ALIBABA CLOUD

Alibaba Cloud

Resource Access Management
Product Introduction

Document Version: 20201117

Alibaba Cloud

Legal disclaimer

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

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice 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.
Warning	A warning notice 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 restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.What is RAM?

Resource Access Management (RAM) is a service provided by Alibaba Cloud. It allows you 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, you can authorize different identities to access different Alibaba Cloud resources. RAM has the following features:

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

Scenarios

Scenario	Description
Use RAM to manage user permissions and resources	An enterprise wants to migrate a project to Alibaba Cloud. The enterprise has purchased several types of Alibaba Cloud resources, such as Elastic Compute Service (ECS) instances, ApsaraDB for RDS instances, Server Load Balancer (SLB) instances, and Object Storage Service (OSS) buckets. Specific employees are required to manage these cloud resources. Different employees require different permissions to fulfill their duties.
Use an STS token for authorizing a mobile app to access Alibaba Cloud resources	An enterprise has developed a mobile app and purchased the OSS service. The mobile app runs on mobile devices. These mobile devices are not controlled by the enterprise. The enterprise must grant the necessary permissions to the mobile app. The mobile app can then upload data to and download data from OSS.
Use a RAM role to grant permissions across Alibaba Cloud accounts	An enterprise (Enterprise A) has purchased multiple types of Alibaba Cloud resource, such as ECS instances, RDS instances, SLB instances, and OSS buckets. Enterprise A wants to authorize another enterprise (Enterprise B) to access specified resources of Enterprise A.

Scenario	Description
Use RAM for authorizing applications to access Alibaba Cloud resources	An enterprise has purchased ECS instances and wants to deploy its applications on these ECS instances. These applications need to use AccessKey pairs to call API operations of other Alibaba Cloud services.

Benefits

RAM allows you to create and manage RAM users for employees, systems, applications, and other identities. You can manage the permissions of RAM users to access Alibaba Cloud resources. RAM allows you to keep your Alibaba Cloud account and password strictly confidential in the scenario where multiple users in your enterprise need to collaboratively manage cloud resources. It also allows you to grant the users the minimum required permissions to ensure high security.

Learning path

You can use the RAM learning path to learn more 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 describes the terms that are used in Resource Access Management (RAM).

Terms for identity management

Term	Description
Alibaba Cloud account	Before you use Alibaba Cloud services, you must create an Alibaba Cloud account. The Alibaba Cloud account is the owner of Alibaba Cloud resources. The Alibaba Cloud account is charged for all of the resources that it owns. The Alibaba Cloud account has full control over the resources. By default, only the Alibaba Cloud account can access Alibaba Cloud resources. Other users can access resources only after being explicitly authorized by the Alibaba Cloud account. The Alibaba Cloud account is the administrator or root user of an operating system.
identity	RAM provides three types of identity: RAM user, RAM user group, and RAM role. RAM users and RAM user groups are physical identities. RAM roles are virtual identities.
default domain name	A unique identifier of an Alibaba Cloud account. Alibaba Cloud assigns a **default domain name** to each Alibaba Cloud account. The format of the default domain name is `<AccountAlias>.onaliyun.com`. This unique identifier can be used for RAM user logon and single sign-on (SSO). For more information, see Manage the default domain name.
account alias or enterprise alias	A unique identifier of an Alibaba Cloud account. When a RAM user logs on to the Alibaba Cloud console, the suffix of the logon name can be the account alias, default domain name, or domain alias. Each Alibaba Cloud account can have an account alias. The account alias is used for RAM user logon and can be displayed after successful logon. For example, an enterprise can set the account alias of its Alibaba Cloud account to company1. The RAM user named alice that belongs to this Alibaba Cloud account can log on to the Alibaba Cloud console by using alice@company1. After a successful logon, the display name of the RAM user is alice@company1.
domain alias	A custom domain name that can be used to replace the default domain name. The custom domain name must be publicly resolvable. A domain alias is the alias of the default domain name. **Note** A domain alias can be used only after domain ownership verification. After verification, you can use the domain alias to replace the default domain name in all scenarios where the default domain name is required. For more information, see Create and verify a domain alias.

Term	Description
RAM user	A physical identity that has a fixed ID and credential information. A RAM user represents a person or an application. • An Alibaba Cloud account can create multiple RAM users. RAM users can be used to represent employees, systems, and applications within an enterprise. • RAM users do not own resources. Fees that are incurred by RAM users are billed to their parent Alibaba Cloud accounts. RAM users do not receive individual bills and cannot make payments. • RAM users are visible only to their parent Alibaba Cloud account. • Before RAM users can log on to the Alibaba Cloud console or call API operations, they must be authorized by Alibaba Cloud accounts. After authorization, RAM users can use resources that are owned by the Alibaba Cloud accounts. For more information, see Create a RAM user.
password	An identity credential that is used to log on to the Alibaba Cloud console. **Note** We recommend that you change your password on a regular basis and keep your password confidential. For more information, see Change the password for an Alibaba Cloud account and Change the password for a RAM user.

Term	Description
AccessKey pair	An identity credential that consists of an AccessKey ID and AccessKey secret. You can use your AccessKey pair or Alibaba Cloud SDK to sign API requests that you send to Alibaba Cloud. The AccessKey ID and AccessKey secret are used for symmetric encryption and identity verification. After the identity is verified, you can manage Alibaba Cloud resources by calling API operations. The AccessKey ID is used to identify a user, and the AccessKey secret is used to encrypt and verify a signature string. **Note** An AccessKey secret is displayed only when you create the AccessKey pair, and is not queryable. We recommend that you save the AccessKey secret for subsequent use. For more information, see Create an AccessKey pair for a RAM user.
multi-factor authentication (MFA)	A simple best practice that adds an extra layer of protection in addition to your username and password. Multi-factor authentication enhances security for your account. If MFA is enabled for a user, the user must enter the following information when the user logs on to the Alibaba Cloud console: 1. Username and password 2. Verification code provided by the MFA device For more information, see Enable an MFA device for an Alibaba Cloud account and Enable an MFA device for a RAM user.
RAM user group	A physical identity that contains a group of RAM users. You can create RAM user groups to classify and authorize RAM users. This simplifies the management of personnel and permissions. • If the responsibilities of a RAM user change, you only need to move the RAM user to a RAM user group with the required permissions. This does not affect other RAM users. For more information, see Create a RAM user group. • If the responsibilities of a RAM user group change, you only need to modify the policy that is attached to the group. Changes to the policy apply to all RAM users in the RAM user group. For more information, see Grant permissions to a RAM user group.

Term	Description
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 logon passwords or AccessKey pairs. • Textbook roles (or traditionally defined roles) indicate a set of permissions, which are similar to policies in RAM. If a user assumes a textbook role, the user can obtain a set of permissions and access the authorized resources. • RAM roles are identities to which permission policies are attached. However, RAM roles do not have logon passwords or AccessKey pairs. After an entity user assumes a RAM role, the entity user can obtain and use an STS token to access the authorized resources. RAM roles are divided into the following types based on the entrusted entity: • **Alibaba Cloud account**: RAM users of a trusted Alibaba Cloud account can assume this type of RAM role. RAM users who assume this type of RAM role can belong to their parent Alibaba Cloud accounts or other Alibaba Cloud accounts. This type of RAM role is used for cross-account access and temporary authorization. • **Alibaba Cloud service**: Alibaba Cloud services can assume this type of RAM role. This type of RAM role is used to authorize Alibaba Cloud services to manage your resources. • **IdP**: Users of a trusted IdP can assume this type of RAM role. The RAM roles of this type are used to implement single sign-on (SSO) between Alibaba Cloud and a trusted IdP. For more information, see Create a RAM role for a trusted Alibaba Cloud account, Create a RAM role for a trusted IdP, and Create a RAM role for a trusted Alibaba Cloud service.
single sign-on (SSO)	Alibaba Cloud supports SAML 2.0-based SSO (also known as identity federation). You can implement SSO between Alibaba Cloud and your identity providers (IdPs), such as Microsoft Active Directory Federation Service (AD FS), based on SAML 2.0. Alibaba Cloud provides the following two SAML 2.0-based SSO methods: • User-based SSO: The RAM user identity that you can use to log on to the Alibaba Cloud console is determined based on an SAML assertion. After you log on to the Alibaba Cloud console, you can access Alibaba Cloud resources as a RAM user. For more information, see Overview of user-based SSO. • Role-based SSO: The RAM role that you can use to log on to the Alibaba Cloud console is determined based on an SAML assertion. After you log on to the Alibaba Cloud console, you can use the RAM role that is specified in the SAML assertion to access Alibaba Cloud resources. For more information, see Overview of role-based SSO.
metadata file	The metadata file that is provided by your IdP. The metadata file is in the XML format in most cases. The metadata file contains the logon URLs, the public key that is used to verify SAML assertions, and the assertion format.

Term	Description
identity provider (IdP)	A RAM entity that provides identity management services. IdPs are classified into the following types: • IdPs that use the on-premises architecture, such as Microsoft Active Directory Federation Service (AD FS) and Shibboleth • IdPs that use the cloud-based architecture, such as Azure AD, Google G Suite, Okta, and OneLogin
service provider (SP)	An application that uses the identity management feature of an IdP to provide users with specific services. An SP uses the user information that is provided by an IdP. In some identity systems (such as OpenID Connect) that do not comply with the SAML protocol, SP is known as the relying party of an IdP.
Security Assertion Markup Language 2.0 (SAML 2.0)	A protocol that is designed for enterprise-level user identity authentication. SAML 2.0 is used for communication between an SP and an IdP. SAML 2.0 is a standard that enterprises use to implement enterprise-level SSO.
SAML assertion	A core element that is defined in the SAML protocol. This element describes the authentication request and response. For example, the SAML assertion for an authentication response can contain user attributes.
trust	A mutual trust relationship between an SP and an IdP. In most cases, the trust relationship is established by using public and private keys. An SP can obtain the SAML metadata of a trusted IdP. The metadata includes a public key. The SP uses the public key to verify the integrity of the SAML assertion that is issued by the IdP.

Terms for access control

Term	Description

Term	Description
permission	Indicates whether a user is allowed to perform specific operations on a specific Alibaba Cloud resource. Permissions include Allow and Deny. Operations include the following two types: • Resource management operations: the lifecycle management and O&M of Alibaba Cloud resources. These operations are performed by the Alibaba Cloud account that purchases the resources or by O&M staff in an organization. For example, an authorized user can create, stop, or restart ECS instances, or create, modify, or delete OSS buckets. • Resource using operations: using the core features of Alibaba Cloud resources. These operations are performed by R&D staff or applications in an organization. For example, an authorized user can perform operations in the operating system of an ECS instance, or upload or download data in an OSS bucket. Note ◦ For elastic computing and database products, the permissions on resource management operations can be managed by using RAM. However, the permissions on resource using operations are managed in product instances. For example, the permissions on the operating systems are managed in ECS instances and the permissions on MySQL databases are managed in ApsaraDB for RDS instances. ◦ For storage products, such as OSS and Tablestore, both resource management operations and resource using operations can be managed by using RAM.
policy	A set of permissions that are described based on the policy structure and syntax. You can use policies to describe the authorized resource sets, authorized operation sets, and authorization conditions. For more information, see Policy structure and syntax. In RAM, a policy is a resource entity that can be created, updated, deleted, and viewed. RAM supports the following two types of policy: • **System policy**: System policies are created and updated by Alibaba Cloud and cannot be modified by users. • **Custom policy**: Custom policies are created, modified, and deleted by users to meet their business requirements. You can attach one or more policies to RAM users, RAM user groups, and RAM roles. For more information, see Grant permissions to a RAM user, Grant permissions to a RAM user group, and Grant permissions to a RAM role.
principal	The subject to which a specific permission is granted. The authorized principal can be a RAM user, RAM user group, or RAM role.
effect	The authorization effect. It is a basic element of a policy. Valid values are Allow and Deny.

Term	Description
action	The operations to be performed on a specific Alibaba Cloud resource. The action is a basic element of a policy. Valid values are the names of API operations from Alibaba Cloud services.
condition	The condition for the authorization to take effect. The condition is a basic element of a policy.
resource	A manageable object that is provided by an Alibaba Cloud service. For example, resources can be OSS buckets and ECS instances.

3.Limits

This topic lists the limits of Resource Access Management (RAM).

Category	Item	Upper limit
RAM user	The number of RAM users that can be created for an Alibaba Cloud account	1,000
	The number of characters that the name of a RAM user can contain	64
	The number of groups that a RAM user can join	5
	The number of AccessKey pairs that a RAM user can create	2
	The number of multi-factor authentication (MFA) devices that can be enabled for a RAM user	1
	The number of system policies that can be attached to a RAM user	20
	The number of custom policies that can be attached to a RAM user	10
RAM user group	The number of RAM user groups that can be created for an Alibaba Cloud account	50
	The number of characters that the name of a RAM user group can contain	64
	The number of system policies that can be attached to a RAM user group	20
	The number of custom policies that can be attached to a RAM user group	5
	The number of RAM roles that can be created for an Alibaba Cloud account	1,000

Category	Item	Upper limit
RAM role	The number of characters that the name of a RAM role can contain	64
	The number of system policies that can be attached to a RAM role	20
	The number of custom policies that can be attached to a RAM role	5
Alibaba Cloud account alias	The number of characters that an account alias can contain	64 **Note** An account alias must be 3 to 64 characters in length.
Policy	The number of characters that the name of a policy can contain	128
MFA	The number of MFA devices that can be created for an Alibaba Cloud account	1,000
Custom policy	The number of custom policies that can be created for an Alibaba Cloud account	1,500
	The number of characters that a custom policy can contain	2,048
	The number of versions that a custom policy can have	5
Identity provider (IdP)	The number of IdPs that can be created for an Alibaba Cloud account	100
	The number of IdP descriptors that an IdP metadata file can contain	1
	The number of certificates that an IdP descriptor in an IdP metadata file can contain	2

4.Alibaba Cloud services that support RAM

This topic describes the Alibaba Cloud services that support Resource Access Management (RAM) and the authorization granularity and system policies for each service. It also provides the links to related topics.

RAM-supported Alibaba Cloud services

The following Alibaba Cloud services support RAM: Elastic computing, Databases, Storage and CDN, Networking, Analytics, Cloud communication,Monitoring and management, Application, IoT, Message queuing, Middleware,Media services, Big data, Security, Marketplace, Domain and hosting, Membership services, Billing management, Ticket services, and Messaging.

For more information about the Alibaba Cloud services that support Security Token Service (STS), see Alibaba Cloud services that support STS.

Each table contains the following columns:

- Service: the name of the service that supports RAM.
- Console: indicates whether RAM can be used to implement access control in the console of the service. A check sign (√) indicates that RAM is supported. A cross sign (×) indicates that RAM is not supported. A circle (○) indicates that no console is supported for the service.
- API: indicates whether RAM can be used to implement access control based on the API of the service. A check sign (√) indicates that RAM is supported. A cross sign (×) indicates that RAM is not supported. A circle (○) indicates that no API is provided for the service.
- Authorization granularity: the minimum authorization granularity of the service. A hyphen (-) indicates that no authorization granularities are defined.

  The following authorization granularities are defined:

  - Service: You can control whether RAM users can access the service. You can grant RAM users the permissions to access all or none of the resources in the service.
  - Operation: You can control whether RAM users can perform specific operations on a type of resource in the service.
  - Resource: You can control whether RAM users can perform a specific operation on a specific resource in the service. For example, you can authorize a RAM user to restart a specific Elastic Compute Service (ECS) instance.
- System policy: the system policies that RAM provides for the service. A hyphen (-) indicates that no system policies are provided for the service.
- Reference: the topics that are related to both RAM and the service. A hyphen (-) indicates that no topics are related to RAM or the service.

Elastic computing

Service	Console	API	Authorization granularity	System policy	Reference

Service	Console	API	Authorization granularity	System policy	Reference
ECS	√	√	Resource	• AliyunECSFullAccess • AliyunECSReadOnlyAccess • AliyunECSNetworkInterfaceManagementAccess	Authentication rules
Auto Scaling	√	√	Service	• AliyunESSFullAccess • AliyunESSReadOnlyAccess	API usage instructions
Container Service for Kubernetes	√	√	Resource	• AliyunCSFullAccess • AliyunCSReadOnlyAccess	Use RAM users
Container Registry	√	√	Resource	• AliyunContainerRegistryFullAccess • AliyunContainerRegistryReadOnlyAccess	Repository access control
Resource Orchestration Service	√	√	Service	• AliyunROSFullAccess • AliyunROSReadOnlyAccess	Use RAM to control resource access
BatchCompute	√	√	Service	-	-
Function Compute	√	√	Resource	• AliyunFCFullAccess • AliyunFCInvocationAccess • AliyunFCReadOnlyAccess	Quick start for using the console as RAM users
Elastic High Performance Computing	√	√	Service	• AliyunEHPCFullAccess • AliyunEHPCReadOnlyAccess	-
Simple Application Server	√	○	Service	AliyunSWASFullAccess	-
Elastic Container Instance	√	√	Resource	• AliyunECIFullAccess • AliyunECIReadOnlyAccess	Grant permissions to a RAM user
Web App Service	√	√	Operation	• AliyunWebPlusFullAccess • AliyunWebPlusReadOnlyAccess	-

Service	Console	API	Authorization granularity	System policy	Reference
Operation Orchestration Service	√	√	Resource	• AliyunOOSFullAccess • AliyunOOSReadOnlyAccess	RAM authorization rules

Databases

Service	Console	API	Authorization granularity	System policy	Reference
PolarDB	√	√	Operation	• AliyunPolardbReadOnlyAccess • AliyunPolardbFullAccess	Create and authorize a RAM user
ApsaraDB RDS	√	√	Resource	• AliyunRDSFullAccess • AliyunRDSReadOnlyAccess	RAM authorization
ApsaraDB for MongoDB	√	√	Resource	• AliyunMongoDBFullAccess • AliyunMongoDBReadOnlyAccess	-
ApsaraDB for Redis	√	√	Resource	• AliyunKvstoreFullAccess • AliyunKvstoreReadOnlyAccess	RAM authorization
ApsaraDB for Memcache	√	√	Service	• AliyunOCSFullAccess • AliyunOCSReadOnlyAccess	-
ApsaraDB for HBase	√	√	Resource	• AliyunHBaseFullAccess • AliyunHBaseReadOnlyAccess	Use RAM users to manage ApsaraDB for HBase clusters
Time Series Database	√	√	Operation	-	-
AnalyticDB for PostgreSQL	√	√	Resource	• AliyunGPDBFullAccess • AliyunGPDBReadOnlyAccess	Authentication rules for APIs
AnalyticDB for MySQL	√	√	Resource	• AliyunADBFullAccess • AliyunADBReadOnlyAccess	RAM users and permissions
Data Transmission Service	√	√	Operation	• AliyunDTSFullAccess • AliyunDTSReadOnlyAccess	

Service	Console	API	Authorization granularity	System policy	Reference
Database Backup	√	√	Service	• AliyunDBSFullAccess • AliyunDBSReadOnlyAccess	-
Database Autonomy Service	√	○	Service	• AliyunHDMReadOnlyAccess • AliyunHDMFullAccess	How do I use a RAM user to access DAS?
PolarDB-X	√	√	Resource	• AliyunDRDSReadOnlyAccess • AliyunDRDSFullAccess	Support for RAM authorization
Advanced Database & Application Migration	√	○	Service	• AliyunADAMReadOnlyAccess • AliyunADAMFullAccess	Authorize a RAM user to log on to the ADAM console
Database Gateway	√	√	Resource	• AliyunDGFullAccess • AliyunDGReadOnlyAccess	-
LedgerDB	√	√	Resource	• AliyunLedgerDBFullAccess • AliyunLedgerDBReadOnlyAccess	RAM user authorization

Storage and CDN

Service	Console	API	Authorization granularity	System policy	Reference
Object Storage Service	√	√	Resource	• AliyunOSSFullAccess • AliyunOSSReadOnlyAccess	Implement access control based on RAM policies
Apsara File Storage NAS	√	○	Operation	• AliyunNASFullAccess • AliyunNASReadOnlyAccess	Manage permission groups
Tablestore	√	√	Resource	• AliyunOTSFullAccess • AliyunOTSReadOnlyAccess • AliyunOTSWriteOnlyAccess	Custom permissions
Cloud Storage Gateway	√	○	Service	AliyunHCSSGWFullAccess	-

Service	Console	API	Authorization granularity	System policy	Reference
Hybrid Backup Recovery	√	○	Resource	• AliyunHBRFullAccess • AliyunHBRReadOnlyAccess	-
Lightning Cube	√	○	Service	AliyunMGWFullAccess	-
Dynamic Route for CDN	√	√	Resource	• AliyunDCDNFullAccess • AliyunDCDNReadOnlyAccess	-
CDN	√	√	Resource	• AliyunCDNFullAccess • AliyunCDNReadOnlyAccess	RAM authentication

Networking

Service	Console	API	Authorization granularity	System policy	Reference
Virtual Private Cloud	√	√	Resource	• AliyunVPCFullAccess • AliyunVPCReadOnlyAccess	RAM authorization
Server Load Balancer	√	√	Resource	• AliyunSLBReadOnlyAccess • AliyunSLBFullAccess	RAM authorization
Elastic IP Address	√	√	Resource	• AliyunEIPFullAccess • AliyunEIPReadOnlyAccess	RAM authorization
Express Connect	√	√	Resource	• AliyunExpressConnectFullAccess • AliyunExpressConnectReadOnlyAccess	RAM authorization
NAT Gateway	√	√	Resource	• AliyunNATGatewayReadOnlyAccess • AliyunNATGatewayFullAccess	RAM authorization
VPN Gateway	√	√	Resource	• AliyunVPNGatewayFullAccess • AliyunVPNGatewayReadOnlyAccess	RAM authorization

Service	Console	API	Authorization granularity	System policy	Reference
EIP Bandwidth Plan	√	√	Resource	• AliyunCommonBandwidthPackageReadOnlyAccess • AliyunCommonBandwidthPackageFullAccess	-
Global Accelerator	√	√	Resource	• AliyunGlobalAccelerationReadOnlyAccess • AliyunGlobalAccelerationFullAccess	RAM authorization
Smart Access Gateway	√	√	Resource	-	RAM authorization
Cloud Enterprise Network	√	√	Resource	• AliyunCENReadOnlyAccess • AliyunCENFullAccess	RAM authorization

Analytics

Service	Console	API	Authorization granularity	System policy	Reference
E-MapReduce	√	√	Service	• AliyunEMRFullAccess • AliyunEMRDevelopAccess • AliyunEMRFlowAdmin	-
Data Lake Analytics	√	√	Operation	• AliyunDLAFullAccess • AliyunDLAReadOnlyAccess	-

Cloud communication

Service	Console	API	Authorization granularity	System policy	Reference
Short Message Service	√	√	Service	-	-

Monitoring and management

Service	Console	API	Authorization granularity	System policy	Reference
Cloud Monitor	√	√	Operation	• AliyunCloudMonitorFullAccess • AliyunCloudMonitorReadOnlyAccess	RAM for Cloud Monitor
ActionTrail	√	√	Resource	-	RAM authorization
Resource Access Management	√	√	Resource	• AliyunRAMFullAccess • AliyunRAMReadOnlyAccess	RAM authorization
Key Management Service	√	√	Resource	• AliyunKMSFullAccess • AliyunKMSReadOnlyAccess • AliyunKMSCryptoAccess	Use RAM to control access to resources
Intelligent Advisor	×	×	Operation	-	-
Resource Management	√	○	Resource	• AliyunResourceDirectoryFullAccess • AliyunResourceDirectoryReadOnlyAccess	RAM authorization
Cloud Config	√	○	Service	• AliyunConfigFullAccess • AliyunConfigReadOnlyAccess	Permission verification

Application

Service	Console	API	Authorization granularity	System policy	Reference
Log Service	√	√	Resource	• AliyunLogFullAccess • AliyunLogReadOnlyAccess	RAM authorization rules
Direct Mail	√	√	Service	• AliyunDirectMailFullAccess • AliyunDirectMailReadOnlyAccess	-
API Gateway	√	√	Service	• AliyunApiGatewayFullAccess • AliyunApiGatewayReadOnlyAccess	Use RAM to manage user permissions for API Gateway

Service	Console	API	Authorization granularity	System policy	Reference
Blockchain as a Service	√	√	Resource	-	Hyperledger Fabric RAM authentication
Mini Program Cloud	√	√	Operation	• AliyunMPCAFullAccess • AliyunMPCAReadOnlyAccess	-

IoT

Service	Console	API	Authorization granularity	System policy	Reference
IoT Platform	√	√	Resource	• AliyunIOTFullAccess • AliyunIOTReadOnlyAccess	Use RAM users
IoT Edge	√	√	Resource	• AliyunIOTFullAccess • AliyunIOTReadOnlyAccess	Access resources of other Alibaba Cloud services

Message queuing

Service	Console	API	Authorization granularity	System policy	Reference
Message Queue for Apache RocketMQ	√	√	Resource	• AliyunMQFullAccess • AliyunMQPubOnlyAccess • AliyunMQSubOnlyAccess	Grant permissions to RAM users
Message Service	√	√	Resource	• AliyunMNSFullAccess • AliyunMNSReadOnlyAccess	-

Middleware

Service	Console	API	Authorization granularity	System policy	Reference
Enterprise Distributed Application Service	√	√	Service	AliyunEDASFullAccess	RAM users

Service	Console	API	Authorization granularity	System policy	Reference
Application Real-Time Monitoring Service	√	√	Service	AliyunARMSFullAccess	Grant different permissions to RAM users
Application Configuration Management	√	√	Resource	AliyunACMFullAccess	Access control
Global Transaction Service	√	○	Service	• AliyunGTSFullAccess • AliyunGTSReadOnlyAccess	-

Media services

Service	Console	API	Authorization granularity	System policy	Reference
ApsaraVideo for Media Processing	√	√	Service	• AliyunMTSFullAccess • AliyunMTSPlayerAuth	Quick start for using the console as RAM users
ApsaraVideo for VOD	√	√	Service	• AliyunVODFullAccess • AliyunVODReadOnlyAccess • AliyunVODPlayAuth • AliyunVODUploadAuth	-
ApsaraVideo for Live	√	√	Resource	AliyunLiveFullAccess	API authentication rules
Real-Time Communication	√	√	Resource	-	-
Cloud Video Conferencing	√	○	Resource	• AliyunCVCFullAccess • AliyunCVCReadOnlyAccess	-

Big data

Service	Console	API	Authorization granularity	System policy	Reference

Service	Console	API	Authorization granularity	System policy	Reference
DataWorks	√	√	Service	AliyunDataWorksFullAccess	Use a RAM user
Quick BI	√	√	Service	-	-
Machine Learning Platform for AI	√	√	Service	-	-
Public Recognition	√	√	Service	-	-
DataV	√	√	Service	-	-
MaxCompute	√	√	Service	-	-
Elasticsearch	√	√	Resource	• AliyunElasticsearchReadOnlyAccess • AliyunElasticsearchFullAccess	Resource types
Machine Translation	×	×	Service	-	-
Image Search	√	√	Resource	• AliyunImagesearchReadOnlyAccess • AliyunImagesearchFullAccess	Grant permissions to RAM users

Security

Service	Console	API	Authorization granularity	System policy	Reference
Security Center	√	○	Service	• AliyunYundunSASFullAccess • AliyunYundunSASReadOnlyAccess	-
Server Guard	√	○	Service	• AliyunYundunAegisFullAccess • AliyunYundunAegisReadOnlyAccess	-
Anti-DDoS Basic	√	○	Service	• AliyunYundunDDosFullAccess • AliyunYundunDDosReadOnlyAccess	-

Service	Console	API	Authorization granularity	System policy	Reference
Anti-DDoS Premium and Anti-DDoS Pro	√	○	Service	• AliyunYundunHighFullAccess • AliyunYundunHighReadOnlyAccess	-
Anti-DDoS Premium	√	○	Service	• AliyunYundunAntiDDoSPremiumFullAccess • AliyunYundunAntiDDoSPremiumReadOnlyAccess	-
GameShield	√	○	Service	AliyunYundunGameShieldReadOnlyAccess	-
Web Application Firewall	√	○	Service	• AliyunYundunWAFFullAccess • AliyunYundunWAFReadOnlyAccess	-
SSL Certificates Service	√	○	Service	• AliyunYundunCertFullAccess • AliyunYundunCertReadOnlyAccess	-
Cloud Security Scanner	√	○	Service	AliyunYundunAvdsFullAccess	-
Content Moderation	√	○	Service	AliyunYundunGreenWebFullAccess	-
Anti-Bot Service	√	○	Service	• AliyunYundunAntibotFullAccess • AliyunYundunAntibotReadOnlyAccess	-
ID Verification for Financial Services	√	○	Service	• AliyunAntCloudAuthFullAccess • AliyunAntCloudAuthReadOnlyAccess	-

Marketplace

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

Domain and hosting

Service	Console	API	Authorization granularity	System policy	Reference
Alibaba Cloud DNS	√	○	Resource	• AliyunDNSFullAccess • AliyunDNSReadOnlyAccess	-
Domains	√	√	Resource	AliyunDomainFullAccess	Authorization rules for the Domains API
Cloud Web Hosting	×	×	-	-	-
Alibaba Mail	×	×	-	-	-

Membership services

Service	Console	API	Authorization granularity	System policy	Documentation
ICP Filing	√	○	Service	AliyunBeianFullAccess	-

Billing management

Service	Console	API	Authorization granularity	System policy	Reference
Billing Management	√	×	Service	• AliyunBSSFullAccess • AliyunBSSReadOnlyAccess • AliyunBSSOrderAccess • AliyunBSSRefundAccess	-

Ticket services

Service	Console	API	Authorization granularity	System policy	Reference
Ticket Management	√	○	Service	AliyunSupportFullAccess	-

Messaging

Service	Console	API	Authorization granularity	System policy	Reference
Message Center	√	○	Service	AliyunNotificationsFullAccess	-

5.Alibaba Cloud services that support STS

This topic lists the Alibaba Cloud services that support Security Token Service (STS).

For information about STS and its application scenarios, see What is STS? and RAM role overview.

STS-supported Alibaba Cloud services

The following Alibaba Cloud products support STS:Elastic computing, Database, Storage and CDN, Networking, Analytics, Cloud communications, Management and monitoring, Application, IoT, Middleware, Message queuing,Media services, Big data, Security, Marketplace, Domain and hosting,Membership services,Billing management, Ticket services, andMessaging.

Each table contains the following columns:

- Service: the name of the service that supports STS.
- Console: indicates whether STS can be used to implement access control in the console of the service. A check sign (√) indicates that STS is supported. A cross sign (×) indicates that STS is not supported.
- API: indicates whether STS can be used to implement access control based on the API of the service. A check sign (√) indicates that STS is supported. A cross sign (×) indicates that STS is not supported. A circle (○) indicates that no API is provided for the service.

Elastic computing

Service	Console	API
Elastic Compute Service	√	√
Auto Scaling	√	√
Container Service for Kubernetes	√	√
Container Registry	√	√
Resource Orchestration Service	√	√
BatchCompute	√	√
Function Compute	√	√
Elastic High Performance Computing	√	√
Simple Application Server	×	○
Elastic Container Instance	√	√
Web App Service	√	√
Operation Orchestration Service	√	√

Database

Service	Console	API
ApsaraDB for RDS	√	√
ApsaraDB for MongoDB	√	√
ApsaraDB for Redis	√	√
ApsaraDB for Memcache	√	√
Time Series and Spatial-Temporal Database	√	√
AnalyticDB for PostgreSQL	√	√
Data Transmission Service	√	√
Database Backup	√	√
Distributed Relational Database Service	√	√
Database Gateway	√	√
LedgerDB	√	√

Storage and CDN

Service	Console	API
Object Storage Service	√	√
Apsara File Storage NAS	√	○
Tablestore	√	√
CDN	√	√
Dynamic Route for CDN	√	√
Cloud Storage Gateway	√	○
Hybrid Backup Recovery	√	○
Lightning Cube	×	○

Networking

Service	Console	API
Virtual Private Cloud	√	√

Service	Console	API
Server Load Balancer	√	√
Elastic IP Address	√	√
Express Connect	√	√
NAT Gateway	√	√
VPN Gateway	√	√
Global Accelerator	√	√
Smart Access Gateway	√	√
Cloud Enterprise Network	√	√

Analytics

Service	Console	API
E-MapReduce	√	√
Data Lake Analytics	×	×

Cloud communications

Service	Console	API
Short Message Service	√	√

Management and monitoring

Service	Console	API
Cloud Monitor	√	√
ActionTrail	√	√
Resource Access Management	√	√
Key Management Service	√	√
Intelligent Advisor	×	×
Cloud Config	√	○

Application

Service	Console	API
Log Service	√	√
Direct Mail	√	√
API Gateway	√	√
Blockchain as a Service	√	√

IoT

Service	Console	API
IoT Platform	√	√
IoT Edge	×	×

Middleware

Service	Console	API
Enterprise Distributed Application Service	×	√
Application Real-Time Monitoring Service	×	×
Application Configuration Management	√	√

Message queuing

Service	Console	API
Message Queue for Apache RocketMQ	√	√
Message Service	√	√
EventBridge	√	√

Media services

Service	Console	API
ApsaraVideo Media Processing	√	√
ApsaraVideo VOD	√	√
ApsaraVideo Live	√	√

Service	Console	API
Real-Time Communication	×	×

Big data

Service	Console	API
DataWorks	×	×
Quick BI	×	×
Machine Learning	×	×
Public Recognition	×	×
DataV	×	×
MaxCompute	×	×
Elasticsearch	√	√
Machine Translation	×	×
Image Search	√	√

Security

Service	Console	API
Security Center	√	○
Server Guard	√	○
Anti-DDoS Basic	√	○
Anti-DDoS Premium and Anti-DDoS Pro	√	○
Anti-DDoS Premium	√	○
GameShield	√	○
Web Application Firewall	√	○
SSL Certificates Service	√	○
Cloud Security Scanner	√	○
Content Moderation	√	○
Anti-Bot Service	√	○

Marketplace

Service	Console	API
Alibaba Cloud Marketplace	√	○

Domain and hosting

Service	Console	API
Alibaba Cloud DNS	√	○
Domains	√	√
Cloud Web Hosting	×	×
Alibaba Mail	×	×

Membership services

Service	Console	API
ICP Filing	√	○

Billing management

Service	Console	API
Billing Management	√	×

Ticket services

Service	Console	API
Ticket Management	√	○

Messaging

Service	Console	API
Message Center	√	○