Resource Access Management

Product Introduction

Product Introduction

What is RAM

Resource Access Management (RAM) is a cloud service that helps you manage user identities and control resources access. 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 AccessKey with other users. Instead, you can grant users the minimum permissions needed to complete their work, reducing security risks of your enterprise.

Identity management and access control

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

Identity

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 are RAM-User and RAM-Role.

> A **RAM-User** is a real identity of a fixed ID and an identity authentication AccessKey. Generally, a RAM-User refers to a person or an application.

RAM user vs. Alibaba Cloud account

> From an **ownership** point of view, the relationship between your Alibaba Cloud account and its RAM users is like parent-child.

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**, the relationship between your Alibaba Cloud account and its RAM users is like root–user (such as the relationship in Linux).

The root user has all operation and control permissions for resources.

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.

A **RAM-Role** is a virtual identity of a fixed ID, but no identity authentication AccessKey. 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)

Authorization

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 attach 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).

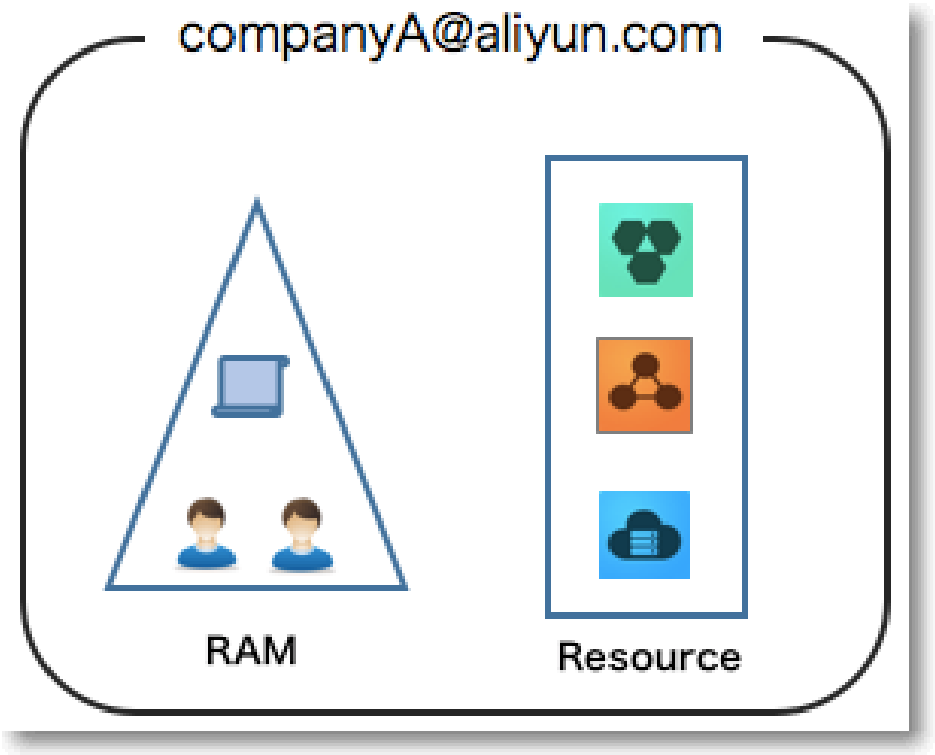
Perform enterprise-level cloud resource management using RAM

RAM is applicable to the following enterprise scenarios:

An enterprise needs 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.

The specific requirements are shown as follows:



Company A 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.

A can use RAM to create independent user accounts for operators under the 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.

Features

RAM helps you deal with the following tasks:

Manage RAM users and their access keys

Under your Alibaba Cloud account, you can create and manage RAM users and their access keys, and enable or disable MFA devices for RAM users.

Grant access permissions to RAM users

You can attach one or more authorization policies to a user, a user group or a role, to grant necessary operation permissions on specified resources.

Restrict user access to cloud resources

You can specify that users use security channels (such as SSL) to request access to specific cloud resources at a designated time or from a specified source IP address.

Authorize roles for external account identities

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 on to a RAM role to access the Alibaba Cloud console or an API.

Centrally control 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 are still under your full control.

Consolidate bills

Your account receives a single bill for all expenses incurred from resource operations performed by all RAM users.

Scenarios

RAM is applicable to the following scenarios.

Account management and authorization in an enterprise

Assume that an enterprise A buys several types of cloud resources such as ECS instances, RDS instances, Server Load Balancer instances and OSS buckets, and the employees at the enterprise A need to perform operations on these resources such as buying, O&M, or online application. Different employees require different permissions, because they have different responsibilities.

Requirements

For security, the Alibaba Cloud account owner of the enterprise A does not want to disclose its account AccessKey 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 but to the account owner.

The account owner can also revoke the permissions of a RAM user account at any time, and delete an account.

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.

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 then further delegates 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 can revoke the permissions of the enterprise B as needed.

Temporary authorization for apps running on untrusted client endpoint

Assume that 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.

Requirements

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 AccessKey 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

This document explains the relevant concepts of RAM for your better understanding of the service.

- Identity management related concepts include Alibaba Cloud account, Account alias, Identity credentials, RAM-User, and RAM-Role.
- Access control related concepts include Resources, Permissions, and Policies.

Alibaba Cloud account

An Alibaba Cloud account (primary 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 must 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, which 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 logon and are displayed after a successful logon.

For example, if the alias abc.com is set for the Alibaba Cloud account admin@abc.com, after a RAM user Alice successfully logs on to the Alibaba Cloud console, the displayed name is alice@abc.com.

Identity credentials

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

Logon name/password

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

AccessKey

You can use the AccessKey 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.

RAM-User

A RAM-User is a real identity, with a fixed ID and identity credentials. Generally they correspond to specific persons or applications.

- 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. The Alibaba Cloud account has all the resources and unified payments of all bills.
- 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.

RAM-Role

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.

RAM-Role vs. Textbook-Role (traditionally defined roles)

Similarities

RAM-Roles and Textbook-Roles can both be bound to a permissions set.

Differences

- 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 Textbook-Role generally only indicates a permissions set. It is not an identity and is mainly used to simplify authorization management.

RAM-Role role assumption and switching

Switch from a logon 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**, if 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 logon identity to a role identity, the user can only use the permissions granted to this role identity. He can no longer use the permissions granted to the logon identity.

- If the user needs to use logon identity permissions, he must switch from the role identity back to the logon identity.

Call 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 AccessKey to call the AssumeRole interface of the STS service to obtain a temporary AccessKey for this RAM-Role.

The temporary AccessKey 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.

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 (ecs), OSS (oss), or ODPS (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 indicate 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 control operations are generally oriented to resource buyers or O&M employees in your organization.

Resource use operations indicate the use of resources' core functions, such as user operations in an ECS instance operating system and OSS bucket data upload/download. Resource use operations are oriented to R&D employees or application systems in your organization.

Note:

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, see 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 automatically updates the system access policy version.

You can create or delete the custom access policies. In addition, you must maintain the policy version by yourself.

Cloud services supporting RAM

A large number of Alibaba Cloud services have been integrated with RAM. This document lists these services and provides relevant links for your quick reference.

When each product is being integrated with RAM functions, different levels of authorization granularity have been defined for RAM users:

- Service level: Authorization is performed at the cloud product level. A RAM user either has all permissions or has no permission for the product.
- Operation level: Authorization is performed at the API level. A RAM user can perform specified operations on a certain type of resource for a specified product.
- Resource level: Authorization is performed at the operation level, which is the finest authorization granularity level. For example, authorizing a RAM user to restart only a specified cloud server.

Cloud services that work with RAM

The following tables list the cloud services that can access RAM either on the management console or from calling an API. In this table,

- The right mark (√) indicates available.
- The circular mark (○) indicates unavailable.
- The hyphen (-) indicates none.

Elastic Computing

Service	Console	API	Authorization granularity	System policy	Reference
Elastic Compute Service	√	√	Resource level	AliyunECSFullAccess AliyunECSReadOnlyAccess	Authentication rules
Auto Scaling	√	√	Service level	AliyunESSFullAccess AliyunESSReadOnlyAccess	API usage instructions
Container Service	√	√	Service level	-	-
Resource Orchestration	√	√	Service level	-	Use RAM to control resource access

Database Services

Service	Console	API	Authorization granularity	System policy	Reference
ApsaraDB for RDS	√	√	Resource level	AliyunRDSFullAccess AliyunRDSReadOnlyAccess	RDS API authentication rules
ApsaraDB for MongoDB	√	√	Resource level	AliyunMongoDBFullAccess AliyunMongoDBReadOnlyAccess	MongoDB API authentication rules
ApsaraDB for Redis	√	√	Resource level	AliyunKvstoreFullAccess AliyunKvstoreReadOnlyAccess	Redis API authentication rules
ApsaraDB for Memcache	√	√	Service level	AliyunOCSFullAccess AliyunOCSReadOnlyAccess	-

Storage & CDN

Service	Console	API	Authorization granularity	System policy	Reference
Object Storage Service	√	√	Resource level	AliyunOSSFullAccess AliyunOSSReadOnlyAccess	-
Network Attached Storage	√	○	Service level	AliyunNASFullAccess AliyunNASReadOnlyAccess	Use permission groups
Table Store	√	√	Resource level	AliyunOTSFullAccess AliyunOTSReadOnlyAccess AliyunOTSWriteOnlyAccess	Customize permissions

CDN	√	√	Resource level	AliyunCDNFullAccess AliyunCDNReadOnlyAccess	CDN API authentication rules

Networking

Service	Console	API	Authorization granularity	System policy	Reference
Server Load Balancer	√	√	Resource level	AliyunSLBFullAccess AliyunSLBReadOnlyAccess	SLB authentication rules
Virtual Private Cloud	√	√	Resource level	AliyunVPCFullAccess AliyunVPCReadOnlyAccess	-
EIP	√	√	Resource level	AliyunEIPFullAccess AliyunEIPReadOnlyAccess	-
Express Connect	√	√	Resource level	AliyunExpressConnectFullAccess AliyunExpressConnectReadOnlyAccess	Authentication rules for Express Connect APIs

Analytics

Service	Console	API	Authorization granularity	System policy	Reference
E-MapReduce	√	√	Service level	AliyunEMRFullAccess	E-MapReduce role authorization

Cloud Communication

Service	Console	API	Authorization	System policy	Reference

			granularity		
Message Service	√	√	Resource level	AliyunMNSFullAccess AliyunMNSReadOnlyAccess	-
Direct Mail	√	√	Service level	AliyunDirectMailFullAccess AliyunDirectMailReadOnlyAccess	-

Monitoring & Management

Service	Console	API	Authorization granularity	System policy	Reference
CloudMonitor	√	√	Service level	AliyunCloudMonitorFullAccess AliyunCloudMonitorReadOnlyAccess	RAM for CloudMonitor
Resource Access Management	√	√	Resource level	AliyunRAMFullAccess AliyunRAMReadOnlyAccess AliyunSTSAssumeRoleAccess	RAM introduction
Key Management Service	√	√	Resource level	-	KMS authentication rules

Application Service

Service	Console	API	Authorization granularity	System policy	Reference
Log Service	√	√	Resource level	AliyunLogFullAccess AliyunLogReadOnlyAccess	Use Log Service as a RAM sub-user Authentication rules
API	√	√	Service level	AliyunApiGa	-

Gateway				tewayFullAccess AliyunApiGatewayReadOnlyAccess	

Middleware

Service	Console	API	Authorization granularity	System policy	Reference
Enterprise Distributed Application Service	√	×	Service level	AliyunEDASFullAccess	EDAS sub-accounts

Media Services

Service	Console	API	Authorization granularity	System policy	Reference
ApsaraVideo for Media Processing	√	√	Service level	AliyunMTSFullAccess AliyunMTSPlayerAuth	Sub-account console operating instructions
ApsaraVideo for Live	√	√	Service level	AliyunMTSFullAccess	-

Security

Service	Console	API	Authorization granularity	System policy	Reference
Server Guard	√	○	Service level	AliyunYundunAegisFullAccess AliyunYundunAegisReadOnlyAccess	-
Anti-DDoS Pro	√	○	Service level	AliyunYundunHighFullAccess AliyunYundunHighReadOnlyAccess	-
Web	√	○	Service level	AliyunYund	-

Application Firewall				unWAFFullAccess AliyunYundunWAFReadOnlyAccess	
Mobile Security	√	○	Service level	AliyunYundunJaqFullAccess	-
Certificates Service	√	○	Service level	AliyunYundunCertFullAccess AliyunYundunCertReadOnlyAccess	-

Alibaba Cloud Marketplace

Service	Console	API	Authorization granularity	System policy	Reference
Alibaba Cloud Marketplace	√	○	Service level	AliyunMarketplaceFullAccess	-

Domains & Websites

Service	Console	API	Authorization granularity	System policy	Reference
Alibaba Cloud DNS	√	○	Service level	AliyunDNSFullAccess AliyunDNSReadOnlyAccess	-
HTTPDNS	√	○	Service level	AliyunHTTPDNSFullAccess AliyunHTTPDNSReadOnlyAccess	-

Cloud services that work with STS

The following table lists the cloud services that work with STS.

Service	Console	API
Elastic Compute Service	√	√

ApsaraDB for RDS	√	√
Server Load Balancer	√	√
Object Storage Service	√	√
Virtual Private Cloud	√	√