Alibaba Cloud
Resource Access Management

Product Introduction

Issue: 20180930

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.
5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade

secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion , or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos , marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).

6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
⛔	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⛔ **Danger:** Resetting will result in the loss of user configuration data.
⚠	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	⚠ **Warning:** Restarting will cause business interruption. About 10 minutes are required to restore business.
📋	This indicates warning information, supplementary instructions, and other content that the user must understand.	📋 **Note:** Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	📋 **Note:** You can use **Ctrl** + **A** to select all files.
>	Multi-level menu cascade.	**Settings** > **Network** > **Set network type**
Bold	It is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
`Italics`	It is used for parameters and variables.	`bae log list --instanceid` *`Instance_ID`*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *`[-all|-t]`*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *`{stand | slave}`*

Contents

1 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 collaboratively work with 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.
- 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), and 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).

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.

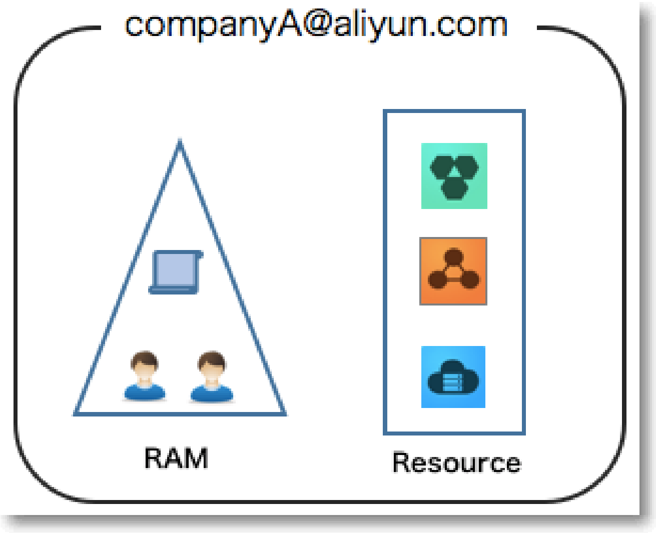
Perform enterprise-level cloud resource management using RAM

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:

Figure 1-1: Enterprise scenario



- 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 who perform operation and maintenance on resources) 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.

2 Feature

RAM helps you with **user identity management** and **resource access management**. Features are shown as follows:

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.

3 Scenarios

RAM is applicable to the following scenarios: account management and authorization in an enterprise, resource management and authorization between enterprises, and temporary authorization for apps running on untrusted client endpoint.

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).

4 Concepts

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

Identity management related concepts

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

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 supports two types of identities, which are 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.

RAM-Role

RAM role The traditional role (textbook-style role) is a set of permissions, which are similar to policies in RAM. If a user is assigned a role, it means that the user is given a set of permissions, and the user can access authorized resources.

The RAM role is different from the textbook role. The RAM role is a virtual user (or shadow account), which is a type of RAM user. This type of virtual user has a fixed ID and can also be assigned a set of permissions (policy), but the user does not have a fixed identity authentication key (logon password or AccessKey). The difference between the RAM role and the ordinary RAM user mainly lies in the usage method. The RAM role needs to be played by an authorized entity user. After the successful play, the entity user will obtain the temporary security token of the RAM role. The temporary security token can be used to access authorized resources as the role identity .

The differences between RAM-Role and Textbook-Role are as follows:

- (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). It is mainly used to solve problems related to Identity Federation. 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 the entity user is already associated with the 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.

RAM related concepts

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 syntax structure*. 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.

5 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 authorizat ion granularity level. For example, authorizing a RAM user to restart only a specified cloud server.

List of cloud services supporting RAM

The following tables list the cloud services that support RAM in the following categories: *Elastic Computing*, *Database Services*, *Storage & CDN*, *Networking*, *Analytics*, *Cloud Communication*, *Monitoring and Management*, *Application Service*, *Middleware*, *Mobile Service*, *Media Services*, *Big Data (data plus)*, *Security (Alibaba Cloud Security)*, *Cloud Marketplace*, and *Domain and Hosting*.

Each table contains the following information:

- Service: name of the cloud service that supports RAM
- Console: whether the current service supports RAM through the console; “v” indicates " supported", “×” indicates "not supported", and “○” indicates "not available".
- API: whether the current service supports RAM through the API; “v” indicates "supported", “×” indicates "not supported", and “○” indicates "not available".
- Authorization granularity: minimum authorization granularity provided by the current service
- System policy: system policy supported by the current service
- Reference: document link

Elastic Computing

Service	Console	API	Authorization granularity	System policy	Reference
Elastic Compute Service	√	√	Resource level	• AliyunECSFullAccess • AliyunECSReadOnlyAccess	*ECS authorization rules*
Server Load Balancer	√	√	Resource level	• AliyunSLBFullAccess • AliyunSLBReadOnlyAccess	*SLB authorization rules*
Auto Scaling	√	√	Service level	• AliyunESSFullAccess • AliyunESSReadOnlyAccess	*Auto Scaling API usage instructions*
Container Service	√	√	Service level	AliyunCSFullAccess	*Use sub-accounts*
Container Registry	√	√	Resource level	• AliyunContainerRegistryFullAccess • AliyunContainerRegistryReadOnlyAccess	*Repository access control*
Resource Orchestration Service	√	√	Service level	• AliyunROSFullAccess • AliyunROSReadOnlyAccess	*Use RAM to control resource access*
BatchCompute	√	√	Service level	-	-

Service	Console	API	Authorization granularity	System policy	Reference
Function Compute	√	√	Resource level	- AliyunFCFullAccess - AliyunFCInvocationAccess - AliyunFCReadOnlyAccess	-
Elastic HPC	√	√	Operation level	- AliyunEHPCFullAccess - AliyunEHPCReadOnlyAccess	-
Simple Application Server	√	○	Operation level	AliyunSWASFullAccess	-

Database Services

Service	Console	API	Authorization granularity	System policy	Reference
ApsaraDB for RDS	√	√	Resource level	- AliyunRDSFullAccess - AliyunRDSReadOnlyAccess	*RDS authorization rules*
ApsaraDB for MongoDB	√	√	Resource level	- AliyunMongoDBFullAccess - AliyunMongoDBReadOnlyAccess	*MongoDB authorization rules*
ApsaraDB for Redis	√	√	Resource level	- AliyunKvstoreFullAccess	*Redis authorization rules*

Service	Console	API	Authorization granularity	System policy	Reference
				• AliyunKvstoreReadOnlyAccess	
ApsaraDB for Memcache	√	√	Service level	• AliyunOCSFullAccess • AliyunOCSReadOnlyAccess	-
HiTSDB	√	√	Operation level	-	-
HybridDB for PostgreSQL	√	○	Resource level	• AliyunGPDBFullAccess • AliyunGPDBReadOnlyAccess	-
Data Transmission Service	√	√	Service level	• AliyunDTSFullAccess • AliyunDTSReadOnlyAccess	-
Distributed Relational Database Service	√	○	Resource level	• AliyunDRDSFullAccess • AliyunDRDSReadOnlyAccess	-

Storage & CDN

Service	Console	API	Authorization granularity	System policy	Reference
Object Storage Service	√	√	Resource level	• AliyunOSSFullAccess • AliyunOSSReadOnlyAccess	• *OSS rights control* • *OSS authorization policy*

Service	Console	API	Authorization granularity	System policy	Reference
					configuration - *OSS rights management best practices*
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 authorization rules*
Cloud Storage Gateway	√	○	Service level	AliyunHCSSGWFullAccess	-
Hybrid Backup	√	○	Resource level	- AliyunHBRFullAccess - AliyunHBRReadOnlyAccess	-

Networking

Service	Console	API	Authorization granularity	System policy	Reference
Virtual Private Cloud	√	√	Resource level	• AliyunVPCFullAccess • AliyunVPCReadOnlyAccess	*VPC authorization rules*
Elastic IP Address	√	√	Resource level	• AliyunEIPFullAccess • AliyunEIPReadOnlyAccess	*EIP authorization rules*
Express Connect	√	√	Resource level	• AliyunExpressConnectFullAccess • AliyunExpressConnectReadOnlyAccess	*Express Connect authorization rules*
NAT Gateway	√	√	Resource level	• AliyunNATGatewayReadOnlyAccess • AliyunNATGatewayFullAccess	-

Analytics

Service	Console	API	Authorization granularity	System policy	Reference
E-MapReduce	√	√	Service level	AliyunEMRFullAccess	*E-MapReduce role authorization*
HybridDB for PostgreSQL	√	√	Resource level	• AliyunGPDBFullAccess	-

Service	Console	API	Authorization granularity	System policy	Reference
				- AliyunGPDBReadOnlyAccess	

Cloud Communication

Service	Console	API	Authorization granularity	System policy	Reference
Message Service	√	√	Resource level	- AliyunMNSFullAccess - AliyunMNSReadOnlyAccess	*Message Service authorization rules*
DirectMail	√	√	Service level	- AliyunDirectMailFullAccess - AliyunDirectMailReadOnlyAccess	-
Short Message Service	√	√	Service level	-	-

Monitoring and Management

Service	Console	API	Authorization granularity	System policy	Reference
CloudMonitor	√	√	Service level	- AliyunCloudMonitorFullAccess - AliyunCloudMonitorReadOnlyAccess	*RAM for CloudMonitor*

Service	Console	API	Authorization granularity	System policy	Reference
Resource Access Management	√	√	Resource level	• AliyunRAMFullAccess • AliyunRAMReadOnlyAccess	*RAM API reference*
ActionTrail	√	√	Resource level	-	-
Key Management Service	√	√	Resource level	• AliyunKMSFullAccess • AliyunKMSReadOnlyAccess • AliyunKMSCryptoAccess	*KMS authorization rules*

Application Service

Service	Console	API	Authorization granularity	System policy	Reference
Log Service	√	√	Resource level	• AliyunLogFullAccess • AliyunLogReadOnlyAccess	• *Grant RAM sub-accounts permissions to access Log Service* • *Authorization rules*
API Gateway	√	√	Service level	• Aliyunapigatewayfullaccess • AliyunApiGatewayReadOnlyAccess	-

Service	Console	API	Authorization granularity	System policy	Reference
DirectMail	√	√	Operation level	- AliyunDirectMailFullAccess - AliyunDirectMailReadOnlyAccess	-
Message Service	√	√	Resource level	- AliyunMNSFullAccess - AliyunMNSReadOnlyAccess	-

Middleware

Service	Console	API	Authorization granularity	System policy	Reference
Enterprise Distributed Application Service	√	×	Service level	AliyunEDASFullAccess	*Sub-accounts*
Message Queue	√	√	Resource level	- AliyunMQFullAccess - AliyunMQPubOnlyAccess - AliyunMQSubOnlyAccess	-
Application Real-Time Monitoring Service	√	×	Service level	-	-
Application configuration management	√	√	Resource level	-	-

Mobile Service

Service	Console	API	Authorization granularity	System policy	Reference
Mobile Security (Application Security)	√	√	Service level	AliyunYundunJaqFullAccess	-

Media Services

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

Big Data (data plus)

Service	Console	API	Authorization granularity	System policy	Reference
Quick BI	√	√	Service level	-	-
Machine Learning	√	√	Service level	-	-
DataV	√	√	Service level	-	-
Elasticsearch	√	√	Resource level	-	-

Security (Alibaba Cloud Security)

Service	Console	API	Authorization granularity	System policy	Reference
Server Guard (Server Security)	√	○	Service level	AliyunYundunAegisFullAccess	-

Service	Console	API	Authorization granularity	System policy	Reference
Anti-DDoS Basic	√	○	Service level	• AliyunYundunDDosFullAccess • AliyunYundunDDosReadOnlyAccess	-
Anti-DDoS Pro	√	○	Service level	• AliyunYundunHighFullAccess • AliyunYundunHighReadOnlyAccess	-
Web Application Firewall (Network Security)	√	○	Service level	• AliyunYundunWAFFullAccess • AliyunYundunWAFReadOnlyAccess	-
Alibaba Content Security Service (Business Security)	√	○	Service level	-	-
Certificate Service	√	○	Service level	AliyunYundunCertFullAccess	-
Mobile Security	√	○	Service level	AliyunYundunJaqFullAccess	-
SSL Certificate (Application Security)	√	○	Service level	• AliyunYundunCertFullAccess • AliyunYundunCertReadOnlyAccess	-

Cloud Marketplace

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

Domain and Hosting

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

List of cloud services supporting STS

The following table lists the cloud services that support STS.

The table conventions in this table are the same as those in *List of cloud services supporting RAM*.

Service	Console	API
Elastic Compute Service	√	√
ApsaraDB for RDS	√	√
Server Load Balancer	√	√
Object Storage Service	√	√
Virtual Private Cloud	√	√