Tag Management Service

Service Overview

Issue 01

Date 2022-11-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to "Vul. Response Process". For details about the policy, see the following website:https://www.huawei.com/en/psirt/vul-response-process For enterprise customers who need to obtain vulnerability information, visit:https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Tag Management Service

Tag Management Service (TMS) is a visualized service for quickly tagging and categorizing cloud services across fast and unified cross-regions.

Tags are used to identify cloud resources. When you have cloud resources of the same type, you can use tags to classify cloud resources by dimension, for example, usage, owner, or environment.

Figure 1-1 Example tags

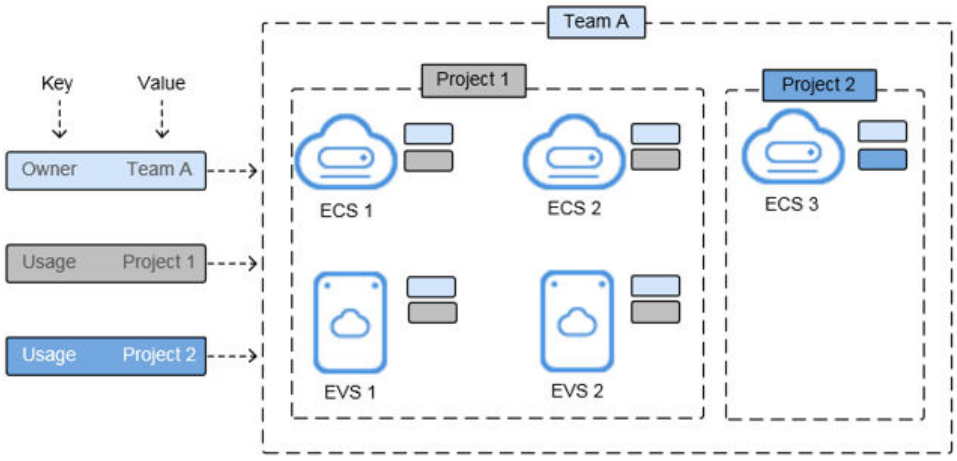


Figure 1-1 shows how tags work. In this example, you assign two tags to each cloud resource. Each tag contains a key and a value that you define. The key of one tag is **Owner**, and that of another tag is **Usage**. Each tag has a value.

You can quickly search for and filter specific cloud resources based on the tags added to them. For example, you can define a set of tags for cloud resources in an account to identify their owners and usage, making resource management easier.

TMS provides the following functions:

- Managing resources: Add tags to resources as needed to classify resources. TMS provides you with a visualized table to manage resource tags, including editing tags in batches.

- Searching for resources: Search for resources across services and regions regions by tag or by tag set.
- Predefined tag management: You can create, import, or export predefined tags. By predefining tags, you can plan tags according to your services to effectively manage tags.

NOTE

TMS is free of charge.

2 Region and AZ

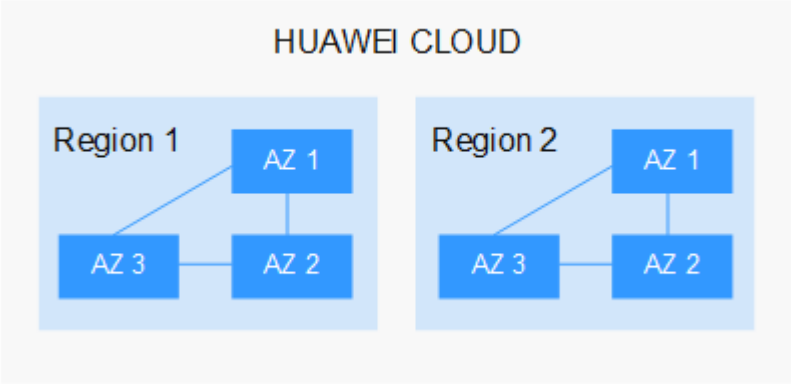
Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers, to support cross-AZ high-availability systems.

Figure 2-1 shows the relationship between regions and AZs.

Figure 2-1 Regions and AZs



Huawei Cloud provides services in many regions around the world. You can select a region and an AZ based on requirements. For more information, see **Huawei Cloud Global Regions**.

Selecting a Region

When selecting a region, consider the following factors:

- Location

  It is recommended that you select the closest region for lower network latency and quick access.

  - If your target users are in Asia Pacific (excluding the Chinese mainland), select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If your target users are in Africa, select the **AF-Johannesburg** region.
  - If your target users are in Latin America, select the **LA-Santiago** region.

    NOTE

    The **LA-Santiago** region is located in Chile.

- Resource price

  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

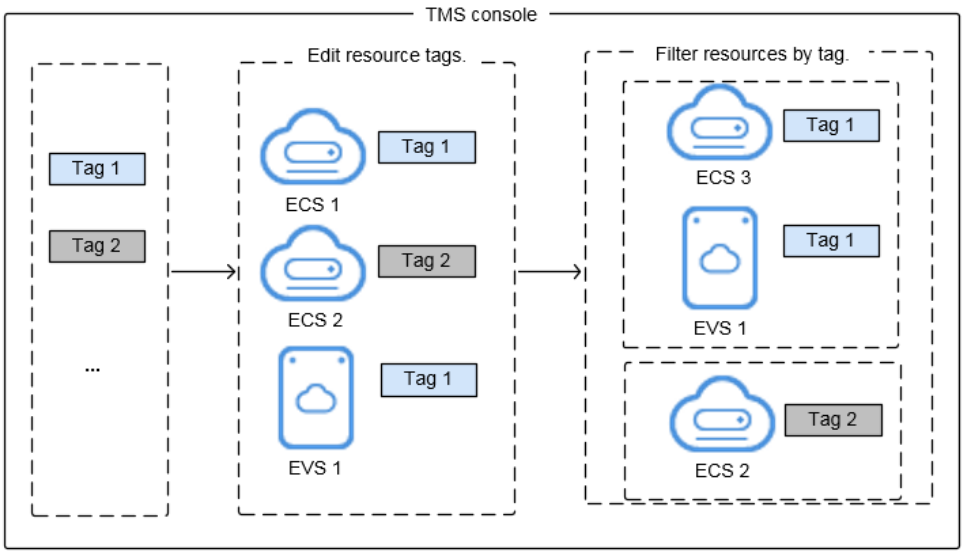
3 Application Scenarios

TMS is useful in the following typical application scenarios:

Central Management of Resources

For users who have many cloud resources, TMS allows them to quickly locate all of their resources with specific tags. TMS also provides a unified tag management platform, on which users can check, modify, or delete tags.

Figure 3-1 Central management of resources



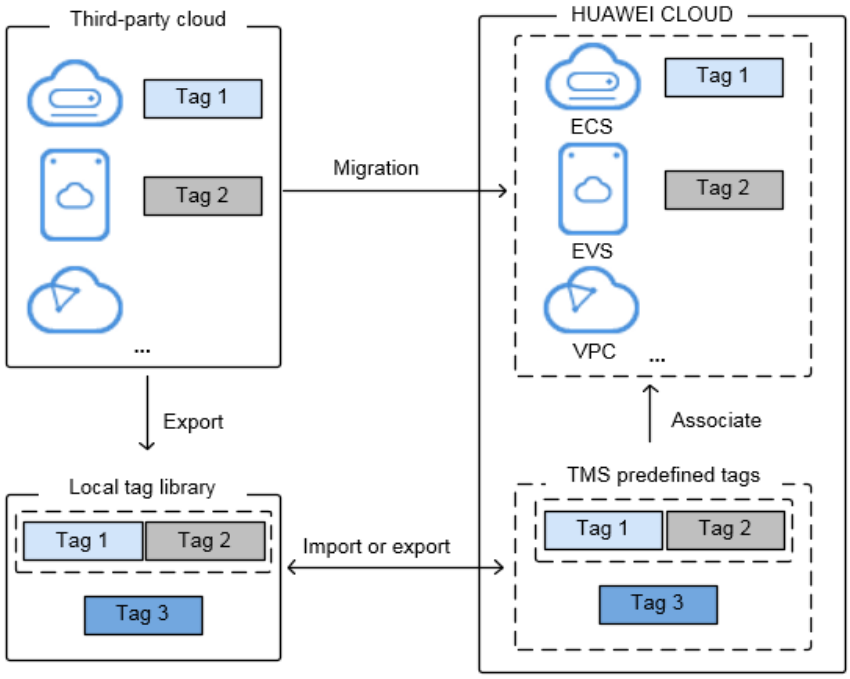
Quick Identification of Resources Migrated and to Be Migrated

For users who need to migrate large numbers of resources, TMS allows for the import and export of predefined tags. This improves the accuracy and efficiency of resource migration while eliminating the need to set tags each time.

- Creating predefined tags: You can create predefined tags on TMS before migrating resources. After resources are migrated, they can be associated directly with predefined tags.

- Importing and exporting predefined tags: If you have inventory tags, you can quickly import them to the predefined tag library of TMS. After resources are migrated, you can associate those resources with predefined tags. In addition, you can export predefined tags for editing.

  Figure 3-2 Quick identification of resources migrated and to be migrated



4 Security

4.1 Shared Responsibilities

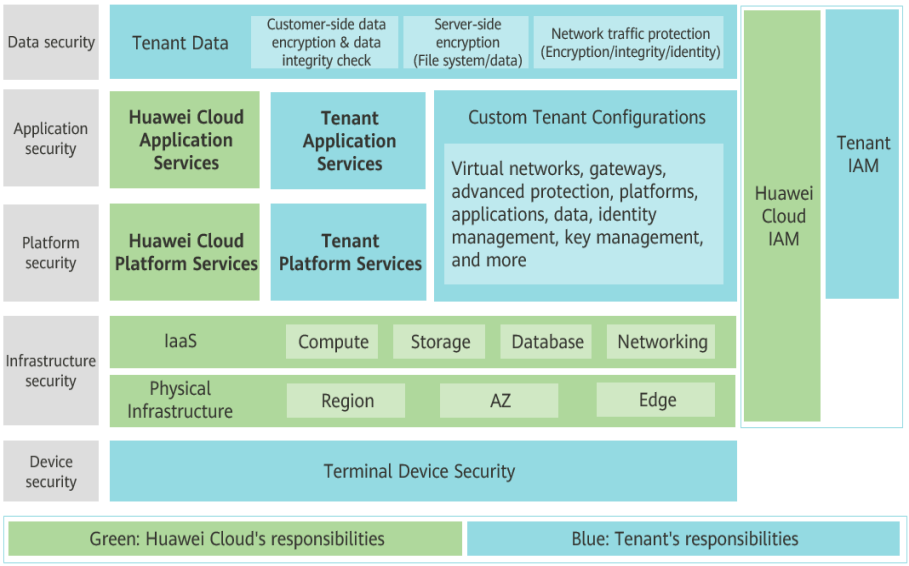
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Figure 4-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 4-1 Huawei Cloud shared security responsibility model



4.2 Identity Authentication and Access Control

Identity and Access Management (IAM) is a basic service provided by Huawei Cloud for permissions management, access control, and identity authentication. You can use IAM to create and manage users and user groups, grant permissions to allow or deny their access to cloud services and resources, and configure policies to improve account and resource security. IAM also provides you with multiple secure access credentials.

You can use IAM to control access to your TMS resources. IAM permissions define which actions on your cloud resources are allowed or denied. After creating an IAM user, the administrator needs to add the user to a user group and grants the required permissions by TMS to the user group. Then, all users in this group automatically inherit the granted permissions.

For details, see **User Permissions** and **Permissions**.

4.3 Auditing and Logging

Cloud Trace Service (CTS) is a log audit service for Huawei Cloud security. It allows you to collect, store, and query cloud resource operation records. You can use these records for security analysis, audit compliance, resource tracking, and fault locating.

After CTS is enabled, TMS operations can be recorded for auditing.

- For details about how to enable and configure CTS, see **Enabling CTS**.
- For details about TMS operations that can be audited, see **Key TMS Operations**.
- For details about how to view CTS traces, see **Viewing CTS Traces**.

4.4 Data Protection Technologies

4.4.1 Static Data Protection

TMS cannot be used to modify, add, or delete Huawei Cloud resources. It collects the following information:

- Predefined tag keys
- Predefined tag values

4.4.2 Data Transmission Protection

An encryption protocol is used when data is transmitted to the internal database of TMS. You cannot configure the encryption protocol during the transmission process.

When you call TMS APIs, you can use HTTP and HTTPS protocols. HTTPS is recommended for higher security.

4.4.3 Data Destruction

After data is deleted, the data is stored in a historical database list. After a Huawei Cloud account is deleted, the data under the account will be retained for seven days before being permanently deleted.

5 TMS and Other Services

- Services that support TMS

  TMS allows you to manage resource tags centrally. For which services are supported by TMS, you need to go to the TMS console to check it out.

  A cloud service can have multiple resource types. You can select a resource type as required on the TMS console and manage the tags of this type of resources in a centralized manner.

- Related services

  Table 5-1 Relationships with other services

Function	Service	Reference
With CTS, you can record operations associated with TMS for later query, audit, and backtrack operations.	Cloud Trace Service (CTS)	**Key TMS Operations**

6 Constraints and Limitations

The following are basic constraints on using tags:

Table 6-1 Constraints

Item	Specifications
Maximum number of key-value pairs you can add for each resource	10
Tags of each resource	For each resource, each tag key must be unique, and each tag key can have only one tag value.
Maximum number of predefined tags that you can create for an account	500
Predefined tags	If the created predefined tag is the same as an existing predefined tag, the existing predefined tag is overwritten. If only keys are the same and values are different, both the tags are available.
Tag keys	A tag key can contain a maximum of 36 characters, including digits, letters, underscores (_), and hyphens (-).
Tag values	A tag value can contain a maximum of 43 characters, including digits, letters, underscores (_), periods (.), and hyphens (-).

NOTE

Not all resources are supported by TMS. For which services and resources are supported, you can go to the service console to check it out..

7 Accessing TMS

Huawei Cloud provides a web-based service management platform. You can use either of the following ways to access TMS:

- APIs

  To integrate TMS into a third-party system for secondary development, call APIs to access TMS. For details, see **Tag Management Service API Reference**.

- Management console

  The management console is a web user interface for you to manage your compute, storage, and other cloud resources. Users who have signed up withthe public cloud can access TMS by selecting **Tag Management Service** under **Management & Governance** on the management console.

8 User Permissions

Permissions for the system are divided into user management and resource management permissions.

- User management refers to the management of users, user groups, and user group permissions.
- Users with resource management permissions can manage the operations performed on cloud service resources.

To use resource tags, you must have the corresponding permissions on the cloud service. Otherwise, the tag operations on cloud resources may not take effect.

Contact the system administrator to assign the corresponding cloud service permissions to the user group to which you belong.

NOTE

If you need to perform operations on tags of cloud resources on TMS console, you must have related permissions for viewing, creating, and deleting resource tags and required permissions for the services to which the resources belong. Modify a resource tag involves a process of deleting the old tag and then creating a new tag (with the same tag key but different tag values). So, to modify a cloud resource tag, you must have both related TMS permissions and service permissions to delete and create tags.

- For system-defined permissions: If you need to add or delete tags for ECS resources on TMS console, both **TMS FullAccess** permissions and **ECS FullAccess** permissions are required.
- For custom permissions: If you need to view ECS resources and tags on the TMS console, not only **tms:resourceTags:list** permissions, but **ecs:servers:getTags** and **ecs:servers:get** permissions are required.

For details about all system-defined permissions of services supported by IAM, see **System-defined Permissions**. For more information about fine-grained permissions of each service, see corresponding documentations of each service.

9 Permissions

If you need to assign different permissions to personnel in your enterprise to access your cloud resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely access your Huawei Cloud resources.

With IAM, you can use your Huawei Cloud account to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. For example, if you need to grant some users the permissions to view TMS resources, but don't want these users to delete predefined tags, you can create users using IAM and assign TMS ReadOnlyAccess permissions to these users.

If your Huawei Cloud account does not require IAM for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account. For more information about IAM, see **IAM Service Overview**.

TMS Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

TMS is a global service deployed for all regions. When you set the authorization scope to **Global services**, users have permission to access TMS resources in all regions.

You can grant permissions by using roles and policies.

- Roles: A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities Only a limited number of service-level roles are available for authorization. When using roles to grant permissions, you must also assign other roles which the permissions depend on to take effect. Roles are not ideal for fine-grained authorization and least privilege access.
- Policies: A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain

conditions. This type of authorization is more flexible and is ideal for least privilege access. The administrator can restrict a user to only specified operations on TMS using IAM policies. For example, if the user is granted a fine-grained permission to only view predefined tags, the user cannot perform other operations on predefined tags (such as creating or deleting predefined tags) with this permission. A majority of fine-grained policies contain permissions for specific APIs. For the API actions supported by TMS, see **Permissions Policies and Supported Actions**.

Table 9-1 lists all the system-defined policies and roles for TMS. Some TMS policies depend on the policies of other services to take effect. When you assign TMS permissions to users, you also assign dependent policies for the TMS permissions to take effect.

Table 9-1 System-defined permissions for TMS

Role/Policy Name	Description	Type	Dependencies
TMS FullAccess	Full permissions for TMS.	System-defined policy	-
TMS ReadOnlyAccess	Read-only permissions for TMS.	System-defined policy	-

Role/Policy Name	Description	Type	Dependencies
TMS Administrator	Full permissions for TMS. Users with these permissions can query, create, delete, import, or export predefined tags, and create, delete, modify, or query resource tags.	System-defined role	Dependent on the following policies: • **Tenant Guest**: a global/project-level policy that grants read-only permissions for all cloud services (except IAM). • **Server Administrator**: A project-level policy, which must be assigned in the same project as the **TMS Administrator** policy. • **Tenant Administrator**: A global/project-level policy that grants permissions of all cloud service administrators (except the IAM administrator permissions). • **IMS Administrator**: a project-level policy, which must be assigned in the same project as the **TMS Administrator** policy • **AutoScaling Administrator**: a project-level policy, which must be assigned in the same project as the **TMS Administrator** policy • **VPC Administrator**: a project-level policy, which must be assigned in the same project as the **TMS Administrator** policy • **VBS Administrator**: a project-level policy, which must be assigned in the same project as the **TMS Administrator** policy

Table 9-2 lists the common operations supported by system-defined permissions for TMS.

Table 9-2 Common operations supported by system-defined permissions

Operation	TMS FullAccess	TMS ReadOnlyAccess	TMS Administrator
Querying the cloud resource list	Supported (permissions of corresponding services for querying resources required)	Supported (permissions of corresponding services for querying resources required)	Supported (Tenant Guest required)
Creating a key	Supported	Not supported	Supported (Tenant Guest required)
Viewing resource tags	Supported	Supported	Supported (Tenant Guest required)
Creating resource tags	Supported (permissions of corresponding services for creating tags required)	Not supported	Supported (Tenant Guest and corresponding project policies of cloud resources required. For example, if you need to manage VPC tags, select **Tenant Guest** in the same project.)
Modifying resource tags	Supported (permissions of corresponding services for creating, deleting, and viewing tags required)	Not supported	Supported (Tenant Guest and corresponding project policies of cloud resources required. For example, if you need to manage VPC tags, select **Tenant Guest** in the same project.)
Deleting resource tags	Supported (permissions of corresponding services for deleting tags required)	Not supported	Supported (Tenant Guest and corresponding project policies of cloud resources required. For example, if you need to manage VPC tags, select **Tenant Guest** in the same project.)
Querying predefined tags	Supported	Supported	Supported

Operation	TMS FullAccess	TMS ReadOnlyAccess	TMS Administrator
Creating predefined tags	Supported	Not supported	Supported
Deleting predefined tags	Supported	Not supported	Supported
Exporting predefined tags	Supported	Supported	Supported
Importing predefined tags	Supported	Not supported	Supported

NOTE

If you need to perform operations on tags of cloud resources on TMS console, you must have related permissions for viewing, creating, and deleting resource tags and required permissions for the services to which the resources belong. Modify a resource tag involves a process of deleting the old tag and then creating a new tag (with the same tag key but different tag values). So, to modify a cloud resource tag, you must have both related TMS permissions and service permissions to delete and create tags.

- For system-defined permissions: If you need to add or delete tags for ECS resources on TMS console, both **TMS FullAccess** permissions and **ECS FullAccess** permissions are required.
- For custom permissions: If you need to view ECS resources and tags on the TMS console, not only **tms:resourceTags:list** permissions, but **ecs:servers:getTags** and **ecs:servers:get** permissions are required.

For details about all system-defined permissions of services supported by IAM, see **System-defined Permissions**. For more information about fine-grained permissions of each service, see corresponding documentations of each service.

Related Documents

- To learn about the IAM service, see **What Is IAM?**.
- For details about how to create a user or a user group and how to grant TMS permissions, see **Creating a User and Granting Permissions**.
- For details about permission policies and supported actions for TMS, see **Permissions Policies and Supported Actions**.

10 SCP-based Access Control

IAM provides system-defined policies to define common actions supported by cloud services. You can also create custom policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the **Organizations** service also provides **service control policies (SCPs)** to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The permissions granted through IAM can only take effect if they are allowed by the SCPs.

This section describes Service Control Policy (SCP) elements. These elements include actions, resources, and conditions.

For details about how to use these elements to create a custom SCP, see **Creating an SCP**.

Actions

Actions are specific operations that are allowed or denied in a policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in a policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("*") in your policy statements.
  - If this column includes a resource type, you must specify the resource URN in the Resource element of your policy statements.
  - Required resources are marked with asterisks (*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by Config, see **Resources**.

- The **Condition Key** column contains keys that you can specify in the Condition element of a policy statement.
  - If the **Resource Type** column of an action is not empty, the condition key takes effect only for the listed resources.
  - If the **Resource Type** column of an action is empty (-), the condition key takes effect for all resources.
  - If this column is empty (-), the action does not support any condition keys.

  For details about the condition keys defined by Config, see **Conditions**.

The following table lists the actions that you can define in SCP statements for TMS.

Table 10-1 Actions supported by TMS

Action	Description	Access Level	Resource Type (* required)	Condition Key
tms:predefineTags:list	Grants permissions to query predefined tags	list	-	-
tms:predefineTags:create	Grants permissions to create predefined tags.	write	-	-
tms:predefineTags:update	Grants permissions to modify predefined tags.	write	-	-
tms:predefineTags:delete	Grants permissions to delete predefined tags.	write	-	-
tms:resourceTags:list	Grants permissions to query resource tags.	list	-	-
tms:resourceTags:create	Grants permissions to create resource tags.	write	-	-

Action	Description	Access Level	Resource Type (* required)	Condition Key
tms:resourceTags:delete	Grants permissions to delete resource tags.	write	-	-
tms:resources:list	Grants permissions to query resources.	list	-	-
tms:tagKeys:list	Grants permissions to query tag keys.	list	-	-
tms:tagValues:list	Grants permissions to query tag values.	list	-	-

Resources

TMS does not support granting permissions for specific resources using a policy. To allow access to TMS, use the wildcard (*) in the Resource element in a policy. Then this policy will apply to all resources of TMS.

Conditions

Only global condition keys applicable to all cloud services can be configured for TMS. Global condition keys that apply to all services are supported by TMS. For details, see **common global condition keys**.

