Alibaba Cloud
Resource Access Management

Best Practices

Issue: 20181121

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.	 **Note:** 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]`*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *`{stand | slave}`*

Contents

1 RAM best practices

This document introduces some best practices of using RAM from the following aspects: **logon verification**, **account authorization**, and **permission assignment**. These suggestions help you make full use of RAM to deploy a secure and controllable environment.

Logon verification

Enable account protection for the root account and RAM users

- We recommend that you enable multi-factor authentication (MFA) for your root account so that MFA is performed each time the root account is used.
- If you have created a RAM user and granted high-risk permissions to the user (such as stopping instances and deleting buckets), you are advised to enable MFA for the RAM user.

Configure strong password policies for user logon

- If you allow a RAM user to change his or her logon password, you should require the user to create a strong logon password and encourage frequent password rotation.
- You can create password policies, such as the minimum length, whether non-letter characters are required, and the rotation cycle, for RAM users on the RAM console.

Rotate logon passwords and AccessKeys of users

- We recommend that you or the RAM users regularly rotate logon passwords or AccessKeys. If a credential is disclosed without your knowledge, the validity of the credential is restricted.
- You can set a password policy to force the RAM users to rotate their logon passwords or AccessKeys in a regular cycle.

Account authorization

Adhere to the minimum authorization rule

The minimum authorization rule is a primary rule for security design. When you need to *Authorize RAM users*, grant the user only the permissions that are required for his work.

For example, in your organization, if the responsibilities of the developers group (or an applicatio n system) only require reading data stored in the OSS buckets, grant the group (or the applicatio n system) read-only permission. All permissions for OSS resources, or the permission to access resources of all products are not required.

Enhance security with policy conditions

We recommend that you set policy conditions when you grant permissions to a user to enhance the security.

For example, you grant a user the permission to stop ECS instances with the condition that the user enacts the stop at a specified time on the company network.

Revoke permissions that are no longer needed

When a user's role changes and the assigned permission is no longer necessary, you need to revoke the permission. See *Authorize RAM users* for the **subsequent operation**.

This can help minimize any security risk caused by disclosure of the access credential of the user without your knowledge.

Permission assignment

Avoid creating an AccessKey for the root account

We recommend that you do not create an AccessKey for the root account, as the root account has full permissions for all resources under it.

Grant permissions to RAM users through groups

Normally, you do not need to *Authorize RAM users*. It is more convenient to create a group (such as admin, developer, and accounting groups) related to the role and responsibilities of the user. Attach an appropriate authorization policy to the group, and then add users to the group. All users in a group share the same permissions.

Therefore, you can modify the permissions of all users in the group with one operation. When a user is transferred in your organization, you only need to change the group to which the user belongs.

Separate user management, permission management and resource management

When using RAM, create separate RAM users responsible for RAM user management, RAM permission management, and the management of resource operations under various products. A secure authority-based management system supports checks and balances to minimize security risks.

Separate console users from API users

It is not recommended that you create both a logon password for console operations and an AccessKey for API operations for one RAM user. We recommend that you create only logon passwords for employees and create only AccessKeys for systems and applications.

2 Best practice of primary account security

A primary account is equivalent to a root account that controls all of your cloud resources. As such, if the primary account password or API AccessKey is lost or disclosed, this may cause immeasurable loss to your enterprise.

So how to protect the security of your primary account? This document makes a reference for you.

Principle 1: Enable account protection for the root account

- Enable account protection for your root account and do not share the MFA device with others.
- Enable MFA for RAM users with special operation permissions. Special operation permission s include user management, authorization, instance stopping/release, instance configuration modification, and data deletion.

Principle 2: Create different RAM accounts for routine O&M management operations

- Create RAM user accounts for employees and use them to perform routine O&M management operations.
- Create independent RAM user accounts for financial employees.
- Create independent RAM user accounts for RAM administrators.

Principle 3: Prohibit creation of an AccessKey for the root account

AccessKeys have the same permissions as logon passwords. However, AccessKeys are used for program access while logon passwords are used to log on to the console. Because AccessKeys are generally stored in configuration files in cleartext format, there is a high leakage risk.

Configure RAM user identities for all application systems and follow the minimum authorization rule in the case of *Attach policies to a RAM user*.

Principle 4: Use authorization policies with IP restrictions

All users that are granted special operation permissions must be *configured with IP restrictions (acs:SourceIp)*.

Therefore, even if a RAM user's logon password or AccessKey is disclosed, attackers will be unable to obtain account information as long as they have not penetrated your trusted network.

Principle 5: Use authorization policies with MFA restrictions

All users that are granted special operation permissions must be *configured with MFA restrictions (acs:MFAPresent)*.

Therefore, even if a RAM user's logon password or AccessKey is disclosed, attackers will be unable to obtain account information as long as the MFA device is not lost.

For more restrictions, see *Syntax*.

There is no such thing as absolute security, but only best practices. In combination with these protection mechanisms, adherence to the best security practice principles will significantly secure your account assets.

3 Use RAM to migrate businesses to the cloud

In the initial phase, start-ups usually have lower secure management requirements on cloud resources and may proceed with a single AccessKey for operations on all resources. However, as start-ups evolve into larger enterprises, or when large customers need to migrate their businesses to the cloud, their organizational structures become increasingly complex. They require even higher security management of cloud resources.

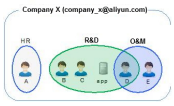
This document examines the demand for resource access management (RAM) after enterprise s migrate businesses to the cloud. We examine the needs from the perspective of an enterprise owner. Using a simple case study, we illustrate, step by step, how to leverage RAM to establish a safe and secure resource management system.

Case Study

For example, suppose you are the owner of Company X. You have registered a cloud account (company-x@aliyun.com) for your Company X, and have purchased basic infrastructure services of ECS, RDS, and OSS. Since your company migrated its services to the cloud, business has been rapidly developing, your team expanding, and cloud resource requirements growing. All operation and management actions on resources use one shared account, which highlights the issue of system vulnerability and the importance of security.

Suppose Company X's organization structure is as shown in the following chart. There are three departments in total: Human Resources (HR), Research & Development (R&D), and Operation & Maintenance (O&M) Departments. The HR Department is in charge of only human resources, the R&D Department is solely responsible for resource usage, and the O&M Department is authorized to manage resources (such as starting or stopping virtual machines).

Figure 3-1: Organization structure of company X



Implementation procedure

Let's take a look at how we use RAM to achieve security management of resource access step by step.

Step 1: Enable Multi-Factor Authentication (MFA) for your primary account

Given the fact that you may have shared your primary account with others, the primary account is highly vulnerable to password leaks. We strongly recommend you enable MFA (Multi-Factor Authentication) for your primary account.

Alibaba Cloud accounts support standard virtual MFA. It is an easy-to-use application that can be installed on mobile devices (for example, smart phones and smart watches). After virtual MFA is enabled in the Account Center, when you log on to Alibaba Cloud platforms, the system not only verifies your user name and password (the first security factor), but also requires you to provide the dynamic security code (the second security factor) generated by the virtual MFA application. These factors work together to enhance security protection for your account.

Step 2: Create user accounts and group them

Based on the preceding organization chart, you can create different user accounts for employees A, B, C, D, and E, and then create a user account for the application “app”. Then, you can create three user groups to match the HR, R&D, and O&M Departments, respectively, and add these users to appropriate groups (note that User D belongs to both the R&D and O&M Departments).

Furthermore, you must *Create a RAM user* based on different user needs.

- The application “app” is only allowed to visit cloud resources through the OpenAPI, so you only need to create an AccessKey for it.
- If an employee only requires operating on cloud resources through the console, you only need to set a logon password for the employee.

Another consideration is that maintenance operations are typically quite sensitive. You may be concerned about the significant risks of maintenance personnel account passwords being leaked. To address this issue, you can set *enforced MFA at logon of these accounts* and have two different persons assigned to maintain the account passwords and MFA devices. In this way, some operations can only be fulfilled in the presence of both persons.

Step 3: Assign minimum permissions for various user groups

RAM provides multiple system authorization policy templates for you to choose from. For example, you can authorize the O&M group the full permission for ECS and RDS, authorize the R&D group the read-only permission for ECS and RDS and the full permission for OSS, and authorize the HR group the administration permission for RAM users.

If you feel that the granularity of the default RAM system authorization policy templates for resource management is not specific enough, you can customize authorization policy templates in the RAM. Custom authorization policies support fine-tuned access management, such as using a specific API operation name and resource instance name. They also support expressions with multiple constraints for flexible management of resource operation approaches, such as limiting the source IP addresses of operation initiators. Custom authorization policies can meet your diversified and rigorous requirements on resource management to achieve minimum authorization . This will only authorize the minimal permission required.

Take conditional authorization, for example. If you are concerned that the leak of a R&D personnel AccessKey may compromise the company's OSS data, you can impose constraints on data access in the OSS. This can be accomplished using the authorization policies for the R&D group, such as requiring OSS operations to be conducted only at company site (using the `acs:SourceIP` conditional expression) during working hours (using the`acs:CurrentTime` conditional expression).

Step 4: Employee job transfer, onboarding, and resignation

When an employee transfers to another post, you can transfer the account of the employee to the destination group. For a new employee, you can create a new user account for the new employee, set the logon password or AccessKey, and then add the account to the appropriate user group *Authorize RAM users*. If an employee quits, you can delete the user account in the RAM console, and the RAM automatically removes all access permissions for the user account.

Step 5: Use STS to authorize a temporary user

Sometimes you may also have users (people or applications) who require ad-hoc access to your cloud resources. We term them as "temporary users". In this scenario, you can use the Security Token Service (STS), an extended authorization service of RAM, to issue access tokens to these users. The permission and automatic expiration time of the tokens can be defined as required when you issue these tokens.

A benefit of using STS access tokens for temporary user authorization is for better management of user authorization. You do not need to create an RAM user account and password for the temporary user. The RAM user password always remains valid, but temporary users do not need to access resources for the long term.

In addition, you can also authorize an RAM user to issue access tokens, using STS to further delegate authority to RAM users.

Step 6: Let the primary account “take a good rest”

Once your employees and application systems start to use RAM user accounts, you do not need to use the primary account for routine work anymore. We suggest that you do not create an AccessKey for your primary account to reduce the risk of leakage.

We also recommend you store your primary account password and MFA devices in the company’s safe to let them “take a good rest”.