Alibaba Cloud
Resource Access Management

RAM Role Management

Issue: 20190919

Legal disclaimer

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

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
⛔	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⛔ Danger: Resetting will result in the loss of user configuration data.
⚠	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	⚠ Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
📋	This indicates warning informatio n, supplementary instructions, and other content that the user must understand.	❗ Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	📋 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

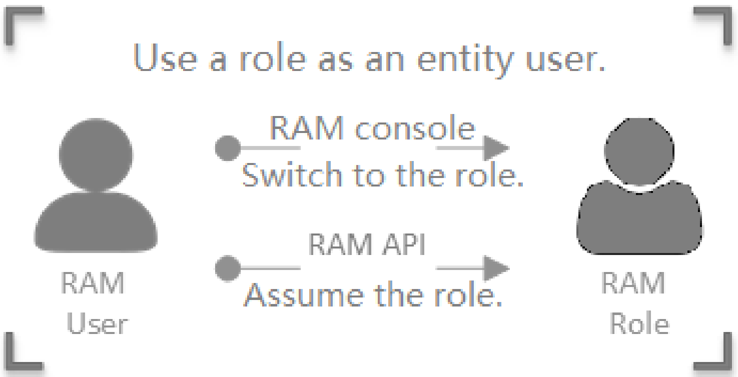
Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

1 Overview of a RAM role

A RAM role is a RAM identity that you can create in your Alibaba Cloud account. A role does not have standard long-term credentials such as a password or an access key. You must first specify a trusted entity that can assume a RAM role before you use the role.

Related concepts



RAM role

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

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

ARN

The Alibaba Cloud Resource Name (ARN) of a RAM role. Each role has a unique ARN. For example, the ARN of the RAM role `devops` under an Alibaba Cloud account is `acs : ram :: 1234567890  12 ****: role / samplerole`. After you create a RAM role, you can click the role name and find its ARN on the Basic Information page.

Trusted entity

The trusted entity that can assume a RAM role. You must specify a trusted entity when you create a RAM role. Only trusted entities can assume RAM roles. The trusted entity can be an Alibaba Cloud account, Alibaba Cloud service, or identity provider (IdP).

Policy

A set of permissions that are described by using policy structure and grammar. Roles that are not attached to any policy can exist, but cannot access resources.

Role assuming

The method for entity users to obtain security tokens of RAM roles.
By calling the `AssumeRole` action of STS, an entity user can obtain the security token of a role and use the token to access Alibaba Cloud service APIs.

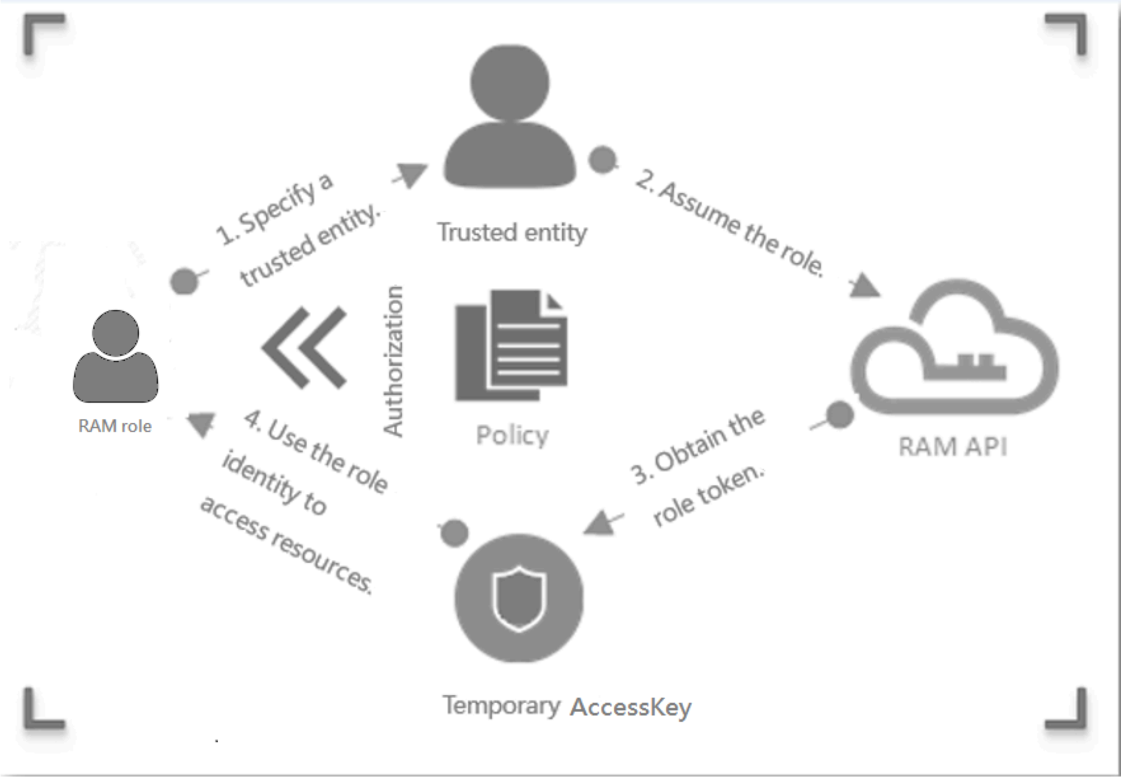
Identity switching

The method by which entity users can switch from the logon identity to role identity in the RAM console. After logging on to the RAM console, an entity user can switch to a RAM role that the user can assume. The user can then use the role identity to operate Alibaba Cloud resources. When the user no longer needs the role identity, the user can switch back to its logon identity.

Role token

A temporary access key to a role identity. RAM roles do not have standard long-term credentials (passwords or access keys). When an entity user wants to use a role, the user must assume the role to obtain the role token. Then, the user can use the role token to call Alibaba Cloud API actions.

Access to Alibaba Cloud resources by using a RAM role


1. Specify a trusted entity.
Trusted entity
2. Assume the role.
RAM role
Authorization
Policy
RAM API
4. Use the role identity to access resources.
3. Obtain the role token.
Temporary AccessKey

1. The Alibaba Cloud account specifies a trusted entity that can assume the RAM role.
2. The trusted entity logs on to the console or calls an API action to assume the role and obtains a role token.
   - The trusted entity can assume the role by switching its identity in the console. For more information, see #unique_4.
   - The trusted entity can assume the role by calling the `AssumeRole` action.

   Note:

   An entity user can obtain a role token by assuming a RAM role and then use the token to access Alibaba Cloud resources.
3. The Alibaba Cloud account attaches a policy to the RAM role. For more information, see #unique_5.

   Note:

   A RAM role can have one or more polices attached. A RAM role without a policy cannot access Alibaba Cloud resources.
4. The trusted entity assumes the RAM role and uses a temporary STS token to access Alibaba Cloud resources.

RAM role types

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

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

Application scenarios

- #unique_6
- #unique_7
- #unique_8

2 Create a RAM role

2.1 Create a RAM role for a trusted Alibaba Cloud account

This topic describes how to create a RAM role for a trusted Alibaba Cloud account. You can create a RAM role for three types of trusted entities: trusted Alibaba Cloud accounts, trusted Alibaba Cloud services, and trusted identity providers (IdPs).

Procedure

1. Log on to the RAM console.
2. In the left-side navigation pane, click RAM Roles.
3. Click Create RAM Role.
4. Select Alibaba Cloud Account and click Next.
5. Enter a RAM role name and description.
6. Select a trusted Alibaba Cloud account and click OK.

> Note:
> If you select Other Alibaba Cloud Account, you must enter the account ID.

What's next

After you create a RAM role, you can click Add Permissions to RAM Role to grant permission to this role. For more information, see #unique_5.

2.2 Create a RAM role for a trusted Alibaba Cloud service

This topic describes how to create a RAM role for a trusted Alibaba Cloud service. You can create a RAM role for three types of trusted entities: trusted Alibaba Cloud accounts, trusted Alibaba Cloud services, and trusted identity providers (IdPs).

Procedure

1. Log on to the RAM console.
2. In the left-side navigation pane, click RAM Roles.
3. Click Create RAM Role.
4. Select Alibaba Cloud Service and click Next.
5. Enter a RAM role name and description.

6. Select a trusted Alibaba Cloud service and click OK.

> Note:
>
> For more information about the trusted services, see the RAM console.

What's next

After you create a RAM role, you can click Add Permissions to RAM Role to grant permission to this role. For more information, see #unique_5.

2.3 Create a RAM role for a trusted IdP

This topic describes how to create a RAM role for a trusted identity provider (IdP). You can create a RAM role for three types of trusted entities: trusted Alibaba Cloud accounts, trusted Alibaba Cloud services, and trusted IdPs.

Procedure

1. Log on to the RAM console.
2. In the left-side navigation pane, click RAM Roles.
3. Click Create RAM Role.
4. Select IdP and click Next.
5. Enter a RAM role name and description.
6. Select a trusted IdP and click OK.

> Note:
>
> In the Condition Keyword column, only the keyword `saml : recipient` (which is required and cannot be modified) is currently allowed.

What's next

After you create a RAM role, you can click Add Permissions to RAM Role to grant permission to this role. For more information, see #unique_5.

3 View basic information about a RAM role

This topic describes how to view basic information about a 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.
2. In the left-side navigation pane, click RAM Roles.
3. In the RAM Role Name column, click the name of the target RAM role.
4. In the Basic Information section, view the role information.

> **Note:**
> The RAM role information can be viewed but cannot not be modified.

4 Grant permission to a RAM role

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

Procedure

1. Log on to the RAM console.
2. Choose Permissions > Grants.
3. Click Grant Permission.
4. In the Principal field, enter the role name and click the target RAM role.

   Note:

   You can also enter keywords to search for a specific RAM role.
5. In the Policy Name column, select the target policy and click OK.

   Note:

   You can click X to revoke your selection.

5 Remove permission from a RAM role

This topic describes how to remove permission from a RAM role when the RAM role no longer needs a permission.

Procedure

1. Log on to the RAM console.
2. Choose Permissions > Grants.
3. In the Principal column, find the target RAM role and click Revoke Permission.
4. Click OK.

6 Edit the policy of a RAM role

This topic describes how to edit the policy of a RAM role to change the trusted entity that assumes the role.

Context

The `Principal` element specifies the trusted entity that assumes the role. You can change a trusted entity by modifying the `Principal` element.

Procedure

1. Log on to the RAM console.
2. In the left-side navigation pane, click RAM Roles.
3. In the RAM Role Name column, click the name of the target RAM role.
4. On the Trust Policy Management tab, click Edit Trust Policy.

   Note:

   For information about how to edit a policy, see #unique_17.
5. Click OK.

7 Change the trusted entity of a RAM role

This topic describes how to change the trusted entity of a RAM role to a specific Alibaba Cloud account, Alibaba Cloud service, or identity provider (IdP). You can change the trusted entity of a RAM role by modifying the policy attached to the RAM role.

Note:

When creating a RAM role, you can specify an Alibaba Cloud account, Alibaba Cloud service, or identity provider (IdP) for the trusted entity of the RAM role. In most cases, you do not need to change the trusted entity after creating a RAM role. If you have to change the trusted entity, you can use either of the following methods. After you change the trusted entity, we recommend that you test whether the RAM role works properly.

Change the trusted entity of a RAM role to a specific Alibaba Cloud account

You can check the trusted entity of a RAM role by viewing the policy. If the `Principal` element contains the `RAM` field, the trusted entity is an Alibaba Cloud account. The role can be assumed by RAM users under the trusted account.

For example, the following policy indicates that the RAM role can be assumed by any RAM user under the Alibaba Cloud account whose ID is 123456789012****.

```
{
    " Statement ": [
        {
            " Action ": " sts : AssumeRole ",
            " Effect ": " Allow ",
            " Principal ": {
                " RAM ": [
                    " acs : ram :: 1234567890  12 ****: root "
                ]
            }
        }
    ],
    " Version ": " 1 "
}
```

If you modify the `Principal` element as follows, the RAM role can be assumed by the RAM user named `testuser` under the Alibaba Cloud account whose ID is 123456789012****.

```
            " Principal ": {
                " RAM ": [
                    " acs : ram :: 1234567890  12 ****: user /
 testuser "
```

Note:
Before modifying the policy, you must ensure that you have created a RAM user named `testuser` whose UPN is testuser@123456789012****.onaliyun.com.

Change the trusted entity of a RAM role to a specific Alibaba Cloud service

If the `Principal` element contains the `Service` field, the trusted entity is an Alibaba Cloud service. The role can be assumed by the trusted Alibaba Cloud service under the current Alibaba Cloud account.

For example, the following policy indicates that the RAM role can be assumed by ECS.

```
{

    " Statement ": [

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

Change the trusted entity of a RAM role to a specific IdP

If the `Principal` element contains the `Federated` field, the trusted entity is an IdP. The RAM role can be assumed by any user in the IdP.

For example, the following policy indicates that the RAM role can be assumed by any user in the IdP named `testprovid  er`. testprovider is the IdP for the current Alibaba Cloud account whose ID is 123456789012****.

```
{
    " Statement ": [

        {
            " Action ": " sts : AssumeRole ",
            " Effect ": " Allow ",
            " Principal ": {
                " Federated ": [
                    " acs : ram :: 1234567890  12 ****: saml -
 provider / testprovid  er "
                ]
            },
            " Condition ":{
                " StringEqua  ls ": {
                    " saml : recipient ":" https :// signin .
 alibabaclo  ud . com / saml - role / sso "
                }
            }
        }
    ],
    " Version ": " 1 "
}
```

8 Assume a RAM role

This topic describes how to assume a RAM role by using a RAM user under a trusted Alibaba Cloud account.

Prerequisites

> Note:
>
> To maintain account security, a trusted Alibaba Cloud account is not allowed to assume RAM roles itself. RAM roles must instead be assumed by RAM users of the Alibaba Cloud account.

1. A RAM user is created. For information about how to create a RAM user, see #unique_20.
2. An access key or a password is set for the RAM user.
   - For information about how to create an access key, see #unique_21.
   - For information about how to set a password, see #unique_22.
3. The system policy `AliyunSTSA ssumeRoleA ccess` is attached to the RAM user. For information about how to grant permission to a RAM role, see #unique_5.

Procedure

1. Log on to the RAM console as a RAM user.
2. Move the pointer over the account icon in the upper-right corner and click Switch Role.
3. On the displayed Switch Role page, enter the enterprise alias or the default domain name in the Enterprise Alias/Default Domain Name filed and the RAM role name in the Role Name field. Then, click Switch.
4. Click Switch Back to Logon User to switch back to your logon identity.

   > Note:
   >
   > After you switch to the logon identity, you will obtain the original permissions and lose the permissions associated with the RAM role.

What's next

A RAM user can also assume a RAM role by calling an API action. After being granted the `AliyunSTSA ssumeRoleA ccess` policy, a RAM user can use its access key to call the #unique_23 action of the Security Token Service (STS) to obtain the temporary security token of a role. Then, the user uses the token to access Alibaba Cloud APIs.

9 Delete a RAM role

This topic describes how to delete a RAM role when you no longer need it.

Prerequisites

Note:

Before you delete a RAM role, make sure that no policy is attached to the role.

Procedure

1. Log on to the RAM console.
2. In the left-side navigation pane, click RAM Roles.
3. In the RAM Role Name column, select the target RAM role and click Delete.
4. Click OK.

10 Best practices

10.1 Use RAM to maintain security of your Alibaba Cloud resources

This topic describes how to use RAM to apply access and security settings to your Alibaba Cloud resources so that you can better manage access permissions with fine-grained access control.

Prerequisites

An Alibaba Cloud account is created. If not, create one before proceeding. To create an Alibaba Cloud account, click Create a new Alibaba Cloud account.

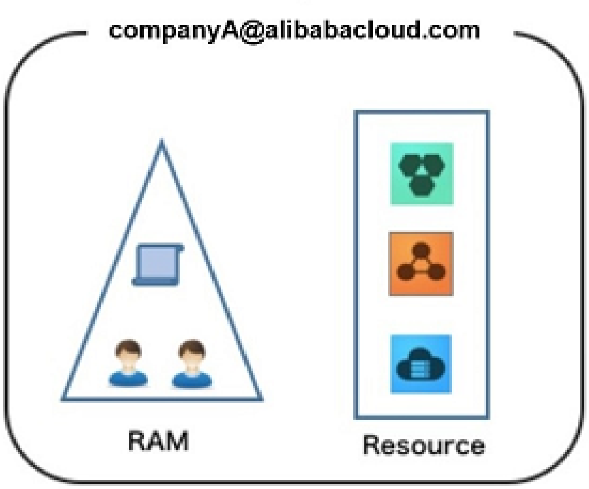
Scenario

When you migrate your business resources to the cloud, the traditional organizati onal structures and previous management methods of your resources may no longer meet your requirements. As a result, the migration of your resources may create higher security management issues as follows:

- The responsibilities of the RAM users are not clear.
- The Alibaba Cloud account owner does not want to share the access key with RAM users due to security risks involved.
- RAM users can access resources by using different methods, which is not unified and may mistakenly cause security risks.
- The resource access permissions of RAM users need to be frequently recalled when the users no longer require these permissions.

Solution

To resolve the preceding issues, you can use RAM to create RAM users and grant resource access permissions to RAM users. Specifically, you can use RAM to separate the access key of your Alibaba Cloud account from RAM users and grant minimum permissions to users as needed to maintain the security of your resources.



Security management solution

- Create independent RAM users.

  An enterprise needs only one Alibaba Cloud account. As a best practice, the Alibaba Cloud account is not used for daily tasks. However, multiple RAM users can be created under the account, and granted the necessary access permissions to resources as needed.

  For more information, see #unique_20.

- Separate console users from API users.

  We recommend that you do not create a logon password for console operations and an access key for API operations for a RAM user at the same time.

  - To allow an application to access cloud resources only through APIs, you only need to create an access key for the application.
  - To allow an employee to operate on cloud resources only through the console, you only need to set a logon password for the employee.

  For more information, see #unique_20.

- Create RAM users and group them.

  If your Alibaba Cloud account has multiple RAM users, you can group RAM users with same responsibilities and grant permissions to the group as needed.

  For more information, see #unique_27.

- Grant the minimum permissions to different RAM user groups.

  You can attach proper system policies to RAM users or user groups as needed. You can also create custom policies for fine-grained permission management. In this way, by granting the minimum permissions to different RAM users and user groups, you can better manage the RAM users' operations on the cloud resources.

For more information, see #unique_28.

- Configure strong password policies.

  You can configure password policies with custom conventions regarding the minimum length, mandatory characters, and validation period, for RAM users in the RAM console. If a RAM user is allowed to change their logon password, the user must create a strong logon password and rotate the password or access key on a regular basis.

  For more information, see #unique_29.

- Enable an MFA device for your Alibaba Cloud account.

  You can enable a multi-factor authentication (MFA) device for your Alibaba Cloud account to enhance the account security. When you log on to Alibaba Cloud with MFA enabled, the system requires the following two security factors:

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

  For more information, see #unique_30.

- Enable SSO for RAM users.

  After Single Sign On (SSO) is enabled, all the internal accounts of your enterprise will be authenticated. Then, users can log on to Alibaba Cloud to access corresponding resources only by using an internal account.

  For more information, see #unique_31.

- Do not share the access key of your Alibaba Cloud account.

  Your Alibaba Cloud account has full control permissions over resources under it, and its access keys have the same permissions as logon passwords. However, access keys are used for programmatic access whereas logon passwords are used to log on to the console. Therefore, to avoid information leaks due to misuse of an access key, we recommend that you do not share or use the access key of your Alibaba Cloud account.

  Instead, create a RAM user and grant this user the relevant permissions.

  For more information, see #unique_21.

- Specify operation conditions to enhance security.

  You can specify the operational conditions that a RAM user must meet before they can use your cloud resources. For example, you can specify that the RAM user must use a secure channel (such as SSL), use a specified source IP address, or operate within a specified period of time.

  For more information, see #unique_32.
- Manage permissions of your cloud resources.

  By default, all your resources are under your Alibaba Cloud account. A RAM user can use the resources but do not own the resources. This allows you to easily manage the instances or data created by RAM users.

  - For an existing RAM user that you no long require, you can remove all of its corresponding permissions by simply removing the RAM user account.
  - For a RAM user that requires a permission, you need to first create the RAM user , set the logon password or access key for it, and then grant the RAM user the relevant permissions as needed.

  For more information, see #unique_33.
- Use STS to grant temporary permissions to RAM users.

  The Security Token Service (STS) is an extended authorization service of RAM. You can use STS to grant temporary permissions to RAM users and specify the permission and automatic expiration time of the tokens as needed.

  For more information, see #unique_34

Result

After migrating your services to the cloud, you can use the preceding solutions to ensure you manage your cloud-based resources effectively and keep your Alibaba Cloud account and all business assets secure.

What to do next

You can use RAM to categorize your O&M requirements and assign tasks to different engineers as needed. For more information, see #unique_35.

11 FAQ

11.1 STS FAQ

Why does an error occur when I use STS?

If the following error message is displayed, it means that the AliyunSTSAssumeRoleAccess policy is not attached to the authorized user:

```
Error   message :  You   are   not   authorized   to   do   this
action .  You   should   be   authorized   by   RAM
```

Attach the AliyunSTSAssumeRoleAccess policy to the authorized user and then continue to use STS.

What permissions does an STS token have?

The permissions of an STS token are the specified role's permissions that are included in the policy set when the AssumeRole API is called.

If you do not set the policy parameter when calling the AssumeRole API, the returned STS token will have all the permissions of the specified role.

What is the validity period of an STS token?

The validity period of an STS token ranges from 900 seconds to 3600 seconds. The default value is 3600 seconds. You can set the DurationSeconds parameter when calling the AssumeRole API to limit the valid period of an STS token.

Is there an upper limit to the number of times that STS API can be called?

STS supports up to 100 Queries Per Second (QPS). If the call requests exceed 100 QPS, an error is reported.

If multiple STS tokens have been obtained at different times, are the old and new tokens valid at the same time?

Both the new and old STS tokens are valid before their expiration time.