

Alibaba Cloud Resource Access Management

Quick Start

Issue: 20190906

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid <i>Instance_ID</i></code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Introduction.....	1
2 Set a security policy for RAM users.....	2
3 Create a RAM user.....	3
4 Create a RAM user group.....	4
5 Create a custom policy.....	5
6 Grant permission to a RAM user.....	6
7 Log on to the console as a RAM user.....	7

1 Introduction

This topic describes how to quickly get started with Alibaba Cloud Resource Access Management (RAM).

Prerequisites

- An Alibaba Cloud account is created. If not, create one before proceeding. To create an Alibaba Cloud account, click [Create a new Alibaba Cloud account](#).
- The RAM service is activated, and you can log on to the [RAM console](#). If the RAM service is not activated, activate the service before proceeding. For more information, see [#unique_4](#).

Operations in the RAM console

1. Set a security policy to protect your Alibaba Cloud account. For more information, see [#unique_5](#).
2. Create a RAM user. For more information, see [#unique_6](#). A RAM user is an entity that you create in Alibaba Cloud to represent the person or application to interact with Alibaba Cloud.
3. Create a RAM user group to classify and organize RAM users under your Alibaba Cloud account for easier user and permission management. For more information, see [#unique_7](#).
4. Grant permission to a RAM user so that the user can access Alibaba Cloud resources. For more information, see [#unique_8](#).
5. Create a custom policy to perform more precise control. For more information, see [#unique_9](#).
6. Log on the RAM console as a RAM user to access Alibaba Cloud resources and perform necessary operations. For more information, see [#unique_10](#).

What to do next

You can visit the [RAM Learning Path](#) for the knowledge you need to become a RAM expert.

2 Set a security policy for RAM users

This topic describes how to set a security policy for RAM users under your Alibaba Cloud account to better manage RAM user permissions.

Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Settings.
3. On the Security Settings tab, click Update RAM user security settings and set the relevant parameters.
 - **Save MFA Logon Status for 7 Days:** Specifies whether to save the multi-factor authentication (MFA) logon status for your RAM users. The default value is Not Allowed. If you select Allow, the MFA logon status is saved for seven days.
 - **Manage Passwords:** Specifies whether RAM users are allowed to change their own passwords.
 - **Manage AccessKey:** Specifies whether RAM users are allowed to manage their access keys.
 - **Manage MFA Devices:** Specifies whether RAM users are allowed to enable or disable an MFA device.
 - **Logon Session Valid For:** The validity period of the logon sessions. The unit is hours.
 - **Logon Address Mask:** Specifies which IP addresses cannot be used for logon. This parameter is left unspecified by default. That is, all IP addresses can be used for logon. If you specify this parameter, you cannot log on to the console by using a password or through Single Sign On (SSO). However, you can call API actions by using an access key. For information about how to set a logon mask, see [#unique_12](#).
4. Click OK.



Note:

The settings of the security policy apply to all RAM users under your Alibaba Cloud account.

3 Create a RAM user

A RAM user is an entity that you create in Alibaba Cloud to represent the person or application to interact with Alibaba Cloud. You can create a RAM user and grant it the relevant permissions to access the necessary Alibaba Cloud resources.

Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Users.
3. Click Create User, and enter the logon name and display name.



Note:

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

4. Select an access mode. The available access modes are Console Password Logon and Programmatic Access.
 - **Console Password Logon:** If you select this check box, you must also complete the basic security settings for logon, including deciding whether to automatically generate a password or customize the logon password, setting whether the user must reset the password upon the next logon, and setting whether to enable multi-factor authentication (MFA).
 - **Programmatic Access:** If you select this check box, an access key is automatically created for the RAM user. The user can access Alibaba Cloud resources by calling an API action or by using a development tool.



Note:

We recommend that you set only one access mode for the user to maintain the security of your Alibaba Cloud account.

5. Click OK.

What's next

- You can add the RAM user to one or more RAM user groups and grant permission to the user as needed. For more information, see [#unique_14](#).
- You can also attach one or more policies to the RAM user to grant the user access permission. For more information, see [#unique_8](#).

4 Create a RAM user group

This topic describes how to create a RAM user group. If you have multiple RAM users under your Alibaba Cloud account, you can create RAM user groups to classify and organize these RAM users for easier user and permission management.

Procedure

1. Log on to the [RAM console](#).
2. Choose Identities > Groups.
3. Click Create Group, and enter the group name, display name, and description.
4. Click OK.

What's next

You can attach one or more policies to the RAM user group. For more information, see [#unique_16](#).

5 Create a custom policy

This topic describes how to create a custom policy. Custom policies provide more precise control than system policies.

Prerequisites

Before you create a custom policy, we recommend that you read about the basic structure and grammar of a policy. For more information, see [#unique_18](#).

Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Policies.
3. Click Create Policy.
4. Enter a policy name and description.
5. Set the configuration mode.
 - If you set the configuration mode to Visualized, click Add Statement and configure the permission effect, actions, and resources as prompted.
 - If you set the configuration mode to Script, edit the policy according to [policy structure and grammar](#).
6. Click OK.

6 Grant permission to a RAM user

This topic describes how to grant permission to a RAM user. A RAM user can access Alibaba Cloud resources after obtaining relevant permissions.

Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Grants.
3. Click Grant Permission.
4. In the Principal field, enter the username or the user ID, and click the target RAM user.



Note:

You can also enter keywords to search for a specific username.

5. In the Policy Name column, select the target policy and click OK.



Note:

You can click X to revoke your selection.

7 Log on to the console as a RAM user

This topic describes how to log on to the RAM console as a RAM user, including the address and method to log on to the console.

Procedure

1. Log on to the [RAM console](#) as a RAM user.



Note:

To view the address that is used by a RAM user to log on to the console, use your Alibaba Cloud account to log on to the [RAM console](#). The address is displayed on the Overview page.

2. Enter the logon name and then click Next.

- Method 1: Use the default domain name to log on to the console. The format of the logon name for a RAM user is `<$ username >@<$ AccountAli as >. onaliyun . com`, for example, `username@company-alias.onaliyun.com`.



Note:

The logon name of a RAM user must be in the User Principal Name (UPN) format. All logon names listed in the RAM console use this format. `<$username>` represents the username of the RAM user. `<$AccountAlias>.onaliyun.com` represents the default domain name.

- Method 2: Use the enterprise alias to log on to the console. The format of the logon name for a RAM user is `<$ username >@<$ AccountAli as >`, for example, `username@company-alias`.



Note:

`<$username>` represents the username of the RAM user. `<$AccountAlias>` represents the enterprise alias.

- Method 3: If you have set a domain alias, you can also use the domain alias to log on to the console. The format of the logon name for a RAM user is `<$ username >@<$ DomainAlia s >`, for example, `username@example.com`.



Note:

<\$username> represents the username of the RAM user. <\$DomainAlias> represents the domain alias.

3. Enter the logon password and click Log On.