ALIBABA CLOUD

Alibaba Cloud

Resource Management

Tag

Document Version: 20220622

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Tag overview

Tags are used to identify cloud resources. Tags allow you to categorize, search for, and aggregate cloud resources that have the same characteristics from different dimensions. This facilitates resource management.

Common scenarios

You can use tags to perform the following operations:

- Search for resources.

  Add tags to resources and search for resources by tag in the Resource Management console or by calling a tag-related API operation. For more information, see Use tags to query cloud resources.

- Implement automated O&M.

  Add different tags to environments such as production and test environments, operating systems such as Windows and Linux, or mobile platforms such as iOS and Android. Then, create a template in Operation Orchestration Service (OOS) and execute the template to implement automated O&M for your resources. For more information, see Overview.

- Control access to resources.

  You can use tags in Resource Access Management (RAM) to manage the access and operation permissions of RAM users on different resources. For more information, see Create a resource with a specific tag and Use tags to control access to ECS resources.

Benefits

The Tag service provides the following benefits:

- Convenience: A unified, visualized console is provided to manage the resources to which tags are added.
- Flexibility: You can add, remove, modify, or query one or more tags in the console or by calling an API operation.
- Visibility: You can use tags to manage separate bills for departments, products, and projects.

Terms

Term	Description
key-value pair	A tag consists of a key-value pair.
custom tag	A custom tag is created by a user. For more information, see Add a custom tag.
preset tag	A preset tag is a tag that you create in advance and is available for the resources in all regions. You can create preset tags in the stage of tag planning and add them to specific cloud resources in the stage of tag implementation. The system provides some common built-in types for preset tags. This allows you to quickly plan tag systems. For more information, see Create a preset tag.

Term	Description
system tag	A system tag is defined by the system. You can only query system tags. System tags present data relationships in a standard manner. In some specific cases, you can use system tags to assist in processing your business. For example, a cluster is associated with an Elastic Compute Service (ECS) instance, and the system adds the system tag of the cluster ID to the ECS instance. This way, you can determine the attribution of the ECS instance based on the system tag. For more information, see View system tags and the resources to which a system tag is added.
tag editor	The tag editor is a tool that is used to manage resource tags in a centralized manner. You can use the tag editor to search for resources that belong to different Alibaba Cloud services and reside in different regions. In addition, you can use the tag editor to add, modify, or remove tags for multiple resources at a time, and export resource lists.
createdby tag	createdby tags are a type of system tag that is generated by Alibaba Cloud and automatically added to resources. This type of tag is used to identify the creators of resources. createdby tags can help you analyze costs and bills and manage the costs of cloud resources in an efficient manner.

Differences between custom tags and preset tags

Different from system tags, custom tags and preset tags are created by users and can be added or removed by users. The following table describes the differences between custom tags and preset tags.

Tag type	Visibility	Lifecycle
Custom tag	Custom tags are visible only in the region where they are created. For example, custom tags created in the China (Hangzhou) region are invisible in the China (Beijing) region.	When you create a custom tag, you must add it to a resource. A custom tag that is not added to resources is deleted within 24 hours after it is created.
Preset tag	Preset tags are visible in all regions. A preset tag is a tag that you create in advance and is available for the resources in all regions.	You can create a preset tag first and add it to resources in subsequent operations. Preset tags have an independent lifecycle. If you no longer require a preset tag, you can delete it.

Alibaba Cloud services that support tags

A series of core Alibaba Cloud services support tags, such as ECS, ApsaraDB RDS, Object Storage Service (OSS), Virtual Private Cloud (VPC), Server Load Balancer (SLB), and Container Service for Kubernetes (ACK). Alibaba Cloud intends to add tag support for other services. For more information, see Services that work with Tag.

Limits

Item	Limit
Maximum number of tags that can be added to a single resource	20
Whether tag information can be shared across regions	No. For example, in the China (Shanghai) region, you cannot view tags created in the China (Hangzhou) region.
Tag key	A tag key must be 1 to 128 characters in length and cannot contain `http://` or `https://`. It cannot start with `aliyun` or `acs:`.
Tag value	A tag value must be 1 to 128 characters in length and cannot contain `http://` or `https://`. It cannot start with `aliyun` or `acs:`.
Adding tags to resources	Each tag key on a resource can have only one tag value. If you create a tag that has the same key as an existing tag, the value of the existing tag is overwritten. For example, the `city:shanghai` tag is added to a resource. If you add the `city:newyork` tag to the resource, the `city:shanghai` tag is automatically removed from the resource.
Maximum number of preset tags that can be created within a single Alibaba Cloud account	1,000
Maximum number of tag values that can be specified for a single preset tag key	1,000

2.Use tags to query cloud resources

This topic describes how to query cloud resources to which a specific tag is added. You can use the methods provided in this topic to query cloud resources.

Query resources on the Tag page of the Resource Management console

For an Alibaba Cloud service that supports tags, you can query resources by tag on the Tag page of the Resource Management console.

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag > Tag**.
3. In the top navigation bar, select the desired region.
4. Click the **Custom Tags**, **Predefined Tags**, or **System Tags** tab.
5. Find the desired tag and click **View Resources** in the **Action** column to view the cloud resources to which the tag is added.

Query resources in the consoles of Alibaba Cloud services

For an Alibaba Cloud service that supports tags, you can query resources by tag in the console of the service. In this example, the Elastic Compute Service (ECS) console is used to query resources.

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the top navigation bar, select the desired region.
4. On the **Instances** page, click **Tags** and select a tag key and a tag value.

   If you do not select a tag value, all ECS instances to which the selected tag key is added are displayed.

Query resources by calling a tag-related API operation

For an Alibaba Cloud service that supports tags, you can use a Tag API operation or a tag-related API operation provided by the service to query resources. The following descriptions demonstrate the preceding operations:

- Tag API operation: Call the ListTagResources operation. Specify the value of the request parameter `Tags` to query the resources to which the tags specified by this parameter are added.
- Tag-related API operations provided by Alibaba Cloud services: Call the tag-related API operation provided by each service to query the resources to which specific tags are added. For more information, see Services that work with Tag.

Query resources by using the tag editor

The tag editor is a tool that is used to manage resource tags in a centralized manner. You can use the tag editor to search for resources that belong to different Alibaba Cloud services and reside in different regions.

1. Log on to the Resource Management console. The Tag page appears.

2. In the left-side navigation pane, choose **Tag > Tag Editor**.
3. In the **Search** section, specify conditions to search for resources.

   You can specify multiple tags that reside in different regions and are added to different resources to search for resources.
4. Click **Search**.
   In the **Search Results** section, view the resources.

3.Custom tags

3.1. Add a custom tag

If multiple cloud resources that are associated with each other exist within your account, you can add custom tags to these resources. This allows you to categorize the resources and manage them in a centralized manner.

Context

- Many Alibaba Cloud services support tags. For more information, see Services that work with Tag.
- A maximum of 20 tags can be added to a resource. If the number of tags that are added to a resource exceeds the upper limit, you must remove some of the tags before you add new tags.
- You can use one of the following methods to add a tag to a resource:
  - Perform operations in a console: You can add tags to resources on the Tag page of the Resource Management console or in the consoles of Alibaba Cloud services.
    - This topic describes how to add a tag to a resource on the Tag page of the Resource Management console.
    - For more information about how to add a tag in the console of an Alibaba Cloud service, see the **References** column in Services that work with Tag.
  - Use an API operation: You can call the TagResources operation of the Tag service or the related operation of an Alibaba Cloud service to add a tag to a resource.
    - For more information about the TagResources operation of the Tag service, see TagResources.
    - For more information about the related operation of each Alibaba Cloud service, see the **References** column in Services that work with Tag.
  - Use Operation Orchestration Service (OOS): You can use OOS to add tags to multiple resources at a time. For more information, see Use OOS to add tags to multiple resources.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag > Tag**.
3. In the top navigation bar, select a region.
4. On the **Custom Tags** tab, click **Create Custom Tags**.
5. In the **Create Custom Tags** dialog box, create a tag or select an existing tag.
   - **Tag key**: required. You can select an existing tag key or enter a new tag key. You can perform a fuzzy match by prefix and add a maximum of 10 tag keys at a time.

     Each tag key can contain a maximum of 128 characters in length and cannot contain *http://* or *https://*. It cannot start with *aliyun* or *acs:*.
   - **Tag value**: optional. You can select an existing tag value or enter a new tag value.

     Each tag value can contain a maximum of 128 characters in length and cannot contain *http://* or *https://*. It cannot start with *aliyun* or *acs:*.

> **Note** If you want to add a tag, select an existing tag key and an existing tag value. If you want to create a tag, enter a new tag key and a new tag value.

6. Click **Next**.
7. Specify **Product**, **Resource Type**, and **Input Types**. Then, select resources or enter resource IDs.

   Input Types includes the following options:

   - **Select resources**: allows you to select resources from the resource list.
   - **Enter multiple resource IDs**: allows you to enter resource IDs. Separate multiple IDs with commas (,).
8. Click **Confirm**.
9. In the message that appears, click **Close**.

Result

View the tag that is added to the resources on the Custom Tags tab.

Related information

- TagResources

3.2. Remove a custom tag

If a custom tag cannot be used to manage or query cloud resources, you can remove the tag from the resources. This topic describes how to remove a custom tag from cloud resources.

Context

After you remove a custom tag from cloud resources, the system automatically deletes the tag within 24 hours if it is not added to other resources.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag > Tag**.
3. In the top navigation bar, select the desired region.
4. On the Tag page, click the **Custom Tags** tab.
5. On the Custom Tags tab, find the custom tag that you want to remove and click the tag key. On the page that appears, click the tag value that corresponds to the tag key.
6. Remove the custom tag from resources.
   - Remove the custom tag from a single resource: Click **Unbind** in the **Action** column.
   - Remove the custom tag from multiple resources at a time: Select the resources from which you want to remove the tag and click **Unbind** below the resource list.
7. In the **Unbind** message, click **Confirm**.

Related information

- UntagResources

3.3. Export resources to which a custom tag is added in a resource group

You can export resources to which a custom tag is added in a resource group as a CSV file.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag > Tag**.
3. In the top navigation bar, select a region.
4. On the Tag page, click the **Custom Tags** tab.
5. On the Custom Tags tab, find the desired custom tag and click **View Resources** in the **Action** column to view the cloud resources to which the tag is added.
6. On the page that appears, select the resources that you want to export and click the icon.
7. In the **Export resource data** dialog box, select **All Resources** or **Selected Resources** and click **OK**.

Related information

- Export resources by using the tag editor

4.Preset tags

4.1. Create a preset tag

This topic describes how to create a preset tag.

Overview

What is a preset tag?

A preset tag is a tag that you create in advance and is available for the resources in all Alibaba Cloud regions. You can create preset tags in the stage of tag planning and add them to specific cloud resources in the stage of tag implementation.

You can create preset tags but do not add them to resources. A preset tag that is not added to resources is invisible in the regions where the resources reside.

You can specify only a tag key when you create a preset tag. You can specify a tag value for the preset tag in subsequent operations.

Limits

- Maximum number of preset tags that can be created within a single Alibaba Cloud account: 1,000
- Maximum number of tag values that can be specified for a single preset tag key: 1,000

Creation methods

You can use one of the following methods to create a preset tag:

- Use a tag template to create a preset tag

  The system presets the tag templates listed in the following table. This allows you to quickly plan a tag system. For more information, see Use a tag template to create a preset tag.

Tag type	Description	Tag key
Environment tag	Indicates the business environments to which resources belong, such as development environment, test environment, and production environment.	Environment
Organization tag	Indicates the organization to which the resources belong, such as company, department, team, and project.	◦ Company ◦ Department ◦ Team ◦ Project
Role tag	Indicates the roles of resource managers, such as network administrator, application administrator, and system administrator.	Role

Tag type	Description	Tag key
Cost tag	Indicates the attribution of internal financial costs, such as department, branch, and business unit. This type of tag is mainly used for internal settlement and cost accounting.	BusinessUnit
User tag	Indicates the owners of resources. This type of tag is used when the resource applicant is not the resource user. An owner can be indicated by their name, employee ID, or email address.	Owner

- Customize a preset tag

  For more information, see Customize a preset tag.
- Use an Excel file to create a preset tag

  For more information, see Use an Excel file to create a preset tag.

Use a tag template to create a preset tag

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag > Predefined Tags**.
3. On the Predefined Tags page, click **Create Predefined Tags**.
4. In the Select Tag Template step of the **Create Predefined Tags** dialog box, set **Creation Method** to **Select Tag Template**.
5. In the **Tag Templates** section, select the desired tag template and click **Next**.
6. In the Configure Tag Keys step of the Create Predefined Tags dialog box, specify a tag key and a tag value and click **Create Predefined Tags**.
7. In the message that appears, click **Close**.

Customize a preset tag

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag > Predefined Tags**.
3. On the Predefined Tags page, click **Create Predefined Tags**.
4. In the Select Tag Template step of the **Create Predefined Tags** dialog box, set **Creation Method** to **Customize Predefined Tag** and click **Next**.
5. In the Configure Tag Keys step of the Create Predefined Tags dialog box, specify a tag key and a tag value and click **Create Predefined Tags**.
6. In the message that appears, click **Close**.

Use an Excel file to create a preset tag

1. Log on to the Resource Management console.

2. In the left-side navigation pane, choose **Tag > Predefined Tags**.
3. On the Predefined Tags page, click **Create Predefined Tags**.
4. In the Select Tag Template step of the **Create Predefined Tags** dialog box, set **Creation Method** to **Import from Excel File**.
5. In the **Import Predefined Tags** section, click **Click here to upload an .xlsx file**, upload the Excel file in which a tag is created, and then click **Next**.

   > **Note** You can click sample.xlsx to download the sample file and refer to the content in the sample file to create a tag in an Excel file. This improves tag creation efficiency and ensures tag validity.

6. View or modify the imported tag key and tag value and click **Create Predefined Tags**.
7. In the message that appears, click **Close**.

What's next

After the preset tag is created, you can add the tag to resources. For more information, see Add a preset tag.

4.2. Add a preset tag

After a preset tag is created, you can add the tag to resources.

Context

A preset tag that is not added to resources is invisible in the regions where the resources reside.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag > Predefined Tags**.
3. In the top navigation bar, select the region where the resources to which you want to add a preset tag reside.
4. On the Predefined Tags page, find the preset tag that you want to add to resources and click **Bind Resources** in the **Action** column.

   > **Note** If a tag key has more than three tag values, you can click **View more** in the Tag Value column to view all the tag values of the tag key.

5. In the **Bind Resources** dialog box, specify **Product**, **Resource Type**, and **Input Types**. Then, select resources from the resource list or enter resource IDs.

   Input Types includes the following options:

   - **Select resources**: allows you to select resources from the resource list.
   - **Enter multiple resource IDs**: allows you to enter resource IDs. Separate multiple IDs with commas (,).

6. Click **Confirm**.
7. In the message that appears, click **Close**.

Result

On the Predefined Tags page, find the preset tag that is added to the resources and click **View Resources** in the **Action** column. Then, you can view the resources to which the tag is added.

4.3. Remove a preset tag

If a preset tag cannot be used to manage or query cloud resources, you can remove the tag from the resources. This topic describes how to remove a preset tag from cloud resources.

Context

After you remove a preset tag from cloud resources, the system retains the tag if it is not added to other resources. You can also delete the preset tag. For more information about how to delete a preset tag, see Delete a preset tag.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag > Predefined Tags**.
3. In the top navigation bar, select the region where the resources from which you want to remove a preset tag reside.
4. On the Predefined Tags tab, find the preset tag that you want to remove and click the tag value in the Tag Value column.

   > **Note** If a tag key has more than three tag values, you can click **View more** in the Tag Value column to view all the tag values of the tag key.

5. Remove the preset tag from resources.
   - Remove the preset tag from a single resource: Click **Unbind** in the **Action** column.
   - Remove the preset tag from multiple resources at a time: Select the resources from which you want to remove the tag and click **Unbind** below the resource list.
6. In the **Unbind** message, click **Confirm**.

4.4. Delete a preset tag

If you do not need a preset tag, you can delete it.

Context

When you add a preset tag to a resource, a custom tag that resides in the same region as the resource is actually added to the resource. When you delete the preset tag, you delete only the preset tag itself. The custom tag that is added to the resource is not deleted.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag > Predefined Tags**.
3. On the Predefined Tags page, find the preset tag that you want to delete and click **Delete** in the **Action** column.

4. In the **Delete Tag** message, click **Confirm**.

4.5. Export resources to which a preset tag is added

You can export resources to which a preset tag is added as a CSV file.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag > Predefined Tags**.
3. On the Predefined Tags page, find the desired preset tag and click **View Resources** in the **Action** column. On the page that appears, you can view the resources to which the tag is added.
4. Specify filter conditions to search for the resources that you want to export.

   For example, you can search for resources by region, tag, or resource type. You can also specify a resource ID to perform this operation.
5. Select the resources that you want to export and click the icon.
6. In the **Export resource data** dialog box, select **All Resources** or **Selected Resources** and click **OK** to export the resources as a CSV file.

Related information

- Export resources by using the tag editor

5.Tag editor

5.1. Search for resources

A tag editor is a tool that is used to manage resource tags in a centralized manner. You can use a tag editor to search for resources that belong to different Alibaba Cloud services and reside in different regions.

Procedure

1. Log on to the Resource Management console. The Tag page appears.
2. In the left-side navigation pane, choose **Tag > Tag Editor**.
3. In the **Search** section, specify conditions to search for resources.

   You can specify multiple tags that reside in different regions and are added to different resources to search for resources.
4. Click **Search**.
   In the **Search Results** section, view the resources.

5.2. Manage tags

You can add, modify, or remove tags for multiple resources at a time.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag > Tag Editor**.
3. Search for resources to which tags are added. For more information, see Search for resources.
4. In the **Search Results** section, select one or more resources and click **Edit Tags**.
5. Manage resource tags.
   - Modify a tag: You can enter a new tag key or tag value for an existing tag.
   - Add a tag: Click **Add Tag**. Then, enter a tag key and a tag value.
   - Remove a tag: Click **Delete** to remove a tag.

     > **Note** After you click Delete, you can click **Cancel Deletion** to recover the tag that you deleted. However, if you have clicked Submit, the tag cannot be recovered.
6. Click **Submit**.
7. Click **OK**.

5.3. Export resources by using the tag editor

You can use the tag editor to export resources as a CSV file. You can export resources that belong to different Alibaba Cloud services, reside in different regions, or have different tags.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag > Tag Editor**.
3. Search for resources to which specific tags are added. For more information, see Search for resources.
4. In the **Search Results** section, select one or more resources.
5. Move the pointer over **Export** and select one of the following methods to export the resources:
   - **Export All Data**: Export all the attributes of the selected resources as a CSV file.
   - **Export Visible Columns**: Export only the displayed attributes of the selected resources as a CSV file.

> **Note** You can click the  icon to view all the attributes of the selected resources or customize the attributes you want to present.

Related information

- Export resources to which a custom tag is added in a resource group
- Export resources to which a preset tag is added

6.Createdby tags

6.1. Overview

createdby is a type of system tag that is provided by Alibaba Cloud and automatically added to resources. This type of tag is used to identify the creators of resources. createdby tags can help you analyze costs and bills and manage the costs of cloud resources in an efficient manner.

Format of createdby tags

Tag key or value	Format
Tag key	`acs:tag:createdby`
Tag value	• If the resource is created by using an Alibaba Cloud account, the tag value is in the `customer:<AccountId>` format. `<AccountId>` indicates the ID of the Alibaba Cloud account. • If the resource is created by using a RAM user, the tag value is in the `sub:<RamUserId>:<RamUserName>` format. `<RamUserId>` indicates the ID of the RAM user, and `<RamUserName>` indicates the username of the RAM user. • If the resource is created by using a RAM user and the RAM user assumes a RAM role by using a security Token Service (STS) token, the tag value is in the `assumedRoleUser:<RamRoleName>:<RolePlayerId>` format. `<RamRoleName>` indicates the name of the RAM role that is assumed by the RAM user, and `<RolePlayerId>` indicates the ID of the RAM user.

Use createdby tags

1. Enable createdby tags on the Createdby Tag page of the Resource Management console.

   Only an Alibaba Cloud account or a RAM user to which the AdministratorAccess policy is attached can be used to enable createdby tags. To enable createdby tags, perform the following steps:

   i. Log on to the Resource Management console.

   ii. In the left-side navigation pane, choose **Tag > CreatedBy Tag**.

   iii. On the Createdby Tag page, click **Enable Createdby Tag**.

   iv. Read the information about the service-linked role for the Tag service and click **OK**.

   For more information, see Service-linked role for the Tag service.

   v. In the **Enable Createdby Tag** message, click **OK**.

   After you enable createdby tags, the system adds `createdby` tags to newly created resources. The system does not add `createdby` tags to the resources that are created before you enable createdby tags.

   You cannot manually add `createdby` tags to resources or remove createdby tags from resources. `createdby` tags are not included in the number of tags that can be added to a resource.

> **Note** You can click **Disable Createdby Tag** to disable `createdby` tags. After you disable `createdby` tags, the system no longer adds createdby tags to newly created resources but retains the createdby tags that are added.

2. View createdby tags.
   - View createdby tags on the Tags page of the Resource Management console or in the console of an Alibaba Cloud service

     You can view the createdby tag of a resource on the Tags page of the Resource Management console or in the console of the Alibaba Cloud service to which the resource belongs 5 to 10 minutes after you create the resource.
   - View createdby tags on the Cost Analysis or Bills page of the User Center

     You can view createdby tags on the Cost Analysis or Bills page of the User Center 24 hours after you enable createdby tags.

Alibaba Cloud services that support createdby tags

createdby tags can be added only to the resources of Alibaba Cloud services listed in the following table.

Alibaba Cloud service	Resource type	Support for viewing of createdby tags in the Alibaba Cloud service console
Elastic Compute Service (ECS)	• instance: instance • ddh: dedicated host • image: image • snapshotpolicy: automatic snapshot policy	Yes
Elastic IP Address (EIP)	• eip: EIP	Yes
Server Load Balancer (SLB)	• instance: instance • certificate: certificate	Yes
Alibaba Cloud CDN (CDN)	• domain: domain name	Yes
Cloud Enterprise Network (CEN)	• cen: CEN instance	No
PolarDB	• cluster: cluster	Yes
ApsaraDB for Redis	• instance: instance	Yes
ApsaraDB RDS	• instance: instance	Yes
ApsaraDB for MongoDB	• instance: instance	Yes

Alibaba Cloud service	Resource type	Support for viewing of createdby tags in the Alibaba Cloud service console
Apsara File Storage NAS (NAS)	• filesystem: file system	Yes
Object Storage Service (OSS)	• bucket: bucket	No
Anti-DDoS Pro	• instance: instance	Yes
NAT Gateway	• natgateway: NAT gateway	Yes
Application Load Balancer (ALB)	• loadbalancer: ALB instance	No
Elastic Container Instance	• containergroup: container group	No
Container Service for Kubernetes (ACK)	• cluster: cluster	Yes
E-MapReduce (EMR)	• cluster: cluster	No
Function Compute	• service: service	Yes
AnalyticDB for MySQL	• cluster: cluster	Yes
Elasticsearch	• instance: cluster	Yes
ApsaraDB for HBase	• cluster: cluster	Yes
Message Queue for Apache RocketMQ	• instance: instance • group: group • topic: topic	No
VPN Gateway	• vpngateway: VPN gateway	Yes
EIP Bandwidth Plan	• commonbandwidthpackage: EIP bandwidth plan	Yes
Bastionhost	• instance: instance	Yes
Anti-DDoS Origin	• instance: instance	Yes
Alibaba Cloud DNS (DNS)	• domain: domain name	No

6.2. Service-linked role for the Tag service

This topic describes the use scenarios, policy, creation, and deletion of the service-linked role AliyunServiceRoleForTag for the Tag service.

Scenarios

When you enable `createdby` tags, the Tag service automatically creates its service-linked role AliyunServiceRoleForTag. The Tag service uses the service-linked role to obtain the access permissions on ActionTrail.

For more information about service-linked roles, see Service-linked roles.

Role description

Role name: AliyunServiceRoleForTag.

Policy name: AliyunServiceRolePolicyForTag.

Permission description: This policy allows the Tag service to create, delete, or view ActionTrail trails and delete the service-linked role of the Tag service.

```
{
   "Version": "1",
   "Statement": [
       {
           "Action": [
               "actiontrail:CreateServiceTrail",
               "actiontrail:DeleteServiceTrail",
               "actiontrail:ListServiceTrail"
           ],
           "Resource": "*",
           "Effect": "Allow"
       },
       {
           "Action": "ram:DeleteServiceLinkedRole",
           "Resource": "*",
           "Effect": "Allow",
           "Condition": {
               "StringEquals": {
                   "ram:ServiceName": "tag.aliyuncs.com"
               }
           }
       }
   ]
}
```

Create the service-linked role for the Tag service

When you enable `createdby` tags, the Tag service automatically creates its service-linked role AliyunServiceRoleForTag. For more information about createdby tags, see Overview.

Delete the service-linked role for the Tag service

You can delete the service-linked role AliyunServiceRoleForTag for the Tag service in the Resource Access Management (RAM) console after you disable `createdby` tags. For more information, see Delete a RAM role.

7.System tags

7.1. View system tags and the resources to which a system tag is added

A system tag is defined by the system. You can only query system tags. System tags present data relationships in a standard manner. In some specific cases, you can use system tags to assist in processing your business. For example, a cluster is associated with an Elastic Compute Service (ECS) instance. In this case, the system automatically adds the ID of the cluster as a system tag to the ECS instance. This way, you can determine the attribution of the ECS instance based on the system tag.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag > Tag**.
3. In the top navigation bar, select the desired region.
4. On the Tag page, click the **System Tags** tab to view the system tags in the region.
5. Click a tag key to view all the tag values that correspond to the tag key.
6. In the **Action** column that corresponds to a tag value, click **View Resources** to view all the resources to which the tag is added.

8.Tag policies

8.1. Overview

Tag policies are a type of policy that is used to standardize the tags that are added to resources. You can use a tag policy to define the tags that must be added to your resources. Compliant tags can help you improve the efficiency in the aspects such as cost allocation by tag and automated O&M. Tag policies support the single-account mode and multi-account mode. The two modes can meet your business requirements for standardized tag management in different stages.

Scenarios

As your resources on the cloud increase, you can add tags to the resources to classify the resources. This way, you can allocate costs by tag and implement automated O&M. When you add tags to a resource, issues may occur. For example, after you create a resource, you forget to add tags to the resource, you add only some tags such as O&M-related tags but forget to add finance-related tags, or the tags that you added contain spelling errors. If these issues occur, the costs of some resources cannot be allocated based on your business requirements when you allocate costs by tag, or automated O&M operations cannot be performed for some resources. Tag policies provide solutions for these issues in the following scenarios:

- **Automatic tag detection**

  After you create a resource and add tags to the resource, you can use a tag policy to periodically check the following items to determine the tag compliance of the resource:

  - Whether the tags added to the resource are compliant
  - Whether the tags defined in the tag policy are added to the resource

  Automatic tag detection can help you identify issues at the earliest opportunity.

- **Automatic remediation for tags**

  If you enable automatic remediation for tags and the remediation rules that you configure match the conditions for triggering automatic remediation, the system remediates the non-compliant tags based on the detection results.

- **Enforce tag compliance when you create a resource**

  Automatic tag detection starts with a latency. After a resource is created, non-compliant tags for the resource cannot be detected before automatic tag detection is started. We recommend that you perform standardized tag management when you create a resource. To achieve this, you can enable tag policy enforcement for a resource type when you create a tag policy. This way, when you create a resource of this type, tag compliance is enforced for the resource. If you add non-compliant tags to the resource, the resource fails to be created. Tag compliance enforcement takes effect only for tags that are defined in a tag policy. If no tags are added to a resource or other tags are added to the resource to which tag policy is applied, tag compliance enforcement does not take effect.

  > **Note** The tag policy enforcement feature is in invitational preview. You can contact the service manager of Alibaba Cloud to apply for a trial.

- **Automatic tag inheritance from a resource group**

After you add a tag to a resource group, if you create a resource in or add a resource to the resource group, the tag is automatically added to the resource.

Procedure

Tag policies support the single-account mode and multi-account mode. You cannot use the two modes at the same time.

- Enable the Tag Policy feature that is in single-account mode

  If your business on the cloud is simple and you use only one Alibaba Cloud account and the RAM users within the Alibaba Cloud account to perform management operations, you can use the Alibaba Cloud account to enable the Tag Policy feature that is in single-account mode. Then, you can use tag policies to manage the tag-related operations performed by using the Alibaba Cloud account or the RAM users.

- Enable the Tag Policy feature that is in multi-account mode

  If your business on the cloud is complex and you use a resource directory to manage all your accounts, you can use the management account of the resource directory to enable the Tag Policy feature that is in multi-account mode. Then, you can use tag policies to manage the tag-related operations performed by using a member within the resource directory.

Limits

Item	Limit
Maximum number of tag policies you can create when you use the Tag Policy feature that is in single-account mode	10
Maximum number of tag policies you can create when you use the Tag Policy feature that is in multi-account mode	100
Maximum number of characters that each tag policy can contain	2,048
Time required before tag policy enforcement takes effect	• After you attach a tag policy for which enforcement is enabled to an object, enforcement takes effect for the object within 5 minutes. • After you modify a tag policy for which enforcement is enabled, enforcement takes effect for the attached object within 5 minutes.

Item	Limit
Time required before the automatic tag detection is started or complete	• After you attach a tag policy to an object, automatic tag detection starts within 1 hour. • After a resource is created within the account to which a tag policy is attached, automatic tag detection starts within 10 minutes. • After a resource within the account to which a tag policy is attached is modified, automatic tag detection starts in real time. • After the document of a tag policy that is attached to an account is modified, automatic tag detection is performed for all resources within the account. The time required for the detection depends on the number of the resources within the account. A larger number of resources indicate a longer detection time.
Time required before automatic remediation is complete	After resources to which non-compliant tags are added are detected, the system remediates the non-compliant tags within 10 minutes.

Best practices

- Enable tag policy enforcement

Alibaba Cloud services that support tag policies

Alibaba Cloud service	Service code	Support for automatic tag detection	Support for tag policy enforcement[1]	Support for automatic tag inheritance from a resource group
Alibaba Cloud CDN (CDN)	cdn	Yes	No	Yes
Apsara File Storage NAS (NAS)	nas	Yes	Yes	No
ApsaraDB RDS	rds	Yes	Yes	Yes
ApsaraDB for Redis	kvstore	Yes	Yes	Yes
ApsaraDB for MongoDB	mongodb	Yes	Yes	Yes
ApsaraDB for HBase	hbase	Yes	Yes	Yes
PolarDB	polardb	Yes	No	Yes

Alibaba Cloud service	Service code	Support for automatic tag detection	Support for tag policy enforcement[1]	Support for automatic tag inheritance from a resource group
Alibaba Cloud DNS (DNS)	dns	Yes	Yes	Yes
Elasticsearch	elasticsearch	Yes	No	Yes
Elastic Compute Service (ECS)	ecs	Yes	Yes	Yes
Auto Scaling (ESS)	ess	Yes	Yes	No
Resource Orchestration Service (ROS)	ros	Yes	Yes	Yes
Server Load Balancer (SLB)	slb	Yes	Yes	Yes
Virtual Private Cloud (VPC)	vpc	Yes	Yes	Yes
NAT Gateway	nat	Yes	Yes	Yes
VPN Gateway	vpn	Yes	Yes	No
EIP Bandwidth Plan	cbwp	Yes	Yes	Yes
Elastic IP Address (EIP)	eip	Yes	Yes	Yes
Cloud Enterprise Network (CEN)	cbn	Yes	Yes	Yes
Operation Orchestration Service (OOS)	oos	Yes	Yes	Yes
Message Queue for Apache RocketMQ	ons	Yes	Yes	No
Bastionhost	bastionhost	Yes	Yes	Yes
Anti-DDoS	ddoscoo	Yes	Yes	No

Additional information:

[1]Tag policy enforcement includes the **enforcement of tag compliance when you create a resource** and the **enforcement of tag compliance when you add tags to a resource**. Support for tag compliance enforcement varies based on the Alibaba Cloud service type. For more information, see Enable tag policy enforcement.

8.2. Getting started

This topic describes how to use a tag policy to standardize tag-related operations.

Context

Tag policies support the single-account mode and multi-account mode. You cannot use the two modes at the same time.

- If your business on the cloud is simple and you use only one Alibaba Cloud account and the RAM users within the Alibaba Cloud account to perform management operations, you can use the Alibaba Cloud account to enable the Tag Policy feature that is in single-account mode. Then, you can use tag policies to manage the tag-related operations performed by using the Alibaba Cloud account or the RAM users.
- If your business on the cloud is complex and you use a resource directory to manage all your accounts, you can use the management account of the resource directory to enable the Tag Policy feature that is in multi-account mode. Then, you can use tag policies to manage the tag-related operations performed by using a member within the resource directory.

When you use the Tag Policy feature for the first time, we recommend that you enable the feature by using a test account that has a small number of resources. If the test is successful, you can enable the feature by using a production account.

Enable the Tag Policy feature that is in single-account mode

Step 1: Enable the Tag Policy feature

Step 2: Create a tag policy

You can create and configure a tag policy to define the tags that must be added to a resource. This ensures that the tags added to the resource are compliant.

1.
2. On the **Policy Library** page, click **Create Tag Policy**.
3.
4.

Step 3: Attach the tag policy

After the tag policy is created, you must attach the policy to the current Alibaba Cloud account. This way, you can use the tag policy to standardize tags added to the resources in the account.

1. In the left-side navigation pane, choose **Tag Policy > Policy Library**.
2. On the **Policy Library** page, find the tag policy that you want to attach and click **Attach** in the **Actions** column.
3. In the **Attach** message, click **OK**.

   The tag policy is attached to the Alibaba Cloud account that you use for logon.

Step 4: (Optional) View the effective policy

After the tag policy is attached to the current Alibaba Cloud account, you can view the effective policy of the account.

1. In the left-side navigation pane, choose **Tag Policies > Effective Policies**.

2. View the document of an effective policy.

   You can view the document of an effective policy in visualized mode or display the document in the JSON format. By default, View in Visualized Mode is used. You can switch from View in Visualized Mode to **View in JSON Format**.

Step 5: Check whether the tag policy is in effect

You can use the current Alibaba Cloud account or a RAM user within the account to perform a tag-related operation to check whether the tag policy is in effect. For example, you apply a tag policy to a VPC, and the tag policy defines that the tag `CostCenter:Beijing` must be added to the VPC. When you add tags to the VPC, only the compliant tag `CostCenter:Beijing` is added to the VPC. Non-compliant tags such as `costCenter:Shanghai` fail to be added to the VPC. This indicates that the tag policy is in effect.

Enable the Tag Policy feature that is in multi-account mode

For security purposes, we recommend that you create a RAM user within the management account of your resource directory, attach the AdministratorAccess policy to the RAM user, and then use the RAM user as the administrator of the resource directory. Perform the following operations by using the RAM user. For more information about how to create a RAM user and grant permissions to the RAM user, see Create a RAM user and Grant permissions to a RAM user.

Step 1: Enable the Tag Policy feature

Step 2: Create a tag policy

You can create and configure a tag policy to define the tags that must be added to a resource. This ensures that the tags added to the resource are compliant.

1.
2. On the **All Tag Policies** tab of the **Policy Library** page, click **Create Tag Policy**.
3.
4.

Step 3: Attach the tag policy

After the tag policy is created, you must attach the tag policy to the Root folder, a specific folder, or a specific member. This way, you can use the tag policy to standardize the tags added to the resources in the members.

1. In the left-side navigation pane, choose **Tag Policy > Policy Library**.
2. On the **Policy Library** page, click the **All Tag Policies** tab.
3. Find the tag policy that you want to attach and click **Attach** in the **Actions** column.
4. In the **Attach** dialog box, select the objects to which you want to attach the tag policy and click **OK**.

   The effective scope of the tag policy varies based on the object type.

   - Root folder: If you attach the tag policy to the Root folder, the tag policy takes effect for all members in the resource directory.
   - Specific folder: If you attach the tag policy to a specific folder, the tag policy takes effect only for all members in the folder.
   - Specific member: If you attach the tag policy to a specific member, the tag policy takes effect

only for the member.

> **Note** You cannot attach tag policies to the management account of a resource directory. Tag policies do not take effect for management accounts.

Step 4: (Optional) View the effective policy

After the tag policy is attached, you can use the RAM user to view the effective policy of the Root folder, the specified folder, or the specified member as the administrator of the resource directory. You can use a member to view the effective policy of the member. An effective policy is obtained based on the inheritance relationship of a tag policy. For more information, see Inheritance of a tag policy and calculation of an effective policy.

1. In the left-side navigation pane, choose **Tag Policies > Effective Policies**.
2. View the document of an effective policy.

   You can view the document of an effective policy in visualized mode or display the document in the JSON format. By default, View in Visualized Mode is used. You can switch from View in Visualized Mode to **View in JSON Format**.

Step 5: Check whether the tag policy is in effect

1. Use the RAM user to access a member to which the tag policy is attached.

   For more information, see Access a member.
2. Perform a tag-related operation on a resource in the member to check whether the tag policy is in effect.

   For example, you apply a tag policy to a VPC, and the tag policy defines that the tag `CostCenter:Beijing` must be added to the VPC. When you add tags to the VPC, only the compliant tag `CostCenter:Beijing` is added to the VPC. Non-compliant tags such as `costCenter:Shanghai` fail to be added to the VPC. This indicates that the tag policy is in effect.

8.3. Perform automatic tag detection

After resources are created, you can use tag policies to detect tag compliance of the resources. This helps you identify the resources to which compliant tags are not added or non-compliant tags are added in an efficient manner. For example, to determine tag compliance of the resources, you can use tag policies to detect whether tags added to the resources are compliant or tags defined in the tag policies are added to the resources. The automatic tag detection feature helps you identify tag non-compliance issues at the earliest opportunity.

Context

The automatic tag detection feature is available when you use the Tag Policy feature that is in single-account mode or multi-account mode. This topic describes how to use a tag policy to automatically detect whether a cost center tag is added to all resources in an Alibaba Cloud account and the RAM users within the Alibaba Cloud account. In this example, the Tag Policy feature in single-account mode is used. The tag key of the cost center tag is `CostCenter`, and the tag value of the cost center tag is `Beijing` or `Shanghai`. This indicates that only `CostCenter:Beijing` and `CostCenter:Shanghai` are compliant tags.

For more information about the Alibaba Cloud services that support automatic tag detection, see the **Support for automatic tag detection** column in the Alibaba Cloud services that support tag policies section in Overview.

Procedure

1. Enable the Tag Policy feature that is in single-account mode

   For more information, see Enable the Tag Policy feature.

2. Create a tag policy.
   i. On the **Policy Library** page, click **Create Tag Policy**.
   ii. On the Create Tag Policy page, enter a policy name in the Policy Name field.
   iii. (Optional)Enter a description in the Policy Description field.
   iv. Configure the tag policy on the **Quick Mode** tab.
      a. In the **Tag Key** field, enter `CostCenter`.
      b. Select **Add Tags with Specified Tag Values to Resources** for the Select Policy Scenario parameter.
      c. Select **Specify Allowed Tag Values** and click **Specify Tag Values**.
      d. In the Specify Allowed Tag Values dialog box, enter a tag value in the Allowed Tag Values field and click **OK**.

         You can click **Add** to add multiple tag values. In this example, two tag values `Beijing` and `Shanghai` are added.
   v. Click **Create**.

3. Attach the tag policy.

   Attach the tag policy created in Step to the current Alibaba Cloud account. After the tag policy is attached to the Alibaba Cloud account, the tag policy takes effect for the Alibaba Cloud account and the RAM users within the Alibaba Cloud account.

   For more information, see Attach a tag policy.

4. View the effective policy.

   Check whether the tag policy attached in Step is displayed on the Effective Policies page.

   For more information, see View the effective policies.

5. View the result of automatic tag detection.

   After the tag policy is attached to the Alibaba Cloud account, the system automatically detects tag compliance of resources in the Alibaba Cloud account and the RAM users within the Alibaba Cloud account and identifies the resources to which compliant tags are not added or non-compliant tags are added. You can view and download the detection result. For resources to which compliant tags are not added or non-compliant tags are added, you can add the compliant tags to or change the tags of the resources. Then, you can view the detection result again. The resources are no longer displayed in the detection result.

   For more information, see View and download non-compliance detection results.

8.4. Enable tag policy enforcement

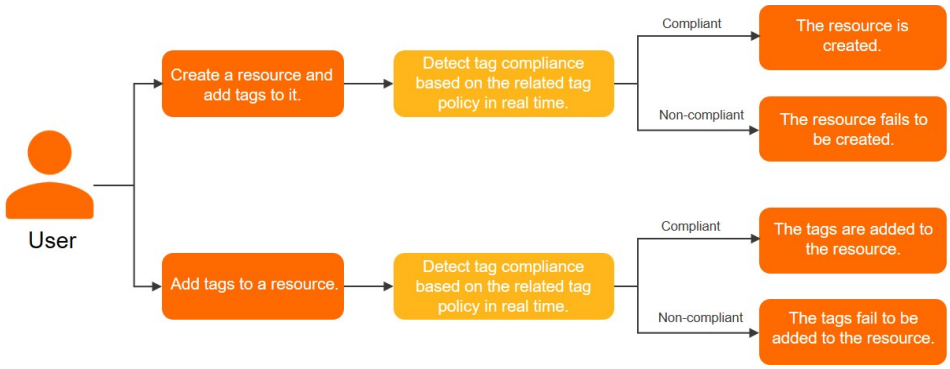
You can use a tag policy to forbid a non-compliant tag-related operation. If a tag-related operation does not conform to the rules defined in the tag policy, the operation fails.

> **Note** The tag policy enforcement feature is in invitational preview. You can contact the service manager of Alibaba Cloud to apply for a trial.

Usage notes

You can use the tag policy enforcement feature in one of the following scenarios:

- Enforce tag compliance with a tag policy when you create a resource.
- Enforce tag compliance with a tag policy when you add tags to a resource.



Before you enable tag policy enforcement, you must take note of the following items:

- If you enable tag policy enforcement, the production of resources may be affected. Before you enforce tag policy enforcement, we recommend that you perform a test by using a test account.
- Only some types of resources support tag policy enforcement. For more information, see the **Support for tag policy enforcement** column in Alibaba Cloud services that support tag policies.
- The enforcement of a tag policy for a cloud service may affect other cloud services. For example, you enable enforcement for a tag policy of Elastic Compute Service (ECS) instances and want to perform scaling for your resources in Auto Scaling or Container Service for Kubernetes (ACK). In this case, the scaling may fail because compliant tags are not added to the resources. Therefore, before you enable tag policy enforcement, make sure that you can perform tag-related operations that meet the requirements of the related services.

Procedure

In this example, the Tag Policy feature in multi-account mode is used. The management account of a resource directory is used to enable the Tag Policy feature that is in multi-account mode and create a tag policy. The tag policy defines that a cost center tag must be added to an ECS instance when you use a member in the resource directory to create the ECS instance. The tag key of the cost center tag is `CostCenter`, and the tag value is `Beijing` or `Shanghai`. The ECS instance can be created only if the cost center tag is added to the ECS instance. The tag key and tag value of the cost center tag are case-sensitive.

For security purposes, we recommend that you create a RAM user within the management account of your resource directory, attach the AdministratorAccess policy to the RAM user, and then use the RAM user as the administrator of the resource directory. Perform the following operations by using the RAM user. For more information about how to create a RAM user and grant permissions to the RAM user, see Create a RAM user and Grant permissions to a RAM user.

1. Enable the Tag Policy feature that is in multi-account mode.

   For more information, see Enable the Tag Policy feature.

2. Create a tag policy.
   i. On the **All Tag Policies** tab of the **Policy Library** page, click **Create Tag Policy**.
   ii. On the Create Tag Policy page, enter a policy name.
   iii. (Optional)Enter a policy description.
   iv. Configure the tag policy on the **Quick Mode** tab.
      a. In the **Tag Key** field, enter `CostCenter`.
      b. Select **Specify Allowed Tag Values** and click **Specify Tag Values**.
      c. In the Specify Allowed Tag Values dialog box, enter the desired tag value and click **OK**.

         You can click **Add** to specify multiple tag values for the tag key. In this example, two tag values `Beijing` and `Shanghai` are specified for the tag key.
      d. Select **Enforcement** and click **Specify Resource Types for Policy Enforcement**.
      e. In the **Specify Resource Types for Policy Enforcement** dialog box, read the risk warning and select I have read and fully understand the risks of enforcement. Then, select **instance** in the **Elastic Compute Service (ECS)** section.
      f. Click **OK**.
   v. Click **Create**.

3. Attach the tag policy.
   i. On the All Tag Policies tab of the Policy Library page, find the tag policy that is created in Step and click **Attach** in the **Actions** column.
   ii. In the **Attach** dialog box, select the object to which you want to attach the tag policy and click **OK**.

      You can attach the tag policy to one of the following objects. You can attach the tag policy to a member for testing. If the test is successful, you can attach the tag policy to the Root folder or a specific folder.

      - Root folder: If you attach the tag policy to the Root folder, the tag policy takes effect for all members in the resource directory.
      - Specific folder: If you attach the tag policy to a specific folder, the tag policy takes effect for all members in the folder and its subfolders.
      - Specific member: If you attach the tag policy to a specific member, the tag policy takes effect only for the member.

4. Check whether the tag policy is in effect.
   i. Access a member to which the tag policy is attached in Step .

      For more information, see Access a member.

ii. Create an ECS instance in the member to check whether the tag policy is in effect.

If you add the tag `CostCenter:Beijing` or `CostCenter:Shanghai` to the ECS instance when you create the ECS instance, the ECS instance will be created. If one of the following situations occur, the ECS instance will fail to be created:

- The case of the tag key or tag value that you enter when you add the tag to the ECS instance is inconsistent with that of the tag key or tag value defined in the tag policy. For example, you add the `costCenter:beijing` tag to the ECS instance.
- You specify only the tag key `CostCenter` and does not specify the tag value when you add the tag to the ECS instance.

> **Note** The system uses the tag policy to detect the compliance of the tag added to the ECS instance based on the tag key of the tag. In this example, the system starts the detection only if you add the tag key `CostCenter` to the ECS instance. After the detection is started, the system checks whether the tag key and tag value that you added to the ECS instance are compliant. For other situations, the system does not perform the detection. For example, no tags are added to the ECS instance, or a tag that has another tag key is added to the ECS instance.

Error code

Error code	Sample error message	Description
Forbidden.TagPolicy	The operation is failure, because the valid tag policy values of 'TagValue' are ["red","green","orange","blue","pink","white","black","grey"], but the value is "xxx".	The error message returned because the tag value is non-compliant and the resource fails to be created. Enter the tag value that is defined in the tag policy.
	The operation is failure, because the valid tag policy values of 'TagKey' are ["colorful"], but the value is "colorFul".	The error message returned because the case of the tag key is non-compliant and the resource fails to be created. Enter the tag key that is defined in the tag policy.

8.5. Enable automatic tag inheritance from a resource group

Resource Management provides the automatic tag inheritance feature. This feature allows resources that are added to or created in a resource group to automatically inherit the tags that are added to the resource group.

Context

- The automatic tag inheritance feature is available only when you use the Tag Policy feature that is in single-account mode.
- For more information about Alibaba Cloud services that support the automatic tag inheritance

feature, see the **Support for automatic tag inheritance from a resource group** column in the Alibaba Cloud services that support tag policies section in Alibaba Cloud services that support tag policies.

Procedure

This example shows how to enable resources such as Elastic Compute Service (ECS) instances in a resource group to automatically inherit the tag `env:test` that is added to the resource group.

1. Add a tag to a resource group.

   In this example, the tag `env:test` is used. For more information, see Add a tag to a resource group.

2. Enable the Tag Policy feature that is in single-account mode.

   For more information, see Enable the Tag Policy feature.

3. Create a tag policy.
   i. On the **Policy Library** page, click **Create Tag Policy**.
   ii. On the Create Tag Policy page, enter a name for the tag policy in the Policy Name field.
   iii. (Optional)Enter a description for the tag policy in the Policy Description field.
   iv. Configure policy information on the **Quick Mode** tab.
      a. Enter `env` in the **Tag Key** field.
      b. Select **Automatically Inherit Tags for Resources from Resource Groups** for Select Policy Scenario.
      c. Select **Specify Resource Groups** and click **Select Resource Groups**. In the Specify Resource Groups dialog box, select the resource group that is used in Step .

      > **Note** If you do not specify a resource group, automatic inheritance of the specified tag is enabled for all resource groups within the current Alibaba Cloud account. You can specify a maximum of 20 resource groups.

      d. (Optional)If you do not want some resources in the resource group to inherit the tag, select **Specify IDs of Resources to Be Excluded** and click **Specify Resource IDs**. In the Specify IDs of Resources to Be Excluded dialog box, enter the resource IDs that you want to exclude. Then, click OK.

      > **Note** You can specify a maximum of 20 resource IDs that you want to exclude.

   v. Click **Create**.

4. Attach the tag policy.
   i. On the Policy Library page, find the tag policy that you created in Step and click **Attach** in the **Actions** column.
   ii. In the **Attach** message, click **OK**.

      The tag policy takes effect for the current Alibaba Cloud account and RAM users within the account.

5. Check whether the tag policy is in effect.

   If the tag `env:test` is automatically added to the resources, such as ECS instances, in the

resource group, the tag policy is in effect. If other tags are added to the resource group but the tags are not defined in the tag policy, the resources in the resource group do not automatically inherit the tags.

> **Note** You must wait a period of time before a tag policy that is attached to an object takes effect. For more information, see Limits.

8.6. Basic operations

8.6.1. Enable the Tag Policy feature

You can use a tag policy only after you enable the Tag Policy feature.

Context

Modes of the Tag Policy feature

- Single-account mode: If your logon account is an independent Alibaba Cloud account, you can enable the Tag Policy feature that is in single-account mode to manage the resources within the account.

  > **Note** After a single account joins a resource directory, if you enable the Tag Policy feature for the resource directory, the tag policy that is attached to the single account becomes invalid. Invalid tag policies cannot be automatically recovered to valid tag policies.

- Multi-account mode: If your logon account is the management account of a resource directory, you can enable the Tag Policy feature that is in multi-account mode to manage resources within the resource directory.

  > **Note** You cannot enable the Tag Policy feature by using a member in a resource directory.

RAM permissions

You can use an Alibaba Cloud account or a RAM user within the Alibaba Cloud account to enable the Tag Policy feature. For security purposes, we recommend that you use a RAM user. To use a RAM user to enable the Tag Policy feature, you must grant the following permissions to the RAM user. For more information, see Create a custom policy and Grant permissions to a RAM user.

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
              "tag:GetConfigRuleReport",
              "tag:GenerateConfigRuleReport",
              "tag:GetEffectivePolicy",
              "tag:ListConfigRulesForTarget",
              "tag:ListPoliciesForTarget",
              "tag:ListTargetsForPolicy",
              "tag:ListPolicies",
              "tag:GetPolicy",
              "tag:GetPolicyEnableStatus",
              "tag:DetachPolicy",
              "tag:DeletePolicy",
              "tag:ModifyPolicy",
              "tag:AttachPolicy",
              "tag:CreatePolicy",
              "tag:DisablePolicyType",
              "tag:EnablePolicyType"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "rd:ListAccountsForParent",
                "rd:ListFoldersForParent",
                "rd:GetResourceDirectory",
                "config:GetAggregateResourceComplianceByConfigRule",
                "config:ListAggregateConfigRuleEvaluationResults",
                "config:GetAggregateConfigRulesReport",
                "config:GetResourceComplianceGroupByRegion",
                "config:ListConfigRuleEvaluationResults",
                "config:GetConfigRulesReport",
                "config:ListRemediations",
                "oos:ListExecutions"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag Policy > Policy Library**.
3. On the **Policy Library** page, click **Enable Tag Policy**.
4. In the **Enable Tag Policy** message, click **OK**.

When you enable the Tag Policy feature, the system creates the service-linked role AliyunServiceRoleForTag. This role can resolve cross-service access issues. For more information, see Service-linked role for Tag Policy.

8.6.2. Disable the Tag Policy feature

After you disable the Tag Policy feature, the attached tag policies are automatically detached.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag Policy > Policy Library**.
3. In the upper-right corner of the **Policy Library** page, click **Disable Tag Policy**.
4. In the **Disable Tag Policy** message, click **OK**.

8.6.3. Create a tag policy

You can create a tag policy and configure the policy document to ensure that compliant tags are added to your resources.

Single-account mode

1. Log on to the Resource Management console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Tag Policy > Policy Library**.
3. On the **Policy Library** page, click **Create Tag Policy**.
4. On the **Create Tag Policy** page, configure the parameters.
   i. Enter a policy name.
   ii. (Optional)Enter a policy description.
   iii. Configure the policy details.

   You can configure the policy details by using one of the following modes:

   - **Quick Mode** (recommended)

     In this mode, you need to enter a tag key and configure one or more rules that are described in the following table for the tag key based on your business requirements.

Scenario	Rule	Description
	Specify Allowed Tag Values	The tag values that are allowed for the tag key. You can use an asterisk (*) to indicate any tag values.

Scenario	Rule	Description
Add Tags with Specified Tag Values to Resources	Enforcement	If you enable the enforcement feature for a tag key, non-compliant operations on the tag key are forcefully stopped. You need to specify the resource types for enforcement. For more information about the Alibaba Cloud services and resource types that support the enforcement feature, see Enable tag policy enforcement. **Note** The enforcement feature is in invitational preview. You can contact the service manager of Alibaba Cloud to apply for a trial.
	Automatic Remediation	If you enable the automatic remediation feature, non-compliant tags of resources are automatically corrected. You need to specify compliant tag values and the resource scope for automatic remediation. You can specify the resource scope only by using tags.
Automatically Inherit Tags for Resources from Resource Groups	Specify Resource Groups	You can specify the resource groups from which resources in them inherit tags. If you do not specify resource groups, resources in all resource groups within the current account inherit tags. You can specify a maximum of 20 resource groups.
	Specify IDs of Resources to Be Excluded	You can specify the IDs of resources that do not inherit tags from the resource groups to which the resources belong. You can specify a maximum of 20 resource IDs.

You can click **Add Tag Key** to add tag keys and configure rules for the tag keys.

- **JSON**

  In this mode, you need to specify the policy details in the JSON format. You can use this mode if you have high requirements for tag policies. Before you use this mode, you must have a command of the syntax of a tag policy. For more information, see Syntax of a tag policy.

5. Click **Create**.

Multi-account mode

1. Log on to the Resource Management console by using the management account of a resource directory.
2. In the left-side navigation pane, choose **Tag Policy > Policy Library**.

3. On the **All Tag Policies** tab of the **Policy Library** page, click **Create Tag Policy**.
4. On the **Create Tag Policy** page, configure the parameters.
   i. Enter a policy name.
   ii. (Optional)Enter a policy description.
   iii. Configure the policy details.

   You can configure the policy details by using one of the following modes:

   - **Quick Mode** (recommended)

     In this mode, you need to enter a tag key and configure one or more rules that are described in the following table for the tag key based on your business requirements.

Rule	Description
Specify Allowed Tag Values	The tag values that are allowed for the tag key. You can use an asterisk (*) to indicate any tag values.
Enforcement	If you enable the enforcement feature for a tag key, non-compliant operations on the tag key are forcefully stopped. You need to specify the resource types for enforcement. For more information about the Alibaba Cloud services and resource types that support the enforcement feature, see Enable tag policy enforcement. For more information, see Enable tag policy enforcement. **Note** The enforcement feature is in invitational preview. You can contact the service manager of Alibaba Cloud to apply for a trial.
Automatic Remediation	If you enable the automatic remediation feature, non-compliant tags of resources are automatically corrected. You need to specify compliant tag values and the resource scope for automatic remediation. You can specify the resource scope only by using tags.

     You can click **Add Tag Key** to add tag keys and configure rules for the tag keys.

   - **JSON**

     In this mode, you need to specify the policy details in the JSON format. You can use this mode if you have high requirements for tag policies. Before you use this mode, you must have a command of the syntax of a tag policy. For more information, see Syntax of a tag policy.
5. Click **Create**.

8.6.4. Modify a tag policy

This topic describes how to modify a tag policy. You can modify the name, description, and details of the tag policy. After a tag policy is modified, the modification immediately takes effect for the object to which the tag policy is attached.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag Policy > Policy Library**.
3. In single-account mode, on the **Policy Library** page, find the tag policy that you want to modify and click **Modify** in the **Actions** column. In multi-account mode, on the **All Tag Policies** tab of the **Policy Library** page, find the tag policy that you want to modify and click **Modify** in the **Actions** column.
4. On the **Modify Tag Policy** page, modify the name, description, or details of the tag policy, and click **Submit**.

8.6.5. View the details of a tag policy

This topic describes how to view the details of a tag policy. The details include the basic information and document of the tag policy and the objects to which the tag policy is attached.

Single-account mode

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag Policy > Policy Library**.
3. On the **Policy Library** page, find the tag policy whose details you want to view and click the policy name.
   - In the **Basic Information** section, view the name and description of the tag policy.
   - On the **Document** tab of the Details section, view the document of the tag policy.
   - On the **Object Attachments** tab of the Details section, view the account to which the tag policy is attached.

Multi-account mode

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag Policy > Policy Library**.
3. On the **All Tag Policies** tab of the **Policy Library** page, find the tag policy whose details you want to view and click the policy name.
   - In the **Basic Information** section, view the name and description of the tag policy.
   - On the **Document** tab of the Details section, view the document of the tag policy.
   - On the **Object Attachments** tab of the Details section, view the folders or members to which the tag policy is attached.
4. On the **Attached Tag Policies** tab of the **Policy Library** page, click a folder or member in the resource directory on the left and view the tag policies that are attached to the folder or member.

8.6.6. Attach a tag policy

After you create a tag policy, you must attach the tag policy to an object. This way, you can manage the tags that are added to the resources in the object.

Single-account mode

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag Policy > Policy Library**.
3. On the **Policy Library** page, find the tag policy that you want to attach and click **Attach** in the **Actions** column.
4. In the **Attach** message, click **OK**.

   The tag policy is attached to the Alibaba Cloud account that you use for logon.

Multi-account mode

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag Policy > Policy Library**.
3. On the **Policy Library** page, click the **All Tag Policies** tab.
4. Find the tag policy that you want to attach and click **Attach** in the **Actions** column.
5. In the **Attach** dialog box, select the objects to which you want to attach the tag policy and click **OK**.

   The effective scope of the tag policy varies based on the object type.

   - Root folder: If you attach the tag policy to the Root folder, the tag policy takes effect for all members in the resource directory.
   - Specific folder: If you attach the tag policy to a specific folder, the tag policy takes effect only for all members in the folder.
   - Specific member: If you attach the tag policy to a specific member, the tag policy takes effect only for the member.

   > **Note** You cannot attach tag policies to the management account of a resource directory. Tag policies do not take effect for management accounts.

8.6.7. Detach a tag policy

You can detach a tag policy from an object based on your business requirements. After you detach a tag policy from an object, the tag policy no longer takes effect for the object.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag Policy > Policy Library**.
3. In single-account mode, on the **Policy Library** page, find the tag policy that you want to detach and click **Detach** in the **Actions** column. In multi-account mode, on the **All Tag Policies** tab of the **Policy Library** page, find the tag policy that you want to detach and click **Detach** in the **Actions** column.
4. In the **Detach** dialog box, select the object from which you want to detach the tag policy and click **OK**.

8.6.8. Delete a tag policy

If you no longer require a tag policy, you can delete the tag policy. You cannot recover tag policies that are deleted.

Prerequisites

The tag policy is detached from all objects to which the tag policy is attached. For more information about how to detach a tag policy from an object, see Detach a tag policy.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag Policy > Policy Library**.
3. In single-account mode, on the **Policy Library** page, find the tag policy that you want to delete and click **Delete** in the **Actions** column. In multi-account mode, on the **All Tag Policies** tab of the **Policy Library** page, find the tag policy that you want to delete and click **Delete** in the **Actions** column.
4. In the **Delete** message, click **OK**.

8.6.9. View the effective policies

In single-account mode, you can use an Alibaba Cloud account to view the effective policy that is attached to the account. In multi-account mode, you can use the management account of a resource directory to view the effective policies that are attached to the Root folder, a specific folder, or a specific member. You can also use a member to view the effective policies that are attached to the member. The effective policies are obtained based on tag policy inheritance.

Context

For information about tag policy inheritance and the calculation of effective policies, see Inheritance of a tag policy and calculation of an effective policy.

Procedure

1. Log on to the Resource Management console. The Tags page appears.
2. In the left-side navigation pane, choose **Tag Policies > Effective Policies**.
3. View the document of an effective policy.

   You can view the document of an effective policy in visualized mode or display the document in the JSON format. By default, View in Visualized Mode is used. You can switch from View in Visualized Mode to **View in JSON Format**.

8.6.10. View and download non-compliance detection results

After you attach a tag policy to an account, the system automatically checks whether the tags added to the resources of the account are compliant with the tag policy. This helps you identify non-compliant resources in a timely manner.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag Policy > Detection Results**.
3. On the **Detection Results** page, view the non-compliance detection results of resources.

   You can click the name of an account to view the detection details, including the total number of resources of the account, the number of non-compliant resources, the percentage of non-compliant resources, and the non-compliant resources.
4. In the **Non-compliance Reports** section, generate a non-compliance report and download the report.
   i. Click **Generate Latest Non-compliance Report**.
   ii. After the non-compliance report is generated, click **Download Report** to download the report in the Excel format.

8.7. Inheritance of a tag policy and calculation of an effective policy

This topic describes the definitions of policy inheritance and an effective policy, the inheritance logic of a tag policy, and the calculation method of an effective policy. This topic also provides examples on how to enable the inheritance of a tag policy and how to obtain an effective policy.

Terms

Term	Description
policy inheritance	A tag policy is inherited by subfolders from parent folders based on the folder levels in a resource directory. If you attach a tag policy to a folder in a resource directory, members in the folder and its subfolders will inherit the tag policy.
parent policy	A parent policy is a policy attached to a higher-level object in a resource directory.
child policy	A child policy is a policy attached to a lower-level object in a resource directory.
effective policy	An effective policy is obtained by aggregating the tag policy that is attached to a member and the tag policy that is inherited by the member. The effective policy is the policy that is actually executed on the member.
inheritance operator	An inheritance operator is used to aggregate the tag policy that is attached to a member and the tag policy that is inherited by the member. For more information, see Inheritance operators.

How a tag policy is inherited and how an effective policy is obtained

- Tag Policy in single-account mode

In single-account mode, if you attach multiple tag policies to an account, the tag policies are aggregated based on the tag keys defined in the tag policies. If the tag keys defined in the tag policies conflict with each other, the tag policy that is first attached is used as the effective policy for the account.

- Tag Policy in multi-account mode

  In multi-account mode, you can use the management account of a resource directory to attach a tag policy to one of the following objects:

  - Root folder: If the tag policy is attached to the Root folder, all members within the resource directory inherit the tag policy.
  - Specific folder: If the tag policy is attached to a specific folder, all members in the folder and its subfolders inherit the tag policy.
  - Specific member: If the tag policy is attached to a specific member, the tag policy takes effect only for the member.

Example

In this example, the environment tag whose tag key is `env` and the project tag whose tag key is `Project` must be added to the resources of an enterprise. This example shows the inheritance logic of a tag policy and the calculation method of an effective policy.

1. Attach a tag policy named PolicyA to the Root folder of the resource directory.

   The following code provides the document of PolicyA:

```
{
    "tags": {
        "env": {
            "tag_key": {
                "@@assign": "env"
            },
              "tag_value": {
                "@@assign": [
                    "Production",
                    "Test"
                ]
            }
        },
        "Project": {
            "tag_key": {
                "@@assign": "Project"
            }
        }
    }
}
```

   PolicyA defines the regulations for the tag keys `env` and `Project` and is attached to the Root folder of the resource directory. After PolicyA is attached to the Root folder, the following situations occur:

   PolicyA takes effect for all members within the resource directory. This indicates that compliant tags whose tag keys are `env` and `Project` must be added to all resources in the members. The valid tag values of the tag key `env` are `Production` and `Test`.

2. Attach a tag policy named PolicyB to a specific member in the Root folder.

   The following code provides the document of PolicyB:

```
{
    "tags": {
        "env": {
            "tag_value": {
                "@@append": [
                    "Development"
                ]
            }
        },
        "Project": {
            "tag_value": {
                "@@assign": [
                    "A",
                    "B"
                ]
            }
        }
    }
}
```

   PolicyB defines that `Development` is added as a tag value for the tag key `env` and the valid tag values of the tag key `Project` are `A` and `B`.

3. Calculate an effective policy for a specific member.

   PolicyB is attached to a specific member, and the member inherits PolicyA. In this case, the effective policy for the member is obtained by aggregating PolicyA and PolicyB. This indicates that the tag values defined in PolicyA and PolicyB are compliant. The following table lists the valid tag values of the tag keys env and Project.

Tag key	Tag value
`env`	○ `Production` ○ `Test` ○ `Development`
`Project`	○ `A` ○ `B`

   The following code provides the document of the effective policy:

```
{
    "tags": {
        "env": {
            "tag_value":  [
                   "Production",
                   "Test",
                   "Development"
               ] ,
             "tag_key": "env"
        },
        "Project": {
            "tag_value":  [
                   "A",
                   "B"
               ],
             "tag_key": "Project"
        }
    }
}
```

8.8. Syntax of a tag policy

This topic describes the syntax of a tag policy and the supported inheritance operators.

Syntax

Tag policies support the JSON format and follow the standard JSON syntax. In this example, a simple tag policy is used to describe the syntax of a tag policy. The following code provides the document of the tag policy:

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "*"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "ecs:instance"
                ]
            }
        },
        "owner": {
            "tag_key": {
                "@@assign": "owner"
            },
            "tag_value": {
                "@@assign": [
                    "*"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "ecs:instance"
                ]
            }
        }
    }
}
```

The preceding tag policy defines that the cost center tag whose tag key is `CostCenter` and the resource owner tag whose tag key is `owner` must be added to all Elastic Compute Service (ECS) instances. The following table describes the elements contained in a tag policy.

Element	Description	Required
Tag	The document of a tag policy starts with `tags`.	Yes
Policy key	A policy key is the unique identifier of a statement in a tag policy. Policy keys are case-sensitive. You can specify multiple policy keys in a tag policy. Policy keys are the same as tag keys. In this example, the policy keys are `CostCenter` and `owner`.	Yes

Element	Description	Required
Tag key	Tag keys are specified by `tag_key` and are case-sensitive. In this example, the tag keys are `CostCenter` and `owner`.	Yes
Tag value	Tag values are specified by `tag_value`. If `tag_value` is not configured, tags added to resources can have any tag values or no tag values. You can also set tag_value to an asterisk (*), which indicates any tag values. In this example, `tag_value` is set to `*`. This indicates that any tag values can be used when you add the cost center tag whose tag key is `CostCenter` and the resource owner tag whose tag key is `owner` to all ECS instances.	No
Enforcement	You can configure `enforced_for` to enforce a tag policy. The enforcement of a tag policy can prevent non-compliant tags from being added to resources. In this example, the tag policy is enforced when an ECS instance is created. The tags whose tag keys are `CostCenter` and `owner` must be added to the ECS instance when the ECS instance is created. Otherwise, the ECS instance fails to be created.	No
Inheritance operator	An inheritance operator is used to aggregate the tag policy that is attached to an object and the tag policy that is inherited by the object to obtain an effective policy for the object. For more information about inheritance operators, see Inheritance operators. In this example, the inheritance operator `@@assign` is used for `tag_key`, `tag_value`, and `enforced_for`.	Yes

Inheritance operators

An inheritance operator is used to aggregate the tag policy that is attached to an object and the tag policy that is inherited by the object to obtain an effective policy for the object. Inheritance operators are classified into value-setting operators and child control operators.

> **Note** If you configure a tag policy on the **Quick Mode** tab in the Resource Management console, you can use only the `@@assign` operator. This operator is a basic operator. If you configure a tag policy on the **JSON** tab in the Resource Management console, you can use all operators described in this section. Operators other than @@assign are advanced operators.

- **Value-setting operators**

Operator	Description
`@@assign`	This operator indicates the overwrite operation. If you specify this operator for a setting in a tag policy attached to an object, and the setting conflicts with the related setting in the tag policy inherited by the object, the setting in the attached tag policy overwrites the related setting in the inherited tag policy.
`@@append`	This operator indicates the append operation. If you specify this operator for a setting in a tag policy attached to an object, the setting is appended to the tag policy inherited by the object. You can use this operator only when you specify multiple tag values for a tag key in a tag policy attached to an object.
`@@remove`	This operator indicates the remove operation. If you specify this operator for a setting in a tag policy attached to an object, the related setting is removed from the tag policy inherited by the object. You can use this operator only when you specify multiple tag values for a tag key in a tag policy attached to an object.

- **Child control operators**

  Child control operators are advanced operators. You can use child control operators if you want to control which value-setting operators can be used in child policies. By default, all value-setting operators are allowed in child policies.

Operator	Description
`"@@operators_allowed_for_child_policies":["@@all"]`	If you specify this operator in a tag policy attached to a folder, you can use any value-setting operator in the policies attached to the subfolders of the folder and members in the folder. By default, if no child control operator is specified in a parent policy, all value-setting operators are allowed in child policies.
`"@@operators_allowed_for_child_policies":["@@assign"`	If you specify this operator in a tag policy attached to a folder, you can use the value-setting operator @@assign in the policies attached to the subfolders of the folder and members in the folder. You can specify one or more value-setting operators in this operator.
`"@@operators_allowed_for_child_policies":["@@none"]`	If you specify this operator in a tag policy attached to a folder, value-setting operators cannot be used in the policies attached to the subfolders of the folder and members in the folder. You can use this operator to lock the settings that are defined in a parent policy. This way, child policies do not take effect when you calculate an effective policy, and the parent policy is used as an effective policy.

8.9. Service-linked role for Tag Policy

This topic describes the usage scenarios and the permission policy of the service-linked role AliyunServiceRoleForTag for the Tag Policy service. This topic also describes how to create and delete the service-linked role.

Scenarios

The Tag service uses the service-linked role AliyunServiceRoleForTag to access operation records and resources in ActionTrail and Cloud Config. This way, the Tag service monitors resource changes in real time and checks the compliance of resource configurations to determine the tag compliance of resources.

For more information, see Service-linked roles.

Role description

Service name: tag.aliyuncs.com.

Role name: AliyunServiceRoleForTag.

Permission policy: AliyunServiceRolePolicyForTag.

Permission description: This permission policy allows the Tag service to access ActionTrail and Cloud Config, and create and delete the service-linked role for the Tag Policy service.

```
{
 "Version": "1",
 "Statement": [
   {
     "Action": [
       "actiontrail:CreateServiceTrail",
       "actiontrail:DeleteServiceTrail",
       "actiontrail:ListServiceTrail"
     ],
     "Resource": "*",
     "Effect": "Allow"
   },
   {
     "Action": "ram:DeleteServiceLinkedRole",
     "Resource": "*",
     "Effect": "Allow",
     "Condition": {
       "StringEquals": {
         "ram:ServiceName": "tag.aliyuncs.com"
       }
     }
   },
   {
     "Action": [
       "config:StartConfigurationRecorder",
       "config:DescribeConfigurationRecorder",
       "config:CreateConfigRule",
       "config:DeleteConfigRules",
       "config:UpdateConfigRule",
       "config:ListConfigRules",
       "config:GetConfigRule",
       "config:CreateAggregateConfigRule",
       "config:DeleteAggregateConfigRules",
       "config:ListAggregateConfigRules",
       "config:GetAggregateConfigRule",
       "config:UpdateAggregateConfigRule",
       "config:ListAggregators"
```

```
          "config:ListAggregators",
          "config:CreateAggregator",
          "config:GetConfigRulesReport",
          "config:GenerateConfigRulesReport",
          "config:CreateRemediation",
          "config:CreateAggregateRemediation"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Condition": {
          "StringEquals": {
            "config:ServiceChannel": "TagPolicy"
          }
        }
      },
      {
        "Action": "ram:CreateServiceLinkedRole",
        "Resource": "*",
        "Effect": "Allow",
        "Condition": {
          "StringEquals": {
            "ram:ServiceName": [
              "config.aliyuncs.com",
              "remediation.config.aliyuncs.com"
            ]
          }
        }
      }
    ]
}
```

Create the service-linked role for the Tag Policy service

After you enable a tag policy, the system creates the service-linked role for the Tag Policy service. For more information, see Enable the Tag Policy feature.

Delete the service-linked role for the Tag Policy service

You cannot delete the service-linked role after the role is created. To delete the service-linked role, submit a ticket.

9.Use tags to implement automated O&M

9.1. Overview

After you bind tags to resources, you can use Operation Orchestration Service (OOS) to implement automated operations and maintenance (O&M) by tag.

Scenarios

Enterprises have an increasing number of cloud resources. O&M is important to these resources. However, manual O&M cannot meet the requirements of enterprises. You can use OOS to implement automated O&M. OOS provides the best practices of operations as code. This allows you to create templates from manuals such as O&M guides, user guides and operation guides. Before you use OOS to implement automated O&M, you must use tags to categorize your resources from different dimensions. This way, OOS can identify the resources by tag during O&M. Therefore, the combination of the Tag service and OOS provides an optimal O&M solution for enterprises.

Benefits

- You can perform automated O&M on multiple objects at a time. For example, you can start, stop, or restart multiple Elastic Compute Service (ECS) instances at a time.
- You can manage multiple tags at a time. For example, you can bind or modify multiple tags at a time.
- You can use tags as a basis to implement operation orchestration from different dimensions. If you do not want to implement automated O&M for a resource, you do not need to modify the script for the orchestration task. You only need to modify the tags bound to the resource in the Resource Management console.

Procedure

1. Use tags of different business dimensions to identify resources for centralized management.
2. Create a template in OOS and execute the template to implement automated O&M.

Best practices

The following topics describe the best practices of using OOS to implement automated O&M by tag:

- Use OOS to start multiple ECS instances with specific tags at a time
- Use OOS to add tags to multiple resources
- Use OOS to modify a tag value of multiple resources

9.2. Use OOS to add tags to multiple resources

You can use an Operation Orchestration Service (OOS) custom template to add tags to multiple resources in the same region at a time. Then, you can manage permissions on these resources based on the tags.

Context

You can add tags to Alibaba Cloud services that support tags. For more information about the services that support tags, see Services that work with Tag.

In this topic, a custom template is created in OOS to add the `owner:zhangsan` tag to multiple Elastic Compute Service (ECS) instances in the same region.

> **Note** The resources to which tags will be added must reside in the same region.

Step 1: Create a RAM role and attach permission policies to it

Create a RAM role named OOSServiceRole for OOS and attach permission policies to the role.

1. Log on to the RAM console by using an Alibaba Cloud account.
2. Create a custom policy named OOSAutoBindTag.

   For more information, see Create a custom policy.

   > **Note** This policy is used for ECS instances, and the permission in the policy is set to `ecs:DescribeInstances`. You can set the permission based on your business requirements. For example, you want to add a tag to multiple security groups. In this case, you can replace `ecs:DescribeInstances` with `ecs:DescribeSecurityGroups`.

   The following policy is created:

   ```
   {
       "Version": "1",
       "Statement": [
           {
               "Action": [
                   "ecs:DescribeInstances",
                   "ecs:TagResources"
               ],
               "Resource": "*",
               "Effect": "Allow"
           }
       ]
   }
   ```

3. Create the OOSServiceRole RAM role.

   For more information, see Create a normal service role.
4. Attach the custom policy OOSAutoBindTag to the RAM role.

   For more information, see Grant permissions to a RAM role.
5. Attach the system policy AliyunOOSFullAccess to the RAM role.

   For more information, see Grant permissions to a RAM role.

Step 2: Add a tag to multiple resources at a time

1. Log on to the OOS console.
2. In the left-side navigation pane, click **My Templates**.

3. In the top navigation bar, select a region.
4. Create a custom template.
   i. On the My Templates page, click **Create Template**.
   ii. In the **Basic Information** section, enter a name for your template, such as OOSAutoBindTag.
   iii. Click the **YAML** tab and write code for the template. Then, click **Create Template**.

   The following code provides an example:

```
FormatVersion: OOS-2019-06-01
Description: Tag Resources Without The Specified Tags
Parameters:
  tags:
    Type: Json
    Description:
      en: The tags to select ECS instances.
    AssociationProperty: Tags
  regionId:
    Type: String
    Description:
      en: The region to select ECS instances.
  OOSAssumeRole:
    Description:
      en: The RAM role to be assumed by OOS.
    Type: String
    Default: OOSServiceRole
RamRole: OOSServiceRole
Tasks:
  - Name: getInstancesByTags
    Action: 'ACS::ExecuteAPI'
    Description: ''
    Properties:
      Service: ECS
      API: DescribeInstances
      Parameters:
        Tags: '{{ tags }}'
        RegionId: '{{ regionId }}'
    Outputs:
      InstanceIds:
        Type: List
        ValueSelector: 'Instances.Instance[].InstanceId'
  - Name: getAllInstances
    Action: 'ACS::ExecuteAPI'
    Description: ''
    Properties:
      Service: ECS
      API: DescribeInstances
      Parameters:
        RegionId: '{{regionId}}'
    Outputs:
      InstanceIds:
        Type: List
        ValueSelector: 'Instances.Instance[].InstanceId'
  - Name: TagResources_ECS_Instances
```

```
    Action: 'ACS::ExecuteAPI'
    Description:
      en: 'tag ecs instances, which are without the specified tags.'
    Properties:
      Service: ECS
      API: TagResources
      Parameters:
        Tags: '{{ tags }}'
        RegionId: '{{regionId}}'
        ResourceType: Instance
        ResourceIds:
          - '{{ACS::TaskLoopItem}}'
    Loop:
      MaxErrors: 100%
      Concurrency: 20
      Items:
        'Fn::Difference':
          - '{{ getAllInstances.InstanceIds }}'
          - '{{ getInstancesByTags.InstanceIds }}'
Outputs:
  InstanceIds:
    Type: List
    Value:
      'Fn::Difference':
        - '{{ getAllInstances.InstanceIds }}'
        - '{{ getInstancesByTags.InstanceIds }}'
```

Parameters:

- tags: the tags that are added to ECS instances
- regionId: the region ID of the ECS instances to which you want to add a tag
- OOSAssumeRole: the RAM role used by OOS

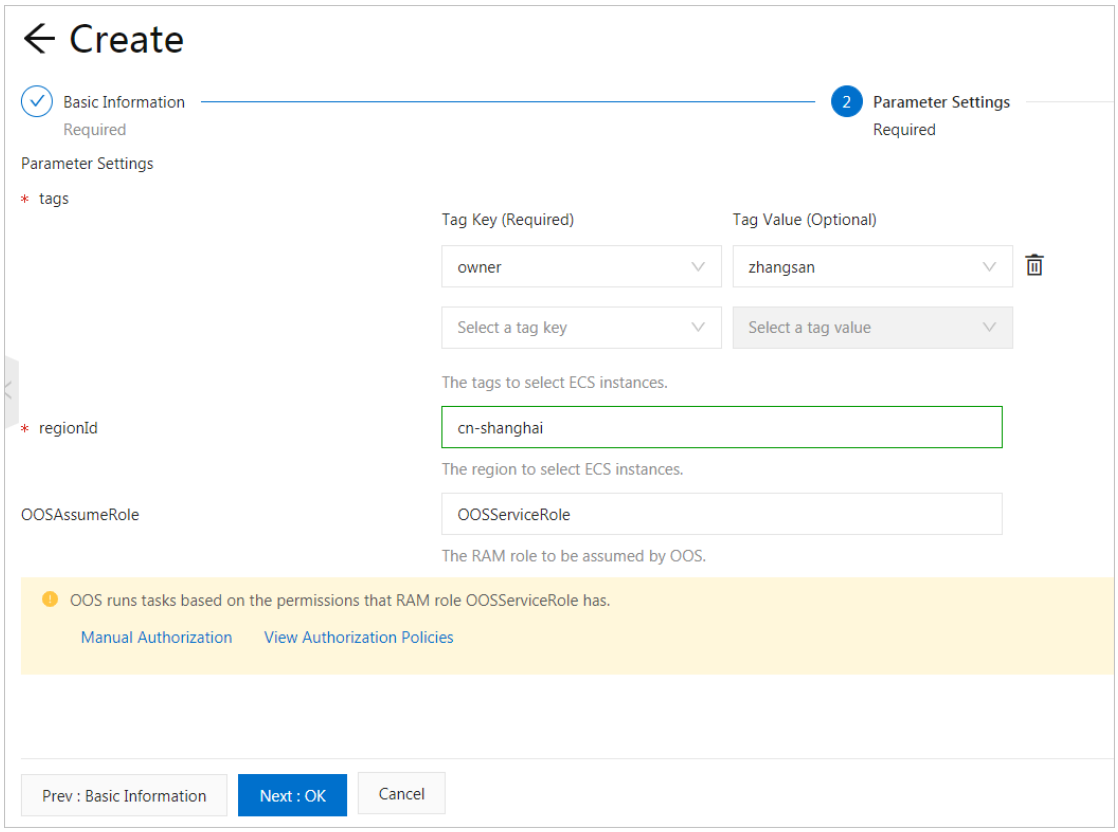
Permissions:

- DescribeInstances: filters resources based on tags.
- TagResources: adds tags to specified resources.

5. Execute the custom template.
   i. In the left-side navigation pane, click **My Templates**. On the My Templates page, find the OOSAutoBindTag custom template that you created, and click **Create Execution** in the **Actions** column.
   ii. Keep the default settings or re-select the execution mode, and click **Next: Parameters Settings**.

iii. In the Parameter Settings step, configure the parameters and click **Next: OK**.

The following parameters are configured in this example:



- tags: Select the tag `owner:zhangsan`.
- regionId: Enter the region ID of the instances, such as `cn-shanghai`.
- oosAssumeRole: Use the OOSServiceRole RAM role.

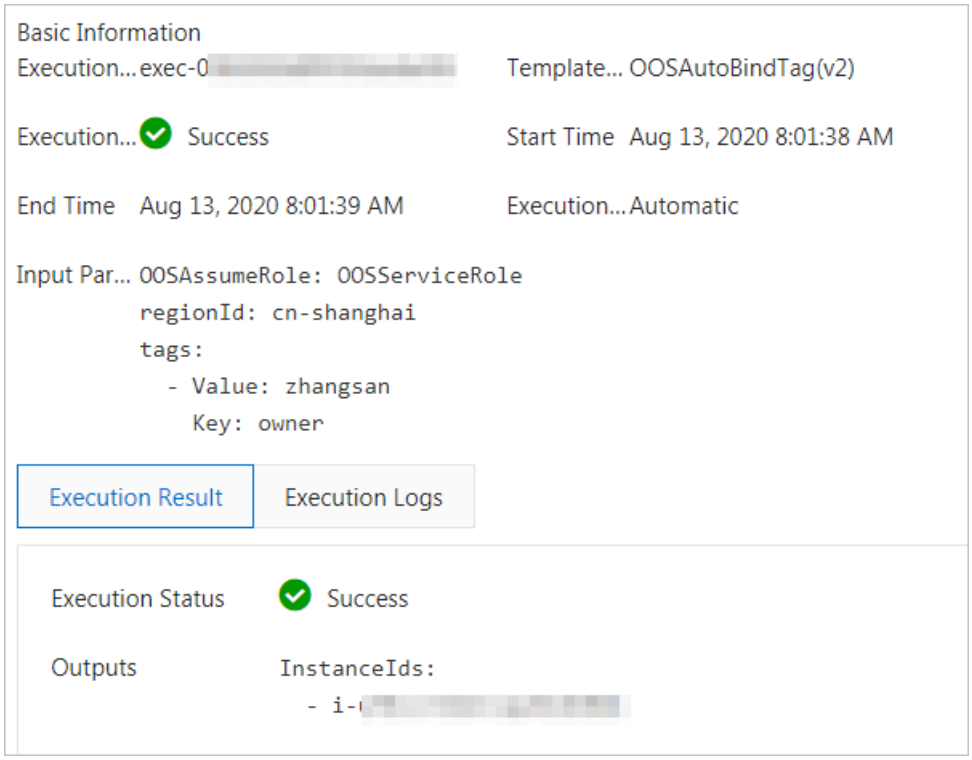
iv. Click **Create**.

v. On the execution details page, click the **Advanced View** tab.

vi. Click the **Execution Result** tab on the right side of the page.

vii. View the execution result.

- If the execution succeeds, the information shown in the following figure appears.



- If the execution fails, you can check logs for the failure cause and make adjustments.

9.3. Use OOS to modify a tag value of multiple resources

This topic describes how to use an Operation Orchestration Service (OOS) custom template to modify a tag value of multiple resources in the same region at a time.

Prerequisites

A tag is added to your Elastic Compute Service (ECS) instances. For more information, see Add a custom tag.

Context

In this topic, a custom template is created in OOS to modify a tag value of multiple ECS instances at a time. In this example, a tag value of the ECS instances is changed from OldTagValue to NewTagValue. The related tag key-value pair is changed from `TagKey:OldTagValue` to `TagKey:NewTagValue`.

> **Note**
>
> - You can use an OOS custom template to modify a tag value for a maximum of 1,000 resources at a time. If the number of resources is greater than 1,000, you must execute the template multiple times.
> - You can use an OOS custom template to modify the tag values of resources that support tags in the same region. You can modify the related API operations in the template to apply them to various resources. For more information about resources that support tags, see Services that work with Tag. For more information about the resources that are supported by OOS, see List of supported cloud services.

Step 1: Create an OOS custom template

You can perform the following steps to create an OOS custom template that is used to modify a tag value of multiple resources at a time.

1. Log on to the OOS console.
2. In the left-side navigation pane, click **My Templates**.
3. In the top navigation bar, select a region.
4. Click **Create Template**.
5. In the **Basic Information** section, enter a name for your template.
6. Click the **JSON** tab and write code for the template.

   The following code provides an example:

```
{
    "Description": "Modify a tag value of multiple resources at a time",
    "FormatVersion": "OOS-2019-06-01",
    "Parameters": {
        "operateId": {
            "Description": "Define the operation ID",
            "Type": "String",
            "MinLength": 1,
            "MaxLength": 64
        },
        "tagKey": {
            "Description": "Current tag key",
            "Type": "String",
            "MinLength": 1,
            "MaxLength": 64
        },
        "tagValue": {
            "Description": "Current tag value",
            "Type": "String",
            "MinLength": 1,
            "MaxLength": 64
        },
        "newTagValue": {
            "Description": "New tag value",
            "Type": "String",
            "MinLength": 1,
            "MaxLength": 64
```

```
            "MaxLength": 64
        }
    },
    "Tasks": [
        {
            "Name": "DescribeInstances_ECS",
            "Action": "ACS::ExecuteAPI",
            "Description": {
                "en": "filter ecs instances by tags"
            },
            "Properties": {
                "Service": "ECS",
                "API": "DescribeInstances",
                "AutoPaging": true,
                "Parameters": {
                    "Tags": [
                        {
                            "Key": "{{ tagKey }}",
                            "Value": "{{ tagValue }}"
                        }
                    ]
                }
            },
            "Outputs": {
                "Instances": {
                    "Type": "List",
                    "ValueSelector": "Instances.Instance[].InstanceId"
                }
            }
        },
        {
            "Name": "TagResources_ECS_Instances",
            "Action": "ACS::ExecuteAPI",
            "Description": {
                "en": "tag ecs instances"
            },
            "Properties": {
                "Service": "ECS",
                "API": "TagResources",
                "Parameters": {
                    "Tags": [
                        {
                            "Key": "{{ tagKey }}",
                            "Value": "{{ newTagValue }}"
                        }
                    ],
                    "ResourceType": "Instance",
                    "ResourceIds": [
                        "{{ACS::TaskLoopItem}}"
                    ]
                }
            },
            "Loop": {
                "MaxErrors": "100%",
                "Concurrency": 20,
```

```
                "Items": "{{DescribeInstances_ECS.Instances}}"
            }
        }
    ],
    "Outputs": {}
}
```

7. Click **Create Template**.

Step 2: Execute the custom template

You can perform the following steps to execute the template created in Step 1: Create an OOS custom template to modify a tag value of multiple resources.

1. In the left-side navigation pane, click **My Templates**.
2. Find the template created in Step 1: Create an OOS custom template and click **Create Execution** in the **Actions** column.
3. On the Create page, specify **Execution Description** and **Execution Mode** in the Basic Information step. Then, click **Next: Parameter Settings**.
4. In the Parameter Settings step, configure the parameters and click **Next: OK**.

   You must configure the following parameters in this step:

   - operateId: the operation ID, which is used to identify an operation. You can specify this parameter based on your requirements.
   - tagKey: the current tag key. In this example, the current tag key is `TagKey`.
   - tagValue: the current tag value. In this example, the current tag value is `OldTagValue`.
   - newTagValue: the new tag value. In this example, the new tag value is `NewTagValue`.
5. Click **Create**.

   The execution details page appears. You can view the execution results on this page.

   > **Note** If the execution fails, you can check logs for the failure cause and make adjustments.

9.4. Use OOS to start multiple ECS instances with specific tags at a time

A key link for enterprises to implement automated O&M is to quickly find multiple resources on which you want to perform O&M at a time. This can be achieved by using resource tags and Operation Orchestration Service (OOS). This topic describes how to use OOS to start multiple Elastic Compute Service (ECS) instances with specific tags at a time.

Step 1: Add tags to ECS instances

In the ECS console or on the Tag page of the Resource Management console, add the `business:bigdata` tag to ECS instances. In this section, the Tag page of the Resource Management console is used.

1. Log on to the Resource Management console.

2. In the left-side navigation pane, choose **Tag > Tag**.
3. In the top navigation bar, select a region.
4. On the **Custom Tags** tab, click **Create Custom Tags**.
5. In the **Create Custom Tags** dialog box, add the `business:bigdata` tag to existing ECS instances.

   For more information, see Add a custom tag.

Step 2: Start multiple ECS instances with specific tags at a time in the OOS console

Execute the ACS-ECS-BulkyStartInstances public template in the OOS console. In this step, set the template execution object to ECS instances to which the `business:bigdata` tag is added.

1. Log on to the OOS console.
2. In the left-side navigation pane, click **Public Templates**.
3. In the top navigation bar, select a region.

   > **Note** By default, OOS deployed in a region can be used to manage resources only in that region. For example, OOS deployed in the China (Hangzhou) region can be used to manage ECS instances only in this region. However, OOS provides a method to manage resources deployed in other regions. If you want to call API operations in other regions, specify the region ID in the ACS::ExecuteAPI action. We recommend that you do not use this method. Make sure that the region of OOS is the same as that of the ECS instances that are specified in Step 1: Add tags to ECS instances.

4. On the **Public Templates** page, find **ACS-ECS-BulkyStartInstances** and click **Create Execution**.
5. On the **Create** page, perform the following operations:
   i. In the **Basic Information** step, keep the default values and click **Next: Parameter Settings**.

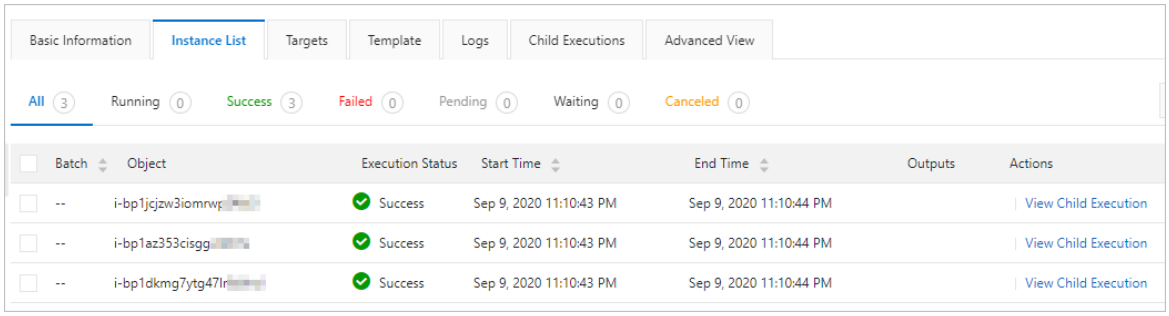
      The default value of Execution Mode is **Automatic**. This indicates that all tasks in the template will automatically run.

   ii. In the Parameter Settings step, set **targets** to **Specify Instance Tags**. Select `business` from the Tag Key drop-down list and select `bigdata` from the Tag Value drop-down list. Set **Permissions** to **Use Existing Permissions of Current Account**. Keep the default values for other parameters.

   iii. Click **Next: OK**.

   iv. Confirm the settings and click **Create**.
6. On the **Instance List** tab of the page that appears, view execution results.

   All ECS instances to which the `business:bigdata` tag is added are started.



9.5. Use tags to enable ECS instances to be automatically added to CloudMonitor application groups

You can create scaling groups in Auto Scaling and use these scaling groups to automatically create instances with specific tags. Then, you can configure application group rules in CloudMonitor based on the tags. This way, the instances are automatically added to different application groups based on the rules. This facilitates centralized O&M of the instances. This strategy has the following characteristics: automatic addition of instances to application groups, high availability of auto scaling, and automated O&M.

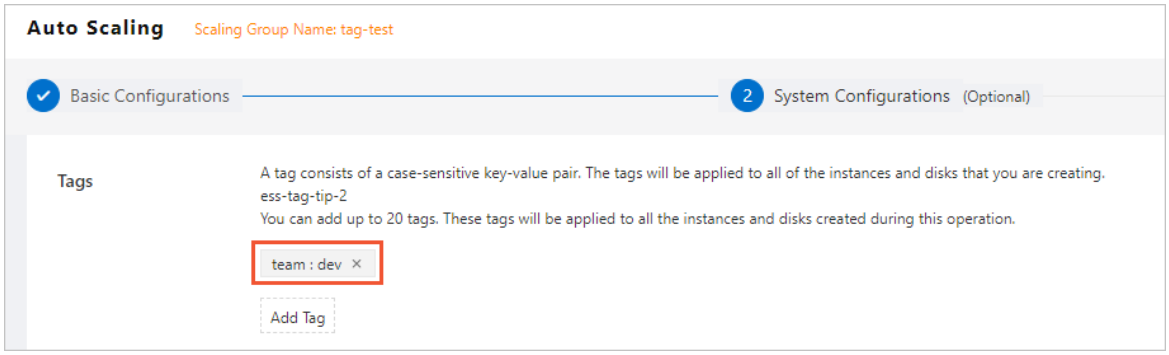
Context

- CloudMonitor can automatically group the resources of the following Alibaba Cloud services: Elastic Compute Service (ECS), ApsaraDB RDS, and Server Load Balancer (SLB). For ECS, only instances can be grouped. Other ECS resources, such as network interface controllers (NICs) and disks, cannot be grouped.
- In this topic, an ECS instance that is automatically created in a scaling group is used. The tag `team:dev` is added to the ECS instance.

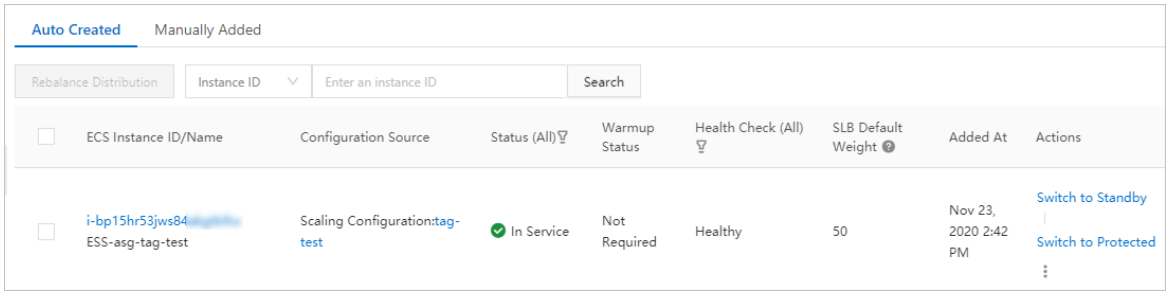
Step 1: Create an ECS instance to which a tag is added in Auto Scaling

1.
2. Create a scaling group. For more information, see Create a scaling group.

   Specify **Balanced Distribution Policy** for the Scaling Policy parameter based on your business requirements to achieve high-availability auto scaling.
3. Create a scaling configuration, create an ECS instance, and then add the `team:dev` tag to the ECS instance. For more information, see Create a scaling configuration (ECS).



4. On the Scaling Groups page, find the scaling group that you created and click its ID. On the page that appears, click the **Instances** tab. On the Instances tab, view the ECS instance that is automatically created in the scaling group.

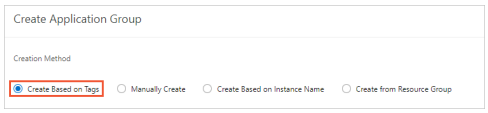


Step 2: Create a CloudMonitor application group

1. Log on to the CloudMonitor console.
2. Create an application group. For more information, see Create an application group.

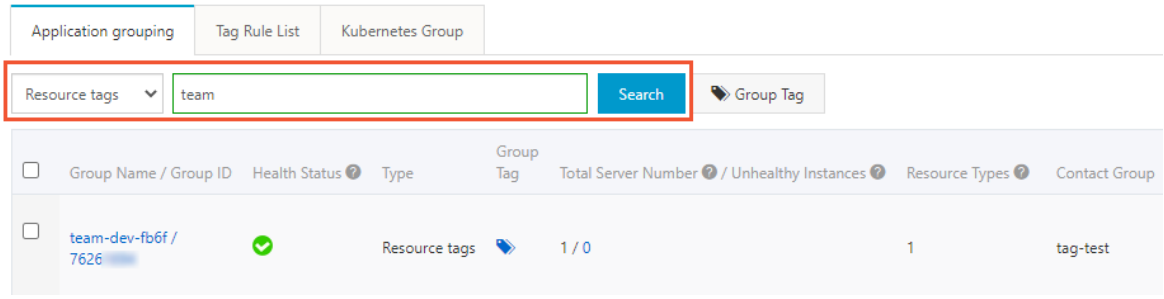
   You must specify Creation method and Match Rule based on the following instructions:

   - Creation method: Select **Smart tag synchronization creation**.

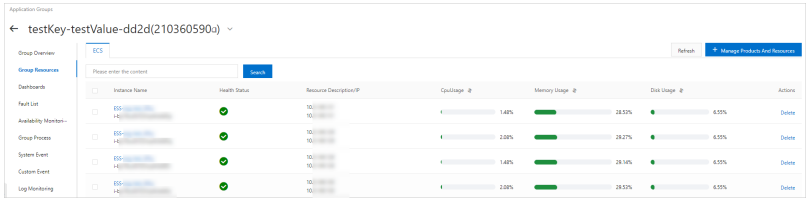


   - Match Rule: Set Resource Tag Key to `team` and specify Tag Value based on your business requirements. In this example, **Contain** and `dev` are specified.

3. On the Application grouping tab of the Application Groups page, select **Resource tags** and enter the tag key `team` in the search box to search for the newly created application group.



4. Click the name of the application group and view the resources in the group.
   The ECS instance that is automatically created in the scaling group is automatically added to the application group.



You can also view the monitoring data of the ECS instance. For more information, see Overview.

10.Use tags to control access to resources

10.1. Create a resource with a specific tag

You can attach a custom policy to a Resource Access Management (RAM) user. This allows the RAM user to add specific tags to the Elastic Compute Service (ECS) resources that the RAM user wants to create. Otherwise, the ECS resources cannot be created. The combination of tags and RAM users allows different RAM users to have different access and operation permissions on cloud resources based on tags.

Prerequisites

A RAM user is created in your Alibaba Cloud account. For more information, see Create a RAM user.

Step 1: Create a custom policy and attach the policy to a RAM user

In this step, the BindTagForRes custom policy is attached to the userTest RAM user. When the RAM user creates an ECS resource, the RAM user must add a specific tag to the resource and select a virtual private cloud (VPC) to which a specific tag is added. In this example, the `user:lisi` tag is added to the VPC, and the `owner:zhangsan` tag is added to the ECS resource.

1. Log on to the RAM console by using an Alibaba Cloud account.
2. Create the BindTagForRes custom policy. For more information, see Create a custom policy.

   Policy document:

```
{
    "Statement": [
        {
           "Effect": "Allow",
            "Action": "ecs:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:tag/owner": "zhangsan"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ecs:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "vpc:tag/user": "lisi"
                }
            }
        },
```

```
        {
            "Action": [
                "ecs:DescribeTagKeys",
                "ecs:ListTagResources",
                "ecs:DescribeTags",
                "ecs:DescribeKeyPairs",
                "ecs:DescribeImages",
                "ecs:DescribeSecurityGroups",
                "ecs:DescribeLaunchTemplates",
                "ecs:DescribeDedicatedHosts",
                "ecs:DescribeDedicatedHostTypes",
                "ecs:DescribeAutoSnapshotPolicyEx",
                "vpc:DescribeVpcs",
                "vpc:DescribeVSwitches",
                "bss:PayOrder"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "ecs:DeleteTags",
                "ecs:UntagResources",
                "ecs:CreateTags",
                "ecs:TagResources"
            ],
            "Resource": "*"
        }
    ],
    "Version": "1"
}
```

The following table lists the permissions defined in the preceding policy.

Permission	Parameter
Create or access a resource to which a specific tag is added	`"ecs:tag/owner": "zhangsan"`
Call the API operations that are used to query tags	○ `ecs:DescribeTagKeys` ○ `ecs:ListTagResources` ○ `ecs:DescribeTags`

Permission	Parameter
Call the API operations that are used to query ECS resources	ecs:DescribeKeyPairs ecs:DescribeImages ecs:DescribeSecurityGroups ecs:DescribeLaunchTemplates ecs:DescribeDedicatedHosts ecs:DescribeDedicatedHostTypes ecs:DescribeAutoSnapshotPolicyEx
Call the API operations that are used to query VPC resources	vpc:DescribeVpcs vpc:DescribeVSwitches
Call the API operation that is used to pay for orders	bss:PayOrder
Not allowed to call the API operations that are used to manage tags	ecs:DeleteTags ecs:UntagResources ecs:CreateTags ecs:TagResources
Add a tag to a VPC	"vpc:tag/user": "lisi"

3. Attach the BindTagForRes custom policy to the userTest RAM user. For more information, see Grant permissions to a RAM user.

Step 2: Add a tag to a VPC

The custom policy created in Step 1: Create a custom policy and attach the policy to a RAM user requires that you select a VPC to which the `user:lisi` tag is added when you create an ECS resource. Therefore, you must have VPCs to which the tag is added. If you do not have such VPCs, you cannot create the ECS resource.

> **Note** If you do not have a VPC, create one first. For more information, see Create and manage a VPC.

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag > Tag**.
3. In the top navigation bar, select a region.
4. On the **Custom Tags** tab, click **Create Custom Tags**.
5. In the **Create Custom Tags** dialog box, create the `user:lisi` tag. Then, add the tag to an existing VPC.

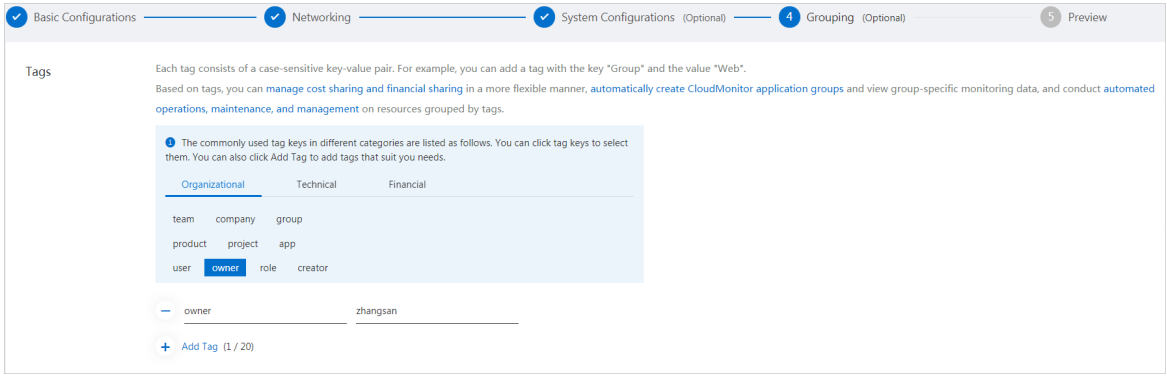
   For more information, see Add a custom tag.

Step 3: Create an ECS resource and add a specific tag to the ECS resource

Log on to the ECS console by using the userTest RAM user and create an ECS instance and add a specific tag to the ECS instance.

1. Log on to the ECS console by using the RAM user.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the top navigation bar, select the desired region.
4. Click **Create Instance** to create an ECS instance.

> **Note** You must select the VPC to which the `user:lisi` tag is added in Step 2: Add a tag to a VPC and add the `owner:zhangsan` tag to the ECS instance. If you do not add the owner:zhangsan tag to the instance, the instance cannot be created, and the **You are not authorized to create ECS instances** message appears.



References

You can add specific tags to existing resources so that you can control access to these resources. You can also access the resources to which specific tags are added. For more information, see Control access to resources by using tags.

10.2. Use tags to control access to ECS resources

After you add tags to your Elastic Compute Service (ECS) resources, you can use the tags to categorize and control access to the resources. This topic describes how to use tags to control the access of a RAM user to ECS instances.

Prerequisites

A RAM user is created within your Alibaba Cloud account. For more information, see Create a RAM user.

Context

Tags are used to identify cloud resources. The tags help you categorize, search for, and aggregate cloud resources that have the same characteristics from different dimensions. This simplifies resource management. You can add multiple tags to each cloud resource. For more information about the cloud services and resources that support tags, see Services that work with Tag and Types of resources that support Tag API operations.

Alibaba Cloud implements policy-based access control. You can configure RAM policies based on the roles of RAM users. You can define multiple tags in each policy and attach one or more policies to RAM users or RAM user groups.

By default, all resources within the current region are displayed in the resource list. To control the resources that are accessible to a RAM user, create a custom policy in which specific tags are specified, attach the policy to the RAM user, and add the tags to the resources.

Step 1: Create a custom policy and attach the policy to a RAM user

Create a custom policy named UserTagAccessRes by using an Alibaba Cloud account and attach the policy to the userTest RAM user. The UserTagAccessRes policy defines that you must specify the `owner:zhangsan` and `environment:production` tags when you use the RAM user to access ECS resources.

1. Log on to the RAM console by using your Alibaba Cloud account.
2. Create a custom policy named UserTagAccessRes.

   For more information, see Create a custom policy.

   The following code provides the document of the policy. You can configure multiple tags for cloud resources in a policy.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ecs:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:tag/owner": "zhangsan",
                    "ecs:tag/environment": "production"
                }
            }
        },
        {
            "Action": [
                "ecs:DescribeTagKeys",
                "ecs:DescribeTags"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "ecs:DeleteTags",
                "ecs:UntagResources",
                "ecs:CreateTags",
                "ecs:TagResources"
            ],
            "Resource": "*"
        }
    ],
    "Version": "1"
}
```

Permission	Configuration	Description
Access resources to which specific tags are added	○ `"ecs:tag/owner": "zhangsan"` ○ `"ecs:tag/environment": "production"`	You can control access to resources to which the specific tags are added.
Call the API operations that are used to query tags	○ `ecs:DescribeTagKeys` ○ `ecs:DescribeTags`	You can query tags in the ECS console.

Permission	Configuration	Description
Not allowed to call the API operations that are used to manage tags	ecs:DeleteTags ecs:UntagResources ecs:CreateTags ecs:TagResources	The policy excludes all tag-related API operations from its permissions. This ensures that users still have permissions regardless of tag modifications.

3. Attach the custom policy to the userTest RAM user.

   For more information, see Grant permissions to a RAM user.

Step 2: Add tags to ECS instances

Use an Alibaba Cloud account to add tags to ECS instances.

> **Note** If you do not have ECS instances, create ECS instances first. For more information, see Creation method overview.

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Tag > Tag**.
3. In the top navigation bar, select a region.
4. On the **Custom Tags** tab, click **Create Custom Tags**.
5. In the **Create Custom Tags** dialog box, add the `owner:zhangsan` and `environment: production` tags to existing ECS instances.

   For more information, see Add a custom tag.

Step 3: Access ECS instances to which specific tags are added

Use the userTest RAM user to log on to the ECS console and access instances to which specific tags are added.

1. Log on to the ECS console by using the RAM user.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the top navigation bar, select a region.
4. On the **Instances** page, click **Tags** next to the search box and select the `owner:zhangsan` and `environment:production` tags.

5. View the resources to which only the `owner:zhangsan` and `environment:production` tags are added.