系统权限

文档版本 01

发布日期 2025-03-26

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 系统权限

默认情况下，管理员创建的IAM用户没有任何权限，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。

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：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。
- 区域级项目：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。
  - 所有项目：选择所有项目后，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）。
  - 项目：选择对应项目，授权将对指定项目生效。

权限类别：权限根据授权粒度分为角色和策略。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策略和角色，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。

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。

服务	作用范围	系统权限	权限类别	权限描述
	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，授权将对全局服务生效。 • 作用范围为所有项目，授权将对全局服务和所有项目（包括未来创建的项目）生效。 • 作用范围为项目，授权仅对指定项目生效。
	所有项目	Tenant Administrator		除统一身份认证服务外，其他所有服务的所有权限。 **说明** • 作用范围为全局服务，授权将对全局服务生效。 • 作用范围为所有项目，授权将对全局服务和所有项目（包括未来创建的项目）生效。 • 作用范围为项目，授权仅对指定项目生效。
	全局服务	Agent Operator		切换角色并访问委托方账号中的资源。

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） （项目级服务）	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。

服务	作用范围	系统权限	权限类别	权限描述
		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） （项目级服务）	区域级项目	IMS FullAccess	策略	镜像服务的所有执行权限。
		IMS ReadOnlyAccess		镜像服务的只读权限。
		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**

服务	作用范围	系统权限	权限类别	权限描述
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。

存储

服务	作用范围	系统权限	权限类别	权限描述
（全局级服务） 对象存储服务（OBS）	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。

服务	作用范围	系统权限	权限类别	权限描述
		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。
		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。**

服务	作用范围	系统权限	权限类别	权限描述
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。**

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。**

服务	作用范围	系统权限	权限类别	权限描述
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 ReadOnlyAccess		云专线服务只读权限。
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。

服务	作用范围	系统权限	权限类别	权限描述
		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）（项目级服务）	区域级项目	ER FullAccess	策略	企业路由器所有权限。
		ER ReadOnlyAccess		企业路由器只读权限。

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	云容器引擎服务的所有执行权限。
		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。

服务	作用范围	系统权限	权限类别	权限描述
		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 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。

服务	作用范围	系统权限	权限类别	权限描述
基因容器（GCS）（项目及服务）	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）（项目级服务）	区域级项目	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。
		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。
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。

服务	作用范围	系统权限	权限类别	权限描述
数据加密服务（DEW）（项目级服务）	区域级项目	KMS Administrator	角色	数据加密服务加密密钥的管理员权限。
		KMS CMKFullAccess	策略	数据加密服务加密密钥所有权限。
		DEW KeypairFullAccess		数据加密服务密钥对所有权限。
		DEW KeypairReadOnlyAccess		数据加密服务密钥对查看权限。
		CSMS FullAccess		凭据管理服务所有权限。
		CSMS ReadOnlyAccess		凭据管理服务凭据只读权限。
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。

服务	作用范围	系统权限	权限类别	权限描述
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）（项目级服务）	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。
		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）（全局级服务）	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。**

服务	作用范围	系统权限	权限类别	权限描述
	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。
	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。
应用运维管理服务（AOM） （项目级服务）	区域级项目	AOM FullAccess	策略	应用运维管理服务的所有执行权限。
		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。

服务	作用范围	系统权限	权限类别	权限描述
		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。

服务	作用范围	系统权限	权限类别	权限描述
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 ResourceShareParticipantAccess		资源访问管理服务资源共享邀请的处理权限。
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。

服务	作用范围	系统权限	权限类别	权限描述
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。**
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	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。

服务	作用范围	系统权限	权限类别	权限描述
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。

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。**

服务	作用范围	系统权限	权限类别	权限描述
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。

服务	作用范围	系统权限	权限类别	权限描述
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。

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。

服务	作用范围	系统权限	权限类别	权限描述
		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。**
数据仓库服务 GaussDB（DWS）	区域级项目	DWS FullAccess	策略	数据仓库服务的所有执行权限。
		DWS ReadOnlyAccess		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。**

服务	作用范围	系统权限	权限类别	权限描述
		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。
		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。**
推荐系统（RES）（项目级服务）	区域级项目	RES FullAccess	策略	推荐系统的所有执行权限。
		RES ReadOnlyAccess		推荐系统的只读权限。
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。

服务	作用范围	系统权限	权限类别	权限描述
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 CommonOperations		Huawei HiLens操作权限，拥有该权限的用户拥有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）（项目级服务）	区域级项目	Workspace FullAccess	策略	云桌面服务所有权限。
		Workspace DesktopsManager		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。

服务	作用范围	系统权限	权限类别	权限描述
ROMA资产中心（ROMA Exchange）（全局级服务、项目级服务）	所有项目	ROMAExchange FullAccess	策略	ROMA资产中心所有权限。

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。

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） （全局服务）	全局服务	RTC FullAccess	策略	实时音视频服务所有权限。
		RTC ReadOnlyAccess		实时音视频服务只读权限。

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。

工业软件

服务	作用范围	系统权限	权限类别	权限描述
工业数字模型驱动引擎（iDME）	区域级项目	DME AppOperationAccess	策略	数据模型驱动引擎服务应用管理权限，拥有创建和修改应用的权限。
		DME EnvOperationAccess		数据模型驱动引擎服务运行环境管理权限，拥有部署和卸载应用的权限。
		DME FullAccess		工业数字模型驱动引擎服务所有权限。
		DME ReadOnlyAccess		工业数字模型驱动引擎的只读策略，拥有应用列表、运行服务列表的只读权限。

服务	作用范围	系统权限	权限类别	权限描述
工业数据转换引擎服务（iDEE）	区域级项目	iDEE FullAccess	策略	工业数据转换引擎云服务所有权限。
		iDEE ReadOnlyAccess		工业数据转换引擎云服务只读权限。

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 （全局级服务、项目级服务）	所有项目	PSDMFullAccess	策略	专业服务交付管理平台的所有权限。
		PSDMReadOnly Access		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	MessageCenterFullAccess	策略	消息中心所有权限。
		MessageCenterReadOnlyAccess		消息中心只读权限。
		MessageCenterRecipientManagement		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。

