Alibaba Cloud
Resource Access Management

Best Practices

Issue: 20200506
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 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 contact Alibaba Cloud directly if you discover any errors in this document.**
# Document conventions

<table>
<thead>
<tr>
<th>Style</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>🚨</td>
<td>A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.</td>
<td>🚨 <strong>Danger:</strong> Resetting will result in the loss of user configuration data.</td>
</tr>
<tr>
<td>🚨危险</td>
<td>A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.</td>
<td>🚨 <strong>Warning:</strong> Restarting will cause business interruption. About 10 minutes are required to restart an instance.</td>
</tr>
<tr>
<td>🚨警告</td>
<td>A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.</td>
<td>🚨 <strong>Notice:</strong> If the weight is set to 0, the server no longer receives new requests.</td>
</tr>
<tr>
<td>📝</td>
<td>A note indicates supplemental instructions, best practices, tips, and other content.</td>
<td>📝 <strong>Note:</strong> 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 <strong>Settings &gt; Network &gt; Set network type</strong>.</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 <strong>OK</strong>.</td>
</tr>
<tr>
<td><strong>Courier font</strong></td>
<td>Courier font is used for commands.</td>
<td>Run the <code>cd /d C:/windows</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>[]</td>
<td>This format is used for an optional value, where only one item can be selected.</td>
<td>`ipconfig [-all</td>
</tr>
<tr>
<td>Style</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------</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>
Contents

Legal disclaimer

Document conventions

1 Use RAM to maintain security of your Alibaba Cloud resources

2 Use RAM to manage user permissions and resources
1 Use RAM to maintain security of your Alibaba Cloud resources

This topic describes how to apply access and security settings to your Alibaba Cloud resources by using RAM. This allows you to better manage resource permissions with fine-grained access control.

Prerequisites

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

Scenario

When you migrate your business resources to the cloud, traditional organizational structures or existing resource management methods may no longer meet your requirements. You may face the following security management issues during the migration of your resources:

- The responsibilities of the RAM users are not clear.
- The Alibaba Cloud account owner does not want to share the access key with RAM users due to security risks.
- RAM users can access resources by using different methods. This is prone to security risks.
- Resource permissions granted to RAM users must be revoked 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 resource permissions to RAM users. You can use RAM to prevent the AccessKey pair of your Alibaba Cloud account from being shared by RAM users. You can also use RAM to grant minimum permissions to RAM users. This simplifies permission management and ensures resource security.
Resource Access Management

Best Practices / 1 Use RAM to maintain security of your Alibaba Cloud resources

Security management solution

- Create separate RAM users.

  You require only one Alibaba Cloud account. You can create separate 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 for daily permission management.

  For more information, see #unique_4.

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

  For more information, see #unique_4.

- 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 #unique_5.

- 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
Use RAM to maintain security of your Alibaba Cloud resources.

For more information, see #unique_6.

• Configure strong logon password policies.

You can configure logon password policies that specify the minimum length, mandatory characters, and validation period 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 #unique_7.

• 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 the account security. After you enable an MFA device, the following two security factors are required when a RAM user logs on to Alibaba Cloud:

1. Username and password
2. Verification code provided by the MFA device

For more information, see #unique_8.

• Enable SSO for RAM users.

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

For more information, see #unique_9.

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

Your Alibaba Cloud account has full permissions on your resources. 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 to log on to the console. To prevent information leaks due to the disclosure of the AccessKey pair, we recommend that you do not create an AccessKey for your Alibaba Cloud account.

You can create an AccessKey pair for your RAM users and grant the RAM user the relevant permissions.

For more information, see #unique_10.
• Specify the condition element in policies to enhance security.

You can specify the condition element in a policy to allow RAM users to use your resources only when the condition is met. For example, you can specify that the RAM user must use a secure channel (for example, SSL), use a specified source IP address, or use your resources within a specified period of time.

For more information, see #unique_11.

• Manage permissions on your cloud resources.

All your resources are in your Alibaba Cloud account. 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 created by the RAM users.

- If you no longer require an existing RAM user, you can delete the RAM user to revoke all permissions 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 relevant permissions.

For more information, see #unique_12.

• Use STS to grant temporary permissions to RAM users.

Security Token Service (STS) is an extended authorization service of RAM. You can use STS tokens to grant temporary permissions to RAM users and specify the permission and automatic expiration time of the tokens.

For more information, see #unique_13.

Result

After you migrate your services to the Alibaba Cloud, you can use the preceding solutions based on your business requirements. These solutions ensure that you manage your cloud resources effectively and protect your Alibaba Cloud account and business assets.

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 #unique_14.
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 #unique_8.

- Create RAM user accounts for different employees or apps, and specify logon passwords or create AccessKey pairs based on the business requirements. For more information, see #unique_4.

- 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 #unique_5.

- Attach one or more system policies to a RAM user or RAM user group. For more information, see #unique_12 and #unique_16. 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 #unique_6.

- Remove permissions from RAM user groups or RAM users when they no longer need the permissions. For more information, see #unique_17 and #unique_18.