

Alibaba Cloud

Resource Management Best Practices

Document Version: 20201112

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 <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.Resource group -----	05
1.1. Use RAM to create and authorize resource groups -----	05
1.2. View billing statements by resource group -----	07
1.3. Use ActionTrail to record operations on resource groups -----	08
2.Tag -----	10
2.1. Design tags -----	10
2.1.1. Best practices for tag design -----	10
2.2. Use tags to implement automated O&M -----	12
2.3. Use tags to control access to resources -----	12
2.3.1. Create a resource with a specific tag -----	12
2.3.2. Use tags to control access to ECS resources -----	16
2.4. Use OOS to modify a tag value of multiple resources -----	19
2.5. Use OOS to add tags to multiple resources -----	22
2.6. Use OOS to start multiple ECS instances with specific tags...-----	26
2.7. Use Cloud Config to search for resources that are not bou...-----	27

1.Resource group

1.1. Use RAM to create and authorize resource groups

This topic describes how to use RAM to create and authorize resource groups in Alibaba Cloud. After you create and authorize resource groups, you can manage your own members, permissions, and resources by group.

Prerequisites

An Alibaba Cloud account is created. To create an Alibaba Cloud account, visit the [account registration page](#).

Context

A gaming company is developing three gaming projects. Each project requires multiple types of cloud resources. The company has an Alibaba Cloud account and more than 100 Elastic Compute Service (ECS) instances under this account.

The requirements of the company are as follows:

- Independent project management: Project managers can manage their own project members and the permissions that the project members require to access cloud resources.
- Separate bills: The financial department of the company requires that each project receives separate bills.
- A shared bottom-layer network: The company requires a shared bottom-layer network for its cloud resources.

The company has the following optional solutions:

- Multi-account solution
 - This solution supports independent project management. The company creates three Alibaba Cloud accounts (one account for each project) and assigns one project manager for each account. Then, project managers can manage their own project members and access permissions of each member.
 - This solution supports separate bills. The accounts receive separate bills by default. The consolidated billing feature provided by Alibaba Cloud for multiple accounts can be used to consolidate the bills and invoices.
 - This solution does not support a shared bottom-layer network. The resources of different accounts are isolated between different networks. Virtual private clouds (VPCs) under the accounts can be connected through peering connections. However, this incurs higher management costs.
- Single-account solution (with tagged resources)
 - This solution does not support independent project management. The company can tag its cloud resources by group, but project managers cannot manage their own members and access permissions of each member.
 - This solution supports separate bills. The company can tag its cloud resources by project. Then, each project can receive separate bills.

- This solution supports a shared bottom-layer network. The company can use tag-based RAM policies to authorize RAM users to access a group of resources. The company does not need to pay for peering connections established between different networks because these resources belong to the same account.
- **Resource group-based management solution**
 - This solution supports independent project management. Each resource group has an administrator. Administrators can manage their own group members and access permissions of each member.
 - This solution supports separate bills. Alibaba Cloud provides the consolidated billing feature that allows resource groups to receive separate bills.
 - This solution supports a shared bottom-layer network. Resource groups belong to the same account and can share a VPC. The cost of peering connections is eliminated.


Solution

The resource group-based management solution can meet all requirements of the company. By using this solution, the company only needs to use one Alibaba Cloud account to create three resource groups that correspond to the three projects.


Resource group-based solution

1. Create three RAM users: `alice@secloud.onaliyun.com` , `bob@secloud.onaliyun.com` , and `charlie@secloud.onaliyun.com` .


For more information, see [Create a RAM user](#).

 **Note** The following steps use the RAM user Alice as an example. The steps demonstrate how to set a RAM user as a resource group administrator.

2. Log on to the [Resource Management console](#).
3. In the left-side navigation pane, click **Resource Group**. On the **Resource Group** page, click **Create Resource Group**.
4. Specify the **Resource Group Name** and **Display Name** parameters, and then click **OK**.

 **Note** Create three resource groups: Game1, Game2, and Game3.

5. Find the target resource group, and click **Manage Permission** in the **Actions** column.
6. On the **Permissions** tab, click **Grant Permission**.
7. In the **Principal** field, enter Alice, and then select the RAM user from the auto-complete results.
8. In the **Authorization Policy Name** column, click `AdministratorAccess` .
9. Click **OK**.
10. Click **Complete**.

 **Note** Repeat the preceding steps to set Bob and Charlie as resource group administrators.

Result

Alice, Bob, and Charlie are the respective resource group administrators of Game1, Game2, and Game3. The administrators have the following permissions:

- After an administrator logs on to the ECS console, the administrator can view the respective resource group. The administrator can also create and manage ECS instances.
- After an administrator logs on to the Resource Management console, the administrator can add RAM users and grant resource access permissions to RAM users.

1.2. View billing statements by resource group

To manage billing statements by resource group after you create your resource groups, you can create cost centers and allocate the resource groups to the cost centers.


Context

A gaming company (Company A) has three gaming projects under development. Each project requires multiple types of cloud resources. Company A has only one Alibaba Cloud account but more than 100 Elastic Compute Service (ECS) instances under this account.


The finance department of Company A wants each project to receive separate bills.

Procedure

1. Create resource groups.
 - i. Log on to the [Resource Management console](#).
 - ii. Create one resource group for each project. For more information, see [Create a resource group](#).
 - iii. Move resources to the appropriate resource groups. For more information, see [Transfer resources across resource groups](#).
2. Create cost centers.
 - i. In the top navigation bar, click **Expenses** to go to the **User Center** console.
 - ii. In the left-side navigation pane, choose **All Menus > Cost Center**.
 - iii. In the navigation tree, click **Add** to create cost centers.

 **Note** To simplify management, the names of the cost centers and resource groups can be the same.

3. Map resource groups to cost centers.
 - i. In the navigation tree, click **Resources Not Allocated**. The right-side section then shows all resources that are not allocated.
 - ii. Filter the resources by **Resource Group** to show all resources in a resource group. Select all the resources and click **Allocate**.

 **Notice** The information of resource groups is not synchronized to cost centers in real time. If you add a resource to a resource group for the first time or change the resource group to which a resource belongs, you can view the information of the resource group in the related cost center about two days later.


- iii. In the dialog box that appears, select a cost center and click **OK**.
 - iv. In the navigation tree, click the cost center name to view all resources that belong to the cost center.
4. View billing statements by cost center.
 - i. In the left-side navigation pane of the **User Center** console, click **Bill**. On the page that appears, click the **Details** tab.
 - ii. Filter the billing statements by cost center to view the billing statements of each resource group.

1.3. Use ActionTrail to record operations on resource groups

This topic describes how to use ActionTrail to record the operations that RAM users or the owners of Alibaba Cloud accounts perform on resource groups.

Procedure

1. Log on to the [ActionTrail console](#).
2. In the left-side navigation pane, choose **ActionTrail > History Search**. On the page that appears, set **EventType** and **Time** to filter events.

 **Note** You can also click **Advance Search** next to the **Time** field and set the following parameters to perform a precise search: **Username**, **Event Name**, **Resource Name**, **Resource Type**, **Product Type**, and **Access Key**.

3. In the event list, click the **+** icon next to an event to view the basic information of the event.
4. Then, click **View Event** to view details.

Result


```
{
  "eventId": "B1CFCA37-83FA-4288-B623-01994CF8****",
  "eventVersion": "1",
  "requestParameters": {
    "RequestId": "B1CFCA37-83FA-4288-B623-01994CF8BDD2",
    "DisplayName": "actiontrail",
    "HostId": "resourcemanager-share.aliyuncs.com",
    "Name": "action"
  },
  "eventSource": "resourcemanager-share.aliyuncs.com",
  "sourceIpAddress": "42.120.XX.XX",
  "userIdentity": {
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-03-08T07:00:04Z"
      }
    }
  },
  "accountId": "123456789012****",
  "principalId": "111749508818****",
  "userName": "root",
  "type": "root-account"
},
"eventType": "ApiCall",
"serviceName": "ResourceManager",
"apiVersion": "2016-11-11",
"requestId": "B1CFCA37-83FA-4288-B623-01994CF8BDD2",
"eventTime": "2019-03-08T07:00:04Z",
"acsRegion": "cn-hangzhou",
"eventName": "CreateResourceGroup"
}
```

2.Tag

2.1. Design tags

2.1.1. Best practices for tag design

Tag design rules are management rules. We recommend that you plan and design tags based on the principles and best practices for tag design in this topic. This avoids business loss caused by frequent changes to tag design rules and helps you develop a tag management system that supports sustainable evolution.

Scenarios

Tags can be used to manage, categorize, and search for resources. The resources include personnel, finance, and cloud services. Tags can be used to perform the following operations:

- Search for and manage resources.
- Manage costs and cost allocation.
- Automate operations and maintenance (O&M).
- Control access to resources.

Design principles

The following content describes the design principles:

- **Mutual exclusivity**

This principle ensures that one resource attribute uses only one tag key. For example, if you have used the tag key `owner` to represent the owner attribute, you cannot use other tag keys such as `own` or `belongto` to represent this attribute again.

- **Collective exhaustion**

When you plan resources, you must plan tags and prioritize tag keys. All resources must be bound with planned tag keys and related values. Each key-value pair must be named in a standard format.

Collective exhaustion is a prerequisite for tag-based resource search, cost allocation, automated O&M, and access control.

- **Limited values**

This principle is used to remove excess tag values and retain only core tag values. It simplifies procedures such as resource management, access control, automated O&M, and cost allocation.

- **Considering consequences of future changes**

When you plan tags, you must consider the impact of adding or removing tag values that may have in the future. This provides extra flexibility to modify tags.

When you modify tags, tag-based access control, automated O&M, and related billing reports may change. For corporate or individual business, we recommend that you create business-related tags. This way, you can manage resources based on the tags from technical, business, and security dimensions. When you use automated O&M tools to manage resources and services, you can add automation-specific tags to facilitate automation.

- **Simplified design**

This principle allows you to simplify the use of tag keys by creating dimension-specific tag keys during the tag planning stage. It also reduces operation errors caused by excessive tag keys.

Examples

The following table lists the tag naming examples in common dimensions. We recommend that you use lowercase letters to name tags.

Dimension	Tag key	Tag value
Organization	<ul style="list-style-type: none"> • company • department • organization • team • group 	Organization-specific names
Business	<ul style="list-style-type: none"> • product • business • module • service 	Business-specific names
Role	<ul style="list-style-type: none"> • role • user 	<ul style="list-style-type: none"> • network administrator • application administrator • system administrator • O&M administrator • R&D personnel • test personnel
Purpose	<ul style="list-style-type: none"> • purpose • use 	Specific purposes
Project	<ul style="list-style-type: none"> • Project dimensions: <ul style="list-style-type: none"> ◦ project ◦ risk ◦ schedule ◦ subtask ◦ environment • Personnel dimensions: <ul style="list-style-type: none"> ◦ sponsor ◦ member ◦ owner ◦ creator 	Project-related values

Dimension	Tag key	Tag value
Business department (to implement cost allocation and business tracking)	<ul style="list-style-type: none"> • costcenter • businessunit • biz • financecontact 	Department-related values
Owner from the finance dimension (to identify the resource owner)	owner	Names or emails
Customer from the finance dimension (to identify the customers that use specific resources)	Custom values or true values	Customer names
Project from the finance dimension (to identify the projects that are supported by specific resources)	project	Project names
Order from the finance dimension	order	Order category IDs

2.2. Use tags to implement automated O&M

2.3. Use tags to control access to resources

2.3.1. Create a resource with a specific tag

You can attach a custom policy to a RAM user. This allows the RAM user to add specific tags to the 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 under 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 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	<ul style="list-style-type: none"> o ecs:DescribeTagKeys o ecs:ListTagResources o ecs:DescribeTags
Call the API operations that are used to query ECS resources	<ul style="list-style-type: none"> o ecs:DescribeKeyPairs o ecs:DescribeImages o ecs:DescribeSecurityGroups o ecs:DescribeLaunchTemplates o ecs:DescribeDedicatedHosts o ecs:DescribeDedicatedHostTypes o ecs:DescribeAutoSnapshotPolicyEx
Call the API operations that are used to query VPC resources	<ul style="list-style-type: none"> o vpc:DescribeVpcs o vpc:DescribeVSwitches

Permission	Parameter
Call the API operation that is used to pay for orders	<code>bss:PayOrder</code>
Not allowed to call the API operations that are used to manage tags	<ul style="list-style-type: none"> ◦ <code>ecs>DeleteTags</code> ◦ <code>ecs:UntagResources</code> ◦ <code>ecs>CreateTags</code> ◦ <code>ecs:TagResources</code>
Add a tag to a VPC	<code>"vpc:tag/user": "lisi"</code>

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 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 a VPC](#).

1. Log on to the [Resource Management console](#). The Tags page appears.
2. In the **Region** section, select a region.
3. Set **Tag Type** to **All Custom Tags**.
4. Click **Create/Bind Tags**. In the panel that appears, create the `user:lisi` tag and bind the tag to an existing VPC. For more information, see [Create and bind a tag](#).

Step 3: Create an ECS resource to which a specific tag is added

Log on to the ECS console by using the userTest RAM user and create an ECS instance to which a tag is 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. Click **Create Instance** in the upper-right corner.

 **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 to the instance, the instance cannot be created, and the **You are not authorized to create ECS instances** message appears.



What to do next

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](#).

2.3.2. 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 uses ECS instances to demonstrate how to attach a policy to a RAM user and how the user uses tags to control access to the ECS instances.

Prerequisites

A RAM user is created under 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 with the same characteristics from different dimensions. This simplifies resource management. You can add multiple tags to each cloud resource. For more information about cloud resources that support tags and the types of these resources, see [Alibaba Cloud services that support tags](#) 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 appear in the resource list. To control the resources that are accessible to a RAM user, create a custom policy, attach the policy to the user, and add tags to the resources.

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

In this step, 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 the RAM user must specify the `owner: zhangsan` and `environment: production` tags before the user accesses ECS resources.

1. Log on to the [RAM console](#) by using an Alibaba Cloud account.
2. For more information about how to create the UserTagAccessRes custom policy, 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"
}

```

Permission	Parameter	Description
------------	-----------	-------------

Permission	Parameter	Description
Access resources to which specific tags are added	<ul style="list-style-type: none"> "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	<ul style="list-style-type: none"> ecs:DescribeTagKeys ecs:DescribeTags 	You can query tags in the ECS console.
Not allowed to call the API operations that are used to manage tags	<ul style="list-style-type: none"> 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

In this step, use an Alibaba Cloud account to add tags to ECS instances.

Note If you do not have ECS instances, create an instance first. For more information, see [Creation method overview](#).

1. Log on to the [Resource Management console](#). The Tags page appears.
2. In the **Region** section, select a region.
3. Set **Tag Type** to **All Custom Tags**.
4. Click **Create/Bind Tags**. In the panel that appears, create the `owner:zhangsan` and `environment:production` tags and bind them to existing ECS instances. For more information, see [Create and bind a tag](#).

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

In this step, use the userTest RAM user who is attached with the UseTagAccessRes policy 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. No instances appear on the Instances page.

4. Specify tags to view resources.



2.4. 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 bound to your Elastic Compute Service (ECS) instances. For more information, see [Create and 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 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 the 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 the OOS custom template to modify the tag values of resources that support tags in the same region. You can modify the API operations in the template to apply it to various resources. For more information about resources that support tags, see [Alibaba Cloud services that support tags](#). For more information about OOS supported resources, see [List of supported cloud services](#).

Step 1: Create a 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 top navigation bar, select a region.
3. In the left-side navigation pane, click **My Templates**.
4. On the My Templates page, 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 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. Sample code:

```
{
  "Description": "Modify a tag value of multiple resources at a time",
  "FormatVersion": "OOS-2019-06-01"
```

```
"Formatversion": "2019-06-01",
"Parameters": {
  "operateld": {
    "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": {
      "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": {}  
}
```

8. Click **Create Template**.

Step 2: Execute the custom template


You can perform the following steps to execute the created template to modify a tag value of multiple resources.

1. In the left-side navigation pane, click **My Templates**.
2. Find the created 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 parameters and click **Next: OK**.

You must configure the following parameters in this step:

- **operatedId**: the operation ID, which is used to identify an operation. You can enter an operation ID.
 - **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 accordingly.

2.5. 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 [Alibaba Cloud services that support tags](#).


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, if you want to add a tag to multiple security groups, 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 AliyunOSSFullAccess 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 top navigation bar, select a region.
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 Templates** tab, select **Empty Templates**, and click **OK**.
 - iii. On the Create Template page, click the **YAML** tab and edit the template. In the Basic Information section, enter OOSAutoBindTag in the Template Name field. After you edit the

template, click **Create Template**.

Sample code:

```
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: getInstanceByTags
    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_InstanceIds
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: creates tags and binds them 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 parameters and click **Next: OK**.

The following parameters are configured in this example:


 - tags: Select the tag `owner:zhangsan`.
 - regionId: Select the region 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 accordingly.

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

A key link for enterprises to implement automated operations and maintenance (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: Create and bind tags to ECS instances

In the ECS console or on the Tags page of the Resource Management console, create the `business:bigdata` tag and bind it to ECS instances. The following content uses the Tags page of the Resource Management console to describe the preceding operations:

1. Log on to the [Resource Management console](#). The Tags page appears.
2. Select a region for **Region**.
3. Set **Tag Type** to **All Custom Tags**.
4. Click **Create/Bind Tags**. In the Create/Bind Tags pane, create the `business:bigdata` tag and bind it to existing ECS instances. For more information, see [Create and bind a 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 targets to ECS instances that are bound with the `business:bigdata` tag.

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 RegionID parameter in the ACS::ExecuteAPI action. We recommend that you do not use this method. Keep the region of OOS the same as the region of the ECS instance that is specified in [Step 1: Create and bind 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 be automatically executed.
 - 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. In the left-side navigation pane, click **Executions**. On the page that appears, click the **Instance List** tab. On this tab, view execution results.

All ECS instances that are bound with the `business:bigdata` tag are started.



2.7. Use Cloud Config to search for resources that are not bound with specific tags

This topic describes how to use Cloud Config to search for resources that are not bound with specific tags. Cloud Config facilitates resource management.

Prerequisites

Make sure that your resource tags comply with the principles for tag design. For more information, see [Best practices for tag design](#).

Procedure

1. Log on to the [Cloud Config console](#).
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, click **Create Rule**.
4. In the **Basic Settings** step, set **Method** to **Managed Rule**, set **Managed rule** to **required-tags**, and specify **Risk Level**. Then, click **Next**.
5. In the **Parameter Settings** step, select the types of the resources that you want to monitor. In this example, ECS, EIP, OSS, and RDS are selected.
6. In the **Parameter Settings** section, specify thresholds for input parameters. Then, click **Next**. In this example, three thresholds are specified. One indicates the project that is supported by resources, one indicates the resource owner, and another indicates the environment in which the resources are running. The following figure shows the thresholds.



Note

- A threshold is a tag key-value pair that is used to search for resources.
- You can specify multiple thresholds. If a threshold is not reached, Cloud Config considers the resources **non-compliant**.

7. In the **Correction Settings** step, select **Disable Correction** and click **Submit**.
8. In the **Complete** step, click **View Details**.
9. On the **Rule Details** tab, view audit results. Cloud Config identifies the resources that are not bound with specific tags. The following figure shows the resources.

