ALIBABA CLOUD

Alibaba Cloud

Elastic Compute Service

Tag & Resource

Document Version: 20220701

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.Tags

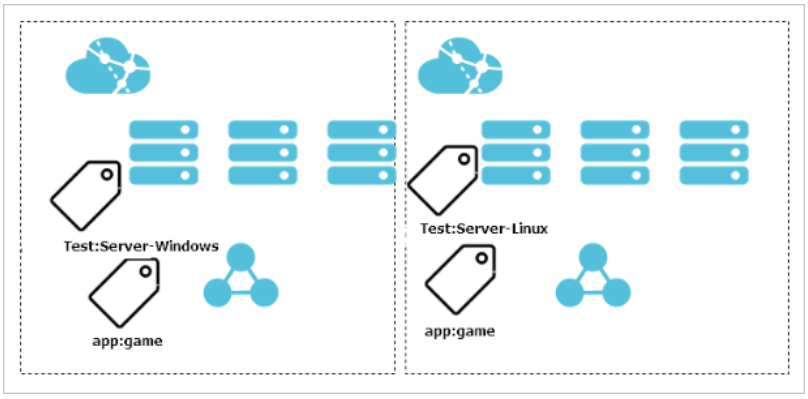
1.1. Overview

Tags can be used to identify resources. Tags allow enterprises and individuals to categorize their ECS resources and simplify the search and management of resources.

Scenarios

Tags can make your search more efficient and allow you to perform batch operations on resources. For example:

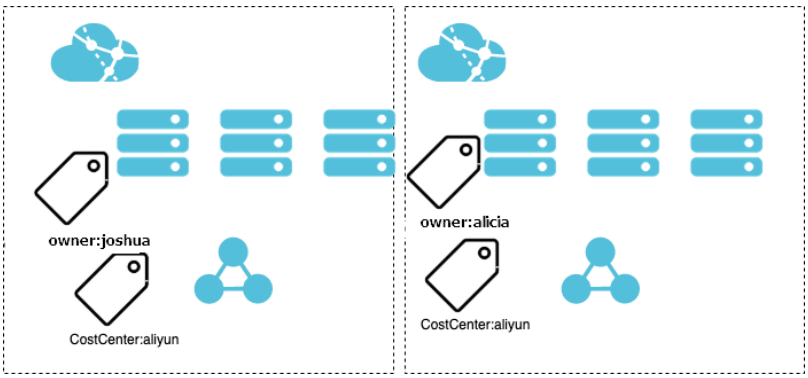
- You can bind different tags to environments such as production and test environments, operating systems such as Windows and Linux, and mobile platforms such as iOS and Android. For example, create the `Test:Server-Windows` tag and bind this tag to all the Windows ECS instances that are in the test environment. You can find these instances based on the tag and perform batch operations on these instances.



  Examples of batch operations:

  - Replace the image to deploy applications.
  - Upgrade patches.
  - Create security group rules to control access.
  - Use Operation Orchestration Service (OOS) to batch start, stop, or restart ECS instances.
  - Use Cloud Assistant to run an O&M script on multiple ECS instances.

- In team or project management, you can add tags such as `CostCenter:aliyun` to groups, projects, or departments. Then, you can categorize the objects, and implement itemized billing and cross authorization based on tags on the Billing Management page of the ECS console.



For more information, see the following topics:

- Create a resource with a specific tag
- Control access to resources by using tags
- Use tags to grant access to ECS instances by group

Precautions

- Each tag consists of a key-value pair.
- A tag must have a unique tag key.

  For example, an ECS instance is bound to the `city:shanghai` tag. If the instance is subsequently bound to the `city:newyork` tag, the `city:shanghai` tag is automatically unbound from the instance.
- Tag information is not shared across regions. For example, tags created in the China (Hangzhou) region are not visible to the China (Shanghai) region.
- Tags are deleted when they are not bound to any resources.
- For more information about the best practices for tag design, see Best practices for tag design.

Limits

For more information about limits and quotas of tags, see the "Tag limits" section in Limits.

Services that support tags

The following table lists Alibaba Cloud services and resources that support tags.

Service	Resource	API operation
Elastic Compute Service (ECS)	• ECS instance • Reserved instance • Elastic Block Storage (EBS) • Snapshot • Automatic snapshot policy • Image • Security group • Elastic network interface (ENI) • Dedicated host • SSH key pair • Launch template	• Bind a tag: TagResources • Unbind a tag: UntagResources • Search for resources based on tags: ListTagResources
Auto Scaling	Scaling group	• Bind a tag: TagResources • Unbind a tag: UntagResources • Search for resources based on tags: ListTagResources

Service	Resource	API operation
Virtual Private Cloud (VPC)	• VPC • vSwitch • Route table • Elastic IP address (EIP)	• Bind a tag: TagResources • Unbind a tag: UnTagResources • Search for resources based on tags: ListTagResources
ApsaraDB for Redis	ApsaraDB for Redis instance	• Bind a tag: TagResources • Unbind a tag: UntagResources • Search for resources based on tags: ListTagResources
Alibaba Cloud Content Delivery Network (CDN)	Domain name	• Bind a tag: TagResources • Unbind a tag: UntagResources • Query the tags of the current user: DescribeUserTags • Search for resources based on tags: DescribeTagResources
Key Management Service (KMS)	Customer master key (CMK)	• Bind a tag: TagResource • Unbind a tag: UntagResource • Search for resources based on tags: ListResourceTags
Apsara PolarDB	Cluster	• Bind a tag: TagResources • Unbind a tag: UntagResources
Object Storage Service (OSS)	Bucket	Add, delete, modify, or query tags for a bucket: bucket-tagging
ApsaraDB for RDS	ApsaraDB for RDS instance	• Bind a tag: Create and bind tags • Unbind a tag: Unbind tags • Search for resources based on tags: Query the tags of ApsaraDB RDS instances
AnalyticDB for PostgreSQL	AnalyticDB for PostgreSQL instance	Query resources based on tags: DescribeDBInstances
Cloud Enterprise Network (CEN)	CEN instance	• Bind a tag: TagResources • Unbind a tag: UntagResources • Search for resources based on tags: DescribeCens
Smart Access Gateway (SAG)	Cloud Connect Network (CCN)	Query resources based on tags: DescribeCloudConnectNetworks

Service	Resource	API operation
Operation Orchestration Service (OOS)	• OOS template • OOS operation tasks	• Bind a tag: TagResources • Unbind a tag: UntagResources • Search for resources based on tags: ListTagResources

1.2. Best practices for tag design

Increased cloud resources are hard to manage without tags. Tags can be used to manage, group, and search for resources. These resources include personnel, financial costs, and cloud services. This topic describes the best practices for tag design.

Scenarios

Tags are applicable to the following scenarios:

- Management of application publishing procedures
- Resource tracking and tag-based group search and management
- Tag- and group-based automated O&M by using Alibaba Cloud services such as Operation Orchestration Service (OOS), Resource Orchestration Service (ROS), Auto Scaling, and Cloud Assistant
- Tag-based cost management and cost allocation
- Resource- or role-based access control

Principles

You can implement the best practice for tag design based on the following principles:

- Mutual exclusivity
- Collective exhaustion
- Limited values
- Considering ramifications of future changes
- Simplified design

Mutual exclusivity

To implement the mutual exclusivity principle, we recommend that an attribute has only a single tag key. For example, if you use the `owner` tag key to represent the owner attribute, you cannot use other tag keys such as *own* or *belonger* to represent this attribute.

Collective exhaustion

Collective exhaustion indicates that when you plan resources, you must plan tags at the same time and prioritize the tag keys. All resources must have tags that consist of the planned tag keys and the corresponding tag values.

- Each tag key-value pair must be named in a standard format.
- Collective exhaustion is a prerequisite for future tag-based access control, cost tracking, automated O&M, and group search.

Limited values

This principle indicates that excess tag values must be removed and that only core tag values are retained.

Procedures for resource management, access control, automated O&M, and cost allocation can be simplified by implementing this principle. You can also use tags and automation tools under this principle to manage resources. Elastic Compute Service (ECS) allows you to control tags by calling API operations, which makes it easy to automatically manage, search for, and filter resources.

Considering ramifications of future changes

When you plan tags under the limited values principle, you must consider the impact of adding or removing tag values to improve the flexibility of modifying tags.

If you modify tags, tag-based access control, automated O&M, or related billing reports may change. For corporate or personal business, the best practice is to create business-related tag groups to manage resources in technical, business, and security dimensions. When you use automated O&M tools to manage resources and services, you can add automation-specific tags to aid in automated O&M.

Simplified design

Simplified design means that when you plan tags, you must create tag keys that have fixed dimensions to simplify the use of tag keys. By implementing this principle, you can reduce operation errors caused by redundant tag keys.

- You can create business-related tag groups to manage resources in technical, business, and security dimensions.
- When you use automated O&M tools to manage resources and services, you can add automation-specific tags to the resources and services.

Examples of designing tag keys

The following table describes the tag naming examples in the business dimension. We recommend that you use lowercase letters to name tags.

Dimension	Tag key	Tag value
Organization	• company • department • organization • team • group	Organization-specific names
Business	• product • business • module • service	Business-specific names

Dimension	Tag key	Tag value
Role	• role • user	• network administrator • application administrator • system administrator • opsuser • devuser • testuser
Purpose	• purpose • use	Specific purposes

Project	• From project dimensions:
	  ○ project
	  ○ risk
	  ○ schedule
	  ○ subtask
	  ○ environment
	• From personnel dimensions:
	  ○ sponsor
	  ○ member
	  ○ decisionmaker or owner
	  ○ creator
		Project-related values

Business department (to implement cost allocation and business tracking)	• costcenter • businessunit • biz • financecontact	Department-related values
Owner from the finance dimension (to identify the resource owner)	owner	Names or emails
Customers from the finance dimension (to identify the customers that a specific resource group serves)	Custom or actual values	Customer names
Project from the finance dimension (to identify the projects that are supported by specific resources)	project	Parameter
Order from the finance dimension	order	Order category IDs

References

- Search for resources by tag
- Use OOS to modify a tag value of multiple resources
- Implement automatic resource monitoring by group based on tags
- Create a resource with a specific tag

Related API operations

- TagResources
- ListTagResources
- UntagResources

1.3. Manage tags

1.3.1. Create or bind a tag

This topic describes how to create or bind a tag to resources in the ECS console. If multiple resources that are associated with each other exist in your account, you can bind tags to the resources. This allows you to categorize and manage the resources in a centralized manner.

Context

- For more information about resource types to which you can bind tags, see Overview.
- A maximum of 20 tags can be bound for a resource. If the number of tags bound to a resource exceeds the upper limit, you must unbind some of the tags before you bind new tags.

Procedure

1.
2.
3.
4. On the Tags tab, click **Create/Bind Tags**.
5. In the **Create/Bind Tags** dialog box, perform the following steps:
   i. Create a tag or select an existing tag. Click **Next**.
      - **Tag Key**: required. You can select an existing tag key or enter a new tag key. You can perform fuzzy search by prefix and bind up to 10 tag keys at a time.

        The tag key can be up to 128 characters in length and cannot contain *http://* or *https://*. It cannot start with *acs:* or *aliyun*.

        > **Note** If you want to bind an existing tag, select its tag key. If you want to create a tag, enter a new tag key.

      - **Tag Value**: optional. You can select an existing tag value or enter a tag value.

        The tag value can be up to 128 characters in length and cannot contain *http://* or *https://*. It cannot start with *acs:* or *aliyun*.

        > **Note** If you want to bind an existing tag, select its tag value.

ii. Click **Next**.

iii. Select one or more resources of the same type and click **OK**. For example, you can select four ECS instances.

iv. (Optional)Click **Bind Other Resources** to go back to the **Select Resources** step and continue to select one or more resources of the same type.

v. Click **Close**.

Result

On the Tags tab, select the tags you have bound and click the **Refresh** icon to view the list of resources to which the tags are bound.

Related information

- TagResources

1.3.2. Delete or unbind a tag

This topic describes how to delete or unbind a tag in the ECS console. You can unbind a tag from a resource when the tag is no longer needed. If you unbind a tag from a resource and the tag is not bound to any other resources, this tag is automatically deleted.

Prerequisites

The resource is bound to a tag.

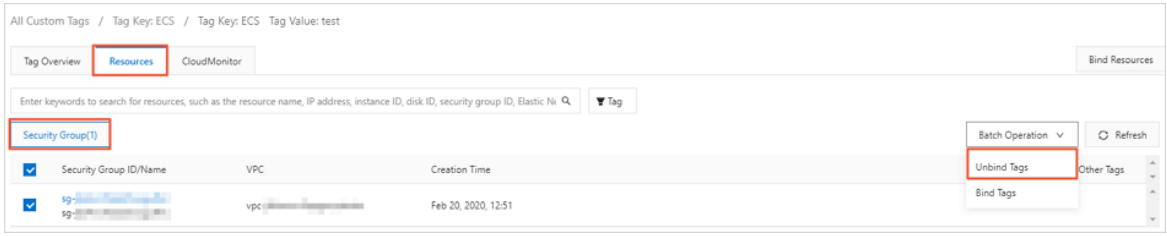
Context

Before you unbind a tag, take note of the following items:

- You can unbind up to 20 tags at a time.
- If you unbind a tag from all its resources such as ECS instances, snapshots, and security groups, this tag is deleted.

Procedure

1.
2.
3. On the **Tags** page, click a tag key.
4. In the tag value list, click a tag value.
5. On the **Tag Value** page that appears, click the **Resources** tab.
6. Select one or more resources, move the pointer over **Batch Operation**, and click **Unbind Tags**.



7. On the **Resources** tab, click **Refresh** to check whether the tags are unbound.

What's next

If you implement access control or automated O&M, or generate bill reports based on tags, you need to pay attention to the business changes caused by tag unbinding. For more information, see the "Considering ramifications of future changes" section in Best practices for tag design.

Related information

- UntagResources

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

This topic describes how to modify a tag value of multiple resources at a time by using an Operation Orchestration Service (OOS) custom template.

Prerequisites

A tag is bound to resources. For more information, see Create or bind a tag.

Context

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

> **Note**
>
> - You can use the OOS custom template to modify a tag value for up to 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 the OOS custom template to modify the tag values of any resources that support tagging in the same region. You can modify the API operations in the template to make it applicable to various resources. For more information about resources that support tagging, see Overview.For information about the resources that OOS supports, see List of supported cloud services.

Step 1: Create a template

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

1.
2.
3. In the left-side navigation pane, click **My Templates**.
4. Click **Create Template**.
5. In the Create Template dialog box, click the **Empty Templates** tab, select **Empty Templates**, and then click **OK**.
6. In the **Basic Information** section on the right of the Create Template page, enter a template

name in the Template Name field and add tags.

7. Click the **JSON** tab and write code in the code editor. The following code provides an example:

```
{
    "Description": "Modify a tag value for multiple resources",
    "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
        }
    },
    "Tasks": [
        {
            "Name": "DescribeInstances_ECS",
            "Action": "ACS::ExecuteAPI",
            "Description": {
                "zh-cn": "Filter ECS instances by tag",
                "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": {
                "zh-cn": "Update the tag of ECS instances",
                "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": {}
}
```

8. Click **Create Template**.

Step 2: Execute the template

You can perform the following steps to execute the template created in Step 1 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 and click **Create Execution** in the **Actions** column.
3. On the Create page, enter an execution description and select an execution mode in the Basic Information step. Then, click **Next: Parameter Settings**.
4. In the Parameter Settings step, configure parameters and click **Next: OK**.

   The following section describes the parameters.

- operateId: the operation ID, which is used to identify each operation. You can customize an operation ID.
- tagKey: the key of the tag whose value you want to modify, which is `TagKey` in this example.
- tagValue: the tag value to be modified, which is `OldTagValue` in this example.
- newTagValue: the new tag value, which is `NewTagValue` in this example.

5. Click **Create**. The execution details page appears. You can view the execution results.

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

1.3.4. Use OOS to bind tags to multiple ECS resources at a time

You can use Operation Orchestration Service (OOS) to bind tags to multiple ECS resources within the same region to control permissions on these ECS resources based on tags.

Context

You can bind tags for the resources of ECS and other Alibaba Cloud services by using OOS custom templates. For more information about the services that support tags, see Services that support tags. In this topic, a custom template is created in OOS to bind the `owner:zhangsan` tag to ECS instances within the same region.

> **Note** The resources must be located within the same region for a tag to bind.

Step 1: Create a custom policy and a RAM role

Create a RAM role named OOSServiceRole for OOS and attach permissions 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.

   The following policy is created.

   > **Note** This policy targets ECS instances, and the permissions in the policy are set to `ecs:DescribeInstances`. You can set the permissions based on your business needs. For example, if you want to add a tag to multiple security groups, you can replace `ecs:DescribeInstances` with `ecs:DescribeSecurityGroups`.

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

3. Create the OOSServiceRole RAM role.

   For more information, see Create a RAM role for a trusted Alibaba Cloud service.

4. Attach the custom policy to the RAM role.

   For more information, see Grant permissions to a RAM role. In this step, the OOSAutoBindTag custom policy is attached to the OOSServiceRole RAM role.

5. Attach the AliyunOSSFullAccess system policy to the OOSServiceRole RAM role.

Step 2: Bind tags to resources at a time

1.
2.
3. In the left-side navigation pane, click **My Templates**.
4. Create a custom template.
   i. On the My Templates page, click **Create Template**.
   ii. In the Create Template dialog box, click the **Empty Template** tab, select Empty Templates, and then click **OK**.
   iii. On the Create Template page, click the **YAML** tab to edit the template. In the upper-right corner of the page, enter OOSAutoBindTag in the Template Name field. After you edit the template, 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.
      zh-cn:
    AssociationProperty: Tags
  regionId:
    Type: String
    Description:
      en: The region to select ECS instances.
      zh-cn:
  OOSAssumeRole:
```

```
  OOSAssumeRole:
    Description:
      en: The RAM role to be assumed by OOS.
      zh-cn:
    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:
      zh-cn:
      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 }}'
```

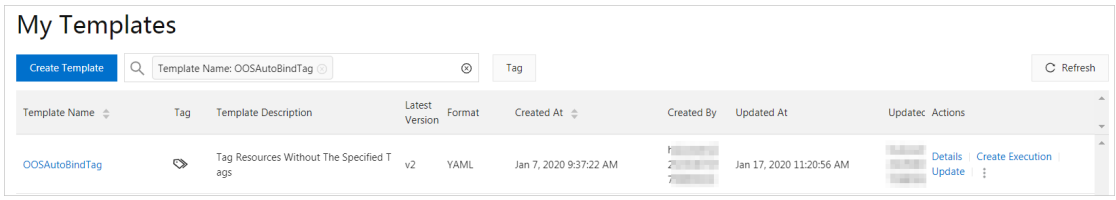
The following section describes the parameters:

- tags: the tags bound to ECS instances.
- regionId: the region ID of the ECS instances to which the selected tags are bound.
- OOSAssumeRole: the RAM role used by OOS.

The following section describes the permissions:

- DescribeInstances: filters resources based on source tags.
- TagResources: creates tags for or binds tags to specified resources.

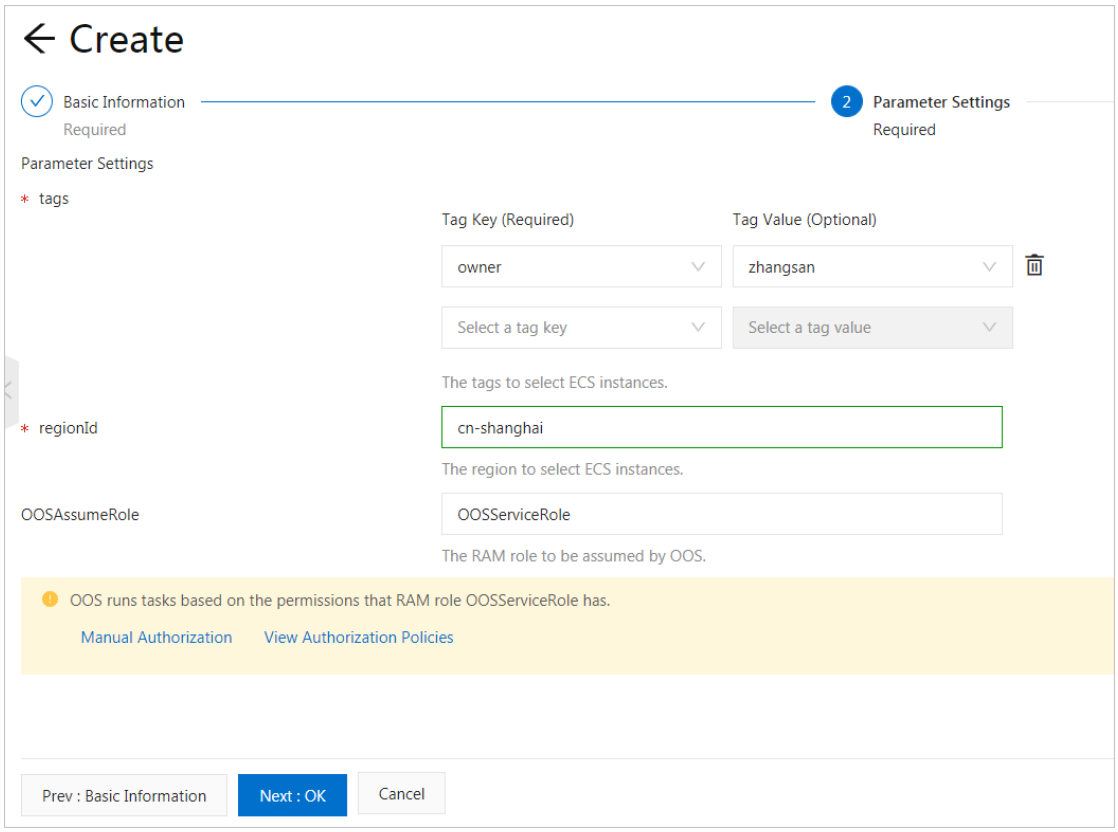
5. Execute the custom template.
   i. In the left-side navigation pane, click **My Templates**. On the My Templates page, find the OOSAutoBindTag custom template that you created in Step 5, and click **Create Execution** in the **Actions** column.



   ii. Keep the default settings or re-select the execution mode, and click **Next: Parameter Settings**.

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

In this example, the following parameters are configured:



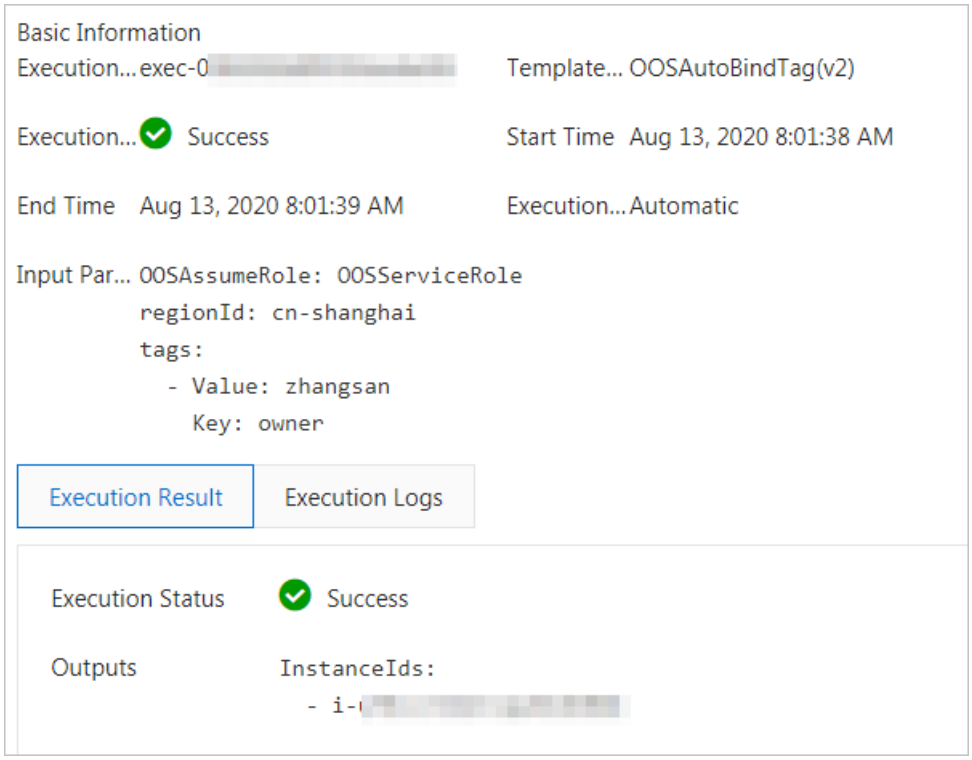
- tags: Select the `owner:zhangsan` tag.
- regionId: Select the region of the instances, such as `cn-shanghai`. For more information, see Regions and zones.
- oosAssumeRole: Use the RAM role OOSServiceRole.

iv. In the OK step, click **Create Execution**.

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

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

View the execution result, which demonstrates that the `owner:zhangsan` tag is bound to all the ECS instances within the selected region.



If Failed is displayed for Execution Status, you can view the information about the execution status and execution logs to make corresponding adjustments.

1.4. Manage resources based on tags

1.4.1. Create a resource with a specific tag

You can create custom policies that provide tag information and attach the policies to Resource Access Management (RAM) users to grant different access and operation permissions on cloud resources based on tags. This topic describes how to attach a custom policy that contains a specific tag to a RAM user to restrict Elastic Compute Service (ECS) resources from being created by the RAM user if they do not have the tag added.

Prerequisites

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

Context

Tags can be added to resources of ECS and other Alibaba Cloud services. For more information about the services that support tagging, see Services that support tags. By default, you can optionally add tags to resources when you create the resources. If you want to ensure that new resources have a specific tag added, you can create a custom policy that contains the tag. Then, you can attach this policy to a RAM user to control what operations the RAM user can perform on resources that have this tag added.

Step 1: Create a RAM policy by using your Alibaba Cloud account and attach the policy to a RAM user

To ensure that resources created by a RAM user have a specific tag added, create a custom policy that contains the tag and attach the policy to the RAM user. In this step, the BindTagForRes custom policy is created and attached to the userTest RAM user. Based on the policy, 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) that has a specific tag added. In this example, the VPC must have the `user:lisi` tag added, and the `owner:zhangsan` tag must be 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.

   The following policy is used in this step. You can configure permissions in the policy based on your business needs.

```
{
    "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:RemoveTags",
                "ecs:UntagResources",
                "ecs:AddTags",
                "ecs:TagResources"
            ],
            "Resource": "*"
        }
    ],
    "Version": "1"
}
```

Permissions granted or denied	Parameter	Description
Permissions are granted to create or access resources that has a specific tag added.	`"ecs:tag/owner": "zhangsan"`	○ The policy statement requires that the specific tag is added when resources are created. ○ The policy statement controls access to resources that have the specific tag added.
Permissions are granted to call API operations that are used to query tags.	○ `ecs:DescribeTagKeys` ○ `ecs:ListTagResources` ○ `ecs:DescribeTags`	The policy statement allows the RAM user to query tags in the ECS console.
Permissions are granted to 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`	The policy statement allows the RAM user to filter resources by tag. These permissions are required to create resources in the ECS console. Permissions on key pairs, images, security groups, instances, dedicated hosts, and snapshots are configured in this step.
Permissions are granted to call the API operations that are used to query VPC resources.	○ `vpc:DescribeVpcs` ○ `vpc:DescribeVSwitches`	The policy statement allows the RAM user to query existing VPCs and vSwitches.

Permissions granted or denied	Parameter	Description
Permissions are granted to call the API operation that is used to pay for orders.	`bss:PayOrder`	This operation applies only to subscription resources.
Permissions are denied to call the API operations that are used to manage tags.	○ `ecs:DeleteTags` ○ `ecs:UntagResources` ○ `ecs:CreateTags` ○ `ecs:TagResources`	The policy statement disallows the RAM user to call tag-related API operations to prevent loss of control on resources caused by tag modifications. You can grant these permissions based on your business needs. Exercise caution when you perform this operation.
Permissions are granted to select a VPC that has a specific tag added.	`"vpc:tag/user": "lisi"`	The policy statement specifies that the VPC used to create resources must have a specific tag added. You can optionally configure the statement to remove this constraint on VPCs.

3. Attach the custom policy to the RAM user or group for which you want to control access. For more information, see Grant permissions to a RAM role. In this step, the BindTagForRes custom policy is attached to the userTest RAM user.

> **Note** Issues may occur if you attach the BindTagForRes policy to an existing RAM user that already has multiple policies.

Step 2: Create and configure a VPC by using the Alibaba Cloud account

Based on the custom policy created in Step 1, when you create an ECS resource, you must select a VPC that has the `user:lisi` tag added. Create a VPC and add the tag to the VPC before you create an ECS resource. If a VPC does not have the user:lisi tag added, you cannot create the ECS resource in the VPC.

> **Note** You cannot add a tag to a VPC while the VPC is being created. You can only call the TagResources operation to add a tag to the VPC after the VPC is created.

1. Create a VPC by using the Alibaba Cloud account. For more information, see Create and manage a VPC.
2. Call the TagResources operation to add the `user:lisi` tag to the VPC.

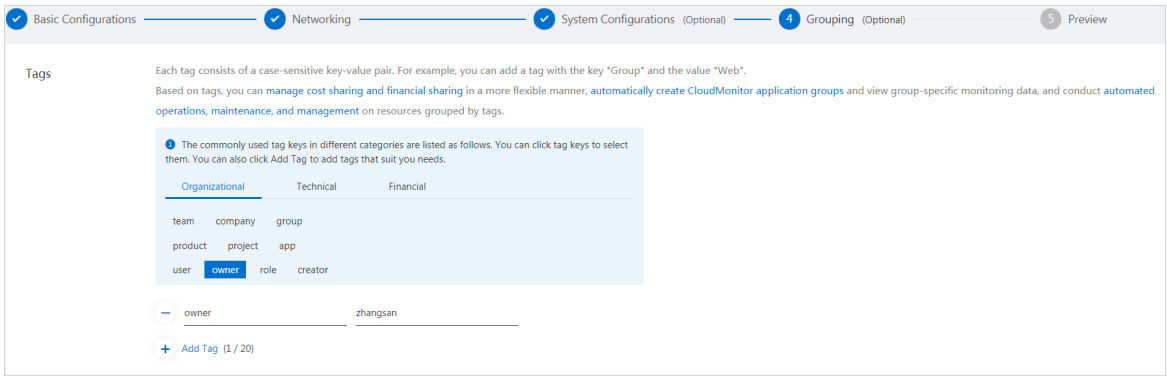
   You can also add other tags to the VPC.
3. Call the ListTagResources operation to query the VPC created in this step. If the response contains `"TagKey": "user"` and `"TagValue": "lisi"`, the `user:lisi` tag is added to the VPC.

Step 3: Create an ECS resource by using the RAM user

Log on to the ECS console as the userTest RAM user and create an ECS instance that has the specific tag added.

1.
2.
3.
4. Click **Create Instance** to create an instance.

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



What to do next

You can add specific tags to control access to existing resources, or access resources that have specific tags added. For more information, see Control access to resources by using tags.

1.4.2. Use the tag editor to manage resource tags

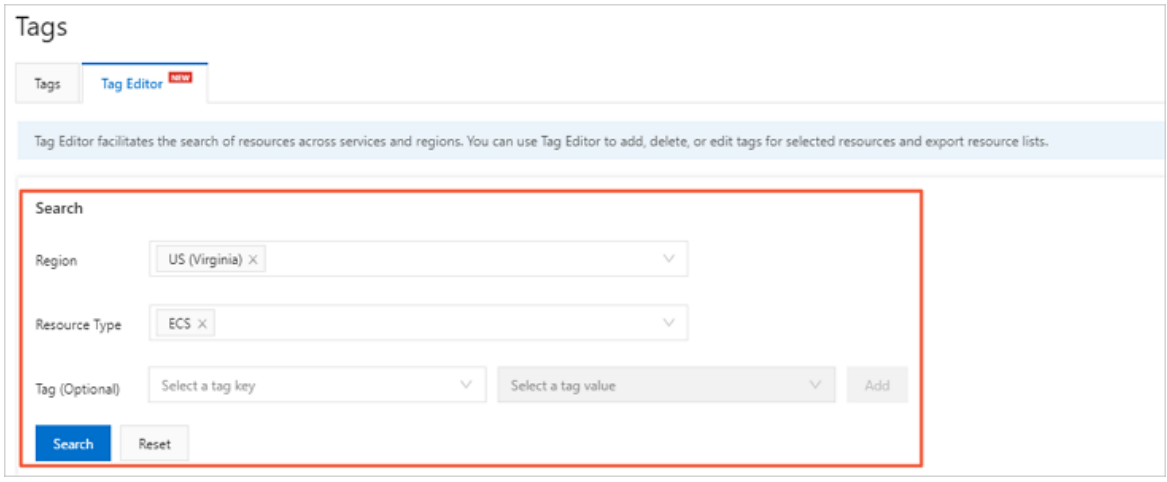
The tag editor is a tool to query and manage tags. You can use this tool to query 5,000 resource data entries across services and regions. You can also use it to edit resource tags and export resource information.

Context

The tag editor allows you to query the following ECS resources: instances, Block Storage devices, images, snapshots, security groups, Elastic Network Interfaces, dedicated hosts, and SSH key pairs.

Search resources

1.
2.
3. On the **Tags** page, click the **Tag Editor** tab.
4. In the **Search** section, configure query conditions and click **Search**.



In the **Search Results** section, you can click the icon to set the items to be displayed.

Edit tags of selected resources

You can edit tags for multiple found resources at a time.

1. In the **Search Results** section, select one or more resources, and click **Edit Tags**.
2. Manage resource tags.
   - Click **Add Tag** to add tags to the selected resources.
   - Click **Delete Tag** to delete tags from the selected resources.
   - After a tag that is bound to a resource is deleted, you can click **Cancel Deletion** to restore the tag.
3. Click **Submit**.

Export resource information

You can export the information of found resources.

1. In the **Search Results** section, select one or more resources, and then click **Export**.
2. Use one of the following methods to export information of resources:

   > **Note** You can click the icon to view all properties of the selected resources or customize properties to be displayed.

   - In the Export drop-down list, click **Export All Data** to export information of the selected resources as a CSV file.
   - In the Export drop-down list, click **Export Visible Columns** to export the displayed information as a CSV file.

Related information

- TagResources
- ListTagResources
- UntagResources

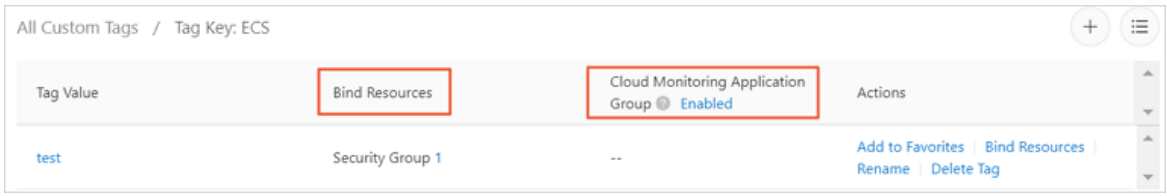
- DescribeInstances

1.4.3. Search for resources by tag

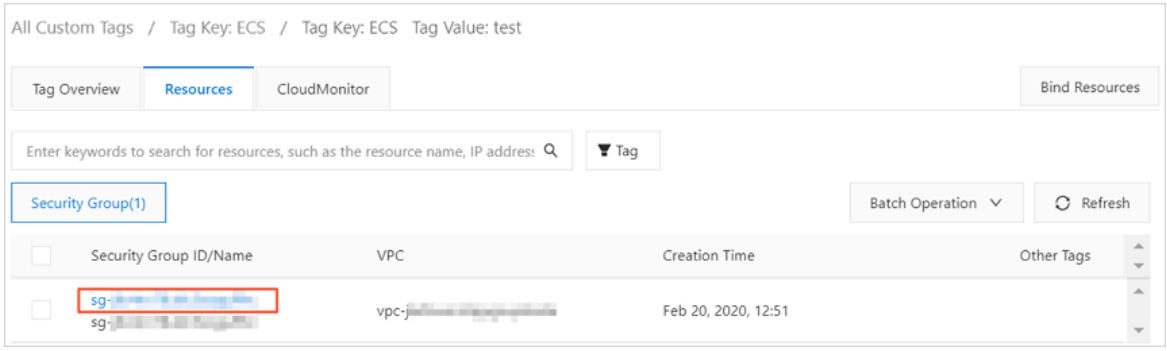
After you bind tags to resources, you can use one of the following methods to quickly search for resources. Exact match and fuzzy search are supported.

Search for resources on the Tags page

1.
2.
3.
4. Click the Tags tab and select a tag key from the tag list.
5. In the corresponding tag value list, view values in the Bind Resources and Cloud Monitoring Application Groups columns.



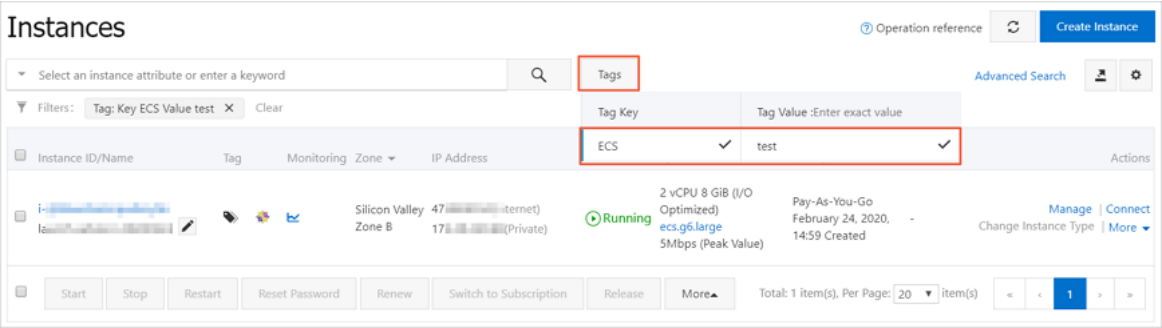
6. Click a tag value. Click **Resources** tab to view the resources bound to the tag. You can click a resource ID to go to the resource details page.



Search for resources on the Resources page

In the ECS console, pages of instances, disks, snapshots, images, security groups, and Elastic Network Interface allow you to set tags to search for these resources. For example, you can complete the following steps to search for ECS instances:

1.
2.
3.
4. On the **Instances** page, click **Tags** and then select a tag key. If you do not select a tag value, all ECS instances to which the tag key is bound are displayed.



Related information

References

- Create or bind a tag
- Delete or unbind a tag
- ListTagResources
- DescribeInstances

1.4.4. Control access to resources by using tags

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

Prerequisites

A RAM user is created by using an Alibaba Cloud account. For more information, see Create a RAM user.

Context

Tags are used to identify cloud resources. You can use tags to 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.

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. If you want to control which resources are accessible to RAM users, you can create custom policies that contain tags to implement access control on resources.

You can add tags to ECS resources and resources of other Alibaba Cloud services. By default, all resources within the current region are displayed in the resource list. If you want to control which resources are accessible to RAM users, you can create custom policies that contain tags to implement access control on resources.

Step 1: Use an Alibaba Cloud account to create a policy and attach it to a RAM user

This section describes how to use an Alibaba Cloud account to create a custom policy that contains specific tags and attach this policy to a RAM user. In the example, the UseTagAccessRes custom policy, the userTest RAM user, and the `owner: zhangsan` and `environment: production` tags are used.

1. Log on to the RAM console by using an Alibaba Cloud account.

2. Create the UserTagAccessRes custom policy. For more information, see Create a custom policy.

   The following code shows how to 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"
}
```

Policy	Policy content	Description
Grants the permissions to access resources to which specific tags are added	○ `"ecs:tag/owner": "zhangsan"` ○ `"ecs:tag/environment": "production"`	This policy allows you to control access to resources to which the specific tags are added.
Grants the permissions to query tags	○ `ecs:DescribeTagKeys` ○ `ecs:DescribeTags`	This policy allows you to query tags in the ECS console.

Policy	Policy content	Description
Does not grant the permissions 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 will not be deprived of permissions due to tag modifications.

3. Attach the custom policy to RAM users or user groups whose access you want to control. For more information, see Grant permissions to a RAM role. In this step, attach the UserTagAccessRes policy to the userTest RAM user.

> **Note** To attach the UserTagAccessRes policy to an existing RAM user, note that multiple policies attached to a single RAM user may cause problems.

Step 2: Use the Alibaba Cloud account to add tags to existing resources

You can add tags to existing resources to control access to the resources. This section describes how to use an Alibaba Cloud account to create an ECS instance and add a tag to the instance.

> **Note** If you have no existing ECS instances, create an instance first. For more information, see Creation method overview.

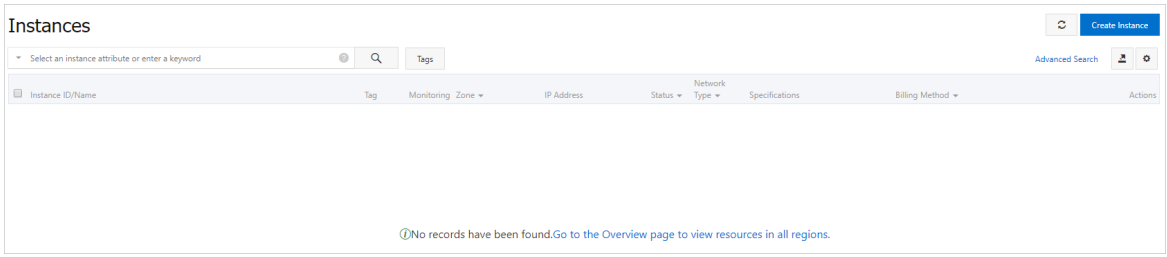
1.
2.
3. On the Tags page, click **Create/Bind Tags**. In the Create/Bind Tags panel, create the `owner: zhangsan` and `environment: production` tags and bind them to existing ECS instances. For more information about how to add a tag to a resource, see Create or bind a tag.

Step 3: Use the RAM user to access instances to which tags are added

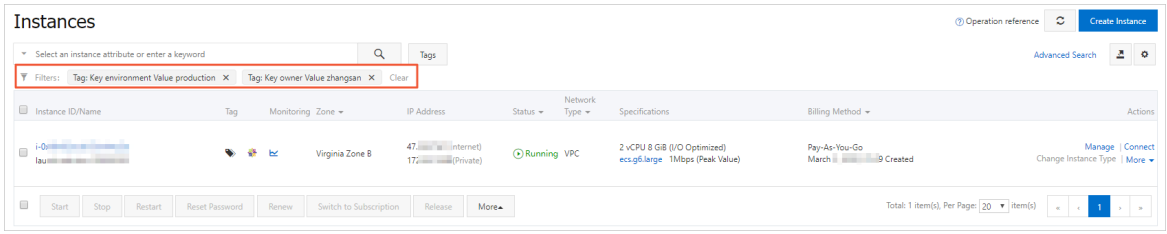
Use the userTest RAM user who is attached with the UseTagAccessRes policy to log on to the ECS console and access instances to which tags are added.

> **Note** ECS resources that can have tags added include instances, Elastic Block Storage (EBS) devices, snapshots, images, security groups, Elastic network interfaces (ENIs), dedicated hosts, SSH key pairs, and launch templates. In the example, ECS instances are used.

1.
2.
3. In the top navigation bar, select a region. No instances are displayed on the Instances page.



4. Specify tags to view instances.



1.4.5. Implement fine-grained access control by using tags

After you add tags to your Elastic Compute Service (ECS) resources, you can use the tags to categorize the resources and control access to them. This topic describes how to use tags to control the permissions of Resource Access Management (RAM) users so that different users can be granted different access and operation permissions on cloud resources based on tags.

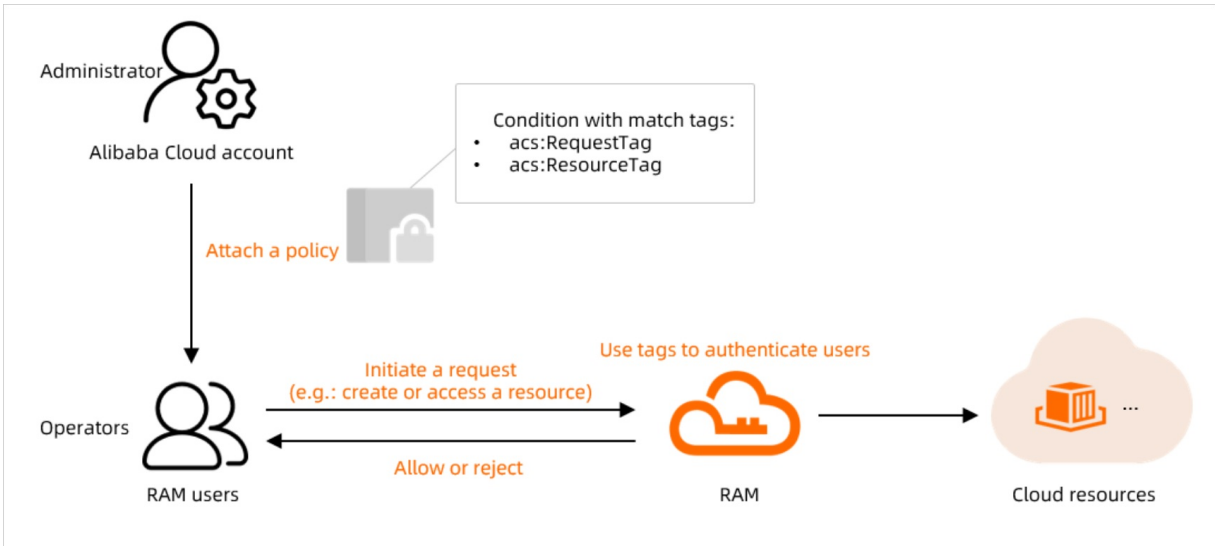
Prerequisites

A RAM user is created. For more information, see Create a RAM user.

Context

Tags can be used to identify, categorize, or classify resources for easy management. RAM allows you to manage user identities and resource access and operation permissions based on policies. You can use tags as conditions in RAM policies to implement fine-grained access control on resources.

The following figure shows how to use tags to manage resource access and operation permissions of RAM users, which is called tag-based authentication.



Scenarios

The procedure in this topic describes how to use tag-based authentication. In the example, the scenario that meets the following requirements is used:

- Resources to which the `costcenter:tony` tag is not added cannot be created.
- Operations can be performed only when requests contain the `costcenter:tony` tag.
- Resources created by other users that do not have the `costcenter:tony` tag added cannot be managed.
- Tag-based authentication supports some API operations that are used to query resources. You can query the instances that have the `costcenter:tony` tag added.
- Tags cannot be modified.

> **Note** For more information about tag-based authentication for API requests, see Tag-based authentication of requests to different API operations.

Procedure

In this procedure, a custom policy named UserTagAccessRes is created by using an Alibaba Cloud account and is attached to the RAM user userTest. The UserTagAccessRes policy specifies that RAM users must specify the `costcenter:tony` tag before they can access and manage ECS resources.

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

   In this example, you can configure multiple tag-based conditions for cloud resources in the `Condition` element of the custom policy to restrict operation permissions. The following table describes supported tag-based authentication conditions.

Tag-based authentication condition	Description
`acs:RequestTag`	Indicates that a specific tag must be included in each API request. If an API request does not include tag-related parameters, the `acs:RequestTag` condition cannot be used. Otherwise, authentication fails.
`acs:ResourceTag`	Indicates that a specific tag must be added to the specified resource. If an API request does not include a resource ID, the `acs:ResourceTag` condition cannot be used. Otherwise, authentication fails.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:Run*",
                "ecs:Create*",
                "ecs:Purchase*",
                "ecs:DescribeInstances",
                "ecs:List*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "acs:RequestTag/costcenter": "tony"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "acs:ResourceTag/costcenter": "tony"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:List*",
                "ecs:DescribeInstanceStatus",
                "ecs:DescribeInstanceVncUrl",
                "ecs:DescribeInstanceAutoRenewAttribute",
                "ecs:DescribeInstanceRamRole",
                "ecs:DescribeInstanceTypeFamilies",
```

```
                "ecs:DescribeInstanceTypes",
                "ecs:DescribeInstanceAttachmentAttributes",
                "ecs:DescribeInstancesFullStatus",
                "ecs:DescribeInstanceHistoryEvents",
                "ecs:DescribeInstanceMonitorData",
                "ecs:DescribeInstanceMaintenanceAttributes",
                "ecs:DescribeInstanceModificationPrice",
                "ecs:DescribeA*",
                "ecs:DescribeC*",
                "ecs:DescribeD*",
                "ecs:DescribeE*",
                "ecs:DescribeH*",
                "ecs:DescribeIm*",
                "ecs:DescribeInv*",
                "ecs:DescribeK*",
                "ecs:DescribeL*",
                "ecs:DescribeM*",
                "ecs:DescribeN*",
                "ecs:DescribeP*",
                "ecs:DescribeR*",
                "ecs:DescribeS*",
                "ecs:DescribeT*",
                "ecs:DescribeZ*",
                "vpc:DescribeVpcs",
                "vpc:DescribeVSwitches",
                "bss:PayOrder"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "ecs:RemoveTags",
                "ecs:UntagResources",
                "ecs:AddTags",
                "ecs:TagResources"
            ],
            "Resource": "*"
        }
    ]
}
```

The preceding policy can provide the following access control:

- Resources to which the `costcenter:tony` tag is not added cannot be created.

  Operations can be performed only when requests contain the `costcenter:tony` tag.

```
{
    "Effect": "Allow",
    "Action": [
        "ecs:Run*",
        "ecs:Create*",
        "ecs:Purchase*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "acs:RequestTag/costcenter": "tony"
        }
    }
}
```

- Resources created by other users that do not have the `costcenter:tony` tag added cannot be managed.

```
{
    "Effect": "Allow",
    "Action": "*",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "acs:ResourceTag/costcenter": "tony"
        }
    }
}
```

- Tag-based authentication supports some API operations that are used to query resources. You can query the instances that have the `costcenter:tony` tag added.

```
{
    "Effect": "Allow",
    "Action": [
    "ecs:DescribeInstances",
        "ecs:List*"
    ],
    "Resource": "*",
    "Condition": {
    "StringEquals": {
    "acs:RequestTag/costcenter": "tony"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ecs:List*",
        "ecs:DescribeInstanceStatus",
        "ecs:DescribeInstanceVncUrl",
        "ecs:DescribeInstanceAutoRenewAttribute",
        "ecs:DescribeInstanceRamRole",
        "ecs:DescribeInstanceTypeFamilies",
        "ecs:DescribeInstanceTypes",
        "ecs:DescribeInstanceAttachmentAttributes",
        "ecs:DescribeInstancesFullStatus",
        "ecs:DescribeInstanceHistoryEvents",
        "ecs:DescribeInstanceMonitorData",
        "ecs:DescribeInstanceMaintenanceAttributes",
        "ecs:DescribeInstanceModificationPrice",
        "ecs:DescribeA*",
        "ecs:DescribeC*",
        "ecs:DescribeD*",
        "ecs:DescribeE*",
        "ecs:DescribeH*",
        "ecs:DescribeIm*",
        "ecs:DescribeInv*",
        "ecs:DescribeK*",
        "ecs:DescribeL*",
        "ecs:DescribeM*",
        "ecs:DescribeN*",
        "ecs:DescribeP*",
        "ecs:DescribeR*",
        "ecs:DescribeS*",
        "ecs:DescribeT*",
        "ecs:DescribeZ*",
        "vpc:DescribeVpcs",
        "vpc:DescribeVSwitches",
        "bss:PayOrder"
    ],
    "Resource": "*"
}
```

- Tags cannot be modified.

```
{
    "Effect": "Deny",
    "Action": [
        "ecs:RemoveTags",
        "ecs:UntagResources",
        "ecs:AddTags",
        "ecs:TagResources"
    ],
    "Resource": "*"
}
```

3. Attach the custom policy to the RAM user or group for which you want to control access. For more information, see Grant permissions to a RAM role.

   In this step, attach the UserTagAccessRes policy to the RAM user userTest.

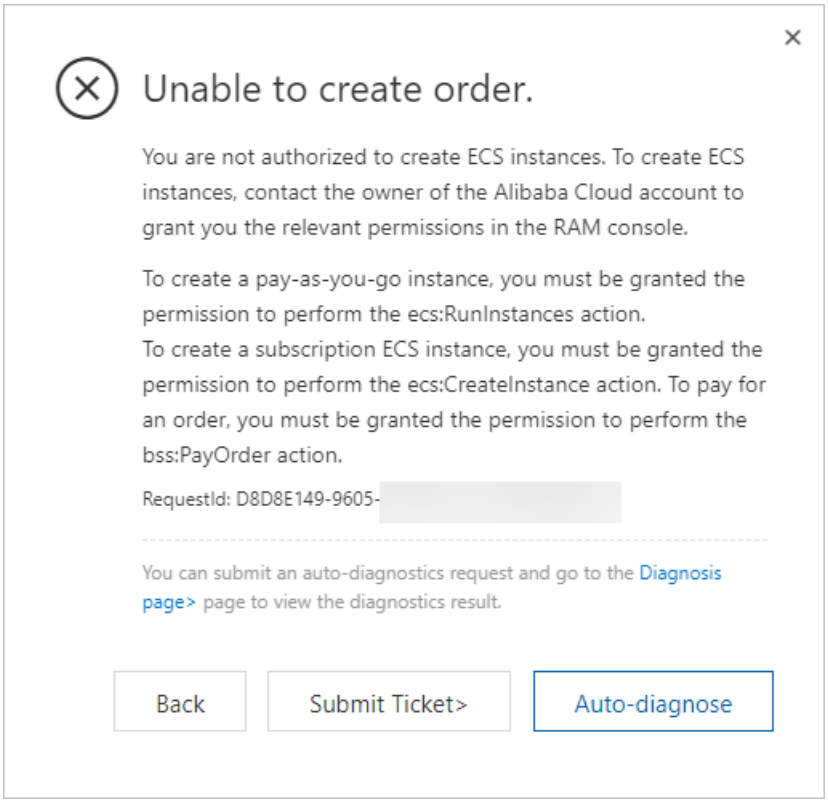
   > **Note** To attach the UserTagAccessRes policy to an existing RAM user, note that multiple policies attached to a single RAM user may cause permission issues.

Result

After the custom policy is attached to the RAM user, the RAM user can access and manage only resources that have the `costcenter:tony` tag added. The following section describes the results that occur when the RAM user accesses or manages resources:

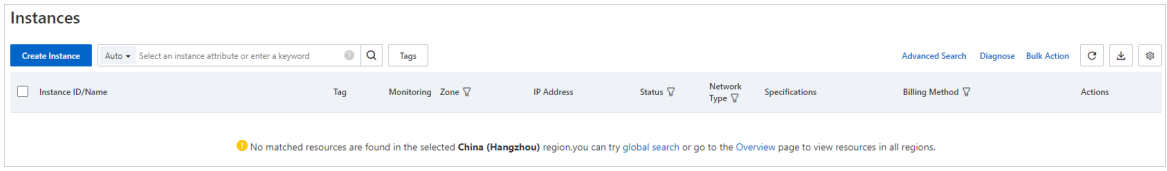
Create ECS instances

- ECS instances that have the `costcenter:tony` tag added can be created.
- When you create an ECS instance to which the `costcenter:tony` tag is not added, an error message is displayed as shown in the following figure.

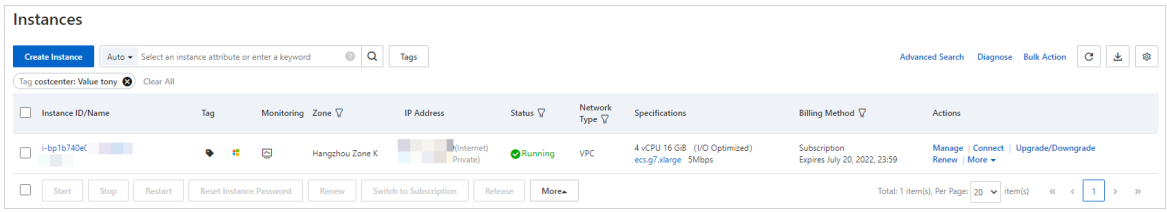


View ECS instances

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 a region. No instances are displayed on the Instances page.

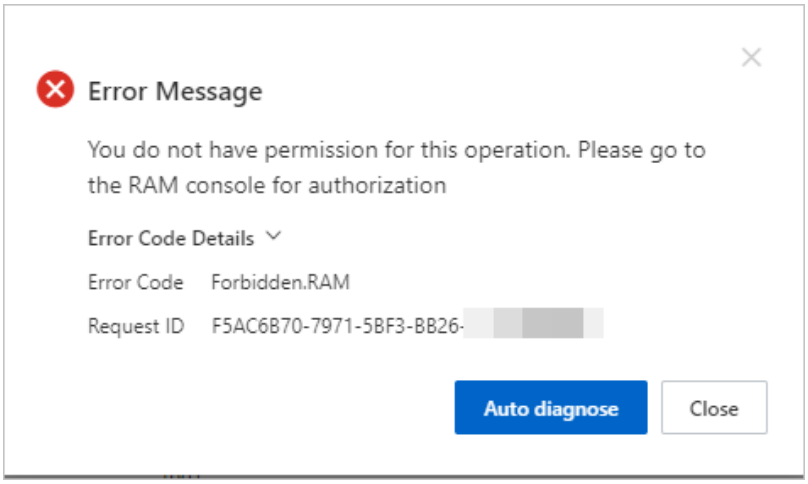


4. After you specify the `costcenter:tony` tag, you can view the instances that you have permissions to access.



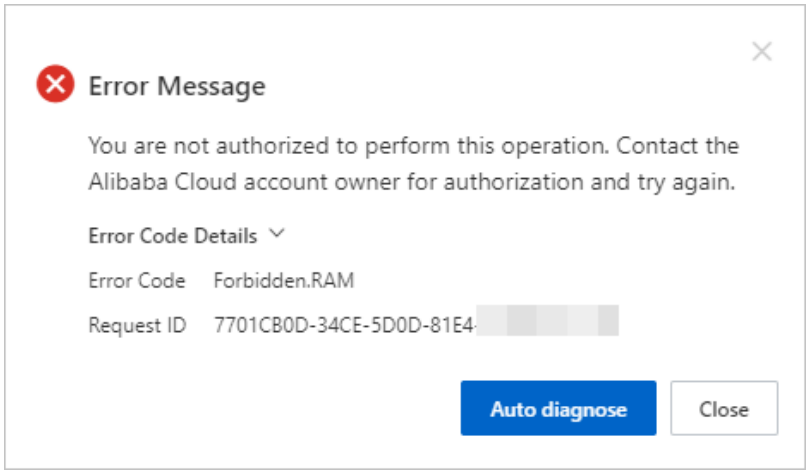
Modify security groups

- Security groups that have the `costcenter:tony` tag added can be modified.
- When you modify a security group to which the `costcenter:tony` tag is not added, the following error message is displayed.



Modify tags

Tags cannot be modified. When you modify a tag, an error message is displayed as shown in the following figure.



1.4.6. Implement automatic resource monitoring by group based on tags

You can add the same tag to Elastic Compute Service (ECS) instances that run the same business. Then, you can use the application group feature of CloudMonitor to configure smart tag synchronization for these instances. CloudMonitor assigns ECS instances with the same tag to the same application group to automatically monitor the instances in the group. In ECS, only ECS instances support automatic resource monitoring by group based on tags.

Context

The application group feature of CloudMonitor allows you to manage alert rules and view monitoring data by group, which reduces management complexity. For more information, see Create an application group. ECS instances with a specified tag are automatically identified and assigned to an application group based on the configuration rule of the group. In this topic, instances that are automatically created in a scaling group and that have the `testKey:testValue` tag added are used, and the instances are identified and assigned to an application group that has the testKey:testValue tag added.

You can use one of the following methods to implement automatic resource monitoring by group based on tags:

- Create resources that have tags added or add tags to existing resources. Then, use CloudMonitor to create an application group that supports smart tag synchronization. Make sure that the tags of the application group are the same as those of the resources.
- Create an application group that supports smart tag synchronization, and add a custom tag to the matching rule of the application group. Then, create resources that have the tag added or add the tag to existing resources. The resources are automatically assigned to the application group.

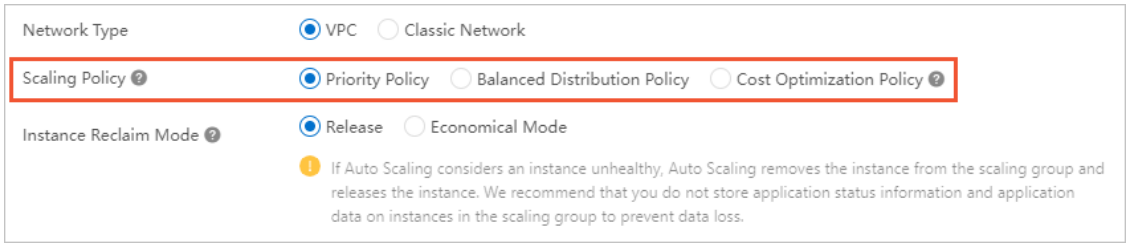
Step 1: Create instances that have a specified tag add

You can create instances that have a specified tag added or add a specified tag to existing instances. For more information, see Create or bind a tag. Alternatively, you can perform the following operations to use Auto Scaling to add a specified tag to the instances in a scaling group:

1.
2. Create a scaling group.

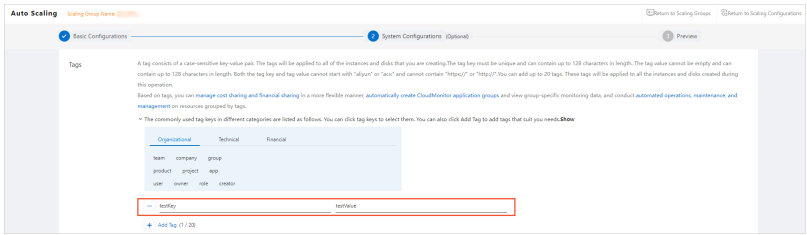
   For more information, see Create a scaling group. In this example, the following operations are performed:

   - Set **Minimum Number of Instances** to 4.
   - Specify **Scaling Policy** based on your business requirements to implement high-availability auto scaling.

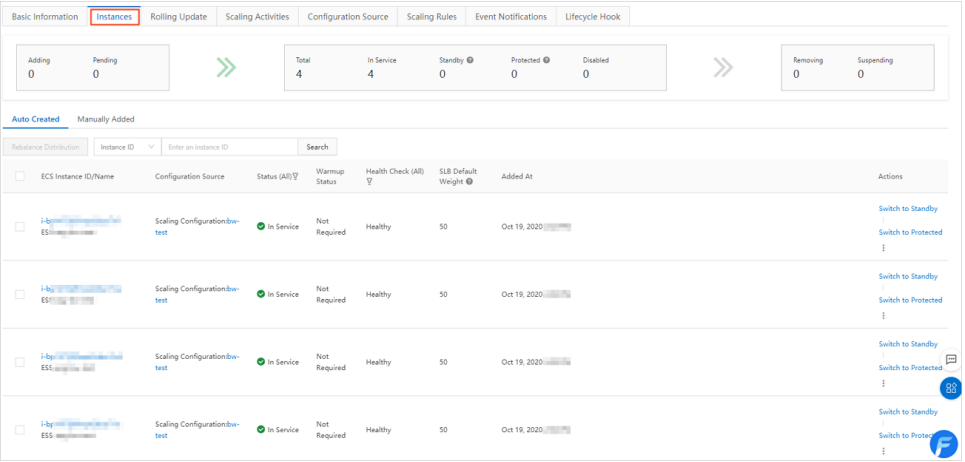


3. Create a scaling configuration.

   For more information, see Create a scaling configuration (ECS). You must add the `testKey:testValue` tag in the **System Configurations (Optional)** step.



4. Go to the scaling group details page, click the **Instances** tab, and then view the ECS instances that are automatically created in the scaling group.

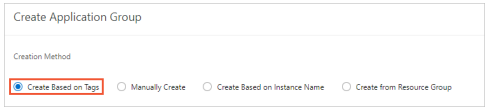


Step 2: Create a CloudMonitor application group

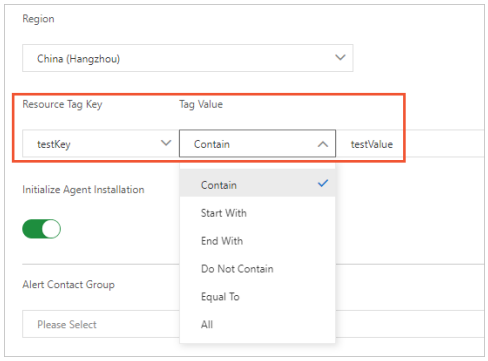
1. Log on to the CloudMonitor console.
2. Create a CloudMonitor application group. For more information, see Create an application group.

   In this example, Creation Method is set to **Create Based on Tags** and the `testKey:testValue` tag is added to the matching rule of an application group. Then, the instances that have the tag added are assigned to the application group.

   i. Set Creation Method to **Create Based on Tags**.

   ii. Set Resource Tag Key to `testKey` and specify the Tag Value parameter based on your needs. In this example, select **Contain** from the Tag Value drop-down list and enter `testValue` in the Tag Value field.

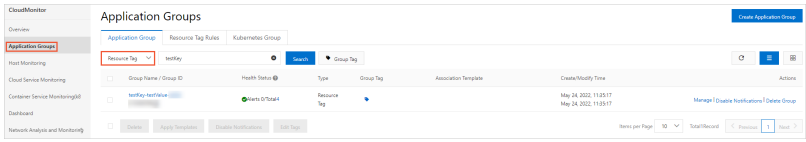
   

Step 3: View monitoring information of the ECS instances

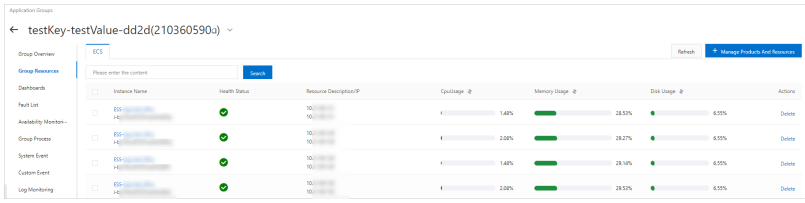
You can use one of the following methods to view the information of the ECS instances:

Method 1: View the monitoring information about the ECS instances based on their application group in the CloudMonitor console.

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, click **Application Groups**.
3. On the Application Group tab, select **Resource Tag** from the drop-down list, enter `testKey` in the search box, and then click Search.

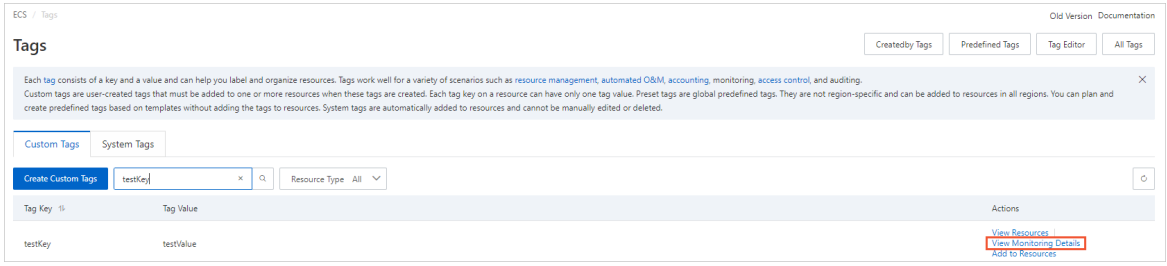


4. Click `testKey-testValue-53** / 22******` in the Group Name / Group ID column to view the resources in the group.
   The ECS instances that are automatically created in the scaling group are automatically added to the application group.



Method 2: View the monitoring information of the ECS instances in the ECS console.

1.
2.
3.
4. On the **Tags** page, click the **Custom Tags** tab.
5. Enter `testKey` in the search box to search for the tag.
6. Click **View Monitoring Details** in the **Actions** column.



Go to the **Monitoring** tab to view the monitoring, alert, and event information of the ECS instances in the application group that has the tag added.

What's next

You can monitor ECS instances in real time by using CloudMonitor. For more information, see Overview.