

# **Alibaba Cloud Resource Access Management Product Introduction**

Issue: 20190911

## 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.	 <b>Danger:</b> 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.	 <b>Warning:</b> 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.	 <b>Notice:</b> 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.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
<b>Bold</b>	It is used for buttons, menus, page names, and other UI elements.	Click OK.
<code>Courier</code> 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 a 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>swich {stand   slave}</code>



# Contents

---

Legal disclaimer.....	I
Generic conventions.....	I
1 What is RAM?.....	1
2 Terms.....	3
3 Limits.....	10
4 Alibaba Cloud services that work with RAM.....	12



# 1 What is RAM?

---

Resource Access Management (RAM) is a service provided by Alibaba Cloud to manage user identities and resource access permissions.

## Features

RAM allows you to create and manage multiple identities under an Alibaba Cloud account, and grant diverse permissions to a single identity or a group of identities. In this way, different RAM users are authorized to access different Alibaba Cloud resources. The following section lists the features of RAM:

- You can manage RAM users and their AccessKey pairs. You can also enable multi-factor authentication (MFA) devices for RAM users.
- You can manage the permissions of RAM users to access Alibaba Cloud resources.
- You can manage resource access channels. This ensures that RAM users access specific Alibaba Cloud resources by using secure channels at the specified time from the specified IP address.
- You can manage the instances or data created by RAM users. For enterprises, RAM ensures that the instances or data created by RAM users are still available even if the users leave the enterprises.
- You can use single sign-on (SSO) services. Alibaba Cloud provides two types of SSO services for enterprise ID providers (IdPs): user-based SSO and role-based SSO.

## Scenarios

Scenario	Description
<a href="#">#unique_4</a>	Enterprise A has purchased several types of Alibaba Cloud resources, such as ECS instances, ApsaraDB for RDS instances, SLB instances, and OSS buckets, for the migration of a project. Certain employees need to perform operations on these cloud resources. Different employees require different permissions to fulfill the corresponding duties.

Scenario	Description
<a href="#">#unique_5</a>	Enterprise A has developed a mobile app and purchased the OSS service. The app running on the users' own mobile devices are not controlled by Enterprise A. Permissions must be granted to the app to access OSS to upload or download data.
<a href="#">#unique_6</a>	Enterprise A has purchased various Alibaba Cloud resources, such as ECS instances, ApsaraDB for RDS instances, SLB instances, and OSS buckets. Enterprise A wants to delegate certain businesses to Enterprise B.
<a href="#">#unique_7</a>	Enterprise A has purchased ECS instances and wants to deploy apps in the ECS instances. The apps need to use AccessKey pairs to call API operations of other Alibaba Cloud services.

## Benefits

RAM allows you to create and manage RAM users, such as employees, systems, and apps. You can manage the permissions of RAM users to access Alibaba Cloud resources. RAM is also applicable in the scenario where multiple users in an enterprise need to collaboratively manage cloud resources. RAM allows you to grant the corresponding users the minimum required permissions, alleviating the need to share your Alibaba Cloud account and password. In this way, security risks for your enterprise are minimized.

## Endpoint

The endpoint for accessing RAM by calling API operations is `https://RAM.aliyuncs.com`.

## Learning path

You can use [RAM learning path](#) to quickly learn about RAM and basic operations. You can also perform custom development by using diverse API operations, SDK packages, and other easy-to-use tools.

## 2 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 an 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.

### Terms related to identity management

#### Identity

Identities can be created in RAM to allow or deny access to resources in your Alibaba Cloud account. RAM users, RAM user groups, and RAM roles are identities that you can create in RAM. RAM users and RAM user groups are entity identities, whereas RAM roles are virtual identities.

#### Default domain name

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

For information about how to set a default domain name, see [#unique\\_9](#).

#### Enterprise alias

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

The enterprise 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 enterprise 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.

### 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.

For information about how to set a domain alias, see [#unique\\_10](#).

### RAM user

An identity with a fixed ID and credential information. Specifically, 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 Alibaba Cloud resources under the Alibaba Cloud account to which they belong after they are authorized to operate on these resources.

For information about how to create a RAM user, see [#unique\\_11](#).

### Password

An identity credential that is used by a user to log on to Alibaba Cloud.



#### Note:

We recommend that you change your password periodically and keep your password private.

For information about how to set a password, see [#unique\\_12](#) and [#unique\\_13](#).

### Access key

The combination of an access key ID and an access key secret. You can use your access key or Alibaba Cloud SDK to sign API requests that you make to Alibaba Cloud.

The access key ID and access key secret are used together to sign programmatic Alibaba Cloud requests cryptographically. The access key ID is used to identify a user, whereas the access key secret is used to encrypt and verify a signature.



#### Note:

The access key secret is displayed only once when you first create it. We recommend that you save the access key secret for subsequent use.

For information about how to create an access key, see [#unique\\_14](#).

### Multi-factor authentication (MFA)

A simple best practice that adds an extra layer of protection on top of your username and password. When you log on to Alibaba Cloud with MFA enabled, the system requires the following two security factors:

1. Your username and password
2. Verification code provided by the MFA device

For information about how to set MFA, see [#unique\\_15](#) and [#unique\\_16](#).

### RAM user group

A type of entity identity in RAM. You can create RAM user groups to classify and organize RAM users under your Alibaba Cloud account. By classifying and organizing your RAM users, you can effectively manage permissions in the RAM console.

- If the responsibilities of a RAM user change, you only need to move the user to a RAM user group with the appropriate permissions. This action does not affect other RAM users.

For information about how to create a RAM user group, see [#unique\\_17](#).

- If the responsibilities of a RAM user group change, you only need to modify the policy attached to the user group. Changes to the policy apply to all RAM users in the group.

For information about how to grant permission to a RAM user group, see [#unique\\_18](#).

## RAM role

A virtual identity that you can create in your Alibaba Cloud account. The differences among RAM roles, entity users (Alibaba Cloud account, RAM users, or Alibaba Cloud services), and textbook roles are as follows:

- Entity users have specific logon passwords or access keys.
- A textbook role (or a traditionally defined role) indicates a permission set, similar to a policy in RAM. If such a role is granted to a user, the user has a set of permissions and can access the authorized resources.
- As virtual users, RAM roles have specific identities and can be granted a set of policies. However, RAM roles do not have standard long-term credentials (passwords or access keys). When an entity user wants to use a role, the user must assume the role to obtain the role token. Then, the user can use the role token to call Alibaba Cloud API actions.

RAM roles are divided into the following types according to different trusted entities:

- Alibaba Cloud account: roles that RAM users can assume. The RAM users may belong to their own Alibaba Cloud accounts or other Alibaba Cloud accounts. Such roles provide solutions to cross-account access and temporary authorization.
- Alibaba Cloud service: roles that Alibaba Cloud services can assume. Such roles are used to authorize Alibaba Cloud services to operate resources as stand-alone applications.
- Identity provider (IdP): roles that users in an entrusted IdP can assume. Such roles are used to implement SSO to Alibaba Cloud.

For information about how to create a RAM role, see

- [#unique\\_19](#)
- [#unique\\_20](#)
- [#unique\\_21](#)

## Single Sign On (SSO)

Alibaba Cloud supports SAML 2.0-based SSO, also known as identity federation.

Enterprises can implement SSO with Alibaba Cloud through SAML 2.0-based IdPs (for example, AD FS). Alibaba Cloud offers the following two SAML 2.0-based SSO methods:

- **User-based SSO:** The RAM user that you can use to log on to Alibaba Cloud can be determined through a SAML assertion. After logon, you can use the RAM user to access Alibaba Cloud. For more information, see [#unique\\_22](#).
- **Role-based SSO:** The RAM role that you can use to log on to Alibaba Cloud can be determined through SAML assertions. After logon, you can use the role specified in the SAML assertion to access Alibaba Cloud. For more information, see [#unique\\_23](#).

## Metadata file

A file, usually in XML format, provided by an IdP. It contains the IdP's logon service address and X.509 public key certificate that is used to verify the validity of the SAML assertion issued by the IdP.

## Identity provider (IdP)

A RAM entity that provides identity management services. IdPs are generally classified into the following types:

- Locally deployed IdPs, such as Microsoft Active Directory Federation Service (AD FS) and Shibboleth
- Cloud-based IdPs, such as Azure AD, Google G Suite, Okta, and OneLogin

## Service provider (SP)

An application that uses the identity management function of an IdP to provide users with specific services. An SP uses the user information provided by an IdP. In some identity systems (such as OpenID Connect) that do not comply with the SAML protocol, SP is known as relying party, which means the relying party of an IdP.

## Security Assertion Markup Language 2.0 (SAML 2.0)

A protocol for enterprise-level user identity authentication. It can be used to achieve communication between an SP and an IdP. SAML 2.0 is a standard that enterprises can use to implement enterprise-level SSO.

## SAML assertion

A core element in the SAML protocol to describe the authentication request and response. For example, specific properties of a user are contained in the authentication response assertion.

## Trust

A mutual trust mechanism between an SP and an IdP. It is usually implemented by using public and private keys. An SP obtains SAML metadata of an IdP in a trusted way. The metadata includes the public key for verifying the SAML Assertion issued by the IdP. The SP can use the public key to verify the assertion integrity.

## Terms related to access control

### Permission

A statement within a policy that allows or denies access to a particular Alibaba 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 set of permissions that are described by using policy structure and grammar. It can accurately describe the authorized resource sets, operation sets, and authorization conditions a user can be granted with. For information about structures and grammars supported by RAM, see [#unique\\_24](#).

In RAM, a policy is a resource entity that can be created, updated, deleted, and viewed by RAM users. RAM supports the following two types of policies:

- **System policy:** System policies are created by Alibaba Cloud and cannot be modified by users. The policies are automatically upgraded by Alibaba Cloud.
- **Custom policy:** If no system policy meets your requirements, you can create a custom policy as needed. You can also modify and delete a custom policy as needed.
- 

You can attach one or more policies to RAM users, RAM user groups, or RAM roles. For more information, see [#unique\\_25](#), [#unique\\_18](#), and [#unique\\_26](#).

## Principal

The RAM user, group, or role that receives permissions that are defined in a policy.

## Effect

A policy element that specifies whether the statement results in an allow or an explicit deny. The valid values are `Allow` and `Deny`.

## Action

A policy element that describes the specific API action or actions that will be allowed or denied.

## Condition

A policy element that specifies when a policy takes effect.

## Resource


An entity that users can work with in Alibaba Cloud, such as an OSS bucket and an ECS instance.

## 3 Limits

---

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

Item	Limit
Maximum number of RAM users that can be created in an Alibaba Cloud account	1,000
Maximum number of characters that a username can contain	64
Maximum number of RAM user groups that a RAM user can join	5
Maximum number of access keys that a RAM user can create	2
Maximum number of multi-factor authentication (MFA) devices that can be attached to a RAM user	1
Maximum number of system policies that can be attached to a RAM user	20
Maximum number of custom policies that can be attached to a RAM user	5
Maximum number of RAM user groups that can be created in an Alibaba Cloud account	50
Maximum number of characters that a RAM user group name can contain	64
Maximum number of system policies that can be attached to a RAM user group	20
Maximum number of custom policies that can be attached to a RAM user group	5
Maximum number of RAM roles that can be created in an Alibaba Cloud account	100
Maximum number of characters that a RAM role name can contain	64
Maximum number of system policies that can be attached to a RAM role	20

Item	Limit
Maximum number of custom policies that can be attached to a RAM role	5
Maximum number of characters that an Alibaba Cloud account alias can contain	64  <b>Note:</b> The Alibaba Cloud account alias must be 3 to 64 characters in length.
Maximum number of characters that a policy name can contain	128
Maximum number of MFA devices that can be created in an Alibaba Cloud account	1,000
Maximum number of custom policies that can be created in an Alibaba Cloud account	200
Maximum number of characters that a custom policy can contain	2,048
Maximum number of versions that a custom policy can have	5
Maximum number of identity providers (IdPs) that can be created in an Alibaba Cloud account	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

## 4 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"> <li>• AliyunECSFullAccess</li> <li>• AliyunECSReadOnlyAccess</li> <li>• AliyunECSNetworkInterfaceManagementAccess</li> </ul>	<a href="#">#unique_29</a>
Auto Scaling	√	√	√	√	Service	<ul style="list-style-type: none"> <li>• AliyunESSFullAccess</li> <li>• AliyunESSReadOnlyAccess</li> </ul>	<a href="#">#unique_30</a>
Container Service	√	√	×	√	Service	<ul style="list-style-type: none"> <li>• AliyunCSFullAccess</li> <li>• AliyunCSReadOnlyAccess</li> </ul>	<a href="#">#unique_31</a>
Container Registry	√	√	×	×	Resource	<ul style="list-style-type: none"> <li>• AliyunContainerRegistryFullAccess</li> <li>• AliyunContainerRegistryReadOnlyAccess</li> </ul>	<a href="#">Repository access control</a>

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"> <li>AliyunROSFullAccess</li> <li>AliyunROSReadOnlyAccess</li> </ul>	<a href="#">#unique_32</a>
Batch Compute	√	√	√	√	Service	N/A	N/A
Function Compute	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunFCFullAccess</li> <li>AliyunFCInvocationAccess</li> <li>AliyunFCReadOnlyAccess</li> </ul>	<a href="#">Sub-account user guide</a>
E-HPC	√	√	√	√	Service	<ul style="list-style-type: none"> <li>AliyunEHPCFullAccess</li> <li>AliyunEHPCReadOnlyAccess</li> </ul>	N/A
Simple Application Server	√	○	×	○	Service	AliyunSWASFullAccess	N/A
Elastic Container Instance	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunECIFullAccess</li> <li>AliyunECIRReadOnlyAccess</li> </ul>	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"> <li>AliyunRDSFullAccess</li> <li>AliyunRDSReadOnlyAccess</li> </ul>	<a href="#">#unique_33</a>
ApsaraDB for MongoDB	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunMongoDBFullAccess</li> <li>AliyunMongoDBReadOnlyAccess</li> </ul>	N/A
ApsaraDB for Redis	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunKvstoreFullAccess</li> <li>AliyunKvstoreReadOnlyAccess</li> </ul>	<a href="#">#unique_34</a>
ApsaraDB for Memcache	√	√	√	√	Service	<ul style="list-style-type: none"> <li>AliyunOCSFullAccess</li> <li>AliyunOCSReadOnlyAccess</li> </ul>	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"> <li>AliyunGPDBFullAccess</li> <li>AliyunGPDBReadOnlyAccess</li> </ul>	<a href="#">#unique_35</a>
Data Transmission Service	√	√	×	×	Service	<ul style="list-style-type: none"> <li>AliyunDTSFullAccess</li> <li>AliyunDTSReadOnlyAccess</li> </ul>	<a href="#">Access DTS with a sub-account</a>
Database Backup	√	√	√	√	Service	<ul style="list-style-type: none"> <li>AliyunDBSFullAccess</li> <li>AliyunDBSReadOnlyAccess</li> </ul>	N/A
Distributed Relational Database Service	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunDRDSReadOnlyAccess</li> <li>AliyunDRDSFullAccess</li> </ul>	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"> <li>AliyunOSSFullAccess</li> <li>AliyunOSSReadOnlyAccess</li> </ul>	<a href="#">RAM policy</a>
Network Attached Storage	√	○	×	○	Operation	<ul style="list-style-type: none"> <li>AliyunNASFullAccess</li> <li>AliyunNASReadOnlyAccess</li> </ul>	<a href="#">#unique_36</a>
Table Store	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunOTSFullAccess</li> <li>AliyunOTSReadOnlyAccess</li> <li>AliyunOTSWriteOnlyAccess</li> </ul>	<a href="#">#unique_37</a>
Alibaba Cloud CDN	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunCDNFullAccess</li> <li>AliyunCDNReadOnlyAccess</li> </ul>	<a href="#">#unique_38</a>
Dynamic Route for CDN	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunDCDNFullAccess</li> <li>AliyunDCDNReadOnlyAccess</li> </ul>	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"> <li>AliyunHBRFullAccess</li> <li>AliyunHBRReadOnlyAccess</li> </ul>	N/A
Lightning Cube	√	○	×	○	Service	AliyunMGWFullAccess	

## 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"> <li>AliyunVPCFullAccess</li> <li>AliyunVPCReadOnlyAccess</li> </ul>	<a href="#">#unique_39</a>
Server Load Balancer	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunSLBReadOnlyAccess</li> <li>AliyunSLBFullAccess</li> </ul>	<a href="#">#unique_40</a>

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"> <li>AliyunEIPFullAccess</li> <li>AliyunEIPReadOnlyAccess</li> </ul>	<a href="#">#unique_39</a>
Express Connect	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunExpressConnectFullAccess</li> <li>AliyunExpressConnectReadOnlyAccess</li> </ul>	<a href="#">#unique_39</a>
NAT Gateway	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunNATGatewayReadOnlyAccess</li> <li>AliyunNATGatewayFullAccess</li> </ul>	<a href="#">#unique_39</a>
VPN Gateway	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunVPNGatewayFullAccess</li> <li>AliyunVPNGatewayReadOnlyAccess</li> </ul>	<a href="#">#unique_39</a>
Global Acceleration	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunGlobalAccelerationReadOnlyAccess</li> <li>AliyunGlobalAccelerationFullAccess</li> </ul>	<a href="#">#unique_39</a>

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	<a href="#">#unique_41</a>
Cloud Enterprise Network	√	√	×	×	Resource	<ul style="list-style-type: none"> <li>• AliyunCENReadOnlyAccess</li> <li>• AliyunCENFullAccess</li> </ul>	<a href="#">#unique_42</a>

## 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"> <li>• AliyunEMRFullAccess</li> <li>• AliyunEMRDevelopAccess</li> <li>• AliyunEMRFlowAdmin</li> </ul>	N/A
Data Lake Analytics	√	√	×	×	Operation	<ul style="list-style-type: none"> <li>• AliyunDLAFullAccess</li> <li>• AliyunDLAReadOnlyAccess</li> </ul>	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"> <li>AliyunMNSFullAccess</li> <li>AliyunMNSReadOnlyAccess</li> </ul>	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"> <li>AliyunCloudMonitorFullAccess</li> <li>AliyunCloudMonitorReadOnlyAccess</li> </ul>	<a href="#">#unique_43</a>
ActionTrail	√	√	√	√	Resource	N/A	<a href="#">#unique_44</a>

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"> <li>AliyunRAMFullAccess</li> <li>AliyunRAMReadOnlyAccess</li> </ul>	<a href="#">RAM authentication</a>
Key Management Service	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunKMSFullAccess</li> <li>AliyunKMSReadOnlyAccess</li> <li>AliyunKMSEncryptAccess</li> </ul>	<a href="#">#unique_45</a>
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"> <li>AliyunLogFullAccess</li> <li>AliyunLogReadOnlyAccess</li> </ul>	<a href="#">#unique_46</a>

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"> <li>AliyunDirectMailFullAccess</li> <li>AliyunDirectMailReadOnlyAccess</li> </ul>	N/A
API Gateway	√	√	√	√	Service	<ul style="list-style-type: none"> <li>AliyunApiGatewayFullAccess</li> <li>AliyunApiGatewayReadOnlyAccess</li> </ul>	<a href="#">API Gateway - RAM</a>
IoT Platform	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunIoTFullAccess</li> <li>AliyunIOTReadOnlyAccess</li> </ul>	<a href="#">Use RAM users</a>
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	AliyunEDAFullAccess	<a href="#">Sub-accounts</a>
Distributed Relational Database Service	√	√	×	√	Resource	<ul style="list-style-type: none"> <li>AliyunDRDSFullAccess</li> <li>AliyunDRDSReadOnlyAccess</li> </ul>	N/A
Application Real-Time Monitoring Service	√	√	×	×	Service	AliyunARMSFullAccess	N/A
Application Configuration Management	√	√	√	√	Resource	AliyunACMFullAccess	<a href="#">Unique_47</a>



## 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"> <li>AliyunMQFullAccess</li> <li>AliyunMQReadOnlyAccess</li> <li>AliyunMQSubOnlyAccess</li> </ul>	RAM sub-account authorization Grant permission to sub-accounts
Message Service	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunMNSFullAccess</li> <li>AliyunMNSReadOnlyAccess</li> </ul>	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"> <li>AliyunMTSPFullAccess</li> <li>AliyunMTSPLayerAuth</li> </ul>	#unique_48
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	<a href="#">#unique_49</a>
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	<a href="#">RAM user operations</a>
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"> <li>AliyunElasticsearchReadOnlyAccess</li> <li>AliyunElasticsearchFullAccess</li> </ul>	<a href="#">#unique_50</a>
Machine Translation	N/A	N/A	N/A	N/A	Service	N/A	N/A
Image Search	√	√	√	√	Resource	<ul style="list-style-type: none"> <li>AliyunImageSearchReadOnlyAccess</li> <li>AliyunImageSearchFullAccess</li> </ul>	<a href="#">Authorization policies</a>

## 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"> <li>AliyunYundunSASFullAccess</li> <li>AliyunYundunSASReadOnlyAccess</li> </ul>	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"> <li>AliyunYundunAegisFullAccess</li> <li>AliyunYundunAegisReadOnlyAccess</li> </ul>	N/A
Anti-DDoS Basic	√	○	√	○	Service	<ul style="list-style-type: none"> <li>AliyunYundunDDoSFullAccess</li> <li>AliyunYundunDDoSReadOnlyAccess</li> </ul>	N/A
Anti-DDoS Pro	√	○	√	○	Service	<ul style="list-style-type: none"> <li>AliyunYundunDDoSFullAccess</li> <li>AliyunYundunDDoSReadOnlyAccess</li> </ul>	N/A
Anti-DDoS Premium	√	○	√	○	Service	<ul style="list-style-type: none"> <li>AliyunYundunAntiDDoSPremiumFullAccess</li> <li>AliyunYundunAntiDDoSPremiumReadOnlyAccess</li> </ul>	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"> <li>AliyunYundunWAFFullAccess</li> <li>AliyunYundunWAFReadOnlyAccess</li> </ul>	N/A
Alibaba Cloud SSL Certificates Service	√	○	√	○	Service	<ul style="list-style-type: none"> <li>AliyunYundunCertFullAccess</li> <li>AliyunYundunCertReadOnlyAccess</li> </ul>	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"> <li>AliyunYundunAntibotFullAccess</li> <li>AliyunYundunAntibotReadOnlyAccess</li> </ul>	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"> <li>AliyunDNSFullAccess</li> <li>AliyunDNSReadOnlyAccess</li> </ul>	N/A
Domain	√	√	√	√	Resource	AliyunDomainFullAccess	<a href="#">#unique_51</a>
Web Hosting	×	×	×	×	N/A	N/A	N/A
Alibaba Mail	×	×	×	×	N/A	N/A	N/A

## Membership Service

Service	Supports RAM console access?	Supports RAM API access?	Supports STS console access?	Supports STS API access?	Authorization granularity (minimum)	System policy	Reference
ICP Filing	√	○	√	○	Service	-	-

## 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"> <li>AliyunBSSFullAccess</li> <li>AliyunBSSReadOnlyAccess</li> <li>AliyunBSSOrderAccess</li> </ul>	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?	Authoriza- tion granularit y (minimum )	System policy	Reference
Message Center	√	○	×	○	Service	AliyunNoti- ficationsF ullAccess	N/A