

Alibaba Cloud

Resource Access Management Best Practices

Document Version: 20220321

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 <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.Use RAM to ensure security of the Alibaba Cloud resources of ...	05
2.Use RAM to manage user permissions and resources	08

1. Use RAM to ensure security of the Alibaba Cloud resources of your enterprise

This topic describes how to use Resource Access Management (RAM) to apply the access and security settings of RAM to Alibaba Cloud resources of your enterprise. This helps you manage resource permissions by implementing fine-grained access control.

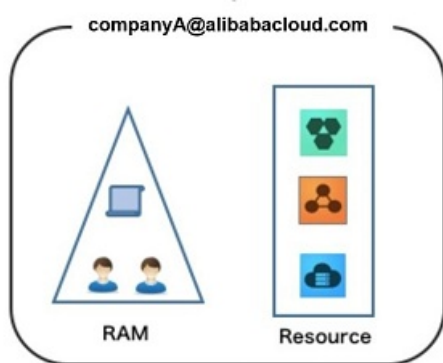
Background information

When you migrate your workloads to the cloud, traditional organizational structures or existing methods used to manage resources may no longer meet your business requirements. You may encounter the following security management issues when you migrate your workloads to the cloud:

- The roles and responsibilities of RAM users are not clear.
- You do not want to share the AccessKey pair of your Alibaba Cloud account with the RAM users due to security concerns.
- The RAM users can use different methods to access resources, which may lead to security risks.
- Resource permissions that are granted to the RAM users must be removed when the RAM users no longer require these permissions.

Solution

To resolve the preceding issues, you can use RAM to create RAM users and grant the RAM users permissions to access the resources. You can use RAM to prevent RAM users from sharing the AccessKey pair of your Alibaba Cloud account. You can also use RAM to grant minimum permissions to RAM users. This way, permission management is simplified, and resource security is ensured.



Security management solution

- **Create RAM users.**

Only one Alibaba Cloud account is required. You can create RAM users for your employees. Then, you can attach different policies to the RAM users. This ensures fine-grained access control. You do not need to use your Alibaba Cloud account to perform O&M.

For more information, see [Create a RAM user](#).

- **Separate console users from API users.**

We recommend that you do not create a logon password for console operations and an AccessKey pair for API operations for a RAM user at the same time.

- To allow an application to access resources by calling API operations, you need only to create an AccessKey pair for the application.
- To allow an employee to manage resources by using the console, you need only to set a logon password for the RAM user of the employee.

For more information, see [Create a RAM user](#).


- **Create and group RAM users.**

If your Alibaba Cloud account has multiple RAM users, you can group the RAM users based on their responsibilities and grant permissions to the groups.

For more information, see [Create a user group](#).

- **Grant the minimum permissions to different RAM user groups.**

You can attach system policies to RAM users or RAM user groups. You can also create custom policies and attach them to RAM users or RAM user groups for fine-grained access control. You can grant the minimum permissions to different RAM users or RAM user groups. This helps you better manage access permissions on resources.

 **Note** In a simple scenario, you can create a few RAM users and grant the required permissions to the RAM users. In a complex scenario, you may have a large number of RAM users. We recommend that you add RAM users with the same responsibilities to the same user group and then grant the required permissions to the user group. This facilitates permission management.

For more information, see [Create a custom policy](#) and [Grant permissions to a RAM user group](#).

- **Configure strong logon password policies.**

You can configure logon password policies that specify the minimum length, mandatory characters, and validity period of passwords for RAM users in the RAM console. If you authorize a RAM user to change the logon password, the RAM user must create a strong logon password and rotate the password or AccessKey pair on a regular basis.

For more information, see [Configure security policies for RAM users](#).

- **Enable an MFA device for your Alibaba Cloud account.**

You can enable a multi-factor authentication (MFA) device for your Alibaba Cloud account to enhance account security. This adds an extra layer of protection in addition to your username and password. After you enable an MFA device, a RAM user must perform the following operations when the RAM user logs on to the Alibaba Cloud Management Console:

- i. Enter a valid username and password.
- ii. Enter the verification code that is generated by the virtual MFA device. Alternatively, pass the U2F authentication.

For more information, see [Enable an MFA device for an Alibaba Cloud account](#).

- **Enable SSO for RAM users.**

After single sign-on (SSO) is enabled, all internal accounts of your enterprise are authenticated. Then, RAM users can log on to Alibaba Cloud and access resources only by using an internal account.

For more information, see [SSO overview](#).

- **Do not create an AccessKey pair for your Alibaba Cloud account.**

The AccessKey pair of your Alibaba Cloud account has the same permissions as the logon password. The AccessKey pair is used for programmatic access whereas the logon password is used for console logon. Your Alibaba Cloud account has full permissions on your resources. To prevent the security risks caused by AccessKey pair leaks, we recommend that you do not create an AccessKey pair for your Alibaba Cloud account or use the AccessKey pair to perform daily operations.

You can create AccessKey pairs for RAM users and use the RAM users to perform daily operations.

For more information, see [Create an AccessKey pair for a RAM user](#).

- **Specify the condition element in policies to enhance security.**

You can specify the condition element in a policy to allow RAM users to use a specified source IP address to access your resources or access your resources within a specified period of time.

For more information, see [Policy elements](#).

- **Manage permissions on your resources.**

By default, your Alibaba Cloud account owns all of your resources and has full control over the resources. The RAM users of your Alibaba Cloud account can use the resources, but do not own the resources. This allows you to manage instances or other resources that are created by the RAM users.

- If you no longer need an existing RAM user, you can delete the RAM user to revoke all permissions that are granted to the RAM user.
- If you require a new RAM user, you can create a RAM user, set a logon password or AccessKey pair for the RAM user, and then grant the RAM user the required permissions.

For more information, see [Grant permissions to a RAM user](#).

- **Use STS to grant temporary permissions to RAM roles.**

A RAM role does not have permanent identity credentials. A RAM role can only be assumed by using an issued Security Token Service (STS) token to access Alibaba Cloud resources.

For more information, see [What is STS?](#).

Result

After you migrate your workloads to Alibaba Cloud, you can use the solution described in this topic based on your business requirements. The solution allows you to manage your resources and protect your Alibaba Cloud account and assets in an effective and efficient manner.

What to do next

You can use RAM to categorize your O&M tasks and assign the tasks to different O&M personnel (RAM users). For more information, see [Use RAM to manage permissions of O&M engineers](#).

2. Use RAM to manage user permissions and resources

This topic describes how an enterprise that has multiple cloud resources can use Resource Access Management (RAM) to manage user permissions to access the cloud resources.

Prerequisites

An Alibaba Cloud account is created. If not, create one before proceeding. To create an Alibaba Cloud account, click [Create an Alibaba Cloud account](#).

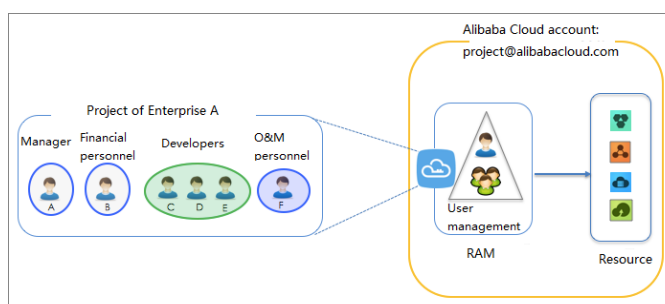
Background information

Enterprise A has purchased various Alibaba Cloud resources, such as Elastic Compute Service (ECS) instances, ApsaraDB for RDS instances, Server Load Balancer (SLB) instances, and Object Storage Service (OSS) buckets, to migrate a project to the cloud. Certain employees need to manage these cloud resources, and different employees require different permissions to fulfill their duties.

Enterprise A has the following requirements:

- To guarantee security, Enterprise A does not want to disclose the AccessKey pair of its Alibaba Cloud account to employees.
- Enterprise A prefers to create different RAM user accounts for the employees and grant different permissions to these user accounts. The employees are granted only the permissions that are required to fulfill their duties.
- The RAM users can only manage resources after they are granted the corresponding permissions. All the operations performed by RAM users can be audited.
- Enterprise A can revoke the permissions granted to RAM users and delete RAM user accounts at any time.
- Fees on resources incurred by RAM users are billed to the parent Alibaba Cloud account.

Solution



- Enable multi-factor authentication (MFA) for an Alibaba Cloud account to avoid the accidental disclosure of the Alibaba Cloud account password. For more information, see [Enable an MFA device for an Alibaba Cloud account](#).
- Create RAM user accounts for different employees or apps, and specify login passwords or create AccessKey pairs based on the business requirements. For more information, see [Create a RAM user](#).
- If multiple employees have the same responsibility, we recommend that you create a RAM user group and add the corresponding users to this group. For more information, see [Create a user group](#).
- Attach one or more system policies to a RAM user or RAM user group. For more information, see [Grant](#)

[permissions to a RAM user](#) and [Grant permissions to a RAM user group](#). For finer-grained permission management, you can create one or more custom policies and attach them to individual RAM users or to a RAM user group. For more information, see [Create a custom policy](#).

- Remove permissions from RAM user groups or RAM users when they no longer need the permissions. For more information, see [Revoke permissions from a RAM user](#) and [Revoke permissions from a RAM user group](#).