Resource Access Management

Best Practices

MORE THAN JUST CLOUD | Alibaba Cloud

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.