标签管理服务

产品介绍

文档版本 01

发布日期 2024-07-19

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 什么是标签管理服务

标签管理服务（Tag Management Service，简称TMS）是一种快速便捷将标签集中管理的可视化服务，提供跨区域、跨服务的集中标签管理和资源分类功能。

标签用于标识云资源，当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境等）对云资源进行分类。

图 1-1 标签示例

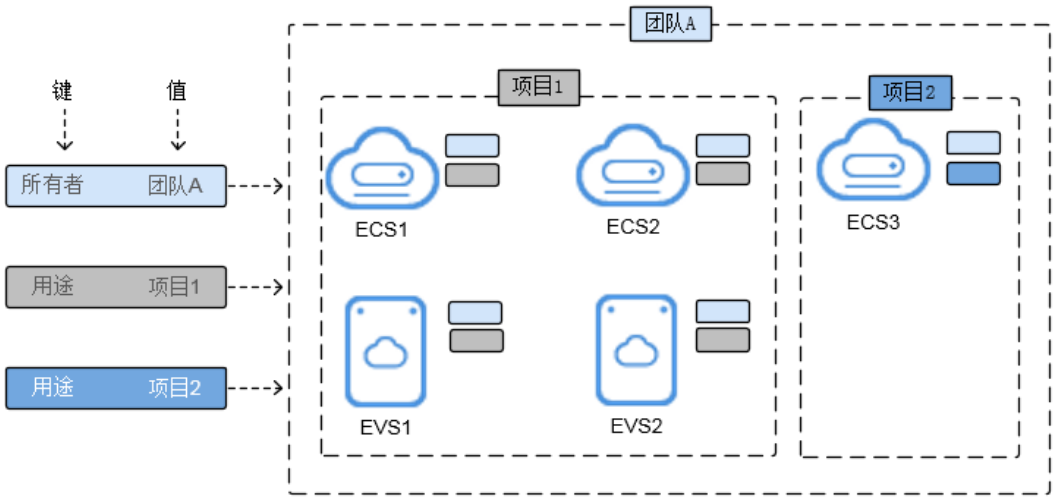


图1-1说明了标签的工作方式。在此示例中，您为每个云资源分配了两个标签，每个标签都包含您定义的一个“键”和一个“值”，一个标签使用键为“所有者”，另一个使用键为“用途”，每个标签都拥有相关的值。

您可以根据为云资源添加的标签快速搜索和筛选特定的云资源。例如，您可以为账号中的云资源定义一组标签，以跟踪每个云资源的所有者和用途，使资源管理变得更加轻松。

标签管理服务主要有以下功能：

- 资源标签管理：通过给账号下资源添加标签，可以对资源进行自定义标记，实现资源的分类。标签管理服务为用户提供可视化表格操作资源标签，并支持对标签进行批量编辑。
- 资源标签搜索：用户可以跨服务、跨区域对资源进行按标签搜索，还可以多标签组合搜索。

- 预定义标签管理：用户可以创建或导入/导出预定义标签。通过标签的预定义操作，用户可以从自身业务角度规划标签，实现标签的高效管理。

说明

标签管理服务为免费服务。

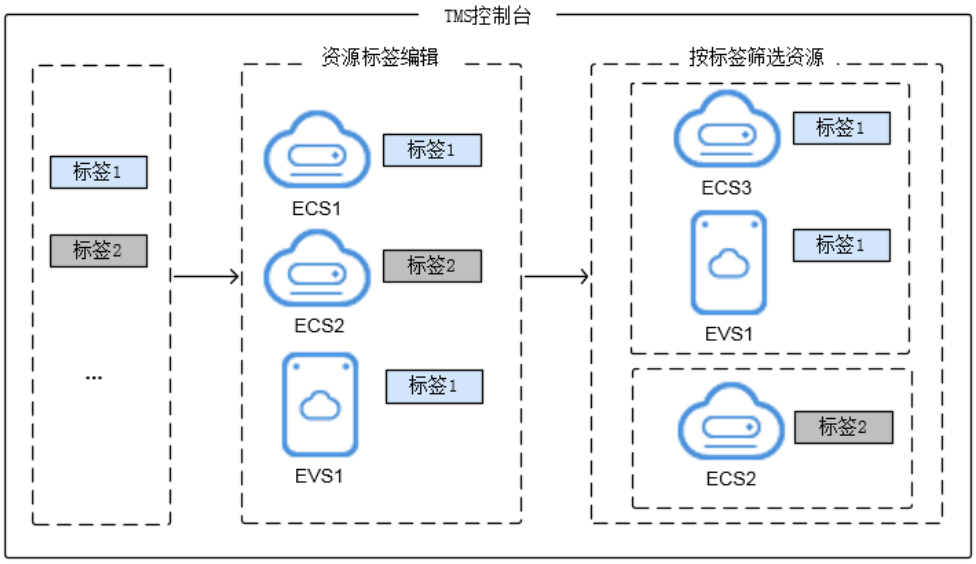
2 使用场景

标签管理服务支持以下两种典型应用场景：

资源集中处理

对于拥有大量云资源的用户，可以通过标签管理服务，快速查找标识有某标签的所有云资源，可对这些资源标签统一进行检视、修改、删除等操作。

图 2-1 资源集中处理

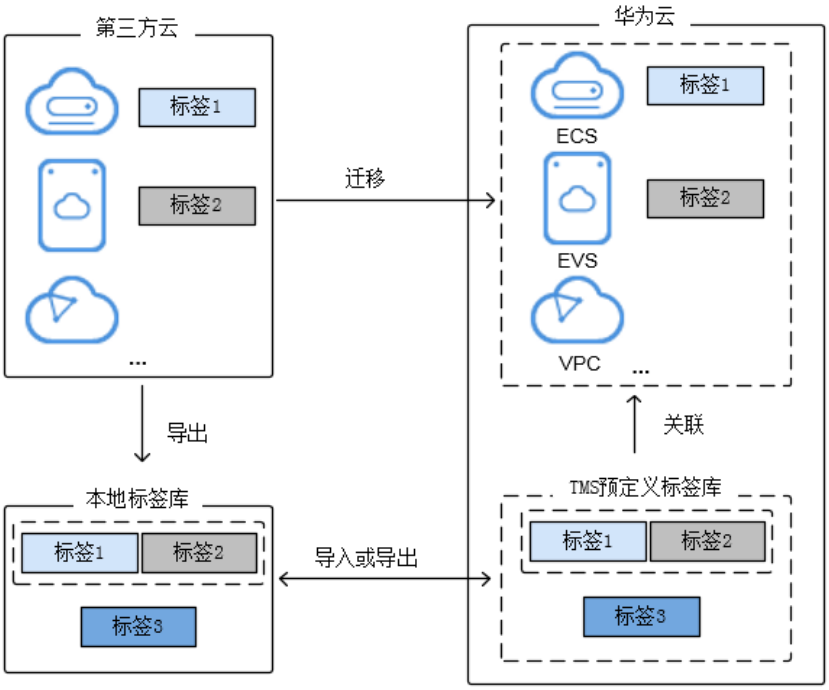


快速标识迁移资源

对于存在大量资源迁移需求的用户，可通过标签管理服务的预定义标签，以及标签的导入、导出功能，提高迁移的准确率和效率，降低了重复设置标签过程中的潜在风险。

- 创建预定义标签：用户可以在迁移资源之前在TMS中创建预定义标签，在资源迁入后直接进行关联。
- 导入、导出预定义标签：已有存量标签的用户可以将标签快速导入TMS预定义标签库，在资源迁入后进行关联，同时也可以导出预定义标签进行编辑操作。

图 2-2 快速标识迁移资源



3 安全

3.1 责任共担

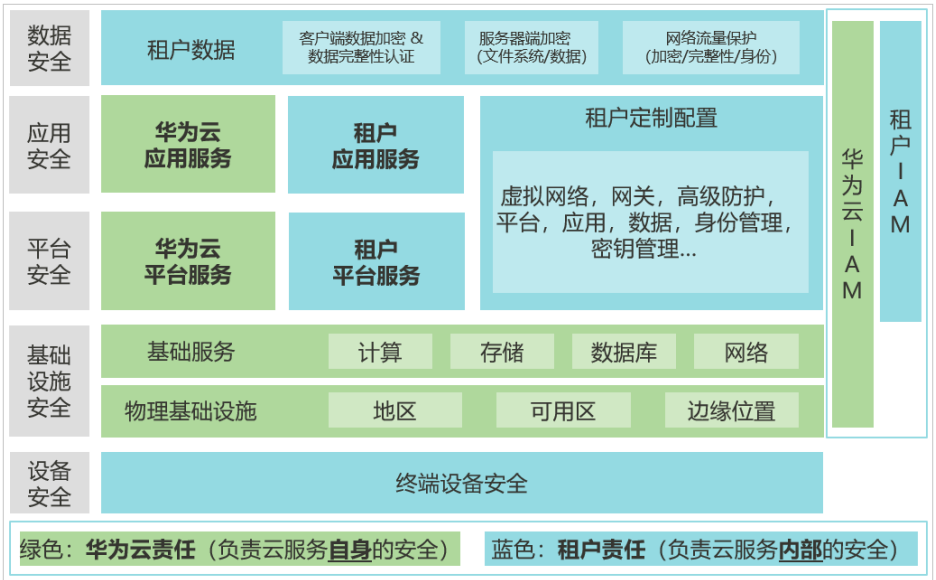
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图3-1所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 3-1 华为云安全责任共担模型



3.2 身份认证与访问控制

统一身份认证（Identity and Access Management，简称IAM）是华为云提供权限管理、访问控制和身份认证的基础服务，您可以使用IAM创建和管理用户、用户组，通过授权来允许或拒绝他们对云服务和资源的访问，通过设置安全策略提高账号和资源的安全性，同时IAM为您提供多种安全的访问凭证。

标签管理服务支持通过IAM权限策略进行访问控制。IAM权限是作用于云资源的，定义了允许和拒绝的访问操作，以此实现云资源权限的访问控制。管理员创建IAM用户后，需要将用户加入到一个用户组中，IAM可以对这个组授予所需的权限，用户组内的用户自动继承用户组的所有权限。

详情请参见**用户权限**和**权限管理**。

3.3 审计与日志

云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

开通云审计服务后，CTS可记录标签管理服务的操作事件用于审计。

- CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。
- 标签管理服务支持审计的操作事件请参见**支持审计的关键操作列表**。
- 如何查看审计日志请参见**查看审计日志**。

3.4 数据保护技术

3.4.1 静态数据保护

标签管理服务不提供更改、添加或删除华为云资源的方法。标签管理服务收集以下特定的信息：

- 预定义标签键
- 预定义标签值

3.4.2 传输中的数据保护

数据传输到标签管理服务内部数据库的过程中使用加密协议。此部分用户不可配置。

调用标签管理服务接口时，标签管理服务支持HTTP和HTTPS两种传输协议，为保证数据传输的安全性，推荐您使用更加安全的HTTPS协议。

3.4.3 数据销毁机制

客户删除数据后，为避免误删除，数据会在数据库历史表中保存。客户注销华为云账号后数据会保留7天，之后彻底删除。

4 与其他服务的关系

- **支持标签集中管理的服务**

  标签管理服务规划对云资源中的所有标签进行统一集中管理，当前支持的服务如表4-1所示。

  一个云服务可以包含多种资源类型，您可以在标签管理服务控制台根据需求选择对应的资源类型，对该类型资源的标签进行集中管理。

  表 4-1 标签管理当前支持的其他服务

服务	资源类型
终端节点服务 VPCEP	• Endpoint（终端节点） • Endpoint service（终端节点服务）
数据复制服务 DRS	• Data Synchronization Task（实时同步任务） • Data Subscription Task（数据订阅任务） • Disaster Recovery Task（实时灾备任务） • Backup Migration Task（备份迁移任务） • Online Migration Task（实时迁移任务）
裸金属服务器 BMS	BMS（裸金属服务器）
弹性云服务器 ECS	ECS（弹性云服务器）
对象存储服务 OBS	Bucket（桶）
虚拟私有云 VPC	• VPC（虚拟私有云） • Subnet（子网）
弹性公网IP EIP	EIP（弹性公网IP）
云硬盘 EVS	Disk（磁盘）
弹性伸缩 AS	AS group（弹性伸缩组）
镜像服务 IMS	Private image（私有镜像）

服务	资源类型
分布式缓存服务 DCS	DCS（缓存实例）
云桌面 Workspace	Desktop（桌面）
云解析服务 DNS	• Private zone（内网域名） • Public zone（公网域名） • PTR record（反向解析记录） • Private record set（内网解析记录集） • Public record set（公网解析记录集）
虚拟专用网络 VPN	• VPN Connection（VPN连接） • VPN Gateway（VPN网关） • Customer Gateway（对端网关）
弹性文件服务 SFS	SFS Turbo
弹性负载均衡 ELB	• Enhanced load balancer（弹性负载均衡器） • Enhanced load balancer listener（监听器）
消息通知服务 SMN	Topic（主题）
分布式消息服务 DMS	• Kafka（Kafka实例） • RabbitMQ（RabbitMQ实例） • RocketMQ（RocketMQ实例）
数据湖探索 DLI	• Queue（队列） • Package Resource（资源包） • Flink Template（Flink模板） • Flink Job（Flink作业） • Basic Datasource（经典型跨源连接） • Enhanced Datasource（增强型跨源连接） • Database（数据库） • Elastic Resource Pool（弹性资源池）
关系型数据库 RDS	DB instance（数据库实例）
MapReduce服务 MRS	Cluster（集群）
数据仓库服务 DWS	Cluster（数据仓库集群）
文档数据库服务 DDS	DB instance（数据库实例）
数据接入服务 DIS	Stream（通道）
Web应用防火墙 WAF	Instance（实例）
云搜索服务 CSS	Cluster（集群）

服务	资源类型
NAT网关 NAT Gateway	• Public NAT Gateway（公网NAT网关） • Private NAT Gateway（私网NAT网关） • Transit IP Address（中转IP）
云备份 CBR	Vault（存储库）
数据加密服务 DEW	KMS Key（密钥）
云容器引擎 CCE	• Cluster（集群） • Autopilot Cluster（Autopilot集群）
数据治理中心 DataArts Studio（原 智能数据湖运营平台 DAYU）	• Workspace（工作空间） • Instance（实例）
云数据库 GaussDB	GaussDB Instance（GaussDB实例）
数据库安全服务 DBSS	DBSS（实例）
内容分发网络 CDN	CDN（域名）
云专线 DC	• Direct Connect（物理连接） • GDGW（虚拟接口）
数据库和应用迁移 UGO	• Migrate（对象迁移） • Evaluate（数据库评估）
云连接 CC	• Cloud Connection（云连接） • Bandwidth Package（带宽包）
云原生DDoS防护 CNAD	Package（防护包）
图引擎服务 GES	GES（GES集群）
企业路由器 ER	Instance（实例）
企业主机安全 HSS	HSS（主机安全）
云日志服务 LTS	Log Stream（日志流）
云数据迁移 CDM	Cluster（集群）
设备接入 IOTDA	Instance（实例）
全球加速 GA	• Accelerators（加速器） • Listeners（监听器）
微服务引擎 CSE	CSE（微服务引擎）
应用管理与运维平台 ServiceStage	• Environment（ServiceStage环境） • Application（ServiceStage应用）
云审计服务 CTS	Tracker（追踪器）

服务	资源类型
云堡垒机 CBH	CBH（堡垒机）
云防火墙 CFW	CFW（云防火墙）
云监控服务 CES	Alarm（告警规则）
API网关 APIG	APIG（专享版实例）
应用运维管理 AOM	Alarm Rules（告警规则）
函数工作流 FunctionGraph	Functions（函数）
分布式数据库中间件 DDM	DDM（DDM实例）
AI开发平台 ModelArts	• Training Job（训练作业） • Resource Pool（资源池） • Notebook（Notebook实例） • Realtime Service（实时服务）
湖仓构建 LakeFormation	Instance（实例）
DDoS原生基础防护（Anti-DDoS流量清洗）	Anti-DDoS（流量清洗）
资源访问管理 RAM	Resource Shares（资源共享实例）
组织 Organizations	• Root（根） • OUs（组织单元） • Accounts（账号） • Policies（策略）
工业数字模型驱动引擎 iDME	• iDME-linkx-f（数字主线引擎） • iDME-mbm（数字化制造基础服务） • iDME-runtime（基础版数据建模引擎节点） • iDME-studio（iDMEStudio基础版）
凭据管理服务 CSMS	Secret（凭据）

- **关联业务**

表 4-2 与其他服务之间关系

交互功能	相关服务	位置
通过CTS服务，您可以记录与标签管理服务相关的操作事件，便于日后的查询、审计和回溯。	云审计服务（Cloud Trace Service，CTS）	审计

5 约束与限制

以下是标签使用的基本限制：

表 5-1 标签约束与限制

限制项	规格
每个资源最多支持的键-值对数	10个
资源绑定限制	对于每个资源，每个标签“键”都必须是唯一的，每个标签“键”只能有一个“值”。
每个账号中允许创建预定义标签的最大数量	500个
创建预定义标签的限制	创建的预定义标签如果与已有的预定义标签完全相同，则会覆盖已有的预定义标签；若只有“键”相同，“值”不同，则为新创建的预定义标签。
标签键限制	键的长度最大36字符，由英文字母、数字、下划线、中划线、中文字符组成。
标签值限制	值的长度最大43字符，由英文字母、数字、下划线、点、中划线、中文字符组成。

说明

并非所有的资源类型都支持添加标签，当前标签支持的服务和资源类型请以控制台界面显示为准。

6 如何访问

公有云提供了Web化的服务管理平台，即管理控制台和基于HTTPS请求的API（Application Programming Interface）管理方式。

- API方式

  如果用户需要将公有云平台上的标签管理服务集成到第三方系统，用于二次开发，请使用API方式访问标签管理服务。具体操作请参见**《标签管理服务API参考》**。

- 管理控制台方式

  管理控制台是网页形式的，您可以使用直观的界面进行相应的操作。登录**管理控制台**，单击主页左上角的  ，选择“管理与监管”下的“标签管理服务”以打开本服务界面。

7 用户权限

系统默认提供两种用户权限：用户管理权限和资源管理权限。

- 用户管理权限可以管理用户、用户组及其权限。
- 资源管理权限可以控制用户对云服务资源执行的操作。

对于资源标签的使用，您需要拥有对应云服务的相关权限。否则，您对云资源进行的标签操作可能无法生效。

请联系系统管理员为您所属的用户组添加对应云服务的相关权限。

说明

在TMS控制台对云资源的标签进行操作时，您需要具有TMS查看、创建、删除资源标签等权限，以及资源所属服务的必要权限。由于修改资源标签是通过先删除旧标签再创建新标签（标签键相同，标签值不同）来实现功能，所以要修改云资源的标签需要具备TMS和相应云服务的创建和删除标签的权限。

- 以系统权限为例：例如您需要在TMS控制台对ECS资源进行增删标签操作，那么您除了需要具有“TMS FullAccess”系统权限外，还需要拥有“ECS FullAccess”系统权限。
- 以自定义策略为例：例如您需要在TMS控制台上查看ECS的资源和标签，那么您除了需要具有“tms:resourceTags:list”权限外，您还需要拥有ECS服务的“ecs:servers:getTags”和“ecs:servers:get”权限。

IAM支持服务的所有系统权限请参见**系统权限**。有关各服务细粒度授权项的更多信息，请参见每个服务的文档。

8 权限管理

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

通过IAM，您可以在华为云账号中给员工创建IAM用户，并使用策略来控制他们对华为云资源的访问范围。例如您希望您的部分员工拥有标签管理服务的查看权限，但是不希望他们拥有删除预定义标签等操作的权限，那么您可以使用IAM为员工创建用户，通过授予标签管理服务的只读权限（TMS ReadOnlyAccess），控制员工对TMS的使用范围。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用标签管理服务的其它功能。

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

TMS 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。

TMS部署时不区分物理区域，为全局级服务。授权时，在全局项目中设置策略，访问TMS时，不需要切换区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于云服务平台各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对TMS服务，管理员能够控制IAM用户仅能对TMS服务进行指定的操作，如仅给IAM用户授予查看预定义标签的细粒度授权项，那么此IAM用户仅能查看预定义标签但不能创建和删除预定义标签。多数细粒度策略以API接口为粒度进行权限拆分，TMS支持的API授权项请参见**策略及授权项说明**。

如表8-1所示，包括了TMS的所有系统策略和系统角色。由于华为云各服务之间存在业务交互关系，标签管理服务的策略依赖其他服务的策略实现功能。因此给用户授予标签管理服务的权限时，需要同时授予依赖的权限，标签管理服务的权限才能生效。

表 8-1 TMS 系统权限

系统角色/策略名称	描述	类别	依赖关系
TMS FullAccess	标签管理服务所有权限。	系统策略	-
TMS ReadOnlyAccess	标签管理服务只读权限。	系统策略	-
TMS Administrator	标签管理服务管理员权限，拥有该服务下的所有权限，包括预定义标签的查询、创建、删除、导入和导出，以及资源标签的增删改查权限。	系统角色	依赖以下策略： • Tenant Guest：全局级/项目级策略，全部云服务只读权限（(除IAM权限)）。 • Server Administrator：项目级策略，在同项目中勾选。 • Tenant Administrator：全局级/项目级策略，全部云服务管理员（除IAM管理权限）。 • 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。

表8-2列出了TMS常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 8-2 常用操作与系统权限的关系

操作	TMS FullAccess	TMS ReadOnlyAccess	TMS Administrator
查询资源列表	√（依赖各云服务的查询资源权限）	√（依赖各云服务的查询资源权限）	√（依赖Tenant Guest）
创建标签键	√	x	√（依赖Tenant Guest）

操作	TMS FullAccess	TMS ReadOnlyAccess	TMS Administrator
查看资源标签	√	√	√（依赖Tenant Guest）
创建资源标签	√（依赖各云服务的创建标签权限）	x	√（依赖Tenant Guest及云资源对应的项目策略，如需要管理VPC的标签，需在同项目中勾选。）
修改资源标签	√（依赖各云服务的创建、删除、查看标签权限）	x	√（依赖Tenant Guest及云资源对应的项目策略，如需要管理VPC的标签，需在同项目中勾选。）
删除资源标签	√（依赖各云服务的删除标签权限）	x	√（依赖Tenant Guest及云资源对应的项目策略，如需要管理VPC的标签，需在同项目中勾选。）
查询预定义标签	√	√	√
创建预定义标签	√	x	√
删除预定义标签	√	x	√
导出预定义标签	√	√	√
导入预定义标签	√	x	√

说明

在TMS控制台对云资源的标签进行操作时，您需要具有TMS查看、创建、删除资源标签等权限，以及资源所属服务的必要权限。由于修改资源标签是通过先删除旧标签再创建新标签（标签键相同，标签值不同）来实现功能，所以要修改云资源的标签需要具备TMS和相应云服务的创建和删除标签的权限。

- 以系统权限为例：例如您需要在TMS控制台对ECS资源进行增删标签操作，那么您除了需要具有“TMS FullAccess”系统权限外，还需要拥有“ECS FullAccess”系统权限。
- 以自定义策略为例：例如您需要在TMS控制台上查看ECS的资源和标签，那么您除了需要具有“tms:resourceTags:list”权限外，您还需要拥有ECS服务的“ecs:servers:getTags”和“ecs:servers:get”权限。

IAM支持服务的所有系统权限请参见**系统权限**。有关各服务细粒度授权项的更多信息，请参见每个服务的文档。

相关文档

- **IAM产品介绍**

- 创建用户组、用户并授予TMS权限请参考：**创建用户并授权使用标签管理服务**
- 细粒度策略支持的授权项，请参见《 TMS API参考 》中的**策略及授权项说明**。

