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 three 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 MFA for the root account and RAM users.

We recommend that you bind multi-factor authentication (MFA) to 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 (such as stopping instances and deleting buckets) to the user, you are advised to bind MFA to 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 access keys of users.

We recommend that you or the RAM users rotate logon passwords or access keys regularly. 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 access keys 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 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.

Cancel permissions that are no longer needed.

When a user’ s role changes and the associated permission is no longer necessary, the permission can be canceled. 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 access key for the root account.

We recommend that you do not create an access key for the root account, as the root account has full permissions for all resources under it. Performing the creating operation requires multi-factor authentication and supports strict risk control check. As long as no access key is created for the root account, the security risks for assets under the account are controllable.

Grant permissions to RAM users through groups.

Normally, you do not need to bind 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. Bind 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 access keys for systems and applications. It is not recommended that you create both a logon password for console operations and an access key for API operations for one RAM user.

Primary account security protection

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 access key is lost or disclosed, this may cause immeasurable loss to your enterprise and even lead to bankruptcy.

So how to protect the security of your root account?

Principle 1: Enable multi-factor authentication for the root account (two-step authentication)

- Enable multi-factor authentication (MFA) for the root account 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.

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 access key for the root account

- Access keys have the same permissions as logon passwords. However, access keys are used for program access while logon passwords are used to log on to the console. Because access keys 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.

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 access key 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 access key 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.