Alibaba Cloud
Resource Access Management

Product Introduction

Issue: 20190228

MORE THAN JUST CLOUD | Alibaba Cloud

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.	 Notice: 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]*

Style	Description	Example
{} 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?

Alibaba Cloud Resource Access Management (RAM) is an identity and access management serves that helps you manage user identities and control access to your cloud resources. By using RAM, you can create and manage users, who may be employees, systems, or applications. and control the resource operation permission s for these RAM users. When multiple RAM users in your enterprise collaboratively operate on resources, RAM keeps the keys for these RAM users confidential and only grants minimum permissions so to reduce information security risks.

Identity management and access control

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

Identity

An identity refers to any person, system, or application that uses resources in the RAM console or through open APIs. To manage identities in different application scenarios, RAM supports two types of identities, RAM users and RAM roles.

- A RAM user is an entity identity with a fixed ID and an identity authentication key. Generally, a RAM user corresponds to a person or an application.
- A RAM role is a virtual identity with a fixed ID but without an identity authentica tion key.

A RAM role must be associated with an entity identity before it can be used. A RAM role can be associated with multiple entity identities, such as:

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

Policy

RAM allows you to create and manage multiple policies under your account. In essence, each policy is a collection of permissions. Administrators can attach one or more policies to a RAM identity (a RAM user or RAM role).

The RAM policy language expresses fine-grained authorization semantics. A policy can grant permissions to a specific API action or resource ID and specify multiple restrictions (such as source IP address, access time, and MFA).

Relationship between accounts and RAM users

- From the ownership perspective, an account and its RAM users are in parent-child relationship.
  - An account is the basic entity for judging the ownership of Alibaba Cloud resources and billing for resource consumption.
  - RAM users exist only in RAM instances of a certain account. RAM users do not possess resources, and the resources they create under authorization belong to their accounts. RAM users do not possess bills, and all fees incurred by their authorized operations are debited to their accounts.
- From the permission perspective, an account and its RAM users are in root–user relationship (similar to the relationship in Linux).
  - The root user has all operation and control permissions on resources.
  - RAM users only have permissions that are granted by the root user. The root user can revoke the permissions at any time.

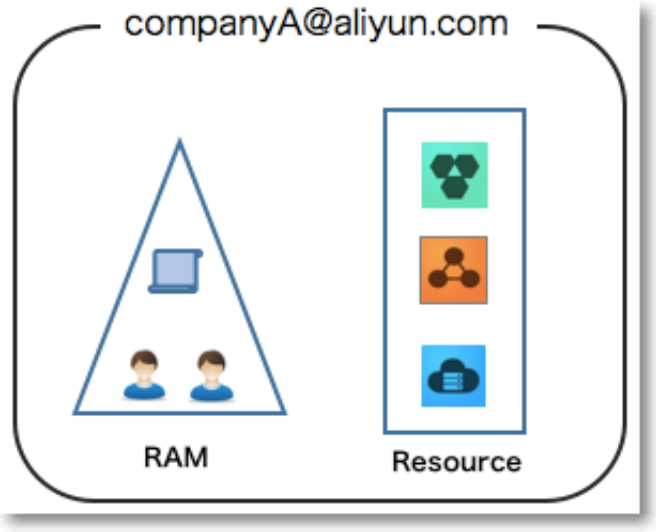
Use RAM to manage cloud resources for enterprises

RAM is applicable to the following enterprise scenarios:

- An enterprise needs to manage the account and permissions of each operator (or application) in a simplified manner.
- An enterprise does not want to calculate the costs and fees for each operator (or application) separately.

The specific requirements are shown in the following figure.

Figure 1-1: Enterprise scenario



- Company A only needs one account (for example, companyA@aliyun.com).
- All resources belong to the account. As the resource owner, the account has full control over all resources. It also pays for all bills.
- Company A can use RAM to create independent RAM users for operators (the employees who perform operation and maintenance on resources) and grant permissions to the RAM users.
- RAM users do not possess resources. By default, they do not have access permissions on the resources they create and can only operate on the resources after they are authorized.
- The fees incurred due to operations of RAM users are billed by their accounts. RAM users have no permission to pay for themselves.

Learning path

You can visit the *RAM Learning Path* for the knowledge you need to become a RAM expert!

2 Features

RAM helps manage identities and control resource access with various features.

Manage RAM users and their keys

You can create and manage RAM users and their keys under your account and attach or detach MFA devices for them.

Control access permissions of RAM users

You can attach one or more policies to a user or a user group to restrict users' operation permissions on resources.

Control resource access methods of RAM users

You can specify that users use security channels (for example, SSL) to operate on the specified cloud resources at a specified time or from specified source IP addresses.

Manage identity associations of RAM roles and external accounts

You can associate a RAM role with an external identity system (such as your local enterprise domain account or app account). In this way, you can directly use the external identity to log on to the Alibaba Cloud console or use APIs as the RAM role identity.

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, you can still fully control the user's instances and data.

Pay for bills

Your account pays for all fees incurred due to resource operations performed by all RAM users.

3 Scenarios

RAM is applicable to user account management and authorization in an enterprise , resource management and authorization between enterprises, and temporary authorization and management for apps running on untrusted UEs.

Account management and authorization in an enterprise

Assume that an enterprise A purchases several types of cloud resources (such as ECS instances, RDS instances, SLB instances, and OSS buckets), and its employees need to operate these resources (such as purchase, O&M, or online application). Different employees require different permissions because the employees have different responsibilities.

Requirements

- For security and reliability, enterprise A does not want to disclose its account key to its employees. Enterprise A prefers to create different RAM user accounts for their employees.
- The employees can operate on resources only after they are authorized. All the fees incurred by the employees will not be charged independently but be paid by enterprise A.
- Enterprise A can revoke the permissions of a RAM user account or delete a user account at any time.

Resource management and authorization between enterprises

Assume that there are enterprises A and B and enterprise A has purchased many cloud resources (such as ECS instances, RDS instances, SLB instances, and OSS buckets) for its business requirements.

Requirements

- Enterprise A wants to focus on its business systems, so it entrusts O&M, monitoring, and management for its cloud resources or grant permissions on its cloud resources to enterprise B.
- Enterprise B can assign O&M tasks to its employees. In this way, enterprise B can precisely control the employees' permissions on the cloud resources of enterprise A.

- If enterprises A and B terminate their O&M entrustment contract, enterprise A can revoke the permissions of enterprise B at any time.

Temporary authorization and management for apps running on untrusted UEs

Assume that an enterprise A has developed a mobile app and has purchased OSS for it . Then, the mobile app can upload data to and download data from the OSS.

Requirements

- Enterprise A does not want the app to use the appServer to transmit data. Instead, enterprise A wants the app to directly upload data to and download data from the OSS.
- Because the mobile app runs on a UE and enterprise A cannot control the UE. For security reasons, enterprise A cannot save its key in the app.
- Enterprise A wants to minimize its security risks by, for example, giving the app an access token with the minimum permissions that the app needs to connect to the OSS and restricting the access duration to a specified period of time (for example, 30 minutes).

4 Terms

This topic defines commonly used terms in the Alibaba Cloud RAM service.

Terms related to identity management

Account

The basic entity for identifying the ownership of Alibaba Cloud resources and measuring and billing the corresponding resources. Before using Alibaba Cloud services, you must register an account. An account owner has full control over all of its resources, and manages payment for all resources under its account (including fees incurred by RAM users under the account)

By default, a resource can be accessed only by its owner (ResourceOwner). Other users can access the resource only after they obtain the corresponding authorizat ion from the owner. Therefore, from the perspective of permission management, an account plays a role similar to the root user or administrator of an operating system (OS). Such an account is also called the root account or primary account.

Account alias

A parameter that, in RAM, each account can set as a globally unique account identifier. The alias is mainly used for RAM user logon, and is presented as a display name after logon.

For example, a company named company1 sets company1 as its account alias. The RAM user alice can then use alice@company1 to log on to the RAM console. The displayed name of RAM user alice is then alice@company1.

Default domain name and domain alias of an account

Default domain name

A unique identifier of an account that is used in scenarios such as RAM user logon and identity federation management. Alibaba Cloud assigns a default domain name for each account in the format `< AccountAli as >. onaliyun . com` .

With a default domain name, you can name a RAM user in the standard format, for example, alice@company1.onaliyun.com.

Domain alias

If you have a domain name that can be parsed on the Internet, you can replace the default domain name with your custom domain name. Such a domain name is called domain alias.

 Note:
A domain alias can be used only after it passes domain ownership verification. After the verification, you can use the domain alias in all scenarios where the default domain name is required.

A RAM user with a suffix of the account alias, default domain name, or domain alias after their user name can log on to the RAM console.

Identity credential

A credential component that is used to verify the real identity of a user. Generally , identity credential refers to a user's logon password or AccessKey (AK). Identity credentials are necessary for account security, so users are strongly recommended to keep their credentials secure and private. The following components are typically involved in an identity credential:

- Logon name/password (Password): You can use your logon name and password to access the Alibaba Cloud console to view orders or bills, and purchase or operate resources.
- AK (AccessKey): You can use your AK to construct an API request (or use a cloud service SDK) to operate resources.
- Multi-Factor Authentication (MFA): MFA is a simple but effective best practice that can provide additional security protection compared with traditional user name and password methods. When you log on to Alibaba Cloud with MFA enabled, the system requires two security factors:
  - The first security factor is your user name and password.
  - The second security factor is the variable verification code provided by your target virtual MFA device.

  When combined, these authentication factors greatly increase the security of your account.

RAM user

A type of sub-user under the account (account owner). An account owner can create multiple RAM users (corresponding to employees, systems, or applications of an

enterprise) under their account. RAM users do not own resources, cannot function independently from the corresponding account, and have no measurement or billing permissions. Instead, the account has full control over its corresponding RAM users and pays the fees associated to them. Additionally, the RAM users are visible only to the corresponding account. RAM users can log on to the RAM console or use APIs to operate the resources under the account only after being authorized by the account.

RAM user identities are divided into:

- RAM user, which includes entity identities with fixed IDs and identity credentials. Generally, a RAM user is associated with a specific person or application (a physical identity).
- RAM role, which is a virtual identity without fixed identity credentials. A RAM role must be associated with an entity identity for it to become valid.

RAM role

A type of RAM user but of a virtual identity. RAM roles can be granted a set of policies . However, RAM roles do not have fixed identity credentials (logon passwords or AKs).

RAM roles and RAM users are different in usage. RAM roles can be used only after being assumed by a trusted entity. The entity obtains temporary security tokens of the RAM role, and then use the token to access the authorized resources as role identities.

- Role assuming and switching
- A trusted entity can switch from the logon identity to a role identity (SwitchRole): After a trusted entity (for example, a RAM user) logs on to the RAM console, the RAM user can click Switch Role if the trusted entity has been associated with a role. The RAM user can only switch to one role at a time. When the RAM user switches from the logon identity to a role identity, the RAM user can only use the permissions granted to the role identity, and the permissions bound to the logon identity are temporarily unavailable. If the RAM user needs to use permissions of the logon identity, the RAM user must switch from the role identity back to the logon identity.
- A trusted entity can assume a role by calling an application (AssumeRole): If the trusted entity (for example, a RAM user) is associated with a RAM role, the RAM user can use an AK to call the AssumeRole API of Security Token Service (STS) to obtain a temporary AK of the RAM role. The temporary AK has a validity period

and restricted access permissions (within the permission set bound to the role). The temporary AK is used to resolve temporary authorization problems.

Terms related to access control

Resource

An abstraction of the objects that are presented by a cloud service to users and are used for interaction with users. OSS buckets, OSS objects, and ECS instances are examples of resources.

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

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

where:

- `acs` is the abbreviation of Alibaba Cloud Service, indicating the public cloud platform of Alibaba Cloud.
- `service - name` indicates the name of a cloud service provided by Alibaba Cloud, such as `ecs` (ECS) and `oss` (OSS).
- `region` indicates region information. If this option is not supported, the wildcard "*" is used instead.
- `account - id` indicates an account ID, for example, `1234567890 123456`.
- `resource - relative - id` indicates resources related services. Its meaning changes based on the specific service type. For example, `acs : oss :: 1234567890 123456 : sample_buc ket / file1 . txt` indicates an OSS resource on the public cloud platform, where `sample_buc ket / file1 . txt` indicates the OSS object name and `1234567890 123456` indicates the object owner.

Permission

An action by which you can allow or deny a user to perform certain operations on a particular cloud resource.

Permission operations can be divided into:

- Resource management and control operations, which indicate managing the cloud resource life cycle and operating and maintaining resources, for example, creating,

stopping, and restarting ECS instances, or creating, modifying, and deleting OSS buckets. Such operations are intended for resource purchasers or O&M employees in your organization.

- Resource use operations, which indicate using core functions of resources, for example, operating an ECS instance OS and uploading/downloading OSS bucket data. Such operations are intended for R&D employees or application systems in your organization.

 Note:
For ECS and database products, resource management and control operations can be managed through RAM, while resource use operations can be managed by instances of each product (for example, permission control on ECS instance OSs or provided by MySQL database). For storage products, such as OSS and Table Store, both types of operations can be managed through RAM.

Policy

A type of simple language specifications that describe a permission. For the language specifications supported by RAM, see *Policy syntax structure*.

RAM supports two types of policies:

- System access policies, which are managed by Alibaba Cloud. You can use but cannot modify such policies. Alibaba Cloud automatically updates system policy versions.
- Custom access policies, which are managed by accounts. You can create or delete the custom access policies at anytime. Additionally, you must maintain custom policy versions by yourself.

5 Alibaba Cloud services that work with RAM

This topic describes the Alibaba Cloud services that integrate with Alibaba Cloud RAM and Alibaba Cloud STS, the authorization granularity and policies supported by each service, and links to these services.

When a product is integrated with RAM, relevant permissions are granted to RAM users according to the following authorization granularities:

- Service: RAM users are authorized by cloud product. A RAM user either has all permissions or has no permission on a cloud product.
- Operation: RAM users are authorized by API. A RAM user can perform specified operations on specified resources of a specified cloud product.
- Resource: RAM users are authorized by resource operation. For example, you can grant the permission of restarting a cloud server to a RAM user. Resource is the finest granularity of authorization in Alibaba Cloud RAM.

Supported services

The following tables detail the cloud services that support RAM and STS, and relevant content for your reference. Note that a circle (○) indicates the corresponding function is not applicable to the corresponding service.

Elastic Computing

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Elastic Compute Service	√	√	√	√	Resource	· AliyunECSFullAccess · AliyunECSReadOnlyAccess	ECS authorization rules

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Server Load Balancer	√	√	√	√	Resource	· AliyunSLBFullAccess · AliyunSLBReadOnlyAccess	SLB authorization rules
Auto Scaling	√	√	×	×	Resource	· AliyunESSFullAccess · AliyunESSReadOnlyAccess	API usage instructions
Container Service for Kubernetes	√	√	×	×	Resource	AliyunCSFullAccess	Use sub-accounts
Container Registry	√	√	×	×	Resource	· AliyunContainerRegistryFullAccess · AliyunContainerRegistryReadOnlyAccess	Repository access control
Resource Orchestration Service	√	√	×	×	Resource	· AliyunROSFullAccess · AliyunROSReadOnlyAccess	Use RAM to control resource access
BatchCompute	√	√	×	×	Resource	-	-

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Function Compute	√	√	×	√	Resource	· AliyunFCFullAccess · AliyunFCInvocationAccess · AliyunFCReadOnlyAccess	
E-HPC	√	√	×	×	Operation	· AliyunEHPCFullAccess · AliyunEHPCReadOnlyAccess	
Simple Application Server	√	○	×	×	Operation	AliyunSWASFullAccess	

ApsaraDB

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
ApsaraDB for RDS	√	√	√	√	Resource	· AliyunRDSFullAccess · AliyunRDSReadOnlyAccess	

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
ApsaraDB for MongoDB	√	√	×	×	Resource	· AliyunMongoDBFullAccess · AliyunMongoDBReadOnlyAccess	
ApsaraDB for Redis	√	√	×	×	Resource	· AliyunKvstoreFullAccess · AliyunKvstoreReadOnlyAccess	
ApsaraDB for Memcache	√	√	×	×	Service	· AliyunOCSFullAccess · AliyunOCSReadOnlyAccess	
(High-Performance Time Series Database) HiTSDB	√	√	×	×	Operation	-	-
HybridDB for PostgreSQL	√	○	×	×	Resource	· AliyunGPDBFullAccess · AliyunGPDBReadOnlyAccess	Authentication rules for APIs

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Data Transmission Service	√	√	×	×	Service	· AliyunDTSFullAccess · AliyunDTSReadOnlyAccess	
Distributed Relational Database Service	√	○	×	×	Resource	· AliyunDRDSFullAccess · AliyunDRDSReadOnlyAccess	

Storage & CDN

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Object Storage Service	√	√	√	√	Resource	· AliyunOSSFullAccess · AliyunOSSReadOnlyAccess	
NAS	√	○	×	×	Service	· AliyunNASFullAccess · AliyunNASReadOnlyAccess	

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Table Store	√	√	×	×	Resource	· AliyunOTSFullAccess · AliyunOTSReadOnlyAccess · AliyunOTSWriteOnlyAccess	
Alibaba Cloud CDN	√	√	×	×	Resource	· AliyunCDNFullAccess · AliyunCDNReadOnlyAccess	
Cloud Storage Gateway	√	○	×	×	Service	AliyunHCSSGWFullAccess	
Hybrid Backup Recovery	√	○	×	×	Resource	· AliyunHBRFullAccess · AliyunHBRReadOnlyAccess	

Networking

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Virtual Private Cloud	√	√	√	√	Resource	· AliyunVPCFullAccess · AliyunVPCReadOnlyAccess	RAM authentication
Elastic IP Address	√	√	×	×	Resource	· AliyunEIPFullAccess · AliyunEIPReadOnlyAccess	
Express Connect	√	√	×	×	Resource	· AliyunExpressConnectFullAccess · AliyunExpressConnectReadOnlyAccess	
NAT Gateway	√	√	×	×	Resource	· AliyunNATGatewayReadOnlyAccess · AliyunNATGatewayFullAccess	

Analysis

Service	Supports console access?	Supports API access?	Authorization granularity (minimum)	System policy	Reference
E-MapReduce	√	√	Service	AliyunEMRFullAccess	-
HybridDB for PostgreSQL	√	√	Resource	· AliyunGPDBFullAccess · AliyunGPDBReadOnlyAccess	*Authentication rules for APIs*

Cloud Communication

Service	Supports console access?	Supports API access?	Authorization granularity (minimum)	System policy	Reference
Message Service	√	√	Resource	· AliyunMNSFullAccess · AliyunMNSReadOnlyAccess	
Direct Mail	√	√	Service	· AliyunDirectMailFullAccess · AliyunDirectMailReadOnlyAccess	-
Short Message Service	√	√	Service	-	-

Monitoring and Management

Service	Supports console access?	Supports API access?	Authorization granularity (minimum)	System policy	Reference
CloudMonitor	√	√	Service	· AliyunCloudMonitorFullAccess · AliyunCloudMonitorReadOnlyAccess	
ActionTrail	√	√	Resource	-	*RAM account authentication*
Key Management Service	√	√	Resource	· AliyunKMSFullAccess · AliyunKMSReadOnlyAccess · AliyunKMSCryptoAccess	*Use RAM for KMS resource authorization*

Application Services

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Log Service	√	√	×	×	Resource	· AliyunLogFullAccess · AliyunLogReadOnlyAccess	*Authentication rules*

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
API Gateway	√	√	×	×	Service	· AliyunApiGatewayFullAccess · AliyunApiGatewayReadOnlyAccess	
Direct Mail	√	√	×	×	Operation	· AliyunDirectMailFullAccess · AliyunDirectMailReadOnlyAccess	
Message Service	√	√	×	×	Resource	· AliyunMNSFullAccess · AliyunMNSReadOnlyAccess	

Middleware

Service	Supports console access?	Supports API access?	Authorization granularity (minimum)	System policy	Reference
Enterprise Distributed Application Service	√	×	Service	AliyunEDASFullAccess	*Sub-accounts*

Service	Supports console access?	Supports API access?	Authorization granularity (minimum)	System policy	Reference
Message Queue	√	√	Resource	· AliyunMQFullAccess · AliyunMQPubOnlyAccess · AliyunMQSubOnlyAccess	
Application Real Time Monitoring Service	√	×	Service	-	-
Application Configuration Management	√	√	Resource	-	-

Alibaba Cloud Mobile Services

Media Services

Service	Supports console access?	Supports API access?	Authorization granularity (minimum)	System policy	Reference
Media Processing Service	√	√	Service	· AliyunMTSFullAccess · AliyunMTSPlayerAuth	*Sub-account console operating instructions*
ApsaraVideo VoD	√	√	Service	AliyunVODFullAccess	-
ApsaraVideo Live	√	√	Service	AliyunLiveFullAccess	*API authentication rules*

DTplus

Service	Supports console access?	Supports API access?	Authorization granularity (minimum)	System policy	Reference
Quick BI	√	√	Service	-	-
Machine Learning	√	√	Service	-	-
DataV	√	√	Service	-	-
Alibaba Cloud Elasticsearch	√	√	Resource	-	-

Security

Service	Supports console access?	Supports API access?	Authorization granularity (minimum)	System policy	Reference
Server Guard	√	○	Service	AliyunYundunAegisFullAccess	-
Anti-DDoS Basic	√	○	Service	· AliyunYundunDDosFullAccess · AliyunYundunDDosReadOnlyAccess	-
Anti-DDoS Pro	√	○	Service	· AliyunYundunHighFullAccess · AliyunYundunHighReadOnlyAccess	-

Service	Supports console access?	Supports API access?	Authorization granularity (minimum)	System policy	Reference
Web Application Firewall	√	○	Service	· AliyunYundunWAFFullAccess · AliyunYundunWAFReadOnlyAccess	-
Content Moderation	√	○	Service	-	-
Mobile Security	√	○	Service	AliyunYundunJaqFullAccess	-
SSL Certificates	√	○	Service	· AliyunYundunCertFullAccess · AliyunYundunCertReadOnlyAccess	-

Marketplace

Service	Supports console access?	Supports API access?	Authorization granularity (minimum)	System policy	Reference
Marketplace	√	○	Service	AliyunMarketplaceFullAccess	-

Domains & Websites

Service	Supports console access?	Supports API access?	Authorization granularity (minimum)	System policy	Reference
Alibaba Cloud DNS	√	○	Service	· AliyunDNSFullAccess · AliyunDNSReadOnlyAccess	
Domains	√	√	Resource	AliyunDomainFullAccess	*Domain API Authentication Rules*