ALIBABA CLOUD

Alibaba Cloud

Resource Access Management

Quick Start

Document Version: 20220129

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.Introduction 05
2.Configure security policies for RAM users 06
3.Create a RAM user 08
4.Create a user group 10
5.Create a custom policy 11
6.Grant permissions to a RAM user 14
7.Log on to the console as a RAM user 16

1.Introduction

This topic describes how to get started with Alibaba Cloud Resource Access Management (RAM). You can use the RAM service to control permissions on Alibaba Cloud resources.

Prerequisites

An Alibaba Cloud account is created. To create an Alibaba Cloud account, visit the account registration page.

Operations in the RAM console

- Set security policies to protect your Alibaba Cloud account. For more information, see Configure security policies for RAM users.
- Create RAM users. A RAM user is an entity that is created in Alibaba Cloud to represent a person or application that interacts with Alibaba Cloud. For more information, see Create a RAM user.
- Create RAM user groups to classify and organize RAM users under your Alibaba Cloud account for easier user and permission management. For more information, see Create a user group.
- Grant permissions to RAM users so that the users can access Alibaba Cloud resources. For more information, see Grant permissions to a RAM user.
- Create custom policies to perform finer-grained permission control. For more information, see Create a custom policy.
- Log on to the Alibaba Cloud Management Console as a RAM user. Then, you can access Alibaba Cloud resources and perform necessary operations. For more information, see Log on to the console as a RAM user.

References

You can also perform custom development by using diverse API operations, SDK packages, and other easy-to-use tools. For more information, visit the RAM learning path.

2.Configure security policies for RAM users

This topic describes how to use your Alibaba Cloud account to configure security policies for RAM users.

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Settings**.
3. On the **Security Settings** tab, click **Modify RAM User Security Settings**.
4. In the **Modify RAM User Security Settings** panel, configure the parameters.
   - **Remember MFA for Seven Days**: specifies whether to allow RAM users to remember the multi-factor authentication (MFA) devices for seven days.
   - **Manage Passwords**: specifies whether to allow RAM users to change their passwords.
   - **Manage AccessKey Pairs**: specifies whether to allow RAM users to manage their AccessKey pairs.
   - **Manage MFA Devices**: specifies whether to allow RAM users to enable and disable MFA devices.
   - **MFA for RAM User Logons**: specifies whether MFA is required for all RAM users when the RAM users use usernames and passwords to log on to the Alibaba Cloud Management Console. If you set this parameter to Apply User-specific Configuration, user-specific settings are applied.

     > **Note** If you select Enable for All Users for the MFA for RAM User Logons parameter, MFA for sensitive operations is enabled for all RAM users. If a RAM user wants to perform a sensitive operation in the Alibaba Cloud Management Console, risk control is triggered and the RAM user is required to pass MFA again. For more information, see MFA for sensitive operations.

   - **Logon Session Validity Period**: specifies the validity period of a logon session. The validity period is measured in hours.

     > **Note** If you assume a RAM role or use single sign-on (SSO) to log on to the Alibaba Cloud Management Console, the validity period of your session is no greater than the value of the **Logon Session Validity Period** parameter. For more information, see Assume a RAM role and SAML response for role-based SSO.

   - **Logon Address Mask**: specifies the IP addresses from which you can log on to the Alibaba Cloud Management Console by using a password or SSO. By default, this parameter is left empty, which indicates that logon from all IP addresses is allowed. If you enter IP addresses in this field, console logons, including password-based and SSO-based logon, from these IP addresses are limited. However, API calls that are initiated from these IP addresses by using AccessKey pairs are not limited. You can enter up to 25 IP addresses. If you enter more than one IP address, separate the IP addresses with semicolons (;). The total length of the IP addresses can be a maximum of 512 characters.
5. Click **OK**.

> **Note** The settings take effect on all the RAM users of your Alibaba Cloud account.

Related information

- SetSecurityPreference

3.Create a RAM user

This topic describes how to create a Resource Access Management (RAM) user. A RAM user is an entity that you create in RAM to represent an O&M engineer or application. After you create a RAM user and grant the relevant permissions to the RAM user, the RAM user can access the required Alibaba Cloud resources.

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click **Create User**.
4. In the **User Account Information** section of the **Create User** page, configure the **Logon Name** and **Display Name** parameters.

   > **Note** You can click **Add User** to create multiple RAM users at a time.

5. In the **Access Mode** section, select an access mode.
   - **Console Access**: If you select this option, you must complete the logon security settings. These settings specify whether to use a system-generated or custom logon password, whether the password must be reset upon the next logon, and whether to enable multi-factor authentication (MFA).

     > **Note** If you select Custom Logon Password in the Console Password section, you must specify a password. The password must meet the complexity requirements. For more information about the complexity requirements, see Configure a password policy for RAM users.

   - **OpenAPI Access**: If you select this option, an AccessKey pair is automatically created for the RAM user. The RAM user can call API operations or use other development tools to access Alibaba Cloud resources.

     > **Note** To ensure the security of the Alibaba Cloud account, we recommend that you select only one access mode for the RAM user. This prevents the RAM user from using an AccessKey pair to access Alibaba Cloud resources after the RAM user leaves the organization.

6. Click **OK**.

What's next

- The created RAM user can be used to log on to the RAM console. For more information, see Log on to the console as a RAM user.
- You can attach policies to the RAM user. After you attach a policy, the RAM user can access the Alibaba Cloud resources that are specified in the policy. For more information, see Grant permissions to a RAM user.
- You can add the RAM user to RAM user groups and grant permissions to the RAM user groups. For more information, see Add a RAM user to a RAM user group.

Related information

- CreateUser

4.Create a user group

This topic describes how to create a Resource Access Management (RAM) user group. If you have multiple RAM users that belong to your Alibaba Cloud account, you can create RAM user groups to classify and authorize the RAM users by group. This simplifies the management of RAM users and permissions.

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Groups**.
3. On the **Groups** page, click **Create Group**.
4. On the **Create Group** page, configure the **Group Name**, **Display Name**, and **Note** parameters.
5. Click **OK**.

What's next

You can attach one or more policies to the RAM user group. For more information, see Grant permissions to a RAM user group.

Related information

- CreateGroup

5.Create a custom policy

This topic describes how to create a custom policy. Custom policies provide more fine-grained access control than system policies.

Methods to create a custom policy

You can create a custom policy on one of the following two tabs. The elements that you configured for a custom policy on one tab are synchronized to the other tab. Therefore, you can switch between the two tabs when you create a custom policy.

- Visual Editor Beta: We recommend that you create a custom policy on this tab. This tab provides a GUI. You need only to select configuration items in the Effect, Service, Action, Resource, and Condition sections to create a custom policy. When you create a custom policy on this tab, the system checks your configurations. This ensures the validity of the custom policy. On this tab, you can perform simple operations to create a custom policy.
- JSON: This tab provides a JSON script compiler. You must compile a custom policy statement based on the syntax and structure of RAM policies. On this tab, you can create a custom policy in a flexible manner. This method is suitable for users who are familiar with the syntax and structure of RAM policies.

Before you create a custom policy, you must understand the basic elements, syntax, and structure of RAM policies. For more information, see Policy elements and Policy structure and syntax.

Create a custom policy on the Visual Editor Beta tab

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the **Policies** page, click **Create Policy**.
4. On the **Create Policy** page, click the **Visual Editor Beta** tab.
5. Configure the parameters for a custom policy and click **Next Step**.
   i. In the **Effect** section, select **Allow** or **Deny**.
   ii. In the **Service** section, select an Alibaba Cloud service.

   > **Note** The Alibaba Cloud services that you can select are displayed in the Service section.

   iii. In the **Action** section, select **All Actions** or **Specified Actions**.

   The system displays the actions that can be configured based on the Alibaba Cloud service you select in the previous step. If you select **Specified Actions**, you must select actions.

iv. In the **Resource** section, select **All Resources** or **Specified Resources**.

The system displays the resources that can be configured based on the actions you select in the previous step. If you select **Specified Resources**, you must click **Add Resource** to configure one or more Alibaba Cloud Resource Names (ARNs) of resources. You can also click **Match All** to select all resources for each action that you select.

> **Note** The resource ARNs that are required for an action are tagged with **Required**. We strongly recommend that you configure the resource ARNs that are tagged with Required. This ensures that the custom policy takes effect as expected.

v. (Optional)In the **Condition** section, click **Add Condition** to configure a condition.

Conditions include Alibaba Cloud common conditions and service-specific conditions. The system displays the conditions that can be configured based on the Alibaba Cloud service and the actions that you select. You need only to select a condition key and configure the Operator and Value parameters.

vi. Click **Add Statement** and repeat the preceding steps to configure multiple custom policy statements.

6. Configure the **Name** and **Note** parameters.
7. Check and optimize the content of the custom policy.
   - Basic optimization

     The system automatically optimizes the policy statement. The system performs the following operations during basic optimization:

     - Delete unnecessary conditions.
     - Delete unnecessary arrays.

   - (Optional)Advanced optimization

     You can move the pointer over **Optional: Advanced Optimize** and click **Perform**. The system performs the following operations during advanced optimization:

     - Split resources or conditions that are incompatible with actions.
     - Narrow down resources.
     - Deduplicate or merge policy statements.
8. Click **OK**.

Create a custom policy on the JSON tab

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the **Policies** page, click **Create Policy**.
4. On the **Create Policy** page, click the **JSON** tab.
5. Enter the policy document and click **Next Step**.

   For more information about the syntax and structure of RAM policies, see Policy structure and syntax.
6. Configure the **Name** and **Note** parameters.

7. Check and optimize the content of the custom policy.
   - Basic optimization

     The system automatically optimizes the policy statement. The system performs the following operations during basic optimization:

     - Delete unnecessary conditions.
     - Delete unnecessary arrays.

   - (Optional)Advanced optimization

     You can move the pointer over **Optional: Advanced Optimize** and click **Perform**. The system performs the following operations during advanced optimization:

     - Split resources or conditions that are incompatible with actions.
     - Narrow down resources.
     - Deduplicate or merge policy statements.
8. Click **OK**.

Related information

- CreatePolicy

6.Grant permissions to a RAM user

After a Resource Access Management (RAM) user is granted the relevant permissions, the RAM user can access the required Alibaba Cloud resources. This topic describes how to grant permissions to a RAM user.

Method 1: Grant permissions to a RAM user on the Users page

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, find the RAM user to which you want to grant permissions and click **Add Permissions** in the **Actions** column.
4. In the **Add Permissions** panel, grant permissions to the RAM user.
   i. Select the authorization scope.
      - **Alibaba Cloud Account**: The authorization takes effect on the current Alibaba Cloud account.
      - **Specific Resource Group**: The authorization takes effect on a specific resource group.

        > **Note** If you select Specific Resource Group for Authorized Scope, make sure that the required cloud service supports resource groups. For more information, see Alibaba Cloud services that support resource groups.

   ii. Specify the principal.

      The principal is the RAM user to which permissions are to be granted. By default, the current RAM user is specified. You can also specify another RAM user.

   iii. Select policies.

      > **Note** You can attach a maximum of five policies to a RAM user at a time. If you need to attach more than five policies to a RAM user, perform the operation multiple times.

5. Click **OK**.
6. Click **Complete**.

Method 2: Grant permissions to a RAM user on the Grants page

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Grants**.
3. On the **Grants** page, click **Grant Permission**.
4. On the **Grant Permission** page, grant permissions to a RAM user.

i. Select the authorization scope.
   - **Alibaba Cloud Account**: The authorization takes effect on the current Alibaba Cloud account.
   - **Specific Resource Group**: The authorization takes effect on a specific resource group.

     > **Note** If you select Specific Resource Group for Authorized Scope, make sure that the required cloud service supports resource groups. For more information, see Alibaba Cloud services that support resource groups.

ii. Specify the principal.

   The principal is the RAM user to which permissions are to be granted.

iii. Select policies.

   > **Note** You can attach a maximum of five policies to a RAM user at a time. If you need to attach more than five policies to a RAM user, perform the operation multiple times.

5. Click **OK**.
6. Click **Complete**.

Related information

- AttachPolicyToUser

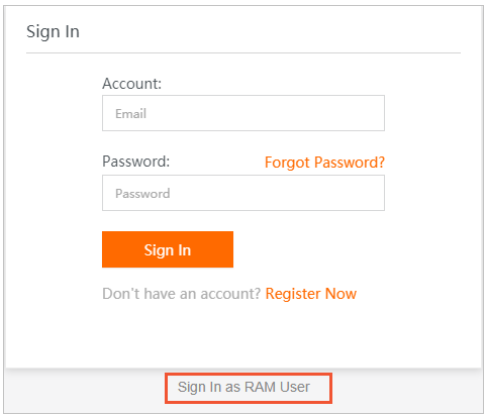
7.Log on to the console as a RAM user

This topic describes how to log on to the Alibaba Cloud Management Console as a RAM user. It also provides the logon methods and URLs.

Context

Two methods are provided to log on to the Alibaba Cloud Management Console:

- On the logon page of the International site (alibabacloud.com) page, click **Sign In as RAM User**.



- Go to the logon page of the Alibaba Cloud Management Console for a RAM user. This topic describes this method.

Procedure

1. Log on to the Alibaba Cloud Management Console as a RAM user.
2. On the **RAM User Logon** page, enter the logon name of the RAM user and click **Next**.
   - Method 1: Use the 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 name of the RAM user. `<AccountAlias>.onaliyun.com` indicates the default domain name. For more information about default domain names, see Terms and View and modify the default domain name.

   - Method 2: Use 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 name of the RAM user. `<AccountAlias>` indicates the account alias. For more information about account aliases, see Terms and View and modify the default domain name.

   - Method 3: Use the domain alias if configured. The format of the logon name of the RAM user is `<UserName>@<DomainAlias>`, such as username@example.com.

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

3. Enter the logon password and click **Log On**.
4. Optional. If you enable multi-factor authentication (MFA), enter the verification code that is provided by the virtual MFA device or configure settings to pass the Universal 2nd Factor (U2F) authentication.

   For more information, see multi-factor authentication (MFA) and Enable an MFA device for a RAM user.