Alibaba Cloud
Resource Access Management

Product Introduction

Issue: 20181122

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 restrictio ns (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.

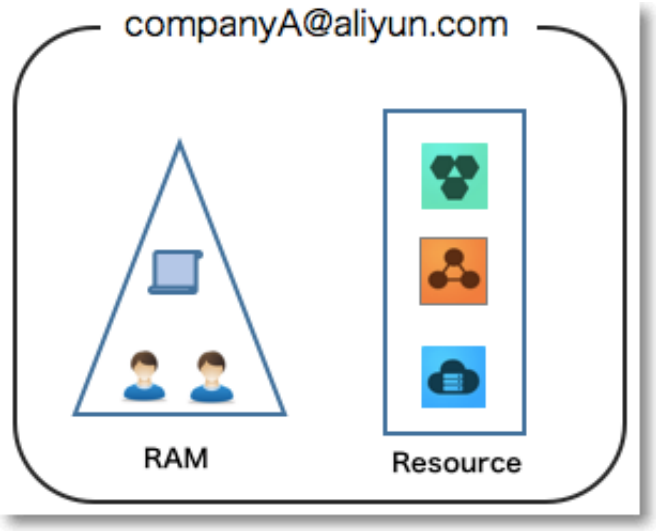
Perform enterprise-level cloud resource management using RAM

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.

Learning path

Visit the *RAM Learning Path* for the knowledge you need to become a RAM expert!

2 Features

RAM helps you with **user identity management** and **resource access management**. RAM provides the following features:

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 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 authorization 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 `<AccountAlias>.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**, wich 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 have specific identities and can be granted a set of policies. However, RAM roles do not have specific identity authentication keys (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, `1234567890123456`.
- `resource-relative-id` indicates resources related services. Its meaning changes based on the specific service type. For example, `acs:oss::1234567890123456:sample_bucket/file1.txt` indicates an OSS resource on the public cloud platform, where `sample_bucket/file1.txt` indicates the OSS object name and `1234567890123456` 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.

4 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	*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	-
ApsaraDB for MongoDB	√	√	Resource level	• AliyunMongoDBFullAccess • AliyunMongoDBReadOnlyAccess	-
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	-

Service	Console	API	Authorization granularity	System policy	Reference
Network Attached Storage	√	○	Service level	• AliyunNASFullAccess • AliyunNASReadOnlyAccess	*Use permission groups*
Table Store	√	√	Resource level	• AliyunOTSFullAccess • AliyunOTSReadOnlyAccess • AliyunOTSWriteOnlyAccess	*Customize permissions*
CDN	√	√	Resource level	• AliyunCDNFullAccess • AliyunCDNReadOnlyAccess	*API authentication 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	-

Service	Console	API	Authorization granularity	System policy	Reference
Elastic IP Address	√	√	Resource level	• AliyunEIPFullAccess • AliyunEIPReadOnlyAccess	-
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 • AliyunGPDBReadOnlyAccess	-

Cloud Communication

Service	Console	API	Authorization granularity	System policy	Reference
Message Service	√	√	Resource level	• AliyunMNSFullAccess • AliyunMNSReadOnlyAccess	-
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*
Resource Access Management	√	√	Resource level	• AliyunRAMFullAccess • AliyunRAMReadOnlyAccess	*RAM API reference*
ActionTrail	√	√	Resource level	-	-

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

Service	Console	API	Authorization granularity	System policy	Reference
				• 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	-
Anti-DDoS Basic	√	○	Service level	• AliyunYundunDDosFullAccess • AliyunYundunDDosReadOnlyAccess	-
Anti-DDoS Pro	√	○	Service level	• AliyunYundunHighFullAccess	-

Service	Console	API	Authorization granularity	System policy	Reference
				• 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	√	√