Resource Access Management

Introduction

Introduction

Resource Access Management (RAM) Overview

What is RAM?

Resource Access Management (RAM) is an Alibaba Cloud service designed for user identity management and access control. Using RAM, you can create and manage user accounts, and control the operation permissions that these user accounts possess for resources under your account, for example, employees, systems and applications. If multiple users in your enterprise need to collaborate with each other to perform operations on resources, using RAM allows you to avoid sharing your Alibaba Cloud account access key with other users. Instead, you can grant users the minimum permissions needed to complete their work, reducing your enterprise's security risks.

RAM scenarios

Account management and authorization in an enterprise

Assume an enterprise A buys several types of cloud resources such as ECS instances, RDS instances, Server Load Balancer instances and OSS buckets, and that employees at the enterprise A need to perform operations on these resources such as buying, O&M, or online application. Because different employees have different responsibilities, they require different permissions. For security reasons, the Alibaba Cloud account owner of the enterprise A does not want to disclose its account access key to its employees. Rather, the account owner prefers to create different RAM user accounts for their employees and associate each RAM user account with different permissions. The employees then can perform resource operations only under their permissions with their RAM user accounts and charges are not billed to these accounts. All expenses are charged to the account owner. The account owner can also revoke the permissions of a RAM user account at any time, as well as delete it.

Resource management and authorization between enterprises

Assume that an enterprise A has bought a lot of cloud resources, such as ECS instances, RDS instances, Server Load Balancer instances and OSS buckets for its business requirements. Enterprise A

wants to focus on its business systems, so it grants cloud resource O&M, monitoring management, and other tasks to the enterprise B. Enterprise B will then further delegate O&M tasks to its employees. Enterprise B needs to precisely control the delegated operations that its employees can perform on the cloud resources of the enterprise A. If A and B terminate this O&M entrustment contract, enterprise A is able to revoke the permissions of the enterprise B as needed.

Temporary authorization management for the apps running on the untrusted client

Assume an enterprise A has developed a mobile app and has bought OSS for it. The mobile app must upload and download data to and from OSS. However, enterprise A does not want to allow all apps to use the AppServer to transmit data. Instead, enterprise A wants the apps to directly upload and download data to and from OSS. Because the mobile app runs on user devices, these devices are out of control of enterprise A. For security reasons, enterprise A cannot save the access key in the app. Enterprise A also wants to minimize its security risks by, for example, giving each app an access token with the minimum permissions that the app needs to connect to OSS and restricting the access duration to a specified period of time (such as 30 minutes).

Concepts

RAM allows you to create and manage multiple user identities under an account, as well as allocate different authorization policies to different identities or identity groups. This grants different resource access permissions to different users.

Identity refers to any person, system or application that uses resources from the console or by using Open APIs. To enable identity management in different application scenarios, RAM supports two types of identities, which is RAM-User and RAM-Role.

- A RAM-User is a real identity of a fixed ID and an identity authentication access key. Generally, a RAM-User refers to a person or an application.
- A RAM-Role is a virtual identity of a fixed ID, but no identity authentication access key. A RAM-Role must be associated with a real identity before it becomes available.

A RAM-Role can be associated with multiple real identities, such as:

- RAM-Users under the current Alibaba Cloud account
- RAM-Users under another Alibaba Cloud account
- Alibaba Cloud services (such as EMR or MTS)
- External real identities (such as a local enterprise account)

RAM allows you to create and manage multiple authorization policies under your Alibaba Cloud account. In essence, each authorization policy is a collection of permissions. Administrators can allocate one or more authorization policies to a RAM identity (including RAM-Users and RAM-Roles). The RAM authorization policy language expresses the meaning of the authorization policy in detail. A

policy can grant permissions to an API-Action and Resource-ID, and specify multiple restrictions (such as source IP address, access time, and MFA).

Alibaba Cloud account vs. RAM user

There is a parent-child type relationship between your Alibaba Cloud account and its RAM users. An Alibaba Cloud account is the basic entity for judging the ownership of Alibaba Cloud resources and billing for resource consumption. RAM users exist only in the RAM instances of a certain Alibaba Cloud account. RAM users do not possess resources, and the resources they create under authorization belong to the parent account. RAM users do not possess bills, and all expenses incurred by their authorized operations are debited to the parent account.

In terms of permissions, there is a root–user relationship between your Alibaba Cloud account and its RAM users (such as the relationship in Linux). The root user has all operation and control permissions for resources, while a RAM user has only some permissions that are granted by the root user. In addition, the root user can revoke the permissions granted to a RAM user at any time.

Functions

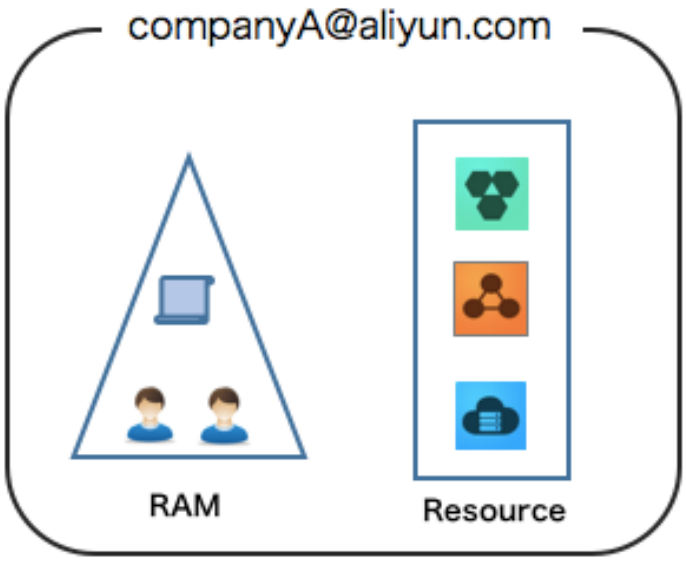
RAM provides the following functions:

- Centralized control of RAM users and their access keys — Under your Alibaba Cloud account, you can create and manage RAM users and their access keys, bind MFA devices to RAM users and unbind MFA devices from RAM users.
- Centralized control of access permissions of RAM users — You can bind one or more authorization policies to each user or user group, to restrict operation permissions of users for specified resources.
- Centralized control of RAM user resource access methods — You can specify that users use security channels (such as SSL) to request access to specific cloud resources at a designated time and from a specified source IP address.
- Centralized control of RAM role and external account identity federation management — You can associate RAM roles with external identity systems (such as your local enterprise domain accounts, or your app accounts). In this way, you can directly use an external identity to log in to a RAM role in order to access the Alibaba Cloud console or an API.
- Centralized control of cloud resources — You can control the instances and data created by RAM users in a centralized manner. Therefore, when a user leaves your organization, these instances and data will still be under your full control.
- Consolidated bill — Your account will receive one bill for all expenses incurred from resource operations performed by all RAM users.

RAM and enterprise-level cloud resource management

RAM can meet the following requirements (as shown in the following figure):

- Your enterprise only needs one Alibaba Cloud account (in the figure, this is companyA@aliyun.com).
- All resources belong to this Alibaba Cloud account. As the resource owner, this account has full control of all resources). This account is also responsible for paying all bills.
- You can use RAM to create independent user accounts for operators under your account (the employees that perform resource O&M control operations) and perform authorization management.
- User accounts do not possess resources. By default they do not have access permissions for the resources they create and can only perform operations on resources after their permissions are authorized.
- The charges incurred due to operations of user accounts are billed to the primary account. Separate billing for user accounts is not supported.



These requirements are applicable to the following enterprise scenarios:

- An enterprise wants to easily manage the account and permissions of each operator (or application).
- An enterprise does not want to calculate the costs and fees for each operator (or application) separately.

Basic concepts

Alibaba Cloud account (primary account)

An Alibaba Cloud account is the basic entity for judging the ownership of Alibaba Cloud resources and billing for resource consumption. Before you start using Alibaba Cloud services, you need to register an Alibaba Cloud account. An Alibaba Cloud account is billed for all the resources under the account and has full permissions for these resources. By default, a resource can be accessed only by the resource owner. Other users must have explicit authorization from the owner to access the resource. Therefore, from the perspective of permissions management, the Alibaba Cloud account is similar to the root or admin account of an operating system, it is often called “root account” or “primary account”.

Alibaba Cloud account alias

In RAM, a globally unique alias can be set for each Alibaba Cloud account. Aliases are mainly used for RAM user login and are displayed after a successful login. For example, if the alias abc.com is set for the Alibaba Cloud account admin@abc.com, after a RAM user Alice successfully logs in to the Alibaba Cloud console, the displayed name is alice@abc.com.

RAM users

The account owner can create multiple RAM users (corresponding to employees, systems, or applications of an enterprise) under an Alibaba Cloud account. RAM users have no resources and are not billed independently. They are controlled and paid by the Alibaba Cloud account in a unified manner. RAM users belong to an Alibaba Cloud account and are visible only under this account. They are not independent Alibaba Cloud accounts. RAM users can log on to the console or use APIs to perform operations on resources under an Alibaba Cloud account only after being authorized by the Alibaba Cloud account.

There are two types of RAM user identities: RAM-User and RAM-Role. A RAM-User is a real identity, with a fixed ID and identity credentials. Generally they correspond to specific persons or applications. A RAM-Role is a virtual identity, with no fixed identity credentials. A RAM-Role must be associated with a real identity so that it becomes available.

Comparison between a RAM-Role and Textbook-Role:

i. (Similarity) RAM-Roles and Textbook-Roles can both be bound to a permissions set.
ii. (Difference) A RAM-Role is a virtual identity or shadow account. It has an independent ID. Permissions need to be bound to a RAM-Role and a list of users with this role (Roleplayers) must be specified for the RAM-Role. A RAM-Role is primarily used to resolve Identity Federation problems. A Textbook-Role generally just indicates a permissions set. It is not an identity and is mainly used to simplify authorization management.

RAM-Role role assumption and switching

i. Switching from a login identity to a role identity (SwitchRole): After an actual user (such as a RAM-User) logs on to the console, the user can choose to "Switch to a role", as long as this user has already been associated with this role. A user can only switch to one role at a time. When the user switches from a "login identity" to a "role identity", the user can only use the permissions bound to this role identity. He can no longer use the permissions bound to the login identity. If the user needs to use login identity permissions, he must switch from the role identity back to the login identity.
ii. Calling a program to assume a role (AssumeRole): If an actual user (such as a RAM-User) is associated with a RAM-Role, this user can use an access key to call the AssumeRole interface of the STS service to obtain a temporary access key for this RAM-Role. The temporary access key has a validity period and restricted access permissions (not beyond the permission set bound to the role). Generally temporary access keys are used to resolve temporary authorization problems.

Identity credentials

An identity credential is used to verify the real identity of a user. It usually refers to a user's login password or access key. Identity credentials are confidential, so users must keep their credentials secure and private.

login name/password. You can use the login name and password to access the Alibaba Cloud console to view orders or bills, buy resources, or perform resource operations.

Access key. You can use the access key to construct an API request (or use cloud service SDKs) to perform resource operations.

Multi-factor authentication. Multi-Factor Authentication (MFA) is a simple but effective best practice that can provide additional security protection apart from usernames and passwords. After MFA is enabled, when a user logs on to Alibaba Cloud website, the system requires the user to enter the username and password (first security factor), and then requires the user to enter a variable verification code (second security factor) provided by the MFA device. All these factors work together to offer higher security protection for your account.

Resources

Resources are abstractions of the objects that are presented by a cloud service to users and used for

interaction with users, such as OSS buckets, OSS objects and ECS instances.

We have defined a global Alibaba Cloud Resource Name (ARN) for each resource. The format is as follows:

```
acs:<service-name>:<region>:<account-id>:<resource-relative-id>
```

Format description:

- acs: This is the abbreviation of Alibaba Cloud Service, indicating an Alibaba Cloud public cloud platform.
- service-name: This indicates the name of an open service provided by Alibaba Cloud, such as ecs, oss, or odps.
- region: This indicates region information. If this option is not supported, use the wildcard "*" instead.
- account-id: This is an account ID, such as 1234567890123456.
- resource-relative-id: This indicates the service-related resource. Its meaning varies with specific services of types. Using OSS as an example, "acs:oss::1234567890123456:sample_bucket/file1.txt" indicates an OSS resource of the public cloud platform, where sample_bucket/file1.txt indicates the OSS object name, and 1234567890123456 indicates the object owner.

Permissions

A permission is used to allow or deny a user to perform a certain operation on a particular cloud resource.

Operations can be divided into two main categories: resource control operations and resource use operations. Resource control operations refer to cloud resource lifecycle management and O&M management operations, such as ECS instance creation, stopping, and restart and OSS bucket creation, modification, and deletion. Resource use operations refer to the use of resources' core functions, such as user operations in an ECS instance operating system and OSS bucket data upload/download. Resource control operations are generally oriented to resource buyers or O&M employees in your organization, while resource use operations are oriented to R&D employees or application systems in your organization.

For elastic computing and database products, resource control operations can be managed using RAM, while resource use operations can be managed in each product instance. For example, ECS instance OS permission control or MySQL database permission control. For storage-type products, such as OSS and Table Store, resource control operations and resource use operations can both be managed through RAM.

Policies

A policy is a type of simple language specification that describes a permission set. For the language

specifications supported by RAM, refer to Policy languages.

RAM supports two types of authorization policies: system access policies and custom access policies. You can use but cannot modify the system access policies managed by Alibaba Cloud. Alibaba Cloud will automatically update the system access policy version. You can create or delete the custom access policies. In addition, you need to maintain the policy version by yourself.

Application scenarios

Enterprise subaccount management and permission allocation

Assume an enterprise A buys several types of cloud resources such as ECS instances, RDS instances, Server Load Balancer instances and OSS buckets, and that employees at the enterprise A need to perform operations on these resources such as buying, O&M, or online application. Because different employees have different responsibilities, they require different permissions. For security reasons, the Alibaba Cloud account owner of the enterprise A does not want to disclose its account access key to its employees. Rather, the account owner prefers to create different RAM user accounts for their employees and associate each RAM user account with different permissions. The employees then can perform resource operations only under their permissions with their RAM user accounts and charges are not billed to these accounts. All expenses are charged to the account owner. The account owner can also revoke the permissions of a RAM user account at any time, as well as delete it.

Resource operations and authorization management between enterprises

Assume that an enterprise A has bought a lot of cloud resources, such as ECS instances, RDS instances, Server Load Balancer instances and OSS buckets for its business requirements. Enterprise A wants to focus on its business systems, so it grants cloud resource O&M, monitoring management, and other tasks to the enterprise B. Enterprise B will then further delegate O&M tasks to its employees. Enterprise B needs to precisely control the delegated operations that its employees can perform on the cloud resources of the enterprise A. If A and B terminate this O&M entrustment contract, enterprise A is able to revoke the permissions of the enterprise B as needed.

Temporary authorization management for untrusted client apps

Assume an enterprise A has developed a mobile app and has bought OSS for it. The mobile app must upload and download data to and from OSS. However, enterprise A does not want to allow all apps

to use the AppServer to transmit data. Instead, enterprise A wants the apps to directly upload and download data to and from OSS. Because the mobile app runs on user devices, these devices are out of control of enterprise A. For security reasons, enterprise A cannot save the access key in the app. Enterprise A also wants to minimize its security risks by, for example, giving each app an access token with the minimum permissions that the app needs to connect to OSS and restricting the access duration to a specified period of time (such as 30 minutes).

List of cloud services supporting RAM

All Alibaba Cloud services will be integrated with RAM. For details about services that are currently integrated with RAM, as well as announcements of upcoming services that will support RAM refer to Cloud services that support RAM.