ALIBABA CLOUD

Alibaba Cloud

Resource Access Management
RAM Role Management

Document Version: 20201231

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.RAM role overview

A RAM role is a virtual RAM identity that you can create in your Alibaba Cloud account. A RAM role does not have a specific logon password or AccessKey pair. A RAM user can be used only after the RAM user is assumed by a trusted entity.

Basic concepts

RAM role

A RAM role is a virtual identity that you can create in your Alibaba Cloud account. The differences among RAM roles, entity users (Alibaba Cloud account, RAM users, or Alibaba Cloud services), and textbook roles are as follows:

- Entity users have specific logon passwords or AccessKey pairs.
- Textbook roles (or traditionally defined roles) indicate a set of permissions, which are similar to policies in RAM. If a user assumes a textbook role, the user can obtain a set of permissions and access the authorized resources.
- RAM roles have specific identities and can be attached a set of policies. However, RAM roles do not have specific logon passwords or AccessKey pairs. If an entity user assumes a RAM role, the entity user can obtain and use the role token to access the authorized resources.

ARN

An Alibaba Cloud Resource Name (ARN) is the global resource identifier of a role. Each RAM role has a unique ARN. For example, the ARN of the RAM role devops of an Alibaba Cloud account is `acs:ram::123456789012****:role/samplerole`. After you create a RAM role, you can click the role name and find its ARN in the **Basic Information** section.

Trusted entity

A trusted entity indicates an entity user who can assume a role. When you create a role, you must specify a trusted entity. A RAM role can be assumed only by a trusted entity. A trusted entity can be an Alibaba Cloud account, Alibaba Cloud service, or identity provider (IdP).

Policy

A RAM role can be attached a set of policies. RAM roles without policies can exist, but cannot access resources.

Role assuming

Role assuming is the method for entity users to obtain security tokens of RAM roles. An entity user can call the AssumeRole STS API operation to obtain the security token of a RAM role. Then, the entity user can use the security token to call API operations of Alibaba Cloud services.

Identity switching

Identity switching is the method by which entity users can switch from the logon identity to the role identity in the RAM console. After logging on to the RAM console, an entity user can switch to a RAM role that the entity user can assume. Then, the entity user can use the RAM role to manage Alibaba Cloud resources. After the management operations are completed, the RAM user can switch back to the logon identity.

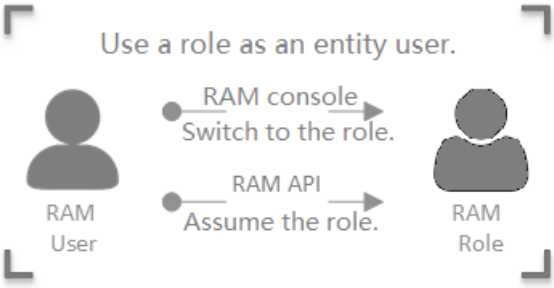
Role token

A role token is a temporary AccessKey pair for a RAM role. A RAM role does not have a specific logon password or AccessKey pair. If an entity user wants to use a RAM role, the entity user must assume the RAM role to obtain a role token. Then, the entity user can use the role token to call API

operations of Alibaba Cloud services.

Access Alibaba Cloud resources by using a RAM role

1. The Alibaba Cloud account specifies a trusted entity that can assume the RAM role.
2. The trusted entity logs on to the console or calls an API operation to assume the RAM role and obtains a role token.



   - The trusted entity can switch its identity in the console to assume the RAM role. For more information, see Assume a RAM role.
   - The trusted entity can also call the AssumeRole API operation to assume the RAM role.

   > **Note** An entity user can obtain a role token by assuming a RAM role and then use the role token to access Alibaba Cloud resources.

3. The Alibaba Cloud account attaches a policy to the RAM role. For more information, see Grant permissions to a RAM role.

   > **Note** Each RAM role can be attached one or more polices. A RAM role without a policy cannot access Alibaba Cloud resources.

4. The trusted entity assumes the RAM role and uses the role token to access Alibaba Cloud resources.

RAM role types

RAM roles are divided into the following types based on the entrusted entity:

- **Alibaba Cloud account**. RAM users of a trusted Alibaba Cloud account can assume this type of RAM role. RAM users who assume this type of role can belong to their parent Alibaba Cloud accounts or other Alibaba Cloud accounts. This type of RAM role is used for cross-account access and temporary authorization.
- **Alibaba Cloud service**. Alibaba Cloud services can assume this type of RAM role. This type of RAM role is used to authorize Alibaba Cloud services to manage your resources.
- **IdP**. Users of an entrusted IdP can assume this type of RAM role. This type of RAM role is used for single sign-on (SSO) between Alibaba Cloud and an entrusted IdP.

Scenarios

- Use an STS token for authorizing a mobile app to access Alibaba Cloud resources
- Use a RAM role to grant permissions across Alibaba Cloud accounts
- Use RAM for authorizing applications to access Alibaba Cloud resources

2.Service-linked roles

A trusted Alibaba Cloud service can assume a Resource Access Management (RAM) role to access other Alibaba Cloud services. RAM roles that a trusted Alibaba Cloud service can assume are classified into two types: normal service role and service-linked role. This topic describes service-linked roles.

What is a service-linked role?

An Alibaba Cloud service may need to access other services to implement a feature. In this case, the Alibaba Cloud service must be authorized. For example, to retrieve resource lists and log data from Elastic Compute Service (ECS) and ApsaraDB RDS, Cloud Config requires the access permissions on ECS and RDS. Alibaba Cloud provides service-linked roles to simplify the authorization in such scenarios.

A service-linked role is a RAM role that only the linked service can assume. In most cases, a service automatically creates or deletes a service-linked role if needed. The service-linked role simplifies the process to authorize a service to access other services and reduces the risks caused by user errors.

The policy that is attached to a service-linked role is predefined by the linked service. You cannot modify or delete the policy. In addition, you cannot attach policies to or detach policies from a service-linked role.

If a service does not support service-linked roles, you can use a normal service role to authorize the service.

Create a service-linked role

Some Alibaba Cloud services automatically create service-linked roles when you perform operations such as creating a cloud resource or enabling a feature. You can view the created service-linked roles on the RAM Roles page of the RAM console. You can also retrieve a list of created service-linked roles by using the API or CLI to call the ListRoles operation.

You can also manually create service-linked roles. For more information, see Create a service linked role.

> **Note**
>
> - Service-linked roles count toward the limit of RAM roles of your Alibaba Cloud account. If the limit is exceeded, you can still create service-linked roles but you can no longer create RAM roles of other types.
> - For more information about how an Alibaba Cloud service creates a service-linked role, see the documentation that is specific to the service.

Delete the service-linked role AliyunServiceRoleForDAS

Some Alibaba Cloud services automatically delete service-linked roles when you perform operations such as deleting a cloud resource or disabling a feature. You can also manually delete service-linked roles in the RAM console. For more information about how to delete a service-linked role, see Delete a RAM role.

When you attempt to delete a service-linked role, RAM first checks whether the role is being assumed by the linked service.

- If the service-linked role is idle, it is deleted.
- If the service-linked role is in use, it cannot be deleted. However, you can view the service resources that assume the service-linked role. If you no longer need the service resources, find and remove the

resources, and then delete the service-linked role.

> **Note** For more information about the conditions that allow you to delete a service-linked role, see the documentation that is specific to the linked service.

Permissions required to create and delete a service-linked role

RAM identities must be granted the required permissions before they can create or delete a service-linked role. The permissions are also required in scenarios where service-linked roles are automatically created when RAM identities perform operations.

> **Note** The permission to create a service-linked role is included in the administrative permission policy of the linked service (for example, AliyunESSFullAccess of ECS). Therefore, after you attach the administrative permission policy of a service to a RAM identity, the RAM identity is allowed to create the service-linked role for the service.

The following sample policy allows authorized RAM identities to create and delete the service-linked role for Resource Management:

```
{
  "Action": [
    "ram:CreateServiceLinkedRole",
    "ram:DeleteServiceLinkedRole"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Condition": {
    "StringEquals": {
      "ram:ServiceName": "resourcemanager.aliyuncs.com"
    }
  }
}
```

Assume a service-linked role

A service-linked role can be assumed by only the linked service and cannot be assumed by identities such as RAM users or other RAM roles.

You can view the service that can assume a service-linked role in the `Service` element on the **Trust Policy Management** tab of the role details page.

Alibaba Cloud services that support service-linked roles

Alibaba Cloud service	The name of the service	Service-linked role	Reference
Resource Management	resourcemanager.aliyuncs.com	AliyunServiceRoleForResourceDirectory	Service linked role for Resource Directory

Alibaba Cloud service	The name of the service	Service-linked role	Reference
Cloud Config	config.aliyuncs.com	AliyunServiceRoleForConfig	Manage the service linked role associated with Cloud Config
PolarDB	polardb.aliyuncs.com	AliyunServiceRoleForPolarDB	RAM role linked to Apsara PolarDB
Hybrid Backup Recovery (HBR)	dr.hbr.aliyuncs.com	AliyunServiceRoleForHbrDr	Service linked role for ECS disaster recovery
Operation Orchestration Service (OOS)	bandwidthscheduler.oos.aliyuncs.com	AliyunServiceRoleForOOSBandwidthScheduler	OOS linked roles
	instancescheduler.oos.aliyuncs.com	AliyunServiceRoleForOOSInstanceScheduler	
Auto Scaling (ESS)	ess.aliyuncs.com	AliyunServiceRoleForAutoScaling	Grant permissions to Auto Scaling
Time Series Database (TSDB)	hitsdb.aliyuncs.com	AliyunServiceRoleForTSDB	N/A
Cloud Monitor	cloudmonitor.aliyuncs.com	AliyunServiceRoleForCloudMonitor	Manage the service linked role for CloudMonitor
Blockchain as a Service (BaaS)	baas.aliyuncs.com	AliyunServiceRoleForBaaS	N/A
Global Traffic Manager	gtm.aliyuncs.com	AliyunServiceRoleForGTM	Service-linked role of Global Traffic Manager
Alibaba Cloud DNS (DNS)	alidns.aliyuncs.com	AliyunServiceRoleForDNS	N/A
Sensitive Data Discovery and Protection	sddp.aliyuncs.com	AliyunServiceRoleForSDDP	Authorize SDDP to access Alibaba Cloud resources
CDN	cdn-ddos.cdn.aliyuncs.com	AliyunServiceRoleForCDNAccessingDDoS	Integrate Alibaba Cloud CDN with Anti-DDoS

3.Create a RAM role

3.1. Create a RAM role for a trusted Alibaba Cloud account

You can create RAM roles for three types of trusted entities: trusted Alibaba Cloud accounts, trusted Alibaba Cloud services, and trusted identity providers (IdPs). This topic describes how to create a RAM role for a trusted Alibaba Cloud account.

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **RAM Roles**.
3. On the **RAM Roles** page, click **Create RAM Role**.
4. In the **Create RAM Role** pane, select **Alibaba Cloud Account** for the **Trusted Entity Type** parameter, and then click **Next**.
5. Specify the **RAM Role Name** and **Note** parameters.
6. Select **Current Alibaba Cloud Account** or **Other Alibaba Cloud Account** for the **Select Trusted Alibaba Cloud Account** parameter, and then click **OK**.

> **Note** If you select **Other Alibaba Cloud Account**, you must enter the ID of the Alibaba Cloud account.

What's next

After you create a RAM role, the RAM role has no permissions by default. You can click **Add Permissions** to grant permissions to the RAM role. For more information, see Grant permissions to a RAM role.

Related information

- CreateRole

3.2. Create a RAM role for a trusted Alibaba Cloud service

You can create RAM roles for three types of trusted entity: Alibaba Cloud account, Alibaba Cloud service, and identity provider (IdP). This topic describes how to create a RAM role for a trusted Alibaba Cloud service.

Context

Two types of RAM role are available for a trusted Alibaba Cloud service:

- Normal service role: You need to name the RAM role, select a trusted service, and attach permission policies to the RAM role.
- Service linked role: You only need to select a trusted service. The name and policy of the RAM role are

predefined by the service. For more information, see Service-linked roles.

Create a normal service role

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **RAM Roles**.
3. On the **RAM Roles** page, click **Create RAM Role**.
4. In the **Create RAM Role** pane, select **Alibaba Cloud Service** for the **Trusted Entity Type** parameter, and then click **Next**.
5. Select **Normal Service Role** for the **Role Type** parameter.
6. Specify the **RAM Role Name** and **Note** parameters.
7. Select a trusted service.

   > **Note** Available services are listed in the **Select Trusted Service** drop-down list.

8. Click **OK**.

After you create a RAM role, the RAM role has no permissions by default. You can click **Add Permissions to RAM Role** to grant permissions to the RAM role. For more information, see Grant permissions to a RAM role.

Create a service linked role

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **RAM Roles**.
3. On the **RAM Roles** page, click **Create RAM Role**.
4. In the **Create RAM Role** pane, select **Alibaba Cloud Service** for the **Trusted Entity Type** parameter, and then click **Next**.
5. Select **Service Linked Role** for the **Role Type** parameter.
6. Select a service. After you select a service, you can view the name, description, and policy that are predefined for the service linked role. You can click **View Policy Details** to view the detailed information of the policy.

   > **Note** Available services are listed in the **Select Trusted Service** drop-down list.

7. Click **OK**.

Related information

- CreateRole

3.3. Create a RAM role for a trusted IdP

You can create RAM roles for three types of trusted entity: Alibaba Cloud account, Alibaba Cloud service, and identity provider (IdP). This topic describes how to create a RAM role for a trusted IdP.

Procedure

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

2. In the left-side navigation pane, click **RAM Roles**.
3. On the **RAM Roles** page, click **Create RAM Role**.
4. In the **Create RAM Role** pane, select **IdP** for the Trusted Entity Type parameter, and then click **Next**.
5. Specify the **RAM Role Name** and **Note** parameters.
6. Select a trusted IdP, view the conditions, and then click **OK**.

> **Note** Only the `saml:recipient` condition key is supported. This condition key is required and cannot be changed.

What's next

After you create a RAM role, you can click **Add Permissions to RAM Role** to grant permissions to the RAM role. For more information, see Grant permissions to a RAM role.

Related information

- CreateRole

4.View the basic information of a RAM role

This topic describes how to view the basic information of a RAM role, such as the role name, the date and time when the role was created, and the Alibaba Cloud Resource Name (ARN).

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **RAM Roles**.
3. In the **RAM Role Name** column, click the name of the RAM role.
4. In the **Basic Information** section, view the RAM role information.

> **Note** The RAM role information cannot be modified.

Related information

- GetRole

5.Grant permissions to a RAM role

You can grant permissions to a RAM role that you have created for a trusted Alibaba Cloud account, Alibaba Cloud service, or identity provider (IdP). This topic describes how to grant permissions to a RAM role.

> **Note** You cannot grant permissions to a service linked role because the policy that is attached to the role is predefined by the linked cloud service. For more information about service linked roles, see Service-linked roles.

Method 1

You can grant permissions to a RAM role by clicking **Add Permissions** on the **RAM Roles** page.

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **RAM Roles**.
3. On the **RAM Roles** page, find the RAM role in the **RAM Role Name** column.
4. In the **Actions** column, click **Add Permissions**. In the **Add Permissions** pane, the **Principal** field is automatically provided.
5. In the **Authorization Policy Name** column, click the policies that you want to attach to the RAM role.

   > **Note** In the **Selected** section, you can click the cross sign (×) next to a policy to remove the policy.

6. Click **OK**.
7. Click **Complete**.

Method 2

You can grant permissions to a RAM role by clicking **Input and Attach** on the **RAM Roles** page.

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **RAM Roles**.
3. On the **RAM Roles** page, find the RAM role in the **RAM Role Name** column.
4. In the **Actions** column, click **Input and Attach**.
5. In the **Add Permissions** pane, select **System Policy** or **Custom Policy** for the **Type** parameter.
6. Enter a policy name.
7. Click **OK**.
8. Click **Close**.

Method 3

You can grant permissions to a RAM role on the **Grants** page.

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **Grants** under **Permissions**.

3. On the **Grants** page, click **Grant Permission**.
4. In the **Add Permissions** pane, enter a RAM role name in the **Principle** field, and then select the RAM role from the auto-complete results.
5. In the **Authorization Policy Name** column, select the policies that you want to attach to the RAM role.

   > **Note** In the **Selected** section, you can click the cross sign (×) next to a policy to remove the policy.

6. Click **OK**.
7. Click **Complete**.

Related information

- AttachPolicyToRole

6.Remove permissions from a RAM role

You can remove permissions from a RAM role if the RAM role no longer needs the permissions. This topic describes how to remove permissions from a RAM role.

> **Note** You cannot remove permissions from a service linked role because the policies that are attached to the role are predefined by the linked cloud service. For more information about service linked roles, see Service-linked roles.

Method 1

You can remove permissions from a RAM role on the **Grants** page.

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **Grants** under **Permissions**.
3. On the **Grants** page, find the RAM role, and click **Revoke Permission** in the **Actions** column.
4. In the message that appears, click **OK**.

Method 2

You can remove permissions from a RAM role on the **RAM Roles** page.

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **RAM Roles**.
3. On the **RAM Roles** page, click the name of the RAM role in the **RAM Role Name** column.
4. On the **Permissions** tab, find the policy that you want to detach from the RAM role, and click **Remove Permission** in the **Actions** column.
5. In the message that appears, click **OK**.

Related information

- DetachPolicyFromRole

7.Edit the trust policy of a RAM role

You can edit the policy that is attached to a RAM role to change the trusted entity of the RAM role. This topic describes how to change the trusted entity of a RAM role to an Alibaba Cloud account, Alibaba Cloud service, or identity provider (IdP).

Context

When you create a RAM role, you can specify an Alibaba Cloud account, Alibaba Cloud service, or IdP as the trusted entity of the RAM role. In most cases, you do not need to change the trusted entity after you create a RAM role. If you must change the trusted entity, you can use one of the methods described in this topic. After you change the trusted entity, you must check whether the RAM role functions as expected.

Procedure

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 page that appears, click the name of the RAM role in the **RAM Role Name** column.
4. On the page that appears, click the **Trust Policy Management** tab. On this tab, click **Edit Trust Policy**.
5. Modify the trust policy and click **OK**.

Change the trusted entity of a RAM role to an Alibaba Cloud account

If the `Principal` element in a policy includes the `RAM` field, the trusted entity is an **Alibaba Cloud account**. A RAM role to which the policy is attached can be assumed by authorized RAM users of the trusted Alibaba Cloud account.

In the following policy, the RAM role can be assumed by all the RAM users of the Alibaba Cloud account whose ID is 123456789012****.

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "RAM": [
          "acs:ram::123456789012****:root"
        ]
      }
    }
  ],
  "Version": "1"
}
```

If you configure the `Principal` element to the following code, the RAM role can be assumed by the RAM user named `testuser` of the Alibaba Cloud account whose ID is 123456789012****.

```
"Principal": {
  "RAM": [
    "acs:ram::123456789012****:user/testuser"
  ]
}
```

> **Note** Before you edit the trust policy, make sure that you have created a RAM user named `testuser`.

If you configure the `Principal` element to the following code, the RAM role can be assumed by the RAM role named `testrole` of the Alibaba Cloud account whose ID is 123456789012****.

```
"Principal": {
  "RAM": [
    "acs:ram::123456789012****:role/testrole"
  ]
}
```

> **Note** Before you edit the trust policy, make sure that you have created a RAM role named `testrole`.

Change the trusted entity of a RAM role to an Alibaba Cloud service

If the `Principal` element in a policy includes the `Service` field, the trusted entity is an **Alibaba Cloud service**. A RAM role to which the policy is attached can be assumed by a trusted Alibaba Cloud service of the current Alibaba Cloud account.

For example, the following trust policy indicates that the RAM role can be assumed by the Elastic Compute Service (ECS) service of the current Alibaba Cloud account.

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ecs.aliyuncs.com"
        ]
      }
    }
  ],
  "Version": "1"
}
```

Change the trusted entity of a RAM role to an IdP

If the `Principal` element includes the `Federated` field, the trusted entity is an **IdP**. The RAM role can be assumed by all users in the IdP.

In the following policy, the RAM role can be assumed by all users in the IdP named `testprovider` of the Alibaba Cloud account whose ID is 123456789012****.

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Federated": [
          "acs:ram::123456789012****:saml-provider/testprovider"
        ]
      },
      "Condition":{
        "StringEquals":{
          "saml:recipient":"https://signin.alibabacloud.com/saml-role/sso"
        }
      }
    }
  ],
  "Version": "1"
}
```

Additional considerations

The trusted entity of a policy that is attached to a service linked role cannot be changed. This is because the policy is defined by the linked service. For more information about service linked roles, see Service-linked roles.

8.Set the maximum session duration for a RAM role

This topic describes how to use the console or API to set the maximum session duration for a RAM role. If you set the maximum session duration to a large value for a RAM role, RAM users can assume the RAM role to complete time-consuming tasks. If the RAM users call an STS API operation to assume the RAM role, the STS tokens that are returned have a long validity period.

Context

- The maximum session duration for a RAM role ranges from 3,600 seconds to 43,200 seconds. The default maximum session duration is 3,600 seconds.
- The maximum session duration of service linked roles is not configurable.

Use the console to set the maximum session duration for a RAM role

1. Log on to the RAM console with an Alibaba Cloud account.
2. In the left-side navigation pane, click **RAM Roles**.
3. On the **RAM Roles** page, click the name of a RAM role in the **RAM Role Name** column.
4. In the **Basic Information** section, click **Edit** next to **Maximum Session Duration**.
5. In the dialog box that appears, modify the maximum session duration and click **OK**.

Call an API operation to set the maximum session duration for a RAM role

You can set the MaxSessionDuration or NewMaxSessionDuration parameter when you call the CreateRole or UpdateRole operation. For more information, see CreateRole and UpdateRole.

What's next

After you set the maximum session duration for a RAM role, you can use the console or an STS API operation to assume the RAM role. You can also use the RAM role for role-based single sign-on (SSO). For more information, see the following topics:

- Assume a RAM role
- Overview of role-based SSO
- AssumeRole
- AssumeRoleWithSAML

9.Assume a RAM role

This topic describes how a Resource Access Management (RAM) user uses the RAM console and API to assume a RAM role whose trusted entity is an Alibaba Cloud account.

Prerequisites

The following prerequisites must be met:

1. A RAM user is created. For more information, see Create a RAM user.
2. An AccessKey pair is created or a logon password is set for the RAM user.
   - For more information about how to set a logon password, see Change the password of a RAM user.
   - For more information about how to create an AccessKey pair, see Create an AccessKey pair for a RAM user.
3. The RAM user is granted the required permissions. For more information, see Grant permissions to a RAM user.
   - You can attach the `AliyunSTSAssumeRoleAccess` system policy to the RAM user. This allows the RAM user to assume all RAM roles.
   - You can attach a custom policy to the RAM user to specify the RAM role that the RAM user can assume. For more information, see FAQ about RAM roles and STS tokens.

Method 1: Use the RAM console

To assume a RAM role, a RAM user must log on to the RAM console and then switch the logon identity to the RAM role. The RAM user can either log on to the console by using a password or using role-based single sign-on (SSO).

1. Log on to the RAM console as a RAM user.
2. Move the pointer over the profile picture in the upper-right corner. Find and copy the value of the **Current Alias** field.
3. Click **Switch Role**.
4. On the **Switch Role** page, enter the alias that you copied earlier.

   > **Note** On the **Switch Role** page, you can also enter the default domain name in the **Enterprise Alias / Default Domain Name** field. For more information about the default domain name, see Manage the default domain name.

5. Specify the **Role Name** field.
6. Click **Switch**.

   After the switch is complete, your logon identity changes to the RAM role and you have the permissions that are granted to the RAM role.

   You can view the logon identity and current identity when you move the pointer over the profile picture in the upper-right corner of the console. The following table describes the logon identity and current identity. The current identity is indicated by the **My Identity** field.

Logon method	Logon identity	Current identity
Password-based logon	The format is <Username of the logon RAM user>.	The format is <RoleName>/<RoleSessionName>. ○ RoleName: the name of the role that is assumed by the RAM user ○ RoleSessionName: the username of the RAM user
Role-based SSO	After you log on to the console as a RAM role, the current identity is displayed and the logon identity is not displayed. If you switch the identity to another RAM role, the logon identity is displayed in the format of <RoleName>/<RoleSessionName>. ○ RoleName: the name of the role that is used for SSO ○ RoleSessionName: the RoleSessionName attribute in the role-based SSO authentication response For example, the tom@example.local user of a trusted IdP logs on to the Alibaba Cloud Management Console as the RAM role test-saml-role1 and switches the identity to the RAM role alice-testrole. In this case, the logon identity is test-saml-role1/tom@example.local.	The format is <RoleName>/<RoleSessionName>. ○ RoleName: the name of the role that is assumed ○ RoleSessionName: the RoleSessionName attribute in the role-based SSO authentication response For example, the tom@example.local user of a trusted IdP logs on to the console as the RAM role test-saml-role1 and switches the identity to the RAM role alice-testrole. In this case, the current identity is alice-testrole/tom@example.local. The value of RoleSessionName remains unchanged.

The maximum duration of the logon session depends on the smaller value of the **Maximum Session Duration** and **Logon Session Valid For** parameters. For more information, see Set the maximum session duration for a RAM role and Set security policies for RAM users.

Method 2: Use the API

An authorized RAM user can use an AccessKey pair to call the AssumeRole operation. This way, the RAM user obtains an STS token. The RAM user can then use the STS token to access Alibaba Cloud resources.

> **Note** If STS tokens that you obtain after assuming RAM roles are disclosed, you can disable all of the STS tokens. For more information, see FAQ about RAM roles and STS tokens.

References

For information about how to log on to the console by using role-based SSO, see Overview of role-based SSO.

10.Delete a RAM role

This topic describes how to delete a RAM role that you no longer need.

Prerequisites

No policies are attached to the RAM role.

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **RAM Roles**.
3. On the **RAM Roles** page, find the target RAM role in the **RAM Role Name** column, and click **Delete** in the **Actions** column.
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 minutes to complete. After the role is deleted, a success message appears. If a RAM role fails to be deleted, click **View Details** in the error message and troubleshoot the error.

Related information

- DeleteRole