Alibaba Cloud

Resource Access Management

FAQ

Document Version: 20201009
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

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

---

> Document Version: 20201009
Table of Contents

1. FAQ about RAM users ......................................................... 05
2. FAQ about RAM roles and STS tokens .................................. 10
3. FAQ about AccessKey pairs .............................................. 13
1. FAQ about RAM users

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

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

You can visit the RAM user logon page.

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 this URL to visit the logon page, the system automatically provides the default domain name and you only need to enter the username.

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

- **Logon name 1**: `<$username>@<$AccountAlias>.onaliyun.com`. Example: `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.

- **Logon name 2**: `<$username>@<$AccountAlias>`. Example: `username@company-alias`.

  Note: `<$username>` indicates the username of the RAM user. `<$AccountAlias>` indicates the account alias.

- **Logon name 3**: `<$username>@<$DomainAlias>`. You can use this logon name if you have configured a domain alias.

  Note: `<$username>` indicates the username of the RAM user. `<$DomainAlias>` indicates the domain alias.

What are the default domain name and domain alias?

For more information about the default domain name and domain alias, see Terms.

To view and manage the default domain name and domain alias, perform the following steps:

1. Log on to the RAM console by using an Alibaba Cloud account or as a RAM user who has the RAM management permissions.
2. In the left-side navigation pane, click Settings under Identities.
3. On the Settings page, click the Advanced tab. On this tab, you can view and manage the default domain name and domain alias.

What permissions does a RAM user need to purchase Alibaba Cloud services?
• If a RAM user wants to purchase an Alibaba Cloud service on a pay-as-you-go basis, the RAM user only needs the permission to create instances or resources.

• If a RAM user wants to use the subscription billing method, both the permission to create instances and the permission to make payments are required. To acquire the permission to make payments, the RAM user must be attached with the `AliyunBSSOrderAccess` policy.

• When a RAM user purchases a service, the RAM user may need to use or create other resources. In this case, the RAM user must be authorized to read or create the resources.

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

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

```json
{
  "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 you need to use or create other resources when creating an ECS instance, the corresponding permissions are required. The following table lists the operations on other resources and the required permissions.
Note
- For information about how to create a custom policy, see Create a custom policy.
- For information about how to attach policies to RAM users, see Grant permissions to a RAM user.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a snapshot to create an ECS instance</td>
<td>ecs:DescribeSnapshots</td>
</tr>
<tr>
<td>Create and use a VPC</td>
<td>vpc:CreateVpc</td>
</tr>
<tr>
<td></td>
<td>vpc:CreateVSwitch</td>
</tr>
<tr>
<td>Create and use a security group</td>
<td>ecs:CreateSecurityGroup</td>
</tr>
<tr>
<td></td>
<td>ecs:AuthorizeSecurityGroup</td>
</tr>
<tr>
<td>Assign a RAM role to an ECS instance</td>
<td>ecs:DescribeInstanceRamRole</td>
</tr>
<tr>
<td></td>
<td>ram:ListRoles</td>
</tr>
<tr>
<td></td>
<td>ram:PassRole</td>
</tr>
<tr>
<td>Use an AccessKey pair</td>
<td>ecs:CreateKeyPair</td>
</tr>
<tr>
<td></td>
<td>ecs:DescribeKeyPairs</td>
</tr>
<tr>
<td>Create an ECS instance on a dedicated host</td>
<td>ecs:AllocateDedicatedHosts</td>
</tr>
</tbody>
</table>

Why is a RAM user unable to access the resources after I have granted the RAM user 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.
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 a RAM user, the RAM user can view the information of ECS, ApsaraDB for RDS, and Server Load Balancer (SLB) instances.

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

You must create a custom policy of renewal management for 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 the service and make payments are required for RAM users to enable renewal management.

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 does a RAM user need 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 are incurred by a RAM user are billed to the parent Alibaba Cloud account.
- A RAM user can use the discounts that are applied to the parent Alibaba Cloud account by default.
- Financial configurations such as 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 or RAM user groups are not separately billed. We recommend that you use Resource Management if you want to obtain bills that contain detailed charges incurred by each RAM user. For more information, see.
2. FAQ about RAM roles and STS tokens

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

How are RAM roles classified?

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

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

What entities can assume the three types of RAM roles?

- **Alibaba Cloud account**: RAM users under an Alibaba Cloud account can assume this type of RAM role. RAM users who assume this type of RAM 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. For example, an ECS instance can assume a RAM role of this type. The trusted entity of the RAM role is the ECS service. 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. The RAM roles of this type are 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 create a custom policy to specify the RAM role that a RAM user can assume. The following sample code gives an example of a custom policy:

```json
{
   "Statement": [
      {
         "Action": "sts:AssumeRole",
         "Effect": "Allow",
         "Resource": "acs:ram::$accountId:role/$roleName"
      }
   ],
   "Version": "1"
}
```
In this policy, the Resource element indicates the Alibaba Cloud Resource Name (ARN) of the RAM role. For more information about how to find the ARN of a RAM role, see How do I find the ARN of the RAM role? In this element, $accountId$ indicates the ID of the Alibaba Cloud account and $roleName$ indicates the name of the RAM role.

The preceding policy specifies the RAM role that a RAM user can assume. For more information about how to attach the policy to the RAM user, see Grant permissions to a RAM user.

How do I find the ARN of a RAM role?

1. To find the ARN of a RAM role, log on to the RAM console.
2. In the left-side navigation pane, click RAM Roles. On the RAM Roles page, click the name of the RAM role.
3. 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, CLI, or 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.

The error message is returned due to the following causes:

- The required permissions are not granted to the RAM user. To resolve this issue, grant the RAM user the required permissions by attaching 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 Change the trusted entity of a RAM role.

Is the number of STS API requests limited?

Yes, STS supports up to 100 AssumeRole API requests per second for each Alibaba Cloud account. API requests that are sent by using RAM users and RAM roles under the Alibaba Cloud account are also counted. If the number of API requests reaches 100, the following error message is returned:
What are the permissions of an STS token?

The permissions of an STS token are the specified RAM role’s permissions in the policy that is specified by the `Policy` parameter when the `AssumeRole` API operation is called.

**Note** If you do not specify the `Policy` parameter when calling the `AssumeRole` API operation, the returned STS token has all the permissions of the specified 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 specify the `DurationSeconds` parameter when you call the `AssumeRole` API operation to set the validity period of an STS token.
- You can use the console or API to set the maximum session duration of a RAM role. For more information, see [Set the maximum session duration for a RAM role](#).

If multiple STS tokens have been obtained at different times, are the old and new tokens valid at the same time?

All STS tokens are valid before their expiration time.

What can I do if STS tokens are disclosed?

If STS tokens that RAM users obtain after assuming a RAM role are disclosed, perform the following steps to disable all of the STS tokens:

1. Log on to the [RAM console](#) with an Alibaba Cloud account.
2. Detach all policies from the RAM role. For more information, see [Remove permissions from a RAM role](#).
3. Delete the RAM role. For more information, see [Delete a RAM role](#).

   After the RAM role is deleted, all of the STS tokens that are obtained by assuming the RAM role and have not expired become invalid.

If you want to continue using the deleted RAM role, create a RAM role with the same name and grant the same permissions to the new RAM role.
3. FAQ about AccessKey pairs

This topic answers some frequently asked questions (FAQ) about AccessKey pairs.

What information is displayed the first time I create an AccessKey pair?

When you create an AccessKey pair for the first time, the following information is displayed:

- AccessKey ID
- AccessKey secret

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

After creating an AccessKey pair, you can view the basic information of the AccessKey pair in the RAM console. For more information, see View the basic information about AccessKey pairs.

Note

You can only view the basic information of the AccessKey pair, such as the AccessKey ID, status, creation time, and last usage time.

Can I view the AccessKey ID in the RAM console after I create an AccessKey pair?

Yes, you can view the AccessKey ID in the RAM console after creating an AccessKey pair.

Can I view the AccessKey secret in the RAM console after I create an AccessKey pair?

No, you cannot view the AccessKey secret in the RAM console after you create an AccessKey pair. The AccessKey secret is only displayed when you create an AccessKey pair, and is unavailable for subsequent queries. We recommend that you save the AccessKey secret for subsequent use.

How can I view the AccessKey secret?

When creating an AccessKey pair, you can save the AccessKey pair information to a local file by using the following two methods:
Click **Download CSV File** to download the file that contains the AccessKey pair information to a local location. The information includes the status, AccessKey ID, and AccessKey secret.

Click **Copy** to save the AccessKey ID and AccessKey secret to a local file.

**How can I check whether an AccessKey pair is in use?**

You can view the last usage time of an AccessKey pair to check whether the pair is in use.

<table>
<thead>
<tr>
<th>AccessKey ID</th>
<th>Status</th>
<th>Last Used</th>
<th>Created</th>
<th>Updated</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample</td>
<td>Enabled</td>
<td>2020-09-25</td>
<td>2020-09-25</td>
<td>2020-09-25</td>
<td>Enable</td>
</tr>
</tbody>
</table>

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

No, you cannot change the AccessKey ID. The AccessKey ID can only be enabled, disabled, or deleted.

**Can I restore an AccessKey pair after it is deleted?**

No, you cannot restore an AccessKey pair that has been deleted, including the AccessKey ID and AccessKey secret.

**Note** Use caution: If you delete an AccessKey pair that is in use, a system error may occur.