Resource Access Management

Best Practices

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

You do the following mainly in the Alibaba Cloud account security settings and RAM settings.

Enable account protection for the root account and RAM users

We recommend that you enable account protection for your root account (for example Time-based One-time Password, that is, TOTP verification) so that TOTP 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 multi-factor authentication (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

You do the following mainly in the RAM console Users and Policies pages.

Adhere to the minimum authorization rule

The minimum authorization rule is a primary rule for security design. When you need to grant permissions to a user, 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 application system) only require reading data stored in the OSS buckets, grant the group (or the application 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 Attach policies to a RAM user for detailed procedure.

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

Permission assignment

You do the following mainly in the RAM console Users and Groups pages.

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 attach an authorization policy to a RAM user. 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

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

Separate console users from API users

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

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.

Security best practices

Follow the listed best practices to secure your primary account.

Enable account protection for the root account

Enable account protection for your root account (for example, Time-based One-time Password, that is, TOTP verification) and do not share the MFA device with others.

Enable MFA for RAM users with special operation permissions. Special operation permissions include user management, authorization, instance stopping/release, instance configuration modification, and data deletion.

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.

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.

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.

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.

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.

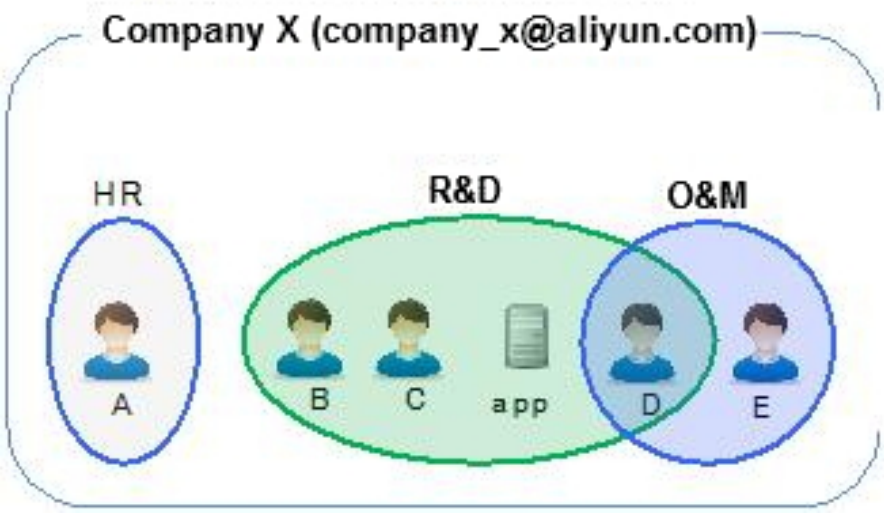
In the initial phase, start-ups usually have lower secure management requirements on cloud resources and may proceed with a single AccessKey for operations on all resources. However, as start-ups evolve into large companies, or when large customers need to migrate their businesses to the cloud, their organization structures get increasingly complicated, with an even stronger demand for secure management of cloud resources.

This article examines the demand for resource access management after enterprises migrate businesses to the cloud, from the perspective of an enterprise owner. Using a case study, it illustrates how to leverage the RAM to establish a safe and secure resource management system step-by-step.

Case Study

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

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



Implementation procedures

Let’ s take a look at how we can use RAM to achieve secure management of access requests to your

resources.

Step 1: Enable MFA for your primary account

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

Alibaba Cloud accounts support standard virtual MFA mechanisms. It is a easy-to-use application that can be installed on mobile devices (such as smart phones and smart watches). After enabling the virtual MFA feature in the Account Center, apart from verifying the user name and password (the first security factor) upon your initial log on to Alibaba Cloud platforms, the system also requires you to provide the dynamic security code (the second security factor) generated by the virtual MFA application. These factors work together to ensure enhanced security protection for your account.

Step 2: Create user accounts and group them

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

Next, you must set the logon password or AccessKey in the user attribute based on different user needs.

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

Another consideration is that maintenance operations are usually 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 different personnel assigned to maintain the account passwords and multi-factor authentication devices, so that some operations can only be fulfilled in the presence of both personnel.

Step 3: Assign minimum permissions for various user groups

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

If you feel that the granularity that 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" (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 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 are to transfer the employee's user account to the destination group. If a new employee is on board, you are to 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. If an employee leaves, you are to 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 case, you can use the STS (Security Token Service, 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 shall always remain 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 do not suggest you create an AccessKey for your primary account, so as to reduce the risk of leakage. We also recommend you store your primary account password and multi-factor authentication devices in the company's safe to let them "take a good rest".

With the versatile resource management capabilities of RAM, as demonstrated in the preceding steps, you can formulate appropriate resource management policies based on your company's actual needs to coordinate the diversified demands of your users for cloud resource access.