ALIBABA CLOUD

# Alibaba Cloud

## Resource Access Management

## FAQ

Document Version: 20220412

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.FAQ about RAM users

This topic provides answers to some frequently asked questions about the logon, billing, and permissions of Resource Access Management (RAM) users.

## What are the logon URL and logon names of RAM users?

RAM users can use the following URL to log on: Logon URL of RAM users.

> **Note** Alternatively, you can log on to the RAM console by using an Alibaba Cloud account and find the logon URL of RAM users on the **Overview** page. If you use the URL on the Overview page to visit the logon page, the system automatically provides the default domain name. This way, you need only to enter the username.

You can log on to the console as a RAM user by using one of the following logon names:

- Logon name 1: default domain name. The format of the logon name of the RAM user is `<UserName>@<AccountAlias>.onaliyun.com`, such as username@company-alias.onaliyun.com.

  > **Note** The logon name of the RAM user is in the User Principal Name (UPN) format. All logon names that are listed in the RAM console follow this format. `<UserName>` indicates the username of the RAM user. `<AccountAlias>.onaliyun.com` indicates the default domain name. For more information, see Terms and View and modify the default domain name.

- Logon name 2: the account alias. The format of the logon name of the RAM user is `<UserName>@<AccountAlias>`, such as username@company-alias.

  > **Note** `<UserName>` indicates the username of the RAM user. `<AccountAlias>` indicates the account alias. For more information, see Terms and View and modify the default domain name.

- Logon name 3: the domain alias. If you have configured a domain alias, you can use this logon name. The format of the logon name of the RAM user is `<UserName>@<DomainAlias>`, such as username@example.com.

  > **Note** `<UserName>` indicates the username of the RAM user. `<DomainAlias>` indicates the domain alias. For more information, see Terms and Create and verify a domain alias.

## What are the default domain name and domain alias?

The default domain name is a unique identifier of an Alibaba Cloud account. Alibaba Cloud assigns a default domain name to each Alibaba Cloud account. The format of the default domain name is `<AccountAlias>.onaliyun.com`. This unique identifier can be used for RAM user logon and single sign-on (SSO). For more information, see View and modify the default domain name.

If you have a custom domain name that is publicly resolvable, you can use this domain name to replace the default domain name. This custom domain name is called a domain alias. A domain alias is the alias of the default domain name. For more information, see Create and verify a domain alias.

> **Note** A domain alias can be used only after the ownership of the custom domain is verified. After the ownership of the custom domain is verified, you can use the domain alias to replace the default domain name in all scenarios in which the default domain name is required.

## What permissions are required for a RAM user to purchase Alibaba Cloud resources?

- If a RAM user wants to purchase an Alibaba Cloud service on a pay-as-you-go basis, the permissions to create instances or resources are required.
- If a RAM user wants to purchase an Alibaba Cloud resource on a subscription basis, both the permissions to create instances and the permissions to make payments are required. To grant the permissions to make payments, you must attach the `AliyunBSSOrderAccess` policy to the RAM user.
- If a RAM user purchases a resource, the RAM user may need to use or create other resources. In this case, the permissions to read or create the resources are required.

  The following example is a policy that contains the permissions required to create Elastic Compute Service (ECS) instances.

  If the following policy is attached to a RAM user, the RAM user can create ECS instances from launch templates.

```
{ "Version": "1", "Statement": [ { "Action": [ "ecs:DescribeLaunchTemplates", "ecs:CreateInstance", "ecs:RunInstances", "ecs:DescribeInstances", "ecs:DescribeImages", "ecs:DescribeSecurityGroups" ], "Resource": "*", "Effect": "Allow" }, { "Action": [ "vpc:DescribeVpcs", "vpc:DescribeVSwitches" ], "Resource": "*", "Effect": "Allow" } ] }
```

  If the RAM user wants to use or create other resources when the RAM user creates an ECS instance, the specific permissions are required. The following table lists the operations on other resources and the required policies.

| Operation | Policy |
| --- | --- |
| Use a snapshot to create an ECS instance | `ecs:DescribeSnapshots` |
| Create and use a VPC | ○ `vpc:CreateVpc`<br>○ `vpc:CreateVSwitch` |
| Create and use a security group | ○ `ecs:CreateSecurityGroup`<br>○ `ecs:AuthorizeSecurityGroup` |
| Assign a RAM role to an ECS instance | ○ `ecs:DescribeInstanceRamRole`<br>○ `ram:ListRoles`<br>○ `ram:PassRole` |
| Use an AccessKey pair | ○ `ecs:CreateKeyPair`<br>○ `ecs:DescribeKeyPairs` |
| Create an ECS instance on a dedicated host | `ecs:AllocateDedicatedHosts` |

> **Note**
>
> - For more information about how to create custom policies, see Create a custom policy.
> - For more information about how to grant permissions to RAM users, see Grant permissions to a RAM user.

## Why is a RAM user unable to access the resources after it has been granted the required permissions?

- Check whether the policy that is attached to the RAM user is accurate.
- Check whether custom policies that are attached to the RAM user contain `"Effect": "Deny"` to restrict the use of resources or operations. The policies may have been attached to the RAM user or a RAM user group that includes the RAM user.

  For example, both the `AliyunECSReadOnlyAccess` system policy and the following custom policy are attached to the RAM user. In this case, the RAM user is not allowed to view ECS resources because a Deny statement takes precedence over an Allow statement.

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

## Why can a RAM user perform operations on resources without the required permissions?

For example, a RAM user can view the list of ECS instances even if the `AliyunECSFullAccess` system policy, the `AliyunECSReadOnlyAccess` system policy, or related custom policies are not attached to the RAM user.

- Check whether the policies are attached to the RAM user group that includes the RAM user.
- Check whether other policies attached to the RAM user contain the required permissions.

  For example, the `AliyunCloudMonitorFullAccess` system policy indicates full access to CloudMonitor. This policy contains the following permissions: `"ecs:DescribeInstances"`, `"rds:DescribeDBInstances"`, and `"slb:DescribeLoadBalancer"`. If the `AliyunCloudMonitorFullAccess` policy is attached to the RAM user, the RAM user can view the information about ECS, ApsaraDB RDS, and Server Load Balancer (SLB) instances.

## How do I grant a RAM user the permissions to manage renewals?

You must create a custom policy to manage the renewals of a specific cloud service and attach the policy to the RAM user. A renewal management policy for all cloud services does not exist. The permissions to purchase a specific service and make payments are required for RAM users to manage renewals.

For example, if you want to authorize a RAM user to manage ECS instance renewals, you must grant the required permissions described in What permissions are required for a RAM user to purchase Alibaba Cloud services? You must also attach the `AliyunBSSOrderAccess` policy to the RAM user.

## How is a RAM user charged for consumed resources?

- The fees that a RAM user is charged are billed to the parent Alibaba Cloud account.
- By default, a RAM user can use the discounts that are applied to the parent Alibaba Cloud account.

- Financial configurations such as the consumption budget, credit limit, and payment methods apply to all RAM users that belong to an Alibaba Cloud account. Financial configurations that apply to a single RAM user are unavailable.
- RAM users can be authorized to add funds to the parent Alibaba Cloud account. The added funds belong to the Alibaba Cloud account.
- RAM users and RAM user groups are not separately billed.

## I have granted permissions in RAM but the permissions do not immediately take effect on cloud services. Why?

RAM is deployed in multiple regions and zones to achieve high availability. RAM copies data between different regions and uses the eventual consistency model. After you grant permissions in RAM, RAM delivers the permission data to all Alibaba Cloud regions and zones. Then, all cloud services can use the information for authentication. If a failure occurs in a region or a zone, RAM switches over to an available region or zone based on its high-availability disaster recovery mechanism.

After RAM delivers the permission data, it takes a period of time for the permissions to take effect. Therefore, if you grant or change permissions, you must wait for a period of time before the permissions take effect on cloud services.

RAM ensures the eventual consistency of permission data.

# 2.FAQ about RAM roles and STS tokens

This topic provides answers to some frequently asked questions about Resource Access Management (RAM) roles and Security Token Service (STS) tokens.

## What are the types of RAM roles?

RAM roles are classified into the following types based on the trusted entity:

- **Alibaba Cloud account**
- **Alibaba Cloud service**
- **Identity provider (IdP)**

## What entities can assume the three types of RAM role?

- **Alibaba Cloud account**: RAM users of a trusted Alibaba Cloud account can assume this type of RAM role. RAM users that assume this type of RAM role can belong to their owner 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 the access across Alibaba Cloud services. RAM roles that Elastic Compute Service (ECS) instances assume are categorized into this type of RAM role. In this case, the trusted entity is ECS. For more information, see Use RAM roles to access other Alibaba Cloud services.
- **IdP**: Users of a trusted IdP can assume this type of RAM role. This type of RAM role is used to implement single sign-on (SSO) between Alibaba Cloud and a trusted IdP.

## Can I specify the RAM role that a RAM user can assume?

Yes, you can specify the RAM role that a RAM user can assume. You can create a custom policy to specify the RAM role that a RAM user can assume. The following sample code provides an example of a custom policy:

```
{ "Statement": [ { "Action": "sts:AssumeRole", "Effect": "Allow", "Resource": "acs:ram:*:<account-id>:role/<role-name>" } ], "Version": "1" }
```

> **Note**
>
> - In this policy, the `Resource` element specifies the Alibaba Cloud Resource Name (ARN) of the RAM role. In this element, `<account-id>` specifies the Alibaba Cloud account and `<role-name>` specifies the name of the RAM role. For more information about how to view the ARN of a RAM role, see How do I find the ARN of the RAM role?
> - You can attach this policy to the RAM user to specify the RAM role that a RAM user can assume. For more information about how to attach a policy to a RAM user, see Grant permissions to a RAM user.

## How do I view the ARN of a RAM role?

1. Log on to the RAM console.

2. In the left-side navigation pane, choose **Identities > Roles**.
3. On the Roles page, click the name of the RAM role whose ARN you want to view.
4. In the **Basic Information** section, view the ARN of the RAM role.


## Why does an error occur when a RAM user accesses STS?

When a RAM user uses the API, a CLI, or an SDK to call the AssumeRole operation, the following error message may be returned:

```
Error message: You are not authorized to do this action. You should be authorized by RAM.
```

You can refer to the following information to troubleshoot the error:

- The required policies are not granted to the RAM user. To resolve this issue, attach the AliyunSTSAssumeRoleAccess policy or a custom policy to the RAM user. For more information, see Can I specify the RAM role that a RAM user can assume?
- The RAM user is not authorized to assume the RAM role. To resolve this issue, add the RAM user to the Principal element in the trust policy of the RAM role. For more information, see Edit the trust policy of a RAM role.

## Is the number of STS API requests limited?

Yes, the number of STS API requests is limited. The AssumeRole operation can be called up to 6,000 times per minute for each Alibaba Cloud account. API requests that are sent by using RAM users and RAM roles within the Alibaba Cloud account are also counted.

If the number of API requests exceeds 6,000, one of the following error messages is returned for the excessive requests:

- Error messages

| Error code | Error message |
| --- | --- |
| Throttling.Api | Request was denied due to api flow control. |
| Throttling.User | Request was denied due to user flow control. |
| Throttling | Request was denied due to flow control. |

- HTTP status code `302`

If one of the preceding error messages or HTTP status code 302 is returned, reduce the number of concurrent STS API requests. If your services require a higher quota on concurrent STS API requests, you can submit a ticket to increase the quota.

## What are the permissions of an STS token?

The permissions of an STS token are the permissions that are owned by the specified RAM role and included in the value that you specify for the `Policy` parameter when you call the AssumeRole operation.

> **Note** If you do not configure the Policy parameter when you call the AssumeRole operation, the returned STS token has all the permissions of the specific RAM role.

## What is the validity period of an STS token?

The validity period of an STS token ranges from 900 seconds to the maximum session duration that you specify. The default validity period is 3,600 seconds.

> **Note**
>
> - You can configure the DurationSeconds parameter when you call the AssumeRole operation to specify the validity period of an STS token.
> - You can use the RAM console or call the API to configure the maximum session duration of a RAM role. For more information, see Specify the maximum session duration for a RAM role.

## If I obtained multiple STS tokens at different points in time, are the old and new tokens valid at the same time?

Yes, the old and new tokens are valid at the same time. All STS tokens are valid before they expire.

## What do I do if STS tokens are disclosed?

If the STS tokens that are obtained after a RAM user assumes a RAM role are disclosed, perform the following steps to disable the STS tokens:

1. Log on to the RAM console by using an Alibaba Cloud account.
2. Detach all policies from the RAM role.

   For more information, see Revoke permissions from a RAM role.
3. Delete the RAM role.

   For more information, see Delete a RAM role.

   After the RAM role is deleted, the STS tokens that are not expired become invalid.

If you want to continue using the deleted RAM role, create a RAM role that has the same name and attach the same policies to the new RAM role.

# 3.FAQ about AccessKey pairs

This topic provides answers to some frequently asked questions about AccessKey pairs.

## What does an AccessKey pair consist of?

An AccessKey pair consists of an AccessKey ID and an AccessKey secret.

- The AccessKey ID is used to identify a user.
- The AccessKey secret is used to verify the identity of the user. You must keep your AccessKey secret strictly confidential.

## What information can I view after I create an AccessKey pair?

After you create an AccessKey pair, you can view basic information such as the AccessKey ID, the status of the AccessKey pair, the time when the AccessKey pair was last used, and the time when the AccessKey pair was created. For more information, see View the information about an AccessKey pair.

## Can I view the AccessKey ID after I create an AccessKey pair?

Yes, you can view the AccessKey ID after you create an AccessKey pair.

## Can I view the AccessKey secret after I create an AccessKey pair?

No, you cannot view the AccessKey secret after you create an AccessKey pair. The AccessKey secret is displayed only when you create the AccessKey pair and is unavailable for subsequent queries.

## How do I check whether an AccessKey pair is in use?

You can view the time when an AccessKey pair was last used in the console or by calling an operation. This helps you check whether the AccessKey pair is in use.

- AccessKey Pair page

  If you access the AccessKey Pair page by using an Alibaba Cloud account, you can view the time when the AccessKey pair of the Alibaba Cloud account was last used. If you access the AccessKey Pair page by using a RAM user, you can view the time when the AccessKey pair of the RAM user was last used.

- RAM console

  If you log on to the RAM console by using an Alibaba Cloud account or a RAM user that has administrative rights, you can view the time when the AccessKey pairs of all RAM users were last used. For more information, see View the information about an AccessKey pair.

- GetAccessKeyLastUsed

  You can call this operation to view the time when the AccessKey pair of an Alibaba Cloud account or RAM user was last used.

## Can I change the AccessKey ID after I create an AccessKey pair?

No, you cannot change the AccessKey ID after you create an AccessKey pair. You can only disable, enable, or delete an AccessKey pair.

## Can I restore an AccessKey pair after I delete it?

No, you cannot restore an AccessKey pair that is deleted.

> **Note** Proceed with caution when you delete an AccessKey pair. If you delete an AccessKey pair that is in use, system failures may occur on your application.

# 4.What can I do if I fail to close my Alibaba Cloud account?

Before you close an Alibaba Cloud account, you must delete all the Resource Access Management (RAM) resources of the Alibaba Cloud account. Otherwise, the Alibaba Cloud account cannot be closed.

- If your Alibaba Cloud account has passed real-name verification, you can use the RAM console or RAM API to delete the custom resources of the account. Perform the following operations:
  - Delete all RAM users.

    For more information, see Delete a RAM user.
  - Delete all RAM user groups.

    For more information, see Delete a RAM user group.
  - Delete all RAM roles.

    For more information, see Delete a RAM role.
  - Delete all custom policies.

    For more information, see Delete a custom policy.
  - Delete all identity providers (IdPs).

    For more information, see Delete a SAML IdP.
  - Delete all virtual multi-factor authentication (MFA) devices.

    In most cases, when a RAM user is deleted, the virtual MFA device bound to the RAM user is synchronously deleted. However, a virtual MFA device cannot be deleted in the following cases:

    - You requested to bind a virtual MFA device to a RAM user but the request failed. In this case, additional virtual MFA devices were generated.
    - You created a virtual MFA device by calling the CreateVirtualMFADevice operation but you did not bind it to a RAM user.

    To resolve the issue, you can call the ListVirtualMFADevices operation to query all the virtual MFA devices of the current Alibaba Cloud account. Then, call the DeleteVirtualMFADevice operation to delete these virtual MFA devices.
  - Change the custom default domain name to the default account ID.

    a. View your account ID

       Log on to the Alibaba Cloud Management Console. In the upper-right corner, move the pointer over the profile and click **Security Settings**. On the Security Settings page, view the account ID.

    b. Change the default domain name to the account ID.

       For more information, see View and modify the default domain name.
- If your Alibaba Cloud account has not passed real-name verification, you cannot use the RAM service. However, you may have created RAM roles to use other cloud services. In this case, you can use RAM API or the command-line interface (CLI) to delete these roles.

  Alibaba Cloud Shell is used as an example to show how to delete RAM roles.

i. Run the following command to query the RAM roles of the account:

```
aliyun ram ListRoles
```

ii. Check whether the RAM roles to be deleted are service-linked roles. For more information, see Service-linked roles.

Roles that start with "AliyunServiceRoleFor" are service-linked roles.

iii. Deletes RAM roles.

- Perform the following steps to delete a service-linked role:
  a. Run the following command to delete the service-linked role:

```
aliyun resourcemanager DeleteServiceLinkedRole --secure --force --RoleName $role_name
```

Replace `$role_name` with the actual role name.

  b. Run the following command to check whether the service-linked role is deleted:

```
aliyun resourcemanager GetServiceLinkedRoleDeletionStatus --DeletionTaskId $task_id
```

Replace `$task_id` with `DeletionTaskId` returned in the previous step. If the returned `Status` is `SUCCEEDED`, the service-linked role is deleted.

- Run the following command to delete a normal service role:

```
aliyun ram DeleteRole --secure --force --RoleName $role_name --CascadingDelete true
```

Replace `$role_name` with the actual role name.

iv. Run the following command to check whether all the RAM roles of your account are deleted:

```
aliyun ram ListRoles
```