Alibaba Cloud
Resource Access Management

Quick Start

Issue: 20190416

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 `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

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

Contents

1 Introduction

This topic lists the prerequisite to get started with Resource Access Management (RAM):

1. *(Optional) Set MFA*
2. *Set up initial RAM configurations*
3. *Create a RAM user*
4. *(Optional) Create a RAM user group*
5. *(Optional) Create a custom policy*
6. *Authorize RAM users*
7. *Log on to the RAM console as a RAM user*

2 (Optional) Set MFA

This topic describes how to enable and use Multi-Factor Authentication (MFA) to log on to the RAM console.

Activate MFA for your account

We recommend that you activate MFA for your account so that, when you log on, you are prompted to enter your user name and password (first factor) in addition to an authentication code from your specified virtual MFA device (second factor). This method greatly increases the overall security of your account.

Prerequisites

You have installed a virtual MFA application on your smartphone.

Procedure

Depending on the OS of your device, we recommend that you install Google Authenticator as follows:

- For iOS: Install Google Authenticator from the App Store.
  1. Open Google Authenticator and click BEGIN SETUP.
  2. Click Scan barcode and scan the barcode generated on the MFA page.

     Note:
     After scanning the barcode successfully, you will see your account name and MFA key.
  3. On the MFA page, enter two consecutive MFA codes and click Confirm to bind.
- For Android: Install Google Authenticator from Google Play.

  Note:

You need to install a barcode scanner from Google Play for Google Authenticator to identify barcodes.

1. Open Google Authenticator and choose Set up account from the drop-down menu in the upper-right corner.
2. Click Scan a barcode and scan the barcode generated on the MFA page.

   Note:
   After scanning the barcode successfully, you will see your account name and MFA key.
3. On the MFA page, enter two consecutive MFA codes and click Confirm to bind.

3 Set up initial RAM configurations

You can set the account alias, RAM user logon password strength, and RAM user security policies through the RAM console.

Set the account alias

Setting a RAM account alias for your account makes it easier for RAM users to remember the logon portal.

To maintain security of your account, the RAM user logon portal is different from the account logon portal. When logging on to the RAM console, RAM users must provide the RAM account alias of the account and their own user names and passwords.

1. Log on to the *RAM Console*.
2. Choose Identities > Settings > Advanced.
3. In the Domain Management area, click Update.
4. In the displayed dialog box, enter the account alias and click OK.

Set logon password requirements for RAM users

You can set the requirements for password strength for all RAM users. When users reset their passwords, the new passwords must conform to all password requirements .

Procedure

1. Log on to the *RAM Console*.
2. Choose Identities > Settings.
3. On the Security Settings tab page, click Edit Password Rule in the Password Strength Settings area.
4. In the displayed dialog box, set the password rules and click OK.

Set RAM user security policies

You can specify Multi-Factor Authentication (MFA) as a mandatory setting for RAM users. Once MFA is set, you can specify whether the MFA status can be stored on the logon device (for seven days). Additionally, you can specify whether users can manage their passwords, AccessKeys (AKs), and MFA devices.

1. Log on to the *RAM Console*.

2. Choose Identities > Settings.
3. On the Security Settings tab page, click Update RAM user security settings in the RAM User Security area.
4. In the displayed dialog box, set the security rules and click OK.

4 Create a RAM user

Before creating a RAM user, you must *set up initial RAM configurations*.

Procedure

To create a RAM user, follow these steps:

1. Log on to the *RAM Console*.
2. Choose Identities > Users. In the right pane, click Create User.
3. Enter a logon name and display name. To create multiple RAM users at a time, click Add User.
4. Select either Console Password Logon or Programmatic Access as the user access mode.

   Note:
   We recommend that you select only one access mode.

   - If you select Console Password Logon, you can set basic access settings, such as whether to automatically generate a logon password or allow password customization, whether to require resetting the password after the first logon, and whether to enable MFA.
   - If you select Programmatic Access: An AccessKey (AK) is automatically generated for the user.

     Note:

     - To maintain security of the AK, you can view or download its AccessKeyS ecret only during AK creation.
     - If an AK is lost or forgotten, you must create a new one. The new AK and original AK both represent the target user identity. Different AKs of a RAM user are equivalent in use.
     - We recommend that you change AKs for applications on a regular basis to prevent AK disclosure.

What to do next

Grant resource access permissions to specific RAM users.

- For details about how to authorize RAM users, see *Authorize RAM users*.
- For details about how to create fine-grained custom policies, see *(Optional) Create a custom policy*.

5 (Optional) Create a RAM user group

This topic describes how to create a RAM user group.

Procedure

1. Log on to the *RAM Console*.
2. Choose Identities > Groups. In the right pane, click Create Group.
3. In the displayed dialog box, enter Group Name, Display Name, and Note. Then click OK.

6 (Optional) Create a custom policy

Alibaba Cloud offers you a variety of system policies. The policies only provide coarse-grained access control, for example, all permissions or the read-only permission of a specific cloud product.

If you have finer-grained authorization requirements, for example, you want user bob to only read objects from the `oss :// samplebuck et / bob /` directory through an office network, you can create custom policies for access control. (You can search for "My IP address" in a search engine to obtain the IP address of your office network.)

Prerequisites

You understand the basic structure and syntax of a policy. For more information, see *Policy language syntax*.

RAM supports authorization at a finest granularity of API. That is, you can grant each operation permission in a policy by calling a specific API. Make sure that you understand the authorization granularity and methods supported by RAM. For more information, see *Cloud services supporting RAM*.

Procedure

1. Log on to the *RAM Console*.
2. Choose Permissions > Policies.

    Note:
   In the Policies pane, choose System Policy or Custom Policy from the Policy Type drop-down list to view the existing policies. You can only view system policies but can modify custom policies as needed.
3. Click Create Policy.
4. In the displayed dialog box, enter Policy Name. You can also choose to enter Note.
5. Select Visualized or Script for Configuration Mode.
   - If you select Visualized, click Add Statement. In the displayed dialog box, set the permission effect, action, and resource.
   - If you select Script, edit the script. For details, see *Policy structure and syntax*.

What to do next

Grant user bob the created policy. Then, bob has the read-only permission for the objects in the `oss :// samplebuck et / bob /` directory only when user bob access RAM through an office network (for example, with an IP address of 121.0.27.1).

Authorize a RAM user with a policy. For details, see *Authorize RAM users*.

7 Authorize RAM users

You can apply policies to authorize individual RAM users directly or authorize entire RAM user groups as needed. Both methods can grant RAM users the resource access permission.

Policy types

System policies are a group of common policies that meet coarse-grained authorization requirements. For example, you can use system policies to authorize a RAM user to manage orders (through the AliyunBSSFullAccess policy), ECS resources (through the AliyunECSFullAccess policy), or all users and their permissions (through the AliyunRAMFullAccess policy).

You can view all system policies supported by RAM in *Policy overview*.

If you require finer-grained authorization, you can create a custom policy as needed. For more information, see *(Optional) Create a custom policy*.

Authorize RAM users directly

Call the `AttachPoli cyToUser` API to authorize RAM users directly.

1. Log on to the *RAM Console*.
2. Choose Identities > Users.
3. In the User Logon Name/Display Name column, select the target user and click Add Permissions.
4. In the Policy Name column on the left, select the target policies and click OK.

> **Note:**
> To remove a policy, select the policy from the area on the right, and then click ×.

Authorize RAM users by authorizing their user groups

Call the `AttachPoli cyToGroup` API to authorize a user group.

> **Note:**
> The user to be authorized must be included in the target user group.

1. Log on to the *RAM Console*.
2. Choose Identities > Groups.

3. In the Group Name/Display Name column, select the target group and click Add Permissions.
4. In the Policy Name column on the left, select the target policies and click OK.

 Note:
To remove a policy, select the policy from the area on the right, and then click ×.

What to do next

- In the User Logon Name/Display Name column, click a user logon name. On the displayed Permissions tab page, you can navigate to the Individual tab page to view or revoke a permission granted directly to the user.
- In the Group Name/Display Name column, click a group name. On the displayed Permissions tab page, you can view or revoke a permission granted to the group.

8 Log on to the RAM console as a RAM user

The RAM user logon portal is different from the account logon portal. This document describes how to log on to the RAM console as a RAM user.

Logon portal

The RAM user logon portal is *https://signin-intl.aliyun.com/login.htm* (which can be queried on the Overview page in the *RAM Console*).

Logon information

To log on as a RAM user, you must have the RAM user name and password. RAM user names are in the format of <$username>@<$AccountAlias> or <$username>@<$AccountAlias>.onaliyun.com.

For details about how to set an account alias, see *Set up initial RAM configurations*. If no account alias is set, the default account alias is your account ID (you can find the account ID by going to Identities > Settings > Advanced > Domain Management > Default Domain).

9 Limits

This topic lists the limitations of RAM, such as the maximum number of users and the maximum number of user groups.

Item	Limit
Maximum number of users	1,000
Maximum number of user groups	50
Maximum number of groups that a user can join	5
Maximum number of AccessKeys (AKs) that a user can create	2
Maximum number of MFA devices to which a user can attach	1
Maximum number of virtual MFA devices	1,000
Maximum number of custom policies	200
Maximum number of versions that a custom policy can have	5
Maximum number of custom policies that can be attached to a user	5
Maximum number of custom policies that can be attached to a user group	5
Maximum number of custom policies that can be attached to a role	5
Maximum number of system policies that can be attached to a user	20
Maximum number of system policies that can be attached to a user group	20
Maximum number of system policies that can be attached to a role	20
Maximum number of characters that a username can contain	64
Maximum number of characters that a user group name can contain	64

Item	Limit
Maximum number of characters that a policy name can contain	128
Maximum number of characters that a role name can contain	64
Maximum number of roles	100
Number of characters that an alias can contain	3-64
Maximum number of characters that a custom policy name can contain	2,048
Maximum number of identity providers (IdPs)	100
Maximum number of IdP descriptors that an IdP metadata file can contain	1
Maximum number of certificates that an IdP descriptor in an IdP metadata file can contain	2