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 the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 What Is Tag Management Service?

Tag Management Service (TMS) helps you centrally categorize and manage cloud resources across regions and services with tags.

You can group cloud resources by usage, owner or the environment where the resources are deployed.

Figure 1-1 Example tags

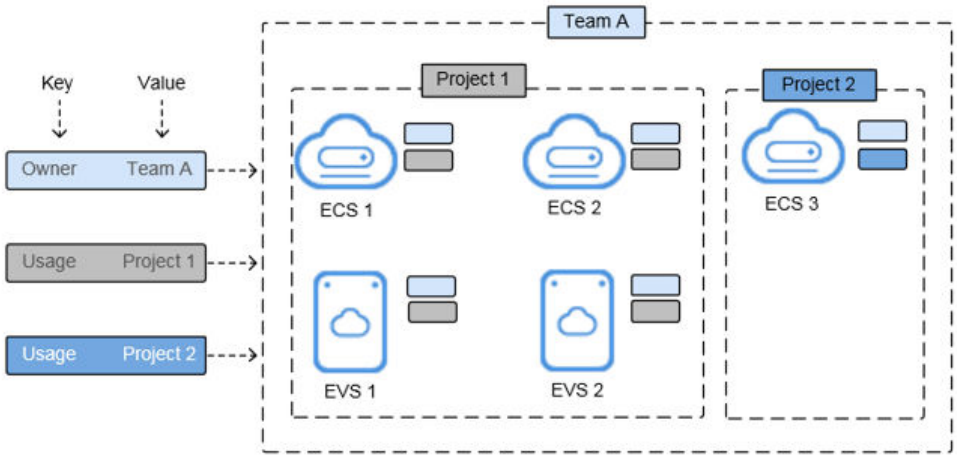


Figure 1-1 shows how tags work. In this example, you assign two tags to each cloud resource. Each tag contains a key and a value that you define. The key of one tag is **Owner**, and that of another tag is **Usage**. Each tag has a value.

You can quickly search for and filter cloud resources based on the tags added to them. For example, if you define a set of tags to specify resource owners or usage and attach these tags to your resources, you can easily filter these resources by owner or usage.

TMS provides the following functions:

- Resource management allows you to classify resources by tag. You can easily manage one tag or multiple tags at the same time in a visualized table.
- 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.

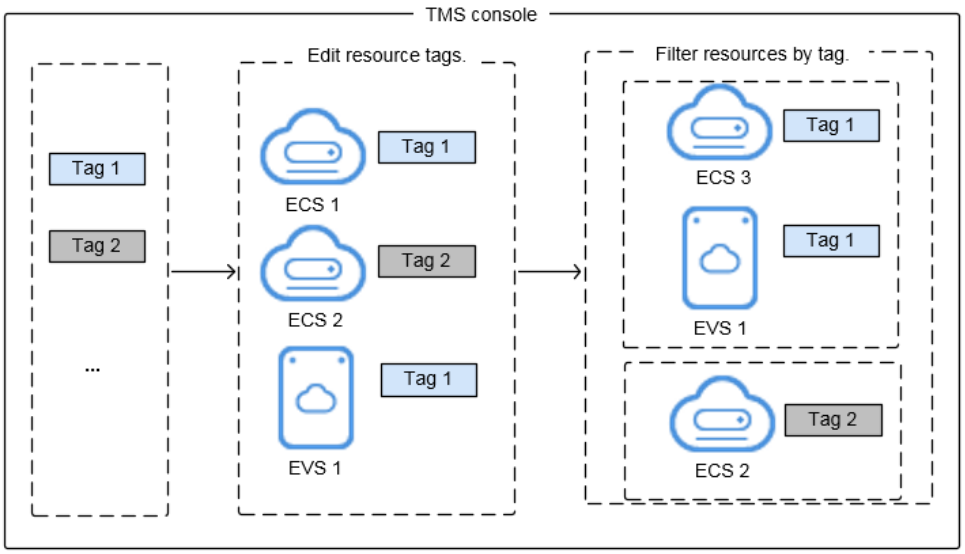
2 Application Scenarios

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 2-1 Central management of resources



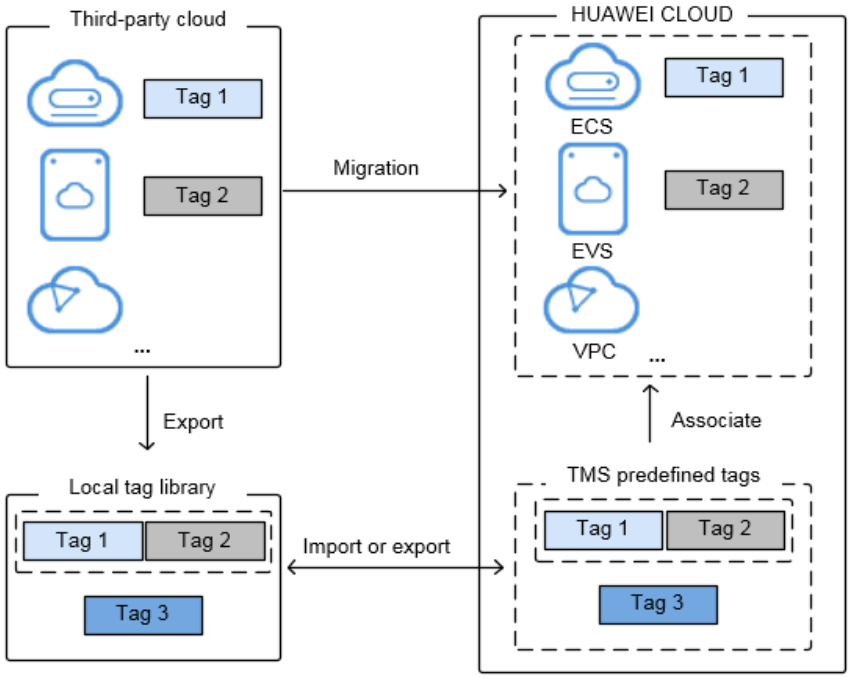
Quick Identification of Resources Migrated and to Be Migrated

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



3 Security

3.1 Shared Responsibilities

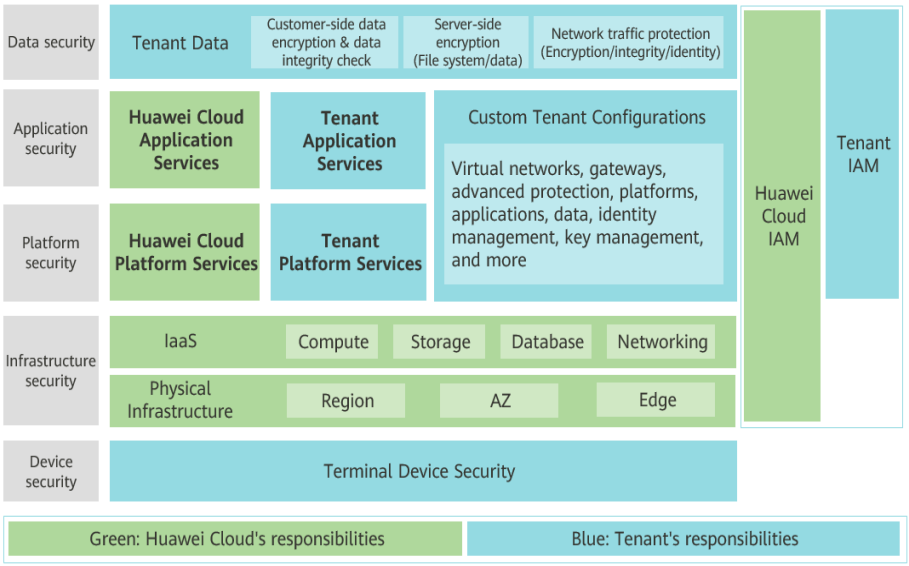
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 3-1 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 3-1 Huawei Cloud shared security responsibility model



3.2 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**.

3.3 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**.

3.4 Data Protection Technologies

3.4.1 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

3.4.2 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.

3.4.3 Data Destruction

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

4 TMS and Other Services

- Services that support TMS

  TMS allows you to manage resource tags centrally. For details about services supported by TMS, see **Table 4-1**.

  A cloud service may contain multiple resource types. You can specify a resource type and then centrally manage tags on TMS console as need.

  Table 4-1 Services that support TMS

Service	Resource Type
VPC Endpoint (VPCEP)	• VPC endpoint • VPC endpoint service
Data Replication Service (DRS)	• Data synchronization task • Data subscription task • Disaster recovery task • Backup migration task • Real-time migration task
Bare Metal Server (BMS)	BMS
Elastic Cloud Server (ECS)	ECS
Object Storage Service (OBS)	Bucket
Virtual Private Cloud (VPC)	• VPC • Subnet
Elastic IP (EIP)	EIP-EIP
Elastic Volume Service (EVS)	Disk
Auto Scaling (AS)	AS group
Image Management Service (IMS)	Private image
Distributed Cache Service (DCS)	DCS-DCS

Service	Resource Type
Workspace	Desktop
Domain Name Service (DNS)	• Private zone • Public zone • PTR record • Private record set • Public record set
Virtual Private Network (VPN)	• VPN connection • VPN gateway • Customer gateway
Scalable File Service (SFS)	SFS Turbo
Elastic Load Balance (ELB)	• Enhanced load balancer • Enhanced load balancer listener
Simple Message Notification (SMN)	Topic
Distributed Message Service (DMS)	• Kafka instance • RabbitMQ instance • RocketMQ instance
Data Lake Insight (DLI)	• Queue • Resource package • Flink template • Flink job • Basic datasource connection • Enhanced datasource connection • Database • Elastic resource pool
Relational Database Service (RDS)	DB instance
MapReduce Service (MRS)	Cluster
Data Warehouse Service (DWS)	Cluster
Document Database Service (DDS)	DB instance
Data Ingestion Service (DIS)	Stream
Web Application Firewall (WAF)	Instance
Cloud Search Service (CSS)	CSS-Cluster
NAT Gateway	• Public gateway • Private gateway • Transit IP

Service	Resource Type
Cloud Backup and Recovery (CBR)	Vault
Data Encryption Workshop (DEW)	KMS key
Cloud Container Engine (CCE)	• Cluster • Autopilot cluster
DataArts Studio (DAYU)	• Workspace • Instance
GaussDB	Instance
Database Security Service (DBSS)	Instance
Content Delivery Network (CDN)	Domain name
Direct Connect	• Direct connection • GDGW (virtual interface)
Database and Application Migration UGO	• Object migration • Database evaluation
Cloud Connect (CC)	• Cloud connection • Bandwidth package
Cloud Native Anti-DDoS (CNAD)	Package
Graph Engine Service (GES)	Cluster
Enterprise Router (ER)	Instance
Host Security Service (HSS)	Host security service
Log Tank Service (LTS)	Log stream
Cloud Data Migration (CDM)	Cluster
IoT Device Access (IoTDA)	Instance
Global Accelerator (GA)	• Accelerator • Listener
Cloud Service Engine (CSE)	Engine
ServiceStage	• Environment • Application
Cloud Trace Service (CTS)	Tracker
Cloud Bastion Host (CBH)	Cloud bastion host
Cloud Firewall (CFW)	Cloud firewall
Cloud Eye	Alarm
API Gateway (APIG)	Dedicated API gateway

Service	Resource Type
Application Operations Management (AOM)	Alarm rule
FunctionGraph	Function
Distributed Database Middleware (DDM)	Instance
ModelArts	• Training job • Resource pool • Notebook instance • Real-time service
LakeFormation	Instance
Anti-DDoS	Cloud Native Anti-DDoS Basic
Resource Access Manager (RAM)	Resource share
Organizations	• Root • OU • Account • Policy
Industrial Digital Model Engine (iDME)	• iDME-linkx-f • iDME-mbm • iDME-runtime • iDME-studio
Cloud Secret Management Service (CSMS)	Secret

- Related services

Table 4-2 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**

5 Constraints and Limitations

The following are basic constraints on using tags:

Table 5-1 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.
The maximum predefined tags that each account can create.	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 (_), hyphens (-), and at signs (@).
Tag values	A tag value can contain a maximum of 43 characters, including digits, letters, underscores (_), periods (.), hyphens (-), and at signs (@).

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..

6 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

  Log in to the **management console**, click  on the upper left corner, and choose **Tag Management Service** under **Management & Governance**. The **Tag Management Service** page is displayed.

7 User Permissions

You have permissions to manage users and resources.

- You add users to user groups so that users can inherit permissions attached to user groups which they are in.
- You can control which resources and what actions a user can access.

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.

8 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 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 do not 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 can be used free of charge. You pay only 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 8-1 lists all TMS system-defined policies and roles. 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 8-1 TMS system-defined permissions

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 8-2 lists the common operations supported by TMS system-defined permissions.

Table 8-2 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**.

