	workspace:networks:listPorts	-
GET /v2/{project_id}/render-desktops/{desktop_id}/remote-consoles	workspace:renderDesktops:createConsole	-
PUT /v2/{project_id}/render-desktops/resize	workspace:renderDesktops:resize	-
POST /v2/{project_id}/exclusive-hosts/{host_id}/resize-lites	workspace:exclusiveHosts:resizeLites	-
GET /services/v2/{project_id}/desktops/{desktop_id}	workspace:desktops:get	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktop-monitor/{desktop_id}	workspace:desktops:getMonitor	ces:metricData:get
GET /v2/{project_id}/desktops/export	workspace:desktops:export	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktops/{desktop_id}/detach-info	workspace:desktops:listDetachInfo	-
GET /v2/{project_id}/desktops/{desktop_id}/sysprep	workspace:desktops:getSysprepVersion	-
POST /v2/{project_id}/internet	workspace:networks:createNat	• vpc:ports:delete • vpc:ports:get • vpc:networks:get • eip:publicIps:create • eip:publicIps:update • eip:publicIps:delete • nat:snatRules:list • nat:snatRules:create

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
		• nat:natGateways:list • nat:natGateways:create
GET /v2/{project_id}/internet	workspace:networks:listNats	• vpc:subnets:get • vpc:vpcs:get • nat:snatRules:list • nat:natGateways:list
POST /v2/{project_id}/quotas/check	workspace:quotas:check	-
GET /v2/{project_id}/subnets	workspace:networks:listSubnets	• vpc:subnets:list • vpc:subnets:get
GET /v2/{project_id}/vpcs	workspace:networks:listVpcs	vpc:vpcs:list
POST /v2/{project_id}/policy-groups/policy-template	workspace:policyGroups:createTemplate	-
GET /v1/{project_id}/policy-templates	workspace:policyGroups:listTemplate	-
PUT /v2/{project_id}/policy-groups/policy-template/{policy_group_id}	workspace:policyGroups:updateTemplate	-
GET /v2/{project_id}/security-groups	workspace:networks:listSecurityGroups	-
GET /v2/{project_id}/availability-zones/summary	workspace:availabilityZones:getSummary	-
GET /v2/{project_id}/availability-zones/detail	workspace:availabilityZones:get	-
POST /v2/{project_id}/users/desktop-users/action/import	workspace:users:importUser	-
POST /v2/{project_id}/users/template-upload	workspace:users:uploadTemplate	-
PUT /v2/{project_id}/access-policy/{access_policy_id}	workspace:accessPolicies:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktops/{desktop_id}/verify-source	workspace:desktops:verifySource	-
GET /v2/{project_id}/desktops/networks	workspace:desktops:listDesktopNetworks	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:securityGroups:get • eip:publicIps:list
POST /v2/{project_id}/desktops/networks/batch-change	workspace:desktops:batchChangeNetwork	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:securityGroups:get • eip:publicIps:list • eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
GET /v2/{project_id}/workspace-jobs/{job_id}	workspace:jobs:get	-
POST /v2/{project_id}/ip/import	workspace:accessPolicies:importIp	-
GET /v2/{project_id}/ip/template/download	workspace:accessPolicies:getIpImportTemplate	-
GET /v2/{project_id}/wks-edge-sites	workspace:sites:listEdgeSites	• ies:edgeSite:list • ies:edgeSite:getMetricData
POST /v2/{project_id}/check-edge-site-resources	workspace:sites:checkEdgeSiteResources	• ies:edgeSite:list • ies:edgeSite:getMetricData
GET /v2/{project_id}/ad-ous	workspace:ou:listAdOus	-
GET /v2/{project_id}/ou-users	workspace:ou:listOuUsers	-
POST /v2/{project_id}/ou-	workspace:ou:importUs	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
users/import	ersByOU	
GET /v1/{project_id}/app-groups	workspace:appGroup:list	-
POST /v1/{project_id}/app-groups	workspace:appGroup:create	-
DELETE /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:delete	-
GET /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:get	-
PATCH /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:update	-
GET /v1/{project_id}/app-groups/{app_group_id}/apps	workspace:app:listPublishedApp	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps	workspace:app:publish	-
GET /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}	workspace:app:get	-
PATCH /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}	workspace:app:update	-
DELETE /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}/icon	workspace:app:deleteIcon	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}/icon	workspace:app:uploadIcon	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/check	workspace:app:check	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/disable	workspace:app:batchDisable	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/enable	workspace:app:batchEnable	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/batch-unpublish	workspace:app:unpublish	-
GET /v1/{project_id}/app-groups/{app_group_id}/publishable-app	workspace:appGroup:listPublishableApp	-
POST /v1/{project_id}/app-groups/actions/batch-delete-authorization	workspace:appGroup:batchDeleteAuthorization	-
POST /v1/{project_id}/app-groups/actions/disassociate-app-group	workspace:appGroup:disassociate	-
GET /v1/{project_id}/app-groups/actions/list-authorizations	workspace:appGroup:listAuthorization	-
POST /v1/{project_id}/app-groups/authorizations	workspace:appGroup:addAuthorization	-
POST /v1/{project_id}/app-groups/batch-delete	workspace:appGroup:batchDelete	-
POST /v1/{project_id}/app-groups/rules/validate	workspace:appGroup:check	-
GET /v1/{project_id}/app-server-groups	workspace:serverGroup:list	-
POST /v1/{project_id}/app-server-groups	workspace:serverGroup:create	• ims:images:list • vpc:ports:get • vpc:subnets:get

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
DELETE /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:delete	-
GET /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:get	-
PATCH /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:update	ims:images:list
GET /v1/{project_id}/app-server-groups/{server_group_id}/state	workspace:serverGroup:getServerState	-
GET /v1/{project_id}/app-server-groups/actions/list	workspace:serverGroup:listDetail	-
GET /v1/{project_id}/app-server-groups/resources/restrict	workspace:serverGroup:getRestrict	-
POST /v1/{project_id}/app-server-groups/rules/validate	workspace:serverGroup:validate	-
POST /v1/{project_id}/server-group/{server_group_id}/tags/create	workspace:serverGroup:tagResource	-
DELETE /v1/{project_id}/server-group/{server_group_id}/tags/delete	workspace:serverGroup:unTagResource	-
GET /v1/{project_id}/server-group/{server_group_id}/tags	workspace:serverGroup:listTagsForResource	-
GET /v1/{project_id}/server-group/tags	workspace:serverGroup:listTags	-
POST /v1/{project_id}/server-	workspace:serverGroup:batchCreateTags	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
group/tags/batch-create		
DELETE /v1/{project_id}/server-group/tags/batch-delete	workspace:serverGroup:batchDeleteTags	-
GET /v1/{project_id}/app-servers	workspace:server:list	-
DELETE /v1/{project_id}/app-servers/{server_id}	workspace:server:delete	• iam:roles:listRoles • vpc:ports:delete • vpc:ports:get
GET /v1/{project_id}/app-servers/{server_id}	workspace:server:get	-
PATCH /v1/{project_id}/app-servers/{server_id}	workspace:server:update	-
POST /v1/{project_id}/app-servers/{server_id}/actions/change-image	workspace:server:changeImage	• ims:images:list • vpc:ports:get • vpc:subnets:get
POST /v1/{project_id}/app-servers/{server_id}/actions/reinstall	workspace:server:reinstall	• ims:images:list • vpc:ports:get • vpc:subnets:get
GET /v1/{project_id}/app-servers/{server_id}/actions/vnc	workspace:server:getVncUrl	-
GET /v1/{project_id}/app-servers/access-agent/upgrade-record	workspace:accessAgent:list	-
PATCH /v1/{project_id}/app-servers/access-agent/actions/upgrade	workspace:accessAgent:batchUpgrade	-
GET /v1/{project_id}/app-servers/access-agent/latest-version	workspace:accessAgent:listLatestVersion	-
GET /v1/{project_id}/app-servers/access-agent/list	workspace:server:listAccessAgentDetails	-
GET	workspace:accessAgent	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
/v1/{project_id}/app-servers/access-agent/upgrade-flag	:getUpgradeFlag	
PATCH /v1/{project_id}/app-servers/access-agent/upgrade-flag	workspace:accessAgent:updateUpgradeFlag	-
GET /v1/{project_id}/app-servers/access-agent/upgrade-record	workspace:accessAgent:listUpgradeRecords	-
POST /v1/{project_id}/app-servers/actions/batch-delete	workspace:server:batchDelete	• iam:roles:listRoles • vpc:ports:delete • vpc:ports:get
PATCH /v1/{project_id}/app-servers/actions/batch-maint	workspace:server:batchChangeMaintainMode	-
PATCH /v1/{project_id}/app-servers/actions/batch-reboot	workspace:server:batchReboot	-
PATCH /v1/{project_id}/app-servers/actions/batch-rejoin-domain	workspace:server:batchRejoinDomain	-
PATCH /v1/{project_id}/app-servers/actions/batch-start	workspace:server:batchStart	-
PATCH /v1/{project_id}/app-servers/actions/batch-stop	workspace:server:batchStop	-
PATCH /v1/{project_id}/app-servers/actions/batch-update-tsvi	workspace:server:batchUpdateTsvi	• vpc:subnets:get • vpc:ports:update
POST /v1/{project_id}/app-servers/actions/create	workspace:server:create	• ims:images:list • ims:images:updateMemberStatus • ims:images:share • ims:images:get • vpc:securityGroups:get • vpc:securityGroupRules:get • vpc:networks:get

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
		• vpc:subnets:get • vpc:ports:create • vpc:ports:get • vpc:ports:delete • vpc:vpcs:get • dss:pools:list
PATCH /v1/{project_id}/app-servers/hosts/batch-migrate	workspace:server:batchMigrateHosts	-
GET /v1/{project_id}/app-servers/metric-data/{server_id}	workspace:server:getMetricData	-
GET /v1/{project_id}/app-server-sub-jobs	workspace:jobs:listSubJobs	-
POST /v1/{project_id}/app-server-sub-jobs/actions/batch-delete	workspace:jobs:batchDeleteSubJobs	-
GET /v1/{project_id}/app-server-sub-jobs/actions/count	workspace:jobs:countSubJobs	-
POST /v1/{project_id}/app-warehouse/action/authorize	workspace:appWarehouse:authorizeObs	• obs:bucket:GetBucketAcl • obs:object:PutObject • obs:object:DeleteObject
POST /v1/{project_id}/app-warehouse/actions/batch-delete	workspace:appWarehouse:batchDeleteApp	• obs:bucket:HeadBucket • obs:object:DeleteObject
GET /v1/{project_id}/app-warehouse/apps	workspace:appWarehouse:ListWarehouseApps	-
POST /v1/{project_id}/app-warehouse/apps	workspace:appWarehouse:createApp	-
DELETE /v1/{project_id}/app-warehouse/apps/{id}	workspace:appWarehouse:deleteApp	• obs:bucket:HeadBucket • obs:object:DeleteObject
POST /v1/{project_id}/app-warehouse/apps/icon	workspace:appWarehouse:uploadAppIcon	obs:object:PutObject

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/app-warehouse/bucket-and-acl/create	workspace:appWarehouse:createBucketOrAcl	• obs:bucket:GetBucketAcl • obs:bucket:HeadBucket • obs:bucket:PutBucketAcl • obs:bucket:PutReplicationConfiguration • obs:bucket:CreateBucket • obs:bucket:PutBucketCORS
GET /v1/{project_id}/check/quota	workspace:quotas:get	-
GET /v1/{project_id}/image-server-jobs	workspace:images:listImageJobs	-
GET /v1/{project_id}/image-server-jobs/{job_id}	workspace:images:getImageJob	-
GET /v1/{project_id}/image-servers	workspace:imageServer:list	-
POST /v1/{project_id}/image-servers	workspace:imageServer:create	• ims:images:list • vpc:ports:get • vpc:subnets:get
GET /v1/{project_id}/image-servers/{server_id}	workspace:imageServer:get	-
PATCH /v1/{project_id}/image-servers/{server_id}	workspace:imageServer:update	-
POST /v1/{project_id}/image-servers/{server_id}/actions/attach-app	workspace:imageServer:attachApp	-
GET /v1/{project_id}/image-servers/{server_id}/actions/latest-attached-app	workspace:imageServer:listLatestAttachedApp	-
POST /v1/{project_id}/image-servers/{server_id}/actions/recreate-image	workspace:imageServer:recreate	• vpc:ports:get • vpc:subnets:get • ims:quotas:get • ims:images:get • ims:images:list

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
		• ims:images:setTags • ims:images:setOrDeleteTags • ims:images:updateMemberStatus • ims:images:copyInRegion • ims:serverImages:create
PATCH /v1/{project_id}/image-servers/actions/batch-delete	workspace:imageServer:batchDelete	-
GET /v1/{project_id}/image-server-sub-jobs	workspace:imageServer:listImageSubJobs	-
PATCH /v1/{project_id}/image-server-sub-jobs/actions/batch-delete	workspace:imageServer:batchDeleteImageSubJobs	-
GET /v1/{project_id}/image-server-sub-jobs/actions/count	workspace:imageServer:countImageSubJobs	-
GET /v2/{project_id}/job/{job_id}	workspace:jobs:get	-
GET /v1/{project_id}/mails	workspace:appGroup:listMailRecord	-
POST /v1/{project_id}/mails/actions/send	workspace:appGroup:resendMail	-
POST /v1/{project_id}/mails/actions/send	workspace:appGroup:resendMail	-
GET /v1/{project_id}/persistent-storages	workspace:storage:listPersistentStorage	-
POST /v1/{project_id}/persistent-storages	workspace:storage:createPersistentStorage	• obs:bucket:HeadBucket • obs:bucket:PutBucketPolicy • obs:bucket:PutBucketAcl • obs:bucket:PutBucketCORS
DELETE /v1/{project_id}/persistent-storages/{storage_id}	workspace:storage:deletePersistentStorage	• obs:object:GetObject • obs:object:DeleteObject

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/assign-folder	workspace:storage:updateUserFolderAssignment	-
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/assign-share-folder	workspace:storage:updateShareFolderAssignment	-
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/create-share-folder	workspace:storage:createShareFolder	• obs:object:GetObject • obs:object:PutObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/delete-storage-claim	workspace:storage:deleteStorageClaim	obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/delete-user-attachment	workspace:storage:deleteUserStorageAttachment	obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/actions/batch-delete	workspace:storage:batchDeletePersistentStorage	-
GET /v1/{project_id}/persistent-storages/actions/list-attachments	workspace:storage:listStorageAssignment	-
GET /v1/{project_id}/persistent-storages/actions/list-share-folders	workspace:storage:listShareFolder	-
GET /v1/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:get	-
GET /v2/{project_id}/policy-groups/{policy_group_id}/policies	workspace:policyGroups:listPolicies	-
GET /v1/{project_id}/policy-groups/{policy_group_id}/target	workspace:policyGroups:listTargets	-
GET /v2/{project_id}/policy-	workspace:policyGroups:listDetail	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
groups/detail		
GET /v1/{project_id}/policy-templates	workspace:policyGroups:listTemplate	-
DELETE /v1/{project_id}/policy-templates/{policy_template_id}	workspace:policyGroups:deleteTemplate	-
PATCH /v1/{project_id}/policy-templates/{policy_template_id}	workspace:policyGroups:updateTemplate	-
GET /v1/{project_id}/privacy-statement	workspace:privacystatements:get	-
DELETE /v1/{project_id}/scaling-policy	workspace:scalingPolicy:delete	-
GET /v1/{project_id}/scaling-policy	workspace:scalingPolicy:list	-
PUT /v1/{project_id}/scaling-policy	workspace:scalingPolicy:create	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records	workspace:scheduledTasks:list	-
POST /v2/{project_id}/scheduled-tasks	workspace:scheduledTasks:create	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records/{record_id}	workspace:scheduledTasks:getRecord	-
DELETE /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:delete	-
POST /v2/{project_id}/scheduled-tasks/future-executions	workspace:scheduledTasks:get	-
PUT /v2/{project_id}/scheduled	workspace:scheduledTasks:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
-tasks/{task_id}		
GET /v2/{project_id}/scheduled-tasks/{task_id}/records	workspace:scheduledTasks:listRecords	-
POST /v2/{project_id}/scheduled-tasks/batch-delete	workspace:scheduledTasks:batchDelete	-
POST /v1/{project_id}/session/app-connection	workspace:session:listAppConnection	-
POST /v1/{project_id}/session/logoff	workspace:session:logoffUserSession	-
POST /v1/{project_id}/session/user-connection	workspace:session:listUserConnection	-
GET /v1/{project_id}/session/user-session-info	workspace:session:listSessionByUserName	-
PUT /v1/{project_id}/storages-policy/actions/create-statements	workspace:storagePolicy:create	-
GET /v1/{project_id}/storages-policy/actions/list-statements	workspace:storagePolicy:list	-
GET /v2/{project_id}/users	workspace:users:list	-
GET /v1/persistent-storages/actions/list-sfs-storages	workspace:storage:listSfs3Storage	• obs:bucket:ListBucket • obs:bucket:GetBucketStorage • obs:bucket:ListAllMyBuckets
GET /v1/{project_id}/availability-zone	workspace:baseResource:list	ecs:availabilityZones:list
POST /v1/{project_id}/bundles/batch-query-config-info	workspace:tenants:listConfigInfo	-
GET /v1/{project_id}/product	workspace:baseResource:list	-
GET /v1/{project_id}/product	workspace:baseResource:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/tenant/action/active	workspace:tenants:active	-
GET /v1/{project_id}/tenant/profile	workspace:tenants:listTenantProfile	-
GET /v1/{project_id}/volume-type	workspace:baseResource:list	-
GET /v1/{project_id}/app-servers/server-metric-data/{server_id}	workspace:server:listServerMetricData	-
GET /v1/{project_id}/session/list-sessions	workspace:session:listSessions	-
PATCH /v1/{project_id}/app-warehouse/apps/{id}	workspace:appWarehouse:updateApp	-
POST /v1/{project_id}/app-servers/actions/batch-change-image	workspace:server:batchChangeImage	• ims:images:list • vpc:ports:get • vpc:subnets:get
POST /v1/{project_id}/app-servers/actions/batch-reinstall	workspace:server:batchReinstall	• ims:images:list • vpc:ports:get • vpc:subnets:get

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-223 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

云桌面定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-219 云桌面支持的资源类型

资源类型	描述	URN
desktop	桌面	workspace:<region>:<account-id>:desktop:<desktop-id>
desktopPool	桌面池	workspace:<region>:<account-

 版权所有 © 华为云计算技术有限公司

资源类型	描述	URN
		id>:desktopPool:<pool-id>
wdh	云办公主机	workspace:<region>:<account-id>:wdh:<wdh-id>
exclusiveHost	专享主机	workspace:<region>:<account-id>:exclusiveHost:<host-id>
user	用户	workspace:<region>:<account-id>:user:<user-id>
userGroup	用户组	workspace:<region>:<account-id>:userGroup:<group-id>
policyGroup	策略组	workspace:<region>:<account-id>:policyGroup:<policy-group-id>
script	脚本	workspace:<region>:<account-id>:script:<script-id>
scheduledTask	定时任务	workspace:<region>:<account-id>:scheduledTask:<task-id>
server	应用服务器	workspace:<region>:<account-id>:server:<server-id>
serverGroup	应用服务器组	workspace:<region>:<account-id>:serverGroup:<server-group-id>
app	应用	workspace:<region>:<account-id>:app:<app-id>
appGroup	应用组	workspace:<region>:<account-id>:appGroup:<app-group-id>
imageServer	应用镜像服务器	workspace:<region>:<account-id>:imageServer:<image-server-id>
storage	存储	workspace:<region>:<account-id>:storage:<storage-id>

条件（Condition）

条件键（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 workspace:）仅适用于对应服务的操作，详情请参见表 3-224。

 版权所有 © 华为云计算技术有限公司

  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

Workspace 定义了以下可以在身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化策略语句应用的条件。

表3-220 云桌面支持的服务级条件键

服务级条件键	类型	单值/多值	说明
workspace:AccessMode	string	多值	根据请求参数中指定的接入方式过滤访问，有效的条件值应为INTERNET、DEDICATED、BOTH。

3.12 视频

3.12.1 视频直播服务 Live

云服务在 IAM 预置了常用的权限，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

 版权所有 © 华为云计算技术有限公司

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 Live 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 Live 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 Live 的相关操作。

表3-221 Live 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
live:domain:createDomain	授予创建直播域名的权限。	Write	-	-	-
live:domain:getDomains	授予查询直播域名的权限。	Read	-	-	-
live:domain:deleteDomain	授予删除直播域名的权限。	Write	-	-	-
live:domain:updateDomain	授予修改直播域名的权限。	Write	-	-	-
live:domain:createDomainsMapping	授予域名映射的权限。	Write	-	-	-
live:domain:deleteDomainsMa	授予删除直播域名映射关系	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
pping	的权限。				
live:domain:updateStreamNotification	授予新增或覆盖直播推流通知配置的权限。	Write	-	-	-
live:domain:getStreamNotifications	授予查询直播推流通知配置的权限。	Read	-	-	-
live:domain:deleteStreamNotification	授予删除直播推流通知配置的权限。	Write	-	-	-
live:domain:createCDNConfig	授予创建直播域名配置项的权限。	Write	-	-	-
live:domain:updateCDNConfig	授予修改直播域名配置项的权限。	Write	-	-	-
live:domain:getCDNConfig	授予查询直播域名配置项的权限。	Read	-	-	-
live:domain:deleteCDNConfig	授予删除直播域名配置项的权限。	Write	-	-	-
live:domain:getIPAuthList	授予查询 IP 黑白名单的权限。	Read	-	-	-
live:domain:updateIPAuthList	授予修改 IP 黑白名单的权限。	Write	-	-	-
live:domain:getGeoBlockingList	授予获取直播业务地域限制列表的权限。	Read	-	-	-
live:domain:updateGeoBlocking	授予修改直播业务地域限制列表的权限。	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
live:domain:updateRefererChain	授予设置referer 防盗链黑白名单的权限。	Write	-	-	-
live:domain:deleteRefererChain	授予删除referer 防盗链黑白名单的权限。	Write	-	-	-
live:domain:getRefererChain	授予查询referer 防盗链黑白名单的权限。	Read	-	-	-
live:logs:listLog	授予获取直播播放日志下载链接的权限。	Read	-	-	-
live:domain:getCertificates	授予查询HTTPS 证书信息的权限。	Read	-	-	-
live:record:createRule	授予创建录制规则的权限。	Write	-	-	-
live:record:listRules	授予查询录制规则列表的权限。	Read	-	-	-
live:record:updateRule	授予修改录制规则的权限。	Write	-	-	-
live:record:deleteRule	授予删除录制规则的权限。	Write	-	-	-
live:record:getRule	授予查询录制规则配置的权限。	Read	-	-	-
live:record:listContents	授予查询录制完成的内容的权限。	Read	-	-	-
live:record:createCommand	授予提交录制控制命令的权	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
live:record:createCallback	授予创建录制回调配置的权限。	Write	-	-	-
live:record:listCallbacks	授予查询录制回调配置列表的权限。	Read	-	-	-
live:record:updateCallback	授予修改录制回调配置的权限。	Write	-	-	-
live:record:getCallback	授予查询录制回调配置的权限。	Read	-	-	-
live:record:deleteCallback	授予删除录制回调配置的权限。	Write	-	-	-
live:snapshot:createRule	授予添加直播截图配置的权限。	Write	-	-	-
live:snapshot:updateRule	授予修改直播截图配置的权限。	Write	-	-	-
live:snapshot:listRules	授予查询直播截图配置的权限。	Read	-	-	-
live:snapshot:deleteRule	授予删除直播截图配置的权限。	Write	-	-	-
live:stream:createStreamForbidden	授予禁止直播推流的权限。	Write	-	-	-
live:stream:listStreamForbidden	授予查询生效的禁播指令列表的权限。	Read	-	-	-
live:stream:deleteStreamForbid	授予禁推恢复	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
den	的权限。				
live:stream:updateStreamForbidden	授予修改禁推属性的权限。	Write	-	-	-
live:stream:createStreamForbiddenOnce	授予直播流闪断的权限。	Write	-	-	-
live:stream:listLiveStreamsOnline	授予查询直播在线流列表的权限。	Read	-	-	-
live:stream:createPullTask	授予创建外网拉流任务的权限。	Write	-	-	-
live:stream:deletePullTask	授予删除外网拉流任务的权限。	Write	-	-	-
live:stream:listPullTask	授予查询外网拉流任务列表的权限。	Read	-	-	-
live:tenant:updateChargingMode	授予设置计费模式的权限。	Write	-	-	-
live:tenant:getTenantInformation	授予查询租户信息的权限。	Read	-	-	-
live:transcode:createTranscodingsTemplate	授予创建直播转码模板的权限。	Write	-	-	-
live:transcode:deleteTranscodingsTemplate	授予删除直播转码模板的权限。	Write	-	-	-
live:transcode:updateTranscodingsTemplate	授予修改直播转码模板的权限。	Write	-	-	-
live:transcode:listTranscodingsTemplate	授予查询直播转码模板的权	Read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
live:transcode:createSEI	授予添加转码 SEI 信息的权限。	Write	-	-	-

Live 的 API 通常对应着一个或多个授权项。表 3-226 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-222 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/domain	live:domain:createDomain	-
DELETE /v1/{project_id}/domain	live:domain:deleteDomain	-
PUT /v1/{project_id}/domain	live:domain:updateDomain	-
GET /v1/{project_id}/domain	live:domain:getDomains	-
PUT /v1/{project_id}/domains_mapping	live:domain:createDomainsMapping	-
DELETE /v1/{project_id}/domains_mapping	live:domain:deleteDomainsMapping	-
PUT /v1/{project_id}/notifications/publish	live:domain:updateStreamNotification	-
GET /v1/{project_id}/notifications/publish	live:domain:getStreamNotifications	-
DELETE /v1/{project_id}/notifications/publish	live:domain:deleteStreamNotification	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/guard/ip	live:domain:getIPAuthList	-
PUT /v1/{project_id}/guard/ip	live:domain:updateIPAuthList	-
PUT /v1/{project_id}/guard/referer-chain	live:domain:updateRefererChain	-
DELETE /v1/{project_id}/guard/referer-chain	live:domain:deleteRefererChain	-
GET /v1/{project_id}/guard/referer-chain	live:domain:getRefererChain	-
GET /v1/{project_id}/logs	live:logs:listLog	-
POST /v1/{project_id}/record/rules	live:record:createRule	-
GET /v1/{project_id}/record/rules	live:record:listRules	-
PUT /v1/{project_id}/record/rules/{id}	live:record:updateRule	-
DELETE /v1/{project_id}/record/rules/{id}	live:record:deleteRule	-
GET /v1/{project_id}/record/rules/{id}	live:record:getRule	-
POST /v1/{project_id}/record/control	live:record:createCommand	-
POST /v1/{project_id}/record/callbacks	live:record:createCallback	-
GET /v1/{project_id}/record/callbacks	live:record:listCallbacks	-
PUT /v1/{project_id}/recor	live:record:updateCallback	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
d/callbacks/{id}		
GET /v1/{project_id}/record/callbacks/{id}	live:record:getCallback	-
DELETE /v1/{project_id}/record/callbacks/{id}	live:record:deleteCallback	-
POST /v1/{project_id}/stream/snapshot	live:snapshot:createRule	-
PUT /v1/{project_id}/stream/snapshot	live:snapshot:updateRule	-
GET /v1/{project_id}/stream/snapshot	live:snapshot:listRules	-
DELETE /v1/{project_id}/stream/snapshot	live:snapshot:deleteRule	-
POST /v1/{project_id}/stream/blocks	live:stream:createStreamForbidden	-
GET /v1/{project_id}/stream/blocks	live:stream:listStreamForbidden	-
DELETE /v1/{project_id}/stream/blocks	live:stream:deleteStreamForbidden	-
PUT /v1/{project_id}/stream/blocks	live:stream:updateStreamForbidden	-
GET /v1/{project_id}/realtime/streams	live:stream:listLiveStreamsOnline	-
POST /v1/{project_id}/template/transcodings	live:transcode:createTranscodingsTemplate	-
DELETE /v1/{project_id}/template/transcodings	live:transcode:deleteTranscodingsTemplate	-
PUT /v1/{project_id}/template/transcodings	live:transcode:updateTranscodingsTemplate	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/template/transcodings	live:transcode:listTranscodingsTemplate	-
GET /v1/{project_id}/guard/key-chain	live:domain:getCDNConfig	-
PUT /v1/{project_id}/guard/key-chain	live:domain:updateCDNConfig	-
DELETE /v1/{project_id}/guard/key-chain	live:domain:deleteCDNConfig	-
PUT /v1/{project_id}/guard/https-cert	live:domain:updateCDNConfig	-
GET /v1/{project_id}/guard/https-cert	live:domain:getCDNConfig	-
DELETE /v1/{project_id}/guard/https-cert	live:domain:deleteCDNConfig	-

资源类型（Resource）

Live 服务不支持在身份策略中的资源中指定资源进行权限控制。如需允许访问 Live 服务，请在身份策略的 Resource 元素中使用通配符号*，表示身份策略将应用到所有资源。

条件（Condition）

Live 服务不支持在身份策略中的条件键中配置服务级的条件键。Live 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.12.2 媒体处理服务 MPC

云服务在 IAM 预置了常用的权限，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

 版权所有 © 华为云计算技术有限公司

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 MPC 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 MPC 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 MPC 的相关操作。

表3-223 MPC 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
mpc:transcodeTemplate:create	授予创建转码模板的权限。	Write	-	-	-
mpc:transcodeTemplate:update	授予更新转码模板的权限。	Write	-	-	-
mpc:transcodeTemplate:delete	授予删除转码模板的权限。	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
mpc:transcodeTemplate:view	授予查看转码模板的权限。	List	-	-	-
mpc:templateGroup:create	授予创建转码模板组的权限。	Write	-	-	-
mpc:templateGroup:view	授予查看多个转码模板组的权限。	Write	-	-	-
mpc:templateGroup:update	授予更新转码模板组的权限。	Write	-	-	-
mpc:templateGroup:delete	授予删除转码模板组的权限。	Write	-	-	-
mpc:watermarkTempate:create	授予创建水印模板的权限。	Write	-	-	-
mpc:watermarkTempate:update	授予更新水印模板的权限。	Write	-	-	-
mpc:watermarkTempate:delete	授予删除水印模板的权限。	Write	-	-	-
mpc:watermarkTempate:view	授予查看水印模板的权限。	List	-	-	-
mpc:transcodeTask:create	授予创建转码任务的权限。	Write	-	-	-
mpc:transcodeTask:delete	授予取消已下发的转码任务的权限。	Write	-	-	-
mpc:transcodeTask:view	授予查询转码任务的权限。	Read	-	-	-
mpc:transcodeTask:deleteRecord	授予删除状态为“已取消”的任务记录的权限。	Write	-	-	-
mpc:transcodeTask:viewSumm	授予查询多个	List	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
aryStatistics	转码任务的统计概览信息的权限。				
mpc:remuxTsk:create	授予创建转封装任务的权限。	Write	-	-	-
mpc:remuxTsk:retry	授予重试转封装任务的权限。	Write	-	-	-
mpc:remuxTsk:view	授予查询多个转封装任务状态的权限。	List	-	-	-
mpc:remuxTsk:delete	授予取消排队中的转封装任务的权限。	Write	-	-	-
mpc:remuxTsk:deleteRecord	授予删除状态为已取消的转封装任务记录的权限。	Write	-	-	-
mpc:animatedGraphicsTask:create	授予新建转动图任务的权限。	Write	-	-	-
mpc:animatedGraphicsTask:view	授予查询多个动图任务状态的权限。	List	-	-	-
mpc:animatedGraphicsTask:delete	授予取消转动图任务的权限。	Write	-	-	-
mpc:extracTask:create	授予创建解析任务的权限。	Write	-	-	-
mpc:extracTask:view	授予查询媒体解析任务的权限。	List	-	-	-
mpc:extracTask:delete	授予取消视频解析任务，仅支持取消排队	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	中的任务的权限。				
mpc:thumbnailsTask:view	授予查询截图任务的权限。	List	-	-	-
mpc:thumbnailsTask:delete	授予取消截图任务的权限。	Write	-	-	-
mpc:notification:config	授予配置转码服务事件通知的权限。	Write	-	-	-
mpc:notification:view	授予查询转码服务端事件通知的权限。	List	-	-	-
mpc:notifyEvent:view	授予查询通知事件的权限。	List	-	-	-
mpc:bucket:view	授予查询桶列表的权限。	List	-	-	-
mpc:bucket:updateAuthorized	授予更新桶授权或取消授权的权限。	Write	-	-	-
mpc:bucketObject:view	授予查询桶里的 object 的权限。	List	-	-	-
mpc:agenciesTask:create	授予开启或关闭委托授权的权限。	Write	-	-	-
mpc:agenciesTask:view	授予查询创建委托任务状态的权限。	Read	-	-	-
mpc:encryptTask:create	授予新建独立加密任务的权限。	Write	-	-	-
mpc:encryptTask:delete	授予取消加密任务的权限。	Write	-	-	-
mpc:encryptTask:view	授予查看加密	List	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	任务的权限。				

MPC 的 API 通常对应着一个或多个授权项。表 3-228 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-224 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/template/transcodings	mpc:transcodeTemplate:create	-
PUT /v1/{project_id}/template/transcodings	mpc:transcodeTemplate:update	-
DELETE /v1/{project_id}/template/transcodings	mpc:transcodeTemplate:delete	-
GET /v1/{project_id}/template/transcodings	mpc:transcodeTemplate:view	-
POST /v1/{project_id}/template_group/transcodings	mpc:templateGroup:create	-
GET /v1/{project_id}/template_group/transcodings	mpc:templateGroup:view	-
PUT /v1/{project_id}/template_group/transcodings	mpc:templateGroup:update	-
DELETE /v1/{project_id}/template_group/transcodings	mpc:templateGroup:delete	-
POST /v1/{project_id}/template/watermark	mpc:watermarkTempate:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/template/watermark	mpc:watermarkTempate:update	-
DELETE /v1/{project_id}/template/watermark	mpc:watermarkTempate:delete	-
GET /v1/{project_id}/template/watermark	mpc:watermarkTempate:view	-
POST /v1/{project_id}/transcodings	mpc:transcodeTask:create	-
DELETE /v1/{project_id}/transcodings	mpc:transcodeTask:delete	-
GET /v1/{project_id}/transcodings	mpc:transcodeTask:view	-
DELETE /v1/{project_id}/transcodings/task	mpc:transcodeTask:deleteRecord	-
GET /v1/{project_id}/transcodings/summaries	mpc:transcodeTask:viewSummaryStatistics	-
POST /v1/{project_id}/remux	mpc:remuxTsk:create	-
PUT /v1/{project_id}/remux	mpc:remuxTsk:retry	-
GET /v1/{project_id}/remux	mpc:remuxTsk:view	-
DELETE /v1/{project_id}/remux	mpc:remuxTsk:delete	-
DELETE /v1/{project_id}/remux/task	mpc:remuxTsk:deleteRecord	-
POST /v1/{project_id}/animated-graphics	mpc:animatedGraphicsTask:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/animated-graphics	mpc:animatedGraphicsTask:view	-
DELETE /v1/{project_id}/animated-graphics	mpc:animatedGraphicsTask:delete	-
POST /v1/{project_id}/extract-metadata	mpc:extracTask:create	-
GET /v1/{project_id}/extract-metadata	mpc:extracTask:view	-
DELETE /v1/{project_id}/extract-metadata	mpc:extracTask:delete	-
POST /v1/{project_id}/thumbnails	mpc:thumbnailsTask:create	-
GET /v1/{project_id}/thumbnails	mpc:thumbnailsTask:view	-
DELETE /v1/{project_id}/thumbnails	mpc:thumbnailsTask:delete	-
PUT /v1/{project_id}/notification	mpc:notification:config	-
GET /v1/{project_id}/notification	mpc:notification:view	-
GET /v1/{project_id}/notification/event	mpc:notifyEvent:view	-
GET /v1/{project_id}/buckets	mpc:bucket:view	-
PUT /v1/{project_id}/authority	mpc:bucket:updateAuthorized	-
GET /v1.0-ext/{project_id}/objects	mpc:bucketObject:view	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/agencies	mpc:ageniesTask:create	-
GET /v1/{project_id}/agencies	mpc:ageniesTask:view	-
POST /v1/{project_id}/encryptions	mpc:encryptTask:create	-
DELETE /v1/{project_id}/encryptions	mpc:encryptTask:delete	-
GET /v1/{project_id}/encryptions	mpc:encryptTask:view	-

资源类型（Resource）

MPC 服务不支持在身份策略中的资源中指定资源进行权限控制。如需允许访问 MPC 服务，请在身份策略的 Resource 元素中使用通配符号*，表示身份策略将应用到所有资源。

条件（Condition）

MPC 服务不支持在身份策略中的条件键中配置服务级的条件键。MPC 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.13 管理与监管

3.13.1 统一身份认证服务 IAM

云服务在 IAM 预置了常用的权限，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

 版权所有 © 华为云计算技术有限公司

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 IAM 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 IAM 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 IAM 的相关操作。

表3-225 IAM 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam::listAccessKeys	授予列举永久访问密钥的权限。	List	-	-	• iam:credentials:listCredentials
iam::createAccessKey	授予创建永久访问密钥的权限。	Write	-	-	• iam:credentials:createCredential

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam::getAccessKey	授予查询永久访问密钥的权限。	Read	-	-	• iam:credentials:getCredential
iam::updateAccessKey	授予修改永久访问密钥的权限。	Write	-	-	• iam:credentials:updateCredential
iam::deleteAccessKey	授予删除永久访问密钥的权限。	Write	-	-	• iam:credentials:deleteCredential
iam:projects:list	授予列举项目的权限。	List	-	-	• iam:projects:listProjects
iam:projects:create	授予创建项目的权限。	Write	-	-	• iam:projects:createProject
iam:projects:listForUser	授予列举指定用户项目的权限。	List	-	-	• iam:projects:listProjectsForUser
iam:projects:update	授予修改项目的权限。	Write	-	-	• iam:projects:updateProject
iam:groups:list	授予列举用户组的权限。	List	-	-	• iam:groups:listGroups
iam:groups:create	授予创建用户组的权限。	Write	-	-	• iam:groups:createGroup
iam:groups:get	授予查询用户组的权限。	Read	-	-	• iam:groups:getGroup
iam:groups:delete	授予删除用户组的权限。	Write	-	-	• iam:groups:deleteGroup
iam:groups:update	授予修改用户组的权限。	Write	-	-	• iam:groups:updateGroup
iam:groups:removeUser	授予从用户组中移除用户的权限。	Write	-	-	• iam:permissions:removeUserFromGroup
iam:groups:list	授予列举指定	List	-	-	• iam:users:lis

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
Users	用户组中用户的权限。				tUsersForGroup
iam:groups:checkUser	授予查询用户是否在用户组中的权限。	Read	-	-	• iam:permissions:checkUserInGroup
iam:groups:addUser	授予添加用户到用户组的权限。	Write	-	-	• iam:permissions:addUserToGroup
iam:users:create	授予创建用户的权限。	Write	-	-	• iam:users:createUser
iam:users:get	授予查询用户的权限。	Read	-	-	• iam:users:getUser
iam:users:update	授予修改用户的权限。	Write	-	-	• iam:users:updateUser
iam:users:list	授予列举用户的权限。	List	-	-	• iam:users:listUsers
iam:users:delete	授予删除用户的权限。	Write	-	-	• iam:users:deleteUser
iam:users:listGroups	授予列举指定用户所属用户组的权限。	List	-	-	• iam:groups:listGroupsForUser
iam:users:listVirtualMFADevices	授予列举指定用户所属虚拟MFA 设备的权限。	List	-	-	• iam:mfa:listVirtualMFADevices
iam:users:createVirtualMFADevice	授予创建虚拟MFA 设备密钥的权限。	Write	-	-	• iam:mfa:createVirtualMFADevice
iam:users:deleteVirtualMFADevice	授予删除虚拟MFA 设备的权限。	Write	-	-	• iam:mfa:deleteVirtualMFADevice
iam:users:getVirtualMFADevice	授予查询虚拟MFA 设备的权限。	Read	-	-	• iam:mfa:getVirtualMFADevice
iam:users:bind	授予绑定虚拟	Write	-	-	• iam:mfa:bin

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
VirtualMFADevice	MFA 设备的权限。				dMFADevice
iam:users:unbindVirtualMFADevice	授予解绑虚拟 MFA 设备的权限。	Write	-	-	• iam:mfa:unbindMFADevice
iam:identityProviders:list	授予列举身份提供商的权限。	List	-	-	• iam:identityProviders:listIdentityProviders
iam:identityProviders:get	授予查询身份提供商的权限。	Read	-	-	• iam:identityProviders:getIdentityProvider
iam:identityProviders:create	授予创建身份提供商的权限。	Write	-	-	• iam:identityProviders:createIdentityProvider
iam:identityProviders:delete	授予删除身份提供商的权限。	Write	-	-	• iam:identityProviders:deleteIdentityProvider
iam:identityProviders:update	授予修改身份提供商的权限。	Write	-	-	• iam:identityProviders:updateIdentityProvider
iam:identityProviders:listMappings	授予列举身份提供商映射关系的权限。	List	-	-	-
iam:identityProviders:getMapping	授予查询身份提供商映射关系的权限。	Read	-	-	-
iam:identityProviders:createMapping	授予创建身份提供商映射关系的权限。	Write	-	-	-
iam:identityProviders:deleteMapping	授予删除身份提供商映射关系的权限。	Write	-	-	-
iam:identityProviders:updateM	授予修改身份	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apping	提供商映射关系的权限。				
iam:identityProviders:listProtocols	授予列举身份提供商协议的权限。	List	-	-	-
iam:identityProviders:getProtocol	授予查询身份提供商协议的权限。	Read	-	-	-
iam:identityProviders:createProtocol	授予创建身份提供商协议的权限。	Write	-	-	-
iam:identityProviders:deleteProtocol	授予删除身份提供商协议的权限。	Write	-	-	-
iam:identityProviders:updateProtocol	授予修改身份提供商协议的权限。	Write	-	-	-
iam:identityProviders:getSAMLMetadata	授予查询身份提供商 SAML metadata 文件的权限。	Read	-	-	• iam:identityProviders:getIDPMetadata
iam:identityProviders:createSAMLMetadata	授予创建身份提供商 SAML metadata 文件的权限。	Write	-	-	• iam:identityProviders:createIDPMetadata
iam:identityProviders:getOIDCConfig	授予查询身份提供商 OIDC 配置的权限。	Read	-	-	• iam:identityProviders:getOpenIDConnectConfig
iam:identityProviders:createOIDCConfig	授予创建身份提供商 OIDC 配置的权限。	Write	-	-	• iam:identityProviders:createOpenIDConnectConfig
iam:identityProviders:updateOIDCConfig	授予修改身份提供商 OIDC 配置的权限。	Write	-	-	• iam:identityProviders:updateOpenIDConnectCon

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
					fig
iam:securityPolicies:getProtectPolicy	授予查询操作保护策略的权限。	Read	-	-	-
iam:securityPolicies:updateProtectPolicy	授予修改操作保护策略的权限。	Write	-	-	-
iam:securityPolicies:getPasswordPolicy	授予查询密码策略的权限。	Read	-	-	-
iam:securityPolicies:updatePasswordPolicy	授予修改密码策略的权限。	Write	-	-	-
iam:securityPolicies:getLoginPolicy	授予查询登录策略的权限。	Read	-	-	-
iam:securityPolicies:updateLoginPolicy	授予修改登录策略的权限。	Write	-	-	-
iam:securityPolicies:getConsoleAclPolicy	授予查询控制台访问策略的权限。	Read	-	-	-
iam:securityPolicies:updateConsoleAclPolicy	授予修改控制台访问策略的权限。	Write	-	-	-
iam:securityPolicies:getApiAclPolicy	授予查询接口访问策略的权限。	Read	-	-	-
iam:securityPolicies:updateApiAclPolicy	授予修改接口访问策略的权限。	Write	-	-	-
iam:securityPolicies:getPrivacyTransferPolicy	授予查询账号信息跨境传输策略的权限。	Read	-	-	-
iam:securityPolicies:updatePrivacyTransferPoli	授予修改账号信息跨境传输策略的权限。	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cy					
iam:users:listLoginProtectSettings	授予列举租户下用户登录保护设置的权限。	List	-	-	• iam:users:listUserLoginProtects
iam:users:getLoginProtectSetting	授予查询登录保护设置的权限。	Read	-	-	• iam:users:getUserLoginProtect
iam:users:updateLoginProtectSetting	授予修改登录保护设置的权限。	Write	-	-	• iam:users:setUserLoginProtect
iam:quotas:list	授予列举配额的权限。	List	-	-	• iam:quotas:listQuotas
iam:quotas:listForProject	授予查询项目配额的权限。	List	-	-	• iam:quotas:listQuotasForProject
iam:agencies:pass	授予向云服务传递委托的权限。	Permission_management	agency *	-	-
iam:roles:list	授予查询权限列表的权限。	List	-	-	• iam:roles:listRoles
iam:roles:get	授予查询权限详情的权限。	Read	-	-	• iam:roles:getRole
iam::listRoleAssignments	授予查询租户授权记录的权限。	List	-	-	• iam:permissions:listRoleAssignments
iam:groups:listRolesOnDomain	授予查询全局服务中用户组权限的权限。	List	-	-	• iam:permissions:listRolesForGroupOnDomain
iam:groups:listRolesOnProject	授予查询项目服务中用户组权限的权限。	List	-	-	• iam:permissions:listRolesForGroupOnProject
iam:groups:grantRoleOnDoma	授予为用户组授予全局服务	Write	-	-	• iam:permissions:grantRoleToGroupO

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
in	权限的权限。				nDomain
iam:groups:grantRoleOnProject	授予为用户组授予项目级服务权限的权限。	Write	-	-	• iam:permissions:grantRoleToGroupOnProject
iam:groups:checkRoleOnDomain	授予查询用户组是否拥有全局服务权限的权限。	Read	-	-	• iam:permissions:checkRoleForGroupOnDomain
iam:groups:checkRoleOnProject	授予查询用户组是否拥有项目服务权限的权限。	Read	-	-	• iam:permissions:checkRoleForGroupOnProject
iam:groups:listRoles	授予查询用户组的所有权限的权限。	List	-	-	• iam:permissions:listRolesForGroup
iam:groups:checkRole	授予查询用户组是否拥有指定权限的权限。	Read	-	-	• iam:permissions:checkRoleForGroup
iam:groups:revokeRole	授予移除用户组指定权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromGroup
iam:groups:revokeRoleOnDomain	授予移除用户组的全局服务权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromGroupOnDomain
iam:groups:revokeRoleOnProject	授予移除用户组的项目服务权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromGroupOnProject
iam:groups:grantRole	授予为用户组授予指定权限的权限。	Write	-	-	• iam:permissions:grantRoleToGroup
iam:roles:create	授予创建自定义策略的权	Write	-	-	• iam:roles:createRole

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
iam:roles:update	授予修改自定义策略的权限。	Write	-	-	• iam:roles:updateRole
iam:roles:delete	授予删除自定义策略的权限。	Write	-	-	• iam:roles:deleteRole
iam:agencies:list	授予列出委托的权限。	List	-	-	• iam:agencies:listAgencies
iam:agencies:listSwitchAgencyHistories	授予列出切换委托历史的权限。	List	-	-	-
iam:agencies:get	授予查询指定委托详情的权限。	Read	-	-	• iam:agencies:getAgency
iam:agencies:create	授予创建委托的权限。	Write	-	-	• iam:agencies:createAgency
iam:agencies:update	授予修改委托的权限。	Write	-	-	• iam:agencies:updateAgency
iam:agencies:delete	授予删除委托的权限。	Write	-	-	• iam:agencies:deleteAgency
iam:agencies:listRolesOnDomain	授予查询委托拥有的全局服务权限的权限。	List	-	-	• iam:permissions:listRolesForAgencyOnDomain
iam:agencies:listRolesOnProject	授予查询委托拥有的指定项目权限的权限。	List	-	-	• iam:permissions:listRolesForAgencyOnProject
iam:agencies:grantRoleOnDomain	授予为委托授予全局服务权限的权限。	Write	-	-	• iam:permissions:grantRoleToAgencyOnDomain

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:agencies:grantRoleOnProject	授予为委托授予项目服务权限的权限。	Write	-	-	• iam:permissions:grantRoleToAgencyOnProject
iam:agencies:checkRoleOnDomain	授予查询委托是否拥有全局服务权限的权限。	Read	-	-	• iam:permissions:checkRoleForAgencyOnDomain
iam:agencies:checkRoleOnProject	授予查询委托是否拥有项目服务权限的权限。	Read	-	-	• iam:permissions:checkRoleForAgencyOnProject
iam:agencies:revokeRoleOnDomain	授予移除委托的全局服务权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromAgencyOnDomain
iam:agencies:revokeRoleOnProject	授予移除委托的项目服务权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromAgencyOnProject
iam:agencies:listRoles	授予查询委托的所有权限的权限。	List	-	-	• iam:permissions:listRolesForAgency
iam:agencies:grantRole	授予为委托授予指定权限的权限。	Write	-	-	• iam:permissions:grantRoleToAgency
iam:agencies:checkRole	授予查询委托是否拥有指定权限的权限。	Read	-	-	• iam:permissions:checkRoleForAgency
iam:agencies:revokeRole	授予移除委托的指定权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromAgency
iam::listGroupsAssignedEnterpriseProject	授予查询企业项目关联的用户组的权限。	List	-	-	• iam:permissions:listGroupsOnEnterpriseProject

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:groups:listRolesOnEnterpriseProject	授予查询企业项目已关联用户组的权限的权限。	List	-	-	• iam:permissions:listRolesForGroupOnEnterpriseProject
iam:groups:grantRoleOnEnterpriseProject	授予基于用户组为企业项目授权的权限。	Write	-	-	• iam:permissions:grantRoleToGroupOnEnterpriseProject
iam:groups:revokeRoleOnEnterpriseProject	授予删除企业项目关联的用户组权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromGroupOnEnterpriseProject
iam:groups:listAssignedEnterpriseProjects	授予查询用户组直接关联的企业项目的权限。	List	-	-	• iam:permissions:listEnterpriseProjectsForGroup
iam:users:listAssignedEnterpriseProjects	授予查询用户直接关联的企业项目的权限。	List	-	-	• iam:permissions:listEnterpriseProjectsForUser
iam::listUsersAssignedEnterpriseProject	授予查询企业项目直接关联用户的权限。	List	-	-	• iam:permissions:listUsersForEnterpriseProject
iam:users:listRolesOnEnterpriseProject	授予查询企业项目直接关联用户权限的权限。	List	-	-	• iam:permissions:listRolesForUserOnEnterpriseProject
iam:users:grantRoleOnEnterpriseProject	授予基于用户为企业项目授权的权限。	Write	-	-	• iam:permissions:grantRoleToUserOnEnterpriseProject
iam:users:revokeRoleOnEnterpriseProject	授予删除企业项目直接关联用户的权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromUserOnEnterpri

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
					seProject
iam:agencies:grantRoleOnEnterpriseProject	授予基于委托为企业项目授权的权限。	Write	-	-	• iam:permissions:grantRoleToAgencyOnEnterpriseProject
iam:agencies:revokeRoleOnEnterpriseProject	授予删除企业项目关联的委托的权限的权限。	Write	-	-	• iam:permissions:revokeRoleFromAgencyOnEnterpriseProject
iam:mfa:listMFADevicesV5	授予列举 MFA 设备的权限。	List	mfa *	-	-
iam:mfa:createVirtualMFADeviceV5	授予创建虚拟 MFA 设备的权限。	Write	mfa *	-	-
iam:mfa:deleteVirtualMFADeviceV5	授予删除虚拟 MFA 设备的权限。	Write	mfa *	-	-
iam:mfa:enableV5	授予启用 MFA 设备的权限。	Write	mfa *	-	-
iam:mfa:disableV5	授予禁用 MFA 设备的权限。	Write	mfa *	-	-
iam:securitypolicies:getPasswordPolicyV5	授予获取密码策略信息的权限。	Read	-	-	-
iam:securitypolicies:updatePasswordPolicyV5	授予修改密码策略的权限。	Write	-	-	-
iam:securitypolicies:getLoginPolicyV5	授予获取登录策略信息的权限。	Read	-	-	-
iam:securitypolicies:updateLoginPolicyV5	授予修改登录策略的权限。	Write	-	-	-
iam:credentials:listCredentialsV	授予权限以列举 IAM 用户的	List	user *	g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
5	永久访问密钥。				
iam:credentials:showAccessKeyLastUsedV5	授予获取指定永久访问密钥最后一次使用时间的权限。	Read	user *	g:ResourceTag/<tag-key>	-
iam:credentials:createCredentialV5	授予为 IAM 用户创建永久访问密钥的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:credentials:updateCredentialV5	授予为 IAM 用户修改永久访问密钥的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:credentials:deleteCredentialV5	授予为 IAM 用户删除永久访问密钥的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:changePasswordV5	授予 IAM 用户修改自己密码的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:showLoginProfileV5	授予获取 IAM 用户登录信息的权限。	Read	user *	g:ResourceTag/<tag-key>	-
iam:users:createLoginProfileV5	授予为 IAM 用户创建登录信息的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:updateLoginProfileV5	授予为 IAM 用户修改登录信息的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:deleteLoginProfileV5	授予为 IAM 用户删除登录信息的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:listUsersV5	授予列举 IAM 用户的权限。	List	user *	-	-
iam:users:getUs	授予获取 IAM	Read	user *	g:ResourceTag/	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
erV5	用户信息的权限。			<tag-key>	
iam:users:showUserLastLoginV5	授予获取 IAM 用户最后一次登录时间的权限。	Read	user *	g:ResourceTag/<tag-key>	-
iam:users:createUserV5	授予创建 IAM 用户的权限。	Write	user *	-	-
iam:users:updateUserV5	授予修改 IAM 用户的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:users:deleteUserV5	授予删除 IAM 用户的权限。	Write	user *	g:ResourceTag/<tag-key>	-
iam:groups:listGroupsV5	授予列举用户组的权限。	List	group *	-	-
iam:groups:getGroupV5	授予获取用户组信息的权限。	Read	group *	-	-
iam:groups:createGroupV5	授予创建用户组的权限。	Write	group *	-	-
iam:groups:updateGroupV5	授予修改用户组的权限。	Write	group *	-	-
iam:groups:deleteGroupV5	授予删除用户组的权限。	Write	group *	-	-
iam:permissions:addUserToGroupV5	授予添加 IAM 用户到用户组的权限。	Write	group *	-	-
iam:permissions:removeUserFromGroupV5	授予从用户组中移除 IAM 用户的权限。	Write	group *	-	-
iam:policies:listV5	授予列举身份策略的权限。	List	policy *	-	-
iam:policies:getV5	授予获取身份策略信息的权限。	Read	policy *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
iam:policies:createV5	授予创建自定义身份策略的权限。	Permission_management	policy *	-	-
iam:policies:deleteV5	授予删除自定义身份策略的权限。	Permission_management	policy *	-	-
iam:policies:listVersionsV5	授予列举身份策略版本的权限。	List	policy *	-	-
iam:policies:getVersionV5	授予获取身份策略版本信息的权限。	Read	policy *	-	-
iam:policies:createVersionV5	授予为自定义身份策略创建新版本的权限。	Permission_management	policy *	-	-
iam:policies:deleteVersionV5	授予为自定义身份策略删除版本的权限。	Permission_management	policy *	-	-
iam:policies:setDefaultVersionV5	授予设置自定义身份策略默认版本的权限。	Permission_management	policy *	-	-
iam:agencies:attachPolicyV5	授予为委托或信任委托附加身份策略的权限。	Permission_management	agency *	g:ResourceTag/<tag-key>	-
			-	iam:PolicyURN	
iam:groups:attachPolicyV5	授予为用户组附加身份策略的权限。	Permission_management	group *	-	-
			-	iam:PolicyURN	
iam:users:attachPolicyV5	授予为 IAM 用户附加身份策略的权限。	Permission_management	user *	g:ResourceTag/<tag-key>	-
			-	iam:PolicyURN	
iam:agencies:de	授予为委托或	Permi	agenc	g:ResourceTag/	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
tachPolicyV5	信任委托分离身份策略的权限。	ssion_management	y *	<tag-key>	
			-	iam:PolicyURN	
iam:groups:detachPolicyV5	授予为用户组分离身份策略的权限。	Permission_management	group *	-	-
			-	iam:PolicyURN	
iam:users:detachPolicyV5	授予为 IAM 用户分离身份策略的权限。	Permission_management	user *	g:ResourceTag/<tag-key>	-
			-	iam:PolicyURN	
iam:policies:listEntitiesV5	授予权限以列举附加在身份策略上的所有实体。	List	policy *	-	-
iam:agencies:listAttachedPoliciesV5	授予权限以列举委托或信任委托附加的身份策略。	List	agency *	g:ResourceTag/<tag-key>	-
iam:groups:listAttachedPoliciesV5	授予权限以列举用户组附加的身份策略。	List	group *	-	-
iam:users:listAttachedPoliciesV5	授予权限以列举 IAM 用户附加的身份策略。	List	user *	g:ResourceTag/<tag-key>	-
iam:agencies:createServiceLinkedAgencyV5	授予创建服务关联委托的权限以允许云服务代表您执行操作。	Write	agency *	-	-
			-	iam:ServicePrincipal	
iam:agencies:deleteServiceLinkedAgencyV5	授予删除服务关联委托的权限。	Write	agency *	g:ResourceTag/<tag-key>	-
			-	iam:ServicePrincipal	
iam:agencies:getServiceLinkedAgencyDeletio	授予获取服务关联委托删除状态的权限。	Read	agency *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
nStatusV5					
iam:agencies:listV5	授予列举委托及信任委托的权限。	List	agency *	-	-
iam:agencies:getV5	授予获取委托或信任委托信息的权限。	Read	agency *	g:ResourceTag/<tag-key>	-
iam:agencies:createV5	授予创建信任委托的权限。	Write	agency *	-	-
iam:agencies:updateV5	授予修改信任委托的权限。	Write	agency *	g:ResourceTag/<tag-key>	-
iam:agencies:deleteV5	授予删除信任委托的权限。	Write	agency *	g:ResourceTag/<tag-key>	-
iam:agencies:updateTrustPolicyV5	授予修改信任委托信任策略的权限。	Write	agency *	g:ResourceTag/<tag-key>	-
iam::listTagsForResourceV5	授予列举资源标签的权限。	List	agency	g:ResourceTag/<tag-key>	-
			user	g:ResourceTag/<tag-key>	
iam::tagForResourceV5	授予设置资源标签的权限。	Tagging	agency	g:ResourceTag/<tag-key>	-
			user	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
iam::untagForResourceV5	授予删除资源标签的权限。	Tagging	agency	g:ResourceTag/<tag-key>	-
			user	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
iam::getAccoun	授予获取此账	List	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
tSummaryV5	号中 IAM 实体使用情况和 IAM 配额的摘要信息的权限。				
iam::getAsymmetricSignatureSwitchV5	授予获取临时令牌非对称签名开关状态的权限。	Read	-	-	-
iam::setAsymmetricSignatureSwitchV5	授予设置临时令牌非对称签名开关状态的权限。	Write	-	-	-

IAM 的 API 通常对应着一个或多个授权项。表 3-230 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-226 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3.0/OS-CREDENTIAL/credentials	iam::listAccessKeys	-
POST /v3.0/OS-CREDENTIAL/credentials	iam::createAccessKey	-
GET /v3.0/OS-CREDENTIAL/credentials/{access_key}	iam::getAccessKey	-
PUT /v3.0/OS-CREDENTIAL/credentials/{access_key}	iam::updateAccessKey	-
DELETE /v3.0/OS-CREDENTIAL/credentials/{access_key}	iam::deleteAccessKey	-
GET /v3.0/OS-QUOTA/domains/{domain_id}	iam:quotas:list	-
GET /v3.0/OS-QUOTA/projects/{project_id}	iam:quotas:listForProject	-
GET /v3/projects	iam:projects:list	-
POST /v3/projects	iam:projects:create	-
GET /v3/users/{user_id}/projects	iam:projects:listForU	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	ser	
PATCH /v3/projects/{project_id}	iam:projects:update	-
PUT /v3-ext/projects/{project_id}	iam:projects:update	-
GET /v3/groups	iam:groups:list	-
POST /v3/groups	iam:groups:create	-
GET /v3/groups/{group_id}	iam:groups:get	-
DELETE /v3/groups/{group_id}	iam:groups:delete	-
PATCH /v3/groups/{group_id}	iam:groups:update	-
GET /v3/groups/{group_id}/users	iam:groups:listUsers	-
HEAD /v3/groups/{group_id}/users/{user_id}	iam:groups:checkUser	-
PUT /v3/groups/{group_id}/users/{user_id}	iam:groups:addUser	-
DELETE /v3/groups/{group_id}/users/{user_id}	iam:groups:removeUser	-
POST /v3.0/OS-USER/users	iam:users:create	-
GET /v3.0/OS-USER/users/{user_id}	iam:users:get	-
PUT /v3.0/OS-USER/users/{user_id}	iam:users:update	-
PUT /v3.0/OS-USER/users/{user_id}/info	iam:users:update	-
GET /v3/users	iam:users:list	-
POST /v3/users	iam:users:create	-
GET /v3/users/{user_id}	iam:users:get	-
DELETE /v3/users/{user_id}	iam:users:delete	-
PATCH /v3/users/{user_id}	iam:users:update	-
GET /v3/users/{user_id}/groups	iam:users:listGroups	-
GET /v3.0/OS-MFA/virtual-mfa-devices	iam:users:listVirtualMFADevices	-
POST /v3.0/OS-MFA/virtual-mfa-devices	iam:users:createVirtualMFADevice	-
DELETE /v3.0/OS-MFA/virtual-mfa-devices	iam:users:deleteVirtualMFADevice	-
GET /v3.0/OS-MFA/users/{user_id}/virtual-mfa-device	iam:users:getVirtualMFADevice	-
PUT /v3.0/OS-MFA/mfa-devices/bind	iam:users:bindVirtualMFADevice	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v3.0/OS-MFA/mfa-devices/unbind	iam:users:unbindVirtualMFADevice	-
GET /v3.0/OS-USER/login-protects	iam:users:listLoginProtectSettings	-
GET /v3.0/OS-USER/users/{user_id}/login-protect	iam:users:getLoginProtectSetting	-
PUT /v3.0/OS-USER/users/{user_id}/login-protect	iam:users:updateLoginProtectSetting	-
GET /v3/OS-FEDERATION/identity_providers	iam:identityProviders:list	-
GET /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:get	-
PUT /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:create	-
DELETE /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:delete	-
PATCH /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:update	-
GET /v3/OS-FEDERATION/mappings	iam:identityProviders:listMappings	-
GET /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:getMapping	-
PUT /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:createMapping	-
DELETE /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:deleteMapping	-
PATCH /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:updateMapping	-
GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols	iam:identityProviders:listProtocols	-
GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:getProtocol	-
PUT /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:createProtocol	-
DELETE /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:deleteProtocol	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PATCH /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:updateProtocol	-
GET /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata	iam:identityProviders:getSAMLMetadata	-
POST /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata	iam:identityProviders:createSAMLMetadata	-
GET /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config	iam:identityProviders:getOIDCConfig	-
POST /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config	iam:identityProviders:createOIDCConfig	-
PUT /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config	iam:identityProviders:updateOIDCConfig	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy	iam:securityPolicies:getProtectPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy	iam:securityPolicies:updateProtectPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy	iam:securityPolicies:getPasswordPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy	iam:securityPolicies:updatePasswordPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy	iam:securityPolicies:getLoginPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy	iam:securityPolicies:updateLoginPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy	iam:securityPolicies:getConsoleAclPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy	iam:securityPolicies:updateConsoleAclPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy	iam:securityPolicies:getApiAclPolicy	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy	iam:securityPolicies:updateApiAclPolicy	-
GET /v3/roles	iam:roles:list	-
GET /v3/roles/{role_id}	iam:roles:get	-
GET /v3.0/OS-PERMISSION/role-assignments	iam::listRoleAssignments	-
GET /v3/domains/{domain_id}/groups/{group_id}/roles	iam:groups:listRolesOnDomain	-
GET /v3/projects/{project_id}/groups/{group_id}/roles	iam:groups:listRolesOnProject	-
PUT /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}	iam:groups:grantRoleOnDomain	-
PUT /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:groups:grantRoleOnProject	-
HEAD /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}	iam:groups:checkRoleOnDomain	-
HEAD /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:groups:checkRoleOnProject	-
GET /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/inherited_to_projects	iam:groups:listRoles	-
HEAD /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects	iam:groups:checkRole	-
DELETE /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects	iam:groups:revokeRole	-
DELETE /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}	iam:groups:revokeRoleOnDomain	-
DELETE /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:groups:revokeRoleOnProject	-
PUT /v3/OS-INHERIT/domains/{domain_id}/groups/{gro	iam:groups:grantRole	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
up_id}/roles/{role_id}/inherited_to_projects		
GET /v3.0/OS-ROLE/roles	iam:roles:list	-
GET /v3.0/OS-ROLE/roles/{role_id}	iam:roles:get	-
POST /v3.0/OS-ROLE/roles	iam:roles:create	-
POST /v3.0/OS-ROLE/roles	iam:roles:create	-
PATCH /v3.0/OS-ROLE/roles/{role_id}	iam:roles:update	-
PATCH /v3.0/OS-ROLE/roles/{role_id}	iam:roles:update	-
DELETE /v3.0/OS-ROLE/roles/{role_id}	iam:roles:delete	-
GET /v3.0/OS-AGENCY/agencies	iam:agencies:list	-
GET /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:get	-
POST /v3.0/OS-AGENCY/agencies	iam:agencies:create	-
PUT /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:update	-
DELETE /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:delete	-
GET /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles	iam:agencies:listRolesOnDomain	-
GET /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles	iam:agencies:listRolesOnProject	-
PUT /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:grantRoleOnDomain	-
PUT /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:grantRoleOnProject	-
HEAD /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:checkRoleOnDomain	-
HEAD /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:checkRoleOnProject	-
DELETE /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:revokeRoleOnDomain	-
DELETE /v3.0/OS-AGENCY/projects/{project_id}/agencies/{ag	iam:agencies:revoke	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ency_id}/roles/{role_id}	RoleOnProject	
GET /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/inherited_to_projects	iam:agencies:listRoles	-
PUT /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:agencies:grantRole	-
HEAD /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:agencies:checkRole	-
DELETE /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:agencies:revokeRole	-
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups	iam::listGroupsAssignedEnterpriseProject	-
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles	iam:groups:listRolesOnEnterpriseProject	-
PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}	iam:groups:grantRoleOnEnterpriseProject	-
DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}	iam:groups:revokeRoleOnEnterpriseProject	-
GET /v3.0/OS-PERMISSION/groups/{group_id}/enterprise-projects	iam:groups:listAssignedEnterpriseProjects	-
GET /v3.0/OS-PERMISSION/users/{user_id}/enterprise-projects	iam:users:listAssignedEnterpriseProjects	-
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users	iam::listUsersAssignedEnterpriseProject	-
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles	iam:users:listRolesOnEnterpriseProject	-
PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}	iam:users:grantRoleOnEnterpriseProject	-
DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_i	iam:users:revokeRoleOnEnterpriseProject	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
d}/roles/{role_id}		
PUT /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments	iam:agencies:grantRoleOnEnterpriseProject	-
DELETE /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments	iam:agencies:revokeRoleOnEnterpriseProject	-
GET /v5/asymmetric-signature-switch	iam::getAsymmetricSignatureSwitchV5	-
PUT /v5/asymmetric-signature-switch	iam::setAsymmetricSignatureSwitchV5	-
GET /v5/mfa-devices	iam:mfa:listMFADevicesV5	-
POST /v5/virtual-mfa-devices	iam:mfa:createVirtualMFADeviceV5	-
DELETE /v5/virtual-mfa-devices	iam:mfa:deleteVirtualMFADeviceV5	-
POST /v5/mfa-devices/enable	iam:mfa:enableV5	-
POST /v5/mfa-devices/disable	iam:mfa:disableV5	-
GET /v5/password-policy	iam:securitypolicies:getPasswordPolicyV5	-
PUT /v5/password-policy	iam:securitypolicies:updatePasswordPolicyV5	-
GET /v5/login-policy	iam:securitypolicies:getLoginPolicyV5	-
PUT /v5/login-policy	iam:securitypolicies:updateLoginPolicyV5	-
GET /v5/users/{user_id}/access-keys	iam:credentials:listCredentialsV5	-
GET /v5/users/{user_id}/access-keys/{access_key_id}/last-used	iam:credentials:showAccessKeyLastUsedV5	-
POST /v5/users/{user_id}/access-keys	iam:credentials:createCredentialV5	-
PUT /v5/users/{user_id}/access-keys/{access_key_id}	iam:credentials:updateCredentialV5	-
DELETE /v5/users/{user_id}/access-	iam:credentials:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
keys/{access_key_id}	CredentialV5	
POST /v5/caller-password	iam:users:changePasswordV5	-
GET /v5/users/{user_id}/login-profile	iam:users:showLoginProfileV5	-
POST /v5/users/{user_id}/login-profile	iam:users:createLoginProfileV5	-
PUT /v5/users/{user_id}/login-profile	iam:users:updateLoginProfileV5	-
DELETE /v5/users/{user_id}/login-profile	iam:users:deleteLoginProfileV5	-
GET /v5/users	iam:users:listUsersV5	-
GET /v5/users/{user_id}	iam:users:getUserV5	-
GET /v5/users/{user_id}/last-login	iam:users:showUserLastLoginV5	-
POST /v5/users	iam:users:createUserV5	-
PUT /v5/users/{user_id}	iam:users:updateUserV5	-
DELETE /v5/users/{user_id}	iam:users:deleteUserV5	-
GET /v5/groups	iam:groups:listGroupsV5	-
GET /v5/groups/{group_id}	iam:groups:getGroupV5	-
POST /v5/groups	iam:groups:createGroupV5	-
PUT /v5/groups/{group_id}	iam:groups:updateGroupV5	-
DELETE /v5/groups/{group_id}	iam:groups:deleteGroupV5	-
POST /v5/groups/{group_id}/add-user	iam:permissions:addUserToGroupV5	-
POST /v5/groups/{group_id}/remove-user	iam:permissions:removeUserFromGroupV5	-
GET /v5/policies	iam:policies:listV5	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v5/policies/{policy_id}	iam:policies:getV5	-
POST /v5/policies	iam:policies:createV5	-
DELETE /v5/policies/{policy_id}	iam:policies:deleteV5	-
GET /v5/policies/{policy_id}/versions	iam:policies:listVersionsV5	-
GET /v5/policies/{policy_id}/versions/{version_id}	iam:policies:getVersionV5	-
POST /v5/policies/{policy_id}/versions	iam:policies:createVersionV5	-
DELETE /v5/policies/{policy_id}/versions/{version_id}	iam:policies:deleteVersionV5	-
POST /v5/policies/{policy_id}/versions/{version_id}/set-default	iam:policies:setDefaultVersionV5	-
POST /v5/policies/{policy_id}/attach-agency	iam:agencies:attachPolicyV5	-
POST /v5/policies/{policy_id}/attach-group	iam:groups:attachPolicyV5	-
POST /v5/policies/{policy_id}/attach-user	iam:users:attachPolicyV5	-
POST /v5/policies/{policy_id}/detach-agency	iam:agencies:detachPolicyV5	-
POST /v5/policies/{policy_id}/detach-group	iam:groups:detachPolicyV5	-
POST /v5/policies/{policy_id}/detach-user	iam:users:detachPolicyV5	-
GET /v5/policies/{policy_id}/attached-entities	iam:policies:listEntitiesV5	-
GET /v5/agencies/{agency_id}/attached-policies	iam:agencies:listAttachedPoliciesV5	-
GET /v5/groups/{group_id}/attached-policies	iam:groups:listAttachedPoliciesV5	-
GET /v5/users/{user_id}/attached-policies	iam:users:listAttachedPoliciesV5	-
PUT /v5/service-linked-agencies	iam:agencies:createServiceLinkedAgencyV5	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /v5/service-linked-agencies/{agency_id}	iam:agencies:deleteServiceLinkedAgencyV5	-
GET /v5/service-linked-agencies/deletion-task/{deletion_task_id}	iam:agencies:getServiceLinkedAgencyDeletionStatusV5	-
GET /v5/agencies	iam:agencies:listV5	-
GET /v5/agencies/{agency_id}	iam:agencies:getV5	-
POST /v5/agencies	iam:agencies:createV5	-
PUT /v5/agencies/{agency_id}	iam:agencies:updateV5	-
DELETE /v5/agencies/{agency_id}	iam:agencies:deleteV5	-
PUT /v5/agencies/{agency_id}/trust-policy	iam:agencies:updateTrustPolicyV5	-
GET /v5/{resource_type}/{resource_id}/tags	iam::listTagsForResourceV5	-
POST /v5/{resource_type}/{resource_id}/tags/create	iam::tagForResourceV5	-
DELETE /v5/{resource_type}/{resource_id}/tags/delete	iam::untagForResourceV5	-
GET /v5/account-summary	iam::getAccountSummaryV5	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-231 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

IAM 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-227 IAM 支持的资源类型

资源类型	URN
agency	iam::<account-id>:agency:<agency-name-with-path>
policy	iam::<account-id>:policy:<policy-name-with-path>

 版权所有 © 华为云计算技术有限公司

资源类型	URN
mfa	iam::<account-id>:mfa:<mfa-name>
user	iam::<account-id>:user:<user-name>
group	iam::<account-id>:group:<group-name>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 iam:）仅适用于对应服务的操作，详情请参见表 3-232。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

IAM 支持的服务级条件键

IAM 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-228 IAM 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
iam:PolicyURN	string	单值	按照身份策略的 URN 筛选访问权限。
iam:ServicePrincipal	string	单值	按照服务关联委托传递的云服务对应的服务标识筛选访问权限。

 版权所有 © 华为云计算技术有限公司

3.13.2 组织 Organizations

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 Organizations 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 Organizations 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 Organizations 的相关操作。

 版权所有 © 华为云计算技术有限公司

表3-229 Organizations 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
organizations:organizations:create	授予创建组织的权限。	Write	-	-	-
organizations:organizations:get	授予查询所属组织信息的权限。	Read	-	-	-
organizations:organizations:delete	授予删除组织的权限。	Write	-	-	-
organizations:organizations:leave	授予离开当前组织的权限。	Write	-	-	-
organizations:roots:list	授予列出组织的根的权限。	List	-	-	-
organizations:ous:create	授予创建组织单元的权限。	Write	ou	g:ResourceTag/<tag-key>	-
			root	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
organizations:ous:list	授予列举组织单元的权限。	List	-	-	-
organizations:ous:get	授予查询有关组织单元的信息的权限。	Read	ou *	g:ResourceTag/<tag-key>	-
organizations:ous:update	授予更改组织单元名称的权限。	Write	ou *	g:ResourceTag/<tag-key>	-
organizations:ous:delete	授予删除组织单元的权限。	Write	ou *	g:ResourceTag/<tag-key>	-
organizations:accounts:create	授予创建账号的权限。	Write	-	• g:RequestTag/<tag-key> • g:TagKeys	-
organizations:a	授予列出组织	List	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ccounts:list	中的账号的权限。				
organizations:accounts:get	授予查询账号信息的权限。	Read	account *	g:ResourceTag/<tag-key>	-
organizations:accounts:remove	授予移除指定的账号的权限。	Write	account *	g:ResourceTag/<tag-key>	-
organizations:accounts:move	授予移动账号的权限。	Write	account *	g:ResourceTag/<tag-key>	-
organizations:accounts:invite	授予邀请账号加入组织的权限。	Write	-	• g:RequestTag/<tag-key> • g:TagKeys	-
organizations:createAccountStatuses:list	授予列出创建账号的状态的权限。	List	-	-	-
organizations:createAccountStatuses:get	授予查询有关创建账号状态的信息的权限。	Read	-	-	-
organizations:handshakes:get	授予查询邀请相关信息的权限。	Read	handshake *	-	-
organizations:handshakes:accept	授予接受邀请的权限。	Write	handshake *	-	-
organizations:handshakes:decline	授予拒绝邀请的权限。	Write	handshake *	-	-
organizations:handshakes:cancel	授予取消邀请的权限。	Write	handshake *	-	-
organizations:receivedHandshakes:list	授予列出收到的邀请的权限。	List	-	-	-
organizations:handshakes:list	授予列出发送的邀请的权	List	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限。				
organizations:trustedServices:enable	授予启用可信服务的权限。	Write	-	organizations:ServicePrincipal	-
organizations:trustedServices:disable	授予禁用受信任服务的权限。	Write	-	organizations:ServicePrincipal	-
organizations:trustedServices:list	授予列出组织的可信服务列表的权限。	List	-	-	-
organizations:delegatedAdministrators:register	授予注册作为服务委托管理员的权限。	Write	account *	g:ResourceTag/<tag-key>	-
			-	organizations:ServicePrincipal	
organizations:delegatedAdministrators:deregister	授予注销服务的委托管理员的权限。	Write	account *	g:ResourceTag/<tag-key>	-
			-	organizations:ServicePrincipal	
organizations:delegatedServices:list	授予列出指定账号是其委托管理员的服务的权限。	List	account *	g:ResourceTag/<tag-key>	-
organizations:delegatedAdministrators:list	授予列出此组织中指定为委托管理员的账号的权限。	List	-	organizations:ServicePrincipal	-
organizations:policies:create	授予创建策略的权限。	Write	-	• g:RequestTag/<tag-key> • g:TagKeys	-
organizations:policies:list	授予列出策略的权限。	List	-	-	-
organizations:policies:get	授予查询策略相关信息的权限。	Read	policy *	g:ResourceTag/<tag-key>	-
organizations:policies:update	授予更新策略的权限。	Write	policy *	g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
organizations:policies:delete	授予删除策略的权限。	Write	policy *	g:ResourceTag/<tag-key>	-
organizations:policies:enable	授予在根中启用策略类型的权限。	Write	root *	g:ResourceTag/<tag-key>	-
organizations:policies:disable	授予禁用根中的策略类型的权限。	Write	root *	g:ResourceTag/<tag-key>	-
organizations:policies:attach	授予将策略跟实体绑定的权限。	Write	policy *	g:ResourceTag/<tag-key>	-
			account	g:ResourceTag/<tag-key>	
			ou	g:ResourceTag/<tag-key>	
			root	g:ResourceTag/<tag-key>	
organizations:policies:detach	授予将策略跟实体解绑的权限。	Write	policy *	g:ResourceTag/<tag-key>	-
			account	g:ResourceTag/<tag-key>	
			ou	g:ResourceTag/<tag-key>	
			root	g:ResourceTag/<tag-key>	
organizations:attachedEntities:list	授予列出跟指定策略绑定的所有实体的权限。	List	policy *	g:ResourceTag/<tag-key>	-
organizations:tags:list	授予列出绑定到指定资源的标签的权限。	List	account	g:ResourceTag/<tag-key>	-
			ou	g:ResourceTag/<tag-key>	
			root	g:ResourceTag/<tag-key>	
			policy	g:ResourceTag/<tag-key>	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
organizations:resources:tag	授予为指定资源添加标签的权限。	Tagging	account	g:ResourceTag/<tag-key>	-
			ou	g:ResourceTag/<tag-key>	
			root	g:ResourceTag/<tag-key>	
			policy	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
organizations:resources:untag	授予从指定资源中删除指定主键标签的权限。	Tagging	account	g:ResourceTag/<tag-key>	-
			ou	g:ResourceTag/<tag-key>	
			root	g:ResourceTag/<tag-key>	
			policy	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
organizations:entities:list	授予列出组织中的根、组织单元和账号的权限。	List	-	-	-
organizations:services:list	授予列出所有可以与组织服务集成的云服务的权限。	List	-	-	-
organizations:tagPolicyServices:list	授予列出被添加到标签策略强制执行的资源类型。	List	-	-	-
organizations:effectivePolicies:	授予查询账号指定策略类型	Read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
get	的有效策略的权限。				
organizations:resources:listByTag	授予列出所有资源类型及标签信息查询实例的权限。	List	-	-	-
organizations:resources:countByTag	授予列出资源类型及标签信息查询实例数量的权限。	List	-	-	-
organizations:resources:list	授予列出项目标签的权限。	List	-	-	-
organizations:quotas:list	授予列出租户组织配额的权限。	List	-	-	-

Organizations 的 API 通常对应着一个或多个授权项。表 3-234 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-230 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/organizations	organizations:organizations:create	iam:agencies:createServiceLinkedAgency
GET /v1/organizations	organizations:organizations:get	-
DELETE /v1/organizations	organizations:organizations:delete	-
POST /v1/organizations/leave	organizations:organizations:leave	-
GET /v1/organizations/roots	organizations:roots:list	-
POST /v1/organizations/organizational-units	organizations:ous:create	organizations:resources:tag
GET	organizations:ous:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/organizations/organizational-units		
GET /v1/organizations/organizational-units/{organizational_unit_id}	organizations:ous:get	-
PATCH /v1/organizations/organizational-units/{organizational_unit_id}	organizations:ous:update	-
DELETE /v1/organizations/organizational-units/{organizational_unit_id}	organizations:ous:delete	-
POST /v1/organizations/accounts	organizations:accounts:create	organizations:resources:tag
GET /v1/organizations/accounts	organizations:accounts:list	-
GET /v1/organizations/accounts/{account_id}	organizations:accounts:get	-
POST /v1/organizations/accounts/{account_id}/remove	organizations:accounts:remove	-
POST /v1/organizations/accounts/{account_id}/move	organizations:accounts:move	-
PATCH /v1/organizations/accounts/{account_id}	organizations:accounts:update	-
POST /v1/organizations/accounts/invite	organizations:accounts:invite	organizations:resources:tag
GET /v1/organizations/create-account-status	organizations:createAccountStatuses:list	-
POST	organizations:accounts:close	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/organizations/accounts/{account_id}/close		
GET /v1/organizations/close-account-status	organizations:closeAccountStatuses:list	-
GET /v1/organizations/create-account-status/{create_account_status_id}	organizations:createAccountStatuses:get	-
GET /v1/organizations/handshakes/{handshake_id}	organizations:handshakes:get	-
POST /v1/received-handshakes/{handshake_id}/accept	organizations:handshakes:accept	iam:agencies:createServiceLinkedAgency
POST /v1/received-handshakes/{handshake_id}/decline	organizations:handshakes:decline	-
POST /v1/organizations/handshakes/{handshake_id}/cancel	organizations:handshakes:cancel	-
GET /v1/received-handshakes	organizations:receivedHandshakes:list	-
GET /v1/organizations/handshakes	organizations:handshakes:list	-
POST /v1/organizations/trusted-services/enable	organizations:trustedServices:enable	-
POST /v1/organizations/trusted-services/disable	organizations:trustedServices:disable	-
GET /v1/organizations/trusted-services	organizations:trustedServices:list	-
POST /v1/organizations/delegated-administrators/register	organizations:delegatedAdministrators:register	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/organizations/delegated-administrators/deregister	organizations:delegatedAdministrators:deregister	-
GET /v1/organizations/accounts/{account_id}/delegated-services	organizations:delegatedServices:list	-
GET /v1/organizations/delegated-administrators	organizations:delegatedAdministrators:list	-
POST /v1/organizations/policies	organizations:policies:create	organizations:resources:tag
GET /v1/organizations/policies	organizations:policies:list	-
GET /v1/organizations/policies/{policy_id}	organizations:policies:get	-
PATCH /v1/organizations/policies/{policy_id}	organizations:policies:update	-
DELETE /v1/organizations/policies/{policy_id}	organizations:policies:delete	-
POST /v1/organizations/policies/enable	organizations:policies:enable	-
POST /v1/organizations/policies/disable	organizations:policies:disable	-
POST /v1/organizations/policies/{policy_id}/attach	organizations:policies:attach	-
POST /v1/organizations/policies/{policy_id}/detach	organizations:policies:detach	-
GET /v1/organizations/policies/{policy_id}/attached-entities	organizations:attachedEntities:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/organizations/resources/{resource_id}/tags	organizations:tags:list	-
POST /v1/organizations/resources/{resource_id}/tag	organizations:resources:tag	-
POST /v1/organizations/resources/{resource_id}/untag	organizations:resources:untag	-
GET /v1/organizations/entities	organizations:entities:list	-
GET /v1/organizations/services	organizations:services:list	-
GET /v1/organizations/tag-policy-services	organizations:tagPolicyServices:list	-
GET /v1/organizations/entities/effective-policies	organizations:effectivePolicies:get	-
GET /v1/organizations/{resource_type}/{resource_id}/tags	organizations:tags:list	-
POST /v1/organizations/{resource_type}/{resource_id}/tags/create	organizations:resources:tag	-
POST /v1/organizations/{resource_type}/{resource_id}/tags/delete	organizations:resources:untag	-
POST /v1/organizations/{resource_type}/resource-instances/filter	organizations:resources:listByTag	-
POST /v1/organizations/{resource_type}/resource-instances/count	organizations:resources:countByTag	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/organizations/{resource_type}/tags	organizations:resources:list	-
GET /v1/organizations/quotas	organizations:quotas:list	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-235 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

Organizations 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-231 Organizations 支持的资源类型

资源类型	URN
builtinpolicy	organizations::system:policy:<policy-type>/<policy-id>
ou	organizations::<management-account-id>:ou:<organization-id>/<organization-unit-id>
root	organizations::<management-account-id>:root:<organization-id>/<root-id>
organization	organizations::<management-account-id>:organization:<organization-id>
account	organizations::<management-account-id>:account:<organization-id>/<account-id>
policy	organizations::<management-account-id>:policy:<organization-id>/<policy-type>/<policy-id>
handshake	organizations::<management-account-id>:handshake:<organization-id>/<handshake-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。

 版权所有 © 华为云计算技术有限公司

  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 organizations:）仅适用于对应服务的操作，详情请参见表 3-236。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

Organizations 支持的服务级条件键

Organizations 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-232 Organizations 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
organizations:ServicePrincipal	string	单值	根据指定的服务主体的名称过滤访问。

3.13.3 资源访问管理 RAM

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

 版权所有 © 华为云计算技术有限公司

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 RAM 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 RAM 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 RAM 的相关操作。

表3-233 RAM 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ram:permissions:list	授予列出 RAM 权限的权限。	List	permission *	-	-
ram:permissions:get	授予获取 RAM 权限内容的权限。	Read	permission *	-	-
ram:resourceShares:create	授予使用提供的资源和/或委托人创建资源共享的权限。	Write	-	• g:RequestTag/<tag-key> • g:TagKeys • ram:RequestedResourceType • ram:ResourceUrn • ram:Principa	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				l • ram:TargetOrgPaths • ram:RequestedAllowExternalPrincipals	
ram:resourceShares:search	授予从提供的列表获取一组资源共享，或获取具有指定状态的资源共享的权限。	Read	-	g:TagKeys	-
ram:resourceShares:update	授予更新资源共享属性的权限。	Write	resourceShare *	• g:ResourceTag/<tag-key> • ram:AllowExternalPrincipals	-
			-	ram:RequestedAllowExternalPrincipals	
ram:resourceShares:delete	授予删除资源共享的权限。	Write	resourceShare *	• g:ResourceTag/<tag-key> • ram:AllowExternalPrincipals	-
ram:resourceShares:associate	授予将资源和/或委托人与资源共享关联的权限。	Write	resourceShare *	• g:ResourceTag/<tag-key> • ram:AllowExternalPrincipals	-
			-	• ram:RequestedResourceType • ram:ResourceUrn • ram:Principal	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• ram:TargetOrgPaths	
ram:resourceShares:disassociate	授予取消资源和/或委托人与资源共享关联的权限。	Write	resourceShare *	• g:ResourceTag/<tag-key> • ram:AllowExternalPrincipals	-
			-	• ram:RequestedResourceType • ram:ResourceUrn • ram:Principal • ram:TargetOrgPaths	
ram:resourceShares:searchResourceShareAssociations	授予从提供的列表中获取一组资源共享关联，或者获取具有指定类型的指定状态的资源共享关联的权限。	Read	-	-	-
ram:resourceShares:associatePermission	授予将权限与资源共享关联的权限。	Write	resourceShare *	g:ResourceTag/<tag-key>	-
			-	ram:PermissionUrn	
ram:resourceShares:disassociatePermission	授予取消权限与资源共享关联的权限。	Write	resourceShare *	g:ResourceTag/<tag-key>	-
			-	ram:PermissionUrn	
ram:resourceShares:listAssociatedPermissions	授予列出与资源共享关联权限的权限。	List	resourceShare *	g:ResourceTag/<tag-key>	-
ram:resourceSh	授予标记指定	Taggi	resour	g:ResourceTag/	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ares:tag	资源共享的权限。	ng	ceShare *	<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
ram:resourceShares:untag	授予取消标记指定资源共享的权限。	Tagging	resourceShare *	g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
ram:resourceShares:listTags	授予查询资源共享标签的权限。	List	-	-	-
ram:resourceShares:listResourceSharesByTag	授予根据标签查询资源共享列表的权限。	List	-	g:TagKeys	-
ram:resourceShares:searchResourceShareCountByTag	授予根据标签查询资源共享数量的权限。	Read	-	g:TagKeys	-
ram:sharedResources:search	授予列出您添加到资源共享的资源或与您共享的资源的权限。	List	-	-	-
ram:sharedPrincipals:search	授予列出您与之共享资源或与您共享了资源的委托人的权限。	List	-	-	-
ram:resourceShareInvitations:accept	授予接受指定资源共享接受的权限。	Write	resourceShareInvitation *	-	-
			-	ram:ShareOwnerAccountId	
ram:resourceSh	授予拒绝指定	Write	resour	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
areInvitations:reject	资源共享邀请的权限。		ceShareInvitation *		
			-	ram:ShareOwnerAccountId	
ram:resourceShareInvitations:search	授予按指定邀请 ID 或资源共享 ID 获取资源共享邀请的权限。	Read	-	-	-
ram:resourceShares:enableSharingWithOrganization	授予开启组织资源共享的权限。	Permission_management	-	-	-
ram:resourceShares:disableSharingWithOrganization	授予关闭组织资源共享的权限。	Permission_management	-	-	-
ram:resourceShares:searchEnableSharingWithOrganization	授予查询是否开启组织资源共享的权限。	Read	-	-	-
ram:sharedResources:searchDistinctResource	授予列出您添加到资源共享的不同资源或与您共享的不同资源的权限。	List	-	-	-
ram:sharedPrincipals:searchDistinctPrincipal	授予列出您与之共享资源或与您共享了资源的不同委托人的权限。	List	-	-	-
ram:resourceShares:listQuota	授予查询资源共享配额权限。	List	-	-	-
ram:resourceTypes:list	授予查询云服务资源类型权限。	List	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ram:permission:listVersions	授予获取 RAM 指定权限所有版本的权限。	List	-	-	-

RAM 的 API 通常对应着一个或多个授权项。表 3-238 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-234 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1/permissions	ram:permissions:list	-
GET /v1/permissions/{permission_id}	ram:permissions:get	-
POST /v1/resource-shares	ram:resourceShares:create	-
POST /v1/resource-shares/search	ram:resourceShares:search	-
PUT /v1/resource-shares/{resource_share_id}	ram:resourceShares:update	-
DELETE /v1/resource-shares/{resource_share_id}	ram:resourceShares:delete	-
POST /v1/resource-shares/{resource_share_id}/associate	ram:resourceShares:associate	-
POST /v1/resource-shares/{resource_share_id}/disassociate	ram:resourceShares:disassociate	-
POST /v1/resource-share-associations/search	ram:resourceShares:searchResourceShareAssociations	-
POST /v1/resource-shares/{resource_share_id}/associate-permission	ram:resourceShares:associatePermission	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/resource-shares/{resource_share_id}/disassociate-permission	ram:resourceShares:disassociatePermission	-
GET /v1/resource-shares/{resource_share_id}/associated-permissions	ram:resourceShares:listAssociatedPermissions	-
POST /v1/resource-shares/{resource_share_id}/tags/create	ram:resourceShares:tag	-
POST /v1/resource-shares/{resource_share_id}/tags/delete	ram:resourceShares:untag	-
GET /v1/resource-shares/tags	ram:resourceShares:listTags	-
POST /v1/resource-shares/resource-instances/filter	ram:resourceShares:listResourceSharesByTag	-
POST /v1/resource-shares/resource-instances/count	ram:resourceShares:searchResourceShareCountByTag	-
POST /v1/shared-resources/search	ram:sharedResources:search	-
POST /v1/shared-principals/search	ram:sharedPrincipals:search	-
POST /v1/resource-share-invitations/{resource_share_invitation_id}/accept	ram:resourceShareInvitations:accept	-
POST /v1/resource-share-invitations/{resource_share_invitation_id}/reject	ram:resourceShareInvitations:reject	-
POST /v1/resource-share-invitations/search	ram:resourceShareInvitations:search	-
POST /v1/organization-share/enable	ram:resourceShares:enableSharingWithOrganization	-
POST	ram:resourceShares:disableSha	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/organization-share/disable	ringWithOrganization	
GET /v1/organization-share	ram:resourceShares:searchEnableSharingWithOrganization	-
POST /v1/shared-resources/search-distinct-resource	ram:sharedResources:searchDistinctResource	-
POST /v1/shared-principals/search-distinct-principal	ram:sharedPrincipals:searchDistinctPrincipal	-
GET /v1/resource-shares/quotas	ram:resourceShares:listQuota	-
GET /v1/resource-types	ram:resourceTypes:list	-
GET /v1/permissions/{permission_id}/versions	ram:permission:listVersions	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-239 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

RAM 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-235 RAM 支持的资源类型

资源类型	URN
resourceShare	ram::<account-id>:resourceShare:<resource-share-id>
resourceShareInvitation	ram::<account-id>:resourceShareInvitation:<resource-share-invitation-id>
permission	ram::system:permission:<permission-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

 版权所有 © 华为云计算技术有限公司

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 ram:）仅适用于对应服务的操作，详情请参见表 3-240。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

RAM 支持的服务级条件键

RAM 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-236 RAM 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
ram:RequestedResourceType	string	多值	根据指定的资源类型过滤访问。
ram:ResourceUrn	string	多值	根据具有指定 URN 的资源过滤访问。
ram:Principal	string	多值	根据指定使用者的格式过滤访问。
ram:TargetOrgPaths	string	多值	根据指定使用者所在的组织路径过滤访问。
ram:PermissionUrn	string	单值	根据指定的权限 URN 过滤访问。
ram:ShareOwnerAccountId	string	单值	根据拥有的资源共享的特定账号过滤访问。例如，您可以使用此条件键指定可以根据资源共享所有者的账号 ID 接受或拒绝资源共享邀请。
ram:AllowExternalPrincipals	boolean	单值	按允许或者拒绝与外部使用者共享的资源共享过滤访问。例如，如果操作只能在允许与外部

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
			使用者共享的资源共享上执行，请指定 true。外部使用者是指在其组织之外的账号。
ram:RequestedAllowExternalPrincipals	boolean	单值	根据指定的 allow_external_principals 过滤访问。外部使用者是指在其组织之外的账号。

3.13.4 IAM 身份中心

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义身份策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 IAM 身份中心定义的资源类型的详细信息请参见资源类型（Resource）。

 版权所有 © 华为云计算技术有限公司

- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 IAM 身份中心定义的条件键的详细信息请参见条件（Condition）。
- **“别名”**列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在自定义身份策略语句的 Action 元素中指定以下 IAM 身份中心的相关操作。

表3-237 IAM 身份中心支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
IdentityCenter:permissionSet:create	授予创建权限集的权限。	write	instance *	-	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	-
IdentityCenter:permissionSet:attachManagedPolicy	授予将系统身份策略添加到权限集的权限。	permission_management	instance *	-	-
			permissionSet *	-	-
IdentityCenter:permissionSet:detachManagedPolicy	授予从指定权限集中分离添加的系统身份策略的权限。	permission_management	instance *	-	-
			permissionSet *	-	-
IdentityCenter:permissionSet:update	授予更新指定实例的权限集的权限。	permission_management	instance *	-	-
			permissionSet *	-	-
IdentityCenter:permissionSet:delete	授予删除指定实例的权限集的权限。	write	instance *	-	-
			permissionSet *	-	-
IdentityCenter:permissionSet:list	授予列出指定实例的权限集的权限。	list	instance *	-	-
IdentityCenter:permissionSet:listAccountsForProvisioned	授予列出指定权限集已授权的所有账号的	list	permissionSet *	-	-
			instance *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	权限。				
IdentityCenter:permissionSet:listProvisioningStatus	授予列出指定实例的权限集授权请求的处理状态的权限。	list	instance *	-	-
IdentityCenter:permissionSet:listManagedPolicies	授予列出添加到指定权限集的系统身份策略的权限。	list	instance *	-	-
			permissionSet *	-	-
IdentityCenter:permissionSet:listProvisionedToAccount	授予列出授权给指定账号的所有权限集的权限。	list	account *	-	-
			instance *	-	-
IdentityCenter:permissionSet:describeProvisioningStatus	授予获取权限集授权请求的处理状态详细信息的权限。	read	instance *	-	-
IdentityCenter:permissionSet:describe	授予获取指定实例的权限集详细信息的权限。	read	instance *	-	-
			permissionSet *	-	-
IdentityCenter:permissionSet:provision	授予将指定权限集授权给指定目标的权限。	write	account *	-	-
			instance *	-	-
			permissionSet *	-	-
IdentityCenter:instance:getIdentityCenterStatus	授予查询 IAM 身份中心服务状态的权限。	read	-	-	-
IdentityCenter:instance:registerRegion	授予注册 region 的权限。	write	-	-	-
IdentityCenter:instance:describeRegisteredRegions	授予查询 IAM 身份中心已开通的 region 的权限。	read	-	-	-
IdentityCenter:instance:startIde	授予开通 IAM 身份中心的权	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ntityCenter	限。				
IdentityCenter:instance:deleteIdentityCenter	授予关闭 IAM 身份中心的权限。	write	-	-	-
IdentityCenter:instance:list	授予查询 IAM 身份中心实例列表的权限。	list	-	-	-
IdentityCenter:accountAssignment:create	授予使用指定权限集为指定账号分配对主体的访问权限的权限。	write	instance *	-	-
			account *	-	-
			permissionSet *	-	-
IdentityCenter:accountAssignment:delete	授予使用指定权限集从指定账号删除主体访问权限的权限。	write	instance *	-	-
			account *	-	-
			permissionSet *	-	-
IdentityCenter:accountAssignment:list	授予列出具有指定权限集的指定账号的受让人的权限。	list	instance *	-	-
			account *	-	-
			permissionSet *	-	-
IdentityCenter:accountAssignment:describeDeletionStatus	授予获取分配删除请求的处理状态详细信息的权限。	read	instance *	-	-
IdentityCenter:accountAssignment:describeCreationStatus	授予获取分配创建请求的处理状态详细信息的权限。	read	instance *	-	-
IdentityCenter:accountAssignment:listCreationStatus	授予列出指定 IAM 身份中心实例的账号分配创建请求的处理状态的权限。	list	instance *	-	-
IdentityCenter:accountAssignment:listDeletionStatus	授予列出指定 IAM 身份中心实例的账号分	list	instance *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	配删除请求的处理状态的权限。				
IdentityCenter:accountAssignment:listProfileAssociation	授予查询账号、权限集关联的所有用户或用户组的权限。	read	-	-	-
IdentityCenter:accountAssignment:disassociationProfile	授予解除用户或用户组绑定的所有授权的权限。	write	-	-	-
IdentityCenter:instance:listIdentityStoreAssociations	授予查询关联到 IAM 身份中心的身份源详细信息的权限。	read	-	-	-
IdentityCenter:ssoConfiguration:update	授予更新当前 IAM 身份中心实例配置的权限。	write	-	-	-
IdentityCenter:ssoConfiguration:describe	授予获取当前 IAM 身份中心实例配置的权限。	read	-	-	-
IdentityCenter:mfaDevices:describeManagementSettings	授予获取 MFA 管理设置信息的权限。	read	-	-	-
IdentityCenter:mfaDevices:updateManagementSettings	授予更新 MFA 管理设置信息的权限。	write	-	-	-
IdentityCenter:instance:createAlias	授予为指定的身份源创建别名的权限。	write	-	-	-
IdentityCenter:user:create	授予创建用户的权限。	write	-	-	-
IdentityCenter:user:list	授予查询用户	read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	列表的权限。				
IdentityCenter:user:describe	授予查询用户详情的权限。	read	-	-	-
IdentityCenter:user:describeUsers	授予批量获取用户详情的权限。	read	-	-	-
IdentityCenter:user:update	授予更新用户的权限。	write	-	-	-
IdentityCenter:user:delete	授予删除用户的权限。	write	-	-	-
IdentityCenter:user:getUserId	授予获取用户 ID 的权限。	read	-	-	-
IdentityCenter:user:enableUser	授予启用用户的权限。	write	-	-	-
IdentityCenter:user:disableUser	授予停用用户的权限。	write	-	-	-
IdentityCenter:group:create	授予创建用户组的权限。	write	-	-	-
IdentityCenter:group:list	授予查询用户组列表的权限。	read	-	-	-
IdentityCenter:group:describe	授予查询用户组详情的权限。	read	-	-	-
IdentityCenter:group:describeGroups	授予批量获取用户组详情的权限。	read	-	-	-
IdentityCenter:group:update	授予更新用户组的权限。	write	-	-	-
IdentityCenter:group:delete	授予删除用户组的权限。	write	-	-	-
IdentityCenter:group:getGroupId	授予获取用户组 Id 的权限。	read	-	-	-
IdentityCenter:	授予绑定用户	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
groupMembership:create	与用户组的权限。				
IdentityCenter:groupMemberships:list	授予查询用户组的所有成员的权限。	read	-	-	-
IdentityCenter:groupMembership:listForMember	授予查询用户加入的所有用户组的权限。	read	-	-	-
IdentityCenter:groupMembership:describe	授予查询绑定关系详情的权限。	read	-	-	-
IdentityCenter:groupMembership:delete	授予解绑用户和用户组的权限。	write	-	-	-
IdentityCenter:groupMembership:getGroupMembershipId	授予查询绑定关系 ID 的权限。	read	-	-	-
IdentityCenter:groupMembership:isMembershipInGroup	授予查询用户是否绑定在用户组的权限。	read	-	-	-
IdentityCenter:externalIdp:create	授予创建外部身份提供商的权限。	write	-	-	-
IdentityCenter:externalIdp:list	授予获取外部身份提供商身份源配置的权限。	read	-	-	-
IdentityCenter:externalIdp:enable	授予启用外部身份提供商的权限。	write	-	-	-
IdentityCenter:externalIdp:disable	授予停用外部身份提供商的权限。	write	-	-	-
IdentityCenter:externalIdp:getSpConfiguration	授予获取 IAM 身份中心服务提供商配置的	read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	权限。				
IdentityCenter:externalIdp:update	授予更新外部身份提供商配置的权限。	write	-	-	-
IdentityCenter:externalIdp:delete	授予删除外部身份提供商配置的权限。	write	-	-	-
IdentityCenter:externalIdp:importCertificate	授予导入证书的权限。	write	-	-	-
IdentityCenter:externalIdp:deleteCertificate	授予删除证书的权限。	write	-	-	-
IdentityCenter:externalIdp:listCertificates	授予获取证书列表的权限。	read	-	-	-
IdentityCenter:externalIdp:createProvisioningTenant	授予创建 Tenant 的权限。	write	-	-	-
IdentityCenter:externalIdp:listProvisioningTenant	授予查询 Tenant 列表的权限。	read	-	-	-
IdentityCenter:externalIdp:deleteProvisioningTenant	授予删除 Tenant 的权限。	write	-	-	-
IdentityCenter:externalIdp:createBearerToken	授予创建 Bearer Token 的权限。	write	-	-	-
IdentityCenter:externalIdp:listBearerTokens	授予查询 Bearer Token 列表的权限。	read	-	-	-
IdentityCenter:externalIdp:deleteBearerToken	授予删除 Bearer Token 的权限。	write	-	-	-
IdentityCenter:user:updatePassword	授予通过电子邮件发送密码重置链接或者	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	生成一次性密码的方式为用户更新密码的权限。				
IdentityCenter:user:deleteUserMfaDevice	授予为指定用户删除 MFA 设备的权限。	write	-	-	-
IdentityCenter:user:updateMfaDevice	授予更新 MFA 设备信息的权限。	write	-	-	-
IdentityCenter:user:listMfaDevice	授予查询 MFA 设备列表的权限。	read	-	-	-
IdentityCenter:user:registerVirtualMfaDevice	授予开始虚拟 MFA 设备创建过程的权限。	write	-	-	-
IdentityCenter:user:verifyEmail	授予验证用户电子邮件地址的权限。	write	-	-	-

IAM 身份中心的 API 通常对应着一个或多个授权项。表 3-242 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-238 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/instances/{instance_id}/permission-sets	IdentityCenter:permissionSet:create	organizations:delegatedAdministrators:list
POST /v1/instances/{instance_id}/permission-sets/{permission_set_id}/attach-managed-policy	IdentityCenter:permissionSet:attachManagedPolicy	• iam:policies:get • organizations:delegatedAdministrators:list
POST /v1/instances/{instance_id}/permission-sets/{permission_set_id}/detach-managed-policy	IdentityCenter:permissionSet:detachManagedPolicy	organizations:delegatedAdministrators:list
PUT	IdentityCenter:permissionSe	organizations:delegatedAdm

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/instances/{instance_id}/permission-sets/{permission_set_id}	t:update	inistrators:list
DELETE /v1/instances/{instance_id}/permission-sets/{permission_set_id}	IdentityCenter:permissionSet:delete	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/permission-sets	IdentityCenter:permissionSet:list	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}/accounts	IdentityCenter:permissionSet:listAccountsForProvisioned	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/permission-sets/provisioning-statuses	IdentityCenter:permissionSet:listProvisioningStatus	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}/managed-policies	IdentityCenter:permissionSet:listManagedPolicies	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/permission-sets/provisioned-to-accounts	IdentityCenter:permissionSet:listProvisionedToAccount	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/permission-sets/provisioning-status/{request_id}	IdentityCenter:permissionSet:describeProvisioningStatus	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}	IdentityCenter:permissionSet:describe	organizations:delegatedAdministrators:list
POST /v1/instances/{instance_id}/permission-sets/{permission_set_id}/provision	IdentityCenter:permissionSet:provision	organizations:delegatedAdministrators:list
GET /v1/instances	IdentityCenter:instance:list	organizations:delegatedAdministrators:list
POST	IdentityCenter:accountAssig	organizations:delegatedAdm

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/instances/{instance_id}/account-assignments/create	nment:create	inistrators:list
POST /v1/instances/{instance_id}/account-assignments/delete	IdentityCenter:accountAssignment:delete	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/account-assignments	IdentityCenter:accountAssignment:list	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/account-assignments/deletion-status/{request_id}	IdentityCenter:accountAssignment:describeDeletionStatus	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/account-assignments/creation-status/{request_id}	IdentityCenter:accountAssignment:describeCreationStatus	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/account-assignments/creation-statuses	IdentityCenter:accountAssignment:listCreationStatus	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/account-assignments/deletion-statuses	IdentityCenter:accountAssignment:listDeletionStatus	organizations:delegatedAdministrators:list
POST /v1/identity-stores/{identity_store_id}/users	IdentityCenter:user:create	organizations:delegatedAdministrators:list
GET /v1/identity-stores/{identity_store_id}/users	IdentityCenter:user:list	organizations:delegatedAdministrators:list
GET /v1/identity-stores/{identity_store_id}/users/{user_id}	IdentityCenter:user:describe	organizations:delegatedAdministrators:list
PUT /v1/identity-stores/{identity_store_id}/users/{user_id}	IdentityCenter:user:update	organizations:delegatedAdministrators:list
DELETE /v1/identity-stores/{identity_store_id}/users/{user_id}	IdentityCenter:user:delete	organizations:delegatedAdministrators:list
POST /v1/identity-	IdentityCenter:user:getUserI	organizations:delegatedAdm

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
stores/{identity_store_id}/users/retrieve-user-id	d	inistrators:list
POST /v1/identity-stores/{identity_store_id}/groups	IdentityCenter:group:create	organizations:delegatedAdministrators:list
GET /v1/identity-stores/{identity_store_id}/groups	IdentityCenter:group:list	organizations:delegatedAdministrators:list
GET /v1/identity-stores/{identity_store_id}/groups/{group_id}	IdentityCenter:group:describe	organizations:delegatedAdministrators:list
PUT /v1/identity-stores/{identity_store_id}/groups/{group_id}	IdentityCenter:group:update	organizations:delegatedAdministrators:list
DELETE /v1/identity-stores/{identity_store_id}/groups/{group_id}	IdentityCenter:group:delete	organizations:delegatedAdministrators:list
POST /v1/identity-stores/{identity_store_id}/groups/retrieve-group-id	IdentityCenter:group:getGroupId	organizations:delegatedAdministrators:list
POST /v1/identity-stores/{identity_store_id}/group-memberships	IdentityCenter:groupMembership:create	organizations:delegatedAdministrators:list
GET /v1/identity-stores/{identity_store_id}/group-memberships	IdentityCenter:groupMemberships:list	organizations:delegatedAdministrators:list
GET /v1/identity-stores/{identity_store_id}/group-memberships-for-member	IdentityCenter:groupMembership:listForMember	organizations:delegatedAdministrators:list
GET /v1/identity-stores/{identity_store_id}/group-memberships/{membership_id}	IdentityCenter:groupMembership:describe	organizations:delegatedAdministrators:list
DELETE /v1/identity-stores/{identity_store_id}/group-memberships/{membership_id}	IdentityCenter:groupMembership:delete	organizations:delegatedAdministrators:list
POST /v1/identity-stores/{identity_store_id}/group-memberships/retrieve-group-membership-id	IdentityCenter:groupMembership:getGroupMembershipId	organizations:delegatedAdministrators:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/identity-stores/{identity_store_id}/is-member-in-groups	IdentityCenter:groupMembership:isMembershipInGroup	organizations:delegatedAdministrators:list

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-243 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的策略语句中指定该资源的 URN，策略仅作用于此资源；如未指定，Resource 默认为“*”，则策略将应用到所有资源。您也可以在策略中设置条件，从而指定资源类型。

IAM 身份中心定义了以下可以在策略的 Resource 元素中使用的资源类型。

表3-239 IAM 身份中心支持的资源类型

资源类型	URN
instance	IdentityCenter::<management-account-id>:instance:<instance-id>
account	IdentityCenter::<management-account-id>:account:<account-id>
permissionSet	IdentityCenter::<management-account-id>:permissionSet:<instance-id>/<permission-set-id>

条件（Condition）

IAM 身份中心服务不支持在身份策略中的条件键中配置服务级的条件键。

IAM 身份中心可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.13.5 配置审计 Config

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

 版权所有 © 华为云计算技术有限公司

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 Config 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 Config 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 Config 的相关操作。

表3-240 Config 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rms:organizationConformancePacks:create	授予权限创建组织合规规则包。	Write	-	-	-
rms:organizationConformancePacks:get	授予权限查看组织合规规则包。	Read	organizationConformancePacks *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rms:organizationConformancePacks:delete	授予权限删除组织合规规则包。	Write	organizationConformancePacks *	-	-
rms:organizationConformancePacks:update	授予权限更新组织合规规则包。	Write	organizationConformancePacks *	-	-
rms:organizationConformancePacks:list	授予权限查询组织合规规则包列表。	List	-	-	-
rms:conformancePacks:create	授予权限创建合规规则包。	Write	-	-	-
rms:conformancePacks:get	授予权限查看合规规则包。	Read	conformancePacks *	-	-
rms:conformancePacks:delete	授予权限删除合规规则包。	Write	conformancePacks *	-	-
rms:conformancePacks:update	授予权限更新合规规则包。	Write	conformancePacks *	-	-
rms:conformancePacks:list	授予权限查询合规规则包列表。	List	-	-	-
rms:storedQueries:create	授予权限保存新的高级查询语句。	Write	-	-	-
rms:storedQueries:update	授予权限更新已存在的高级查询语句。	Write	storedQueries *	-	-
rms:storedQueri	授予权限删除	Write	stored	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
es:delete	已存在的高级查询语句。		Queries *		
rms:storedQueries:get	授予权限查看已存在的高级查询语句详情。	Read	storedQueries *	-	-
rms:storedQueries:list	授予权限查看已存在的高级查询语句列表。	List	-	-	-
rms:policyAssignments:create	授予权限创建新的合规规则以评估你的资源。	Write	-	• g:TagKeys • g:RequestTag/<tag-key>	-
rms:policyAssignments:update	授予权限更新已存在的合规规则以评估你的资源。	Write	policyAssignments *	g:ResourceTag/<tag-key>	-
			-	• g:TagKeys • g:RequestTag/<tag-key>	
rms:policyAssignments:delete	授予权限删除已存在的合规规则和相应的评估状态结果。	Write	policyAssignments *	g:ResourceTag/<tag-key>	-
rms:policyAssignments:get	授予权限查看已存在的合规规则详情。	Read	policyAssignments *	g:ResourceTag/<tag-key>	-
rms:organizationPolicyAssignments:put	授予权限对整个组织创建或更新合规规则以评估你的资源。	Write	-	-	-
rms:organizationPolicyAssignments:delete	授予权限删除指定的组织合规规则和组织	Write	organizationPolicyAssig	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	内所有成员账号的合规评估状态结果。		nments *		
rms:organizationPolicyAssignments:get	授予权限查看组织合规规则详情。	Read	organizationPolicyAssignments *	-	-
rms:organizationPolicyAssignments:list	授予权限查看组织合规规则列表。	List	-	-	-
rms:policyStates:runEvaluation	授予权限运行指定的合规规则以评估你的资源。	Write	policyAssignments	g:ResourceTag/<tag-key>	-
rms:policyStates:update	授予权限FunctionGraph函数将评估结果传输到Config。	Write	-	-	-
rms:aggregators:create	授予权限创建聚合器聚合指定租户资源。	Write	-	-	-
rms:aggregators:update	授予权限更新已存在的聚合器。	Write	aggregators *	-	-
rms:aggregators:delete	授予权限删除指定聚合器并删除被聚合的租户资源。	Write	aggregators *	-	-
rms:aggregators:list	授予权限查看已存在的聚合器列表。	List	-	-	-
rms:aggregators:get	授予权限查看已存在的聚合器详情。	Read	aggregators *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rms:aggregatorResources:list	授予权限查看已被聚合的资源。	List	-	-	-
rms:aggregatorResources:runQuery	授予权限执行高级查询语句返回被聚合的资源属性。	List	-	-	-
rms:aggregatorResources:get	授予权限查看用户指定被聚合的资源详情。	Read	-	-	-
rms:aggregationAuthorizations:create	授予权限创建聚合授权。	Write	aggregationAuthorizations *	-	-
			-	rms:AuthorizedAccountOrgPath	
rms:aggregationAuthorizations:list	授予权限查看已存在的聚合授权列表。	List	-	-	-
rms:aggregationAuthorizations:delete	授予权限删除已存在聚合授权并删除被聚合的租户资源。	Write	aggregationAuthorizations *	-	-
			-	rms:AuthorizedAccountOrgPath	
rms:aggregationRequests:delete	授予权限删除来自其他账号的聚合请求。	Write	-	-	-
rms:aggregationRequests:list	授予权限查看来自其他账号的聚合请求列表。	List	-	-	-
rms:trackerCon	授予权限创建	Write	-	• rms:Tracker	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
fig:put	或更新资源记录器配置以记录指定资源类型的资源历史数据。			BucketName • rms:TrackerBucketPathPrefix	
rms:trackerConfig:delete	授予权限删除资源记录器配置以停止记录指定资源类型的资源历史数据。	Write	-	-	-
rms:trackerConfig:get	授予权限查看资源记录器配置。	Read	-	-	-
rms:schemas:list	授予权限查看高级查询资源Schema。	List	-	-	-
rms:policyDefinitions:get	授予权限查看预定义合规策略。	List	-	-	-
rms:resources:getHistory	授予权限查看指定资源的历史配置数据。	List	-	-	-
rms:resources:getRelation	授予权限查看资源关系。	List	-	-	-
rms:resources:get	授予权限查看用户指定的资源详情。	Read	-	-	-
rms:resources:list	授予权限查看用户所有的资源列表。	List	-	-	-
rms:resources:runQuery	授予权限执行高级查询语句。	List	-	-	-
rms::tagResource	授予权限批量创建资源标	Tagging	policyAssignment	g:ResourceTag/<tag-key>	rms:resources:tagResource

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	签。		s		
			-	• g:RequestTag/<tag-key> • g:TagKeys	
rms::unTagResource	授予权限批量删除资源标签。	Tagging	policyAssignments	g:ResourceTag/<tag-key>	rms:resources:unTagResource
			-	• g:RequestTag/<tag-key> • g:TagKeys	
rms::listTagsForResource	授予权限查询资源标签。	List	policyAssignments	g:ResourceTag/<tag-key>	rms:resources:listTagsForResource
rms::listTags	授予权限查询项目标签。	List	-	-	rms:resources:listTags
rms::listResourcesByTag	授予权限查询资源实例。	List	-	g:TagKeys	rms:resources:listResourcesByTag
rms:policyAssignmentsRemediation:putRemediationConfiguration	授予权限创建合规修正配置。	Write	policyAssignmentsRemediation *	-	-
rms:policyAssignmentsRemediation:deleteRemediationConfiguration	授予权限删除合规修正配置。	Write	policyAssignmentsRemediation *	-	-
rms:policyAssignmentsRemediation:getRemediationConfiguration	授予权限查看合规修正配置。	Read	policyAssignmentsRemediation *	-	-
rms:policyAssignmentsRemedi	授予权限执行合规修正配	Write	policyAssig	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ation:runRemediation	置。		nmentsRemediation *		
rms:policyAssignmentsRemediation:listRemediationExecutionStatuses	授予权限查看合规修正执行状态。	List	policyAssignmentsRemediation *	-	-
rms:policyAssignmentsRemediation:createRemediationExceptions	授予权限创建合规修正例外。	Write	policyAssignmentsRemediation *	-	-
rms:policyAssignmentsRemediation:deleteRemediationExceptions	授予权限删除合规修正例外。	Write	policyAssignmentsRemediation *	-	-
rms:policyAssignmentsRemediation:listRemediationExceptions	授予权限查看合规修正例外。	List	policyAssignmentsRemediation *	-	-

Config 的 API 通常对应着一个或多个授权项。表 3-245 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-241 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/resource-manager/organizations/{organization_id}/conformance-packs	rms:organizationConformancePacks:create	• organizations:organizations:get • organizations:accounts:list • organizations:delegatedAdministrators:list • organizations:trustedServic

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
		es:enable • organizations:trustedServices:list
DELETE /v1/resource-manager/organizations/{organization_id}/conformance-packs/{conformance_pack_id}	rms:organizationConformancePacks:delete	organizations:organizations:get
PUT /v1/resource-manager/organizations/{organization_id}/conformance-packs/{conformance_pack_id}	rms:organizationConformancePacks:update	• organizations:organizations:get • organizations:accounts:list • organizations:delegatedAdministrators:list • organizations:trustedServices:enable • organizations:trustedServices:list
GET /v1/resource-manager/organizations/{organization_id}/conformance-packs	rms:organizationConformancePacks:list	organizations:organizations:get
GET /v1/resource-manager/organizations/{organization_id}/conformance-packs/{conformance_pack_id}	rms:organizationConformancePacks:get	organizations:organizations:get
GET /v1/resource-manager/organizations/{organization_id}/conformance-packs/statuses	rms:organizationConformancePacks:list	organizations:organizations:get
GET /v1/resource-manager/organizations/{organization_id}/conformance-packs/detailed-statuses	rms:organizationConformancePacks:get	organizations:organizations:get
POST /v1/resource-manager/domains/{domain_id}/conformance-packs	rms:conformancePacks:create	• rf:stack:createStack • rf:stack:getStackMetadata • rf:stack:listStackResources
DELETE /v1/resource-manager/domains/{do	rms:conformancePacks:delete	• rf:stack:deleteStack • rf:stack:getStackMetadata

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
main_id}/conformance-packs/{conformance_pack_id}		
PUT /v1/resource-manager/domains/{domain_id}/conformance-packs/{conformance_pack_id}	rms:conformancePacks:update	• rf:stack:deployStack • rf:stack:getStackMetadata • rf:stack:listStackResources
GET /v1/resource-manager/domains/{domain_id}/conformance-packs/{conformance_pack_id}	rms:conformancePacks:get	-
GET /v1/resource-manager/domains/{domain_id}/conformance-packs/{conformance_pack_id}/compliance	rms:conformancePacks:get	-
GET /v1/resource-manager/domains/{domain_id}/conformance-packs/{conformance_pack_id}/compliance/details	rms:conformancePacks:get	-
GET /v1/resource-manager/domains/{domain_id}/conformance-packs	rms:conformancePacks:list	-
GET /v1/resource-manager/domains/{domain_id}/conformance-packs/compliance/summary	rms:conformancePacks:list	-
GET /v1/resource-manager/domains/{domain_id}/conformance-packs/scores	rms:conformancePacks:list	-
POST /v1/resource-manager/domains/{domain_id}/stored-queries	rms:storedQueries:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v1/resource-manager/domains/{domain_id}/stored-queries/{query_id}	rms:storedQueries:update	-
DELETE /v1/resource-manager/domains/{domain_id}/stored-queries/{query_id}	rms:storedQueries:delete	-
GET /v1/resource-manager/domains/{domain_id}/stored-queries/{query_id}	rms:storedQueries:get	-
GET /v1/resource-manager/domains/{domain_id}/stored-queries	rms:storedQueries:list	-
PUT /v1/resource-manager/domains/{domain_id}/policy-assignments	rms:policyAssignments:create	-
DELETE /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}	rms:policyAssignments:delete	-
GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}	rms:policyAssignments:get	-
GET /v1/resource-manager/domains/{domain_id}/policy-assignments	rms:policyAssignments:get	-
PUT /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}	rms:policyAssignments:update	-
POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/disable	rms:policyAssignments:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/enable	rms:policyAssignments:update	-
PUT /v1/resource-manager/organizations/{organization_id}/policy-assignments	rms:organizationPolicyAssignments:put	• organizations:organizations:get • organizations:accounts:list • organizations:delegatedAdministrators:list • organizations:trustedServices:enable • organizations:trustedServices:list
GET /v1/resource-manager/organizations/{organization_id}/policy-assignments	rms:organizationPolicyAssignments:list	organizations:organizations:get
GET /v1/resource-manager/organizations/{organization_id}/policy-assignments/{organization_policy_assignment_id}	rms:organizationPolicyAssignments:get	organizations:organizations:get
GET /v1/resource-manager/organizations/{organization_id}/policy-assignment-statuses	rms:organizationPolicyAssignments:list	organizations:organizations:get
GET /v1/resource-manager/organizations/{organization_id}/policy-assignment-detailed-status	rms:organizationPolicyAssignments:list	organizations:organizations:get
DELETE /v1/resource-manager/organizations/{organization_id}/policy-assignments/{organization_policy_assignment_id}	rms:organizationPolicyAssignments:delete	organizations:organizations:get
GET /v1/resource-manager/domains/{domain_id}/policy-	rms:policyStates:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
assignments/{policy_assignment_id}/policy-states		
GET /v1/resource-manager/domains/{domain_id}/policy-states	rms:policyStates:get	-
GET /v1/resource-manager/domains/{domain_id}/resources/{resource_id}/policy-states	rms:policyStates:get	-
POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/policy-states/run-evaluation	rms:policyStates:runEvaluation	-
GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/policy-states/evaluation-state	rms:policyStates:get	-
PUT /v1/resource-manager/domains/{domain_id}/policy-states	rms:policyStates:update	-
PUT /v1/resource-manager/domains/{domain_id}/aggregators	rms:aggregators:create	• organizations:organizations:get • organizations:accounts:list • organizations:delegatedAdministrators:list • organizations:trustedServices:enable • organizations:trustedServices:list
PUT /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}	rms:aggregators:update	• organizations:organizations:get • organizations:accounts:list • organizations:delegatedAdministrators:list • organizations:trustedServices:enable • organizations:trustedServices:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}	rms:aggregators:delete	-
GET /v1/resource-manager/domains/{domain_id}/aggregators	rms:aggregators:list	-
GET /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}	rms:aggregators:get	-
GET /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}/aggregator-sources-status	rms:aggregators:get	-
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-states/compliance-summary	rms:aggregatorResources:list	• organizations:organizations:get • organizations:delegatedAdministrators:list • organizations:trustedServices:list
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-assignments/compliance	rms:aggregatorResources:list	• organizations:organizations:get • organizations:delegatedAdministrators:list • organizations:trustedServices:list
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-states/compliance-details	rms:aggregatorResources:list	• organizations:organizations:get • organizations:delegatedAdministrators:list • organizations:trustedServices:list
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-assignment/detail	rms:aggregatorResources:list	• organizations:organizations:get • organizations:delegatedAdministrators:list • organizations:trustedServices:list
POST /v1/resource-manager/domains/{domain_id}/aggregators/	rms:aggregatorResources:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
aggregate-resource-config		
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/aggregate-discovered-resources	rms:aggregatorResources:list	• organizations:organizations:get • organizations:delegatedAdministrators:list • organizations:trustedServices:list
POST /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}/run-query	rms:aggregatorResources:runQuery	-
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/aggregate-discovered-resource-counts	rms:aggregatorResources:list	• organizations:organizations:get • organizations:delegatedAdministrators:list • organizations:trustedServices:list
GET /v1/resource-manager/domains/{domain_id}/aggregators/aggregation-authorization	rms:aggregationAuthorizations:list	-
PUT /v1/resource-manager/domains/{domain_id}/aggregators/aggregation-authorization	rms:aggregationAuthorizations:create	-
DELETE /v1/resource-manager/domains/{domain_id}/aggregators/aggregation-authorization/{authorized_account_id}	rms:aggregationAuthorizations:delete	-
DELETE /v1/resource-manager/domains/{domain_id}/aggregators/pending-aggregation-request/{requester_account_id}	rms:aggregationRequests:delete	-
GET /v1/resource-manager/domains/{domain_id}/aggregators/	rms:aggregationRequests:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
pending-aggregation-request		
PUT /v1/resource-manager/domains/{domain_id}/tracker-config	rms:trackerConfig:put	-
DELETE /v1/resource-manager/domains/{domain_id}/tracker-config	rms:trackerConfig:delete	-
GET /v1/resource-manager/domains/{domain_id}/tracker-config	rms:trackerConfig:get	-
GET /v1/resource-manager/domains/{domain_id}/schemas	rms:schemas:list	-
GET /v1/resource-manager/policy-definitions	rms:policyDefinitions:get	-
GET /v1/resource-manager/policy-definitions/{policy_definition_id}	rms:policyDefinitions:get	-
GET /v1/resource-manager/domains/{domain_id}/resources/{resource_id}/history	rms:resources:getHistory	-
GET /v1/resource-manager/domains/{domain_id}/all-resources/{resource_id}/relations	rms:resources:getRelation	-
GET /v1/resource-manager/domains/{domain_id}/provider/{provider}/type/{type}/resources/{resource_id}	rms:resources:get	-
GET /v1/resource-manager/domains/{domain_id}/all-resources	rms:resources:list	-
GET /v1/resource-manager/domains/{domain_id}/provider/{pr	rms:resources:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ovider}/type/{type}/resources		
POST /v1/resource-manager/domains/{domain_id}/run-query	rms:resources:runQuery	-
GET /v1/resource-manager/domains/{domain_id}/all-resources/summary	rms:resources:list	-
GET /v1/resource-manager/domains/{domain_id}/all-resources/tags	rms:resources:list	-
GET /v1/resource-manager/domains/{domain_id}/all-resources/count	rms:resources:list	-
GET /v1/resource-manager/domains/{domain_id}/all-resources/{resource_id}	rms:resources:get	-
GET /v1/resource-manager/domains/{domain_id}/resources/{resource_id}/relations	rms:resources:summarize	-
POST /v1/resource-manager/{resource_type}/{resource_id}/tags/create	rms::tagResource	-
POST /v1/resource-manager/{resource_type}/{resource_id}/tags/delete	rms::unTagResource	-
GET /v1/resource-manager/{resource_type}/{resource_id}/tags	rms::listTagsForResource	-
GET /v1/resource-manager/{resource_type}/tags	rms::listTags	-
POST /v1/resource-manager/{resource_type}/resource-instances/count	rms::listResourcesByTag	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/resource-manager/{resource_type}/resource-instances/filter	rms::listResourcesByTag	-
PUT /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-configuration	rms:policyAssignmentsRemediation:putRemediationConfiguration	• iam:agencies:pass • iam:agencies:createServiceLinkedAgencyV5
DELETE /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-configuration	rms:policyAssignmentsRemediation:deleteRemediationConfiguration	-
GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-configuration	rms:policyAssignmentsRemediation:getRemediationConfiguration	-
POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-execution	rms:policyAssignmentsRemediation:runRemediation	• functiongraph:function:invokeAsync • functiongraph:function:getFunctionConfig • rf:stack:create • rf:stack:delete • rf:stack:getTemplate • rf:stack:getMetadata • rf:privateTemplate:showMetadata
GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-execution-statuses	rms:policyAssignmentsRemediation:listRemediationExecutionStatuses	-
POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-execution-	rms:policyAssignmentsRemediation:listRemediationExecutionStatuses	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
statuses/summary		
POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-exception/create	rms:policyAssignmentsRemediation:createRemediationExceptions	-
POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-exception/delete	rms:policyAssignmentsRemediation:deleteRemediationExceptions	-
GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-exception	rms:policyAssignmentsRemediation:listRemediationExceptions	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-246 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

Config 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-242 Config 支持的资源类型

资源类型	URN
policyAssignments	rms::<account-id>:policyAssignments:<policy-assignment-id>
aggregationAuthorizations	rms::<account-id>:aggregationAuthorizations:<authorized-account-id>
policyAssignmentsRemediation	rms::<account-id>:policyAssignmentsRemediation:<policy-assignment-id>
aggregators	rms::<account-id>:aggregators:<aggregator-id>
organizationConformancePacks	rms::<account-id>:organizationConformancePacks:<organization-id>/<organization-conformance-pack-id>
conformancePacks	rms::<account-id>:conformancePacks:<conformance-pack-id>
storedQueries	rms::<account-id>:storedQueries:<query-id>

 版权所有 © 华为云计算技术有限公司

资源类型	URN
organizationPolicyAssignments	rms::<account-id>:organizationPolicyAssignments:<organization-id>/<organization-policy-assignments-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 config:）仅适用于对应服务的操作，详情请参见表 3-247。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

Config 支持的服务级条件键

Config 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-243 Config 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
rms:AuthorizedAccountOrgPath	string	单值	根据指定的资源聚合授权账号的 Organizations Path 过滤访问。
rms:TrackerBucketName	string	单值	根据指定的转储目标桶名称进行过滤访问。
rms:TrackerBucketPathPrefix	string	单值	根据指定的转储目标桶桶前缀进行过滤访问。

条件键示例

 版权所有 © 华为云计算技术有限公司

- rms:AuthorizedAccountOrgPath

  示例：禁止组织内账号给组织外的账号进行聚合授权。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "rms:aggregationAuthorizations:create"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotMatch": {
          "rms:AuthorizedAccountOrgPath": [
            "organization_id/root_id/ou_id"【备注：此处需填写组织的路径 ID】
          ]
        }
      }
    }
  ]
}
```

- rms:TrackerBucketName

  示例：禁止资源记录器转储到非预期的 OBS 桶。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "rms:trackerConfig:put"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotMatch": {
          "rms:TrackerBucketName": [
            "BucketName"
          ]
        }
      }
    }
  ]
}
```

- rms:TrackerBucketPathPrefix

  示例：禁止资源记录器转储到非预期的 OBS 路径下。

```
{
  "Version": "5.0",
  "Statement": [
    {
```

 版权所有 © 华为云计算技术有限公司

```
      "Effect": "Deny",
      "Action": [
        "rms:trackerConfig:put"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotMatch": {
          "rms:TrackerBucketPathPrefix": [
            "BucketFolder"
          ]
        }
      }
    }
  ]
}
```

3.13.6 标签管理服务 TMS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。

 版权所有 © 华为云计算技术有限公司

- 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

关于 TMS 定义的资源类型的详细信息请参见资源类型（Resource）。

- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 TMS 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 TMS 的相关操作。

表3-244 TMS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
tms:predefineTags:create	授予权限以创建预定义标签。	Write	-	-	-
tms:predefineTags:update	授予权限以更新预定义标签。	Write	-	-	-
tms:predefineTags:delete	授予权限以删除预定义标签。	Write	-	-	-

TMS 的 API 通常对应着一个或多个授权项。表 3-249 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-245 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1.0/predefine_tags/action	tms:predefineTags:create	-
PUT /v1.0/predefine_tags	tms:predefineTags:update	-
POST 01 /v1.0/predefine_tags/a	tms:predefineTags:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ction		

资源类型（Resource）

TMS 服务不支持在身份策略中的资源中指定资源进行权限控制。如需允许访问 TMS 服务，请在身份策略的 Resource 元素中使用通配符号*，表示身份策略将应用到所有资源。

条件（Condition）

TMS 服务不支持在身份策略中的条件键中配置服务级的条件键。TMS 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.13.7 企业管理 EPS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。

 版权所有 © 华为云计算技术有限公司

- 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

关于 EPS 定义的资源类型的详细信息请参见资源类型（Resource）。

- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 EPS 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 EPS 的相关操作。

表3-246 EPS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
eps:enterpriseProjects:list	授予权限以查看企业项目列表。	List	enterpriseProject *	-	-
eps:enterpriseProjects:create	授予权限以创建企业项目。	Write	enterpriseProject *	-	-
eps:enterpriseProjects:update	授予权限以修改企业项目。	Write	enterpriseProject *	-	-
eps:enterpriseProjects:enable	授予权限以启用企业项目。	Write	enterpriseProject *	-	-
eps:enterpriseProjects:disable	授予权限以停用企业项目。	Write	enterpriseProject *	-	-
eps:enterpriseProjects:delete	授予权限以删除企业项目。	Write	enterpriseProject *	-	-
eps:resources:list	授予权限以查看企业项目资源列表。	List	enterpriseProject *	-	-
eps:resources:add	授予权限将资源迁入至企业项目。	Write	enterpriseProject *	-	-

 版权所有 © 华为云计算技术有限公司

EPS 的 API 通常对应着一个或多个授权项。表 3-251 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-247 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1.0/enterprise-projects	eps:enterpriseProjects:list	-
POST /v1.0/enterprise-projects	eps:enterpriseProjects:create	-
PUT /v1.0/enterprise-projects/{enterprise_project_id}	eps:enterpriseProjects:update	-
POST /v1.0/enterprise-projects/{enterprise_project_id}/action	eps:enterpriseProjects:enable	-
POST 01 /v1.0/enterprise-projects/{enterprise_project_id}/action	eps:enterpriseProjects:disable	-
DELETE /v1.0/enterprise-projects/{enterprise_project_id}	eps:enterpriseProjects:delete	-
POST /v1.0/enterprise-projects/{enterprise_project_id}/resources/filter	eps:resources:list	-
POST /v1.0/enterprise-projects/{enterprise_project_id}/resources-migrate	eps:resources:add	eps:resources:remove

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-252 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的 URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

EPS 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

 版权所有 © 华为云计算技术有限公司

表3-248 EPS 支持的资源类型

资源类型	URN
enterpriseProject	eps::<account-id>:enterpriseProject:<enterprise-project-id>

条件（Condition）

EPS 服务不支持在身份策略中的条件键中配置服务级的条件键。EPS 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.13.8 云监控服务 CES

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 CES 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。

 版权所有 © 华为云计算技术有限公司

- 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
- 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
- 如果此列条件键没有值（-），表示此操作不支持指定条件键。

关于 CES 定义的条件键的详细信息请参见条件（Condition）。

- “**别名**”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 CES 的相关操作。

表3-249 CES 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ces:widgets:put	授予批量更新视图的权限。	write	dashboard	-	-
ces:widgets:create	授予创建视图的权限。	write	dashboard	-	-
ces:widgets:put	授予更新指定视图的权限。	write	dashboard	-	-
ces:widgets:delete	授予删除指定视图的权限。	write	dashboard	-	-
ces:dashboards:create	授予创建dashboard 的权限。	write	dashboard	g:EnterpriseProjectId	-
ces:dashboards:list	授予批量查询dashboard 列表的权限。	list	dashboard	g:EnterpriseProjectId	-
ces:dashboards:put	授予更新指定dashboard 的权限。	write	dashboard	g:EnterpriseProjectId	-
ces:widgets:list	授予批量查询指定 dashboard 的视图列表权限。	list	dashboard	-	-
ces:widgets:create	授予创建指定dashboard 的视图权限。	write	dashboard	-	-
ces:dashboards:delete	授予批量删除dashboard 的权限	write	dashboard	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ces:widgets:get	授予查询指定视图的权限。	read	dashboard	-	-
ces:widgets:delete	授予删除指定视图的权限。	write	dashboard	-	-
ces:widgets:put	授予批量更新视图的权限。	write	dashboard	-	-
ces:dashboards:list	授予批量查询dashboard 列表的权限。	list	dashboard	g:EnterpriseProjectId	-
ces:dashboards:create	授予创建dashboard 的权限。	write	dashboard	g:EnterpriseProjectId	-
ces:dashboards:put	授予更新指定dashboard 的权限。	write	dashboard	g:EnterpriseProjectId	-
ces:dashboards:delete	授予删除指定dashboard 的权限。	write	dashboard	g:EnterpriseProjectId	-
ces:metrics:list	授予查询指标列表的权限。	list	-	-	-
ces:metricData:get	授予查询单条指标数据的权限。	read	-	-	ces:metricData:list
ces:metricData:create	授予上报指标数据的权限。	write	-	-	-
ces:namespacesDimensions:listAgentDimensions	授予查询指定实例下 agent 维度指标信息的权限。	list	-	-	ces:namespacesDimensions:list
ces:namespacesDimensions:list	授予批量查询指定指标维度的权限。	list	-	-	-
ces:metaData:get	授予批量查询维度元数据的权限。	read	-	-	ces:metaData:list
ces:metricD	授予批量查询指	list	-	-	ces:reso

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ata:list	标数据的权限。				urcesMetadata:list
ces:namespacesDimensions:list	授予查询指标TopN 维度的权限。	list	-	-	-
ces:alarms:list	授予查询告警规则列表的权限。	list	alarm	g:EnterpriseProjectId	-
ces:alarms:create	授予创建告警规则的权限。	write	alarm	g:EnterpriseProjectId	-
ces:alarms:put	授予更新告警规则的权限。	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	ces:alarmsonoff:put
ces:alarms:get	授予查询指定告警规则的权限。	read	alarm	g:EnterpriseProjectId	ces:alarms:list
ces:alarms:putAction	授予启停告警规则的权限。	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	ces:alarms:put
ces:alarms:delete	授予批量删除告警规则的权限。	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
ces:alarms:listOneClickAlarms	授予查询一键告警列表的权限。	list	alarm	g:EnterpriseProjectId	ces:oneClickAlarms:list
ces:alarms:putOneClickAlarms	授予修改一键告警状态的权限。	write	alarm	g:EnterpriseProjectId	ces:oneClickAlarms:put

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ces:alarms:list	授予查询告警规则列表的权限。	list	alarm	g:EnterpriseProjectId	-
ces:alarms:create	授予创建告警规则的权限。	write	alarm	g:EnterpriseProjectId	-
ces:alarms:putAlarmNotifications	授予修改告警通知信息的权限。	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	ces:alarms:put
ces:alarms:getPolicies	授予查询指定告警规则的策略列表权限。	read	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	ces:alarms:get
ces:alarms:updatePolicies	授予更新指定告警规则的策略列表权限。	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	ces:alarms:put
ces:alarms:getResources	授予查询指定告警规则的资源列表权限。	read	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
ces:alarms:addResources	授予为指定告警规则批量增加资源的权限。	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	ces:alarms:put
ces:alarms:deleteResources	授予为指定告警规则批量删除资源的权限。	write	alarm	• g:EnterpriseProjectId	ces:alarms:put

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:ResourceTag/<tag-key>	
ces:alarms:putNotificationMaskRules	授予修改告警通知屏蔽规则的权限。	write	alarm	g:EnterpriseProjectId	ces:notificationMasks:update
ces:alarms:listNotificationMaskResources	授予查询告警通知屏蔽资源列表的权限。	list	alarm	g:EnterpriseProjectId	ces:notificationMasks:list
ces:alarms:deleteNotificationMaskRules	授予批量删除告警通知屏蔽规则的权限。	write	alarm	g:EnterpriseProjectId	ces:notificationMasks:delete
ces:alarms:listNotificationMaskRules	授予查询告警通知屏蔽列表的权限。	list	alarm	g:EnterpriseProjectId	ces:notificationMasks:list
ces:alarms:createOneClickAlarms	授予创建一键告警的权限。	write	alarm	g:EnterpriseProjectId	ces:oneClickAlarms:post
ces:alarms:putOneClickAlarmPolicies	授予批量启停一键告警策略权限。	write	alarm	g:EnterpriseProjectId	ces:oneClickAlarms:put
ces:alarms:putOneClickAlarmNotifications	授予批量修改一键告警通知规则的权限。	write	alarm	g:EnterpriseProjectId	ces:oneClickAlarms:updateNotifications
ces:alarms:deleteOneClickAlarms	授予批量删除一键告警的权限。	write	alarm	g:EnterpriseProjectId	ces:oneClickAlarms:delete
ces:alarms:list	授予查询告警列表的权限。	list	alarm	g:EnterpriseProjectId	-
ces:alarmHistory:list	授予查询告警记录列表的权限。	list	alarm	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ces:customAlarmTemplates:create	授予创建自定义告警模板的权限。	write	alarm	g:EnterpriseProjectId	-
ces:customAlarmTemplates:delete	授予删除指定自定义告警模板的权限。	write	alarm	g:EnterpriseProjectId	-
ces:customAlarmTemplates:list	授予查询自定义告警模板列表的权限。	list	alarm	g:EnterpriseProjectId	-
ces:customAlarmTemplates:listAssociatedAlarms	授予查询指定自定义告警模板关联的告警规则列表的权限。	read	alarm	g:EnterpriseProjectId	ces:customAlarmTemplates:list
ces:customAlarmTemplates:put	授予更新指定自定义告警模板的权限。	write	alarm	g:EnterpriseProjectId	-
ces:quotas:get	授予查询配额的权限。	read	-	-	-
ces:quotas:get	授予批量查询配额的权限。	read	-	-	-
ces:events:get	授予查询指定事件详情的权限。	read	-	-	-
ces:events:list	授予查询事件列表的权限。	list	-	-	-
ces:agent:listTaskInvocations	授予批量查询指定服务器的agent 任务的权限。	list	-	-	ces:taskInvocation:get
ces:agent:createAgentInvocations	授予批量创建agent 任务的权限。	write	-	-	ces:taskInvocation:post
ces:events:post	授予上报事件的权限。	write	-	-	-
ces:resourceGroups:addResources	授予为指定资源分组批量添加关	write	-	g:EnterpriseProjectId	ces:resourceGroups:put

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	联资源的权限。				
ces:resourceGroups:create	授予创建资源分组的权限。	write	-	g:EnterpriseProjectId	-
ces:resourceGroups:delete	授予删除指定资源分组的权限。	write	-	g:EnterpriseProjectId	-
ces:resourceGroups:deleteResources	授予为指定资源分组批量删除关联资源的权限。	write	-	g:EnterpriseProjectId	ces:resourceGroups:put
ces:resourceGroups:get	授予查询指定资源分组的权限。	read	-	g:EnterpriseProjectId	-
ces:resourceGroups:getServiceResources	授予查询指定资源分组指定服务类别指定维度的资源的权限。	read	-	g:EnterpriseProjectId	ces:resourceGroups:get
ces:resourceGroups:put	授予更新指定资源分组的权限。	write	-	g:EnterpriseProjectId	-
ces:tags:list	授予批量查询CES 标签列表的权限。	list	-	-	-
ces:eventData:get	授予查询主机配置的权限。	list	-	-	ces:sapEventData:list
ces:resourceGroups:list	授予查询所有资源分组的权限。	list	-	g:EnterpriseProjectId	ces:resourceGroups:get
ces:resourceGroups:get	授予查询指定资源分组的权限。	read	-	g:EnterpriseProjectId	-
ces:customAlarmTemplates:list	授予查询自定义告警模板列表的权限。	list	alarm	g:EnterpriseProjectId	-
ces:customAlarmTemplates:get	授予查询指定自定义告警模板的权限。	read	alarm	g:EnterpriseProjectId	ces:customAlarmTemplates:list
ces:alarms:c	授予创建告警规	writ	alarm	g:Enterprise	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
reate	则的权限。	e		ProjectId	
ces:dashboards:put	授予更新云服务看板的权限	write	dashboard	-	-
ces:namespacesDimensions:list	授予查询指标TopN 维度的权限。	list	-	-	-
ces:namespacesDimensions:list	授予批量查询指定指标维度的权限。	list	-	-	-

CES 的 API 通常对应着一个或多个授权项。表 3-254 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-250 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/dashboards	ces:dashboards:create	-
GET /v2/{project_id}/dashboards	ces:dashboards:list	-
PUT /v2/{project_id}/dashboards/{dashboard_id}	ces:dashboards:put	-
GET /v2/{project_id}/dashboards/{dashboard_id}/widgets	ces:widgets:list	-
POST /v2/{project_id}/dashboards/{dashboard_id}/widgets	ces:widgets:create	-
POST /v2/{project_id}/dashboards/batch-delete	ces:dashboards:delete	-
GET /v2/{project_id}/widgets/{widget_id}	ces:widgets:get	-
DELETE /v2/{project_id}/widgets/{widget_id}	ces:widgets:delete	-
POST /v2/{project_id}/widgets/batch-	ces:widgets:put	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
update		
GET /V1.0/{project_id}/metrics	ces:metrics:list	-
GET /V1.0/{project_id}/metric-data	ces:metricData:get	ces:metricData:list
POST /V1.0/{project_id}/metric-data	ces:metricData:create	-
POST /V1.0/{project_id}/batch-query-metric-data	ces:metricData:list	-
GET /v2/{project_id}/instances/{instance_id}/agent-dimensions	ces:namespacesDimensions:listAgentDimensions	ces:namespacesDimensions:list
GET /V1.0/{project_id}/alarms	ces:alarms:list	-
POST /V1.0/{project_id}/alarms	ces:alarms:create	-
PUT /V1.0/{project/V1.0/{project_id}/events_id}/alarms/{alarm_id}	ces:alarms:put	ces:alarmsonoff:put
DELETE /V1.0/{project_id}/alarms/{alarm_id}	ces:alarms:delete	-
GET /V1.0/{project_id}/alarms/{alarm_id}	ces:alarms:get	ces:alarms:list
PUT /V1.0/{project_id}/alarms/{alarm_id}/action	ces:alarms:putAction	ces:alarms:put
GET /v2/{project_id}/alarms	ces:alarms:list	-
POST /v2/{project_id}/alarms	ces:alarms:create	-
PUT /v2/{project_id}/alarms/{alarm_id}/notifications	ces:alarms:putAlarmNotifications	ces:alarms:put
GET /v2/{project_id}/alarms/{alarm_id}/policies	ces:alarms:getPolicies	ces:alarms:get
PUT /v2/{project_id}/alarms/{alarm_id}/policies	ces:alarms:updatePolicies	ces:alarms:put
GET /v2/{project_id}/alarms/{alarm_id}/resources	ces:alarms:getResources	-
POST /v2/{project_id}/alarms/{alarm_id}/	ces:alarms:addResources	ces:alarms:put

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
resources/batch-create		
POST /v2/{project_id}/alarms/{alarm_id}/resources/batch-delete	ces:alarms:delete	ces:alarms:put
POST /v2/{project_id}/alarms/action	ces:alarms:putAction	ces:alarms:put
PUT /v2/{project_id}/notification-masks	ces:alarms:putNotificationMaskRules	ces:notificationMasks:update
PUT /v2/{project_id}/notification-masks/{notification_mask_id}	ces:alarms:putNotificationMaskRules	ces:notificationMasks:update
GET /v2/{project_id}/notification-masks/{notification_mask_id}/resources	ces:alarms:listNotificationMaskResources	ces:notificationMasks:list
POST /v2/{project_id}/notification-masks/batch-delete	ces:alarms:deleteNotificationMaskRules	ces:notificationMasks:delete
POST /v2/{project_id}/notification-masks/batch-query	ces:alarms:listNotificationMaskRules	ces:notificationMasks:list
POST /v2/{project_id}/notification-masks/batch-update	ces:alarms:putNotificationMaskRules	ces:notificationMasks:update
GET /v2/{project_id}/one-click-alarms	ces:alarms:listOneClickAlarms	ces:oneClickAlarms:list
POST /v2/{project_id}/one-click-alarms	ces:alarms:createOneClickAlarms	ces:oneClickAlarms:post
PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarm-rules/action	ces:alarms:putOneClickAlarms	ces:oneClickAlarms:put
GET /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarms	ces:alarms:listOneClickAlarms	ces:oneClickAlarms:list
PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarms/{alarm_id}/policies/action	ces:alarms:putOneClickAlarmPolicies	ces:oneClickAlarms:put
PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/notifications	ces:alarms:putOneClickAlarmNotifications	ces:oneClickAlarms:updateNotifications
POST /v2/{project_id}/one-click-alarms/batch-delete	ces:alarms:deleteOneClickAlarms	ces:oneClickAlarms:delete
POST /v2/{project_id}/alarms/batch-delete	ces:alarms:deleteResources	ces:alarms:put
GET /V1.0/{project_id}/alarm-	ces:alarmHistory:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
histories		
GET /v2/{project_id}/alarm-histories	ces:alarmHistory:list	-
POST /V1.0/{project_id}/alarm-template	ces:customAlarmTemplates:create	-
POST /v2/{project_id}/alarm-templates	ces:customAlarmTemplates:create	-
DELETE /V1.0/{project_id}/alarm-template/{template_id}	ces:customAlarmTemplates:delete	-
POST /v2/{project_id}/alarm-templates/batch-delete	ces:customAlarmTemplates:delete	-
GET /v2/{project_id}/alarm-templates/{template_id}	ces:customAlarmTemplates:get	ces:customAlarmTemplates:list
GET /V1.0/{project_id}/alarm-template	ces:customAlarmTemplates:list	-
GET /v2/{project_id}/alarm-templates	ces:customAlarmTemplates:list	-
GET /v2/{project_id}/alarm-templates/{template_id}/association-alarms	ces:customAlarmTemplates:listAssociatedAlarms	ces:customAlarmTemplates:list
PUT /V1.0/{project_id}/alarm-template/{template_id}	ces:customAlarmTemplates:put	-
PUT /v2/{project_id}/alarm-templates/{template_id}	ces:customAlarmTemplates:put	-
GET /V1.0/{project_id}/quotas	ces:quotas:get	-
GET /V1.0/{project_id}/event/{event_name}	ces:events:get	-
GET /V1.0/{project_id}/events	ces:events:list	-
GET /v3/{project_id}/agent-invocations	ces:agent:listTaskInvocations	ces:taskInvocation:get
POST /v3/{project_id}/agent-invocations/batch-create	ces:agent:createAgentInvocations	ces:taskInvocation:post
POST /V1.0/{project_id}/events	ces:events:post	-
POST /v2/{project_id}/resource-groups/{group_id}/resources/batch-create	ces:resourceGroups:addResources	ces:resourceGroups:put
POST /V1.0/{project_id}/resource-groups	ces:resourceGroups:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/resource-groups	ces:resourceGroups:create	-
DELETE /V1.0/{project_id}/resource-groups/{group_id}	ces:resourceGroups:delete	-
POST /v2/{project_id}/resource-groups/batch-delete	ces:resourceGroups:delete	-
POST /v2/{project_id}/resource-groups/{group_id}/resources/batch-delete	ces:resourceGroups:deleteResources	ces:resourceGroups:put
GET /V1.0/{project_id}/resource-groups/{group_id}	ces:resourceGroups:get	-
GET /v2/{project_id}/resource-groups/{group_id}	ces:resourceGroups:get	-
GET /v2/{project_id}/resource-groups/{group_id}/services/{service}/resources	ces:resourceGroups:getServiceResources	ces:resourceGroups:get
GET /V1.0/{project_id}/resource-groups	ces:resourceGroups:list	ces:resourceGroups:get
GET /v2/{project_id}/resource-groups	ces:resourceGroups:list	ces:resourceGroups:get
PUT /V1.0/{project_id}/resource-groups/{group_id}	ces:resourceGroups:put	-
PUT /v2/{project_id}/resource-groups/{group_id}	ces:resourceGroups:put	-
GET /v2/{project_id}/{resource_type}/tags	ces:tags:list	-
GET /V1.0/{project_id}/event-data	ces:eventData:get	ces:sapEventData:list
POST /v3/{project_id}/agent-status/batch-query	ces:agent:listStatuses	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的 URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

CES 定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

 版权所有 © 华为云计算技术有限公司

表3-251 CES 支持的资源类型

资源类型	URN
alarm	ces:<region>:<account-id>:alarm:<alarm-id>
dashboard	ces:<region>:<account-id>:dashboard:<dashboard-id>

条件（Condition）

CES 服务支持配置 ces:namespace 自定义条件键，具体操作请参考《云监控服务用户指南》中“按云服务粒度给用户授权”章节。

CES 服务适用除 g:requetedRegion 条件键外所有服务的全局条件键，请参考全局条件键。

说明

CES 有提供全局服务的能力（例如：告警通知、任务中心），所以按全局级服务处理，不支持 g:RequetedRegion 全局条件键。

3.13.9 消息通知服务 SMN

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。

 版权所有 © 华为云计算技术有限公司

  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 SMN 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 SMN 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 SMN 的相关操作。

表3-252 SMN 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
smn:topic:create	授予创建主题的权限。	Write	topic *	-	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	
smn:topic:listTopic	授予查询主题列表的权限。	List	topic *	-	smn:topic:list
			-	g:EnterpriseProjectId	
smn:topic:updateTopic	授予更新主题信息的权限。	Write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	smn:topic:update
smn:topic:get	授予查询主题详情的权限。	Read	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	smn:topic:list
smn:topic:delet	授予删除主题	Write	topic *	• g:Enterprise	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
e	的权限。			ProjectId • g:ResourceTag/<tag-key>	
smn:topic:listAttributes	授予查询主题策略的权限。	List	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	smn:topic:list
smn:topic:deleteAttribute	授予删除主题策略的权限。	Write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	smn:topic:update
smn:topic:updateAttribute	授予更新主题策略的权限。	Write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	smn:topic:update
			-	• smn:TargetAccountId • smn:TargetAccountId • smn:TargetAccountId	
smn:topic:subscribe	授予主题下创建订阅的权限。	Write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	smn:topic:update
			-	• smn:TargetAccountId • smn:TargetAccountId	
smn:topic:listSubscriptionsByTopic	授予查询指定主题的订阅列表的权限。	List	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	smn:topic:list
smn:topic:listSu	授予查询所有	List	topic *	-	smn:topic:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
bscriptions	主题的订阅列表的权限。				
smn:topic:deleteSubscription	授予删除指定主题下的订阅的权限。	Write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	smn:topic:update
smn:topic:updateSubscription	授予更新指定主题下的订阅的权限。	Write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	smn:topic:update
smn:topic:publish	授予发送消息的权限。	Write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
smn:template:create	授予创建模板的权限。	Write	template *	-	-
smn:template:listTemplates	授予查询模板列表的权限。	List	template *	-	smn:template:list
smn:template:update	授予修改模板的权限。	Write	template *	-	-
smn:template:get	授予查询模板详情的权限。	Read	template *	-	smn:template:list
smn:template:delete	授予删除模板的权限。	Write	template *	-	-
smn:tag:create	授予指定主题创建标签的权限。	Write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
smn:tag:delete	授予删除主题	Write	topic *	• g:EnterpriseProjectId	smn:tag:update

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	标签的权限。			• g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
smn:tag:batchModify	授予批量修改主题标签的权限。	Write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	smn:tag:update
			-	• g:RequestTag/<tag-key> • g:TagKeys	
smn:tag:list	授予查询主题标签的权限。	Read	topic *	g:ResourceTag/<tag-key>	-
smn:topic:createLogTank	授予为主题关联日志组和日志流的权限。	Write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
smn:topic:listLogTank	授予查询主题的日志组和日志流的权限。	List	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	smn:topic:list
smn:topic:updateLogTank	授予更新主题的日志组和日志流的权限。	Write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	smn:topic:update
smn:topic:deleteLogTank	授予解除主题的日志组和日志流关系的权限。	Write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	smn:topic:update
smn:topic:createNotifyPolicy	授予创建通知策略的权限	Write	topic *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
smn:topic:updateNotifyPolicy	授予修改通知策略的权限	Write	topic *	-	-
smn:topic:getNotifyPolicy	授予查询通知策略的权限	Read	topic *	-	-
smn:topic:deleteNotifyPolicy	授予删除通知策略的权限	Write	topic *	-	-

SMN 的 API 通常对应着一个或多个授权项。表 3-257 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-253 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/notifications/topics	smn:topic:create	-
GET /v2/{project_id}/notifications/topics	smn:topic:listTopic	-
PUT /v2/{project_id}/notifications/topics/{topic_urn}	smn:topic:updateTopic	-
GET /v2/{project_id}/notifications/topics/{topic_urn}	smn:topic:get	-
DELETE /v2/{project_id}/notifications/topics/{topic_urn}	smn:topic:delete	-
GET /v2/{project_id}/notifications/topics/{topic_urn}/attributes	smn:topic:listAttributes	-
DELETE /v2/{project_id}/notifications/topics/{topic_urn}/attributes	smn:topic:deleteAttribute	-
PUT /v2/{project_id}/notificat	smn:topic:updateAttribute	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ions/topics/{topic_urn}/attributes/{name}		
DELETE /v2/{project_id}/notifications/topics/{topic_urn}/attributes/{name}	smn:topic:deleteAttribute	-
POST /v2/{project_id}/notifications/topics/{topic_urn}/subscriptions	smn:topic:subscribe	-
GET /v2/{project_id}/notifications/topics/{topic_urn}/subscriptions	smn:topic:listSubscriptionsByTopic	-
PUT /v2/{project_id}/notifications/topics/{topic_urn}/subscriptions/{subscription_urn}	smn:topic:updateSubscription	-
DELETE /v2/{project_id}/notifications/subscriptions/{subscription_urn}	smn:topic:deleteSubscription	-
GET /v2/{project_id}/notifications/subscriptions	smn:topic:listSubscriptions	-
POST /v2/{project_id}/notifications/topics/{topic_urn}/publish	smn:topic:publish	-
POST /v2/{project_id}/notifications/message_template	smn:template:create	-
GET /v2/{project_id}/notifications/message_template	smn:template:listTemplates	-
PUT /v2/{project_id}/notifications/message_template/{message_template_id}	smn:template:update	-
GET /v2/{project_id}/notifications/message_template/{message_template_id}	smn:template:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /v2/{project_id}/notifications/message_template/{message_template_id}	smn:template:delete	-
POST /v2/{project_id}/{resource_type}/{resource_id}/tags	smn:tag:create	-
GET /v2/{project_id}/{resource_type}/{resource_id}/tags	smn:tag:list	-
POST /v2/{project_id}/{resource_type}/{resource_id}/tags/action	smn:tag:batchModify	• smn:tag:create • smn:tag:delete
DELETE /v2/{project_id}/{resource_type}/{resource_id}/tags/{key}	smn:tag:delete	-
GET /v2/{project_id}/{resource_type}/tags	smn:tag:list	-
POST /v2/{project_id}/{resource_type}/resource_instances/action	smn:tag:list	-
GET /v2/{project_id}/notifications/topics/{topic_urn}/logtanks	smn:topic:listLogTank	-
POST /v2/{project_id}/notifications/topics/{topic_urn}/logtanks	smn:topic:createLogTank	-
PUT /v2/{project_id}/notifications/topics/{topic_urn}/logtanks/{logtank_id}	smn:topic:updateLogTank	-
DELETE /v2/{project_id}/notifications/topics/{topic_urn}/logtanks/{logtank_id}	smn:topic:deleteLogTank	-
POST /v2/{project_id}/notificat	smn:topic:updateSubscription	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
ions/subscriptions/filter_polices		
PUT /v2/{project_id}/notifications/subscriptions/filter_polices	smn:topic:updateSubscription	-
DELETE /v2/{project_id}/notifications/subscriptions/filter_polices	smn:topic:updateSubscription	-
POST /v2/{project_id}/notifications/topics/{topic_urn}/subscriptions/from-subscription-users	smn:topic:subscribe	-
POST /v2/{project_id}/notifications/topics/{topic_urn}/notify-policy	smn:topic:createNotifyPolicy	smn:topic:listSubscriptionsByTopic
PUT /v2/{project_id}/notifications/topics/{topic_urn}/notify-policy/{notify_policy_id}	smn:topic:updateNotifyPolicy	smn:topic:listSubscriptionsByTopic
GET /v2/{project_id}/notifications/topics/{topic_urn}/notify-policy	smn:topic:getNotifyPolicy	-
DELETE /v2/{project_id}/notifications/topics/{topic_urn}/notify-policy/{notify_policy_id}	smn:topic:deleteNotifyPolicy	-
GET /v2/{project_id}/notifications/topics/{topic_urn}/statistics	smn:topic:get	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-258 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的

 版权所有 © 华为云计算技术有限公司

URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

SMN 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-254 SMN 支持的资源类型

资源类型	URN
topic	smn:<region>:<account-id>:topic:<topic-id>
template	smn:<region>:<account-id>:template:<template-id>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 smn:）仅适用于对应服务的操作，详情请参见表 3-259。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

SMN 支持的服务级条件键

SMN 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-255 SMN 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
smn:TargetOrgPath	string	单值	主题策略授权的组织路径。
smn:TargetOrgId	string	单值	主题策略授权的组织ID。
smn:TargetAccountId	string	单值	主题策略授权的账号

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
			ID。
smn:Protocol	string	单值	订阅终端协议。
smn:Endpoint	string	单值	订阅终端地址。

3.13.10 云日志服务 LTS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 LTS 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

 版权所有 © 华为云计算技术有限公司

关于 LTS 定义的条件键的详细信息请参见条件（Condition）。

- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 LTS 的相关操作。

表3-256 LTS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
lts:logGroup:deleteLogGroup	授予权限以删除指定日志组。	Write	logGroup *	-	lts:groups:delete
lts:logGroup:listLogGroup	授予权限以查询日志组列表。	List	-	-	lts:groups:get
lts:logGroup:createLogGroup	授予权限以创建日志组。	Write	-	-	lts:groups:create
lts:logGroup:updateLogGroup	授予权限以修改指定日志组。	Write	logGroup *	-	lts:groups:put
lts:logStream:listLogStream	授予权限以查询日志流列表。	List	logGroup *	-	lts:topics:get
lts:logStream:deleteLogStream	授予权限以删除指定日志流。	Write	logStream *	-	lts:topics:delete
lts:logStream:createLogStream	授予权限以创建日志流。	Write	logGroup *	-	lts:topics:create
lts:logStream:searchLog	授予权限以查询日志。	List	logStream *	-	lts:logs:list
lts:logStream:searchStructLog	授予权限以查询结构化日志。	List	logStream *	-	-
lts:logStream:searchLogHistogram	授予权限以查询日志直方图。	List	logStream *	-	lts:sqlalarmrules:create
lts:transfer:createTransfer	授予权限以创建转储任务。	Write	-	-	lts:transfers:create

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
lts:transfer:deleteTransfer	授予权限以删除转储任务。	Write	transfer *	-	lts:transfers:delete
lts:transfer:listTransfer	授予权限以查询日志转储任务列表。	List	-	-	lts:transfers:list
lts:transfer:updateTransfer	授予权限以修改转储任务。	Write	transfer *	-	lts:transfers:put
lts:transfer:registerDmsKafkaInstance	授予权限以注册 DmsKafka 实例。	Write	-	-	-
lts:configCenter:updateOverCollectSwitch	授予权限以修改超额采集开关。	Write	-	-	aom:quota:set
lts:structConfig:createStructConfig	授予权限以创建 LTS 结构化配置。	Write	logStream *	-	lts:topics:create
lts:structConfig:deleteStructConfig	授予权限以删除 LTS 结构化配置。	Write	logStream *	-	lts:structConfig:delete
lts:structConfig:getStructConfig	授予权限以查询 LTS 结构化配置。	Read	logStream *	-	lts:topics:get
lts:structConfig:listStructTemplate	授予权限以查询结构化模板列表。	List	-	-	lts:topics:get
lts:structConfig:updateStructConfig	授予权限以修改 LTS 结构化配置。	Write	logStream *	-	lts:topics:put
lts:mappingRule:create	授予权限以创建映射规则。	Write	-	-	lts:topics:create
lts:mappingRule:delete	授予权限以删除映射规则。	Write	-	-	lts:topics:delete
lts:mappingRule:get	授予权限以查看映射规则详情。	Read	-	-	lts:topics:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
lts:mappingRule:list	授予权限以查询映射规则列表。	List	-	-	lts:topics:get
lts:mappingRule:update	授予权限以修改映射规则。	Write	-	-	lts:topics:put
lts:logStream:getHistorySql	授予权限以查看日志流历史sql。	Read	logStream *	-	lts:topics:get
lts:alarmRule:createSqlAlarmRule	授予权限以创建 sql 告警规则的规则。	Write	-	-	lts:sqlalarmrules:create
lts:alarmRule:deleteSqlAlarmRule	授予权限以删除 sql 告警规则。	Write	alarmRule *	-	lts:sqlalarmrules:delete
lts:alarmRule:updateSqlAlarmRule	授予权限以修改 sql 告警规则。	Write	alarmRule *	-	lts:sqlalarmrules:put
lts:alarmRule:listSqlAlarmRule	授予权限以查看 sql 告警规则。	List	-	-	lts:sqlalarmrules:get
lts:alarmRule:createWordAlarmRule	授予权限以创建关键词告警规则。	Write	-	-	lts:sqlalarmrules:create
lts:alarmRule:deleteWordAlarmRule	授予权限以删除关键词告警规则。	Write	alarmRule *	-	lts:sqlalarmrules:delete
lts:alarmRule:updateWordAlarmRule	授予权限以修改关键词告警规则。	Write	alarmRule *	-	lts:sqlalarmrules:put
lts:alarmRule:listWordAlarmRule	授予权限以查看关键词告警规则。	List	-	-	-
lts:alarm:cleanAlarm	授予权限以删除告警。	Write	-	-	lts:sqlalarms:delete
lts:alarm:listAla	授予权限以查	List	-	-	lts:sqlalarms:ge

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rm	看警列表。				t
lts:logStream:listChart	授予权限以查询日志流图表。	List	-	-	-
lts:alarmNoticeTemplate:create	授予权限以创建告警通知模板。	Write	-	-	lts:sqlalarmrules:create
lts:alarmNoticeTemplate:update	授予权限以修改告警通知模板。	Write	-	-	lts:sqlalarmrules:put
lts:alarmNoticeTemplate:delete	授予权限以删除告警通知模板。	Write	-	-	lts:sqlalarmrules:delete
lts:alarmNoticeTemplate:list	授予权限以查询告警通知模板列表。	List	-	-	lts:sqlalarmrules:get
lts:alarmNoticeTemplate:get	授予权限以查询告警通知模板详情。	Read	-	-	lts:sqlalarmrules:get
lts:hostGroup:create	授予权限以创建主机组。	Write	-	-	lts:topics:create
lts:hostGroup:delete	授予权限以删除主机组。	Write	hostGroup *	-	lts:topics:delete
lts:host:list	授予权限以查询主机列表。	List	-	-	-
lts:hostGroup:list	授予权限以查询主机组列表。	List	accessConfig *	-	-
lts:hostGroup:update	授予权限以修改主机组。	Write	hostGroup *	-	lts:topics:put
lts:accessConfig:create	授予权限以创建日志接入。	Write	logStream *	-	lts:topics:create
lts:accessConfig:delete	授予权限以删除日志接入。	Write	accessConfig *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
lts:accessConfig:list	授予权限以查询日志接入列表。	List	-	-	-
lts:accessConfig:update	授予权限以修改日志接入。	Write	accessConfig *	-	-
			hostGroup	-	
lts:tag:create	授予权限以创建标签。	Write	-	-	lts:resourceTags:put
lts:tag:delete	授予权限以删除标签。	Write	-	-	lts:resourceTags:delete
lts:logStream:createQuickQuery	授予权限以创建快速查询。	Write	logStream *	-	lts:searchcriterias:create
lts:logStream:deleteQuickQuery	授予权限以删除快速查询。	Write	logStream *	-	lts:searchcriterias:delete
lts:logStream:listQuickQuery	授予权限以查询快速查询列表。	List	logGroup *	-	lts:searchcriterias:list
lts:logFavorite:create	授予权限以创建日志收藏。	Write	logStream *	-	lts:topics:create
lts:logFavorite:delete	授予权限以删除日志收藏。	Write	-	-	lts:topics:delete
lts:dashboardGroup:create	授予权限以创建仪表盘分组。	Write	-	-	lts:topics:create
lts:dashboard:create	授予权限以创建仪表盘。	Write	-	-	lts:topics:create
lts:trafficStatistic:get	授予权限以获取资源统计详情。	Read	-	-	lts:logs:list
lts:tokenizer:get	授予权限以获取已配置的分	Read	-	-	lts:topic:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	词符。				
lts:tokenizer:create	授予权限以保存分词符。	Write	-	-	lts:topic:put
lts:tokenizer:preview	授予权限以预览分词符。	Read	-	-	lts:topic:put
lts:usageAlarm:update	授予权限以打开或者关闭使用量预警。	Write	-	-	lts:topics:put
lts:csvTable:list	授予权限以获取关联数据源配置信息表。	List	-	-	lts:sqlalarmrules:list
lts:csvTable:upload	授予权限以上传 csv 文件。	Write	-	-	lts:sqlalarmrules:create
lts:csvTable:get	授予权限以预览关联数据和查看关联数据源信息。	Read	-	-	lts:sqlalarmrules:get
lts:csvTable:create	授予权限以创建关联数据源。	Write	-	-	lts:sqlalarmrules:create
lts:csvTable:update	授予权限以更新关联数据源。	Write	-	-	lts:sqlalarmrules:put
lts:csvTable:delete	授予权限以删除关联数据源。	Write	-	-	lts:sqlalarmrules:delete
lts:scheduledSql:create	授予权限以创建定时 sql。	Write	-	-	lts:sqlalarmrules:create
lts:scheduledSql:delete	授予权限以删除定时 sql。	Write	-	-	lts:sqlalarmrules:delete
lts:scheduledSql:update	授予权限以修改定时 sql。	Write	-	-	lts:sqlalarmrules:put
lts:scheduledSql:list	授予权限以获取定时 sql 列	List	-	-	lts:sqlalarmrules:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	表。				
lts:scheduledSql:get	授予权限以获取定时 sql 详情。	Read	-	-	lts:sqlalarmrules:get
lts:scheduledSql:retry	授予权限以重试执行实例。	Write	-	-	lts:sqlalarmrules:delete
lts:transfer:getDisList	授予权限以获取 Dis 通道列表。	List	-	-	lts:disStreams:list
lts:transfer:listKafkaInstance	授予权限以获取 kafka 列表。	List	-	-	lts:kafka:list
lts:transfer:updateKafkaInstance	授予权限以更新 kafka 信息。	Write	-	-	lts:kafka:update
lts:transfer:deleteKafkaInstance	授予权限以删除 kafka 信息。	Write	-	-	lts:kafka:delete
lts:transfer:listKafkaAuthorization	授予权限以查询用户配置 kafka 授权列表。	List	-	-	lts:kafka:list
lts:transfer:createKafkaAuthorization	授予权限以增加用户配置 kafka 授权列表。	Write	-	-	lts:kafka:create
lts:transfer:deleteKafkaAuthorization	授予权限以删除用户配置 kafka 授权列表。	Write	-	-	lts:kafka:delete
lts:transfer:getTransfer	授予权限以获取转储任务的信息。	Read	transfer *	-	lts:transfers:list
lts:transfer:getDwsInfo	授予权限以查询租户的 dws 信息。	Read	-	-	lts:transfers:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
lts:transfer:registerDwsCluster	授予权限以注册 dws 集群。	Write	-	-	lts:transfers:create
lts:hostGroup:getHost	授予权限以通过查询条件获取所有主机。	Read	-	-	lts:topics:list
lts:hostGroup:get	授予权限以通过查询条件获取单个主机组加入的所有配置。	Read	-	-	lts:topics:list
lts:accessConfig:get	授予权限以获取单个采集配置。	Read	accessConfig *	-	lts:topics:get
lts:logFavorite:list	授予权限以获取收藏列表。	List	-	-	lts:topics:get
lts:logFavorite:update	授予权限以修改收藏。	Write	logStream *	-	lts:topics:put
lts:logGroup:getLogGroup	授予权限以查询日志组。	Read	logGroup *	-	lts:groups:get
lts:IndexConfig:list	授予权限以查询索引。	List	logGroup *	-	lts:topics:get
lts:IndexConfig:create	授予权限以创建索引。	Write	logGroup *	-	lts:topics:put
lts:structConfig:listStructConfig	授予权限以获取日志流结构化信息。	List	logStream *	-	lts:wordFreq:get
lts:logStream:updateLogStream	授予权限以修改日志流。	Write	logStream *	-	lts:topics:put
lts:logStream:getRealtimeLog	授予权限以获取实时日志。	Read	logStream *	-	lts:logs:list
lts:logStream:getLogStream	授予权限以查询日志流信息。	Read	logStream *	-	lts:topics:get
lts:logStream:cr	授予权限以创	Write	logStr	-	lts:topics:create

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
eateLogFilterRules	建日志清洗规则。		eam *		
lts:logStream:updateLogFilterRules	授予权限以修改日志清洗规则。	Write	logStream *	-	lts:topics:put
lts:logStream:deleteLogFilterRules	授予权限以删除日志清洗规则。	Write	logStream *	-	lts:topics:delete
lts:logStream:listLogFilterRules	授予权限以查询日志清洗规则。	List	logStream *	-	lts:topics:delete
lts:logStream:getQuickQuery	授予权限以查看快速查询。	List	logStream *	-	lts:searchcriterias:list
lts:logStream:updateQuickQuery	授予权限以修改快速查询。	Write	logStream *	-	lts:searchcriterias:put
lts:logStream:searchLogContext	授予权限以查询日志上下文。	Read	logStream *	-	lts:logs:list
lts:structConfig:getCustomTemplate	授予权限以查询用户自定义模板。	Read	-	-	lts:topics:get
lts:structConfig:createCustomTemplate	授予权限以创建用户自定义模板。	Write	-	-	lts:topics:create
lts:structConfig:updateCustomTemplate	授予权限以修改用户自定义模板。	Write	-	-	lts:topics:put
lts:structConfig:deleteCustomTemplate	授予权限以删除用户自定义模板。	Write	-	-	lts:topics:delete
lts:structConfig:listCustomTemplate	授予权限以查询用户自定义模板列表。	Read	-	-	lts:topics:get
lts:structConfig:smartExtra	授予权限以智能提取结构化	Write	-	-	lts:topics:create

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	字段。				
lts:logStream:getAggrResult	授予权限以获取快速分析结果。	Read	logStream *	-	lts:topics:get
lts:logStream:getAggr	授予权限以查询快速分析聚合器。	Read	-	-	lts:topics:get
lts:logStream:createAggr	授予权限以创建快速分析聚合器。	Write	-	-	lts:topics:create
lts:logStream:deleteAggr	授予权限以删除快速分析聚合器。	Write	-	-	lts:topics:delete
lts:logStream:getQuickAnalysisAggValue	授予权限以获取数值类型的快速分析结果。	Read	logStream *	-	-
lts:logStream:getWordFreqConfig	授予权限以查询用户已创建的快速分析字段。	Read	logStream *	-	lts:wordFreq:get
lts:logStream:refreshWordFreqConfig	授予权限以修改快速分析字段。	Write	logStream *	-	lts:wordFreq:set
lts:logCrux:list	授予权限以查询日志聚类信息。	List	-	-	lts:logreduce:list
lts:logCrux:get	授予权限以获取日志聚类开关信息。	Read	-	-	lts:logreduce:get
lts:logCrux:enable	授予权限以开启日志聚类开关。	Write	-	-	lts:logreduce:put
lts:logCrux:disable	授予权限以关闭日志聚类开关。	Write	-	-	lts:logreduce:put

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
lts:logStream:updateChart	授予权限以更新用户日志看板。	Write	-	-	lts:topics:put
lts:logStream:createChart	授予权限以创建用户日志看板。	Write	-	-	lts:topics:create
lts:logStream:deleteChart	授予权限以删除用户日志看板。	Write	logStream *	-	lts:topics:delete
lts:logStream:getChart	授予权限以获取用户日志看板。	Read	logStream *	-	lts:topics:get
lts:dashboard:deleteChart	授予权限以删除图表。	Write	dashboard *	-	lts:topics:delete
lts:dashboard:listCharts	授予权限以展示仪表盘层级的图表。	List	-	-	lts:topics:delete
lts:dashboard:updateChart	授予权限以移动图表。	Write	dashboard *	-	lts:topics:put
lts:dashboard:getDashboard	授予权限以查询用户日志仪表盘。	Read	-	-	lts:topics:put
lts:dashboardGroup:getDashboardsGroup	授予权限以查询用户日志仪表盘分组。	Read	-	-	lts:topics:get
lts:dashboardGroup:updateDashboardsGroup	授予权限以修改用户日志仪表盘分组。	Write	-	-	lts:topics:put
lts:dashboardGroup:deleteDashboardsGroup	授予权限以更新用户日志仪表盘分组。	Write	-	-	lts:topics:delete
lts:dashboard:CreateDashBoard	授予权限以根据日志仪表盘模板批量创建仪表盘。	Write	-	-	lts:topics:create

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
lts:dashboard:CreateDashBoardTemplate	授予权限以创建用户日志仪表盘模板。	Write	-	-	lts:topics:create
lts:dashboard:getDashBoardTemplate	授予权限以查询用户日志仪表盘模板。	Read	-	-	lts:topics:get
lts:dashboard:updateDashBoardTemplate	授予权限以修改用户日志仪表盘模板。	Write	-	-	lts:topics:put
lts:dashboard:deleteDashBoardTemplate	授予权限以删除用户日志仪表盘模板。	Write	-	-	lts:topics:delete
lts:dashboardGroup:createLogDashboardTemplateGroup	授予权限以创建仪表盘模板分组。	Write	-	-	lts:topics:create
lts:dashboardGroup:updateLogDashboardTemplateGroup	授予权限以修改仪表盘模板分组。	Write	-	-	lts:topics:put
lts:dashboardGroup:deleteLogDashboardTemplateGroup	授予权限以删除用户日志仪表盘模板分组。	Write	-	-	lts:topics:delete
lts:dashboard:listFilter	授予权限以查询仪表盘过滤器。	List	dashboard *	-	-
lts:dashboard:createFilter	授予权限以创建仪表盘过滤器。	Write	dashboard *	-	-
lts:dashboard:updateFilter	授予权限以修改仪表盘过滤器。	Write	dashboard *	-	-
lts:dashboard:deleteFilter	授予权限以删除仪表盘过滤器。	Write	dashboard *	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
lts:alarmRule:listAlarmRules	授予权限以查询告警规则列表。	List	-	-	lts:sqlalarmrules:get
lts:alarmRule:getKeywordsAlarmRule	授予权限以查询关键词告警规则。	Read	alarmRule *	-	lts:sqlalarmrules:get
lts:alarmRule:getSqlAlarmRule	授予权限以查询 sql 告警规则。	Read	alarmRule *	-	lts:sqlalarmrules:get
lts:alarm:listAlarmStatistic	授予权限以查询 sql 告警数据。	List	-	-	lts:sqlalarmstatistics:get
lts:dashboard:update	授予权限以修改用户日志仪表盘。	Write	-	-	lts:topics:put
lts:dashboard:delete	授予权限以删除用户日志仪表盘。	Write	-	-	lts:topics:delete
lts:logSearch:list	授予权限以获取集群列表，命名空间，组件，实例，日志，节点，日志文件页面组件列表，文件列表。	List	-	-	aom:log:list
lts:logSearch:getTime	授予权限以获取后端节点当前时间。	Read	-	-	aom:log:get
lts:logSearch:getLogContext	授予权限以获取日志上下文。	Read	-	-	aom:log:get
lts:logSearch:exportLogs	授予权限以下载日志。	Write	-	-	aom:log:list
lts:ageingTime:get	授予权限以获取配额管理。	List	-	-	aom:log:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
lts:ageingTime:update	授予权限以修改配额管理。	Write	-	-	aom:quota:set
lts:logConfigPath:list	授予权限以查询 VM 日志路径配置。	List	-	-	aom:log:list
lts:logConfigPath:create	授予权限以新建 VM 日志路径配置。	Write	-	-	aom:subscribe:set
lts:structRule:get	授予权限以获取结构化规则。	Read	-	-	aom:log:get
lts:structRule:create	授予权限以创建结构化规则。	Write	-	-	aom:subscribe:set
lts:structRule:delete	授予权限以删除结构化规则。	Write	-	-	aom:subscribe:set
lts:structRule:regex	授予权限以结构化提取。	Write	-	-	aom:subscribe:set
lts:logPail:list	授予权限以查询日志桶、桶内日志和日志柱状图。	List	-	-	aom:log:list
lts:structSql:list	授予权限以查询结构化日志。	List	-	-	aom:log:list
lts:logPail:create	授予权限以添加日志桶。	Write	-	-	aom:subscribe:set
lts:logPail:update	授予权限以修改日志桶。	List	-	-	aom:subscribe:set
lts:logPail:delete	授予权限以删除日志桶。	Write	-	-	aom:subscribe:set
lts:storageRelation:list	授予权限以查询当前租户下的转储关系。	List	-	-	aom:log:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
lts:storageRelation:delete	授予权限以删除当前租户下的转储关系。	Write	-	-	aom:subscribe:set
lts:storage:batchAction	授予权限以周期性批量启停。	Write	-	-	aom:subscribe:set
lts:logPailDump:create	授予权限以添加日志转储。	Write	-	-	aom:subscribe:set
lts:statisticsRule:list	授予权限以查询统计规则。	List	-	-	aom:log:list
lts:statisticsRule:create	授予权限以创建统计规则。	Write	-	-	aom:subscribe:set
lts:statisticsRule:update	授予权限以修改统计规则。	Write	-	-	aom:subscribe:set
lts:statisticsRule:delete	授予权限以删除统计规则。	Write	-	-	aom:subscribe:set
lts:transfer:listKafkaInstanceTopic	授予权限以获取用户 kafka 所有 topic。	List	-	-	lts:kafka:list
lts:logPackage:create	授予权限以购买资源包。	Write	-	-	lts:topics:put
lts:consumerGroup:create	授予权限以创建消费组。	Write	-	-	lts:topics:create
lts:consumerGroup:delete	授予权限以删除消费组。	Write	-	-	lts:topics:delete
lts:consumerGroup:list	授予权限以查询消费组列表。	List	-	-	lts:topics:list
lts:consumerGroup:get	授予权限以查询消费组详情。	Read	-	-	lts:topics:get
lts:consumerGroup:update	授予权限以修改消费组。	Write	-	-	lts:topics:put
lts:logStream:g	授予权限以获	Read	-	-	lts:topics:get

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
et	取日志流详情。				
lts:agency:listGroupAndStream	授予权限以获取委托方日志组日志流列表。	List	-	-	lts:topics:get
lts:agency:listEps	授予权限以获取委托方 EPS 列表。	List	-	-	lts:topics:get
lts:agency:listStructConfig	授予权限以获取委托方结构化配置。	List	-	-	lts:topics:get
lts:logConverge:get	授予权限以获取多账号日志汇聚配置。	Read	-	-	lts:logConverge:get
lts:logConverge:update	授予权限以更新多账号日志汇聚配置。	Write	-	-	lts:logConverge:update
lts:logManager:createAggr	授予权限以创建快速分析聚合器。	Write	logStream *	-	lts:topics:create
lts:logManager:createAggrs	授予权限以批量创建快速分析聚合器。	Write	logStream *	-	lts:topics:create
lts:logManager:deleteAggr	授予权限以删除快速分析聚合器。	Write	logStream *	-	lts:topics:delete
lts:logManager:deleteAggrs	授予权限以批量删除快速分析聚合器。	Write	logStream *	-	lts:topics:delete
lts:logmanager:createLogFilter	授予权限以创建日志清洗规则。	Write	logStream *	-	lts:filters:create
lts:logmanager:listLogFilters	授予权限以查看日志清洗规则。	Read	logStream *	-	lts:filters:list

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
lts:logmanager:updateLogFilters	授予权限以修改日志清洗规则。	Write	logStream *	-	lts:filters:put
lts:logmanager:deleteLogFilters	授予权限以删除日志清洗规则。	Write	logStream *	-	lts:filters:delete
lts:structConfig:regex	授予权限以正则结构化示例日志。	Write	-	-	lts:regex:create

LTS 的 API 通常对应着一个或多个授权项。表 3-261 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-257 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/groups	lts:logGroup:createLogGroup	-
DELETE /v2/{project_id}/groups/{log_group_id}	lts:logGroup:deleteLogGroup	-
GET /v2/{project_id}/groups	lts:logGroup:listLogGroup	-
POST /v2/{project_id}/groups/{log_group_id}	lts:logGroup:updateLogGroup	-
POST /v2/{project_id}/groups/{log_group_id}/streams	lts:logStream:createLogStream	-
PUT /v2/{project_id}/groups/{log_group_id}/streams-ttl/{log_stream_id}	lts:logStream:updateLogStream	-
DELETE	lts:logStream:deleteLogStream	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v2/{project_id}/groups/{log_group_id}/streams/{log_stream_id}		
GET /v2/{project_id}/groups/{log_group_id}/streams	lts:logStream:listLogStream	-
GET /v2/{project_id}/log-streams	lts:logStream:listLogStream	-
POST /v2/{project_id}/lts/keyword-count	lts:logStream:searchLogHistogram	-
POST /v2/{project_id}/groups/{log_group_id}/streams/{log_stream_id}/content/query	lts:logStream:searchLog	-
POST /v2/{project_id}/groups/{log_group_id}/streams/{log_stream_id}/struct-content/query	lts:logStream:searchStructLog	-
POST /v2/{project_id}/streams/{log_stream_id}/struct-content/query	lts:logStream:searchStructLog	-
POST /v2/{project_id}/transfers	lts:transfer:createTransfer	• obs:bucket:PutBucketAcl • obs:bucket:GetBucketAcl • obs:bucket:GetEncryptionConfiguration • obs:bucket:HeadBucket • dis:streams:list • dis:streamPolicies:list
DELETE /v2/{project_id}/transfers	lts:transfer:deleteTransfer	-
GET /v2/{project_id}/transfers	lts:transfer:listTransfer	-
POST /v2/{project_id}/lts/dms/kafka-instance	lts:transfer:registerDmsKafkaInstance	dms:instance:list

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/transfers	lts:transfer:updateTransfer	• obs:bucket:PutBucketAcl • obs:bucket:GetBucketAcl • obs:bucket:GetEncryptionConfiguration • obs:bucket:HeadBucket • dis:streams:list • dis:streamPolicies:list
POST /v2/{project_id}/collection/disable	lts:configCenter:updateOverCollectSwitch	-
POST /v2/{project_id}/collection/enable	lts:configCenter:updateOverCollectSwitch	-
POST /v3/{project_id}/lts/struct/template	lts:structConfig:createStructConfig	-
POST /v2/{project_id}/lts/struct/template	lts:structConfig:createStructConfig	-
DELETE /v2/{project_id}/lts/struct/template	lts:structConfig:deleteStructConfig	-
GET /v3/{project_id}/lts/struct/customtemplate/list	lts:structConfig:listStructTemplate	-
GET /v3/{project_id}/lts/struct/customtemplate	lts:structConfig:listStructTemplate	-
GET /v2/{project_id}/lts/struct/template	lts:structConfig:getStructConfig	-
PUT /v3/{project_id}/lts/struct/template	lts:structConfig:updateStructConfig	-
PUT /v2/{project_id}/lts/struct/template	lts:structConfig:updateStructConfig	-
POST /v2/{project_id}/lts/aom-mapping	lts:mappingRule:create	-
DELETE	lts:mappingRule:delete	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v2/{project_id}/lts/aom-mapping		
GET /v2/{project_id}/lts/aom-mapping/{rule_id}	lts:mappingRule:get	-
GET /v2/{project_id}/lts/aom-mapping	lts:mappingRule:list	-
PUT /v2/{project_id}/lts/aom-mapping	lts:mappingRule:update	-
GET /v2/{project_id}/lts/notifications/topics	lts:alarmNoticeTemplate:list	smn:topic:list
POST /v2/{project_id}/lts/alarms/sql-alarm-rule	lts:alarmRule:createSqlAlarmRule	-
DELETE /v2/{project_id}/lts/alarms/sql-alarm-rule/{sql_alarm_rule_id}	lts:alarmRule:deleteSqlAlarmRule	-
GET /v2/{project_id}/lts/alarms/sql-alarm-rule	lts:alarmRule:listSqlAlarmRule	-
PUT /v2/{project_id}/lts/alarms/status	lts:alarmRule:updateSqlAlarmRule	-
PUT /v2/{project_id}/lts/alarms/sql-alarm-rule	lts:alarmRule:updateSqlAlarmRule	-
POST /v2/{project_id}/lts/alarms/keywords-alarm-rule	lts:alarmRule:createWordAlarmRule	-
DELETE /v2/{project_id}/lts/alarms/keywords-alarm-rule/{keywords_alarm_rule_id}	lts:alarmRule:deleteWordAlarmRule	-
GET /v2/{project_id}/lts/alarms/keywords-alarm-rule	lts:alarmRule:listWordAlarmRule	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/lts/alarms/keywords-alarm-rule	lts:alarmRule:updateWordAlarmRule	-
POST /v2/{project_id}/{domain_id}/lts/alarms/sql-alarm/clear	lts:alarm:cleanAlarm	-
POST /v2/{project_id}/{domain_id}/lts/alarms/sql-alarm/query	lts:alarm:listAlarm	-
GET /v2/{project_id}/groups/{log_group_id}/streams/{log_stream_id}/charts	lts:logStream:listChart	-
POST /v2/{project_id}/{domain_id}/lts/events/notification/templates	lts:alarmNoticeTemplate:create	-
DELETE /v2/{project_id}/{domain_id}/lts/events/notification/templates	lts:alarmNoticeTemplate:delete	-
POST /v2/{project_id}/{domain_id}/lts/events/notification/templates/view	lts:alarmNoticeTemplate:list	-
GET /v2/{project_id}/{domain_id}/lts/events/notification/templates	lts:alarmNoticeTemplate:list	-
GET /v2/{project_id}/{domain_id}/lts/events/notification/template/{template_name}	lts:alarmNoticeTemplate:get	-
PUT /v2/{project_id}/{domain_id}/lts/events/notification/templates	lts:alarmNoticeTemplate:update	-
POST /v3/{project_id}/lts/host-group	lts:hostGroup:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
DELETE /v3/{project_id}/lts/host-group	lts:hostGroup:delete	-
POST /v3/{project_id}/lts/host-list	lts:host:list	• aom:icmgr:get • aom:icmgr:list
POST /v3/{project_id}/lts/host-group-list	lts:hostGroup:list	-
PUT /v3/{project_id}/lts/host-group	lts:hostGroup:update	-
POST /v3/{project_id}/lts/access-config	lts:accessConfig:create	-
DELETE /v3/{project_id}/lts/access-config	lts:accessConfig:delete	-
POST /v3/{project_id}/lts/access-config-list	lts:accessConfig:list	-
PUT /v3/{project_id}/lts/access-config	lts:accessConfig:update	-
POST /v1/{project_id}/{resource_type}/{resource_id}/tags/action	lts:tag:create	-
POST /v1.0/{project_id}/groups/{group_id}/topics/{topic_id}/search-criterias	lts:logStream:createQuickQuery	-
DELETE /v1.0/{project_id}/groups/{group_id}/topics/{topic_id}/search-criterias	lts:logStream:deleteQuickQuery	-
GET /v1.0/{project_id}/groups/{group_id}/topics/{topic_id}/search-criterias	lts:logStream:listQuickQuery	-
GET	lts:logStream:getHistorySql	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v2/{project_id}/lts/history-sql		
GET /v1.0/{project_id}/lts/groups/{group_id}/search-criterias	lts:logStream:listQuickQuery	-
POST /v1.0/{project_id}/lts/favorite	lts:logFavorite:create	-
DELETE /v1.0/{project_id}/lts/favorite/{fav_res_id}	lts:logFavorite:delete	-
POST /v2/{project_id}/dashboard	lts:dashboard:create	-
POST /v2/{project_id}/lts/dashboard-group	lts:dashboardGroup:create	-
POST /v2/{project_id}/lts/timeline-traffic-statistics	lts:trafficStatistic:get	-
POST /v2/{project_id}/lts/topn-traffic-statistics	lts:trafficStatistic:get	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-262 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

LTS 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-258 LTS 支持的资源类型

资源类型	URN
logStream	lts:<region>:<account-id>:logStream:<group_id>/<stream_id>
logGroup	lts:<region>:<account-id>:logGroup:<group_id>
dashboard	lts:<region>:<account-id>:dashboard:<dashboard_id>
accessConfig	lts:<region>:<account-id>:accessConfig:<config_id>

 版权所有 © 华为云计算技术有限公司

资源类型	URN
alarmRule	lts:<region>:<account-id>:alarmRule:<alarm_rule_id>
transfer	lts:<region>:<account-id>:transfer:<transfer_id>
hostGroup	lts:<region>:<account-id>:hostGroup:<host_group_id>

条件（Condition）

LTS 服务不支持在身份策略中的条件键中配置服务级的条件键。LTS 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.13.11 云审计服务 CTS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 cts 定义的资源类型的详细信息请参见资源类型（Resource）。

 版权所有 © 华为云计算技术有限公司

- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 cts 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 cts 的相关操作。

表3-259 cts 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cts:trace:list	授予查询审计事件权限。	List	-	-	-
cts:tracker:create	授予创建追踪器的权限。	Write	-	-	-
cts:tracker:list	授予查询追踪器权限。	List	-	-	-
cts:tracker:update	授予更新追踪器的权限。	Write	tracker	-	-
cts:tracker:delete	授予删除追踪器的权限。	Write	tracker	-	-
cts:quota:get	授予查询追踪器配额权限。	Read	-	-	-
cts:notification:create	授予创建通知规则权限。	Write	-	-	-
cts:notification:update	授予更新关键操作通知权限。	Write	notification	-	-
cts:notification:list	授予查询关键操作通知权限。	List	-	-	-
cts:notification:delete	授予删除通知规则权限。	Write	notification	-	-
cts:tag:create	授予创建资源	Tagging	tracker	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	标签的权限。		-	• g:TagKeys • g:RequestTag/<tag-key>	
cts:tag:delete	授予删除资源标签的权限。	Tagging	tracker	-	-
			-	• g:TagKeys • g:RequestTag/<tag-key>	
cts:notification:listOperation	授予查询所有操作列表的权限。	List	-	-	-
cts:trace:listTraceUser	授予查询所有操作用户列表的权限。	List	-	-	-
cts:trace:listResource	授予查询所有事件资源类型列表的权限。	List	-	-	-

cts 的 API 通常对应着一个或多个授权项。表 3-264 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-260 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/traces	cts:trace:list	-
GET /v3/{project_id}/quotas	cts:quota:get	-
POST /v3/{project_id}/tracker	cts:tracker:create	• lts:topics:list • lts:topics:create • lts:groups:list • lts:groups:create • obs:bucket:CreateBucket • obs:bucket:HeadBucket • obs:bucket:GetLifecycleCo

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
		nfiguration • obs:bucket:PutLifecycleConfiguration • obs:bucket:GetBucketAcl • obs:bucket:PutBucketAcl • kms:cmk:list
PUT /v3/{project_id}/tracker	cts:tracker:update	• lts:topics:list • lts:topics:create • lts:groups:list • lts:groups:create • obs:bucket:CreateBucket • obs:bucket:HeadBucket • obs:bucket:GetLifecycleConfiguration • obs:bucket:PutLifecycleConfiguration • obs:bucket:GetBucketAcl • obs:bucket:PutBucketAcl • kms:cmk:list
GET /v3/{project_id}/trackers	cts:tracker:list	-
DELETE /v3/{project_id}/trackers	cts:tracker:delete	-
POST /v3/{project_id}/notifications	cts:notification:create	• smn:topic:listTopic • iam:users:listUsers • iam:groups:listGroups
PUT /v3/{project_id}/notifications	cts:notification:update	• smn:topic:listTopic • iam:users:listUsers • iam:groups:listGroups
DELETE /v3/{project_id}/notifications	cts:notification:delete	-
GET /v3/{project_id}/notifications/{notification_type}	cts:notification:list	-
POST /v3/{project_id}/{resource_type}/{resource_	cts:tag:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
id}/tags/create		
DELETE /v3/{project_id}/{resource_type}/{resource_id}/tags/delete	cts:tag:delete	-
GET /v3/{domain_id}/resources	cts:trace:listResource	-
GET /v3/{project_id}/operations	cts:notification:listOperation	-
GET /v3/{project_id}/user-resources	cts:trace:listTraceUser	-
POST /v3/{domain_id}/checkbucket	cts:tracker:list	obs:bucket:ListAllMyBuckets

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-265 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

cts 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-261 cts 支持的资源类型

资源类型	URN
tracker	cts:<region>:<account-id>:tracker:<tracker-id>
notification	cts:<region>:<account-id>:notification:<notification-id>

条件（Condition）

条件键（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。

 版权所有 © 华为云计算技术有限公司

- 服务级条件键（前缀通常为服务缩写，如 cts:）仅适用于对应服务的操作，详情请参见表 3-266。
- 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。

- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

CTS 定义了以下可以在 SCP 的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化 SCP 语句应用的条件。

表3-262 CTS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
cts:TargetType	string	单值	按照数据转储类型筛选访问权限。
cts:TargetAccountId	string	单值	按照 obs 桶所属用户的 DomainID（账号 ID）筛选访问权限。
cts:TargetOrgId	string	单值	按照 obs 桶所属组织筛选访问权限。
cts:TargetOrgPath	string	单值	按照 obs 桶所属组织 OU 路径筛选访问权限。

3.13.12 安全令牌服务 STS

云服务在 IAM 预置了常用的权限，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。

 版权所有 © 华为云计算技术有限公司

- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 STS 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 STS 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 STS 的相关操作。

表3-263 STS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
sts:agencies:assume	授予权限以获取一组可用来访问您通常无法访问的资源的临时安全凭证。	Write	agency *	g:ResourceTag/<tag-key>	-
			-	• sts:ExternalId • sts:SourceIdentity • sts:TransitiveTagKeys • sts:AgencySessionName • g:RequestTag/<tag-key> • g:TagKeys	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
				• g:SourceAccount • g:SourceUrn	
sts::decodeAuthorizationMessage	授予权限以从为响应请求而返回的编码消息中解码有关请求授权状态的其他信息。	Write	-	-	-
sts::setSourceIdentity	授予在 STS 会话上设置源身份的权限。	Write	agency *	g:ResourceTag/<tag-key>	-
			-	sts:SourceIdentity	
sts::tagSession	授予权限以将标签添加至 STS 会话。	Tagging	agency *	g:ResourceTag/<tag-key>	-
			-	• sts:TransitiveTagKeys • g:RequestTag/<tag-key> • g:TagKeys	
sts::createServiceBearerToken	授予权限获取一个绑定至某服务的 Bearer Token。	Write	-	• sts:DurationTime • sts:ServiceName	-

STS 的 API 通常对应着一个或多个授权项。表 3-268 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-264 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v5/agencies/assume	sts:agencies:assume	• sts::tagSession • sts::setSourceIdentity
POST /v5/decode-authorization-message	sts::decodeAuthorizationMessage	-

 版权所有 © 华为云计算技术有限公司

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-269 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

STS 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-265 STS 支持的资源类型

资源类型	URN
agency	iam::<account-id>:agency:<agency-name-with-path>

条件（Condition）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 sts:）仅适用于对应服务的操作，详情请参见表 3-270。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

STS 支持的服务级条件键

STS 定义了以下可以在自定义身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-266 STS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
sts:ExternalId	string	单值	按您代入另一个账号中的委托时所需的唯一标识符筛选访问权限。

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
sts:SourceIdentity	string	单值	按照在请求中传递的源身份筛选访问权限。
sts:TransitiveTagKeys	string	多值	按照在请求中传递的可传递标签键筛选访问权限。
sts:AgencySessionName	string	单值	按您代入委托时所需的委托会话名称筛选访问权限。
sts:DurationTime	numeric	单值	按照创建 Bearer Token 的持续时间筛选访问权限。
sts:ServiceName	string	单值	按照创建 Bearer Token 的服务名筛选访问权限。

3.13.13 访问分析 IAM Access Analyzer

云服务在 IAM 预置了常用的权限，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。

 版权所有 © 华为云计算技术有限公司

  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 IAM Access Analyzer 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 IAM Access Analyzer 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 IAM Access Analyzer 的相关操作。

表3-267 IAM Access Analyzer 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
AccessAnalyzer:analyzer:create	授予创建分析器的权限。	Write	analyzer *	-	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
AccessAnalyzer:analyzer:get	授予查询分析器的权限。	Read	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:list	授予查询分析器列表的权限。	List	analyzer *	-	-
AccessAnalyzer:analyzer:delete	授予删除分析器的权限。	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:update	授予更新分析器的权限。	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:scan	授予启动分析器扫描的权限。	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer	授予查询分析	Read	analyz	g:ResourceTag/	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
:analyzer:getFinding	结果的权限。		er *	<tag-key>	
AccessAnalyzer:analyzer:listFindings	授予查询分析结果列表的权限。	List	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:updateFindings	授予更新分析结果的权限。	Write	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer::tagResource	授予给资源添加标签的权限。	Tagging	analyzer *	g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
AccessAnalyzer::untagResource	授予给资源删除标签的权限。	Tagging	analyzer *	g:ResourceTag/<tag-key>	-
			-	g:TagKeys	
AccessAnalyzer:archiveRule:create	授予创建存档规则的权限。	Write	archiveRule *	-	-
AccessAnalyzer:archiveRule:get	授予查询存档规则的权限。	Read	archiveRule *	-	-
AccessAnalyzer:archiveRule:list	授予查询存档规则列表的权限。	List	archiveRule *	-	-
AccessAnalyzer:archiveRule:update	授予更新存档规则的权限。	Write	archiveRule *	-	-
AccessAnalyzer:archiveRule:delete	授予删除存档规则的权限。	Write	archiveRule *	-	-
AccessAnalyzer:archiveRule:apply	授予应用存档规则的权限。	Write	archiveRule *	-	-
AccessAnalyzer:analyzer:createPreview	授予创建访问分析预览的权限。	Write	analyzer *	g:ResourceTag/<tag-key>	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
AccessAnalyzer:analyzer:getPreview	授予查询访问分析预览的权限。	Read	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:listPreviews	授予查询访问分析预览列表的权限。	List	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer:analyzer:listPreviewFindings	授予查询访问分析预览分析结果列表的权限。	List	analyzer *	g:ResourceTag/<tag-key>	-
AccessAnalyzer::validatePolicy	授予验证策略的权限。	Read	-	-	-
AccessAnalyzer::checkNoNewAccess	授予检查更新后的策略是否有新的访问权限。	Read	-	-	-
AccessAnalyzer:notificationSetting:list	授予查询消息通知配置列表的权限。	Read	notificationSetting *	-	-
AccessAnalyzer:notificationSetting:create	授予创建消息通知配置的权限。	Write	notificationSetting *	-	-
AccessAnalyzer:notificationSetting:get	授予查询消息通知配置的权限。	Read	notificationSetting *	-	-
AccessAnalyzer:notificationSetting:update	授予更新消息通知配置的权限。	Write	notificationSetting *	-	-
AccessAnalyzer:notificationSetting:delete	授予删除消息通知配置的权限。	Write	notificationSetting *	-	-

 版权所有 © 华为云计算技术有限公司

IAM Access Analyzer 的 API 通常对应着一个或多个授权项。表 3-272 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-268 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v5/analyzers	AccessAnalyzer:analyzer:create	iam:agencies:createServiceLinkedAgencyV5
GET /v5/analyzers/{analyzer_id}	AccessAnalyzer:analyzer:get	-
GET /v5/analyzers	AccessAnalyzer:analyzer:list	-
DELETE /v5/analyzers/{analyzer_id}	AccessAnalyzer:analyzer:delete	-
PUT /v5/analyzers/{analyzer_id}	AccessAnalyzer:analyzer:update	-
POST /v5/analyzers/{analyzer_id}/scan	AccessAnalyzer:analyzer:scan	-
GET /v5/analyzers/{analyzer_id}/findings/{finding_id}	AccessAnalyzer:analyzer:getFinding	-
POST /v5/analyzers/{analyzer_id}/findings	AccessAnalyzer:analyzer:listFindings	-
PUT /v5/analyzers/{analyzer_id}/findings	AccessAnalyzer:analyzer:updateFindings	-
POST /v5/{resource_type}/{resource_id}/tags/create	AccessAnalyzer::tagResource	-
POST /v5/{resource_type}/{resource_id}/tags/delete	AccessAnalyzer::untagResource	-
POST /v5/analyzers/{analyzer_id}/archive-rules	AccessAnalyzer:archiveRule:create	-
GET /v5/analyzers/{analyzer_id}/archive-	AccessAnalyzer:archiveRule:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
rules/{archive_rule_id}		
GET /v5/analyzers/{analyzer_id}/archive-rules	AccessAnalyzer:archiveRule:list	-
PUT /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}	AccessAnalyzer:archiveRule:update	-
DELETE /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}	AccessAnalyzer:archiveRule:delete	-
POST /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}/apply	AccessAnalyzer:archiveRule:apply	-
POST /v5/analyzers/{analyzer_id}/access-previews	AccessAnalyzer:analyzer:createPreview	-
GET /v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}	AccessAnalyzer:analyzer:getPreview	-
GET /v5/analyzers/{analyzer_id}/access-previews	AccessAnalyzer:analyzer:listPreviews	-
POST /v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}/findings	AccessAnalyzer:analyzer:listPreviewFindings	-
POST /v5/policies/validate	AccessAnalyzer::validatePolicy	-
POST /v5/policies/check-no-new-access	AccessAnalyzer::checkNoNewAccess	-
GET /v5/notification-settings	AccessAnalyzer:notificationSetting:list	-
POST /v5/notification-	AccessAnalyzer:notificationSet	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
settings	ting:create	
GET /v5/notification-settings/{notification_setting_id}	AccessAnalyzer:notificationSetting:get	-
PUT /v5/notification-settings/{notification_setting_id}	AccessAnalyzer:notificationSetting:update	-
DELETE /v5/notification-settings/{notification_setting_id}	AccessAnalyzer:notificationSetting:delete	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-273 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

IAM Access Analyzer 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-269 IAM Access Analyzer 支持的资源类型

资源类型	URN
analyzer	AccessAnalyzer:<region>:<account-id>:analyzer:<analyzer-id>
notificationSetting	AccessAnalyzer:<region>:<account-id>:notificationSetting:<notification-setting-id>
archiveRule	AccessAnalyzer:<region>:<account-id>:archiveRule:<analyzer-id>/<archive-rule-id>

条件（Condition）

IAM Access Analyzer 服务不支持在身份策略中的条件键中配置服务级的条件键。IAM Access Analyzer 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.13.14 资源治理中心 RGC

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

 版权所有 © 华为云计算技术有限公司

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 RGC 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 RGC 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 RGC 的相关操作。

表3-270 RGC 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rgc:control:list	授予列出控制策略的权限。	List	-	-	-
rgc:controlViolation:list	授予列出不合规信息的权限。	List	-	-	-
rgc:control:get	授予获取控制策略详细信息的权限。	Read	-	-	-
rgc:control:enable	授予开启控制策略的权限。	Write	-	-	-
rgc:control:disable	授予关闭控制策略的权限。	Write	-	-	-
rgc:controlOperate:get	授予获取控制策略操作状态的权限。	Read	-	-	-
rgc:enabledControl:list	授予列出开启的控制策略的权限。	List	-	-	-
rgc:controlsForOrganizationalUnit:list	授予列出某个注册组织单元下开启的控制策略的权限。	List	-	-	-
rgc:controlsForAccount:list	授予列出某个纳管账号开启的控制策略的权限。	List	-	-	-
rgc:complianceStatusForAccount:get	授予获取组织里某个纳管账号的资源合规状态的权限。	Read	-	-	-
rgc:complianceStatusForOrganizationalUnit:get	授予获取组织里某个注册组织单元下所有纳管账号的资源合规状态的权限。	Read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rgc:controlsForOrganizationalUnit:get	授予获取某个组织单元开启的控制策略的权限。	Read	-	-	-
rgc:controlsForAccount:get	授予获取某个账号开启的控制策略的权限。	Read	-	-	-
rgc:configRuleCompliance:list	授予列出纳管账号的 Config 规则合规性信息的权限。	List	-	-	-
rgc:externalConfigRuleCompliance:list	授予列出纳管账号的外部 Config 规则合规性信息的权限。	List	-	-	-
rgc:driftDetail:list	授予列出漂移信息的权限。	List	-	-	-
rgc:managedOrganizationalUnit:register	授予注册组织单元的权限。	Write	-	-	-
rgc:managedOrganizationalUnit:reRegister	授予重新注册组织单元的权限。	Write	-	-	-
rgc:managedOrganizationalUnit:deRegister	授予取消注册组织单元的权限。	Write	-	-	-
rgc:operation:get	授予获取注册过程信息的权限。	Read	-	-	-
rgc:managedOrganizationalUnit:delete	授予删除注册组织单元的权限。	Write	-	-	-
rgc:managedOrganizationalUnit:get	授予获取已注册组织单元的	Read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	权限。				
rgc:managedOrganizationalUnit:create	授予创建组织单元的权限。	Write	-	-	-
rgc:managedOrganizationalUnit:list	授予列举控制策略生效的注册组织单元信息的权限。	List	-	-	-
rgc:managedAccount:enroll	授予纳管账号的权限。	Write	-	-	-
rgc:managedAccount:unEnroll	授予取消纳管账号的权限。	Write	-	-	-
rgc:managedAccount:update	授予更新纳管账号的权限。	Write	-	-	-
rgc:managedAccount:get	授予获取纳管账号的权限。	Read	-	-	-
rgc:managedAccountsForParent:list	授予列出注册组织单元下所有纳管账号信息的权限。	List	-	-	-
rgc:managedAccount:create	授予创建账号的权限。	Write	-	-	-
rgc:managedAccount:list	授予列出控制策略生效的纳管账号信息的权限。	List	-	-	-
rgc:managedCoreAccount:get	授予获取核心纳管账号的权限。	Read	-	-	-
rgc:homeRegion:get	授予查询主区域的权限。	Read	-	-	-
rgc:preLaunch:check	授予设置Landing Zone前检查的权限。	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rgc:landingZone:setup	授予设置 Landing Zone 的权限。	Write	-	-	-
rgc:landingZone:delete	授予删除 Landing Zone 的权限。	Write	-	-	-
rgc:landingZoneStatus:get	授予获取查询 Landing Zone 设置状态的权限。	Read	-	-	-
rgc:availableUpdate:get	授予获取 Landing Zone 可更新状态的权限。	Read	-	-	-
rgc:landingZoneConfiguration:get	授予获取 Landing Zone 配置信息的权限。	Read	-	-	-
rgc:landingZoneIdentityCenter:get	授予获取当前客户的 Identity Center 用户信息的权限。	Read	-	-	-
rgc:operation:list	授予获取注册组织单元或纳管账号的当前操作状态的权限。	List	-	-	-
rgc:templateDeployParam:get	授予获取模板部署参数的权限。	Read	-	-	-
rgc:template:create	授予创建模板的权限。	Write	-	-	-
rgc:template:delete	授予删除模板的权限。	Write	-	-	-
rgc:predefinedTemplate:list	授予列出预置模板的权限。	List	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rgc:managedAccountTemplate:get	授予获取纳管账号模板详情的权限。	Read	-	-	-

RGC 的 API 通常对应着一个或多个授权项。表 3-275 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-271 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1/governance/controls	rgc:control:list	-
GET /v1/governance/control-violations	rgc:controlViolation:list	-
GET /v1/governance/controls/{control_id}	rgc:control:get	-
POST /v1/governance/controls/enable	rgc:control:enable	-
POST /v1/governance/controls/disable	rgc:control:disable	-
GET /v1/governance/operation-control-status/{operation_control_status_id}	rgc:controlOperate:get	-
GET /v1/governance/enabled-controls	rgc:enabledControl:list	-
GET /v1/governance/managed-organizational-units/{managed_organizational_unit_id}/controls	rgc:controlsForOrganizationalUnit:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/governance/managed-accounts/{managed_account_id}/controls	rgc:controlsForAccount:list	-
GET /v1/governance/managed-accounts/{managed_account_id}/compliance-status	rgc:complianceStatusForAccount:get	-
GET /v1/governance/managed-organizational-units/{managed_organizational_unit_id}/compliance-status	rgc:complianceStatusForOrganizationalUnit:get	-
GET /v1/governance/managed-organizational-units/{managed_organizational_unit_id}/controls/{control_id}	rgc:controlsForOrganizationalUnit:get	-
GET /v1/governance/managed-accounts/{managed_account_id}/controls/{control_id}	rgc:controlsForAccount:get	-
GET /v1/governance/managed-accounts/{managed_account_id}/config-rule-compliances	rgc:configRuleCompliance:list	-
GET /v1/governance/managed-accounts/{managed_account_id}/external-config-rule-compliances	rgc:externalConfigRuleCompliance:list	-
GET /v1/governance/drift-details	rgc:driftDetail:list	-
POST /v1/managed-organization/organizati	rgc:managedOrganizationalUnit:register	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
onal-units/{organizational_unit_id}/register		
POST /v1/managed-organization/organizational-units/{organizational_unit_id}/re-register	rgc:managedOrganizationalUnit:reRegister	-
POST /v1/managed-organization/managed-organizational-units/{managed_organizational_unit_id}/de-register	rgc:managedOrganizationalUnit:deRegister	-
GET /v1/managed-organization/{operation_id}	rgc:operation:get	-
DELETE /v1/managed-organization/managed-organizational-units/{managed_organizational_unit_id}	rgc:managedOrganizationalUnit:delete	-
GET /v1/managed-organization/managed-organizational-units/{managed_organizational_unit_id}	rgc:managedOrganizationalUnit:get	-
POST /v1/managed-organization/managed-organizational-units	rgc:managedOrganizationalUnit:create	-
GET /v1/managed-organization/managed-organizational-units	rgc:managedOrganizationalUnit:list	-
POST /v1/managed-organization/accounts/{managed_account_id}/enroll	rgc:managedAccount:enroll	-
POST /v1/managed-organization/managed-accounts/{managed_account_id}/un-enroll	rgc:managedAccount:unEnroll	-
POST /v1/managed-organization/managed-accounts/{managed_account_id}/update	rgc:managedAccount:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/managed-organization/managed-accounts/{managed_account_id}	rgc:managedAccount:get	-
GET /v1/managed-organization/managed-organizational-units/{managed_organizational_unit_id}/managed-accounts	rgc:managedAccountsForParent:list	-
POST /v1/managed-organization/managed-accounts	rgc:managedAccount:create	-
GET /v1/managed-organization/managed-accounts	rgc:managedAccount:list	-
GET /v1/managed-organization/managed-core-accounts	rgc:managedCoreAccount:get	-
GET /v1/landing-zone/home-region	rgc:homeRegion:get	-
POST /v1/landing-zone/pre-launch-check	rgc:preLaunch:check	-
POST /v1/landing-zone/setup	rgc:landingZone:setup	-
POST /v1/landing-zone/delete	rgc:landingZone:delete	-
GET /v1/landing-zone/status	rgc:landingZoneStatus:get	-
GET /v1/landing-zone/available-updates	rgc:availableUpdate:get	-
GET /v1/landing-zone/configuration	rgc:landingZoneConfiguration:get	-
GET /v1/landing-zone/identity-center	rgc:landingZoneIdentityCenter:get	-
GET /v1/managed-organization	rgc:operation:list	-
GET /v1/rgc/templates/{template_name}/deploy-params	rgc:templateDeployParam:get	-
POST	rgc:template:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/rgc/templates		
DELETE /v1/rgc/templates/{template_name}	rgc:template:delete	-
GET /v1/rgc/predefined-templates	rgc:predefinedTemplate:list	-
GET /v1/managed-organization/managed-accounts/{managed_account_id}/blueprint	rgc:managedAccountTemplate:get	-

资源类型（Resource）

RGC 服务不支持在身份策略中的资源中指定资源进行权限控制。如需允许访问 RGC 服务，请在身份策略的 Resource 元素中使用通配符号*，表示身份策略将应用到所有资源。

条件（Condition）

RGC 服务不支持在身份策略中的条件键中配置服务级的条件键。RGC 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.13.15 云运维中心 COC

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

 版权所有 © 华为云计算技术有限公司

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 COC 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 COC 定义的条件键的详细信息请参见条件（Condition）。
- **“别名”**列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 COC 的相关操作。

表3-272 COC 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
coc:application:list	授予权限以查询应用列表	list	application	-	-
coc:application:create	授予创建应用的权限	write	application	-	-
coc:application:update	授予修改应用的权限	write	application	-	-
coc:application:delete	授予删除应用的权限	write	application	-	-
coc:application:createGroup	授予创建应用分组的权限	write	application	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
coc:application:listGroups	授予查询指定应用分组列表的权限	list	application	-	-
coc:application:updateGroup	授予修改应用分组的权限	write	application	-	-
coc:application:deleteGroup	授予删除应用分组的权限	write	application	-	-
coc:application:syncGroupResource	授予同步应用分组资源的权限	write	application	-	-
coc:application:updateResources	授予修改应用资源的权限	write	application	-	-
coc:application:addResources	授予为应用添加资源的权限	write	application	-	-
coc:application:removeResources	授予移除应用资源的权限	write	application	-	-
coc:application:listResources	授予查询应用资源列表的权限	list	application	-	-
coc:application:countResourceRelations	授予查询资源关系数量的权限	list	application	-	-
coc:application:getCapacity	授予查询应用中的资源容量的权限	list	application	-	-
coc:application:getSortedCapacity	授予查询应用中有序的资源容量的权限	list	application	-	-
coc:application:listModel	授予查询应用模型的权限	list	application	-	-
coc:vendorAccount:create	授予新增云厂商账户的权限	write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
coc:vendorAccount:list	授予查询云厂商账户的权限	list	-	-	-
coc:vendorAccount:update	授予修改云厂商账户的权限	write	-	-	-
coc:vendorAccount:delete	授予删除云厂商账户的权限	write	-	-	-
coc:resourceView:list	授予查询资源视图的权限	list	-	-	-
coc:resourceView:create	授予创建资源视图的权限	write	resourceView	-	-
coc:resourceView:update	授予更新资源视图的权限	write	resourceView	-	-
coc:resourceView:delete	授予删除资源视图的权限	write	resourceView	-	-
coc:resourceView:syncResources	授予同步某个具体资源视图下的资源列表的权限	write	resourceView	-	-
coc:resourceView:listResources	授予查询某个具体资源视图下的资源列表的权限	list	resourceView	-	-
coc:resourceView:countResources	授予查询某个具体资源视图中资源数量的权限	list	-	-	-
coc:instance:listResources	授予查询资源列表的权限	list	-	-	-
coc:instance:syncResources	授予同步资源列表的权限	write	-	-	-
coc:instance:countOtherResources	授予查询离线资源(如物理机、中间件等)总数的权限	list	-	-	-
coc:instance:listTagsForResource	授予查询资源标签的权限	list	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
coc:instance:addResourceToTags	授予添加资源标签的权限	write	-	-	-
coc:instance:countResources	授予查询资源总数的权限	list	-	-	-
coc::listEpsCollection	授予查询企业项目收藏的权限	list	-	-	coc:enterpriseProject:listCollect
coc::updateEpsCollection	授予修改企业项目收藏的权限	write	-	-	coc:enterpriseProject:updateCollect
coc::getLastSyncStatus	授予查询实例最新同步状态的权限	list	-	-	coc:system:getLastSyncStatus
coc::getResourceSyncJobDetail	授予查询资源同步任务详情的权限	list	-	-	coc:system:getResourceSyncJobDetail
coc:schedule:create	授予创建定时任务的权限。	write	schedule	coc:ApplicationCode coc:ApplicationGroupCode coc:DocumentRiskLevel g:EnterpriseProjectId	-
coc:schedule:list	授予查询定时任务列表的权限。	list	schedule	g:EnterpriseProjectId	-
coc:schedule:update	授予更新定时任务的权限。	write	schedule	coc:ApplicationCode coc:ApplicationGroupCode coc:DocumentRiskLevel g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
coc:schedule:get	授予查询定时任务详情的权限。	read	schedule	g:EnterpriseProjectId	-
coc:schedule:delete	授予删除定时任务的权限。	write	schedule	g:EnterpriseProjectId	-
coc:schedule:enable	授予启用定时任务的权限。	write	schedule	g:EnterpriseProjectId	-
coc:schedule:disable	授予禁用定时任务的权限。	write	schedule	g:EnterpriseProjectId	-
coc:schedule:getHistories	授予查询定时任务执行历史的权限。	read	schedule	g:EnterpriseProjectId	-
coc:instance:executeDocument	授予在弹性云服务器上执行文档的权限	write	instance	• coc:ApplicationId • coc:ApplicationGroupId • g:EnterpriseProjectId	-
			document	• coc:DocumentRiskLevel • g:EnterpriseProjectId	
coc:alarm:clear	授予清除告警的权限	write	-	-	-
coc:alarm:createAlarmLinkedIncident	授予创建告警关联事件的权限	write	-	-	-
coc:alarm:listHandleHistories	授予查询告警处理历史列表的权限	list	-	-	-
coc:alarm:get	授予查询告警信息的权限	list	-	-	-
coc:ticket:list	授予查询事件单列表的权限	list	-	-	-
coc:ticket:create	授予创建事件单的权限	write	-	-	-
coc:ticket:get	授予查询事件单详情的权限	read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
coc:ticket:action	授予处理事件单的权限	write	-	-	-
coc:ticket:delete	授予删除事件单的权限	write	-	-	-
coc:ticket:uploadFile	授予为事件单上传附件的权限	write	-	-	-
coc:warroom:create	授予创建 warroom 的权限	write	-	-	-
coc:ticket:update	授予修改事件单的权限	write	-	-	-
coc:ticket:getOperationHistories	授予查询事件单操作历史的权限	list	-	-	-
coc:ticket:listActions	授予查询可以执行操作列表的权限	list	-	-	-
coc:warroom:list	授予查询 warroom 列表的权限	list	-	-	-
coc:document:analyzeRisk	授予分析文档风险的权限。	read	-	-	-
coc:document:get	授予查看文档内容的权限。	read	-	-	-
coc:document:getDocument	授予查询文档详情权限。	read	document	-	-
coc:document:create	授予创建文档的权限。	write	document	-	-
coc:document:createDocument	授予创建文档权限。	write	document	-	-
coc:document:delete	授予删除文档的权限。	write	document	-	-
coc:document:deleteDocument	授予删除文档权限。	write	document	-	-
coc:document:execute	授予执行文档权限。	write	document	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
coc:document:update	授予修改文档的权限。	write	document	-	-
coc:document:updateDocument	授予更新文档权限。	write	document	-	-
coc:document:list	授予查询文档列表的权限。	list	document	-	-
coc:document:listDocument	授予查询文档列表权限。	list	-	-	-
coc:quota:get	授予查询配额的权限。	read	-	-	-
coc:instance:executeDocument	授予在弹性云服务器上执行文档的权限。	write	instance、document	-	-
coc:job:get	授予查询工单详情的权限。	read	job	-	-
coc:job:action	授予操作工单的权限。	write	job	-	-
coc:job:list	授予查询工单列表的权限。	list	job	-	-
coc:instance:autoBatchInstances	授予为实例自动化分批的权限。	write	-	-	-
coc:documentAtomic:list	授予查询文档原子能力列表权限。	list	-	-	-
coc:documentAtomic:get	授予查询文档原子能力详情权限。	read	-	-	-
coc:execution:get	授予查询执行工单详情权限。	read	-	-	-
coc:execution:listExecutionStep	授予查询执行工单步骤列表权限。	read	-	-	-
coc:execution:list	授予查询执行工单列表权限。	list	-	-	-
coc:execution:listE	授予查询执行工单	read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
xecutionStepInstance	步骤列表权限。				
coc:execution:operate	授予操作执行工单。	write	-	-	-
coc:job:list	授予查询工单列表的权限	list	job	-	-
coc:job:action	授予操作工单的权限	write	job	coc:JobType	-
coc:job:get	授予查询工单详情的权限	read	job	coc:JobType	-

COC 的 API 通常对应着一个或多个授权项。表 3-277 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-273 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1/resources/count	coc:instance:countResources	-
GET /v1/applications	coc:application:list	-
POST /v1/applications	coc:application:create	-
PUT /v1/applications/{id}	coc:application:update	-
DELETE /v1/applications/{id}	coc:application:delete	-
POST /v1/groups	coc:application:createGroup	-
GET /v1/groups	coc:application:listGroups	-
PUT /v1/groups/{id}	coc:application:updateGroup	-
DELETE /v1/groups/{id}	coc:application:deleteGroup	-
POST /v1/groups/{id}/sync	coc:application:syncGroup	-
PUT /v1/group-resource-relations	coc:application:updateResources	-
POST /v1/group-resource-relations	coc:application:addResources	-
DELETE /v1/group-resource-relations	coc:application:removeResources	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/group-resource-relations	coc:application:listResources	-
GET /v1/group-resource-relations/count	coc:application:countResourceRelations	-
POST /v1/other-resources/import	coc:instance:syncResources	-
POST /v1/components	coc:application:create	-
GET /v1/components	coc:application:list	-
PUT /v1/components/{id}	coc:application:update	-
DELETE /v1/components/{id}	coc:application:delete	-
GET /v1/application-view/search	coc:application:list	-
POST /v1/capacity	coc:application:getCapacity	-
GET /v1/capacity/order	coc:application:getSortedCapacity	-
POST /v1/vendor-account	coc:vendorAccount:create	-
GET /v1/vendor-account	coc:vendorAccount:list	-
PUT /v1/vendor-account	coc:vendorAccount:update	-
DELETE /v1/vendor-account	coc:vendorAccount:delete	-
GET /v1/multicloud-resources/count	coc:instance:countResources	-
POST /v1/multicloud-resources/sync	coc:instance:syncResources	-
GET /v1/resource/views	coc:resourceView:list	-
POST /v1/resource/views	coc:resourceView:create	-
PUT /v1/resource/views/{id}	coc:resourceView:update	-
DELETE /v1/resource/views/{id}	coc:resourceView:delete	-
POST /v1/resource/views/{id}/sync	coc:resourceView:syncResources	-
GET /v1/resource/views/resources	coc:resourceView:listResources	-
GET /v1/resource/views/resources/count	coc:resourceView:countResources	-
GET /v1/other-resources	coc:instance:listResources	-
DELETE /v1/other-resources	coc:instance:syncResources	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v1/other-resources/{id}	coc:instance:syncResources	-
GET /v1/other-resources/count	coc:instance:countOtherResources	-
GET /v1/resources/{resource_id}/tags	coc:instance:listResourceTags	-
POST /v1/resources/{resource_id}/tags	coc:instance:addResourceToTags	-
POST /v1/resources/uniagent/sync	coc:instance:syncResources	-
POST /v1/other-resources/uniagent/sync	coc:instance:syncResources	-
GET /v1/enterprise-project-collect	coc:enterpriseProject:listCollect	-
PUT /v1/enterprise-project-collect	coc:enterpriseProject:updateCollect	-
GET /v1/multicloud-resources/last-sync-status	coc:system:getLastSyncStatus	-
GET /v1/jobs/{job_id}	coc:system:getResourceSyncJobDetail	-
GET /v1/multicloud-resources	coc:instance:listResources	-
GET /v1/application-model/next	coc:application:listModel	-
POST /v1/application-view/batch-create	coc:application:create	-
GET /v1/resources	coc:instance:listResources	-
GET /v1/resources/multi-count	coc:instance:countResources	-
POST /v1/schedule/task	coc:schedule:create	iam:agencies:pass（授予向云服务传递委托的权限）
GET /v1/schedule/task	coc:schedule:list	-
PUT /v1/schedule/task/{task_id}	coc:schedule:update	iam:agencies:pass（授予向云服务传递委托的权限）
GET /v1/schedule/task/{task_id}	coc:schedule:get	-
DELETE /v1/schedule/task/{task_id}	coc:schedule:delete	-
POST /v1/schedule/task/{task_id}/enabl	coc:schedule:enable	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
e		
POST /v1/schedule/task/{task_id}/disable	coc:schedule:disable	-
GET /v1/schedule/task/history	coc:schedule:getHistories	-
POST /v1/alarm-mgmt/alarm/{alarm_id}/auto-process	coc:instance:executeDocument	-
POST /v1/alarm-mgmt/alarms/cancel	coc:alarm:clear	-
POST /v1/alarm-mgmt/alarms-linked-incident	coc:alarm:createAlarmLinkedIncident	-
GET /v1/alarm-mgmt/alarm/{alarm_id}/handle-histories	coc:alarm:listHandleHistories	-
GET /v1/alarm-mgmt/alarm/{alarm_id}	coc:alarm:get	-
POST /v2/incidents/{incident_id}/actions	coc:ticket:action	-
POST /v2/incidents/list	coc:ticket:list	-
POST /v2/incidents/{incident_id}/histories	coc:ticket:getOperationHistories	-
GET /v2/incidents/{incident_id}/tasks	coc:ticket:listActions	-
POST /v1/external/incident/create	coc:ticket:create	-
POST /v1/external/incident/attachments	coc:ticket:uploadFile	-
POST /v1/external/incident/handle	coc:ticket:action	-
POST /v1/external/{ticket_type}/list-histories	coc:ticket:getOperationHistories	-
GET /v1/incident-tickets	coc:ticket:list	-
GET /v1/external/incident/{incident_num}	coc:ticket:get	-
POST /v1/external/issues/create	coc:ticket:create	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v1/external/issues/{ticket_id}	coc:ticket:get	-
POST /v1/external/warrooms	coc:warroom:create	-
POST /v1/external/warrooms/list	coc:warroom:list	-
POST /v1/instances/batches	coc:instance:autoBatchInstances	-
POST /v1/job/analyze-job	coc:document:analyzeRisk	-
POST /v1/job/scripts/{script_uuid}	coc:instance:executeDocument	-
POST /v1/job/public-scripts/{script_uuid}	coc:instance:executeDocument	-
GET /v1/job/scripts	coc:document:list	-
GET /v1/job/scripts/{script_uuid}	coc:document:get	-
POST /v1/job/scripts	coc:document:create	-
PUT /v1/job/scripts/{script_uuid}	coc:document:update	-
DELETE /v1/job/scripts/{script_uuid}	coc:document:delete	-
POST /v1/job/scripts/{script_uuid}/action	coc:document:update	-
GET /v1/job/public-scripts	coc:document:list	-
GET /v1/job/public-scripts/{script_uuid}	coc:document:get	-
GET /v1/job/script/orders	coc:job:list	-
GET /v1/job/script/orders/{execute_uuid}	coc:job:get	-
GET /v1/job/script/orders/{execute_uuid}/batches/{batch_index}	coc:job:get	-
GET /v1/job/script/orders/{execute_uuid}/batches	coc:job:get	-
GET /v1/job/script/orders/{execute_uuid}/statistics	coc:job:get	-
PUT /v1/job/script/orders/{execute_uui	coc:job:action	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
d}/operation		
GET /v1/documents	coc:document:createDocument	-
POST /v1/documents	coc:document:listDocument	-
GET /v1/atomics	coc:documentAtomic:list	-
GET /v1/atomics/{atomic_unique_key}	coc:documentAtomic:get	-
PUT /v1/documents/{document_id}	coc:document:updateDocument	-
POST /v1/documents/{document_id}	coc:document:execute	-
GET /v1/documents/{document_id}	coc:document:getDocument	-
DELETE /v1/documents/{document_id}	coc:document:deleteDocument	-
GET /v1/executions/{execution_id}	coc:execution:get	-
GET /v1/executions/{execution_id}/steps	coc:execution:listExecutionStep	-
GET /v1/executions	coc:execution:list	-
GET /v1/executions/instances	coc:execution:listExecutionStepInstance	-
POST /v1/executions	coc:execution:operate	-
GET /v1/diagnosis/tasks	coc:job:list	-
POST /v1/diagnosis/tasks	coc:job:action	aom:uniagentAgent:install aom:uniagentAgent:uninstall dcs:instance:createDiagnosisTask dcs:instance:listDiagnosisTask dms:instance:getDetail dms:instance:getDiagnosisReport dms:instance:createDiagnosisTask dms:instance:listDiagnosisReport

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
		elb:members:show rds:instance:listAll
GET /v1/diagnosis/tasks/{task_id}/node/{code}	coc:job:get	-
GET /v1/diagnosis/tasks/{task_id}	coc:job:get	-
POST /v1/diagnosis/tasks/{task_id}/retry	coc:job:action	aom:uniagentAgent:install aom:uniagentAgent:uninstall dcs:instance:createDiagnosisTask dcs:instance:listDiagnosisTask dms:instance:getDetail dms:instance:getDiagnosisReport dms:instance:createDiagnosisTask dms:instance:listDiagnosisReport elb:members:show rds:instance:listAll
POST /v1/diagnosis/tasks/{task_id}/cancel	coc:job:action	-
GET /v1/diagnosis/tasks/{task_id}/summary	coc:job:action	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的策略语句中指定该资源的 URN，策略仅作用于此资源；如未指定，Resource 默认为“*”，则策略将应用到所有资源。您也可以在策略中设置条件，从而指定资源类型。

COC 定义了以下可以在策略的 Resource 元素中使用的资源类型。

 版权所有 © 华为云计算技术有限公司

表3-274 COC 支持的资源类型

资源类型	URN
instance	ecs:<region>:<account-id>:instance:<server-id>
document	coc::<account-id>:document:<document-name>
application	coc::<account-id>:application:<application-code>
resourceView	coc::<account-id>:resourceView:<resourceViewId>
schedule	coc::<account-id>:schedule:<schedule-id>
job	coc::<account-id>:job:<job-id>
faultMode	coc::<account-id>:faultMode:<fault-mode-id>
contingencyPlan	coc::<account-id>:contingencyPlan:<contingency-plan-id>
attackTask	coc::<account-id>:attackTask:<attack-task-name>
attackRecord	coc::<account-id>:attackRecord:<attack-record-id>
drillTask	coc::<account-id>:drillTask:<drill-task-id>
attackTargetRecord	coc::<account-id>:attackTargetRecord:<attack-target-record-id>
drillRecord	coc::<account-id>:drillRecord:<drill-record-id>
drillPlan	coc::<account-id>:drillPlan:<drill-plan-id>
slaTemplate	coc::<account-id>:slaTemplate:<sla_template-id>
parameter	coc:<region>:<account-id>:parameter:<parameter-name>
accountBaseline	coc::<account-id>:accountBaseline:<account_baseline_id>
provisionedProduct	coc::<account-id>:provisionedProduct:<provisioned-product-id>
product	coc::<account-id>:product:<product-id>
portfolio	coc::<account-id>:portfolio:<portfolio-id>
sloDiagram	coc::<account-id>:sloDiagram:<diagram-id>
template	coc::<account-id>:template:<template-id>
templateInstance	coc::<account-id>:templateInstance:<template-instance-id>

条件（Condition）

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

 版权所有 © 华为云计算技术有限公司

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 coc:）仅适用于对应服务的操作，详情请参见表 4。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

COC 定义了以下可以在身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-275 COC 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
coc:TicketLevel	String	单值	根据请求参数中的工单级别进行过滤访问。
coc:TicketCurrentHandlers	String	多值	根据请求参数中的工单操作人进行过滤访问。
coc:TicketStatus	String	单值	根据请求参数中的工单状态进行过滤访问。
coc:TicketType	String	单值	根据请求参数中的工单类型进行过滤访问。
coc:TicketBeginTime	date	单值	根据请求参数中的工单开始时间进行过滤访问。
coc:TicketEndTime	date	单值	根据请求参数中的工单结束时间进行过滤访问。
coc:OperatorName	String	单值	根据请求参数中的操作人进行过滤访问。
coc:RequestTarget	String	单值	根据请求参数中的提权应用进行过滤访问。
coc:TicketTarget	String	多值	根据请求参数中的工单应用进行过滤访问。
coc:TicketScope	String	多值	根据请求参数中的工单的范围进行过滤

 版权所有 © 华为云计算技术有限公司

服务级条件键	类型	单值/多值	说明
			访问。
coc:RequestScope	String	单值	根据请求参数中的提权范围进行过滤访问。
coc:EscapeSwitchIsEnabled	boolean	单值	根据请求参数中的逃生开关进行过滤访问。
coc:Creator	String	单值	根据 COC 中的资源的创建人过滤访问。
coc:Executor	String	单值	根据 COC 中的工单指定的执行人过滤访问。
coc:DocumentRiskLevel	String	单值	根据请求参数中指定的文档风险等级过滤访问。
coc:JobType	String	单值	根据请求参数中指定的工单类型过滤访问。
coc:ApplicationCode	String	多值	根据请求参数中指定的应用编码过滤访问。
coc:ApplicationGroupCode	String	单值	根据请求参数中指定的应用分组编码过滤访问。
coc:AttackTargetType	String	单值	根据请求参数中攻击目标的类型进行过滤访问。
coc:QuickSetupType	String	单值	根据请求参数中请求配置类型进行过滤访问。

3.13.16 应用性能管理 APM

云服务在 IAM 预置了常用的权限，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

 版权所有 © 华为云计算技术有限公司

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 APM 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 APM 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 APM 的相关操作。

表3-276 APM 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apm:application:list	授予获取应用信息列表的权限。	List	-	-	apm:apm2BusinessBusiness:list
apm:application:getService	授予获取服务信息数据的权限。	Read	-	g:EnterpriseProjectId	apm:apm2Service:get
apm::retrieveCredential	授予获取接入凭证的权限。	Permission_management	-	-	apm:apm2AkSk:read
apm::createCre	授予创建接入	Permi	-	-	apm:apm2AkSk

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dential	凭证的权限。	ssion_management			:create
apm::deleteCredential	授予删除接入凭证的权限。	Permission_management	-	-	apm:apm2AkSk:delete
apm:application:get	授予获取应用信息数据的权限。	Read	-	g:EnterpriseProjectId	apm:apm2BusinessBusiness:get
apm:application:updateInstance	授予修改实例的权限。	Write	-	g:EnterpriseProjectId	apm:apm2BusinessInstance:update
apm:application:deleteInstance	授予删除实例的权限。	Write	-	g:EnterpriseProjectId	apm:apm2BusinessInstance:delete
apm:application:getInstance	授予获取实例信息数据的权限。	Read	-	g:EnterpriseProjectId	apm:apm2BusinessInstance:get
apm:application:getEnv	授予获取环境信息数据的权限。	Read	-	g:EnterpriseProjectId	apm:apm2BusinessEnv:get
apm:application:getMonitorItemConf	授予获取监控项配置数据的权限。	Read	-	g:EnterpriseProjectId	apm:apm2BusinessMonitorItem:get
apm:application:updateMonitorItemConf	授予修改监控项配置的权限。	Write	-	g:EnterpriseProjectId	apm:apm2BusinessMonitorItem:update
apm:application:delete	授予删除应用的权限。	Write	-	g:EnterpriseProjectId	apm:apm2BusinessBusiness:delete
apm::getTopology	授予获取拓扑数据的权限。	Read	-	-	apm:apm2BusinessTopology:get apm:apm2TraceTopology:get
apm::updateConf	授予修改配置的权限。	Write	-	-	apm:apm2Service:update

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apm:application:getTransaction	授予获取事务数据的权限。	Read	-	g:EnterpriseProjectId	apm:apm2BusinessBusiness:get
apm::createAdminInfo	授予创建系统管理的权限。	Write	-	g:EnterpriseProjectId	apm:apm2Admin:create
apm:application:update	授予修改应用的权限。	Write	-	g:EnterpriseProjectId	apm:apm2BusinessBusiness:update
apm::getConf	授予获取配置数据的权限。	Read	-	-	apm:apm2BusinessView:get apm:apm2Service:get
apm:application:getTraceEvents	授予获取自研版调用链数据的权限。	Write	-	g:EnterpriseProjectId	apm:apm2TraceEvent:get apm:apm2TraceEvents:get apm:apm2BusinessSpanSearch:get
apm:application:listTagsForResource	授予查询应用标签列表权限。	Read	application *	-	apm:apm2BusinessBusiness:list
			-	g:ResourceTag/<tag-key>	
apm:application:tagResource	授予创建应用标签权限。	Tagging	application *	-	apm:apm2BusinessBusiness:list
			-	g:ResourceTag/<tag-key>	
apm:application:unTagResource	授予权限以删除应用标签。	Tagging	application *	-	apm:apm2BusinessBusiness:list
			-	g:ResourceTag/<tag-key>	
apm:application:create	授予创建应用的权限。	Write	-	g:EnterpriseProjectId	apm:apm2BusinessBusiness:create
apm::deleteAdminInfo	授予删除系统管理的权限。	Write	-	-	apm:apm2Admin:delete
apm::getAdmin	授予查询系统	Read	-	-	apm:apm2Admi

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
Info	管理的权限。				n:get
apm::updateAdminInfo	授予更新系统管理的权限。	Write	-	-	apm:apm2Admin:update
apm::getAlarmData	授予获取告警数据的权限。	Read	-	-	apm:apm2BusinessBusiness:get
apm::createAlarmRule	授予创建告警规则的权限。	Write	-	-	apm:apm2BusinessBusiness:create
apm::deleteAlarmRule	授予删除告警规则的权限。	Write	-	-	apm:apm2BusinessBusiness:delete
apm::getAlarmRule	授予获取告警规则的权限。	Read	-	-	apm:apm2BusinessBusiness:get
apm::listAlarmRule	授予获取告警规则列表的权限。	List	-	-	apm:apm2BusinessBusiness:get
apm::updateAlarmRule	授予修改告警规则的权限。	Write	-	-	apm:apm2BusinessBusiness:update
apm::updateCredential	授予修改接入凭证的权限。	Permission_management	-	-	apm:apm2AkSk:update

APM 的 API 通常对应着一个或多个授权项。表 3-281 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-277 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1/apm2/access-keys	apm::retrieveCredential	-
POST /v1/apm2/access-keys	apm::createCredential	-
DELETE /v1/apm2/access-keys/{ak}	apm::deleteCrede	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
	ntial	
POST /v1/apm2/openapi/alarm/data/get-alarm-data-list	apm:application:get	-
POST /v1/apm2/openapi/alarm/data/get-alarm-notify-list	apm:application:get	-
POST /v1/apm2/openapi/apm-service/agent-mgr/change-status	apm:application:updateInstance	-
POST /v1/apm2/openapi/apm-service/agent-mgr/delete-agent	apm:application:deleteInstance	-
POST /v1/apm2/openapi/apm-service/agent-mgr/search	apm:application:getInstance	-
POST /v1/apm2/openapi/apm-service/app-mgr/search	apm:application:getEnv	-
POST /v1/apm2/openapi/apm-service/monitor-item-mgr/get-env-monitor-item-list	apm:application:getMonitorItemConf	-
GET /v1/apm2/openapi/apm-service/monitor-item-mgr/get-monitor-item-detail	apm:application:getMonitorItemConf	-
POST /v1/apm2/openapi/apm-service/monitor-item-mgr/save-monitor-item-config	apm:application:updateMonitorItemConf	-
DELETE /v1/apm2/openapi/cmdb/apps/delete-app/{application_id}	apm:application:delete	-
GET /v1/apm2/openapi/cmdb/apps/get-apps	apm:application:get	-
GET /v1/apm2/openapi/cmdb/business/get-business-detail/{business_id}	apm:application:get	-
GET /v1/apm2/openapi/cmdb/business/get-business-list	apm:application:list	-
GET /v1/apm2/openapi/cmdb/envs/get-app-envs	apm:application:getEnv	-
GET /v1/apm2/openapi/cmdb/sub-business/get-sub-business-detail/{sub_business_id}	apm:application:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/apm2/openapi/cmdb/tag/get-env-tag-list	apm:application:get	-
GET /v1/apm2/openapi/cmdb/topology-trees/get-topology-trees	apm::getTopology	-
GET /v1/apm2/openapi/region/get-all-supported-region	apm:application:getService	-
GET /v1/apm2/openapi/region/get-opened-region	apm:application:getService	-
GET /v1/apm2/openapi/systemmng/get-ak-sk-list	apm::retrieveCredential	-
GET /v1/apm2/openapi/systemmng/get-master-address	apm:application:getService	-
POST /v1/apm2/openapi/topology/business-search	apm:application:getTransaction	-
POST /v1/apm2/openapi/topology/env-search	apm:application:getTransaction	-
POST /v1/apm2/openapi/tracing/access/get-access-point/{business_id}	apm:application:get	-
POST /v1/apm2/openapi/tracing/business/create	apm::createAdminInfo	-
GET /v1/apm2/openapi/tracing/business/token/{business_id}	apm:application:update	-
POST /v1/apm2/openapi/transaction/buiness-env	apm:application:get	-
POST /v1/apm2/openapi/transaction/detail	apm:application:getTransaction	-
POST /v1/apm2/openapi/transaction/search	apm:application:getTransaction	-
POST /v1/apm2/openapi/transaction/transaction-config-search	apm:application:getTransaction	-
GET	apm::getConf	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v1/apm2/openapi/view/config/get-monitor-item-view-config		
POST /v1/apm2/openapi/view/mainview/get-env-instance-list	apm:application:getInstance	-
GET /v1/apm2/openapi/view/mainview/get-env-monitor-item-list	apm:application:getMonitorItemConf	-
POST /v1/apm2/openapi/view/metric/get-clob-detail	apm::getConf	-
POST /v1/apm2/openapi/view/metric/raw-table	apm::getConf	-
POST /v1/apm2/openapi/view/metric/sum-table	apm::getConf	-
POST /v1/apm2/openapi/view/metric/trend	apm::getConf	-
POST /v1/apm2/openapi/view/profiling/flame-line-tree	apm::getTopology	-
GET /v1/apm2/openapi/view/trace/get-event-detail	apm:application:getTraceEvents	-
GET /v1/apm2/openapi/view/trace/get-trace-events	apm:application:getTraceEvents	-
POST /v1/apm2/openapi/view/trace/span-search	apm:application:getTraceEvents	-
GET /v1/apm2/openapi/view/trace/topology	apm::getTopology	-
GET /v2/{resource_type}/{resource_id}/tags	apm:application:listTagsForResource	-
POST /v2/{resource_type}/{resource_id}/tags/create	apm:application:tagResource	-
DELETE /v2/{resource_type}/{resource_id}/tags/delete	apm:application:unTagResource	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v2/{resource_type}/resource-instances/count	apm:application:listTagsForResource	-
POST /v2/{resource_type}/resource-instances/filter	apm:application:listTagsForResource	-
GET /v2/{resource_type}/tags	apm:application:listTagsForResource	-
POST /v2/account-mgt/business/create-account	apm:application:create	-
DELETE /v2/account-mgt/business/delete/{id}	apm:application:delete	-
POST /v2/account-mgt/business/get-accounts	apm:application:get	-
PUT /v2/account-mgt/business/update-account	apm:application:update	-
POST /v2/account-mgt/domain/create-account	apm::createAdminInfo	-
DELETE /v2/account-mgt/domain/delete/{id}	apm::deleteAdminInfo	-
POST /v2/account-mgt/domain/get-accounts	apm::getAdminInfo	-
PUT /v2/account-mgt/domain/update-account	apm::updateAdminInfo	-
GET /v2/alarm/data/get-alarm-data-detail/{alarm_data_id}	apm::getAlarmData	-
POST /v2/alarm/data/get-alarm-data-list	apm:application:get	-
GET /v2/alarm/data/get-alarm-notify-detail/{alarm_data_notify_id}	apm::getAlarmData	-
POST /v2/alarm/data/get-alarm-notify-list	apm:application:get	-
POST /v2/alarm/rule/create-alarm-rule	apm::createAlarmRule	-
DELETE /v2/alarm/rule/delete-alarm-rule/{alarm_rule_id}	apm::deleteAlarmRule	-
GET /v2/alarm/rule/get-alarm-rule-detail	apm::getAlarmRule	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v2/alarm/rule/get-alarm-rule-list	apm::listAlarmRule	-
PUT /v2/alarm/rule/update-alarm-rule	apm::updateAlarmRule	-
PUT /v2/alarm/rule/update-alarm-rule-status	apm::updateAlarmRule	-
POST /v2/alarm/template/copy-template	apm::createAlarmRule	-
POST /v2/alarm/template/create-template-alarm-rule	apm::createAlarmRule	-
POST /v2/alarm/template/create-template-base	apm::createAlarmRule	-
POST /v2/alarm/template/create-template-recommend	apm::createAlarmRule	-
DELETE /v2/alarm/template/delete-template-alarm-rule/{alarm_rule_id}	apm::deleteAlarmRule	-
DELETE /v2/alarm/template/delete-template-relation	apm::deleteAlarmRule	-
DELETE /v2/alarm/template/delete-template/{template_id}	apm::deleteAlarmRule	-
GET /v2/alarm/template/get-template-alarm-rule-detail/{template_alarm_rule_id}	apm::getAlarmRule	-
GET /v2/alarm/template/get-template-alarm-rule-list	apm::listAlarmRule	-
GET /v2/alarm/template/get-template-base/{template_id}	apm::getAlarmRule	-
GET /v2/alarm/template/get-template-list	apm::listAlarmRule	-
GET /v2/alarm/template/get-template-relation-env-list	apm::listAlarmRule	-
GET /v2/alarm/template/get-template-relation-list	apm::listAlarmRule	-
PUT /v2/alarm/template/update-template-alarm-rule	apm::updateAlarmRule	-
PUT /v2/alarm/template/update-template-alarm-rule-env-status	apm::updateAlarmRule	-
PUT /v2/alarm/template/update-template-alarm-rule-status	apm::updateAlarmRule	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v2/cmdb/topology-trees/get-topology-trees	apm::getTopology	-
POST /v2/cmdb/tag/get-env-tag-list	apm:application:get	-
GET /v2/cmdb/apps/get-apps	apm:application:get	-
GET /v2/cmdb/envs/get-app-envs	apm:application:getEnv	-
GET /v2/cmdb/apps/{application_id}	apm:application:get	-
DELETE /v2/cmdb/apps/{application_id}	apm:application:delete	-
GET /v2/cmdb/business/get-business-detail/{business_id}	apm:application:get	-
GET /v2/cmdb/sub-business/get-sub-business-detail/{sub_business_id}	apm:application:get	-
GET /v2/view/config/get-monitor-item-view-config	apm::getConf	-
GET /v2/view/trace/topology	apm::getTopology	-
GET /v2/view/trace/get-event-detail	apm:application:getTraceEvents	-
POST /v2/view/trace/span-search	apm:application:getTraceEvents	-
GET /v2/view/trace/get-trace-events	apm:application:getTraceEvents	-
POST /v2/view/metric/trend	apm::getConf	-
POST /v2/view/metric/sum-table	apm::getConf	-
POST /v2/view/metric/raw-table	apm::getConf	-
POST /v2/view/metric/get-clob-detail	apm::getConf	-
POST /v2/view/mainview/get-env-instance-list	apm:application:getInstance	-
GET /v2/view/mainview/get-env-monitor-item-list	apm:application:getMonitorItemConf	-
POST /v2/systemmng/access-ak-sk/create-ak-sk	apm::createCredential	-
POST /v2/systemmng/access-ak-	apm::deleteCrede	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
sk/delete-ak-sk	ntial	
GET /v2/systemmng/access-ak-sk/get-ak-sk-list	apm::retrieveCredential	-
POST /v2/systemmng/access-ak-sk/update-ak-sk	apm::updateCredentntial	-
POST /v2/topology/business-search	apm:application:getTransaction	-
POST /v2/topology/env-search	apm:application:getTransaction	-
POST /v2/transaction/transaction-config-search	apm:application:getTransaction	-
POST /v2/transaction/business-env	apm:application:get	-
POST /v2/transaction/search	apm:application:getTransaction	-
POST /v2/transaction/detail	apm:application:get	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的 URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

APM 服务定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-278 APM 支持的资源类型

资源类型	URN
application	apm::<account-id>:application:<application-id>

条件（Condition）

APM 服务不支持在身份策略中的条件键中配置服务级的条件键。APM 服务可以使用适用于所有服务的全局条件键，请参考全局条件键。

 版权所有 © 华为云计算技术有限公司

3.13.17 应用运维管理 AOM

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policy，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（List、Read 和 Write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 AOM 定义的资源类型的详细信息请参见资源类型（Resource）。
- “条件键”列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 AOM 定义的条件键的详细信息请参见条件（Condition）。
- “别名”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 AOM 的相关操作。

 版权所有 © 华为云计算技术有限公司

表3-279 AOM 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
aom:view:delete	授予权限以删除仪表盘。	Write	-	-	-
aom:view:get	授予权限以获取仪表盘。	Read	-	-	-
aom:view:create	授予权限以创建仪表盘。	Write	-	-	-
aom:metric:delete	授予权限以删除监控配置信息。	Write	-	-	-
aom:icmgr:get	授予权限以获取采集组件版本信息。	Read	-	-	-
aom:agency:get	授予权限以查询委托权限。	Read	-	-	-
aom:icmgr:list	授予权限以获取采集组件版本信息。	List	-	-	-
aom:metric:set	授予权限以修改监控配置。	Write	-	-	-
aom:metric:list	授予权限以查询指标项。	List	-	-	aom:metric:get
aom:metric:put	授予权限以上报指标。	Write	-	-	-
aom:discoveryRule:set	授予权限以创建或者更新服务发现规则列表。	Write	-	-	-
aom:discoveryRule:delete	授予权限以删除服务发现规则列表。	Write	-	-	-
aom:discoveryRule:list	授予权限以查询服务发现规则列表。	List	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
aom:alarmRule:create	授予权限以创建告警规则。	Write	alarmRule *	g:ResourceTag/<tag-key>	-
			-	• g:TagKeys • g:RequestTag/<tag-key>	
aom:alarmRule:list	授予权限以查询告警规则列表。	List	-	-	-
aom:alarmRule:update	授予权限以更新告警规则。	Write	-	-	aom:alarmRule:set
aom:alarmRule:delete	授予权限以删除告警规则。	Write	alarmRule *	g:ResourceTag/<tag-key>	-
aom:alarm:put	授予权限以上报告警和事件。	Write	-	-	-
aom:alarmRule:get	授予权限以查询告警规则。	Read	-	-	-
aom:uniagentAgent:install	授予权限以安装 UniAgent。	Write	-	-	-
aom:uniagentAgent:upgrade	授予权限以升级 UniAgent。	Write	-	-	-
aom:uniagentAgent:list	授予权限以查看 UniAgent 列表。	List	-	-	-
aom:event2AlarmRule:list	授予权限以查询事件类告警规则列表。	List	-	-	-
aom:event2AlarmRule:create	授予权限以创建事件类告警规则。	Write	-	-	-
aom:event2AlarmRule:update	授予权限以更新事件类告警规则。	Write	-	-	aom:event2AlarmRule:set
aom:event2AlarmRule:delete	授予权限以删除事件类告警	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	规则。				
aom:muteRule:create	授予权限以创建静默规则。	Write	-	-	-
aom:muteRule:list	授予权限以查询静默规则列表。	List	-	-	-
aom:muteRule:update	授予权限以更新静默规则。	Write	-	-	-
aom:muteRule:delete	授予权限以删除静默规则。	Write	-	-	-
aom:actionRule:get	授予权限以查询行动规则。	Read	-	-	-
aom:actionRule:list	授予权限以查询行动规则列表。	List	-	-	-
aom:actionRule:create	授予权限以创建行动规则。	Write	-	-	-
aom:actionRule:update	授予权限以修改行动规则。	Write	-	-	-
aom:actionRule:delete	授予权限以删除行动规则。	Write	-	-	-
aom:alarm:list	授予权限以查询告警和事件。	List	-	-	-
aom:notificationTemplate:create	授予权限以创建告警消息模板。	Write	-	-	-
aom:notificationTemplate:delete	授予权限以删除告警消息模板。	Write	-	-	-
aom:notificationTemplate:update	授予权限以更新告警消息模板。	Write	-	-	-
aom:notificatio	授予权限以获	List	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
nTemplate:list	取告警消息模板列表。				
aom:notificationTemplate:get	授予权限以获取告警消息模板列表。	Read	-	-	-
aom:routeGroupRule:delete	授予权限以删除分组规则。	Write	-	-	-
aom:routeGroupRule:create	授予权限以创建分组规则。	Write	-	-	-
aom:routeGroupRule:update	授予权限以更新分组规则。	Write	-	-	-
aom:routeGroupRule:list	授予权限以获取分组规则列表。	List	-	-	-
aom:inhibitRule:delete	授予权限以删除抑制规则。	Write	-	-	-
aom:inhibitRule:create	授予权限以创建抑制规则。	Write	-	-	-
aom:inhibitRule:update	授予权限以更新抑制规则。	Write	-	-	-
aom:inhibitRule:list	授予权限以获取抑制规则列表。	List	-	-	-
aom:alarmRuleTemplate:list	授予权限以查询告警规则模板 V4 列表。	List	-	-	-
aom:alarmRuleTemplate:delete	授予权限以删除告警规则模板 V4。	Write	-	-	-
aom:alarmRuleTemplate:create	授予权限以创建告警规则模板 V4。	Write	-	-	-
aom:alarmRuleTemplate:set	授予权限以更新告警规则模	Write	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	板 V4。				

AOM 的 API 通常对应着一个或多个授权项。表 3-284 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-280 API 与授权项的关系

API	对应的授权项	依赖的授权项
DELETE /v2/{project_id}/aom/dashboards/{dashboard_id}	aom:view:delete	-
GET /v2/{project_id}/aom/dashboards	aom:view:get	-
GET /v2/{project_id}/aom/dashboards/{dashboard_id}	aom:view:get	-
DELETE /v2/{project_id}/aom/dashboards-folder/{folder_id}	aom:view:delete	-
GET /v2/{project_id}/aom/dashboards-folder	aom:view:get	-
PUT /v2/{project_id}/aom/dashboards-folder/{folder_id}	aom:view:create	-
DELETE /v1/{project_id}/aom/prometheus	aom:metric:delete	-
GET /v1/{project_id}/aom/prometheus	aom:metric:list	-
POST /v1/{project_id}/aom/prometheus	aom:metric:put	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/aom/prometheus	aom:metric:set	-
POST /v1/{project_id}/{prometheus_instance}/aom/api/v1/rules	aom:metric:put	-
GET /v1/{project_id}/access-code	aom:icmgr:get	-
GET /v1/{project_id}/aom/auth/grant	aom:agency:get	-
GET /v1/{project_id}/{cluster_id}/{namespace}/agents	aom:icmgr:list	-
GET /v1/{project_id}/{prometheus_instance}/aom/api/v1/rules	aom:metric:list	-
PUT /v1/{project_id}/{prometheus_instance}/aom/api/v1/rules/{rule_id}	aom:metric:put	-
POST /v2/{project_id}/series	aom:metric:list	-
POST /v2/{project_id}/samples	aom:metric:list	-
GET /v1/{project_id}/aom/api/v1/query_range	aom:metric:list	-
POST /v1/{project_id}/aom/api/v1/query_range	aom:metric:list	-
GET /v1/{project_id}/aom/api/v1/query	aom:metric:list	-
POST /v1/{project_id}/aom/api/v1/query	aom:metric:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/{prometheus_instance}/aom/api/v1/query	aom:metric:list	-
GET /v1/{project_id}/{prometheus_instance}/aom/api/v1/query	aom:metric:list	-
POST /v1/{project_id}/{prometheus_instance}/aom/api/v1/query_range	aom:metric:list	-
POST /v1/{project_id}/{prometheus_instance}/aom/api/v1/series	aom:metric:list	-
GET /v1/{project_id}/aom/api/v1/label/{label_name}/values	aom:metric:list	-
GET /v1/{project_id}/{prometheus_instance}/aom/api/v1/label/{label_name}/values	aom:metric:list	-
GET /v1/{project_id}/aom/api/v1/labels	aom:metric:list	-
POST /v1/{project_id}/aom/api/v1/labels	aom:metric:list	-
POST /v1/{project_id}/{prometheus_instance}/aom/api/v1/labels	aom:metric:list	-
GET /v1/{project_id}/aom/api/v1/metadata	aom:metric:list	-
GET /v1/{project_id}/{prometheus_instance}/aom/api/v1/metadata	aom:metric:list	-
POST /v1/{project_id}/ams/metrics	aom:metric:list	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/ams/metricdata	aom:metric:list	-
POST /v1/{project_id}/ams/report/metricdata	aom:metric:put	-
PUT /v1/{project_id}/inv/servicediscoveryrules	aom:discoveryRule:set	-
DELETE /v1/{project_id}/inv/servicediscoveryrules	aom:discoveryRule:delete	-
GET /v1/{project_id}/inv/servicediscoveryrules	aom:discoveryRule:list	-
POST /v2/{project_id}/alarm-rules	aom:alarmRule:create	-
GET /v2/{project_id}/alarm-rules	aom:alarmRule:list	-
PUT /v2/{project_id}/alarm-rules	aom:alarmRule:update	-
DELETE /v2/{project_id}/alarm-rules/{alarm_rule_id}	aom:alarmRule:delete	-
GET /v2/{project_id}/alarm-rules/{alarm_rule_id}	aom:alarmRule:get	-
POST /v2/{project_id}/alarm-rules/delete	aom:alarmRule:delete	-
POST /v2/{project_id}/events	aom:alarm:list	-
POST /v2/{project_id}/events/statistic	aom:alarm:list	-
PUT /v2/{project_id}/push/events	aom:alarm:put	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/uniagent-console/mainview/batch-import	aom:uniagentAgent:install	-
POST /v1/{project_id}/uniagent-console/upgrade/batch-upgrade	aom:uniagentAgent:upgrade	-
POST /v1/uniagent-console/agent-list/all	aom:uniagentAgent:list	-
GET /v2/{project_id}/alarm-notified-histories	aom:alarm:list	-
GET /v2/{project_id}/event2alarm-rule	aom:event2AlarmRule:list	-
POST /v2/{project_id}/event2alarm-rule	aom:event2AlarmRule:create	-
PUT /v2/{project_id}/event2alarm-rule	aom:event2AlarmRule:update	-
DELETE /v2/{project_id}/event2alarm-rule	aom:event2AlarmRule:delete	-
POST /v2/{project_id}/alert/action-rules	aom:actionRule:create	-
GET /v2/{project_id}/alert/action-rules	aom:actionRule:list	-
PUT /v2/{project_id}/alert/action-rules	aom:actionRule:update	-
DELETE /v2/{project_id}/alert/action-rules	aom:actionRule:delete	-
GET /v2/{project_id}/alert/action-rules/{rule_name}	aom:actionRule:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/alert/mute-rules	aom:muteRule:create	-
DELETE /v2/{project_id}/alert/mute-rules	aom:muteRule:delete	-
PUT /v2/{project_id}/alert/mute-rules	aom:muteRule:update	-
GET /v2/{project_id}/alert/mute-rules	aom:muteRule:list	-
POST /v4/{project_id}/alarm-rules	aom:alarmRule:create	-
GET /v4/{project_id}/alarm-rules	aom:alarmRule:list	-
DELETE /v4/{project_id}/alarm-rules	aom:alarmRule:delete 说明 该授权项的资源类型“alarmRule ”仅对 DELETE /v4/{project_id}/alarm-rules 接口适用。	-
POST /v2/{project_id}/events/notification/templates	aom:notificationTemplate:create	-
DELETE /v2/{project_id}/events/notification/templates	aom:notificationTemplate:delete	-
PUT /v2/{project_id}/events/notification/templates	aom:notificationTemplate:update	-
GET /v2/{project_id}/events/notification/templates	aom:notificationTemplate:list	-
GET /v2/{project_id}/events/notification/template/	aom:notificationTemplate:get	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
{name}		
POST /v4/{project_id}/alarm-rules-template	aom:alarmRuleTemplate:create	-
DELETE /v4/{project_id}/alarm-rules-template	aom:alarmRuleTemplate:delete	-
PUT /v4/{project_id}/alarm-rules-template	aom:alarmRuleTemplate:set	-
GET /v4/{project_id}/alarm-rules-template	aom:alarmRuleTemplate:list	-
PUT /v4/{project_id}/alarm-rules/batch-update	aom:alarmRule:create	-
POST /v2/{project_id}/alert/inhibit-rules	aom:inhibitRule:create	-
DELETE /v2/{project_id}/alert/inhibit-rules	aom:inhibitRule:delete	-
PUT /v2/{project_id}/alert/inhibit-rules	aom:inhibitRule:update	-
GET /v2/{project_id}/alert/inhibit-rules	aom:inhibitRule:list	-
POST /v2/{project_id}/alert/group-rules	aom:routeGroupRule:create	-
DELETE /v2/{project_id}/alert/group-rules	aom:routeGroupRule:delete	-
PUT /v2/{project_id}/alert/group-rules	aom:routeGroupRule:update	-
GET /v2/{project_id}/alert/group-rules	aom:routeGroupRule:list	-

 版权所有 © 华为云计算技术有限公司

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3-285 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource 默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

AOM 定义了以下可以在自定义身份策略的 Resource 元素中使用的资源类型。

表3-281 AOM 支持的资源类型

资源类型	URN
alarmRule	aom:<region>:<account-id>:alarmRule:<alarm_rule_id>

条件（Condition）

AOM 服务不支持在身份策略中的条件键中配置服务级的条件键。AOM 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.13.18 优化顾问 OA

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的操作项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。

 版权所有 © 华为云计算技术有限公司

- 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
- 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
- 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

关于优化顾问定义的资源类型的详细信息请参见资源类型（Resource）。

- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于优化顾问定义的条件键的详细信息请参见条件（Condition）。

您可以在身份策略语句的 Action 元素中指定以下优化顾问的相关操作。

表3-282 优化顾问支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
oa::listAuthorizations	授予获取用户授权列表。	read	-	-
oa::updateAuthorizations	授予修改用户授权。	write	-	-
oa::deleteAuthorizations	授予删除用户授权。	write	-	-
oa:monthReports:list	授予获取月度报告列表。	read	-	-
oa:monthReports:get	授予获取月度报告详情。	read	-	-
oa:monthReports:download	授予下载月度报告。	read	-	-
oa:checkItemRules:update	授予修改检查项规则。	write	-	-
oa:checkItemRules:list	授予获取检查项规则列表。	read	-	-
oa:autoCheckRule:update	授予修改自动检查规则。	write	-	-
oa:autoCheckRule:get	授予获取自动检查规则。	read	-	-
oa:riskItemsCheck:createTask	授予创建风险项检查任务。	write	-	-
oa:riskItemsCheck:getTaskProgress	授予获取风险项检查任务进度。	read	-	-
oa:riskItemsCheck:getTaskResult	授予获取风险项检查结果。	read	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
oa:riskItemsCheck:getTaskResultDimension	授予获取风险项检查结果维度。	read	-	-
oa:riskItemsCheck:listReportSubscriptions	授予获取风险项报告的订阅列表。	read	-	-
oa:riskItemsCheck:getReportSubscriptionRule	授予获取风险项报告的订阅规则。	read	-	-
oa:riskItemsCheck:updateReportSubscriptionRule	授予修改风险项报告的订阅规则。	write	-	-
oa:riskItemsCheck:getRiskItemNum	授予获取风险项个数。	read	-	-
oa:riskItemsCheck:exportCheckItemResult	授予导出风险检查报告。	read	-	-
oa:riskItemsCheck:getExportProgress	授予获取风险检查报告导出进度。	read	-	-
oa:riskItemsCheck:downloadCheckItemResult	授予下载风险检查报告。	read	-	-
oa:riskItemCheck:createTask	授予创建单个风险项检查任务。	write	-	-
oa:riskItemCheck:getTaskProgress	授予获取单个风险项检查任务进度。	read	-	-
oa:riskItemCheck:getTaskResult	授予获取单个风险项检查结果。	read	-	-
oa:riskItemCheck:listTaskResultRegions	授予获取单个风险项检查结果所属局点列表。	read	-	-
oa:riskItemsCheck:listCheckItems	授予获取检查项列表。	read	-	-
oa::saveWellArchitectedRecord	授予保存良好架构问卷。	write	-	-
oa::deleteWellArchitectedRecord	授予删除良好架构问卷。	write	-	-
oa::listWellArchitectedRecord	授予查看良好架构问卷列表。	read	-	-
oa::getWellArchitectedRecordDetail	授予获取良好架构问卷详情。	read	-	-
oa::generateWellArchit	授予生成良好架构报告。	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
ectedReport				
oa::getWellArchitectedReportDetail	授予查看良好架构报告详情。	read	-	-
oa::listOrgAccounts	授予获取组织成员账号列表。	read	-	-
oa:capacityAnalysis:getConfig	授予获取容量优化分析配置。	read	-	-
oa:capacityAnalysis:updateConfig	授予修改容量优化分析配置。	write	-	-
oa:capacityAnalysis:listResourceTypes	授予获取容量优化分析配置支持的资源类型列表。	read	-	-
oa:capacityAnalysis:listResources	授予获取容量优化分析配置关联的资源列表。	read	-	-
oa:capacityAnalysis:listResourceGroups	授予获取容量优化分析配置关联的资源分组列表。	read	-	-
oa:capacityAnalysis:createJob	授予创建容量优化分析任务。	write	-	-
oa:capacityAnalysis:getJobProgress	授予获取容量优化分析任务进度。	read	-	-
oa:capacityAnalysis:stopJob	授予停止容量优化分析任务。	write	-	-
oa:capacityAnalysis:getResultSummary	授予获取容量优化分析结果概要信息。	read	-	-
oa:capacityAnalysis:listResultDetails	授予获取容量优化分析结果详情列表。	read	-	-
oa:capacityAnalysis:deleteResultDetails	授予删除容量优化分析结果详情。	write	-	-
oa:capacityAnalysis:listReports	授予获取容量优化分析报告列表。	read	-	-
oa:capacityAnalysis:deleteReport	授予删除容量优化分析报告。	write	-	-
oa:capacityAnalysis:getReportExportProgress	授予获取容量优化分析报告导出进度。	read	-	-
oa:capacityAnalysis:downloadReport	授予下载容量优化分析报告。	read	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
oa:capacityAnalysis:exportReport	授予导出容量优化分析报告。	read	-	-
oa:capacityAnalysis:exportExpertReport	授予导出容量优化专家分析报告。	read	-	-
oa:applications:list	授予获取架构图列表。	read	-	-
oa:applications:get	授予获取架构图详情。	read	-	-
oa:applications:update	授予修改架构图基本信息。	write	-	-
oa:applications:delete	授予删除架构图。	write	-	-
oa:applications:updateView	授予修改架构图图元配置。	write	-	-
oa:applications:listServiceConfigs	授予获取架构图服务配置列表。	read	-	-
oa:applications:getResourceConfig	授予获取架构图资源解析配置。	read	-	-
oa:applications:updateRiskSwitchStatus	授予修改架构图风险数统计开关状态。	write	-	-
oa:applications:listRisks	授予获取架构图风险数。	read	-	-
oa:applications:listHistorys	授予获取架构图编辑历史列表。	read	-	-
oa:applications:getHistory	授予获取架构图编辑历史详情。	read	-	-
oa:applications:restoreHistory	授予恢复历史架构图。	write	-	-
oa:applications:deleteHistory	授予删除架构图编辑历史记录。	write	-	-
oa:applications:listRecycleApplications	授予获取回收站架构图列表。	read	-	-
oa::listSystemCesMetrics	授予获取 CES 指标列表。	read	-	-
oa::listSystemCesMetricData	授予获取 CES 指标数据。	read	-	-
oa::getSystemConfigItem	授予获取配置中心配置	read	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
	项。			
oa:capacityAnalysis:listHistoryReports	授予获取容量优化历史分析记录列表。	read	-	-
oa:capacityAnalysis:listMetrics	授予获取容量优化风险资源的监控指标列表。	read	-	-
oa:capacityAnalysis:listMonitor	授予获取容量优化风险资源的监控数据列表。	read	-	-
oa::getAutoloadData	授予获取自助接入结果数据。	read	-	-
oa:capacityAnalysis:listResultMonitorData	授予获取重保风险分析结果列表风险数据的监控数据。	read	-	-
oa:applications:getSummary	授予获取架构图概要信息。	read	-	-
oa:applications:listCapacityAnalysisSupportedServices	授予获取容量优化大屏支持服务列表。	read	-	-
oa:applications:listCapacityAnalysisResults	授予获取容量优化大屏分析结果列表。	read	-	-
oa:applications:startAutomaticDrawAnalysis	授予创建自动画图分析任务。	write	-	-
oa:applications:getAutomaticDrawAnalysisProgress	授予获取自动画图分析任务进度。	read	-	-
oa:applications:getAutomaticDrawAnalysisResult	授予获取自动画图分析任务结果。	read	-	-
oa:applications:getVpcFlowLogsDockingStatus	授予获取 VPC 流日志对接状态。	read	-	-
oa::listResourceGroups	授予获取资源分组列表。	read	-	-
oa::getResourceGroups	授予获取资源分组详情。	read	-	-
oa::updateResourceGroups	授予修改资源分组。	write	-	-
oa::deleteResourceGroups	授予删除资源分组。	write	-	-
oa::listResourceGroups	授予获取资源分组局点列	read	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
Regions	表。			
oa::listResourceGroupsResources	授予获取资源分组资源列表。	read	-	-
oa::listEnterpriseProjectResources	授予获取企业项目下的资源列表。	read	-	-
oa::listServiceMetrics	授予获取云服务指标项列表。	read	-	-
oa::listAlarmMetrics	授予获取告警指标项列表。	read	-	-
oa:applications:listServiceResources	授予获取架构设计云服务资源列表。	read	-	-
oa:applications:saveResourceGroup	授予保存架构设计资源分组。	write	-	-
oa::listResourceTypes	授予获取资源类型列表。	read	-	-
oa::listAllResourceGroups	授予获取所有资源分组。	read	-	-
oa:applications:downloadResourceTemplate	授予架构设计下载资源导入模板。	read	-	-
oa:applications:importResources	授予架构设计导入资源。	read	-	-
oa:applications:getResourcesImportResult	授予获取架构设计资源导入结果。	read	-	-
oa:applications:saveResourceGroupsBatch	授予架构设计批量保存资源分组。	write	-	-
oa:applications:getBatchSaveResourceGroupsResult	授予获取架构设计批量保存资源分组结果。	read	-	-
oa::downloadResourceTemplate	授予资源分组下载资源导入模板。	read	-	-
oa::importResourceGroups	授予资源分组导入资源。	read	-	-
oa::getResourcesGroupsImportResult	授予获取资源分组资源导入结果。	read	-	-
oa:applications:startServiceRecommendAnalysis	授予开始服务推荐分析。	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
oa:applications:getServiceRecommendAnalysisResult	授予获取服务推荐分析结果。	read	-	-
oa:applications:listAttachedResources	授予展示架构图关联资源列表。	read	-	-
oa:applications:listNodeAttachedResources	授予展示图元对应的资源列表。	read	-	-
oa:applications:downloadAttachedResources	授予架构图资源导出。	write	-	-
oa::getAutoloadConfigs	授予获取翻译项。	read	-	-
oa::listRiskItemsCheckReportsV4	授予获取风险项报告列表。	read	-	-
oa::getResources	授予获取自主接入资源数据。	read	-	-
oa:capacityAnalysis:getListMetrics	授予获取容量优化风险资源的监控指标列表。	read	-	-
oa:capacityAnalysis:getListMonitor	授予获取容量优化风险资源的监控数据列表。	read	-	-

资源类型（Resource）

优化顾问不支持在身份策略中的资源中指定资源进行权限控制。如需允许访问优化顾问，请在身份策略的 Resource 元素中使用通配符号*，表示身份策略将应用到所有资源。

条件（Condition）

优化顾问不支持在身份策略中的条件键中配置服务级的条件键。优化顾问可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.14 迁移

3.14.1 对象存储迁移服务 OMS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

 版权所有 © 华为云计算技术有限公司

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 OMS 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 OMS 定义的条件键的详细信息请参见条件（Condition）。
- **“别名”**列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 OMS 的相关操作。

表3-283 OMS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
oms:task:list	授予查询任务列表权限	list	task	-	-
oms:task:cre	授予创建任务权	write	task	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
ate	限				
oms:task:get	授予查询指定任务权限	read	task	-	-
oms:task:delete	授予删除任务权限	write	task	-	-
oms:task:update	授予更新指定任务权限	write	task	-	-
oms:synctask:list	授予查询同步任务列表权限	list	synctask	-	-
oms:synctask:create	授予创建同步任务权限	write	synctask	-	-
oms:synctask:get	授予查询指定同步任务权限	read	synctask	-	-
oms:synctask:delete	授予删除指定同步任务权限	write	synctask	-	-
oms:synctask:statistics	授予查询指定同步任务统计信息权限	read	synctask	-	-
oms:synctask:update	授予更新指定同步任务权限	write	synctask	-	-
oms:synctask:createEvent	授予创建指定同步任务事件权限	write	synctask	-	-
oms:taskgroup:create	授予创建任务组权限	write	taskgroup	-	-
oms:taskgroup:list	授予查询任务组列表权限	list	taskgroup	-	-
oms:taskgroup:get	授予查询指定任务组信息权限	read	taskgroup	-	-
oms:taskgroup:delete	授予删除指定任务组权限	write	taskgroup	-	-
oms:taskgroup:update	授予更新指定任务组权限	write	taskgroup	-	-
oms::listObjects	授予查询桶的对象列表权限	list	-	-	-
oms::checkC	授予检查桶的	read	-	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
dnInfo	CDN 连通性权限				
oms::listBuckets	授予查询桶列表权限	list	-	-	-
oms::listBucketRegions	授予查询桶区域列表的权限	list	-	-	-
oms::checkBucketPrefix	授予检查桶对象前缀的权限	read	-	-	-
oms::listCloudRegions	授权查询源端厂商支持区域列表的权限	list	-	-	-
oms::listCloudTypes	授予查询支持云厂商列表的权限	list	-	-	-

OMS 的 API 通常对应着一个或多个授权项。表 3-288 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-284 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/tasks/batch-update	oms:task:update	-
GET /v2/{project_id}/tasks	oms:task:list	-
POST /v2/{project_id}/tasks	oms:task:create	-
GET /v2/{project_id}/tasks/{task_id}	oms:task:get	-
DELETE /v2/{project_id}/tasks/{task_id}	oms:task:delete	-
POST /v2/{project_id}/tasks/{task_id}/stop	oms:task:update	-
POST /v2/{project_id}/tasks/{task_id}/start	oms:task:update	-
PUT /v2/{project_id}/tasks/{task_id}/bandwidth-policy	oms:task:update	-
PUT	oms:task:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v2/{project_id}/tasks/{task_id}/access-keys		
GET /v2/{project_id}/sync-tasks	oms:synctask:list	-
POST /v2/{project_id}/sync-tasks	oms:synctask:create	-
GET /v2/{project_id}/sync-tasks/{sync_task_id}	oms:synctask:get	-
DELETE /v2/{project_id}/sync-tasks/{sync_task_id}	oms:synctask:delete	-
GET /v2/{project_id}/sync-tasks/{sync_task_id}/statistics	oms:synctask:statistics	-
POST /v2/{project_id}/sync-tasks/{sync_task_id}/stop	oms:synctask:update	-
POST /v2/{project_id}/sync-tasks/{sync_task_id}/start	oms:synctask:update	-
POST /v2/{project_id}/sync-tasks/{sync_task_id}/events	oms:synctask:createEvent	-
POST /v2/{project_id}/taskgroups	oms:taskgroup:create	-
GET /v2/{project_id}/taskgroups	oms:taskgroup:list	-
GET /v2/{project_id}/taskgroups/{group_id}	oms:taskgroup:get	-
DELETE /v2/{project_id}/taskgroups/{group_id}	oms:taskgroup:delete	-
PUT /v2/{project_id}/taskgroups/{group_id}/stop	oms:taskgroup:update	-
PUT /v2/{project_id}/taskgroups/{group_id}/start	oms:taskgroup:update	-
PUT /v2/{project_id}/taskgroups/{group_id}/retry	oms:taskgroup:update	-
PUT /v2/{project_id}/taskgroups/{group_id}/update	oms:taskgroup:update	-
POST	oms::listObjects	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
/v2/{project_id}/objectstorage/buckets/objects		
POST /v2/{project_id}/objectstorage/buckets/cdn-info	oms::checkCdnInfo	-
POST /v2/{project_id}/objectstorage/buckets	oms::listBuckets	-
POST /v2/{project_id}/objectstorage/buckets/regions	oms::listBucketRegions	-
POST /v2/{project_id}/objectstorage/buckets/prefix	oms::checkBucketPrefix	-
GET /v2/{project_id}/objectstorage/data-center	oms::listCloudRegions	-
GET /v2/{project_id}/objectstorage/cloud-type	oms::listCloudTypes	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的策略语句中指定该资源的 URN，策略仅作用于此资源；如未指定，Resource 默认为“*”，则策略将应用到所有资源。您也可以在策略中设置条件，从而指定资源类型。

OMS 定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-285 OMS 支持的资源类型

资源类型	URN
Task	oms:<region>:<account-id>:task:*
	oms:<region>:<account-id>:task:<task-id>
SyncTask	oms:<region>:<account-id>:synctask:*
	oms:<region>:<account-id>:synctask:<synctask-id>
TaskGroup	oms:<region>:<account-id>:taskgroup:*
	oms:<region>:<account-id>:taskgroup:*

 版权所有 © 华为云计算技术有限公司

须知

同步任务 API 当前仅支持华南-广州-友好、华北-北京四、华东-上海一区域。

条件（Condition）

OMS 服务不支持在身份策略中的条件键中配置服务级的条件键。

OMS 可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.14.2 主机迁移服务 SMS

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 SMS 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。

 版权所有 © 华为云计算技术有限公司

- 如果此列条件键没有值（-），表示此操作不支持指定条件键。

关于 SMS 定义的条件键的详细信息请参见条件（Condition）。

- “**别名**”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 SMS 的相关操作。

表3-286 SMS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
sms:template:list	授予查询模板列表权限	list	template	-	-
sms:template:create	授予新增模板信息权限	write	template	-	-
sms:template:batchDelete	授予批量删除指定 ID 的模板权限	write	template	-	-
sms:template:get	授予查询指定 ID 模板信息权限	read	template	-	-
sms:template:update	授予修改模板信息权限	write	template	-	-
sms:template:getTargetPassword	授予查询指定 ID 的模板中的目的端服务器的密码权限	read	template	-	-
sms:template:delete	授予删除指定 ID 的模板权限	write	template	-	-
sms:server:listErrors	授予查询待迁移源端的所有错误权限	list	server	-	-
sms:server:list	授予查询源端服务器列表权限	list	server	g:EnterpriseProjectId	-
sms:server:register	授予上报源端服务器基本信息权限	write	server	g:EnterpriseProjectId	-
sms:server:batchDelete	授予批量删除源端服务器信息权限	write	server	g:EnterpriseProjectId	-
sms:server:get	授予查询指定 ID 的源端服务器权限	read	server	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
sms:server:update	授予修改指定 ID 的源端服务器名称权限	write	server	g:EnterpriseProjectId	-
sms:server:delete	授予删除指定 ID 的源端服务器信息权限	write	server	g:EnterpriseProjectId	-
sms:server:updateDiskInfo	授予更新磁盘信息权限	write	server	g:EnterpriseProjectId	-
sms:server:overview	获取服务器总览权限	read	server	-	-
sms:server:updateState	授予更新任务对应源端复制状态权限	write	server	g:EnterpriseProjectId	-
sms:server:listTask	授予查询迁移任务列表权限	list	server	g:EnterpriseProjectId	-
sms:server:createTask	授予创建迁移任务权限	write	server	g:EnterpriseProjectId	-
sms:server:batchDeleteTask	授予批量删除迁移任务权限	write	server	g:EnterpriseProjectId	-
sms:server:getTask	授予查询指定 ID 的迁移任务权限	read	server	g:EnterpriseProjectId	-
sms:server:updateTask	授予更新指定 ID 的迁移任务权限	write	server	g:EnterpriseProjectId	-
sms:server:deleteTask	授予删除指定 ID 的迁移任务权限	write	server	g:EnterpriseProjectId	-
sms:server:manageTask	授予管理迁移任务权限	write	server	g:EnterpriseProjectId	-
sms:server:updateTaskProgress	授予上报数据迁移进度和速率权限	write	server	g:EnterpriseProjectId	-
sms:server:unlock	授予解锁指定任务的目的端服务器权限	write	server	g:EnterpriseProjectId	-
sms:server:collectLog	授予上传迁移任务的日志权限	write	server	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
sms:server:getTaskPassphrase	授予查询指定任务 ID 的安全传输通道的证书 passphrase 权限	read	server	g:EnterpriseProjectId	-
sms:server:checkNetwork	授予检查网卡安全组端口是否符合要求权限	read	server	-	-
sms:server:getTaskSpeedLimit	授予查询任务限速规则权限	read	server	g:EnterpriseProjectId	-
sms:server:updateTaskSpeedLimit	授予设置迁移限速规则权限	write	server	g:EnterpriseProjectId	-
sms:server:getCommand	授予获取服务端命令权限	read	server	g:EnterpriseProjectId	-
sms:server:updateCommandResult	授予上报服务端命令执行结果权限	write	server	g:EnterpriseProjectId	-
sms:server:getCert	授予获取 SSL 证书和私钥权限	read	server	g:EnterpriseProjectId	-
sms:migproject:list	授予获取项目列表权限	list	migproject	-	-
sms:migproject:create	授予新建迁移项目权限	write	migproject	-	-
sms:migproject:get	授予查询指定 ID 迁移项目详情权限	read	migproject	-	-
sms:migproject:update	授予更新迁移项目信息权限	write	migproject	-	-
sms:migproject:delete	授予删除迁移项目权限	write	migproject	-	-
sms:migproject:update	授予更新默认迁移项目权限	write	migproject	-	-
sms::getConfig	授予获取 Agent 配置信息权限	read	-	-	-
sms:server:updateNetworkCheckInfo	授予更新网络检测相关的信息权	write	task	g:EnterpriseProjectId	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
	限				
sms:server:getTaskConfig	授予查询任务配置权限	read	task	g:EnterpriseProjectId	-
sms:server:updateTaskConfig	授予更新任务配置权限	write	task	g:EnterpriseProjectId	-

SMS 的 API 通常对应着一个或多个授权项。表 3-291 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表3-287 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3/vm/templates	sms:template:list	-
POST /v3/vm/templates	sms:template:create	-
POST /v3/vm/templates/delete	sms:template:batchDelete	-
GET /v3/vm/templates/{id}	sms:template:get	-
PUT /v3/vm/templates/{id}	sms:template:update	-
GET /v3/vm/templates/{id}/target-password	sms:template:getTargetPassword	-
DELETE /v3/vm/templates/{id}	sms:template:delete	-
GET /v3/errors	sms:server:listErrors	-
GET /v3/sources	sms:server:list	-
POST /v3/sources	sms:server:register	-
POST /v3/sources/delete	sms:server:batchDelete	• ecs:cloudServers:showServer • ecs:cloudServers:attach • evs:volumes:use • ecs:cloudServers:stop • ecs:cloudServers:start • ecs:cloudServers:detachVolume • evs:volumes:delete • evs:snapshots:delete • evs:volumes:get

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v3/sources/{source_id}	sms:server:get	-
PUT /v3/sources/{source_id}	sms:server:update	-
DELETE /v3/sources/{source_id}	sms:server:delete	• ecs:cloudServers:showServer • ecs:cloudServers:attach • evs:volumes:use • ecs:cloudServers:stop • ecs:cloudServers:start • ecs:cloudServers:detachVolume • evs:volumes:delete • evs:snapshots:delete • evs:volumes:get
PUT /v3/sources/{source_id}/diskinfo	sms:server:updateDiskInfo	-
GET /v3/sources/overview	sms:server:overview	-
PUT /v3/sources/{source_id}/changestate	sms:server:updateState	-
GET /v3/tasks	sms:server:listTask	-
POST /v3/tasks	sms:server:createTask	-
POST /v3/tasks/delete	sms:server:batchDeleteTask	• ecs:cloudServers:showServer • ecs:cloudServers:attach • evs:volumes:use • ecs:cloudServers:stop • ecs:cloudServers:start • ecs:cloudServers:detachVolume • evs:volumes:delete • evs:snapshots:delete • evs:volumes:get
GET /v3/tasks/{task_id}	sms:server:getTask	-
PUT /v3/tasks/{task_id}	sms:server:updateTask	-
DELETE /v3/tasks/{task_id}	sms:server:deleteTask	• ecs:cloudServers:showServer • ecs:cloudServers:attach • evs:volumes:use

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
		• ecs:cloudServers:stop • ecs:cloudServers:start • ecs:cloudServers:detachVolume • evs:volumes:delete • evs:snapshots:delete • evs:volumes:get
POST /v3/tasks/{task_id}/action	sms:server:manageTask	-
PUT /v3/tasks/{task_id}/progress	sms:server:updateTaskProgress	-
POST /v3/tasks/{task_id}/unlock	sms:server:unlock	-
POST /v3/tasks/{task_id}/log	sms:server:collectLog	-
GET /v3/tasks/{task_id}/passphrase	sms:server:getTaskPassphrase	-
GET /v3/tasks/{t_project_id}/networkacl/{t_network_id}/check	sms:server:checkNetwork	-
GET /v3/tasks/{task_id}/speed-limit	sms:server:getTaskSpeedLimit	-
POST /v3/tasks/{task_id}/speed-limit	sms:server:updateTaskSpeedLimit	-
GET /v3/sources/{server_id}/command	sms:server:getCommand	-
POST /v3/sources/{server_id}/command_result	sms:server:updateCommandResult	-
GET /v3/tasks/{task_id}/certkey	sms:server:getCert	-
GET /v3/migprojects	sms:migproject:list	-
POST /v3/migprojects	sms:migproject:create	-
GET /v3/migprojects/{mig_project_id}	sms:migproject:get	-
PUT /v3/migprojects/{mig_project_id}	sms:migproject:update	-
DELETE /v3/migprojects/{mig_project_id}	sms:migproject:delete	-
PUT /v3/migprojects/{mig_project_id}/default	sms:migproject:update	-

 版权所有 © 华为云计算技术有限公司

API	对应的授权项	依赖的授权项
GET /v3/config	sms::getConfig	-
POST /v3/{task_id}/update-network-check-info	sms:server:updateNetworkCheckInfo	-
POST /v3/tasks/{task_id}/configuration-setting	sms:server:updateTaskConfig	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如表 3 中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的策略语句中指定该资源的 URN，策略仅作用于此资源；如未指定，Resource 默认为“*”，则策略将应用到所有资源。您也可以在策略中设置条件，从而指定资源类型。

SMS 定义了以下可以在身份策略的 Resource 元素中使用的资源类型。

表3-288 SMS 支持的资源类型

资源类型	URN
server	sms::<account-id>:server:*
	sms::<account-id>:server:<server-id>
Task	sms::<account-id>:task:*
	sms::<account-id>:task:<task-id>
template	sms::<account-id>:template:*
	sms::<account-id>:template:<template-id>
migproject	sms::<account-id>:migproject:*
	sms::<account-id>:migproject:<migproject-id>

条件（Condition）

SMS 服务不支持在身份策略中的条件键中配置服务级的条件键。

SMS 可以使用适用于所有服务的全局条件键，请参考全局条件键。

 版权所有 © 华为云计算技术有限公司

3.15 用户服务

3.15.1 费用中心

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的操作项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在身份策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

您可以在身份策略语句的 Action 元素中指定以下费用中心的相关操作。

 版权所有 © 华为云计算技术有限公司

表3-289 费用中心支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
billing:balance:update	提现，充值/还款，汇款认领，余额预警	write	-	-
billing:balance:view	查看收支明细，付款历史记录，消费配额，调账记录，欠费查询	list	-	g:EnterpriseProjectId
billing:balance:export	导出收支明细、付款记录	read	-	-
billing:bill:update	账单设置	write	-	-
billing:bill:view	查看账单、本月消费、近 7 天扣费资源，消费走势	list	-	g:EnterpriseProjectId
billing:bill:export	导出账单概览	read	-	g:EnterpriseProjectId
billing:billDetail:update	账单明细设置	write	-	g:EnterpriseProjectId
billing:billDetail:view	查看账单明细	read	-	g:EnterpriseProjectId
billing:billDetail:export	导出账单明细	read	-	g:EnterpriseProjectId
billing:resourcePackages:view	查看资源包，剩余量汇总，使用明细查询/导出	list	-	-
billing:resourcePackages:update	资源包剩余量预警设置	write	-	-
billing:contract:update	申请、修改、作废、查看线上合同，查看线下合同	write	-	-
billing:coupon:view	查看优惠券、储值卡，激活代金券	read	-	-
billing:coupon:update	购买储值卡	write	-	-
billing:contract:viewDiscount	查看商务折扣	read	-	-
billing:invoice:manage	发票管理：索取发票、管理发票抬头和管理收件地址	write	-	-
billing:invoice:view	查看开票记录，发票详情	read	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
billing:invoice:export	导出发票信息，下载发票	read	-	-
billing:order:pay	支付订单	write	-	g:EnterpriseProjectId
billing:order:view	查看订单信息、查看按需套餐包	list	-	g:EnterpriseProjectId
billing:subscription:renew	续费、设置自动续费、设置到期策略、按需转包年/包月	write	-	g:EnterpriseProjectId
billing:subscription:view	查看续费管理信息，查询可按需转包年/包月资源列表	list	-	g:EnterpriseProjectId
billing:subscription:unsubscribe	查看可退订资源，退订资源，取消发货，硬件退换货	write	-	g:EnterpriseProjectId
billing:consumption:view	查看企业项目消耗分析	read	-	-
billing::activeEPFinance	开通/关闭企业项目功能	write	-	-
billing::activeEPFundQuota	开通/关闭企业项目资金配额功能	write	-	-
billing::viewEPFundQuota	查询企业项目资金配额	read	-	-
billing::updateEPFundQuota	修改企业项目资金配额	write	-	-
billing::listEPFundQuotaHistory	查询企业项目资金配额调整记录	read	-	-
billing::updateEPGroup	修改企业项目群	write	-	-
billing::viewEPGroup	查看企业项目群	read	-	-

资源类型（Resource）

费用中心不支持在身份策略中的资源中指定资源进行权限控制。如需允许访问费用中心，请在身份策略的 Resource 元素中使用通配符号*，表示身份策略将应用到所有资源。

条件（Condition）

费用中心不支持在身份策略中的条件键中配置服务级的条件键。费用中心可以使用适用于所有服务的全局条件键，请参考全局条件键。

 版权所有 © 华为云计算技术有限公司

3.15.2 成本中心

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的操作项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于成本中心定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在身份策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于成本中心定义的条件键的详细信息请参见条件（Condition）。

您可以在身份策略语句的 Action 元素中指定以下成本中心的相关操作。

表3-290 成本中心支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
costCenter:accessAccount:view	授予查看接入账号的权限。	read	-	-
costCenter:costAnalysis:listCosts	授予查看成本分析的权限。	read	-	-
costCenter:costAnalysis:configReport	授予设置成本报告，新建、修改、删除自定义成本报告的权限。	write	-	-
costCenter:costAnalysis:listReports	授予查看成本报告列表的权限。	read	-	-
costCenter:costDetail:listCostDetails	授予查询成本明细的权限。	read	-	-
costCenter:budget:configBudget	授予设置预算，包括新建、修改、删除预算的权限。	write	-	-
costCenter:budget:viewBudget	授予查看预算信息，包括查看预算列表、查看预算详情的权限。	read	-	-
costCenter:budget:deleteBudgetReport	授予删除预算报告的权限。	write	-	-
costCenter:budget:configBudgetReport	授予新增、修改预算报告的权限。	write	-	-
costCenter:budget:viewBudgetReport	授予查看预算报告，包括预算报告列表和详情的权限。	read	-	-
costCenter:costAnomalyDetection:deleteMonitor	授予删除监视器的权限。	write	-	-
costCenter:costAnomalyDetection:configMonitor	授予新增、编辑监控器的权限。	write	-	-
costCenter:costAnomalyDetection:viewMonitor	授予查看监视器列表和异常成本记录的权限。	read	-	-
costCenter:costAnomalyDetection:configMonitorAlert	授予设置异常成本监控提醒的权限。	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
costCenter:costAnomalyDetection:viewMonitorAlert	授予查看异常成本监控提醒的权限。	read	-	-
costCenter:recommendation:viewRecommendationSummary	授予查看成本建议概览的权限。	read	-	-
costCenter:recommendation:viewRecommendationSubscription	授予查询成本建议订阅的权限。	read	-	-
costCenter:recommendation:configRecommendationSubscription	授予设置/删除成本建议订阅的权限。	write	-	-
costCenter:recommendation:viewYearlyMonthlyRecommendation	授予查看按需转包年包月成本优化评估的权限。	read	-	-
costCenter:recommendation:viewResourcePkgRecommendation	授予查看资源包购买建议的权限。	read	-	-
costCenter:recommendation:viewResourceOptimizeRecommendation	授予查看空闲资源优化建议的权限。	read	-	-
costCenter:recommendation:configPreference	授予设置空闲资源规则的权限。	write	-	-
costCenter:costTag:updateStatus	授予激活/取消激活成本标签的权限。	write	-	-
costCenter:costTag:listCostTags	授予查看成本标签的权限。	read	-	-
costCenter:costCategory:deleteCostCategory	授予删除成本分组的权限。	write	-	-
costCenter:costCategory:configCostCategory	授予设置成本分组，包括新建、编辑成本分组的权限。	write	-	-
costCenter:resour	授予查看多级成本目录的权	read	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
ceCategory:view	限。			
costCenter:costCategory:viewCostCategory	授予查看成本分组，包括成本分组列表和详情的权限。	read	-	-
costCenter:cloudIntelligenceDashboard:view	授予查看云智能看板的权限。	read	-	-
costCenter:uniCostAnalysis:listCosts	授予查看多云成本分析的权限。	read	-	-
costCenter:resourcePackage:viewResourcePkgAnalysis	授予查看资源包使用率/覆盖率分析的权限。	read	-	-
costCenter::updateCostConfig	授予开启成本特性的权限。	write	-	-
costCenter:preference:delete	授予关闭成本特性的权限。	write	-	-
costCenter:costdetailreport:viewReportTask	授予查看成本明细 OBS 导出任务列表的权限。	read	-	-
costCenter:costdetailreport:configReportTask	授予创建/修改/删除成本明细 OBS 导出任务的权限。	write	-	-
costCenter:resourcePackage:viewLowUsageAlert	授予查看低使用率资源包订阅的权限。	read	-	-
costCenter:helper:listCostAllocations	授予查看成本分配占比统计的权限。	list	-	-
costCenter:helper:viewCostRating	授予查看成熟度评分的权限。	read	-	-
costCenter:resourceCategory:config	授予设置多级成本目录的权限。	write	-	-
costCenter:accessAccount:config	授予设置接入账号的权限。	write	-	-
costCenter:resourcePackage:configLowUsageAlert	授予设置低使用率资源包订阅的权限。	write	-	-
costCenter:costA	授予提供异常成本评估的权	read	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
nomalyDetection:provideFeedback	限。			

资源类型（Resource）

成本中心不支持在身份策略中的资源中指定资源进行权限控制。如需允许访问成本中心，请在身份策略的 Resource 元素中使用通配符号*，表示身份策略将应用到所有资源。

条件（Condition）

成本中心不支持在身份策略中的条件键中配置服务级的条件键。成本中心可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.15.3 账号中心

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统策略无法满足授权要求，管理员可以根据账号中心支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务基于策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的操作项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。

 版权所有 © 华为云计算技术有限公司

  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。
- **“条件键”**列包括了可以在策略语句的 Condition 元素中支持指定的键值。
  - 如果该操作项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该操作项资源类型列没有值（-），则表示条件键对整个操作项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

您可以在策略语句的 Action 元素中指定以下账号中心的相关操作。

表3-291 账号中心支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
account:accountInfo:update	更新账号信息，包括基本信息、首选项等。	write	-	-
account:cps:view	云推官查看奖励推广计划推广数据。	read	-	-
account:cps:update	加入奖励推广计划。	write	-	-
account:privilege:view	查看我的特权、实物奖品。	read	-	-

资源类型（Resource）

账号中心不支持在身份策略中的资源中指定资源进行权限控制。如需允许访问账号中心，请在策略的 Resource 元素中使用通配符号*，表示策略将应用到所有资源。

条件（Condition）

账号中心不支持在身份策略中的条件键中配置服务级的条件键。账号中心可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.15.4 企业中心

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统策略无法满足授权要求，管理员可以根据企业中心支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM 身份策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

 版权所有 © 华为云计算技术有限公司

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别。

本章节介绍 IAM 服务身份策略授权场景中自定义身份策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略。
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为策略中支持的操作项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在身份策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。
- **“条件键”**列包括了可以在策略语句的 Condition 元素中支持指定的键值。
  - 如果该操作项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该操作项资源类型列没有值（-），则表示条件键对整个操作项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

您可以在策略语句的 Action 元素中指定以下企业中心的相关操作。

表3-292 企业中心支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
businessUnitCenter::active	开通与关闭企业中心功能	write	-	-
businessUnitCenter:bill:update	企业中心子账号账单操作	write	-	-
businessUnitCenter:bill:view	企业中心子账号账单查看	read	-	-
businessUnitCenter:billDetail:update	企业中心子账号账单明细操作	write	-	-
businessUnitCenter:billDetail:view	企业中心子账号账单明细查看	read	-	-
businessUnitCenter:businessU	修改企业组织财	write	-	-

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键
nitFinance:update	务信息			
businessUnitCenter:businessUnitFinance:view	查看企业组织财务信息	read	-	-
businessUnitCenter:businessUnit:update	修改企业组织与子账号	write	-	-
businessUnitCenter:businessUnit:view	查看企业组织与子账号	read	-	-
businessUnitCenter:businessUnitBudget:update	操作企业组织预算	write	-	-
businessUnitCenter:businessUnitBudget:view	查看企业组织预算	read	-	-
businessUnitCenter:businessUnitPolicy:update	修改企业组织控制策略	write	-	-

资源类型（Resource）

企业中心不支持在身份策略中的资源中指定资源进行权限控制。如需允许访问企业中心，请在策略的 Resource 元素中使用通配符号*，表示策略将应用到所有资源。

条件（Condition）

企业中心不支持在身份策略中的条件键中配置服务级的条件键。企业中心可以使用适用于所有服务的全局条件键，请参考全局条件键。

3.15.5 客户运营能力

云服务在 IAM 预置了常用授权项，称为系统身份策略。如果 IAM 系统身份策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建 IAM 自定义身份策略来进行精细的访问控制，IAM 自定义身份策略是对系统身份策略的扩展和补充。

除 IAM 服务外，Organizations 服务中的服务控制策略（Service Control Policies，以下简称 SCP）也可以使用这些授权项元素设置访问控制策略。

SCP 不直接进行授权，只划定权限边界。将 SCP 绑定到组织单元或者成员帐号时，并没有直接对组织单元或成员帐号授予操作权限，而是规定了成员帐号或组织单元包含的成员帐号的授权范围。IAM 策略授予权限的有效性受 SCP 限制，只有在 SCP 允许范围内的权限才能生效。

IAM 服务与 Organizations 服务在使用这些元素进行访问控制时，存在着一些区别，详情请参见：IAM 服务与 Organizations 服务权限访问控制的区别

 版权所有 © 华为云计算技术有限公司

本章节介绍 IAM 服务基于身份策略授权场景中自定义策略和组织服务中 SCP 使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑 IAM 自定义身份策略，请参考创建自定义身份策略
- 如何使用这些元素编辑 SCP 自定义策略，请参考创建 SCP。

操作（Action）

操作（Action）即为身份策略中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read 和 write 等）。此分类可帮助您了解在策略中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在策略语句的 Resource 元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的 URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于 **BSS** 定义的资源类型的详细信息请参见资源类型（Resource）。
- **“条件键”**列包括了可以在策略语句的 Condition 元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于 **BSS** 定义的条件键的详细信息请参见条件（Condition）。
- “**别名**”列包括了可以在身份策略中配置的策略授权项。通过这些授权项，可以控制支持策略授权的 API 访问。详细信息请参见身份策略兼容性说明。

您可以在身份策略语句的 Action 元素中指定以下 API 的相关操作。

说明

billing:contract:viewDiscount 授权项仅影响响应中的折扣信息返回。即使没有该权限，接口仍可正常调用，但响应中将不返回折扣信息。

表3-293 **BSS** 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
billing:contract:viewDiscount	授予查看商务折扣的权限	read	-	-	
billing:balance:view	授予查看收支明细，付款历史记录，消费配额，调账记录，欠费查询的权限	list	-	-	
billing:coupon:vie	授予查看优惠券、储值	read	-	-	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
w	卡、激活代金券的权限				
billing:order:view	授予查看订单信息、查看按需套餐包的权限	list	-	-	
billing:order:pay	授予支付订单的权限	write	-	-	
billing:subscription:renew	授予续费、设置自动续费、设置到期策略、按需转包年/包月的权限	write			
billing:subscription:unsubscribe	授予查看可退订资源，退订资源，取消发货，硬件退换货的权限	write	-	-	
billing:resourcePackages:view	授予查看资源包，剩余量汇总，使用明细查询/导出的权限	list	-	-	
billing:billDetail:view	授予查看账单明细的权限	read	-	-	
billing:bill:view	授予查看账单、本月消费、近 7 天扣费资源，消费走势的权限	list	-	-	
costCenter:costAnalysis:listCosts	授予查看成本分析的权限	read	-	-	
Billing::activeEPFinance	授予开通企业项目功能的权限	write	-	-	
businessUnitCenter:businessUnit:view	授予查看组织与账号的权限	read	-	-	
businessUnitCenter:businessUnitFinance:view	授予查看企业组织财务信息的权限	read	-	-	
businessUnitCenter:businessUnit:update	授予修改企业组织与子账号的权限	write	-	-	
businessUnitCenter:businessUnitFinance:update	授予修改企业组织财务信息的权限	write	-	-	
Billing::updateEPFundQuota	授予开通企业项目功能的权限	write	-	-	
Billing::viewEPFundQuota	授予查询企业项目资金配额的权限	read	-	-	

 版权所有 © 华为云计算技术有限公司

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
Billing::activeEPFundQuota	授予开通/关闭企业项目资金配额功能的权限	write	-	-	

BSS 的 API 通常对应着一个或多个授权项。表 3-297 展示了 API 与授权项的关系，以及该 API 需要依赖的授权项。

表 2 API 与授权项的关系

说明

细粒度鉴权失败情况下，响应字段 encoded_authorization_message 的值需要调安全令牌服务 STS 提供的接口解密后才能查看。解密接口的 APIE 地址：解密鉴权失败的原因。

注意：调用者需要有 sts::decodeAuthorizationMessage 的权限才在 APIE 调用解密接口，否则报错：STS5.1001。

场景	子场景	接口名称	接口 URL（API）	对应的授权项	授权项名称	依赖的授权项
管理产品	查询商品价格	查询按需产品价格	POST /v2/bills/ratings/on-demand-resources	billing:contract:viewDiscount	查看折扣、价格信息。	-
		查询包年/包月产品价格	POST /v2/bills/ratings/period-resources/subscribe-rate	billing:contract:viewDiscount	查看折扣、价格信息	
		查询待续订包年/包月资源的续订金额	POST /v2/bills/ratings/period-resources/renew-rate	billing:contract:viewDiscount	查看折扣、价格信息。	
管理账户	管理账户	查询账户余额	GET /v2/accounts/customer-accounts/balances	billing:balance:view	查看账户信息。	
		查询储值卡列表	GET /v2/promotions/benefits/stored-value-cards	billing:coupon:view	查看优惠券、现金券、代金券。	
		查询收支明细	GET /v2/accounts/customer-accounts/account-change-records	billing:balance:view	查看账户信息。	

 版权所有 © 华为云计算技术有限公司

场景	子场景	接口名称	接口 URL（API）	对应的授权项	授权项名称	依赖的授权项
管理交易	管理优惠券	查询优惠券列表	GET /v2/promotions/benefits/coupons	billing:coupon:view	查看优惠券、现金券、代金券。	
	管理包年/包月订单	查询订单列表	GET /v2/orders/customer-orders	billing:order:view	查看订单信息。	
		查询订单详情	GET /v2/orders/customer-orders/details/{order_id}	billing:order:view	查看订单信息。	
		支付包年/包月产品订单	POST /v2/orders/customer-orders/pay	billing:order:pay	订单支付。	
		查询订单可用优惠券	GET /v2/orders/customer-orders/order-coupons	billing:order:view	查看订单信息。	
		查询订单可用折扣	GET /v2/orders/customer-orders/order-discounts	billing:contract:viewDiscount	查看折扣、价格信息。	
		支付包年/包月产品订单	POST /v3/orders/customer-orders/pay	billing:order:pay	订单支付。	
		查询退款订单的金额详情	GET /v2/orders/customer-orders/refund-orders	billing:order:view	查看订单信息。	
	管理包年/包月资源	查询客户包年/包月资源列表	POST /v2/orders/suscriptions/resources/query	• billing:subscription:view • billing:order:view（待下线）	查看订单信息。	
		续订包年/包月资源	POST /v2/orders/subscriptions/resources/renew	billing:subscription:renew	下单、取消订单、修改收货地址。	

 版权所有 © 华为云计算技术有限公司

场景	子场景	接口名称	接口 URL（API）	对应的授权项	授权项名称	依赖的授权项
		退订包年/包月资源	POST /v2/orders/subscriptions/resources/unsubscribe	billing:subscription:unsubscribe	下单、取消订单、修改收货地址。 **云服务粒度退订鉴权常见问题.**	
		设置包年/包月资源自动续费	POST /v2/orders/subscriptions/resources/autorenew/**	billing:subscription:renew	下单、取消订单、修改收货地址。	
		取消包年/包月资源自动续费	DELETE /v2/orders/subscriptions/resources/autorenew/{resource_id}	billing:subscription:renew	下单、取消订单、修改收货地址。	
		设置或取消包年/包月资源到期转按需	POST /v2/orders/subscriptions/resources/to-on-demand	billing:subscription:renew	下单、取消订单、修改收货地址。	
		设置包年/包月资源自动续费扣款日和续费后资源统一到期日	POST /v2/orders/subscriptions/resources/renew/config	billing:subscription:renew	下单、取消订单、修改收货地址。	
	管理资源包	查询资源包列表	POST /v3/payments/free-resources/query	billing:resourcePackages:view	查看账单、月度成本、用量明细、成本管理、收支以及总览页面的费用走势。	
		查询资源包使用明细	GET /v2/bills/customer-bills/free-resources-usage-records	• billing:resourcePackages:view • billing:b	查看消费明细、资源消费、账单分析、付款历	

 版权所有 © 华为云计算技术有限公司

场景	子场景	接口名称	接口 URL（API）	对应的授权项	授权项名称	依赖的授权项
				illDetail:view（待下线）	史记录。	
		查询资源包使用量	POST /v2/payments/free-resources/usages/details/query	billing:resourcePackages:view	查看账单、月度成本、用量明细、成本管理、收支以及总览页面的费用走势。	
管理账单	管理账单	查询资源详单	POST /v2/bills/customer-bills/res-records/query	billing:billDetail:view	查看消费明细、资源消费、账单分析、付款历史记录。	
		查询汇总账单	GET /v2/bills/customer-bills/monthly-sum	billing:bill:view	查看账单、月度成本、用量明细、成本管理、收支以及总览页面的费用走势。	
		查询资源消费记录	GET /v2/bills/customer-bills/res-fee-records	• billing:billDetail:view • billing:bill:view（待下线）	查看账单、月度成本、用量明细、成本管理、收支以及总览页面的费用走势。	
		查询流水账单	GET /v2/bills/customer-bills/fee-records	• billing:billDetail:view • billing:bill:view（待下线）	查看账单、月度成本、用量明细、成本管理、收支以及总览页面的费用走势。	
	查询95计	查询 95 计费资源用量明细	GET /v2/bills/customer-bills/resources/usage/details	billing:billDetail:view	查看消费明细、资源消费、账单分析、付款历	

 版权所有 © 华为云计算技术有限公司

场景	子场景	接口名称	接口 URL（API）	对应的授权项	授权项名称	依赖的授权项
	费资源用量				史记录。	
		查询 95 计费资源用量汇总	GET /v2/bills/customer-bills/resources/usage/summary	billing:resourcePackages:view	查看账单、月度成本、用量明细、成本管理、收支以及总览页面的费用走势。	
管理成本	管理成本	查询月度成本	GET /v2/costs/cost-analysed-bills/monthly-breakdown	• costCenter:costDetail:listCostDetails • costCenter:costAnalysis:listCosts（待下线）	查看成本分析。	
		查询成本数据	POST /v4/costs/cost-analysed-bills/query	costCenter:costAnalysis:listCosts	查看成本分析。	
管理企业	管理企业项目	开通客户企业项目权限	POST /v2/enterprises/enterprise-projects/authority	Billing::activeEPFinance	开通企业项目功能。	
	管理企业多账号	查询企业子账号列表	GET /v2/enterprises/multi-accounts/sub-customers	businessUnitCenter:businessUnit:view	企业中心组织与账号查看权限。	
		查询企业组织结构	GET /v2/enterprises/multi-accounts/enterprise-organizations	businessUnitCenter:businessUnit:view	企业中心组织与账号查看权限。	
		查询企业主的可拨款余额	GET /v2/enterprises/multi-accounts/transfer-amount	businessUnitCenter:businessUnitFinance:view	查看企业组织财务信息。	
		查询企业子账	GET /v2/enterprises/multi-	businessUnitCenter:busi	查看企业组织财务信	

 版权所有 © 华为云计算技术有限公司

场景	子场景	接口名称	接口 URL（API）	对应的授权项	授权项名称	依赖的授权项
		号可回收余额	accounts/retrieve-amount	nessUnitFinance:view	息。	
		创建企业子账号	POST /v2/enterprises/multi-accounts/sub-customers	businessUnitCenter:businessUnit:view	修改企业组织与子账号	
		企业主账号向企业子账号拨款	POST /v2/enterprises/multi-accounts/transfer-amount	businessUnitCenter:businessUnitFinance:update	修改企业组织财务信息。	
		企业主账号从企业子账号回收余额	POST /v2/enterprises/multi-accounts/retrieve-amount	businessUnitCenter:businessUnitFinance:update	修改企业组织财务信息。	
		查询企业主账号可拨款优惠券列表	GET /v2/enterprises/multi-accounts/transfer-coupons	businessUnitCenter:businessUnitFinance:view	查看企业组织财务信息	
		查询企业子账号可回收优惠券列表	GET /v2/enterprises/multi-accounts/retrieve-coupons	businessUnitCenter:businessUnitFinance:view	查看企业组织财务信息	
		企业主账号向企业子账号拨款优惠券	POST v2/enterprises/multi-accounts/transfer-coupon	businessUnitCenter:businessUnitFinance:update	修改企业组织财务信息	
		企业主账号从企业子账号回收优惠券	POST /v2/enterprises/multi-accounts/retrieve-coupon	businessUnitCenter:businessUnitFinance:update	修改企业组织财务信息	

 版权所有 © 华为云计算技术有限公司

资源类型（Resource）

BSS 服务不支持在身份策略中的资源中指定资源进行权限控制。如需允许访问 **BSS** 服务，请在策略的 Resource 元素中使用通配符号*，表示策略将应用到所有资源。

条件（Condition）

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的 Condition 元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为 g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如 BSS:）仅适用于对应服务的操作，详情请参见表 3。
  - 单值/多值表示 API 调用时请求中与条件关联的值数。单值条件键在 API 调用时的请求中最多包含一个值，多值条件键在 API 调用时请求可以包含多个值。例如：g:SourceVpce 是单值条件键，表示仅允许通过某个 VPC 终端节点发起请求访问某资源，一个请求最多包含一个 VPC 终端节点 ID 值。g:TagKeys 是多值条件键，表示请求中携带的所有标签的 key 组成的列表，当用户在调用 API 请求时传入标签可以传入多个值。
- 运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，身份策略才能生效。支持的运算符请参见：运算符。

BSS 定义了以下可以在身份策略的 Condition 元素中使用的条件键，您可以使用这些条件键进一步细化身份策略语句应用的条件。

表3-294 BSS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
billing:cloudServiceType	string	多值	根据请求参数中云服务的类型，过滤访问。常见问题

条件键示例

- billing:cloudServiceType

  示例：表示仅支持退订 hws.service.type.ebs 云服务资源订单

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "billing:subscription:unsubscribe"
        ],
        "Condition": {
            "ForAnyValue:StringEquals": {
                "billing:cloudServiceType": [
```

 版权所有 © 华为云计算技术有限公司

```
                "hws.service.type.ebs"
            ]
        }
    }
}]
}
```

 版权所有 © 华为云计算技术有限公司