

Alibaba Cloud

Resource Access Management RAM Role Management

Document Version: 20220425

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 <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.RAM role overview	05
2.Service-linked roles	08
3.Create a RAM role	15
3.1. Create a RAM role for a trusted Alibaba Cloud account	15
3.2. Create a RAM role for a trusted Alibaba Cloud service	16
3.3. Create a RAM role for a trusted IdP	17
4.View the basic information about a RAM role	20
5.Grant permissions to a RAM role	21
6.Revoke permissions from a RAM role	23
7.Edit the trust policy of a RAM role	24
8.Specify the maximum session duration for a RAM role	27
9.Assume a RAM role	28
10.Delete a RAM role	31

1.RAM role overview

A RAM role is a virtual Resource Access Management (RAM) identity that you can create within your Alibaba Cloud account. A RAM role does not have a specific logon password or AccessKey pair. A RAM role can be used only after the RAM role is assumed by a trusted entity.

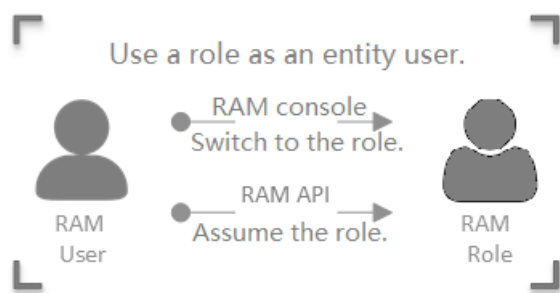
Terms

Term	Description
RAM role	<p>A virtual identity that you can create within your Alibaba Cloud account. RAM roles, entity users, and textbook roles have the following differences. Entity users include Alibaba Cloud accounts, RAM users, or Alibaba Cloud services.</p> <ul style="list-style-type: none">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 resources on which the user has permissions.RAM roles are identities to which policies are attached. However, RAM roles do not have logon passwords or AccessKey pairs. If an entity user assumes a RAM role, the entity user can obtain and use the Security Token Service (STS) token of the role to access the authorized resources.
role ARN	<p>The Alibaba Cloud Resource Name (ARN) of a RAM role is the globally unique resource identifier of the RAM role. ARNs follow the ARN naming conventions that are provided by Alibaba Cloud. For example, the ARN of the devops RAM role that belongs to an Alibaba Cloud account is <code>acs:ram::123456789012****:role/samplerole</code>. After you create a RAM role, you can click the role name and find its ARN in the Basic Information section.</p>
trusted entity	<p>A trusted entity indicates an entity user who can assume a role. When you create a role, you must specify a trusted entity. A RAM role can be assumed only by a trusted entity. A trusted entity can be an Alibaba Cloud account, Alibaba Cloud service, or identity provider (IdP).</p>
policy	<p>One or more policies can be attached to a RAM role. RAM roles without policies can exist, but cannot access Alibaba Cloud resources.</p>
role assuming	<p>Role assuming is the method that is used by entity users to obtain Security Token Service (STS) tokens of RAM roles. An entity user can call the AssumeRole STS API operation to obtain the STS token of a RAM role. Then, the entity user can use the STS token to call API operations of Alibaba Cloud services.</p>
identity switching	<p>Identity switching is the method by which entity users can switch from the logon identity to the role identity in the RAM console. After an entity user logs on to the RAM console, the entity user can switch to a RAM role that the entity user can assume. Then, the entity user can use the RAM role to manage Alibaba Cloud resources. If the entity user no longer needs to use the role identity, the RAM user can switch back to the logon identity.</p>

Term	Description
role token	A role token is a temporary AccessKey pair for a RAM role. A RAM role does not have a specific logon password or AccessKey pair. If an entity user wants to use a RAM role, the entity user must assume the RAM role to obtain a role token. Then, the entity user can use the role token to call API operations of Alibaba Cloud services.

Access Alibaba Cloud resources by using a RAM role

1. The Alibaba Cloud account specifies a trusted entity that can assume the RAM role.
2. The trusted entity logs on to the RAM console or calls an API operation to assume the RAM role, and obtains a role token.



- The trusted entity can switch the identity in the RAM console to assume the RAM role. For more information, see [Assume a RAM role](#).
- The trusted entity can also call the AssumeRole operation to assume the RAM role.

Note An entity user can obtain a role token by assuming a RAM role and then use the role token to access Alibaba Cloud resources.

3. The Alibaba Cloud account attaches a policy to the RAM role. For more information, see [Grant permissions to a RAM role](#).

Note Each RAM role can be attached one or more policies. RAM roles without policies can exist, but cannot access Alibaba Cloud resources.

4. The trusted entity assumes the RAM role and uses the role token to access Alibaba Cloud resources.

RAM role types

RAM roles are classified into three types based on trusted entities.

Role type	Scenario	References
-----------	----------	------------

Role type	Scenario	References
Alibaba Cloud account	RAM users within an 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.	<ul style="list-style-type: none">• Create a RAM role for a trusted Alibaba Cloud account• Use an STS token for authorizing a mobile app to access Alibaba Cloud resources• Use a RAM role to grant permissions across Alibaba Cloud accounts
Alibaba Cloud service	Alibaba Cloud services can assume this type of RAM role. This type of RAM role is used to authorize the access across Alibaba Cloud services.	<ul style="list-style-type: none">• Create a RAM role for a trusted Alibaba Cloud service• Service-linked roles
IdP	Users of a trusted IdP can assume this type of RAM role. This type of RAM role is used to implement single sign-on (SSO) between Alibaba Cloud and a trusted IdP.	<ul style="list-style-type: none">• Create a RAM role for a trusted IdP• Implement role-based SSO from AD FS• Implement role-based SSO from Okta• Implement role-based SSO from Azure AD• Implement role-based SSO from OneLogin to Alibaba Cloud• Implement OIDC-based SSO from Okta

2. Service-linked roles

A trusted Alibaba Cloud service can assume a Resource Access Management (RAM) role to access other Alibaba Cloud services. RAM roles that a trusted Alibaba Cloud service can assume are classified into two types: normal service role and service-linked role. This topic describes service-linked roles.

Background information

An Alibaba Cloud service may need to access other services to implement a feature. In this case, the Alibaba Cloud service must be authorized to access other services. For example, to retrieve resource lists and log data from Elastic Compute Service (ECS) and ApsaraDB RDS, Cloud Config requires the access permissions on ECS and ApsaraDB RDS. Alibaba Cloud provides service-linked roles to simplify the process to authorize a service to access other services.

A service-linked role is a RAM role that only the linked service can assume. In most cases, a service automatically creates or deletes the service-linked role if needed. A service-linked role simplifies the process to authorize a service to access other services and reduces the risks caused by misoperations.

The policy that is attached to a service-linked role is predefined by the linked service. You cannot modify or delete the policy. You cannot attach policies to or detach policies from a service-linked role.

If a service does not support service-linked roles, you can use a normal service role to authorize the service.

Create a service-linked role

Some Alibaba Cloud services automatically create service-linked roles when you perform operations. For example, when you create a cloud resource or enable a feature, a service-linked role may be automatically created. You can view the created service-linked roles on the Roles page of the RAM console. You can also retrieve the list of created service-linked roles by using the API or a CLI to call the ListRoles operation.

You can also manually create service-linked roles. For more information, see [Create a service-linked role](#).

Note

- The number of service-linked roles that you can create is based on the limit of the number of RAM roles that you can create within your Alibaba Cloud account. If the limit is exceeded, you can still create service-linked roles. However, you can no longer create other types of RAM roles.
- For more information about how an Alibaba Cloud service creates a service-linked role, see the documentation of the service.


Delete a service-linked role

Some Alibaba Cloud services automatically delete service-linked roles when you perform operations. For example, when you delete a cloud resource or disable a feature, a service-linked role may be automatically deleted. You can also manually delete service-linked roles in the RAM console. For more information, see [Delete a RAM role](#).

If you attempt to delete a service-linked role, RAM checks whether the role is being assumed by the linked service.


- If the role is not being assumed, the role can be deleted.

- If the role is being assumed, the role cannot be deleted. However, you can view the cloud resources of the linked service that assume the service-linked role. If you no longer need the cloud resources of the linked service, find and remove the resources of the linked service. Then, delete the service-linked role.

 **Note** For more information about the conditions that allow you to delete a service-linked role, see the documentation of the linked service.

Permissions required to create and delete a service-linked role

RAM identities must be granted the required permissions before the RAM identities can create or delete a service-linked role. The permissions are also required when service-linked roles are automatically created.

 **Note** The permissions to create a service-linked role are included in the administrative policy of the linked service. For ECS, the administrative policy is AliyunESSFullAccess. If you attach the administrative policy of a service to a RAM identity, the RAM identity can create the service-linked role for the service.

The following sample policy allows authorized RAM identities to create and delete the service-linked role for Resource Management:

```
{
  "Action": [
    "ram:CreateServiceLinkedRole",
    "ram>DeleteServiceLinkedRole"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Condition": {
    "StringEquals": {
      "ram:ServiceName": "resourcemanager.aliyuncs.com"
    }
  }
}
```

Assume a service-linked role

A service-linked role can be assumed only by the linked service. The role cannot be assumed by identities such as RAM users or other RAM roles.

You can view the service that can assume a service-linked role in the `Service` parameter on the **Trust Policy Management** tab of the role details page.

Alibaba Cloud services that support service-linked roles

Alibaba Cloud service	Service name	Service-linked role	References
Resource Management	resourcemanager.aliyuncs.com	AliyunServiceRoleForResourceDirectory	Service-linked role for Resource Directory

Alibaba Cloud service	Service name	Service-linked role	References
Cloud Config	config.aliyuncs.com	AliyunServiceRoleForConfig	Manage the service-linked role for Cloud Config
	remediation.config.aliyuncs.com	AliyunServiceRoleForConfigRemediation	
PolarDB	polardb.aliyuncs.com	AliyunServiceRoleForPolarDB	RAM role linked to Apsara PolarDB
Hybrid Backup Recovery (HBR)	dr.hbr.aliyuncs.com	AliyunServiceRoleForHbrDr	Service linked role for ECS disaster recovery
	ecsbackup.hbr.aliyuncs.com	AliyunServiceRoleForHbrEcsBackup	Service-linked roles for HBR
	ossbackup.hbr.aliyuncs.com	AliyunServiceRoleForHbrOssBackup	
	nasbackup.hbr.aliyuncs.com	AliyunServiceRoleForHbrNasBackup	
	csgbackup.hbr.aliyuncs.com	AliyunServiceRoleForHbrCsgBackup	
	vaultencryption.hbr.aliyuncs.com	AliyunServiceRoleForHbrVaultEncryption	
	otsbackup.hbr.aliyuncs.com	AliyunServiceRoleForHbrOtsBackup	
Operation Orchestration Service (OOS)	bandwidthscheduler.oos.aliyuncs.com	AliyunServiceRoleForOOSBandwidthScheduler	OOS linked roles
	instancescheduler.oos.aliyuncs.com	AliyunServiceRoleForOOSInstanceScheduler	
	executiondelivery.oos.aliyuncs.com	AliyunServiceRoleForOOSExecutionDelivery	
Auto Scaling (ESS)	ess.aliyuncs.com	AliyunServiceRoleForAutoScaling	Grant permissions to Auto Scaling
Time Series Database (TSDB)	hitsdb.aliyuncs.com	AliyunServiceRoleForTSDB	None
CloudMonitor	cloudmonitor.aliyuncs.com	AliyunServiceRoleForCloudMonitor	Manage the service-linked role for CloudMonitor
Blockchain as a Service (BaaS)	baas.aliyuncs.com	AliyunServiceRoleForBaaS	None

Alibaba Cloud service	Service name	Service-linked role	References
Global Traffic Manager (GTM)	gtm.aliyuncs.com	AliyunServiceRoleForGTM	Service-linked role for Global Traffic Manager
Alibaba Cloud DNS (DNS)	alidns.aliyuncs.com	AliyunServiceRoleForDNS	None
Data Security Center (DSC)	sddp.aliyuncs.com	AliyunServiceRoleForSDDP	Authorize DSC to access Alibaba Cloud resources
CDN	cdn-ddos.cdn.aliyuncs.com	AliyunServiceRoleForCDNAccessingDDoS	Integrate Alibaba Cloud CDN with Anti-DDoS
	cdn-waf.cdn.aliyuncs.com	AliyunServiceRoleForCDNAccessingWAF	None
	logdelivery.cdn.aliyuncs.com	AliyunServiceRoleForCDNLogDelivery	Manage the SLR for log storage
Application Real-Time Monitoring Service (ARMS)	arms.aliyuncs.com	AliyunServiceRoleForARMS	Service-linked role for ARMS
	security.arms.aliyuncs.com	AliyunServiceRoleForARMSecurity	Service-linked role for application security
EventBridge	sendevent-fc.eventbridge.aliyuncs.com	AliyunServiceRoleForEventBridgeSendToFC	Service-linked roles for EventBridge
	sendevent-mns.eventbridge.aliyuncs.com	AliyunServiceRoleForEventBridgeSendToMNS	
	sendevent-sms.eventbridge.aliyuncs.com	AliyunServiceRoleForEventBridgeSendToSMS	
	sendevent-directmail.eventbridge.aliyuncs.com	AliyunServiceRoleForEventBridgeSendToDirectMail	
	source-rocketmq.eventbridge.aliyuncs.com	AliyunServiceRoleForEventBridgeSourceRocketMQ	
	connect-vpc.eventbridge.aliyuncs.com	AliyunServiceRoleForEventBridgeConnectVPC	
DataWorks	di.dataworks.aliyuncs.com	AliyunServiceRoleForDataWorksDI	Service linked role of DataWorks Data Integration

Alibaba Cloud service	Service name	Service-linked role	References
Elastic High Performance Computing (E-HPC)	ehpc.aliyuncs.com	AliyunServiceRoleForEHP	Service-linked roles for E-HPC
Server Migration Center (SMC)	smc.aliyuncs.com	AliyunServiceRoleForSMC	Service linked roles for SMC
Message Queue for Apache Kafka	connector.alikafka.aliyuncs.com	AliyunServiceRoleForAlikafkaConnector	Service-linked roles for Message Queue for Apache Kafka
	instanceencryption.alikafka.aliyuncs.com	AliyunServiceRoleForAlikafkaInstanceEncryption	
	alikafka.aliyuncs.com	AliyunServiceRoleForAlikafka	
	etl.alikafka.aliyuncs.com	AliyunServiceRoleForAlikafkaETL	
Tracing Analysis	xtrace.aliyuncs.com	AliyunServiceRoleForXtrace	Service linked role for Tracing Analysis
NAT Gateway (NAT)	nat.aliyuncs.com	AliyunServiceRoleForNatgw	Service-linked role for NAT Gateway
Alibaba Cloud DNS PrivateZone	pvtz.aliyuncs.com	AliyunServiceRoleForPvtz	Service-linked role for Alibaba Cloud DNS PrivateZone
ActionTrail	actiontrail.aliyuncs.com	AliyunServiceRoleForActionTrail	Manage the service-linked role
Cloud Storage Gateway (CSG)	hcs-sgw.aliyuncs.com	AliyunServiceRoleForHCS SGW	Service-linked roles for CSG
	logmonitor.hcs-sgw.aliyuncs.com	AliyunServiceRoleForHCS SGWLogMonitor	
Data Lake Analytics (DLA)	openanalytics.aliyuncs.com	AliyunServiceRoleForOpenAnalytics	AliyunServiceRoleForOpenAnalytics
API Gateway	apigateway.aliyuncs.com	AliyunServiceRoleForApiGateway	None
	monitor.apigateway.aliyuncs.com	AliyunServiceRoleForApiGatewayMonitoring	None
Elasticsearch	ops.elasticsearch.aliyuncs.com	AliyunServiceRoleForElasticsearchOps	None
	collector.elasticsearch.aliyuncs.com	AliyunServiceRoleForElasticsearchCollector	

Alibaba Cloud service	Service name	Service-linked role	References
Bastionhost	bastionhost.aliyuncs.com	AliyunServiceRoleForBastionhost	Service-linked role for Bastionhost
Global Accelerator (GA)	vpcendpoint.ga.aliyuncs.com	AliyunServiceRoleForGaVpcEndpoint	AliyunServiceRoleForGaVpcEndpoint
	ddos.ga.aliyuncs.com	AliyunServiceRoleForGaAntiDdos	None
Message Queue for Apache RocketMQ	ons.aliyuncs.com	AliyunServiceRoleForOns	Service-linked role for Message Queue for Apache RocketMQ
AnalyticDB for PostgreSQL	adbpq.aliyuncs.com	AliyunServiceRoleForADBPQ	Service-linked role for AnalyticDB for PostgreSQL
Key Management Service (KMS)	secretsmanager-rds.kms.aliyuncs.com	AliyunServiceRoleForKMSSecretsManagerForRDS	Manage the service-linked role for dynamic ApsaraDB RDS secrets
	keystore.kms.aliyuncs.com	AliyunServiceRoleForKMSKeyStore	Service-linked role for dedicated KMS
ApsaraDB for MongoDB	mongodb.aliyuncs.com	AliyunServiceRoleForMongoDB	ApsaraDB for MongoDB service-linked roles
ApsaraDB RDS	pgsql-onecs.rds.aliyuncs.com	AliyunServiceRoleForRdsPsqlOnEcs	Service-linked role for ApsaraDB RDS
PrivateLink	privatelink.aliyuncs.com	AliyunServiceRoleForPrivateLink	Service-linked role for PrivateLink
AnalyticDB for MySQL	ads.aliyuncs.com	AliyunServiceRoleForAnalyticDBForMySQL	Manage the service-linked role
ApsaraDB for ClickHouse	clickhouse.aliyuncs.com	AliyunServiceRoleForClickHouse	ApsaraDB for ClickHouse service-linked role
Real-Time Communication	rtc.aliyuncs.com	AliyunServiceRoleForRTC	RTC service linked role
Application Load Balancer (ALB)	alb.aliyuncs.com	AliyunServiceRoleForAlb	Service-linked roles for ALB
	logdelivery.alb.aliyuncs.com	AliyunServiceRoleForAlbLogDelivery	
Dynamic Route for CDN (DCDN)	logdelivery.dcdn.aliyuncs.com	AliyunServiceRoleForDCDNLogDelivery	SLR for log delivery
Server Load Balancer (SLB)	logdelivery.slb.aliyuncs.com	AliyunServiceRoleForSlbLogDelivery	Service-linked role for SLB

Alibaba Cloud service	Service name	Service-linked role	References
Cloud Enterprise Network	cen.aliyuncs.com	AliyunServiceRoleForCEN	AliyunServiceRoleForCEN
Elastic Container Instance	eci.aliyuncs.com	AliyunServiceRoleForECI	Elastic Container Instance service-linked role
	vnode.eci.aliyuncs.com	AliyunServiceRoleForECIVnode	Service-linked role for virtual nodes
Database Backup (DBS)	db.aliyuncs.com	AliyunServiceRoleForDBS	How do I activate DBS?
Cloud Governance Center	governance.aliyuncs.com	AliyunServiceRoleForGovernance	Service-linked roles in Cloud Governance Center
CloudSSO	cloudsso.aliyuncs.com	AliyunServiceRoleForCloudSSO	Use the service-linked role for CloudSSO
Resource Sharing	resourcesharing.aliyuncs.com	AliyunServiceRoleForResourceSharing	Service-linked role for Resource Sharing


3. Create a RAM role

3.1. Create a RAM role for a trusted Alibaba Cloud account

This topic describes how to create a Resource Access Management (RAM) role for a trusted Alibaba Cloud account. This type of RAM role is used to implement cross-account access and temporary authorization. The RAM role can be assumed by a RAM user that belongs to your Alibaba Cloud account or to a different Alibaba Cloud account.

Procedure

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Roles**.
3. On the **Roles** page, click **Create Role**.
4. In the **Create Role** panel, select **Alibaba Cloud Account** for the Select Trusted Entity parameter and click **Next**.
5. Configure parameters for the RAM role.
 - i. Specify **RAM Role Name**.
 - ii. (Optional) Specify **Note**.
 - iii. Select **Current Alibaba Cloud Account** or **Other Alibaba Cloud Account**.
 - **Current Alibaba Cloud Account**: If you want a RAM user that belongs to your Alibaba Cloud account to assume the RAM role, select **Current Alibaba Cloud Account**.
 - **Other Alibaba Cloud Account**: If you want a RAM user that belongs to a different Alibaba Cloud account to assume the RAM role, select **Other Alibaba Cloud Account** and enter the ID of the Alibaba Cloud account. This option is provided to authorize different Alibaba Cloud accounts.

 **Note** You can view the ID of an Alibaba Cloud account on the [Security Settings](#) page.

6. Click **OK**.
7. Click **Close**.

What's next

After the RAM role is created, the RAM role has no permissions. You can grant permissions to the RAM role. For more information, see [Grant permissions to a RAM role](#).

Related information

- [CreateRole](#)
- [Use a RAM role to grant permissions across Alibaba Cloud accounts](#)

3.2. Create a RAM role for a trusted Alibaba Cloud service

This topic describes how to create a Resource Access Management (RAM) role for a trusted Alibaba Cloud service. This type of RAM role is used to authorize access across Alibaba Cloud services.


Context

Two types of RAM roles are available for a trusted Alibaba Cloud service:

- **Normal service role:** You must enter a name for the RAM role, select a trusted service, and then attach policies to the RAM role.
- **Service-linked role:** You need only to select a trusted service. The name and policy of the RAM role are predefined by the service. For more information, see [Service-linked roles](#).

Create a normal service role

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Roles**.
3. On the **Roles** page, click **Create Role**.
4. In the **Create Role** panel, select **Alibaba Cloud Service** for the Select Trusted Entity parameter and click **Next**.
5. Select **Normal Service Role** for the Role Type parameter.
6. Specify the **RAM Role Name** and **Note** parameters.
7. Select a trusted service.

 **Note** Available services are provided in the Select Trusted Service drop-down list.

8. Click **OK**.
9. Click **Close**.

After a RAM role is created, the RAM role has no permissions. You can grant permissions to the RAM role. For more information, see [Grant permissions to a RAM role](#).

Create a service-linked role

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Roles**.
3. On the **Roles** page, click **Create Role**.
4. In the **Create Role** panel, select **Alibaba Cloud Service** for the Select Trusted Entity parameter and click **Next**.
5. Select **Service Linked Role** for the Role Type parameter.
6. Select a service.

After you select the service, you can view the name, description, and policy that are predefined for the service-linked role. You can click **View Policy Details** to view the detailed information about the policy.

 **Note** Available services are provided in the Select Service drop-down list.

7. Click **OK**.
8. Click **Close**.

Related information

- [CreateRole](#)
- [CreateServiceLinkedRole](#)

3.3. Create a RAM role for a trusted IdP

This topic describes how to create a Resource Access Management (RAM) role for a trusted identity provider (IdP). This type of RAM role is used to implement single sign-on (SSO) between Alibaba Cloud and a trusted IdP.

Prerequisites


An IdP is created.

- For more information about how to create a SAML IdP, see [Create a SAML IdP](#).
- For more information about how to create an OpenID Connect (OIDC) IdP, see [Create an OIDC IdP](#).

Create a RAM role for a SAML IdP

To implement SAML 2.0-based SSO, you must create a RAM role for a SAML IdP.

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Roles**.
3. On the **Roles** page, click **Create Role**.
4. In the **Create Role** panel, select **IdP** for Select Trusted Entity and click **Next**.
5. Specify the **RAM Role Name** and **Note** parameters.
6. Select **SAML** for IdP Type.
7. Select a trusted IdP, read the conditions, and then click **OK**.

 **Note** Only the `saml:recipient` condition key is supported. This condition key is required and cannot be changed.

8. Click **Close**.

Create a RAM role for an OIDC IdP

To implement OIDC-based SSO, you must create a RAM role for an OIDC IdP.

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Roles**.
3. On the **Roles** page, click **Create Role**.
4. In the **Create Role** panel, select **IdP** for Select Trusted Entity and click **Next**.
5. Specify the **RAM Role Name** and **Note** parameters.

6. Select **OIDC** for IdP Type.
7. Select a trusted IdP, specify the conditions in the Conditions section, and then click **OK**.

The following table describes the supported conditions.

Condition key	Description	Required	Example
oidc:iss	<p>The issuer. You can assume the RAM role only if the iss field of the OIDC token that you want to use to assume the RAM role meets this condition.</p> <p>The conditional operator must be StringEquals. The value must be the URL of the issuer that you specify for the selected OIDC IdP. You can specify this condition to ensure that you can use the OIDC token to assume the RAM role only if the OIDC token is issued by a trusted IdP.</p>	Yes	https://dev-xxxxxx.okta.com
oidc:aud	<p>The audience. You can assume the RAM role only if the aud field of the OIDC token that you want to use to assume the RAM role meets this condition.</p> <p>The conditional operator must be StringEquals. The value can be one or more client IDs that you specify for the selected OIDC IdP. You can specify this condition to ensure that you can use the OIDC token to assume the RAM role only if the OIDC token is generated by using the client ID that you specify.</p>	Yes	00a294vi1vJoClev****
oidc:sub	<p>The subject. You can assume the RAM role only if the sub field of the OIDC token that you want to use to assume the RAM role meets this condition.</p> <p>The conditional operator can be a string of all types. The value can be up to 10 subjects. You can specify this condition to further limit the identity that you can use to assume the RAM role. You can also leave this condition unspecified.</p>	No	00u294e3mzNXt4Hi****

8. Click **Close**.

What's next

After a RAM role is created, the RAM role has no permissions. You can grant permissions to the RAM role. For more information, see [Grant permissions to a RAM role](#).

Related information

- [CreateRole](#)

4. View the basic information about a RAM role

This topic describes how to view the basic information about a Resource Access Management (RAM) role, such as the role name, the date and time when the role was created, and the Alibaba Cloud Resource Name (ARN) of the role.

Procedure


1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Roles**.
3. On the **Roles** page, click the name of a specific RAM role.
4. In the **Basic Information** section of the page that appears, view information such as **Role Name**, **Created**, and **ARN**.

Related information

- [GetRole](#)

5. Grant permissions to a RAM role

You can grant permissions to a Resource Access Management (RAM) role that you created for a trusted Alibaba Cloud account, Alibaba Cloud service, or identity provider (IdP). This topic describes how to grant permissions to a RAM role.

 **Note** You cannot grant permissions to service-linked roles by attaching policies to the roles. This is because the policies that are attached to this type of role are defined by the linked cloud services. For more information, see [Service-linked roles](#).

Limits

You can attach up to 20 system policies and 5 custom policies to a RAM role.

Method 1: Grant permissions to a RAM role by clicking Add Permissions on the Roles page


1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Roles**.
3. On the **Roles** page, find the RAM role to which you want to grant permissions and click **Add Permissions** in the **Actions** column.
4. In the **Add Permissions** panel, grant permissions to the RAM role.
 - i. Select the authorization scope.
 - **Alibaba Cloud Account**: The authorization takes effect on the current Alibaba Cloud account.
 - **Specific Resource Group**: The authorization takes effect in a specific resource group.

 **Note** If you select **Specific Resource Group** for Authorized Scope, make sure that the required cloud service supports resource groups. For more information, see [Alibaba Cloud services that support resource groups](#).

- ii. Specify the principal.

The principal is the RAM role to which permissions are granted. By default, the current RAM role is specified. You can also specify a different RAM role.

- iii. Select policies.


 **Note** You can attach a maximum of five policies to a RAM user at a time. If you want to attach more than five policies to a RAM user, perform the operation multiple times.

5. Click **OK**.
6. Click **Complete**.

Method 2: Grant permissions to a RAM role by clicking Input and Attach on the Roles page

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.

2. In the left-side navigation pane, choose **Identities > Roles**.
3. On the **Roles** page, find the RAM role to which you want to grant permissions and click **Input and Attach** in the **Actions** column.
4. In the **Add Permissions** panel, set **Type** to **System Policy** or **Custom Policy** and enter a policy name.

 **Note** To view a policy name, choose **Permissions > Policies** in the left-side navigation pane.

5. Click **OK**.
6. Click **Close**.


Method 3: Grant permissions to a RAM role on the Grants page

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Grants**.
3. On the **Grants** page, click **Grant Permission**.
4. On the **Grant Permissions** page, grant permissions to the RAM role.
 - i. Select the authorization scope.
 - **Alibaba Cloud Account**: The permissions take effect on the current Alibaba Cloud account.
 - **Specific Resource Group**: The permissions take effect in a specific resource group.

 **Note** If you select **Specific Resource Group** for **Authorized Scope**, make sure that the required cloud service supports resource groups. For more information, see [Alibaba Cloud services that support resource groups](#).

- ii. Specify the principal.

The principal is the RAM role to which permissions are granted.
- iii. Select policies.

 **Note** You can attach a maximum of five policies to a RAM user at a time. If you want to attach more than five policies to a RAM user, perform the operation multiple times.


5. Click **OK**.
6. Click **Complete**.

Related information

- [AttachPolicyToRole](#)

6.Revoke permissions from a RAM role

If a Resource Access Management (RAM) role no longer needs specific permissions, you can revoke the permissions from the RAM role. This topic describes how to revoke the permissions from a RAM role.

 **Note** You cannot revoke permissions from service-linked roles by detaching policies from the roles. This is because the policies that are attached to this type of role are defined by the linked cloud services. For more information, see [Service-linked roles](#).

Method 1: Revoke permissions from a RAM role on the Roles page

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Roles**.
3. On the **Roles** page, click the name of a specific RAM role.
4. On the page that appears, click the **Permissions** tab, find the policies that you want to detach from the RAM role, and then click **Remove Permission** in the **Actions** column.
5. Click **OK**.

Method 2: Revoke permissions from a RAM role on the Grants page

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Grants**.
3. On the **Grants** page, find the RAM role from which you want to revoke permissions and click **Revoke Permission** in the **Actions** column.
4. Click **OK**.

Related information

- [DetachPolicyFromRole](#)

7. Edit the trust policy of a RAM role

You can edit the trust policy that is attached to a Resource Access Management (RAM) role to change the trusted entity of the RAM role. This topic describes how to change the trusted entity of a RAM role to an Alibaba Cloud account, an Alibaba Cloud service, or an identity provider (IdP).

Context

When you create a RAM role, you can specify an Alibaba Cloud account, an Alibaba Cloud service, or an IdP as the trusted entity of the RAM role. In most cases, you do not need to change the trusted entity after you create a RAM role. If you need to change the trusted entity, you can use one of the methods described in this topic. After you change the trusted entity, you must check whether the RAM role functions as expected.

Procedure

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Roles**.
3. On the **Roles** page, find the RAM role whose trusted entity you want to change and click its name.
4. Click the **Trust Policy Management** tab. On this tab, click **Edit Trust Policy**.
5. In the **Edit Trust Policy** panel, modify the content of the trust policy and click **OK**.

Example 1: Change the trusted entity of a RAM role to an Alibaba Cloud account


If the `Principal` element in a policy includes the `RAM` field, the trusted entity is an **Alibaba Cloud account**. A RAM role to which the policy is attached can be assumed by authorized RAM users and RAM roles of the trusted Alibaba Cloud account.

In the following policy, the RAM role can be assumed by all the RAM users and RAM roles of the Alibaba Cloud account whose ID is 123456789012****.

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "RAM": [
          "acs:ram::123456789012****:root"
        ]
      }
    ]
  },
  "Version": "1"
}
```


If you reconfigure the `Principal` element based on the following code, the RAM role can be assumed only by the RAM user named `testuser` of the Alibaba Cloud account whose ID is 123456789012****.


```
"Principal": {
  "RAM": [
    "acs:ram::123456789012****:user/testuser"
  ]
}
```

 **Note** Before you edit the trust policy, make sure that a RAM user named `testuser` is created.

If you reconfigure the `Principal` element based on the following code, the RAM role can be assumed only by the RAM role named `testrole` of the Alibaba Cloud account whose ID is 123456789012****.

```
"Principal": {
  "RAM": [
    "acs:ram::123456789012****:role/testrole"
  ]
}
```

 **Note** Before you edit the trust policy, make sure that a RAM role named `testrole` is created.

Example 2: Change the trusted entity of a RAM role to an Alibaba Cloud service

If the `Principal` element in a policy includes the `Service` field, the trusted entity is an **Alibaba Cloud service**. A RAM role to which the policy is attached can be assumed by a trusted Alibaba Cloud service of the current Alibaba Cloud account.

In the following policy, the RAM role can be assumed by the Elastic Compute Service (ECS) service of the current Alibaba Cloud account.

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ecs.aliyuncs.com"
        ]
      }
    }
  ],
  "Version": "1"
}
```

Example 3: Change the trusted entity of a RAM role to an IdP

If the `Principal` element includes the `Federated` field, the trusted entity is an identity provider (IdP). The RAM role can be assumed by all users in the IdP.

In the following policy, the RAM role can be assumed by all users in the IdP named `testprovider` of the Alibaba Cloud account whose ID is 123456789012****.

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Federated": [
          "acs:ram::123456789012****:saml-provider/testprovider"
        ]
      },
      "Condition": {
        "StringEquals": {
          "saml:recipient": "https://signin.alibabacloud.com/saml-role/sso"
        }
      }
    }
  ],
  "Version": "1"
}
```

Limits

You cannot change the trusted entity of a policy that is attached to a service-linked role because this policy is defined by the linked service. For more information, see [Service-linked roles](#).

8.Specify the maximum session duration for a RAM role

This topic describes how to use the Resource Access Management (RAM) console or API to specify the maximum session duration for a RAM role. If you set the maximum session duration for a RAM role to a large value, RAM users can assume the RAM role to complete time-consuming tasks. If the RAM users call a Security Token Service (STS) operation to assume the RAM role, the STS tokens that are returned have a long validity period.

Context

- Valid values of the maximum session duration for a RAM role: 3600 to 43200. Unit: seconds. Default value of the maximum session duration: 3600. Unit: seconds.
- The maximum session duration is not configurable for service-linked roles.

Use the RAM console to specify the maximum session duration for a RAM role

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Roles**.
3. On the **Roles** page, click the name of a specific RAM role.
4. In the **Basic Information** section, click **Edit** to the right of **Maximum Session Duration**.
5. In the dialog box that appears, change the maximum session duration and click **OK**.

Use the API to specify the maximum session duration for a RAM role

When you call the `CreateRole` or `UpdateRole` operation, you can configure the `MaxSessionDuration` or `NewMaxSessionDuration` parameter to specify the duration. For more information, see [CreateRole](#) and [UpdateRole](#).

What's next

After you specify the maximum session duration for a RAM role, you can log on to the RAM console and switch the logon identity to the RAM role or call an STS operation to assume the RAM role. You can also use the RAM role for role-based single sign-on (SSO). For more information, see the following topics:

- [Assume a RAM role](#)
- [Overview](#)
- [AssumeRole](#)
- [AssumeRoleWithSAML](#)

9. Assume a RAM role

This topic describes how to assume a Resource Access Management (RAM) role whose trusted entity is an Alibaba Cloud account as a RAM user by using the Alibaba Cloud Management Console or the RAM API.

Prerequisites

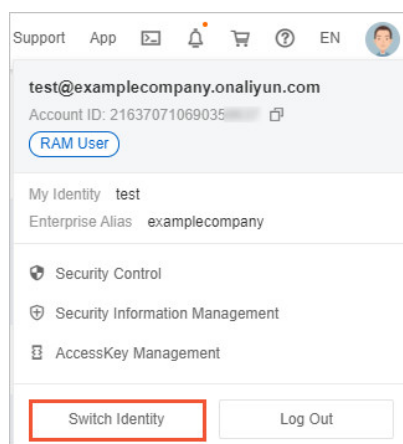
Before you can assume a RAM role, make sure that you have completed the following operations:

1. [Create a RAM user.](#)
2. Create an AccessKey pair or configure a logon password for the RAM user.
 - If you want to assume a RAM role as the RAM user by logging on to the Alibaba Cloud Management Console, configure a logon password for the RAM user. For more information, see [Change the password of a RAM user.](#)
 - If you want to assume a RAM role as the RAM user by using the RAM API, create an AccessKey pair for the RAM user. For more information, see [Create an AccessKey pair for a RAM user.](#)
3. [Grant permissions to a RAM user.](#)
 - To allow the RAM user to assume all RAM roles, attach the system policy `AliyunSTSAssumeRoleAccess` to the RAM user.
 - To allow the RAM user to assume a specific RAM role, attach a custom policy to the RAM user. For more information, see [Can I specify the RAM role that a RAM user can assume?](#)

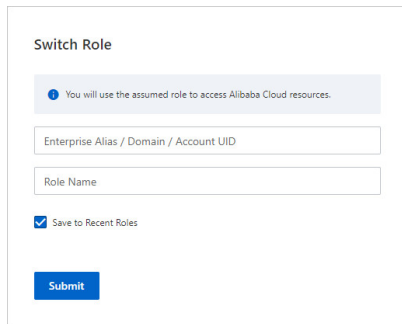
Use the Alibaba Cloud Management Console

After you log on to the Alibaba Cloud Management Console as a RAM user, you can switch your logon identity to a RAM role. You can also log on to the RAM console by using a password or role-based single sign-on (SSO).

1. Log on to the [RAM console](#) as a RAM user.
2. Move the pointer over the profile picture in the upper-right corner of the console and click **Switch Identity**.



3. On the **Switch Role** page, configure the parameters.



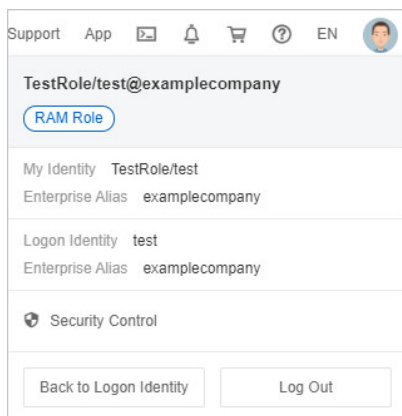
The 'Switch Role' dialog box contains a blue header bar with the title 'Switch Role'. Below it is a light blue box with a blue dot icon and the text 'You will use the assumed role to access Alibaba Cloud resources.' There are two input fields: 'Enterprise Alias / Domain / Account UID' and 'Role Name'. A checkbox labeled 'Save to Recent Roles' is checked. At the bottom is a blue 'Submit' button.

- i. Enter the enterprise alias (account alias), default domain name, or ID of the Alibaba Cloud account to which the RAM role belongs. For more information, see [View and modify the default domain name](#).
- ii. Enter the name of the RAM role. For more information, see [View the basic information about a RAM role](#).

4. Click **Submit**.

After the switch is complete, your login identity changes to the RAM role, and your RAM user has the permissions that are granted to the RAM role.

You can move the pointer over the profile picture in the upper-right corner of the Alibaba Cloud Management Console to view the login identity and current identity.



The dropdown menu shows the user's profile information. At the top is the text 'TestRole/test@examplecompany' with a 'RAM Role' label below it. Below this is a section titled 'My Identity' showing 'TestRole/test' and 'examplecompany'. Another section titled 'Logon Identity' shows 'test' and 'examplecompany'. At the bottom are two buttons: 'Back to Logon Identity' and 'Log Out'.

The following table describes the logon identity and current identity. The My Identity parameter shows the current identity.


Logon type	Logon identity	Current identity
Password-based logon	The format is <Username of the logon RAM user>.	<p>The format is <RoleName>/<RoleSessionName>.</p> <ul style="list-style-type: none">RoleName: the name of the role that is assumed by the RAM userRoleSessionName: the username of the RAM user

Logon type	Logon identity	Current identity
Role-based SSO	<p>After you log on to the RAM console as a RAM role, only the current identity is displayed. The logon identity is not displayed.</p> <p>If you switch the logon identity to a different RAM role, the logon identity is displayed in the format of <code><RoleName>/<RoleSessionName></code>.</p> <ul style="list-style-type: none">◦ RoleName: the name of the role that is used for SSO◦ RoleSessionName: the RoleSessionName attribute in the role-based SSO authentication response <p>For example, if the tom@example.local user of a trusted IdP logs on to the Alibaba Cloud Management Console as the RAM role test-saml-role1 and switches the identity to the RAM role alice-testrole, the logon identity is test-saml-role1/tom@example.local.</p>	<p>The format is <code><RoleName>/<RoleSessionName></code>.</p> <ul style="list-style-type: none">◦ RoleName: the name of the assumed role◦ RoleSessionName: the RoleSessionName attribute in the role-based SSO authentication response <p>For example, if the tom@example.local user of a trusted IdP logs on to the Alibaba Cloud Management Console as the RAM role test-saml-role1, the current identity is test-saml-role1/tom@example.local. If the tom@example.local user switches the identity to the RAM role alice-testrole, the current identity is alice-testrole/tom@example.local. The value of RoleSessionName remains unchanged.</p>

The smaller value between the **Maximum Session Duration** and **Logon Session Valid For** parameters is used as the maximum session duration for a RAM role. For more information, see [Specify the maximum session duration for a RAM role](#) and [Configure security policies for RAM users](#).

Use the RAM API

An authorized RAM user can use an AccessKey pair to call the [AssumeRole](#) operation. This way, the RAM user obtains an STS token and can use the STS token to access Alibaba Cloud resources.

 **Note** If the obtained STS token is disclosed, you can disable all the STS tokens. For more information, see [What do I do if STS tokens are disclosed?](#).

References

For more information about how to log on to the Alibaba Cloud Management Console by using role-based SSO, see [Overview](#).

10.Delete a RAM role

This topic describes how to delete a Resource Access Management (RAM) role that you no longer need.

Prerequisites

No policies are attached to the RAM role. For more information, see [Revoke permissions from a RAM role](#).

Procedure

1. Log on to the [RAM console](#) by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Roles**.
3. On the **Roles** page, find the RAM user that you want to delete and click **Delete** in the **Actions** column.
4. Click **OK**.

Related information

- [DeleteRole](#)
- [DeleteServiceLinkedRole](#)