ALIBABA CLOUD

Alibaba Cloud

Resource Management
Best Practices

Document Version: 20220621

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.Resource sharing

1.1. Use a resource directory to share a VPC with multiple Alibaba Cloud accounts

1.1.1. Overview

You can use a resource directory to manage multiple accounts and share a virtual private cloud (VPC) with these accounts.

Background information

As cloud computing becomes popularized, an increasing number of enterprises deploy services in the cloud and purchase more and more cloud resources. An issue arises: How can enterprises manage cloud resources in an efficient manner? Enterprises have high requirements for the division of business, business isolation, and multiple payment methods. The single-account mode can no longer support the sustainable development of enterprises. To resolve this issue, enterprises can use the multi-account mode to meet business development requirements. However, the following issues may arise during the use of the multi-account mode:

- **Management of multiple accounts**

  Enterprises may not be able to manage multiple isolated Alibaba Cloud accounts in a centralized manner. Therefore, more refined management is required.

- **Communication among multiple accounts**

  Enterprises can use Cloud Enterprise Network (CEN) to connect VPCs that belong to different accounts. This way, cloud resources within different accounts can communicate with each other. However, as the business complexity increases, the following issues may occur:

  - Complex network O&M due to isolated deployment of network resources

    The network of an enterprise can be large and complex because the network resources may be deployed and managed by different accounts. As a result, it is difficult for O&M personnel to manage an enterprise network in a centralized manner.

  - Increased costs due to frequent network resource configurations

    O&M and instance costs increase due to frequent VPC configurations by different accounts.

  - Increased network complexity due to an increasing number of VPCs

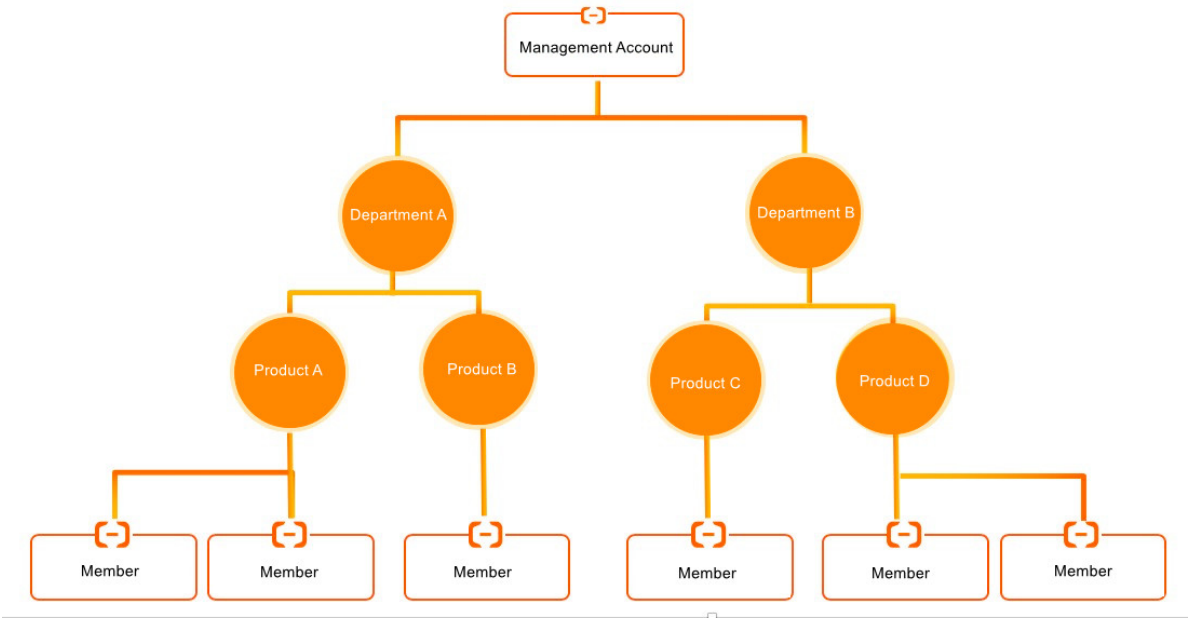
    To meet business requirements, more and more VPCs need to be deployed. As a result, issues such as complex network, difficult management, and resource quota limits arise. For example, the number of VPCs attached to a CEN instance may reach the upper limit.

Solution

Alibaba Cloud offers the Resource Directory service to facilitate the management of multiple accounts and offers the Resource Sharing service and VPC sharing feature to facilitate communication among multiple accounts. The following descriptions provide details:

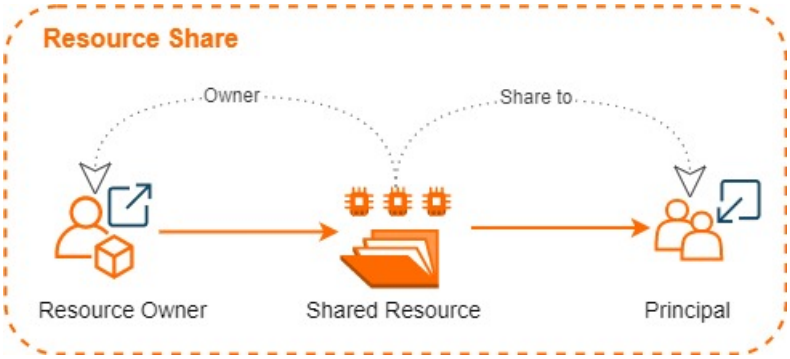
- **Use Resource Directory to manage multiple accounts**

  The Resource Directory service provided by Alibaba Cloud allows you to manage the relationships among multiple levels of resources and accounts. You can enable a resource directory and create folders in the resource directory based on the organizational structure or business form of your enterprise. Then, you can consolidate the accounts used by your enterprise into the resource directory to establish multi-level relationships for the accounts and the resources within the accounts. This way, you can manage the accounts and resources in a centralized manner based on the relationships. In addition, your requirements for finance, security, audit, and compliance can be met. For more information, see Resource Directory.



- **Use Resource Sharing to share resources with members within the same resource directory**

  The Resource Sharing service provided by Alibaba Cloud allows you to share resources with one or more members within your resource directory. To use this feature, create a resource share and add the resources and members to the resource share. For more information, see Resource Sharing overview.

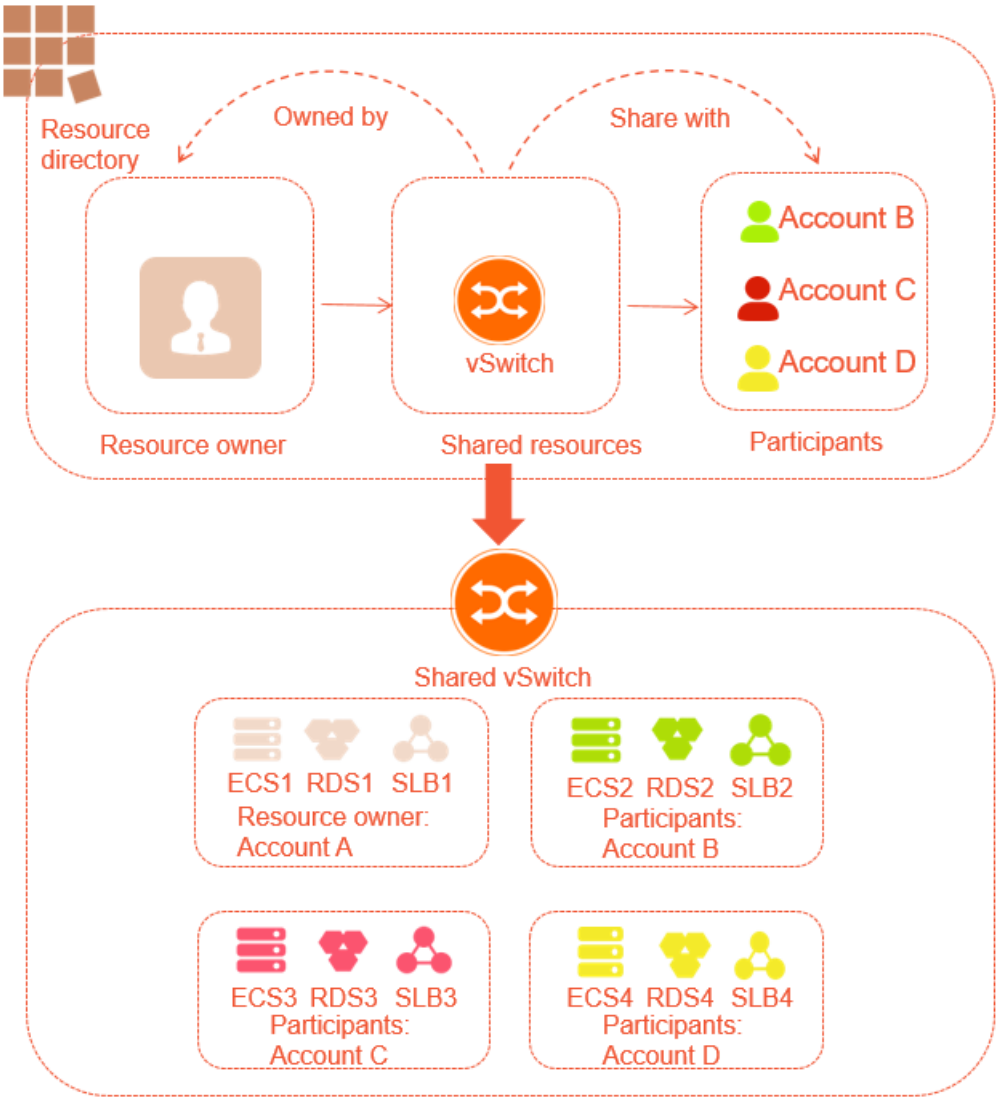


Term	Description
resource share	A resource share is an instance of the Resource Sharing service. It is also a cloud resource and has a unique ID and an Alibaba Cloud Resource Name (ARN). A resource share consists of a resource owner, principals, and shared resources.

Term	Description
resource owner	A resource owner initiates resource sharing and owns shared resources. It is the management account or a member of a resource directory.
principal	A principal shares the resources of resource owners. It has specific operation permissions on the shared resources. A principal is a member of a resource directory. Multiple principals can share the same resource. **Note** The operation permissions of each principal on the shared resources are determined based on the Alibaba Cloud service to which the resources belong. For example, the operation permissions of principals on the shared vSwitches in a VPC are determined based on the VPC service. For more information, see Permissions related to VPC sharing.
shared resource	A shared resource is a resource of an Alibaba Cloud service.
resource sharing	Resource sharing allows you to share your resources with all members in your resource directory, all members in a specific folder in your resource directory, or a specific member in your resource directory. For more information, see Enable resource sharing.

- **Share a VPC with members within the same resource directory**

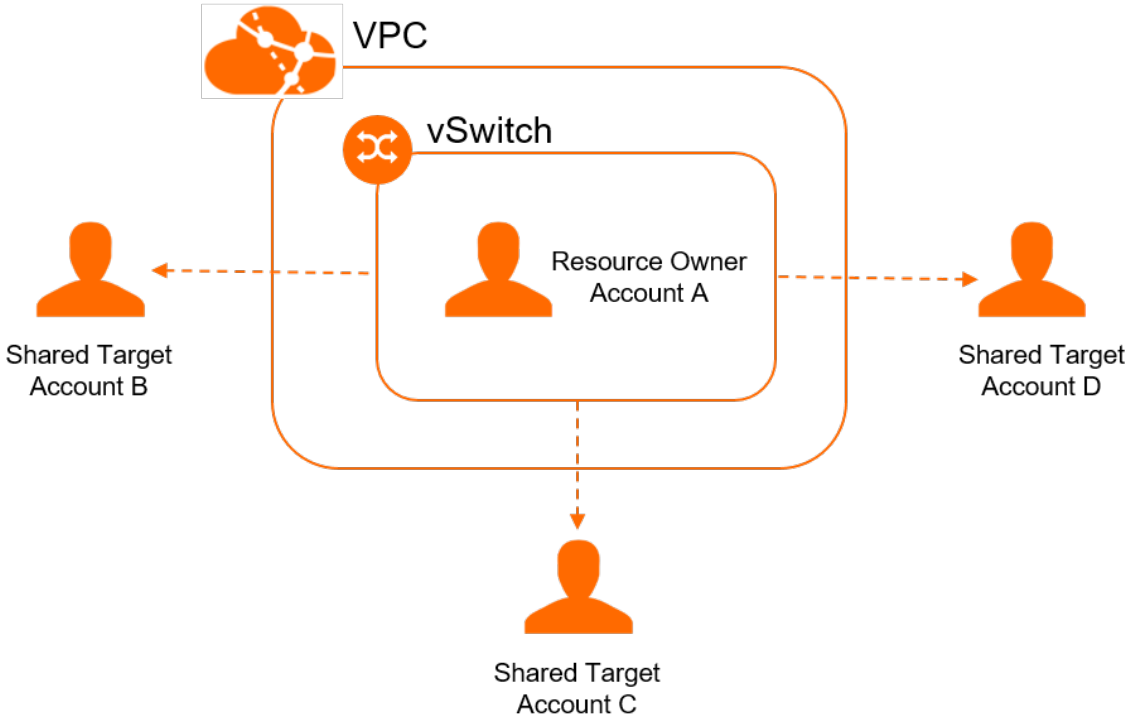
  You can use the Resource Sharing service to share the vSwitches in a VPC that belongs to a member (resource owner) with other members (principals) within the same resource directory. This way, the principals can create resources, such as Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, and ApsaraDB RDS instances, in the shared VPC. By default, after a vSwitch is shared, principals can use the shared vSwitch without confirmation, and the resources created by the resource owner and principals can communicate with each other within the shared VPC. For more information, see Overview of VPC sharing.



The following figure and descriptions provide details about how a VPC is shared.

- **vSwitch sharing among multiple accounts**

  You can share a vSwitch in a VPC with multiple accounts without the need to configure a VPC for each account. This reduces the number of VPCs.



- **Permissions of the resource owner and principals**

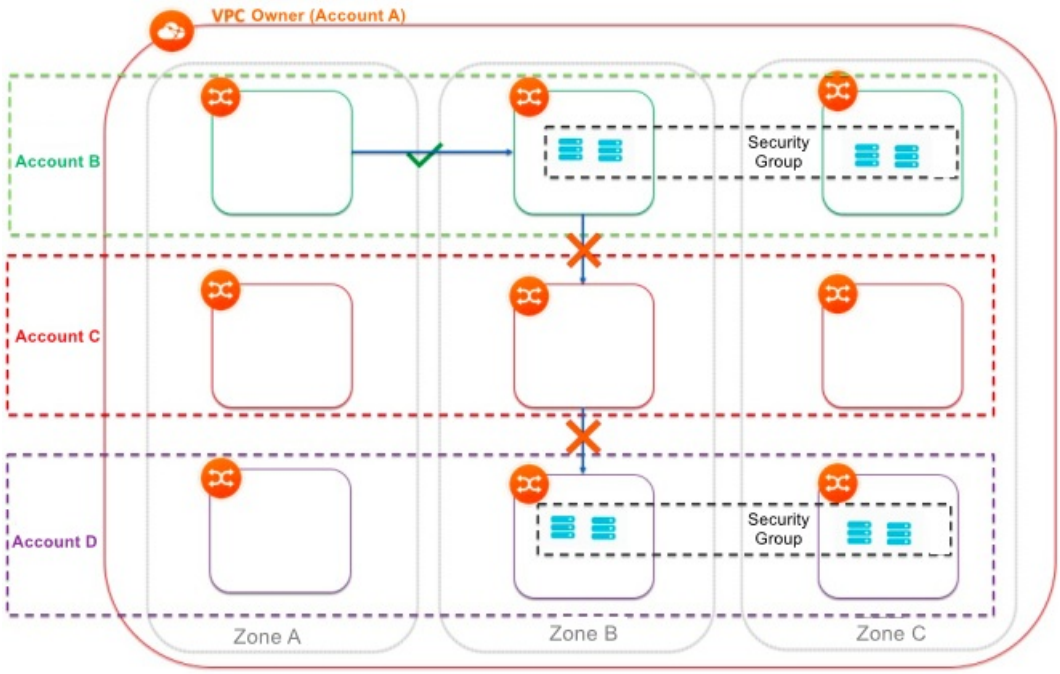
  The following table describes the permissions of the resource owner and principals on the cloud resources that belong to the shared vSwitch.

  The following table describes the permissions of the resource owner and principals on other network resources.

- **Isolation**

  If you share vSwitches in the same VPC with different accounts, the vSwitches can communicate with each other by default. If you want to isolate the vSwitches in some scenarios, use one of the following methods:

  - Configure a network access control list (ACL) to isolate the vSwitches.
  - Configure a security group to isolate the instances that belong to the vSwitches. You can use security groups that belong to other accounts.

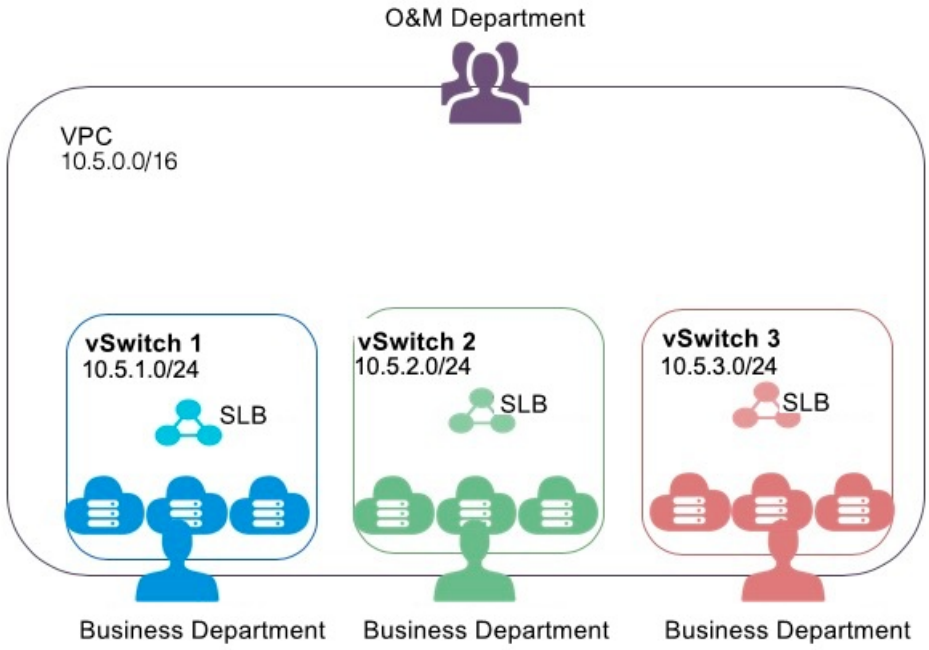


> **Note** You can configure ACL rules to isolate instances that belong to different vSwitches. However, if you want to isolate instances that belong to the same vSwitch, you can configure security group rules for the instances. You can use security groups that belong to other accounts. To isolate networks between different vSwitches and different accounts, configure source and destination IP addresses in security groups.

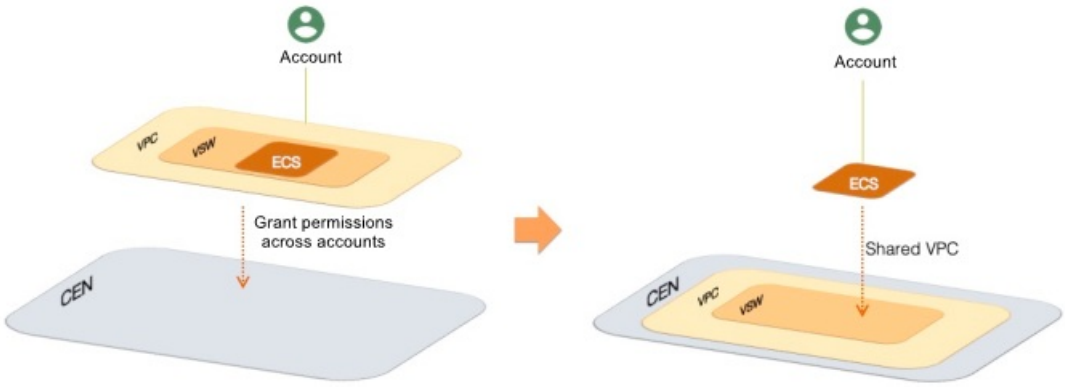
Benefits

The solution has the following benefits:

- The O&M department can plan, configure, and manage VPCs in a centralized manner. In addition, the O&M department can share the vSwitches in the VPCs with the business department.



- The business department can view and manage only the resources that belong to the shared vSwitches. In addition, the business department can create resources in the shared vSwitches or delete resources from the shared vSwitches, such as cloud instances and databases, based on business requirements.



- In this solution, your enterprise uses a unified network architecture and security policy. This allows the business department to focus on business requirements.
- You can use the network and security capabilities as a service for the business department, and standardize the O&M system. This improves the IT efficiency throughout your enterprise.

1.1.2. Procedure

In a resource directory, the vSwitches in a virtual private cloud (VPC) within a member (resource owner) can be shared with another member (principal). This topic describes how a resource owner shares vSwitches with other members.

Limits

Make sure that you understand the limits on shared VPCs. For more information, see Limits.

Step 1: Use a resource directory to manage multiple accounts

The Resource Directory service provided by Alibaba Cloud allows you to create members in your resource directory or invite accounts to join your resource directory as members. This way, you can manage all members in the resource directory in a centralized manner.

1. Enable a resource directory.

   For more information, see Enable a resource directory.

2. Use the management account of the resource directory to create folders based on the organizational structure of your enterprise.

   For more information, see Create a folder.

3. Use the management account of the resource directory to create members in the resource directory or invite accounts to join the resource directory as members.

   For more information, see Create a member or Invite an Alibaba Cloud account to join a resource directory.

Step 2: Enable resource sharing

1. Use the management account of your resource directory to log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Sharing > Configure**.
3. On the Settings page, click **Enable**.
4. In the **Service-linked Role for Resource Sharing** dialog box, click **OK**.

   The system creates a service-linked role named AliyunServiceRoleForResourceSharing to obtain the organizational structure of the resource directory. For more information, see Service-linked role for Resource Sharing.

Step 3: Create a resource share as the resource owner

Create a resource share in the Resource Management console. Then, add the VPC resources that you want to share and the accounts with which you want to share the resources to the resource share.

1. Create a resource share. Then, add the VPC resources that you want to share and the accounts with which you want to share the resources to the resource share.
   i. Log on to the Resource Management console.
   ii. In the left-side navigation pane, choose **Resource Sharing > Resources I Share**.
   iii. In the top navigation bar, select the region where the VPC resources that you want to share are deployed.
   iv. On the page that appears, click **Create Resource Share**.
   v. On the **Create Resource Share** page, enter a name for the resource share in the **Resource Share Name** field. For example, you can enter Finance_VPC.
   vi. In the **Select Shared Resource** section, select the resource type and resource IDs, and click **Add**. For example, you can select the vSwitch type and select the ID vsw-bp183p93qs667muql****.

vii. In the **Add Principal** section, configure the Add Mode parameter and add principals. For example, you can add the principal whose ID is 177242285274****

- Add from Resource Directory

  > **Note** This mode can be used only by the management account of the resource directory.

  Select principals from the resource directory.

  - If you select the Root folder, the added resources are shared with all members in the resource directory.
  - If you select a folder other than the Root folder, the added resources are shared with all members in the selected folder.
  - If you select a member, the added resources are shared only with the member.

- Add Manually

  Configure the Principal Type parameter, specify a folder or member ID if required, and then click **Add**. You can select one of the following options from the Principal Type drop-down list:

  - **Resource Directory**: If you select this option, the ID of the current resource directory is automatically displayed for the Resource Directory ID parameter that appears. In this case, the added resources are shared with all members in the resource directory.
  - **Folder**: If you select this option, you must enter a folder ID in the Folder ID field that appears. In this case, the added resources are shared with all members in the folder.
  - **Alibaba Cloud Account**: If you select this option, you must enter a member ID. In this case, the added resources are shared only with the member.

viii. Click **OK**.

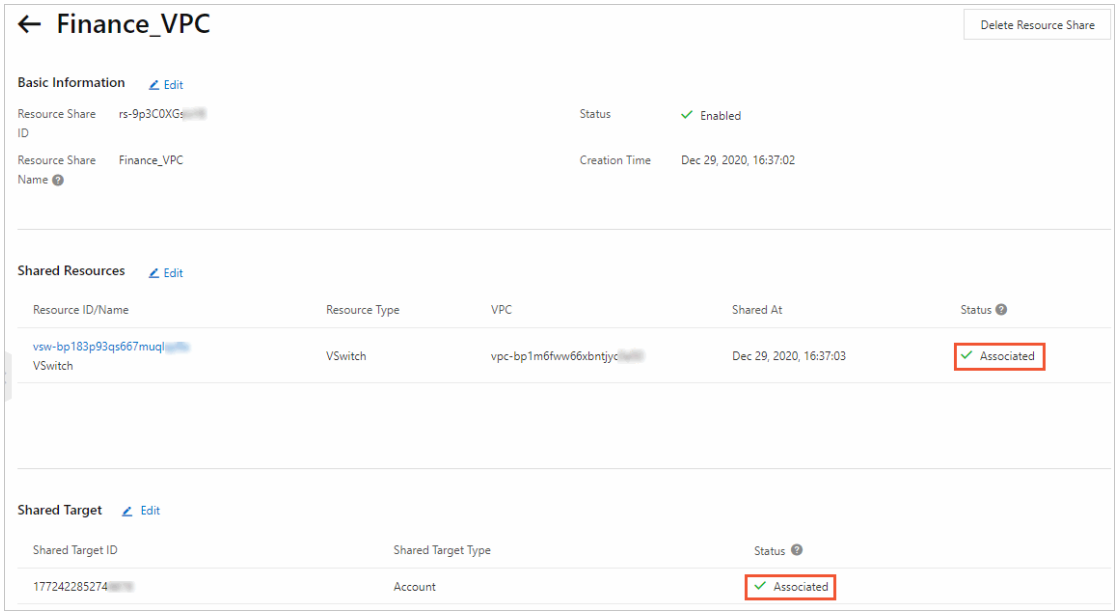
2. View the details about the resource share.

   i. On the Resources I Share page, view the following information of the resource share: **Resource Share ID/Name**, **Status**, and **Creation Time**.

   If the resource share is in the **Enabled** state, it is created.

ii. Click the ID of the resource share to view its detailed information.

If **Associated** is displayed in the Status columns of the **Shared Resources** and **Principals** sections, the resources that you want to share and the accounts with which you want to share the resources are added to the resource share.



3. (Optional) Modify the information of the resource share.

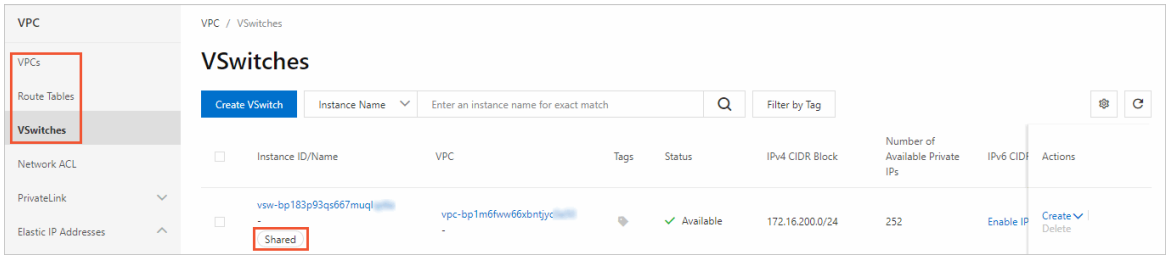
On the details page of the resource share, you can click **Edit** in each section to change the resource share name, add or remove shared resources, or add or remove principals. For more information, see Change the name of a resource share, Add or remove a shared resource, or Add or remove a principal.

Step 4: View and use the shared vSwitches as a principal

By default, after the resource owner shares a vSwitch, a principal can use the shared vSwitch without confirmation. Principals can view the vSwitches that other accounts share with them. They can also create cloud resources, such as Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, and ApsaraDB RDS instances, in the shared vSwitches.

1. Log on to the Resource Management or VPC console to view the shared vSwitches. In this example, the member 177242285274**** is used to log on to the VPC console to view the shared vSwitch vsw-bp183p93qs667muql****.

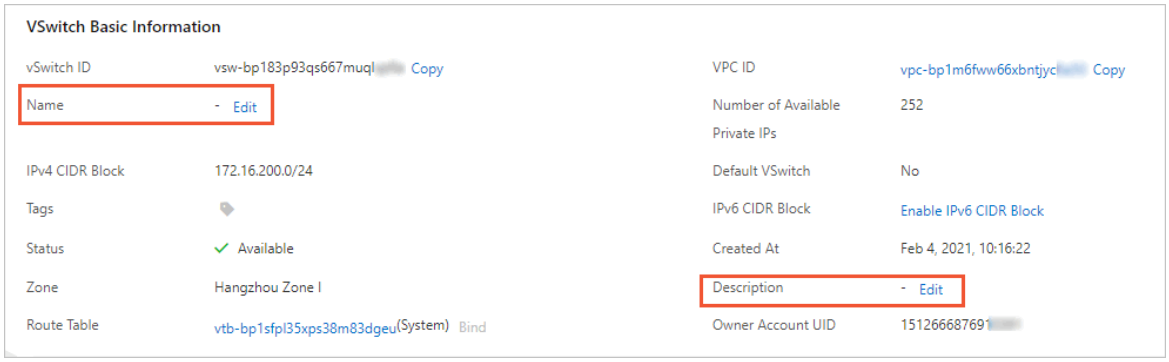
> **Note** A principal can log on to the Resource Management or VPC console to view shared vSwitches. For more information about how to view shared vSwitches, see View shared vSwitches.



> **Note** When a resource owner shares vSwitches, the VPC console generates records of shared VPCs, route tables, and vSwitches due to network requirements.

2. In the VPC console, change the name and description of the shared VPC, route table, and vSwitch.

> **Note** The preceding information is exclusive to you and cannot be viewed or changed by the resource owner.



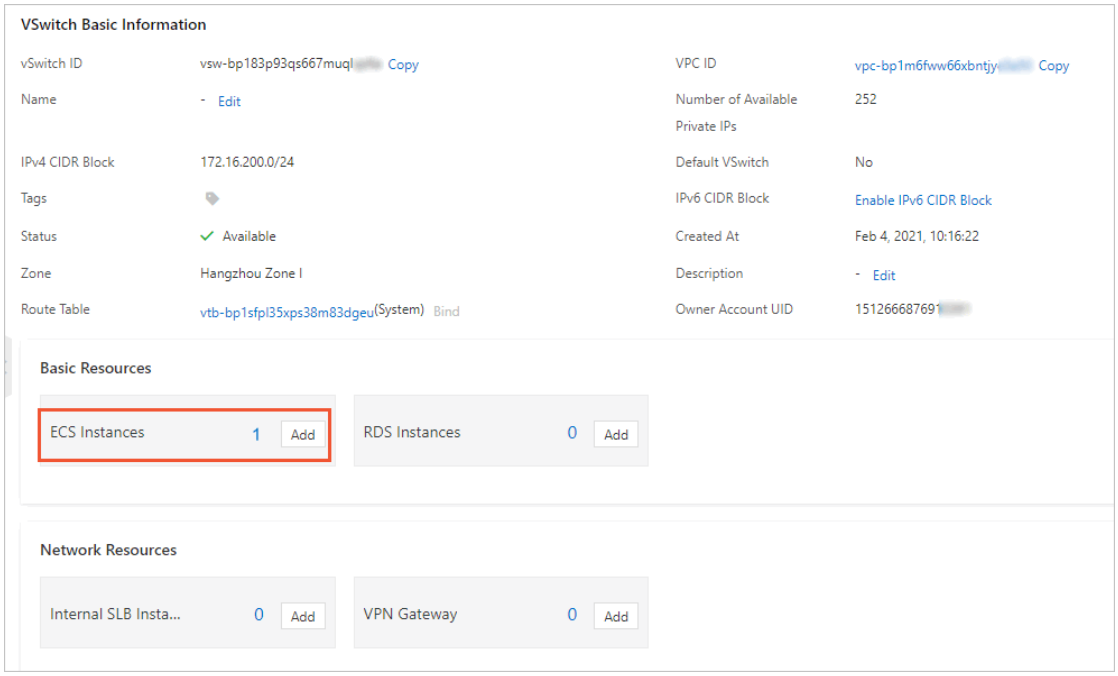
3. Create a cloud resource in the shared vSwitch.

   i. On the **vSwitch** page, find the shared vSwitch, move the pointer over **Create** in the **Actions** column, select the type of resource that you want to create, and then create a cloud resource.

> **Note** You can also create cloud resources in the consoles of the related Alibaba Cloud services. When you configure networks for the resources, select the shared vSwitch.

   ii. View the cloud resource that is created in the shared vSwitch.

   Principals can view the cloud resources that are created in the shared vSwitches in the VPC console or in the consoles of the related Alibaba Cloud services. The following figure shows the cloud resource that is created in the shared vSwitch in the VPC console.



2.Resource group

2.1. Use RAM to create and authorize resource groups

This topic describes how to use Resource Access Management (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.

Context

A gaming enterprise is developing three gaming projects. Each project requires various cloud resources. The enterprise has an Alibaba Cloud account and more than 100 Elastic Compute Service (ECS) instances that belong to the Alibaba Cloud account.

The enterprise has the following requirements:

- 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 enterprise requires that each project receives separate bills.
- Shared bottom-layer network: The enterprise requires a shared bottom-layer network for its cloud resources.

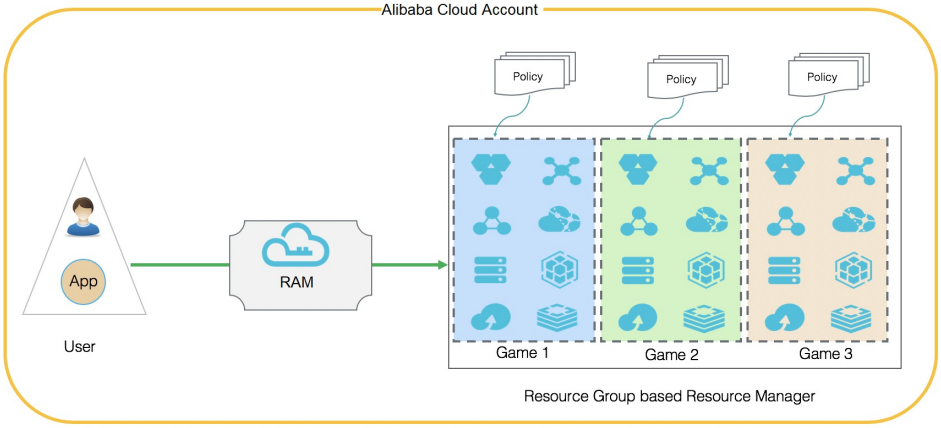
The enterprise has the following optional solutions:

- Multi-account solution
  - This solution supports independent project management. The enterprise 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. By default, each Alibaba Cloud account receives separate bills. The enterprise can use the consolidated billing feature provided by Alibaba Cloud to consolidate the bills and invoices of the multiple Alibaba Cloud accounts.
  - This solution does not support a shared bottom-layer network. The resources of different accounts are isolated between different networks. Virtual private clouds (VPCs) of the accounts can be connected by using peering connections. However, this leads to higher management costs.
- Single-account solution (with tagged resources)
  - This solution does not support independent project management. The enterprise 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 enterprise can tag its cloud resources by project. Then, each project can receive separate bills.
  - This solution supports a shared bottom-layer network. The enterprise can use tag-based RAM policies to authorize RAM users to access a group of resources. These resources belong to the same Alibaba Cloud account, and the enterprise does not need to pay for peering connections.
- 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 Alibaba Cloud account and can share a VPC. The enterprise does not need to pay for peering connections. This helps reduce management costs.

Solution

The resource group-based management solution can meet all requirements of the enterprise. This solution allows the enterprise to create three resource groups that correspond to the three projects by using one Alibaba Cloud account.



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 show how to specify a RAM user as a resource group administrator. The RAM user Alice is used as an example.

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. In the **Create Resource Group** panel, specify **Resource Group Name** and **Display Name**, and click **OK**.

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

5. Find a resource group that you created and click **Manage Permission** in the **Actions** column.
6. On the **Permissions** tab of the page that appears, click **Grant Permission**.
7. In the **Principal** field of the **Grant Permission** panel, enter `Alice@secloud.onaliyun.com`.
8. In the Authorization Policy Name column of the Select Policy section, click `AdministratorAccess`.
9. Click **OK**.

10. Click **Complete**.

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

Result

Alice, Bob, and Charlie are the 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 resource group on which the administrator has permissions. The administrator can also create and manage ECS instances.
- After an administrator logs on to the Resource Management console, the administrator can manage the RAM users, RAM user groups, and RAM roles in a resource group on which the administrator has permissions.

2.2. View billing statements by resource group

To manage billing statements by resource group after you create resource groups, you can create cost centers and map 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 within 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 desired resource groups.

   For more information, see Transfer resources across resource groups.
2. Create cost centers.
   i. In the top navigation bar of the Resource Management console, choose **Expenses > User Center**.
   ii. In the left-side navigation pane, choose **Corporate Finance > Cost Center**.
   iii. In the navigation tree, click **Add** to create cost centers.

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

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

   > **Notice** The information of resource groups is not synchronized to cost centers in real time. If you add resources to a resource group for the first time or have changed 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 the resources that are allocated to the cost center.
4. View billing statements by cost center.
   i. In the left-side navigation pane of the **User Center**, choose **Spending Summary > Spending Summary**.
   ii. On the page that appears, click the **Details** tab. On this tab, filter billing statements by cost center and view the billing statements of each resource group.

Related information

-
- Cost center

2.3. 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": "1234567890120****",
  "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"
}
```


2.4. Use a resource group to manage an ECS instance

This topic describes how to add an Elastic Compute Service (ECS) instance to a resource group and authorize a Resource Access Management (RAM) user to view and manage the ECS instance in the resource group.

Procedure

In this example, the RAM user Alice is authorized to view and manage only the ECS instance i-001. You can add the ECS instance to a resource group and grant the permissions on the resource group to Alice.

1. Log on to the RAM console and create a RAM user named Alice.

   For more information, see Create a RAM user.

2. Log on to the Resource Management console and create a resource group named ECS-Admin.

   For more information, see Create a resource group.

3. In the Resource Management console, add the ECS instance i-001 to the resource group ECS-Admin.

You can use one of the following methods to add the ECS instance to the resource group:

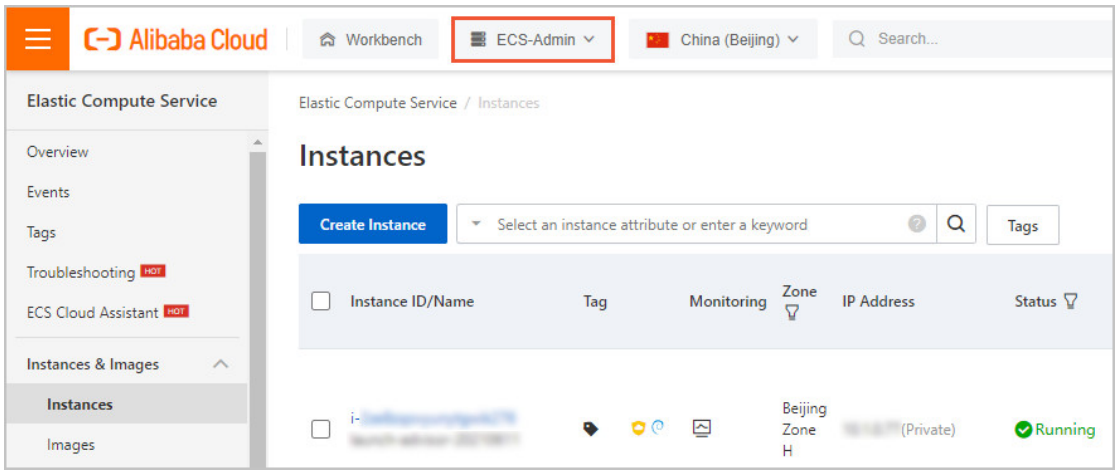
- Add the ECS instance to the resource group when you create the instance. For more information, see Create an instance by using the wizard.
- Move the ECS instance to the resource group. For more information, see Transfer resources across resource groups.

4. In the RAM console, grant the required permissions to Alice.

   In this step, set Authorization Scope to Specific Resource Group, enter ECS-Admin in the field below, enter Alice in the Principal field, and then select the system policy AliyunECSFullAccess. For more information, see Grant permissions to a RAM user.

   > **Note** If you want to authorize Alice only to view the ECS instance, select the system policy AliyunECSReadOnlyAccess in this step.

5. Log on to the ECS console and view and manage the ECS instance.
   i. In the left-side navigation pane, choose **Instances & Images > Instances**.
   ii. In the top navigation bar, select the resource group ECS-Admin.



   iii. On the Instances page, view the information about the instance and manage the instance.

2.5. Example of the RAM policy for resource groups

This topic provides an example of the Resource Access Management (RAM) policy for resource groups.

The following policy defines that you are allowed to create and delete resource groups, and view and modify the basic information about resource groups in Resource Management.

```
{
    "Statement": [{
        "Action": "ram:*ResourceGroup*",
        "Effect": "Allow",
        "Resource": "*"
    }],
    "Version": "1"
}
```

> **Note** If you want to authorize a RAM user to perform more group-related operations, such as managing resources in a resource group, granting permissions to a resource group, or migrating resources across resource groups, you must attach other policies to the RAM user. For more information, see Resource Group.

3.Tag

3.1. Design and manage tags

3.1.1. Best practices for tag design

This topic describes the background information, principles, best practices, and examples of tag design.

Background information

If your enterprise has only a few or a dozen cloud resources, you can easily classify the resources. However, as your business develops, your enterprise may have tens of thousands of resources. In this case, it becomes difficult and unreliable to manually classify resources. As a result, a platform is required to resolve this issue.

We recommend that you use tags to classify your resources. When a user creates a resource, the user must add a tag to the resource to indicate the attribute of the resource, such as the business or finance attribute. For example, when a user creates a resource, the user adds a tag to the resource to indicate the creator, region, or project of the resource. This facilitates resource management.

Principles

- **Mutual exclusivity**

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

- **Collective exhaustion**

  This principle requires that you plan tag keys and tag values for resources that belong to different branches, departments, or projects. For example, Company A has three gaming project departments and plans to use the tag key **project** for the resources that belong to these departments. In this case, the company must plan at least three tag values to distinguish between the departments. In addition, all the resources of the company must be marked with the planned tag keys and tag values.

  Collective exhaustion is a prerequisite for tag-based resource searches, cost allocation, automated operations and maintenance (O&M), and access control.

- **Limited values**

  This principle is used to retain only core tag values and remove excess tag values. For example, Company A has five departments. In this case, the company can have only one tag for each department to facilitate management.

  This principle simplifies procedures such as resource searches, cost allocation, automated O&M, and access control.

- **Consideration of future consequences**

When you plan tags, you must consider the impact of adding or removing tag values in the future. In addition, make sure that you can easily identify service types by using the planned tags. This enables extra flexibility to modify tags. For example, Company A uses the tag key **department** to manage resource ownership, finance ownership, and automated O&M for departments in the early days of data migration to the cloud. However, as business develops, this tag key cannot be used to easily distinguish resources. Therefore, we recommend that enterprises evaluate the business requirements for tags in the early days of data migration to the cloud. In the preceding example, the company can plan to use the following tag keys: **department**, **costcenter**, and **ops**.

If you modify tags, tag-based access control, automated O&M, or 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. If you use automated O&M tools to manage resources and services, you can add automation-specific tags to facilitate automation.

- **Simplified design**

  This principle is used to simplify the use of tags. When you design tags, simplify the values of tag keys and tag values. We recommend that you specify fixed values for tag keys and tag values to meet business requirements. For example, when you design tags to indicate test environments, use the tag key **test** for all types of test environments. Do not use different tag keys to indicate various types of test environments, such as **pretest** and **formal test**.

  This principle reduces the operation errors caused by excessive tag keys.

- **Standardized naming**

  This principle requires that tag keys and tag values be named in a standardized format that is compatible with various open source tools. This facilitates API integration in the future. For example, use lowercase letters to specify tag keys and tag values.

Best practices

An Internet company has three departments: business department, marketing department, and O&M department. Each department manages one or more projects. A production environment, a development environment, and a test environment are provided for different stages in the lifecycle of each project. The O&M department monitors resource usage in real time, periodically allocates costs for projects, controls access to resources in real time, and implements automated O&M.

The company designs tags based on the following requirements.

Requirement	Tag design description	Description
Search for and manage resources	Create and add the following tag keys for resources: • department: indicates the department to which a resource belongs. • project: indicates the project to which a resource belongs. • environment: indicates the type of the environment in which a resource runs.	If the organizational structure of your enterprise is more complex, you can use higher-level tag keys, such as company.

Requirement	Tag design description	Description
Manage and allocate costs	Create and add cost center tags for resources: • Tag key: **costcenter** • Tag values: **proj-1**, **proj-2**, **proj-3**, and **proj-4**	None.
Control access to resources	Prohibit personnel that are not the members of a project from accessing the resources that belong to the project, such as Elastic Compute Service (ECS) instances.	For more information, see Use tags to control access to ECS resources.
Implement automated O&M	Create the tag key **purpose** for routine resource inspections. You can create a tag value **autocheck-8am** for the tag key. This tag value indicates that an automated inspection is performed at 08:00 every day on the resources to which the tag is added. If an exception is detected during the inspection, the owner of the resource on which the exception occurs is notified based on the tag key **owner**.	None.

Examples

The following table lists some example tags from common dimensions.

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 • O&M administrator • R&D personnel • test personnel
Purpose	• purpose • use	Specific purposes

Project	• Project dimensions:
	  ◦ project
	  ◦ risk
	  ◦ schedule
	  ◦ subtask
	  ◦ environment
	• Personnel dimensions:
	  ◦ sponsor
	  ◦ member
	  ◦ 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
Customer from the finance dimension (to identify the customers that use specific resources)	Custom or actual 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

3.1.2. Best practices for tag management

You can add tags to resources when you activate Alibaba Cloud services. These tags facilitate resource management. This topic describes the methods that are used to manage tags in different scenarios. These methods are for reference only.

Scenario	Console	API operation
Manage cloud resources by using a multi-cloud management platform or self-developed management platform	None.	• Call the API operations of each Alibaba Cloud service. For more information about the API operations of the Alibaba Cloud services that support tags, see Services that work with Tag. • Call the unified Tag API operation TagResources.
Manage cloud resources by using the Alibaba Cloud Management Console	• Add tags to resources when you activate services. For more information, see the **Reference** column in Services that work with Tag. • Add and manage tags on the Tags page of the Alibaba Cloud Resource Management console.	

3.2. Use tags to allocate costs

3.2.1. Determine the ownership of existing resources

Many enterprises do not effectively manage their resources in the early days of data migration to the cloud. As their business develops, the enterprises realize that standardized management of cloud resources is necessary for their business development. As a result, the issue of how the enterprises determine the ownership of the resources arises. This topic provides several methods for reference.

Method	Description
Determine the ownership of resources based on their names	If you customize names for resources when you create the resources, you can easily determine the ownership of the resources based on the names, such as **Business A-DEV-2020**.
Determine the ownership of resources based on their creators	If O&M engineers use different accounts to perform operations, you can determine the ownership of resources based on the creators of the resources. You can query the creator of a resource in the ActionTrail console or by calling an ActionTrail API operation. For more information, see Query events in the ActionTrail console or LookupEvents.

Method	Description
Determine the ownership of resources based on their regions	If resources for different services or branches are purchased in different regions, you can determine the ownership of the resources based on the regions. You can query the region where a resource resides in the ActionTrail console or by calling an ActionTrail API operation. For more information, see Query events in the ActionTrail console or LookupEvents.
Determine the ownership of resources based on the IP addresses of service requests	If different Classless Inter-Domain Routing (CIDR) blocks are planned for different services, you can determine the ownership based on the IP addresses of service requests. You can query the IP address of a service request in the ActionTrail console or by calling an ActionTrail API operation. For more information, see Query events in the ActionTrail console or LookupEvents.
Determine the ownership of resources based on inquiries	If you still cannot determine resource ownership by using the preceding methods, you can send resource claim notifications or sort resources with all departments or branches.

3.3. Use tags to implement automated O&M

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

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

Prerequisites

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

Context

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

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

Step 1: Create an OOS custom template

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

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

   The following code provides an example:

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

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

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

7. Click **Create Template**.

Step 2: Execute the custom template

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

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

   You must configure the following parameters in this step:

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

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

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

3.3.2. Use OOS to add tags to multiple resources

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

Context

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

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

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

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

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

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

   For more information, see Create a custom policy.

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

   The following policy is created:

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

3. Create the OOSServiceRole RAM role.

   For more information, see Create a normal service role.

4. Attach the custom policy OOSAutoBindTag to the RAM role.

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

5. Attach the system policy AliyunOOSFullAccess to the RAM role.

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

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

1. Log on to the OOS console.
2. In the left-side navigation pane, click **My Templates**.
3. In the top navigation bar, select a region.
4. Create a custom template.
   i. On the My Templates page, click **Create Template**.
   ii. In the **Basic Information** section, enter a name for your template, such as OOSAutoBindTag.
   iii. Click the **YAML** tab and write code for the template. Then, click **Create Template**.

   The following code provides an example:

   ```
   FormatVersion: OOS-2019-06-01
   Description: Tag Resources Without The Specified Tags
   ```

```
Description: Tag Resources Without The Specified Tags
Parameters:
  tags:
    Type: Json
    Description:
      en: The tags to select ECS instances.
    AssociationProperty: Tags
  regionId:
    Type: String
    Description:
      en: The region to select ECS instances.
  OOSAssumeRole:
    Description:
      en: The RAM role to be assumed by OOS.
    Type: String
    Default: OOSServiceRole
RamRole: OOSServiceRole
Tasks:
  - Name: getInstancesByTags
    Action: 'ACS::ExecuteAPI'
    Description: ''
    Properties:
      Service: ECS
      API: DescribeInstances
      Parameters:
        Tags: '{{ tags }}'
        RegionId: '{{ regionId }}'
    Outputs:
      InstanceIds:
        Type: List
        ValueSelector: 'Instances.Instance[].InstanceId'
  - Name: getAllInstances
    Action: 'ACS::ExecuteAPI'
    Description: ''
    Properties:
      Service: ECS
      API: DescribeInstances
      Parameters:
        RegionId: '{{regionId}}'
    Outputs:
      InstanceIds:
        Type: List
        ValueSelector: 'Instances.Instance[].InstanceId'
  - Name: TagResources_ECS_Instances
    Action: 'ACS::ExecuteAPI'
    Description:
      en: 'tag ecs instances, which are without the specified tags.'
    Properties:
      Service: ECS
      API: TagResources
      Parameters:
        Tags: '{{ tags }}'
        RegionId: '{{regionId}}'
        ResourceType: Instance
        ResourceIds:
```

```
          - '{{ACS::TaskLoopItem}}'
    Loop:
      MaxErrors: 100%
      Concurrency: 20
      Items:
        'Fn::Difference':
          - '{{ getAllInstances.InstanceIds }}'
          - '{{ getInstancesByTags.InstanceIds }}'
Outputs:
  InstanceIds:
    Type: List
    Value:
      'Fn::Difference':
        - '{{ getAllInstances.InstanceIds }}'
        - '{{ getInstancesByTags.InstanceIds }}'
```

Parameters:

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

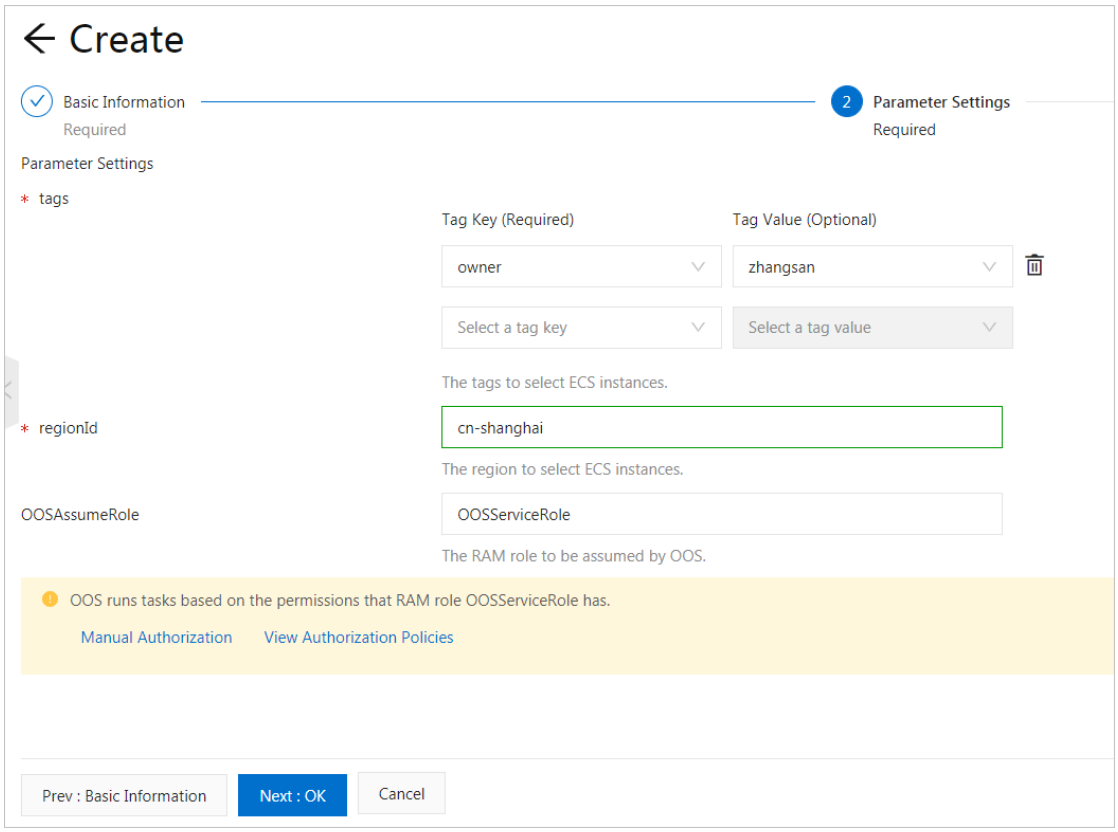
Permissions:

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

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

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

The following parameters are configured in this example:



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

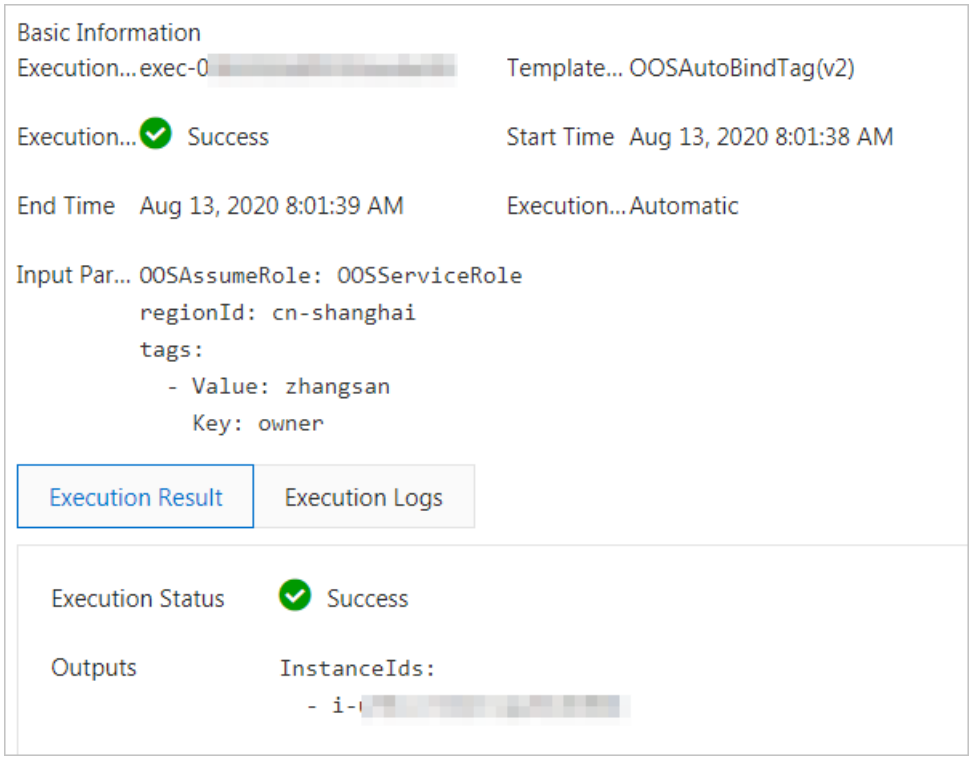
iv. Click **Create**.

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

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

vii. View the execution result.

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



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

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

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

Step 1: Add tags to ECS instances

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

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

   For more information, see Add a custom tag.

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

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

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

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

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

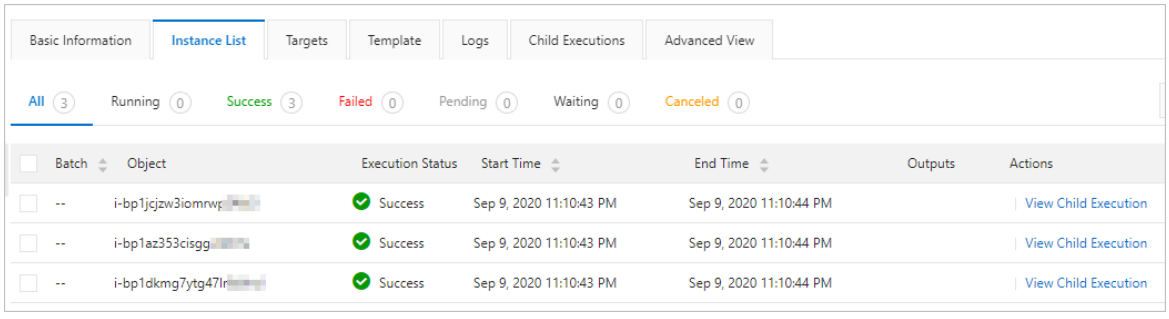
      The default value of Execution Mode is **Automatic**. This indicates that all tasks in the template will automatically run.

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

   iii. Click **Next: OK**.

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

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



3.3.4. Use OOS to add tags to resources associated with an ECS instance

Elastic Compute Service (ECS) instances are typically configured with resources such as cloud disks, elastic network interfaces (ENIs), and elastic IP addresses (EIPs). When you add tags to ECS instances, you can use Operation Orchestration Service (OOS) to automatically add the tags to the resources that are associated with the ECS instances. This ensures tag consistency between ECS instances and their associated resources and facilitates subsequent maintenance.

Context

In this topic, an OOS custom template is created to add the `owner:alice` tag to the cloud disk, elastic network interfaces (ENIs), and elastic IP addresses (EIPs) associated with an ECS instance.

> **Note** The OOS custom template, ECS instance, cloud disk, ENIs, and EIPs must reside in the same region.

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

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

   The following policy is created:

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

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

Permission	Parameter
Query the information of ECS instances, ENIs, and EIPs	`ecs:DescribeInstances`
Query the information of cloud disks	`ecs:DescribeDisks`
Add tags to ECS instances, cloud disks, and ENIs	`ecs:TagResources`

Permission	Parameter
Add tags to EIPs	`vpc:TagResources`

3. Create the OOSServiceRole RAM role.

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

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

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

Step 2: Create and execute an OOS custom template

1. Log on to the OOS console.
2. In the left-side navigation pane, click **My Templates**.
3. In the top navigation bar, select a region.
4. Create a custom template.
   i. On the My Templates page, click **Create Template**.
   ii. In the **Basic Information** section, enter a name for your template, such as AutoTag.
   iii. Click the **JSON** tab. Then, write code for the template and click **Create Template**.

   The following code provides an example:

```
{
  "FormatVersion": "OOS-2019-06-01",
  "Description": {
    "en": "When instance is labeled with the specified tag, Tags will be propagated
to the related resources.",
    "name-zh-cn": "zh-cn":
    "categories": [
      "event-trigger"
    ]
  },
  "Parameters": {
    "TagKey": {
      "Type": "String",
      "Description": "Tag key for tag instance"
    },
    "TagValue": {
      "Type": "String",
      "Description": "Tag value for tag instance"
    },
    "OOSAssumeRole": {
      "Description": {
        "en": "The RAM role to be assumed by OOS.",
      },
      "Type": "String",
      "Default": "OOSServiceRole"
    }
  },
```

```
  },
  "RamRole": "{{ OOSAssumeRole }}",
  "Tasks": [
    {
      "Name": "eventTrigger",
      "Description": {
        "en": "Monitor the ECS instance TAG event.",
      },
      "Action": "ACS::EventTrigger",
      "Properties": {
        "Product": "tag",
        "Name": [
          "Tag:ChangeOnResource"
        ],
        "Level": [
          "INFO"
        ],
        "Content": {
          "product": [
            "ecs"
          ],
          "resourceType": [
            "instance"
          ]
        }
      },
      "Outputs": {
        "instanceId": {
          "ValueSelector": ".content.resourceId",
          "Type": "String"
        },
        "isTag": {
          "ValueSelector": ".content.addedTags|select(.{{TagKey}}==\"{{TagValue}}\"
) |[.] |all|tostring",
          "Type": "String"
        }
      }
    },
    {
      "Name": "whetherNeedTag",
      "Action": "ACS::Choice",
      "Description": {
        "en": "Determine whether the tag needs to be propagated"
      },
      "Properties": {
        "DefaultTask": "describeInstancesFinally",
        "Choices": [
          {
            "When": {
              "Fn::Equals": [
                "true",
                "{{ eventTrigger.isTag }}"
              ]
            },
            "NextTask": "describeInstances"
```

```
          }
        ]
      }
    },
    {
      "Name": "describeInstances",
      "Action": "ACS::ExecuteAPI",
      "Description": {
        "en": "Query the instance to obtain the network interface and elastic publi
c network IP resources related to the instance."
      },
      "Properties": {
        "Service": "ECS",
        "API": "DescribeInstances",
        "Parameters": {
          "RegionId": "{{ ACS::RegionId }}",
          "InstanceIds": [
            "{{ eventTrigger.instanceId }}"
          ]
        }
      },
      "Outputs": {
        "eips": {
          "Type": "List",
          "ValueSelector": "Instances.Instance[].EipAddress.AllocationId"
        },
        "enis": {
          "Type": "List",
          "ValueSelector": "Instances.Instance[].NetworkInterfaces.NetworkInterface
[].NetworkInterfaceId"
        }
      }
    },
    {
      "Name": "describeDisks",
      "Action": "ACS::ExecuteAPI",
      "Description": {
        "en": "Obtain disk ids based on instance id."
      },
      "Properties": {
        "Service": "ECS",
        "API": "DescribeDisks",
        "Parameters": {
          "RegionId": "{{ ACS::RegionId }}",
          "InstanceId": "{{ eventTrigger.instanceId }}"
        }
      },
      "Outputs": {
        "diskIds": {
          "Type": "List",
          "ValueSelector": "Disks.Disk[].DiskId"
        }
      }
    },
```

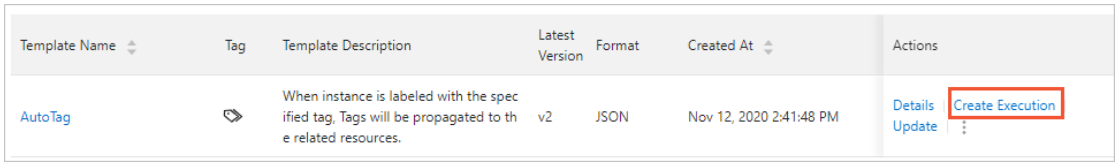
```
    {
      "Name": "tagResourcesDisks",
      "Action": "ACS::ExecuteAPI",
      "Description": {
        "en": "Tag disks"
      },
      "Properties": {
        "Service": "ECS",
        "API": "TagResources",
        "Parameters": {
          "RegionId": "{{ ACS::RegionId }}",
          "ResourceIds": [
            "{{ ACS::TaskLoopItem }}"
          ],
          "ResourceType": "disk",
          "Tags": [
            {
              "Key": "{{TagKey}}",
              "Value": "{{TagValue}}"
            }
          ]
        }
      },
      "Loop": {
        "RateControl": {
          "Mode": "Batch",
          "MaxErrors": 0,
          "Batch": [
            50
          ],
          "BatchPauseOption": "Automatic",
          "ConcurrencyInBatches": [
            1
          ]
        },
        "Items": "{{ describeDisks.diskIds }}"
      }
    },
    {
      "Name": "tagResourcesEnis",
      "Action": "ACS::ExecuteAPI",
      "Description": {
        "en": "Tag network interface."
      },
      "Properties": {
        "Service": "ECS",
        "API": "TagResources",
        "Parameters": {
          "RegionId": "{{ ACS::RegionId }}",
          "ResourceIds": [
            "{{ ACS::TaskLoopItem }}"
          ],
          "ResourceType": "eni",
          "Tags": [
```

```
            {
              "Key": "{{TagKey}}",
              "Value": "{{TagValue}}"
            }
          ]
        }
      },
      "Loop": {
        "RateControl": {
          "Mode": "Batch",
          "MaxErrors": 0,
          "Batch": [
            50
          ],
          "BatchPauseOption": "Automatic",
          "ConcurrencyInBatches": [
            1
          ]
        },
        "Items": "{{ describeInstances.enis }}"
      }
    },
    {
      "Name": "tagResourcesEips",
      "Action": "ACS::ExecuteAPI",
      "Description": {
        "en": "Tag eips"
      },
      "Properties": {
        "Service": "VPC",
        "API": "TagResources",
        "Parameters": {
          "RegionId": "{{ ACS::RegionId }}",
          "ResourceIds": [
            "{{ ACS::TaskLoopItem }}"
          ],
          "ResourceType": "eip",
          "Tags": [
            {
              "Key": "{{TagKey}}",
              "Value": "{{TagValue}}"
            }
          ]
        }
      },
      "Loop": {
        "RateControl": {
          "Mode": "Batch",
          "MaxErrors": 1,
          "Batch": [
            50
          ],
          "BatchPauseOption": "Automatic",
          "ConcurrencyInBatches": [
            1
```

```
            ]
          },
          "Items": "{{ describeInstances.eips }}"
        }
      },
      {
        "Name": "describeInstancesFinally",
        "Action": "ACS::ExecuteAPI",
        "Description": {
          "en": "Views the ECS instances Status."
        },
        "Properties": {
          "Service": "ECS",
          "API": "DescribeInstances",
          "Parameters": {
            "RegionId": "{{ ACS::RegionId }}",
            "InstanceIds": [
              "{{ eventTrigger.instanceId }}"
            ]
          }
        },
        "Outputs": {
          "status": {
            "Type": "String",
            "ValueSelector": "Instances.Instance[].Status"
          }
        }
      }
    ],
    "Outputs": {
      "instanceId": {
        "Value": "{{ eventTrigger.instanceId}}",
        "Type": "String"
      },
      "diskIds": {
        "Value": "{{ describeDisks.diskIds }}",
        "Type": "String"
      },
      "eips": {
        "Value": "{{ describeInstances.eips  }}",
        "Type": "String"
      },
      "enis": {
        "Value": "{{ describeInstances.enis  }}",
        "Type": "String"
      }
    }
}
```

5. Execute the custom template.

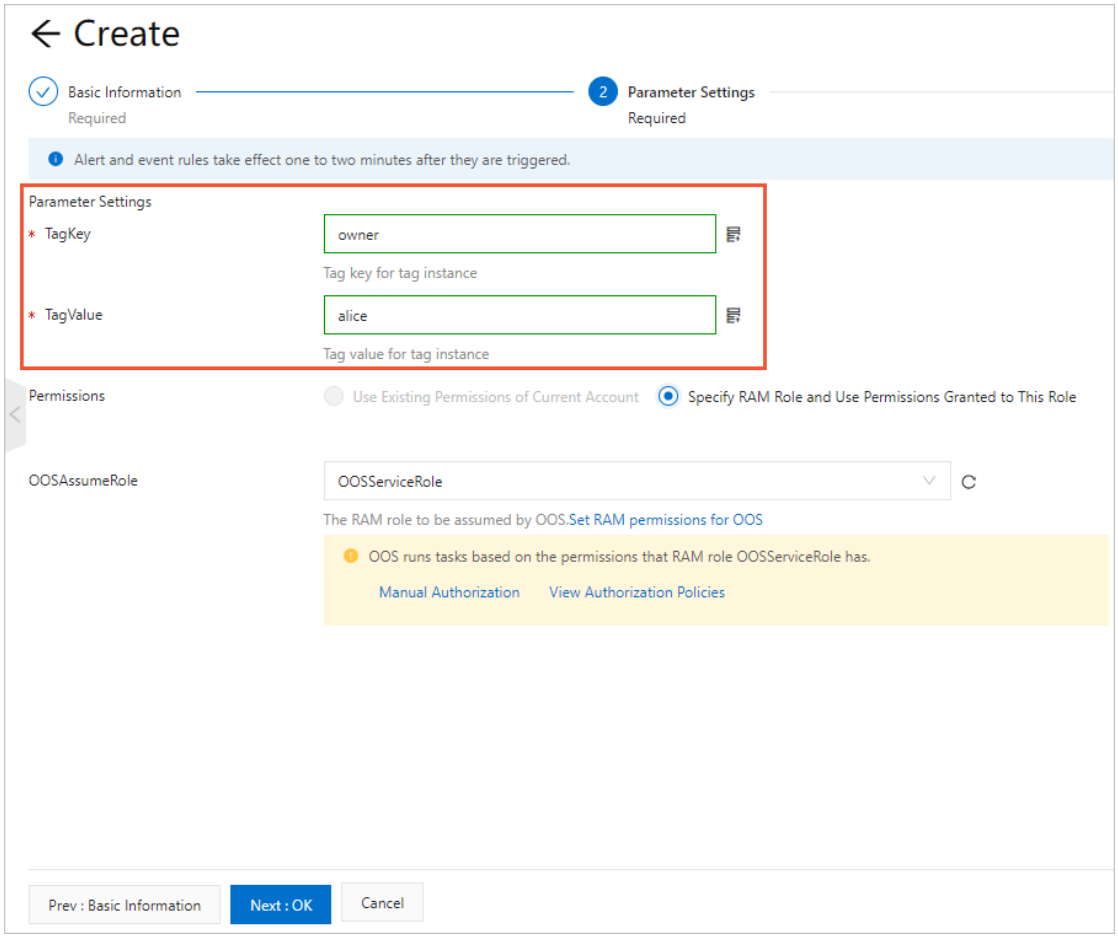
i. In the left-side navigation pane, click **My Templates**. On the My Templates page, find the AutoTag custom template that you created, and click **Create Execution** in the **Actions** column.



ii. In the Basic Information step, keep the default values and click **Next: Parameter Settings**.

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

The following parameters are configured in this example:



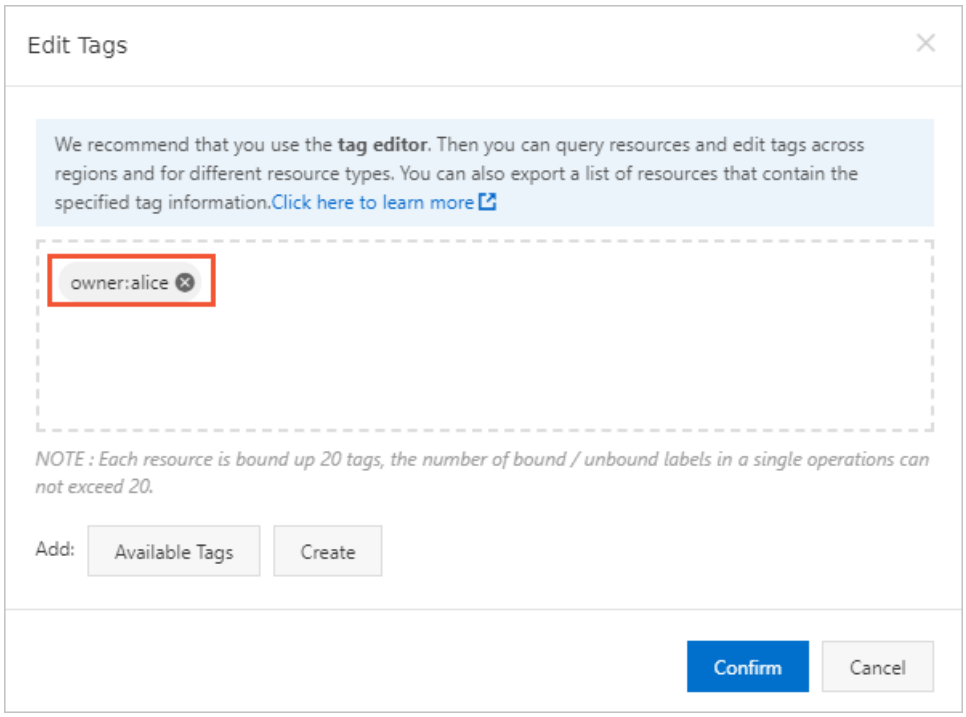
- TagKey: Enter the tag key `owner`.
- TagValue: Enter the tag value `alice`.
- OOSAssumeRole: Select the OOSServiceRole RAM role.

iv. Click **Create**.

Step 3: Add the tag to the ECS instance

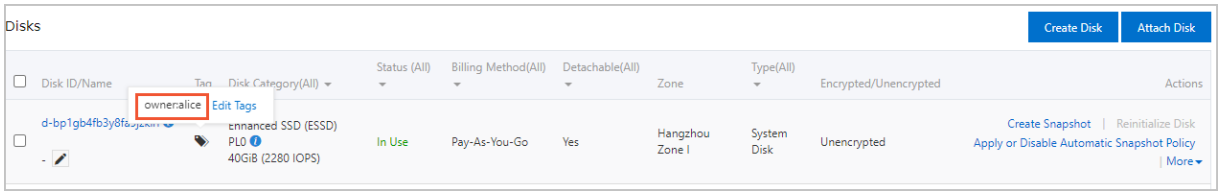
1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the upper-left corner of the top navigation bar, select a region.

4. On the Instances page, find your desired ECS instance, move the pointer over the icon in the **Tag** column, and click Edit Tags. Then, add the `owner:alice` tag to the instance.



Result

After the `owner:alice` tag is added to the ECS instance, the OOS custom template AutoTag is automatically executed. Then, the tag is automatically added to the cloud disk, ENIs, and EIPs that are associated with the ECS instance.



3.3.5. Use OOS to inherit tags from ECS instances at a time

You can execute a public template provided by Operation Orchestration Service (OOS) to inherit the tags of Elastic Compute Service (ECS) instances for the disks, elastic network interfaces (ENIs), elastic IP addresses (EIPs), or snapshots of the ECS instances at a time. This improves O&M efficiency.

Context

In this example, the tag `team:dev` is added to multiple ECS instances and is expected to be automatically added to the disks of the ECS instances. However, after you bind the tag to the ECS instances, you may find that the tag is not added to some disks of the ECS instances. This does not meet the requirements. In this case, you can execute the public template **ACS-TAG-ExtendEcsInstanceTagsByInputParams** provided by OOS to quickly find the disks to which the tag is not added and add the tag to them at a time.

Procedure

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

   > **Note** By default, OOS deployed in a region can be used to manage resources only in that region. For example, OOS deployed in the China (Hangzhou) region can be used to manage ECS instances only in this region. However, OOS provides a method to manage resources deployed in other regions. If you want to call API operations in other regions, specify the region ID in the ACS::ExecuteAPI action. We recommend that you do not use this method. Select the region where the desired ECS instances reside. For more information about the limits on OOS, see Limits.

4. On the **Public Templates** page, find the **ACS-TAG-ExtendEcsInstanceTagsByInputParams** template and click **Create Execution**.
5. In the **Basic Information** step, configure the parameters and click **Next Step: Parameter Settings**.

   In this example, default values are retained for parameters in the **Basic Information** step.

   > **Note** The default value of **Execution Mode** is **Automatic**. This indicates that all tasks defined in the template are automatically run in sequence.

6. In the **Parameter Settings** step, configure the parameters and click **Next Step: OK**.
   i. Set the **The id of region** parameter to the region where the desired ECS instances reside.
   ii. For the **TargetInstance** parameter, select the ECS instances.

   Multiple methods are provided to select the ECS instances. You can select a method based on your business requirements. In this example, the **Specify Instance Tags** method is used to select the ECS instances to which the tag `team:dev` is added.

   iii. In the **The list of tag keys** field, enter the tag key that you want to inherit from the ECS instances.

   In this example, the tag key is `team`. You can enter multiple tag keys.

   iv. Set the **The resourcetype to extend tag** parameter to the desired resource type.

   Supported resource types include disk, snapshot, eni, and eip. In this example, disk is selected.

   v. Choose whether to turn on the switch **Whether to overwrite the tag value if the tag key is the same**.

   In this example, the switch is turned on. This way, if the tag keys are the same but the tag values are different, the new tag value overwrites the original tag value.

   vi. Keep the default value for the **The RAM role to be assumed by OOS** parameter.
7. Confirm the settings and click **Create**.

Result

If Success is displayed for Execution Status on the Basic Information tab of the execution, the tag `team:dev` is inherited for the disks of the ECS instances. You can also check whether the tag is added to the disks on the Cloud Disk tab of each related ECS instance in the ECS console.

3.3.6. Use OOS to automatically add operating system tags to ECS instances

You can execute a public template provided by Operation Orchestration Service (OOS) to obtain the operating system type of an Elastic Compute Service (ECS) instance and add an operating system tag to the instance. This facilitates operations and maintenance (O&M) of the instance. The operating system types include Windows and Linux.

Procedure

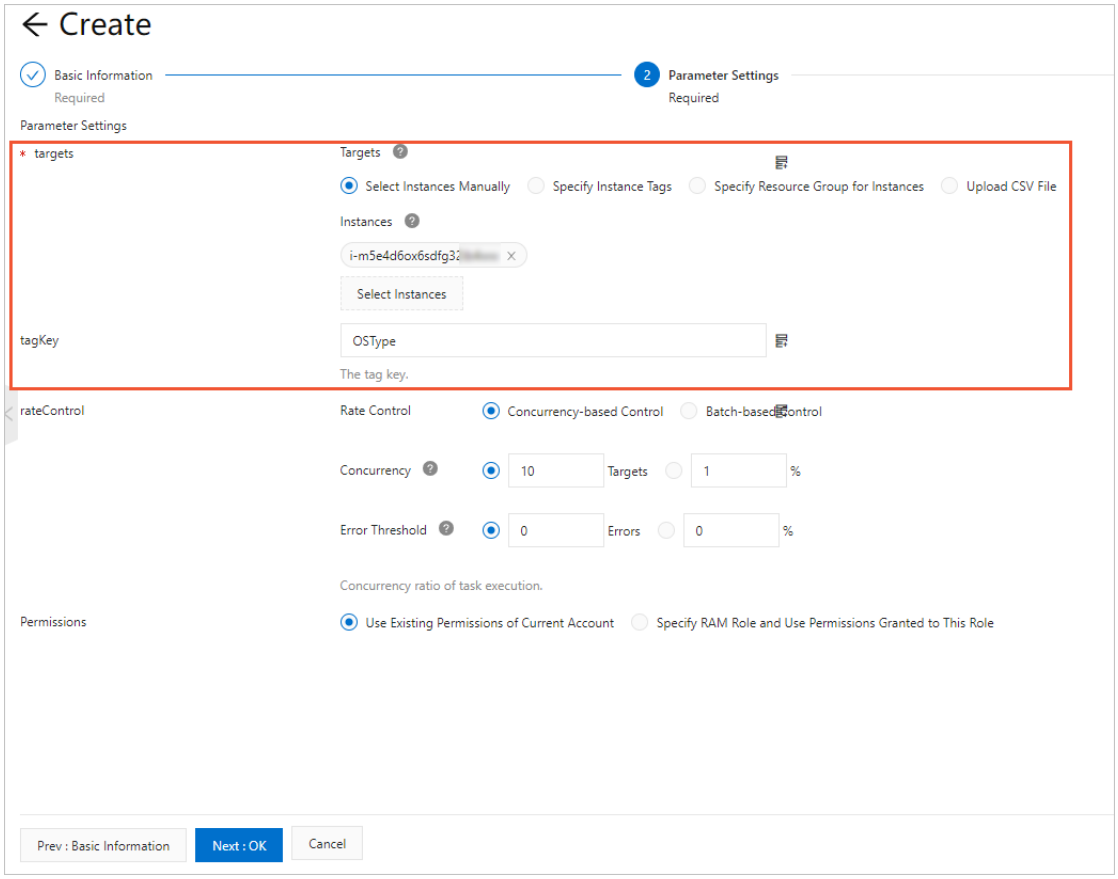
1. Log on to the OOS console.
2. In the left-side navigation pane, click **Public Templates**.
3. In the top navigation bar, select a region.

   > **Note** By default, OOS deployed in a region can be used to manage resources only in that region. For example, OOS deployed in the China (Hangzhou) region can be used to manage ECS instances only in this region. However, OOS provides a method to manage resources deployed in other regions. If you want to call API operations in other regions, specify the region ID in the ACS::ExecuteAPI action. We recommend that you do not use this method. Select the region where the ECS instance to which you want to add a tag resides.

4. On the **Public Templates** page, find **ACS-ECS-BulkyTagInstanceByOSType** 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**.

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

ii. In the Parameter Settings step, set **targets** to **Select Instances Manually**. Then, select the ECS instance to which you want to add a tag.



> **Note** You can select multiple ECS instances at a time.

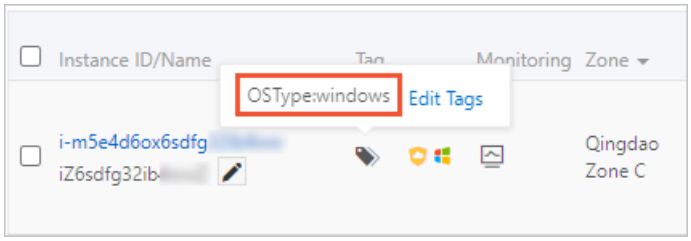
iii. Set **tagKey** to **OSType**.

iv. Click **Next: OK**.

v. Confirm the settings and click **Create**.

Result

You can log on to the ECS console to check whether an operating system tag is added to the ECS instance. For example, the `OSType:windows` tag is added to an ECS instance that runs the Windows operating system.



3.3.7. Use OOS to automatically add Linux kernel version tags to ECS instances

You can execute a public template provided by Operation Orchestration Service (OOS) to obtain information about the Linux kernel version of an Elastic Compute Service (ECS) instance and add a kernel version tag to the instance.

Procedure

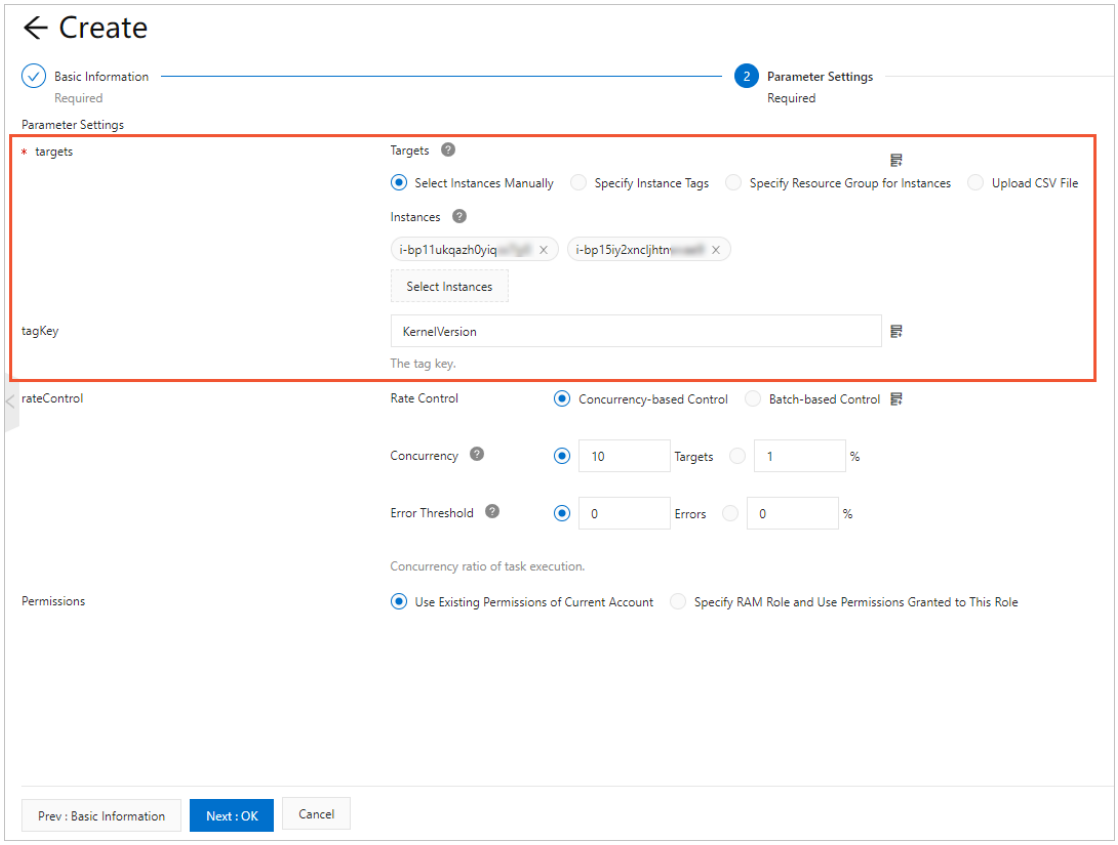
1. Log on to the OOS console.
2. In the left-side navigation pane, click **Public Templates**.
3. In the top navigation bar, select a region.

   > **Note** By default, OOS deployed in a region can be used to manage resources only in that region. For example, OOS deployed in the China (Hangzhou) region can be used to manage ECS instances only in this region. However, OOS provides a method to manage resources deployed in other regions. If you want to call API operations in other regions, specify the region ID in the ACS::ExecuteAPI action. We recommend that you do not use this method. Select the region where the ECS instance to which you want to add a tag resides.

4. On the **Public Templates** page, find **ACS-ECS-BulkyTagInstanceByLinuxKernelVersion** 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**.

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

ii. In the Parameter Settings step, set **targets** to **Select Instances Manually**. Then, select the ECS instance to which you want to add a tag.



> **Note**
>
> - You can select multiple ECS instances at a time.
> - You can select only the ECS instances that run the Linux operating system. Otherwise, the execution fails.

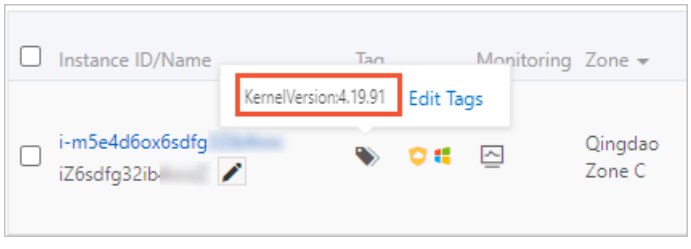
iii. Set **tagKey** to **KernelVersion**.

iv. Click **Next : OK**.

v. Confirm the settings and click **Create**.

Result

You can log on to the ECS console to check whether a Linux kernel version tag is added to the ECS instance.



3.3.8. Use Cloud Config to search for resources to which specific tags are not added

This topic describes how to use Cloud Config to search for resources to which specific tags are not added. Cloud Config facilitates resource management.

Prerequisites

Make sure that your resource tags comply with the principles of tag design. For more information, see Best practices for tag design.

Procedure

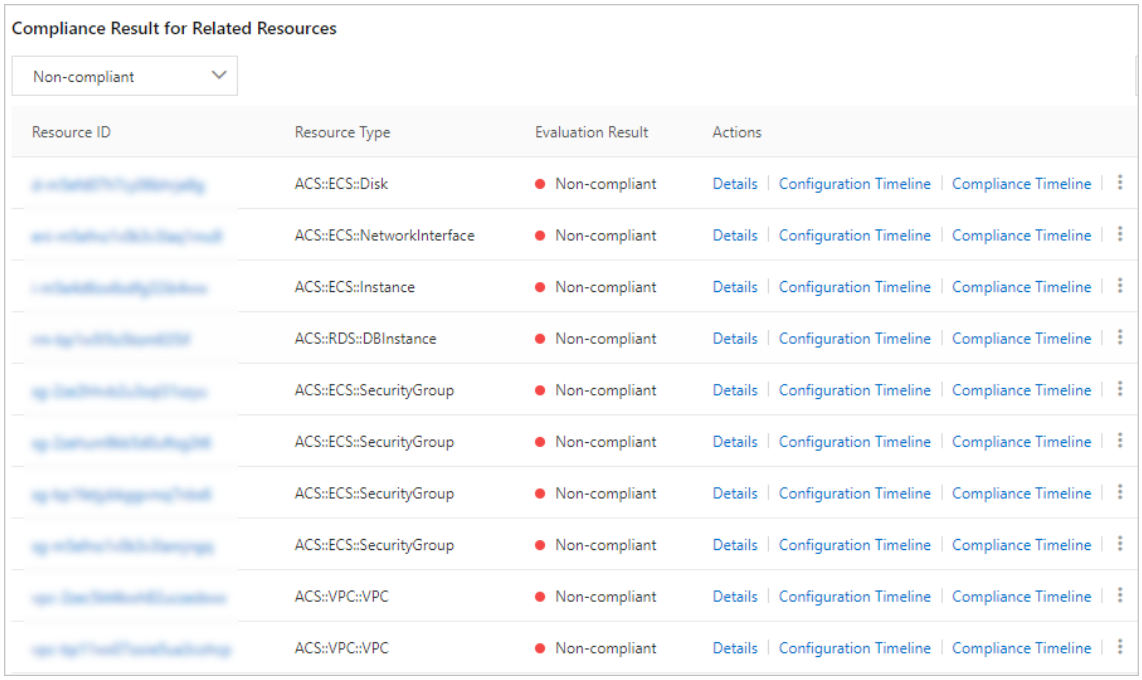
1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Rules**.
3. On the **Rules** page, click **Create Rule**.
4. On the **Create Rule** page, find the rule named **required-tags** and click **Apply Rule**.
5. In the **Properties** step, specify Rule Name, Risk Level, and Description. You can also keep the default values for these parameters. Then, click **Next**.
6. In the **Assess Resource Scope** step, select the resource types that you want to monitor and click **Next**.

   In this example, ECS, EIP, OSS, and RDS are selected.
7. In the **Parameters** step, configure the specified values for the specified keys. Then, click **Next**.
8. In the **Modify** step, select **Modify** and select a correction method. Then, click **Next**.

   The following correction methods are supported:

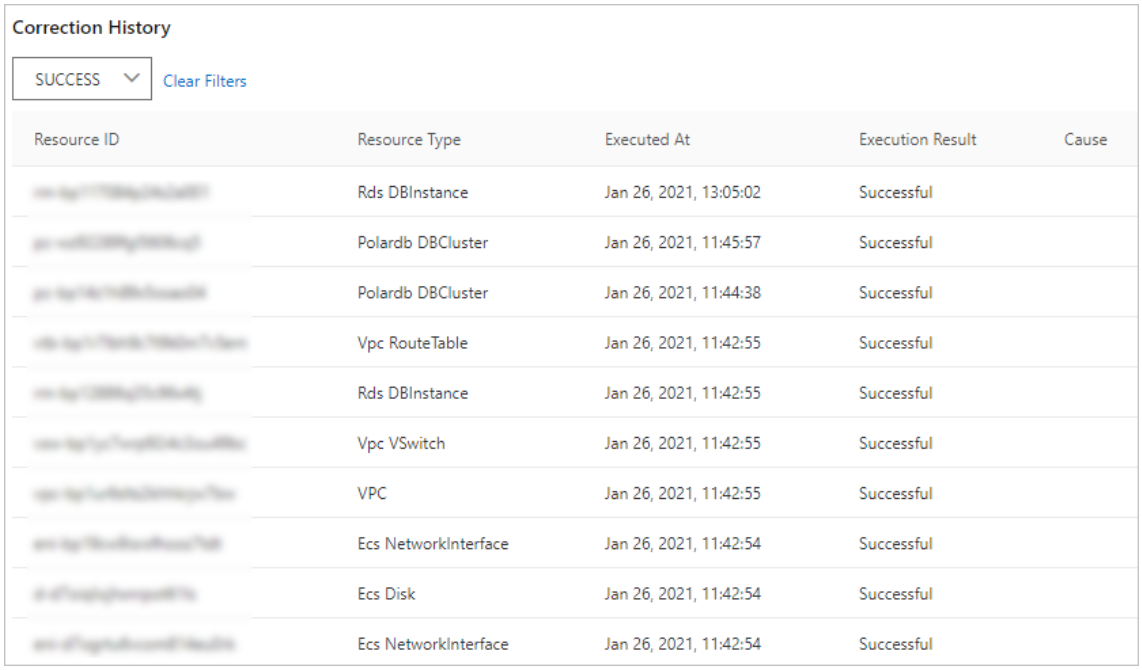
   - **Automatic Remediation**: When non-compliant resources are detected, the system automatically corrects the configurations of the resources.
   - **Manual Remediation**: When non-compliant resources are detected, you must manually correct the configurations of the resources.
9. In the **Preview and Save** step, click **Submit**.
10. Find the newly created rule and click **Details** in the Actions column. Then, you can view the details of the rule.
    - On the **Rule Details** tab, view the auditing results.

      Cloud Config identifies the resources to which specific tags are not added. The following figure shows the resources.



- On the **Correction Details** tab, view the correction results.

  If corrections are performed, the specific tags are automatically added to the resources, as shown in the following figure.



What to do next

Configure Cloud Config to send resource non-compliance events to Message Service (MNS). For more information, see Deliver resource data to an MNS topic.

3.3.9. Use ActionTrail to automatically add tags to resources

This topic describes a program that is used to automatically add creator tags to new resources. These tags indicate the users that create the resources. This program improves the efficiency of cost allocation. You can use the trail feature provided by ActionTrail to implement this program.

Prerequisites

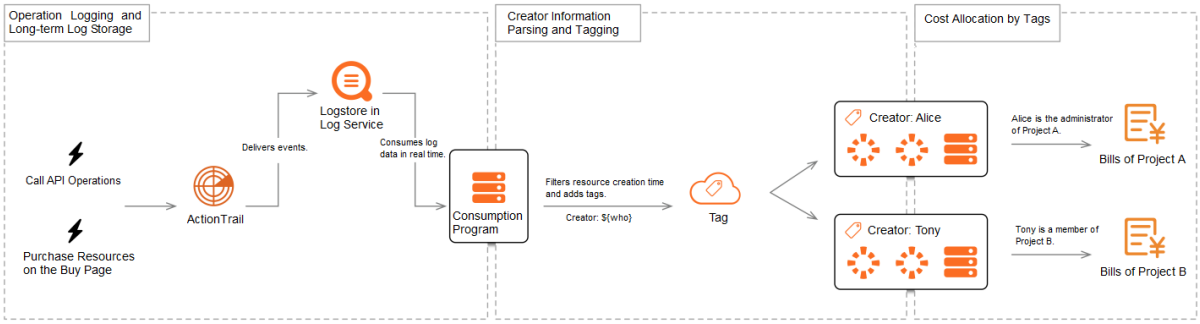
The following Alibaba Cloud services are activated:

- Resource Access Management (RAM)
- ActionTrail
- Function Compute
- Log Service

> **Note** RAM and ActionTrail are free of charge. In terms of Function Compute and Log Service, if the number of used resources exceeds the free quotas, you need to pay the extra fees. For more information, see Billing of Log Service and Billing of Function Compute.

Introduction

ActionTrail records the operations logs of an Alibaba Cloud account. These logs can be consumed in real time. In this case, you can deploy a consumption program. When the program processes a resource creation event, it calls the related Tag API operation and adds a creator tag to the resource that you want to create. This way, you can allocate the costs of this resource in the User Center based on the tag. The following figure shows the detailed process.



1. Create a trail in ActionTrail.

   You can use the trail feature provided by ActionTrail to record operations logs on the cloud and ship these logs to Log Service.

2. Consume log data in Log Service.

   You can use Function Compute, Apache Flink, or a custom program to consume log data. In this topic, Function Compute is used.

   After the log data is consumed, Function Compute calls the related Tag API operation to add a creator tag to the resource that you want to create.

3. View bills in the User Center.

   You can use the Split Bill, Bill Analysis, or Cost Center feature to view the bills of the resource based on the creator tag.

Deploy a consumption program

In this section, a consumption program is deployed to add a creator tag to a new virtual private cloud (VPC).

1. Visit OpenAPI Explorer.
2. In the dialog box that appears, click **OK** to clone code to Cloud Shell.
3. Run the following command to create a trail and deploy the consumption program:

```
./install.sh
```

4. After the program is deployed, wait for at least one minute. Then, run the following command to create a VPC:

```
sleep 60
CREATED_VPC_ID=`aliyun vpc CreateVpc --RegionId cn-huhehaote | jq ".VpcId"`
```

5. Wait for one to five minutes and run the following command to check whether a creator tag is added to the created VPC:

```
aliyun vpc DescribeVpcs --RegionId cn-huhehaote --VpcId $CREATED_VPC_ID | jq ".Vpcs.Vpc
[0].Tags"
```

If the following information is returned, the creator tag is added to the created VPC.

```
{
  "Tag": [
    {
      "Key": "created_by",
      "Value": "ram-user:221357305020244****"
    }
  ]
}
```

(Optional) Delete resources

Run the following command to delete all resources created in the program. After the resources are deleted, the consumption program becomes unavailable.

```
./uninstall.sh
```

(Optional) Modify a resource type

The preceding program can be used to automatically add creator tags to the following types of resources:

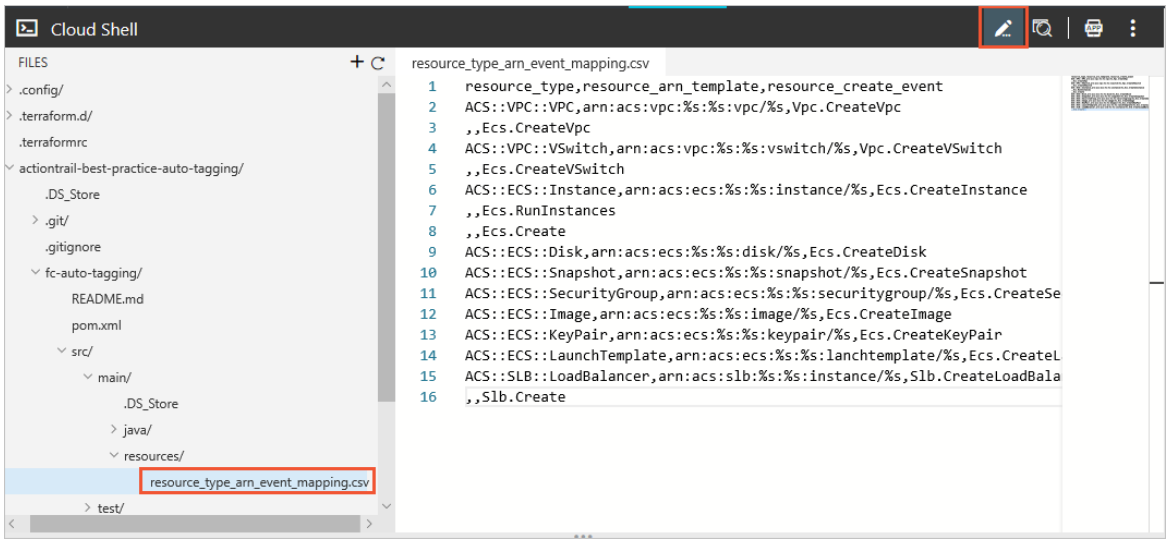
- Elastic Compute Service (ECS): ECS instances, cloud disks, snapshots, security groups, images, key pairs, and launch templates
- ApsaraDB RDS instances
- Server Load Balancer (SLB) instances
- VPC: VPCs and vSwitches

You can also modify the configuration file of the program to enable the program to support more resource types. These resource types must support ActionTrail and tags. For more information, see Types of resources that support ActionTrail and Services that work with Tag.

1. In the upper-right corner of Cloud Shell, click the Editor icon. Then, copy the content in the resource_type_arn_event_mapping.csv file to a CSV file on your on-premises machine.

   Path of the resource_type_arn_event_mapping.csv file:

   actiontrail-best-practice-auto-tagging/fc-auto-tagging/src/main/resources/resource_type_arn_event_mapping.csv



2. Modify the resource types in the CSV file on the on-premises machine.
3. Copy the new content to the resource_type_arn_event_mapping.csv file.
4. Run the following command to deploy the program again:

```
./reinstall.sh
```

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

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

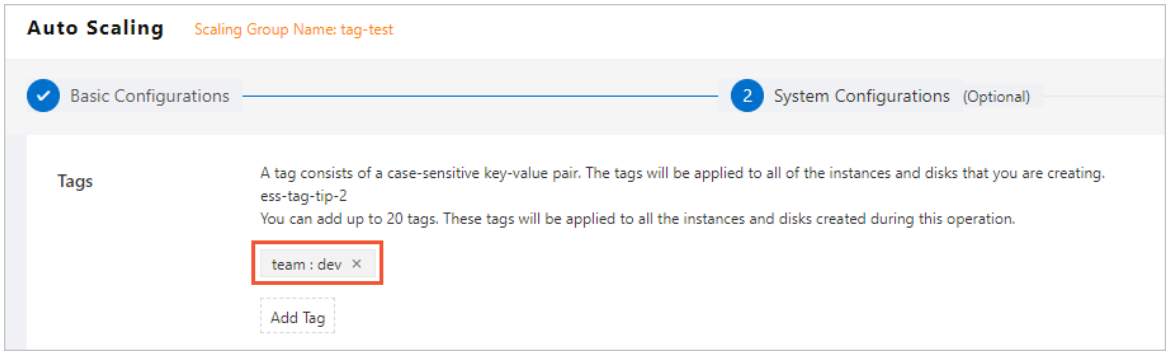
Context

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

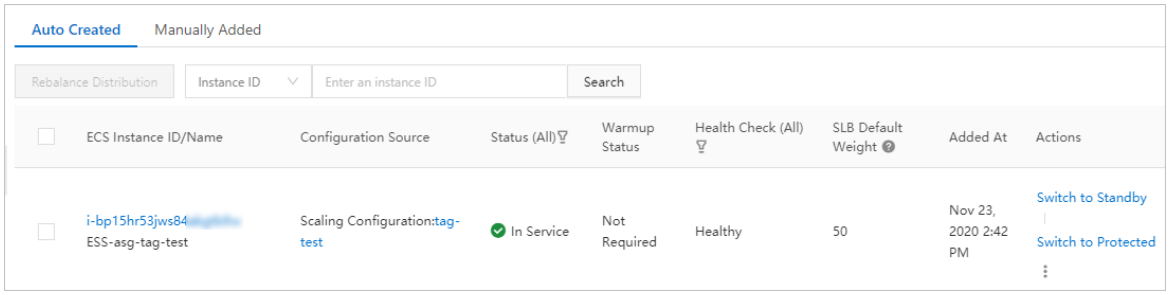
Step 1: Create an ECS instance to which a tag is added in Auto Scaling

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

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



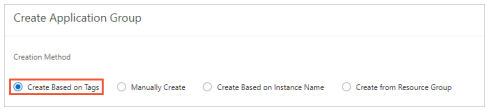
4. On the Scaling Groups page, find the scaling group that you created and click its ID. On the page that appears, click the **Instances** tab. On the Instances tab, view the ECS instance that is automatically created in the scaling group.



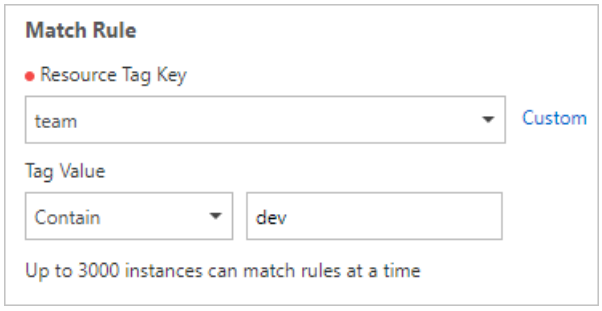
Step 2: Create a CloudMonitor application group

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

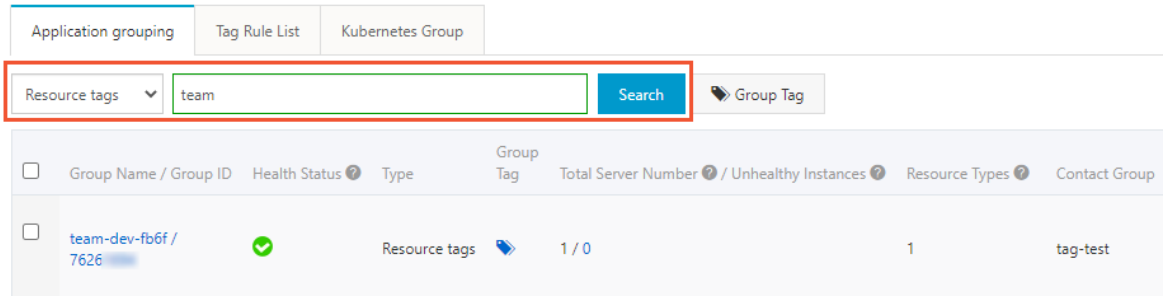
   You must specify Creation method and Match Rule based on the following instructions:
   - Creation method: Select **Smart tag synchronization creation**.



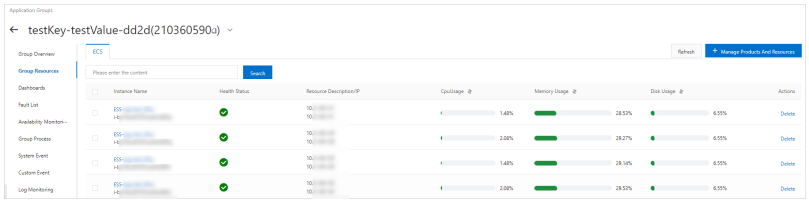
   - Match Rule: Set Resource Tag Key to `team` and specify Tag Value based on your business requirements. In this example, **Contain** and `dev` are specified.



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



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



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

3.3.11. Use ROS to add or update tags for multiple cloud resources at a time

You can use Resource Orchestration Service (ROS) to create stacks and create resources within the stacks. To facilitate subsequent O&M, you can also use ROS to add tags to the resources. ROS allows you to add or update tags for multiple resources at a time to enhance O&M efficiency.

Background information

In this topic, ROS SDK for Python is used to create stacks. For more information, see Use SDK for Python.

Add the same tag to multiple cloud resources

In the following example, ROS is used to create a virtual private cloud (VPC) named `mytest-vpc` and a vSwitch named `mytest-vsw-h` and add the `app:test` tag to both the VPC and vSwitch.

1. Create a template.

```
{
  "ROSTemplateFormatVersion": "2015-09-01",
  "Resources": {
    "VPC": {
      "Type": "ALIYUN::ECS::VPC",
      "Properties": {
        "VpcName": "mytest-vpc"
      }
    },
    "VSwitch": {
      "Type": "ALIYUN::ECS::VSwitch",
      "Properties": {
        "VpcId": { "Ref": "VPC" },
        "ZoneId": "cn-hangzhou-h",
        "CidrBlock": "172.16.0.0/24",
        "VSwitchName": "mytest-vsw-h"
      }
    }
  }
}
```

In the template, a VPC and a vSwitch are created.

2. Create a stack and add the `app:test` tag to the VPC and vSwitch.

```
# pip install aliyun-python-sdk-ros
import json
from aliyunsdkcore.client import AcsClient
from aliyunsdkros.request.v20190910.CreateStackRequest import CreateStackRequest
client = AcsClient(
    '<AccessKeyId>',
    '<AccessKeySecret>',
    'cn-hangzhou',
)
template = '''
<Template>
'''
req = CreateStackRequest()
req.set_StackName('vpc-vswitch-test')
req.set_TemplateBody(template)
req.set_TimeoutInMinutes(10)
req.set_Tags([{'Key': 'app', 'Value': 'test'}])
ret = client.do_action_with_exception(req)
print(ret)
```

Parameters:

- Replace <AccessKeyId> and <AccessKeySecret> with your AccessKey ID and AccessKey secret.
- Replace <Template> with the template created in Step 1.

3. (Optional)Log on to the VPC console and check whether the `app:test` tag is added to both the VPC and vSwitch.

Add different tags to multiple cloud resources

In the following example, ROS is used to create a VPC named `mytest-vpc` and a vSwitch named `mytest-vsw-h`, add the `app:test` tag to both the VPC and vSwitch, and add the `group:test` tag only to the vSwitch.

Expected result:

- The tag added to the VPC `mytest-vpc` is `app:test`.
- The tags added to the vSwitch `mytest-vsw-h` are `app:test` and `group:test`.

1. Create a template.

```
{
  "ROSTemplateFormatVersion": "2015-09-01",
  "Resources": {
    "VPC": {
      "Type": "ALIYUN::ECS::VPC",
      "Properties": {
        "VpcName": "mytest-vpc"
      }
    },
    "VSwitch": {
      "Type": "ALIYUN::ECS::VSwitch",
      "Properties": {
        "VpcId": { "Ref": "VPC" },
        "ZoneId": "cn-hangzhou-h",
        "CidrBlock": "172.16.0.0/24",
        "VSwitchName": "mytest-vsw-h",
        "Tags": [{ "Key": "group", "Value": "test" }]
      }
    }
  }
}
```

   A VPC and a vSwitch are created, and the `group:test` tag is added to the vSwitch.

2. Create a stack and add the `app:test` tag to the VPC and vSwitch.

```
# pip install aliyun-python-sdk-ros
import json
from aliyunsdkcore.client import AcsClient
from aliyunsdkros.request.v20190910.CreateStackRequest import CreateStackRequest
client = AcsClient(
    '<AccessKeyId>',
    '<AccessKeySecret>',
    'cn-hangzhou',
)
template = '''
<Template>
'''
req = CreateStackRequest()
req.set_StackName('vpc-vswitch-test')
req.set_TemplateBody(template)
req.set_TimeoutInMinutes(10)
req.set_Tags([{'Key': 'app', 'Value': 'test'}])
ret = client.do_action_with_exception(req)
print(ret)
```

Parameters:

- Replace <AccessKeyId> and <AccessKeySecret> with your AccessKey ID and AccessKey secret.
- Replace <Template> with the template created in Step 1.

3. (Optional)Log on to the VPC console and check whether the `app:test` tag is added to the VPC and whether the `app:test` and `group:test` tags are added to the vSwitch.

Update tags for multiple cloud resources

In the following example, the `app:test` tag added to the VPC `mytest-vpc` and the vSwitch `mytest-vsw-h` in the Add the same tag to multiple cloud resources section is changed to `app:normal`.

1. Create a stack and add the `app:normal` tag to the VPC and vSwitch.

```
# pip install aliyun-python-sdk-ros
import json
from aliyunsdkcore.client import AcsClient
from aliyunsdkros.request.v20190910.UpdateStackRequest import UpdateStackRequest
client = AcsClient(
    '<AccessKeId>',
    '<AccessKeySecret>',
    'cn-hangzhou',
)
template = '''
<Template>
'''
req = UpdateStackRequest()
req.set_StackId('<StackId>')
req.set_TemplateBody(template)
req.set_Tags([{'Key': 'app', 'Value': 'normal'}])
ret = client.do_action_with_exception(req)
print(ret)
```

Parameters:

- Replace <AccessKeyId> and <AccessKeySecret> with your AccessKey ID and AccessKey secret.
- Replace <Template> with the template created in Step 1 of the Add the same tag to multiple cloud resources section.

2. (Optional)Log on to the VPC console and check whether the `app:normal` tag is added to the VPC and vSwitch.

3.4. Use tags to control access to resources

3.4.1. Create a resource with a specific tag

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

Prerequisites

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

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

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

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

   Policy document:

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

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

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

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

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

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

Step 2: Add a tag to a VPC

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

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

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

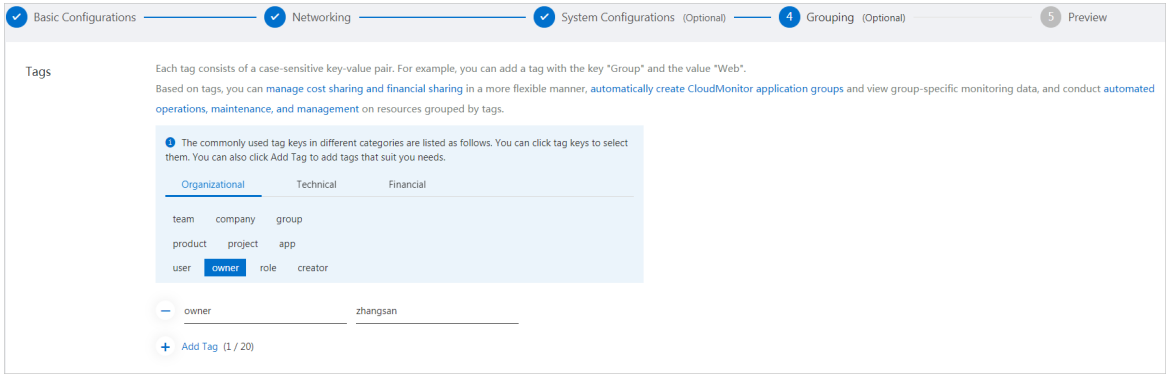
   For more information, see Add a custom tag.

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

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

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

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



References

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

3.4.2. Use tags to control access to ECS resources

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

Prerequisites

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

Context

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

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

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

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

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

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

   For more information, see Create a custom policy.

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

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

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

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

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

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

Step 2: Add tags to ECS instances

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

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

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

   For more information, see Add a custom tag.

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

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

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

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