

# Alibaba Cloud

## Alibaba Cloud Service Mesh Authorization Management

Document Version: 20220624

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

# Table of Contents

1. Overview	05
2. Grant permissions to RAM users	07
2.1. Grant permissions to RAM users and RAM roles	07
2.2. Grant RBAC permissions to RAM users and RAM roles	13
3. Service Mesh product authorization	15
3.1. Manage the service-linked role for ASM	15

# 1. Overview

Alibaba Cloud Service Mesh (ASM) supports both Resource Access Management (RAM) and Role-based Access Control (RBAC) authorization systems. This topic introduces the two authorization systems and describes how to use them in ASM.

## Authorize ASM to access other cloud services

If you want to use all ASM features, you must authorize ASM to access other cloud services. For example, if you want to use ASM to collect the access logs of the data plane, you must authorize ASM to access Log Service. Log Service is used to create projects and Logstores for storing audit logs. ASM uses a service-linked role to obtain permissions on cloud services. You must create the service-linked role for ASM and use the role to grant required permissions to ASM. For more information, see [Manage the service-linked role for ASM](#).

## RAM user authorization

If you use ASM as a RAM user, you must grant required permissions to your account by using the RAM and RBAC authorization systems as needed.

### RAM authorization

In scenarios where RAM is integrated with enterprise account systems, O&M engineers often manage cloud resources as RAM users. By default, a RAM user is not authorized to call the APIs of cloud services. To allow a RAM user to call the APIs, you must grant required permissions to the RAM user.

You can grant specific permissions to a RAM user to restrict the operations that can be performed by the RAM user in the ASM console and the APIs that can be called by the RAM user. This implements fine-grained access control on cloud resources. For more information, see [Grant permissions to RAM users and RAM roles](#).

### RBAC authorization

RBAC authorization is used to implement permission control on ASM instances and restrict the operations on custom ASM resources (such as virtual services and destination rules) by RAM users. A RAM user can have different RBAC permissions on different ASM instances.

ASM provides three preset roles that correspond to different RBAC permissions. The following table describes the preset roles that you can assign to RAM users in the .

Role	RBAC permissions on cluster resources
Administrator	Has read and write permissions on all custom ASM resources in all namespaces.
Restricted user	Has read-only permissions on custom ASM resources visible in the ASM console in all namespaces or specified namespaces.
Unauthorized user	Has no read or write permissions on all custom ASM resources in all namespaces.

### Grant permissions to a RAM user

1. Create a RAM user in the RAM console. For more information, see [Create a RAM user](#).
2. Grant RBAC permissions to the RAM user as needed. For more information, see [Grant RBAC permissions](#)

[to RAM users and RAM roles.](#)

3. Attach RAM policies to the RAM user as needed. For more information, see [Grant permissions to RAM users and RAM roles.](#)

## 2. Grant permissions to RAM users

### 2.1. Grant permissions to RAM users and RAM roles

You can authorize a RAM user or a RAM role to use Alibaba Cloud Service Mesh (ASM) by granting permissions to the RAM user or RAM role as needed. Only authorized RAM users and RAM roles can perform operations such as creating ASM instances and updating ASM configurations in the ASM console. This eliminates security risks caused by the leakage of passwords of Alibaba Cloud accounts. This topic describes how to grant permissions to a RAM user and a RAM role.

#### Prerequisites

- A RAM user and a RAM role are created. For more information, see [Create a RAM user](#) and [Create a RAM role for a trusted Alibaba Cloud account](#).
- You have a basic knowledge of the policy elements, structure, and syntax. For more information, see [Policy structure and syntax](#).

#### Context

The permissions required by RAM users and RAM roles vary with different scenarios.

- If a RAM user or a RAM role needs to manage ASM instances but not Container Service for Kubernetes (ACK) clusters, you need to grant only permissions on ASM instances to the RAM user or RAM role. For more information, see [Attach system policies to RAM users and RAM roles](#) and [Attach custom policies to RAM users and RAM roles](#).
- If a RAM user or a RAM role needs to manage both ASM instances and ACK clusters, you must grant permissions on ASM instances and ACK clusters to the RAM user or RAM role. For example, the RAM user or RAM role needs to add ACK clusters to ASM instances and remove ACK clusters from ASM instances. For more information, see [Attach system policies to RAM users and RAM roles](#), [Attach custom policies to RAM users and RAM roles](#), and [Create a custom RAM policy](#).

#### Attach system policies to RAM users and RAM roles

By default, ASM creates two system policies: AliyunASMReadOnlyAccess and AliyunASMFulAccess. You can attach the policies to RAM users and RAM roles. The following part describes the two system policies:

- AliyunASMReadOnlyAccess


The policy contains only read-only permissions on ASM instances. After you attach the policy to a RAM user, the RAM user can only view the information about ASM instances but cannot modify the configurations of ASM instances.

- AliyunASMFulAccess


The policy contains all permissions on ASM instances. After you attach the policy to a RAM user, the RAM user has the same permissions on ASM instances as an Alibaba Cloud account and can perform all operations on ASM instances.

The following part describes how to attach a system policy to a RAM user or RAM role. In the following example, the AliyunASMReadOnlyAccess policy is attached to a RAM user.


- 1.
2. In the left-side navigation pane, choose **Identities > Users**.

 **Note** To attach a policy to a RAM role, choose **Identities > Roles** in the left-side navigation pane.

3. On the **Users** page, find the RAM user to which you want to attach a policy and click **Add Permissions** in the **Actions** column.

 **Note** To grant permissions to a RAM role, find the RAM role on the **Roles** page and click **Add Permissions** in the **Actions** column.

4. In the **Add Permissions** panel, attach a policy to the RAM user.
  - i. Specify the authorization scope.
    - **Alibaba Cloud Account**: The permissions take effect on all resources of the current Alibaba Cloud account.
    - **Specific Resource Group**: The permissions take effect in a specific resource group.

 **Note** If you want to select **Specific Resource Group**, make sure that ASM supports resource groups. For more information, see [Services that work with Resource Group](#).

- ii. Specify a principal.  
The principal is the RAM user to which you want to grant permissions. By default, the current RAM user is specified. You can also specify another RAM user.
  - iii. Click **System Policy** in the **Select Policy** section, enter **AliyunASMReadOnlyAccess** in the field, and then click **AliyunASMReadOnlyAccess** in the **Authorization Policy Name** column.
  - iv. Click **OK**.
5. Click **Complete**.

## Attach custom policies to RAM users and RAM roles

If you want to enforce fine-grained control on permissions, you can create custom policies and attach custom policies to RAM users and RAM roles.

1. Log on to the **RAM console** by using your Alibaba Cloud account or as an authorized RAM user.
2. Create a policy that is used to grant permissions on ASM instances.
  - i. In the left-side navigation pane, choose **Permissions > Policies**.
  - ii. On the **Policies** page, click **Create Policy**.
  - iii. On the **Create Policy** page, click the **JSON** tab. In the code editor, write your policy and click **Next Step**.

You can modify the **Action** field in the **Statement** block to enable fine-grained authentication for API operations. In this example, a policy with limited permissions is created. The policy grants all RAM permissions on ASM except role-based access control (RBAC) authorization permissions. A RAM user to which the policy is attached cannot grant RBAC



permissions to other users but has all other permissions.


```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "servicemesh:Add*",
        "servicemesh:CRBatchDeletion",
        "servicemesh:Create*",
        "servicemesh>Delete*",
        "servicemesh:Describe*",
        "servicemesh:Enable*",
        "servicemesh:Disable*",
        "servicemesh:Get*",
        "servicemesh:InvokeApiServer",
        "servicemesh:List*",
        "servicemesh:Modify*",
        "servicemesh:Re*",
        "servicemesh:Run*",
        "servicemesh:Set*",
        "servicemesh:Sync*",
        "servicemesh:Update*",
        "servicemesh:Upgrade*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "log:ListLogStores",
        "log:ListDashboard",
        "log:GetDashboard",
        "log:ListSavedSearch",
        "log:ListProject"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "log:GetLogStoreLogs",
      "Resource": "acs:log:*:*:project/*/logstore/audit-*"
    },
    {
      "Effect": "Allow",
      "Action": "log:GetLogStoreLogs",
      "Resource": "acs:log:*:*:project/*/logstore/istio-*"
    },
    {
      "Action": "ram:CreateServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "servicemesh-ecsfedex-ecsfedex"
        }
      }
    }
  ]
}
```

```


        "ram:ServiceName": "servicemesh.aliyuncs.com"
      }
    }
  ],
  "Version": "1"
}

```

- iv. In the **Basic Information** section, enter a policy name in the Name field. In this example, the policy name is ASMPolicy1. Then, click **OK**.
3. Attach the custom policy to a RAM user or RAM role.
  - i. In the left-side navigation pane, choose **Identities > Users**.

 **Note** To attach a policy to a RAM role, choose **Identities > Roles** in the left-side navigation pane.

- ii. On the **Users** page, find the RAM user to which you want to attach the policy and click **Add Permissions** in the **Actions** column.


 **Note** To grant permissions to a RAM role, find the RAM role on the **Roles** page and click **Add Permissions** in the **Actions** column.

- iii. In the **Add Permissions** panel, select **Alibaba Cloud Account** for the **Authorized Scope** parameter. The name of the current RAM user is automatically filled in the **Principal** field. Click **Custom Policy** in the **Select Policy** section, enter and select ASMPolicy1, and then click **OK**.

## Sample scenarios of custom policies

### Scenario 1: Grant the permissions on a single ASM instance

You can use the following script to create a policy that grants the permissions on a single ASM instance. After you attach the policy to a RAM user or RAM role, the RAM user or RAM role can manage only the ASM instance with the specified ID.

 **Note** When you create the policy, replace `<ServicemeshId>` in the script with the ID of the ASM instance on which you want to grant permissions.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "servicemesh:*",
      "Resource": "acs:servicemesh:*:*:servicemesh/<ServicemeshId>"
    },
    {
      "Effect": "Allow",
      "Action": "servicemesh:DescribeServiceMeshes",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "log:GetLogStoreLogs",
      "Resource": "acs:log:*:*:project/*/logstore/audit-<ServicemeshId>"
    },
    {
      "Effect": "Allow",
      "Action": "log:GetLogStoreLogs",
      "Resource": "acs:log:*:*:project/*/logstore/istio-<ServicemeshId>"
    }
  ],
  "Version": "1"
}
```

## Scenario 2: Grant the permissions to read and write Istio resources in the ASM console

By default, the system policy AliyunASMReadOnlyAccess provided by ASM grants RAM users or RAM roles the read-only permissions on ASM instances. RAM users or RAM roles to which this policy is attached cannot manage Istio resources in ASM.

You can use the following script to create a policy that grants the read and write permissions on Istio resources. After you attach the policy to a RAM user or RAM role, the RAM user or RAM role can use the ASM console to manage Istio resources on ASM instances. However, the RAM user or RAM role cannot change other settings of the ASM instances, such as feature settings.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "servicemesh:List*",
        "servicemesh:Describe*",
        "servicemesh:Get*",
        "servicemesh:InvokeApiServer"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "log:ListLogStores",
        "log:ListDashboard",
        "log:GetDashboard",
        "log:ListSavedSearch"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "log:GetLogStoreLogs",
      "Resource": "acs:log:*:*:project/*/logstore/audit-*"
    }
  ],
  "Version": "1"
}
```

### Scenario 3: Grant RBAC authorization permissions

You can use the following script to create a policy that grants RBAC authorization permissions. After you attach the policy to a RAM user or RAM role, the RAM user or RAM role can use the ASM console to manage the RBAC permissions of other RAM roles or RAM users. However, the RAM user or RAM role cannot manage ASM instances.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "servicemesh:DescribeUserPermissions",
        "servicemesh:GrantUserPermissions",
        "servicemesh:DescribeServiceMeshes",
        "servicemesh:DescribeUsersWithPermissions"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ims:ListUserBasicInfos",
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

## 2.2. Grant RBAC permissions to RAM users and RAM roles


If a RAM user or a RAM role needs to manage custom Alibaba Cloud Service Mesh (ASM) resources, you can assign required role-based Access Control (RBAC) roles to the RAM user or the RAM role. This topic describes how to assign RBAC roles to a RAM user.

### Configuration description

You can use an Alibaba Cloud account or a RAM user to assign RBAC roles to RAM users.

### Procedure

- 1.
2. In the left-side navigation pane, choose **Service Mesh > Authorization**.
3. On the **Authorization** page, find the RAM user that you want to authorize and click **Authorize** in the Actions column.

 **Note** To assign RBAC roles to a RAM role, click the **RAM Role** tab on the **Authorization** page, select the RAM role that you want to authorize, and then click **Authorize**.

4. Assign a preset RBAC role to the RAM user for each ASM instance and click **Submit**.

The following table describes the preset RBAC roles.

Role	RBAC permissions on cluster resources
Administrator	Has read and write permissions on all custom ASM resources in all namespaces.

Role	RBAC permissions on cluster resources
Restricted user	Has read-only permissions on custom ASM resources visible in the ASM console in all namespaces or specified namespaces.
Unauthorized user	Has no read or write permissions on all custom ASM resources in all namespaces.

# 3.service mesh product authorization

## 3.1. Manage the service-linked role for ASM

AliyunServiceRoleForServiceMesh is a service-linked role that is provided by Resource Access Management (RAM) to grant Alibaba Cloud Service Mesh (ASM) the access permissions on other Alibaba Cloud resources. This topic describes how to create and delete the service-linked role for ASM.

### Context

Service-linked roles are RAM roles that only the linked Alibaba Cloud services can assume. AliyunServiceRoleForServiceMesh is the service-linked role that is used to grant ASM the access permissions on other Alibaba Cloud services, such as Container Service for Kubernetes (ACK), Virtual Private Cloud (VPC), Server Load Balancer (SLB), Log Service, Tracing Analysis, Application Real-Time Monitoring Service (ARMS), and Cloud Enterprise Network. For more information about service-linked roles, see [Service-linked roles](#).

### Precautions

By default, Alibaba Cloud accounts have the permission to create the service-linked role for ASM. To create the service-linked role for ASM as a RAM user, you must attach the CreateServiceLinkedRole policy to the RAM user. This policy contains the permission to create the service-linked role for ASM, as shown in the following code. For more information, see [Grant permissions to a RAM user](#).

```
{
  "Statement": [
    {
      "Action": "ram:CreateServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "servicemesh.aliyuncs.com"
        }
      }
    }
  ],
  "Version": "1"
}
```


### Create the service-linked role for ASM

When you use ASM, the system checks whether the AliyunServiceRoleForServiceMesh service-linked role is created for your ASM service. If the AliyunServiceRoleForServiceMesh service-linked role is not created for your ASM service, the system instructs you to create the service-linked role. You can click **Create** on the Service-linked Role for ASM page to create the service-linked role.


System policies that are attached to service-linked roles are defined and used by the linked Alibaba Cloud services. You cannot add, modify, or remove permissions for service-linked roles. You can view the policies that are attached to a service-linked role on the details page of the service-linked role. For more information, see [View the basic information about a RAM role](#).

## Delete the service-linked role for ASM

If you do not need the AliyunServiceRoleForServiceMesh service-linked role for the moment and understand the impacts of not using the service-linked role, you can delete it. For example, if you do not need to use ASM or create ASM instances, you can delete the AliyunServiceRoleForServiceMesh service-linked role.

 **Note** Before you can delete the AliyunServiceRoleForServiceMesh service-linked role, you must delete the ASM instances in all regions in the current account. Otherwise, the delete operation will fail. Each Alibaba Cloud account has only one AliyunServiceRoleForServiceMesh service-linked role. After the AliyunServiceRoleForServiceMesh service-linked role is deleted from an Alibaba Cloud account, the Alibaba Cloud account and its RAM users can no longer use ASM or create ASM instances.

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, click **RAM Roles**.
3. On the **RAM Roles** page, enter AliyunServiceRoleForServiceMesh in the search box to find the AliyunServiceRoleForServiceMesh service-linked role. Then, click **Delete** in the **Actions** column of the AliyunServiceRoleForServiceMesh service-linked role.
4. In the message that appears, click **OK**.

 **Note** If you delete a service-linked role, **Deleting** appears in the **Actions** column. The delete operation takes a few seconds to complete. After the role is deleted, a success message appears. If a service-linked role fails to be deleted, click **View Details** in the error message and troubleshoot the error.