

Alibaba Cloud Resource Access Management Product Introduction

Issue: 20190530

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 <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>switch {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 What is RAM?.....	1
2 Features.....	3
3 Scenarios.....	4
4 Terms.....	6
5 Limits.....	11
6 Alibaba Cloud services that work with RAM.....	13

1 What is RAM?

Alibaba Cloud Resource Access Management (RAM) is an identity and access management service that helps you manage user identities and access to your cloud resources. You can use RAM to create and manage RAM users and control their level of access permissions to resources under your Alibaba Cloud account. RAM allows you to give users the minimum level of necessary permissions to reduce security risks.

Identity

An identity refers to any person, system, or application that uses resources in the RAM console or through APIs. To manage identities in different application scenarios, RAM supports two types of identities: RAM users and RAM roles. For more information, see [Terms](#).

Features of RAM

RAM allows you to create and manage multiple identities under an Alibaba Cloud account and to attach different policies to different identities or identity groups. That is, RAM grants different resource access permissions to different RAM users. The features of RAM are as follows:

- **Manage RAM users and their keys:** You can create and manage RAM users and their keys under your Alibaba Cloud account and attach Multi-Factor Authentication (MFA) devices for them.
- **Manage access permissions of RAM users:** You can manage a RAM user's permission for operating on resources.
- **Manage resource access methods of RAM users:** You can specify that RAM users must use security channels to operate on specified cloud resources at a specified time or from specified source IP addresses.
- **Manage cloud resources:** You can manage the instances and data created by RAM users. Therefore, when a user leaves your organization, you can still fully control the user's instances and data.
- **Manage Single Sign On (SSO):** You can perform user-based SSO or role-based SSO to Alibaba Cloud by using your identity provider (IdP).

Policy

RAM allows you to create and manage multiple policies under your Alibaba Cloud account. Each policy is a collection of permissions. Administrators can attach one or more policies to a RAM user, a RAM user group, or a RAM role.

The RAM policy language expresses fine-grained authorization semantics. A policy can grant permissions to a specific action or resource and specify multiple restrictions (such as the source IP address, access time, and MFA). For more information, see [Policy management](#).

Accessing RAM

The endpoint for API access is `https://ram.aliyuncs.com`.

Free to use

You can use RAM for free after creating an Alibaba Cloud account.

You can go to the [RAM logon](#) page to create an Alibaba Cloud account.

Alibaba Cloud services that work with RAM

See [Alibaba Cloud services that work with RAM](#).

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

This topic describes some of the common application scenarios of Resource Access Management (RAM).

Application scenario	Description
<i>User management and access control</i>	Enterprise A has bought several types of Alibaba Cloud resources, such as ECS instances, RDS instances, SLB instances, and OSS buckets for a project . During this project, many employees need to perform operations on these cloud resources, but different employees require different permissions to complete different operations.
<i>Temporary authorization for mobile apps</i>	Enterprise A has developed a mobile app, which runs on users' own devices . Enterprise A cannot manage these devices directly and wants to use Alibaba Cloud OSS so that the app can upload data to and download data from OSS.
<i>Cross-account resource authorization and access</i>	Account A and Account B are Alibaba Cloud accounts of two different enterprises (Enterprise A and Enterprise B, respectively). Enterprise A has bought various cloud resources (such as ECS instances, RDS instances, SLB instances, and OSS buckets) to support its business . Account A is the resource owner and wants to grant Account B the relevant permissions to perform operations on resources of Account A.
<i>Dynamic identity and permission management of cloud applications</i>	An enterprise has bought ECS instances and wants to deploy its applications in ECS. The enterprise wants to allow the applications to access other Alibaba Cloud APIs by using AccessKeys.

Application scenario	Description
<i>Externally authorized account logon</i>	Enterprise A has two departments that use Alibaba Cloud resources. Each department has its own Alibaba Cloud account (named A1 and A2). Enterprise A also has its own domain account system , namely Microsoft Active Directory (AD) and Active Directory Federation Services (AD FS).

4 Terms

This topic explains terms that are commonly used in Alibaba Cloud RAM.

Alibaba Cloud account

An Alibaba Cloud account, also known as the root account or primary account, is the account type used to own Alibaba Cloud resources and manage the billing of these resources. You must register an Alibaba Cloud account before using Alibaba Cloud services. An Alibaba Cloud account owner has full operational control over all associated resources. Furthermore, the account owner can manage the payment for all resources under the Alibaba Cloud account (including fees incurred by RAM users under this account).

By default, a resource can be accessed only by the owner of Alibaba Cloud account. Other users must be granted the corresponding authorization from the owner to access and operate on the resource. As a result, the Alibaba Cloud account functions similar to that of the root user or administrator of an operating system.

RAM user

A RAM user is an identity with a fixed ID and credential information. Generally, a RAM user directly corresponds to a specific identity, which can be either a person or an application.

- An Alibaba Cloud account owner can create multiple RAM users (which correspond to employees, systems, or applications of their enterprise) under their account.
- RAM users do not own resources. Rather, the fees incurred by RAM users are billed to the Alibaba Cloud accounts to which they belong. RAM users do not receive individual bills and cannot make payments.
- RAM users are visible only to the corresponding Alibaba Cloud account to which they belong.
- RAM users have permissions for only the resources under the Alibaba Cloud account to which they belong after they are authorized to operate on these resources.

RAM role

A RAM role is a virtual identity with a fixed ID but without an identity authentication key. A RAM role must be associated with the identity of a target entity before it can be used for a valid role.

More specifically, RAM roles can be used only after they are assumed by a user or service of a trusted entity. The user or service obtains the temporary security tokens of RAM roles, and then uses these tokens to access the authorized resources.

RAM roles can be associated with the following trusted entities:

- **Alibaba Cloud account:** a type of role that RAM users can assume. The RAM users may belong to their own Alibaba Cloud account or another Alibaba Cloud account. Such type of role can be assumed to achieve cross-account access through temporary authorization.
- **Alibaba Cloud service:** a type of role that cloud services can assume. Such type of role can be used to authorize cloud services to operate resources as stand-alone applications.
- **Identity provider (IdP):** a type of role that users in a trusted identity provider (IdP) can assume. Such type of role can be used to implement Single Sign On (SSO) to Alibaba Cloud.

Identity credential

An identity credential is used to verify the real identity of a user. Generally, an identity credential refers to the logon password or AccessKey (AK) of a RAM user.



Note:

Identity credentials are necessary for account security, so we recommend that you keep your credentials secure and private.

An identity credential usually contains the following:

- **Logon name and password:** You can use your logon name and password to access the Alibaba Cloud console to view order or billing information, or to purchase or operate on resources.
- **AccessKey (AK):** You can use your AK to create an API request, or to use a cloud service SDK to operate on resources.

- **Multi-Factor Authentication (MFA):** MFA is a simple but effective means for achieving a higher level security protection. When you log on to Alibaba Cloud with MFA enabled, the system requires the following two security factors:
 - Your username and password
 - The verification code provided by your target virtual MFA device

Account alias

To log on to the RAM console, a RAM user must have a username that contains the account alias, default domain name, or domain alias as a suffix.

The alias is a unique account identifier that appears at the end of the RAM user's username and forms part of the RAM user's 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 display name of RAM user Alice is then alice@company1.

Default domain name

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

Domain alias

A custom domain name that can be used to replace the default domain name provided by the system.



Note:

A domain alias can be used only after domain ownership verification.

Single Sign On (SSO)

Enterprises can implement SSO to Alibaba Cloud through an SAML 2.0-based IdP. Alibaba Cloud offers the following two SAML 2.0-based SSO methods:

- **User-based SSO:** After logging on, an Enterprise employee can use the RAM user to access Alibaba Cloud.
- **Role-based SSO:** Enterprises can manage their employees with their IdP with no need of synchronizing user information to Alibaba Cloud. In addition, an Enterprise employee can use a specified role to access Alibaba Cloud.

Permission

The means by which you can allow or deny a user to be authorized to perform certain operations on a particular cloud resource.

Permission can be used to authorize the following operations:

- **Resource management and control operations:** Used to allow managing the cloud resources, such as creating, stopping, and restarting ECS instances, or creating, modifying, and deleting OSS buckets. Such operations are intended for resource purchasers or O&M engineers in your organization.
- **Resource-use operations:** Used to allow core operations related to resources, such as operating an ECS instance operating system, and uploading or downloading OSS bucket data. Such operations are intended for R&D engineers or application systems in your organization.



Note:

- For ECS and database services, resource management and control operations can be managed through RAM, whereas resource-use operations can be managed through the instances of each product (for example, by using the permission control function provided by the ECS instance operating system or by the MySQL database running on the instance).
- For storage services, such as OSS and Table Store, both types of operations can be managed by using RAM.

Policy

A specification that defines a permission for an identity or resource on Alibaba Cloud. For more information about the policies supported by RAM, see [Policy syntax structure](#).

RAM supports two types of policies:

- **System policies:** Policies managed by Alibaba Cloud. You can use but cannot modify these policies. Alibaba Cloud automatically updates system policy versions.
- **Custom policies:** Policies managed by Alibaba Cloud account owners or RAM users. You can create or delete the custom access policies at any time. However, you must maintain custom policy versions by yourself.

Resource

An object that serves as a service package provided by Alibaba Cloud. OSS buckets, OSS objects, and ECS instances are examples of resources.

A global Alibaba Cloud Resource Name (ARN) is defined for each resource on Alibaba Cloud. The format of an ARN is as follows:

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

For more information, see [Policy elements](#).

5 Limits

This topic lists the limitations of RAM, such as the maximum number of users and the maximum number of user groups.

Item	Limit
Maximum number of users	1,000
Maximum number of user groups	50
Maximum number of groups that a user can join	5
Maximum number of AccessKeys (AKs) that a user can create	2
Maximum number of MFA devices to which a user can attach	1
Maximum number of virtual MFA devices	1,000
Maximum number of custom policies	200
Maximum number of versions that a custom policy can have	5
Maximum number of custom policies that can be attached to a user	5
Maximum number of custom policies that can be attached to a user group	5
Maximum number of custom policies that can be attached to a role	5
Maximum number of system policies that can be attached to a user	20
Maximum number of system policies that can be attached to a user group	20
Maximum number of system policies that can be attached to a role	20
Maximum number of characters that a username can contain	64
Maximum number of characters that a user group name can contain	64

Item	Limit
Maximum number of characters that a policy name can contain	128
Maximum number of characters that a role name can contain	64
Maximum number of roles	100
Number of characters that an alias can contain	3-64
Maximum number of characters that a custom policy name can contain	2,048
Maximum number of identity providers (IdPs)	100
Maximum number of IdP descriptors that an IdP metadata file can contain	1
Maximum number of certificates that an IdP descriptor in an IdP metadata file can contain	2

6 Alibaba Cloud services that work with RAM

This topic lists the Alibaba Cloud services that work with Alibaba Cloud Resource Access Management (RAM) and Alibaba Cloud Security Token Service (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 at the cloud service level. A RAM user either has all permissions or has no permissions to perform operations with a cloud service.
- **Operation:** RAM users are authorized at the API level. A RAM user can perform specified operations on specified resources of a specified cloud service.
- **Resource:** RAM users are authorized at the resource operation level. For example, you can grant a RAM user the permission to restart a cloud server. 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:

Note that a tick (✓) indicates the corresponding function is supported by the corresponding service, a cross (×) indicates the corresponding function is not supported by the corresponding service, and 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	<ul style="list-style-type: none"> • AliyunECSFullAccess • AliyunECSReadOnlyAccess • AliyunECSNetworkInterfaceManagementAccess 	Authentication rules
Auto Scaling	√	√	√	√	Service	<ul style="list-style-type: none"> • AliyunESSFullAccess • AliyunESSReadOnlyAccess 	API usage instructions
Container Service	√	√	×	√	Service	<ul style="list-style-type: none"> • AliyunCSFullAccess • AliyunCSReadOnlyAccess 	Use sub-accounts
Container Registry	√	√	×	×	Resource	<ul style="list-style-type: none"> • AliyunContainerRegistryFullAccess • AliyunContainerRegistryReadOnlyAccess 	Repository access control

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Resource Orchestration Service	√	√	√	√	Service	<ul style="list-style-type: none"> • AliyunROSFullAccess • AliyunROSReadOnlyAccess 	Use RAM to control resource access
Batch Compute	√	√	√	√	Service	N/A	N/A
Function Compute	√	√	√	√	Resource	<ul style="list-style-type: none"> • AliyunFCFullAccess • AliyunFCInvocationAccess • AliyunFCReadOnlyAccess 	Sub-account user guide
E-HPC	√	√	√	√	Service	<ul style="list-style-type: none"> • AliyunEHPCFullAccess • AliyunEHPCReadOnlyAccess 	N/A
Simple Application Server	√	○	×	○	Service	AliyunSWASFullAccess	N/A
Elastic Container Instance	√	√	√	√	Resource	<ul style="list-style-type: none"> • AliyunECIFullAccess • AliyunECIRReadOnlyAccess 	N/A

Databases

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	<ul style="list-style-type: none"> AliyunRDSFullAccess AliyunRDSReadOnlyAccess 	RAM authorization
ApsaraDB for MongoDB	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunMongoDBFullAccess AliyunMongoDBReadOnlyAccess 	N/A
ApsaraDB for Redis	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunKvstoreFullAccess AliyunKvstoreReadOnlyAccess 	RAM authorization
ApsaraDB for Memcache	√	√	√	√	Service	<ul style="list-style-type: none"> AliyunOCSFullAccess AliyunOCSReadOnlyAccess 	N/A
Time Series & Spatial Temporal Database	√	√	√	√	Operation	N/A	N/A

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
HybridDB for PostgreSQL	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunGPDBFullAccess AliyunGPDBReadOnlyAccess 	Authentication rules for APIs
Data Transmission Service	√	√	×	×	Service	<ul style="list-style-type: none"> AliyunDTSFullAccess AliyunDTSReadOnlyAccess 	Access rules with STS with RAM sub-account
Database Backup	√	√	√	√	Service	<ul style="list-style-type: none"> AliyunDBSFullAccess AliyunDBSReadOnlyAccess 	N/A
Distributed Relational Database Service	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunDRDSReadOnlyAccess AliyunDRDSFullAccess 	N/A

Storage and 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	<ul style="list-style-type: none"> AliyunOSSFullAccess AliyunOSSReadOnlyAccess 	RAM policy
Network Attached Storage	√	○	×	○	Operation	<ul style="list-style-type: none"> AliyunNASFullAccess AliyunNASReadOnlyAccess 	Use permission groups
Table Store	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunOTSFullAccess AliyunOTSReadOnlyAccess AliyunOTSWriteOnlyAccess 	Customize permissions
Alibaba Cloud CDN	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunCDNFullAccess AliyunCDNReadOnlyAccess 	API authentication token
Dynamic Route for CDN	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunDCDNFullAccess AliyunDCDNReadOnlyAccess 	N/A

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Cloud Storage Gateway	√	○	×	○	Service	AliyunHCS/A GWFullAccess	
Hybrid Backup Recovery	√	○	×	○	Resource	<ul style="list-style-type: none"> AliyunHBRFullAccess AliyunHBRReadOnlyAccess 	N/A
Lightning Cube	√	○	×	○	Service	AliyunMGWFullAccess	N/A

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	<ul style="list-style-type: none"> AliyunVPCFullAccess AliyunVPCReadOnlyAccess 	RAM authentication
Server Load Balancer	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunSLBReadOnlyAccess AliyunSLBFullAccess 	RAM authentication

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Elastic IP Address	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunEIPFullAccess AliyunEIPReadOnlyAccess 	RAM authentication
Express Connect	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunExpressConnectFullAccess AliyunExpressConnectReadOnlyAccess 	RAM authentication
NAT Gateway	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunNATGatewayReadOnlyAccess AliyunNATGatewayFullAccess 	RAM authentication
VPN Gateway	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunVPNGatewayFullAccess AliyunVPNGatewayReadOnlyAccess 	RAM authentication
Global Acceleration	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunGlobalAccelerationReadOnlyAccess AliyunGlobalAccelerationFullAccess 	RAM authentication

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Smart Access Gateway	√	√	×	×	Resource	N/A	RAM authentication
Cloud Enterprise Network	√	√	×	×	Resource	<ul style="list-style-type: none"> • AliyunCENReadOnlyAccess • AliyunCENFullAccess 	RAM authentication

Analysis

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
E-MapReduce	√	√	×	×	Service	<ul style="list-style-type: none"> • AliyunEMRFullAccess • AliyunEMRDevelopAccess • AliyunEMRFlowAdmin 	N/A
Data Lake Analytics	√	√	×	×	Operation	<ul style="list-style-type: none"> • AliyunDLAFullAccess • AliyunDLAReadOnlyAccess 	N/A

Cloud Communications

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Message Service	√	√	×	×	Resource	<ul style="list-style-type: none"> AliyunMNSFullAccess AliyunMNSReadOnlyAccess 	N/A
Short Message Service	√	√	√	√	Service	N/A	N/A

Management and Monitoring

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
CloudMonitor	√	√	√	√	Service	<ul style="list-style-type: none"> AliyunCloudMonitorFullAccess AliyunCloudMonitorReadOnlyAccess 	RAM for CloudMonitor
ActionTrail	√	√	√	√	Resource	N/A	RAM account authentication

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Resource Access Management	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunRAMFullAccess AliyunRAMReadOnlyAccess 	RAM authentication
Key Management Service	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunKMSFullAccess AliyunKMSReadOnlyAccess AliyunKMSCryptographicAccess 	Use RAM for KMS resource authorization
Intelligent Advisor	N/A	N/A	N/A	N/A	Operation	N/A	N/A

Application Service

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	<ul style="list-style-type: none"> 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
DirectMail	√	√	√	√	Service	<ul style="list-style-type: none"> AliyunDirectMailFullAccess AliyunDirectMailReadOnlyAccess 	N/A
API Gateway	√	√	√	√	Service	<ul style="list-style-type: none"> AliyunApiGatewayFullAccess AliyunApiGatewayReadOnlyAccess 	API Gateway _RAM
IoT Platform	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunIoTPlatformFullAccess AliyunIoTPlatformReadOnlyAccess 	Use RAM users
Blockchain as a Service	√	√	√	√	Resource	N/A	N/A

Middleware

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Enterprise Distributed Application Service	√	√	×	×	Service	AliyunEDASFullAccess	Sub-accounts
Distributed Relational Database Service	√	√	×	√	Resource	<ul style="list-style-type: none"> AliyunDRDSFullAccess AliyunDRDSReadOnlyAccess 	N/A
Application Real-Time Monitoring Service	√	√	×	×	Service	AliyunARMSFullAccess	N/A
Application Configuration Management	√	√	√	√	Resource	AliyunACMFullAccess	Access control

Message Queue

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
AliwareMQ for RocketMQ	√	√	×	√	Resource	<ul style="list-style-type: none"> AliyunMQFullAccess AliyunMQPublishOnlyAccess AliyunMQSubscribeOnlyAccess 	RAM Sub-account authorization
Message Service	√	√	×	√	Resource	<ul style="list-style-type: none"> AliyunMNSFullAccess AliyunMNSReadOnlyAccess 	N/A

Media Services

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
ApsaraVideo for Media Processing	√	√	×	√	Service	<ul style="list-style-type: none"> AliyunMPSFullAccess AliyunMPSFLayerAuth 	Sub-account console operating instructions
ApsaraVideo for VOD	√	√	√	√	Service	AliyunVODFullAccess	N/A

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
ApsaraVideo for Live	√	√	×	√	Resource	AliyunLiveFullAccess	API authentication rules
Real-Time Communication	√	√	×	×	Resource	N/A	N/A

Big Data (DTplus)

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
DataWorks	√	√	×	×	Service	AliyunDataWorksFullAccess	RAM User Operations
Quick BI	√	√	×	×	Service	N/A	N/A
Machine Learning	√	√	×	×	Service	N/A	N/A
Public Recognition	√	√	×	×	Service	N/A	N/A
DataV	√	√	×	×	Service	N/A	N/A
MaxCompute	√	√	×	×	Service	N/A	N/A

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Elasticsearch	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunElasticsearchReadOnlyAccess AliyunElasticsearchFullAccess 	Authorized resources
Machine Translation	N/A	N/A	N/A	N/A	Service	N/A	N/A
Image Search	√	√	√	√	Resource	<ul style="list-style-type: none"> AliyunImageSearchReadOnlyAccess AliyunImageSearchFullAccess 	Authorized policies

Security

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Threat Detection Service	√	○	√	○	Service	<ul style="list-style-type: none"> AliyunYundunSASFullAccess AliyunYundunSASReadOnlyAccess 	N/A

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Server Guard	√	○	√	○	Service	<ul style="list-style-type: none"> AliyunYundunAegisFullAccess AliyunYundunAegisReadOnlyAccess 	N/A
Anti-DDoS Basic	√	○	√	○	Service	<ul style="list-style-type: none"> AliyunYundunDDoSFullAccess AliyunYundunDDoSReadOnlyAccess 	N/A
Anti-DDoS Pro	√	○	√	○	Service	<ul style="list-style-type: none"> AliyunYundunDDoSFullAccess AliyunYundunDDoSReadOnlyAccess 	N/A
Anti-DDoS Premium	√	○	√	○	Service	<ul style="list-style-type: none"> AliyunYundunAntiDDoSPremiumFullAccess AliyunYundunAntiDDoSPremiumReadOnlyAccess 	N/A
GameShield	√	○	√	○	Service	AliyunYundunGameShieldReadOnlyAccess	N/A

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Web Application Firewall	√	○	√	○	Service	<ul style="list-style-type: none"> AliyunYundunWAFFullAccess AliyunYundunWAFReadOnlyAccess 	N/A
Alibaba Cloud SSL Certificates Service	√	○	√	○	Service	<ul style="list-style-type: none"> AliyunYundunCertFullAccess AliyunYundunCertReadOnlyAccess 	N/A
Cloud Firewall	N/A	N/A	N/A	N/A	Service	N/A	N/A
Website Threat Inspector	√	○	√	○	Service	N/A	N/A
Content Moderation	√	○	√	○	Service	AliyunYundunGreenWebFullAccess	N/A
Anti-Bot Service	√	○	√	○	Service	<ul style="list-style-type: none"> AliyunYundunAntibotFullAccess AliyunYundunAntibotReadOnlyAccess 	N/A

Marketplace

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Marketplace	√	○	√	○	Service	AliyunMarketplaceFullAccess	N/A

Domains and Websites

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Alibaba Cloud DNS	√	○	√	○	Resource	<ul style="list-style-type: none"> AliyunDNSFullAccess AliyunDNSReadOnlyAccess 	N/A
Domain	√	√	√	√	Resource	AliyunDomainFullAccess	Domain API Authentication Rules
Web Hosting	×	×	×	×	N/A	N/A	N/A
Alibaba Mail	×	×	×	×	N/A	N/A	N/A

Billing Management

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Billing Management	√	×	×	×	Service	<ul style="list-style-type: none"> AliyunBSSFullAccess AliyunBSSReadOnlyAccess AliyunBSSOrderAccess 	N/A

Support

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Support	√	○	×	○	Service	AliyunSupportFullAccess	N/A

Message

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
Message Center	√	○	×	○	Service	AliyunNotificationsFullAccess	N/A