Alibaba Cloud
Resource Access Management

Best Practices

Issue: 20190906

Legal disclaimer

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

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

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

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

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `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 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.

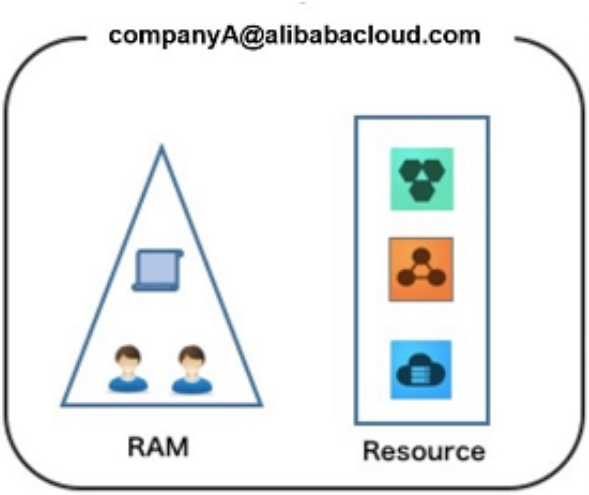
Scenario

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_4.
- 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_4.
- 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_5.
- 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_6.

- 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_7.

- 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_8.

- 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_9.

- 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_10.

- 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_11.

- 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_12.

- 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_13

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_14.

2 Use RAM to limit the IP addresses used to access Alibaba Cloud resources

This topic describes how to use RAM to limit the IP addresses that are used to access Alibaba Cloud resources. This feature of RAM enables a higher level of security.

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.
- The RAM service is activated, and you can log on to the RAM console. If the RAM service is not activated, activate the service before proceeding. For more information, see #unique_16.
- You have a basic knowledge of the policy elements, structure, and syntax before creating a custom policy. For more information, see #unique_11 and #unique_17.

Context

Enterprise A has purchased more than one type of Alibaba Cloud resources, such as ECS instances, RDS instances, SLB instances, and OSS buckets. To ensure business and data security, this enterprise wants to only allow RAM users to access Alibaba Cloud resources from its IP addresses of the corporate intranet.

Solution

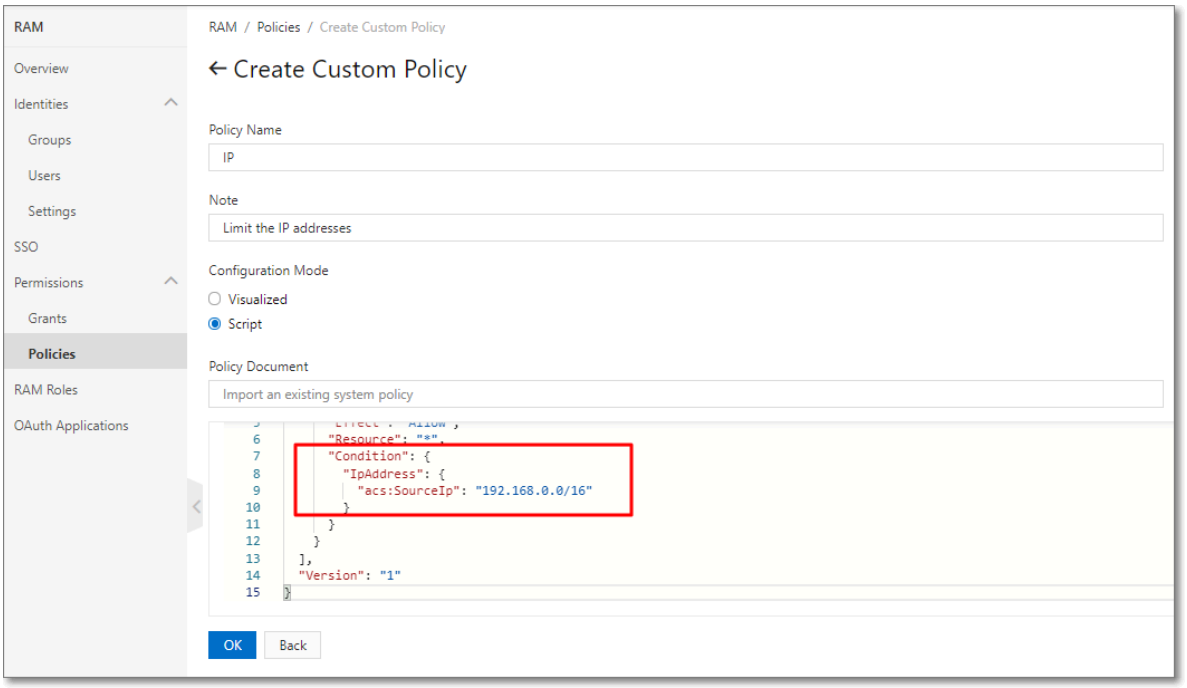
To only allow RAM users to access Alibaba Cloud resources from the specified IP addresses, create and attach a custom policy for the RAM users.

1. #unique_4.
2. Create a custom policy.
3. #unique_12.

Create a custom policy

1. In the left-side navigation pane, click Policies under Permissions.
2. On the Policies page, click Create Policy.
3. On the page that appears, specify the Policy Name and Note parameters.

4. Under Configuration Mode, select Script. Copy and paste the following sample script to the Policy Document area, and edit the script based on your business needs.



If the following policy is attached to a RAM user, the RAM user can only access ECS instances from the IP addresses in the CIDR block range of 192.168.0.0/16. In this case, the `acs : SourceIp` parameter in `Condition` is set to `192 . 168 . 0 . 0 / 16`.

```
{
  " Statement ": [
    {
      " Action ": " ecs :*",
      " Effect ": " Allow ",
      " Resource ": "*",
      " Condition ": {
        " IpAddress ": {
          " acs : SourceIp ": " 192 . 168 . 0 . 0 / 16 "
        }
      }
    }
  ],
  " Version ": " 1 "
}
```

Note:

The `Condition` setting only applies to the actions that are specified for the current policy. You can change the `192 . 168 . 0 . 0 / 16` CIDR block to the IP address of your corporate intranet.

5. Click OK.

3 Use RAM to limit the time of accessing Alibaba Cloud resources

This topic describes how to use RAM to limit the time of accessing Alibaba Cloud resources to enable a higher level of security.

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.
- The RAM service is activated, and you can log on to the RAM console. If the RAM service is not activated, activate the service before proceeding. For more information, see #unique_16.
- You have a basic knowledge of the policy elements, structure, and syntax before creating a custom policy. For more information, see #unique_11 and #unique_17.

Context

Enterprise A has purchased more than one type of Alibaba Cloud resources, such as ECS instances, RDS instances, SLB instances, and OSS buckets. To ensure business and data security, this enterprise wants RAM users to only access Alibaba Cloud resources during the working hours.

Solution

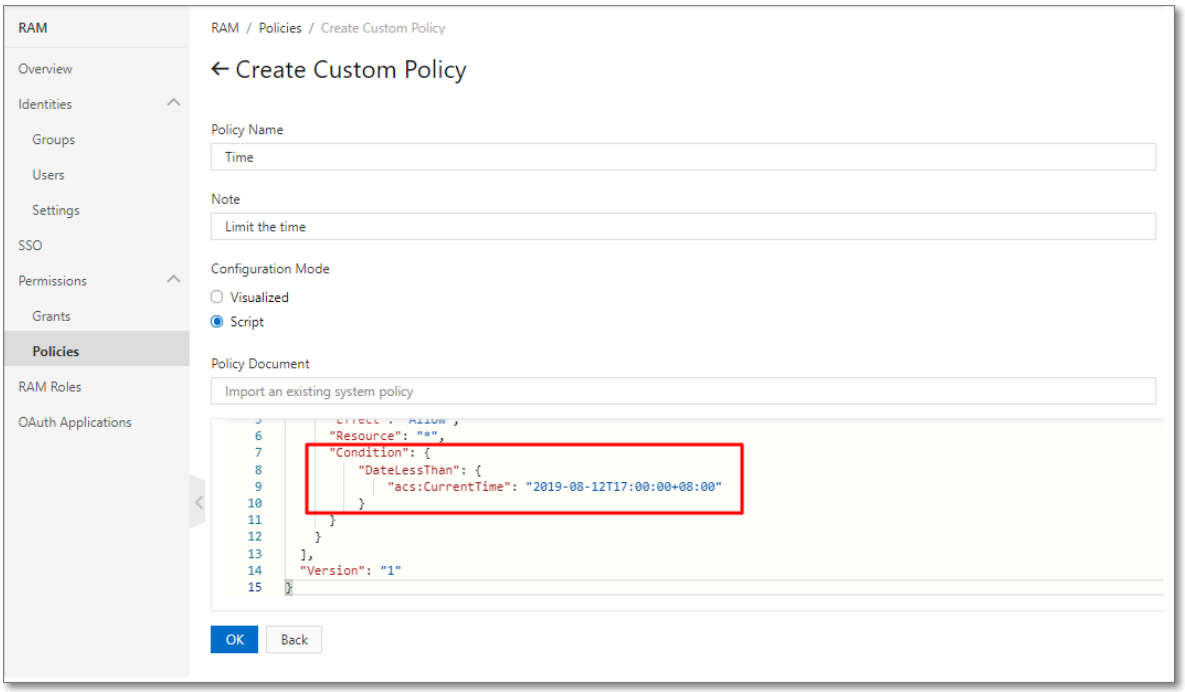
To only allow RAM users to access Alibaba Cloud resources during the specified period, create and attach a custom policy for the RAM users.

1. #unique_4.
2. Create a custom policy.
3. #unique_12.

Create a custom policy

1. In the left-side navigation pane, click Policies under Permissions.
2. On the Policies page, click Create Policy.
3. On the page that appears, specify the Policy Name and Note parameters.

4. Under Configuration Mode, select Script. Copy and paste the following sample script to the Policy Document area, and edit the script based on your business needs.



If the following policy is attached to a RAM user, the RAM user can only access ECS instances before 17:00 on August 12, 2019 (UTC+8). In this case, the `acs : CurrentTim e` parameter in `Condition` is set to `2019 - 08 - 12T17 : 00 : 00 + 08 : 00`.

```
{
  " Statement ": [
    {
      " Action ": " ecs :*",
      " Effect ": " Allow ",
      " Resource ": "*",
      " Condition ": {
          " DateLessTh  an ": {
              " acs : CurrentTim  e ": " 2019 - 08 - 12T17 : 00 : 00
 + 08 : 00 "
          }
      }
    }
  ],
  " Version ": " 1 "
}
```

Note:

The `Condition` setting only applies to the actions that are specified for the current policy. You can change the `2019-08-12T17:00:00+08:00` value if necessary.

5. **Click OK.**

4 Use RAM to limit the methods of accessing Alibaba Cloud resources

This topic describes how to use RAM to limit the methods of accessing Alibaba Cloud resources to enable a higher level of security.

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.
- The RAM service is activated, and you can log on to the RAM console. If the RAM service is not activated, activate the service before proceeding. For more information, see #unique_16.
- You have a basic knowledge of the policy elements, structure, and syntax before creating a custom policy. For more information, see #unique_11 and #unique_17.

Context

Enterprise A has purchased more than one type of Alibaba Cloud resources, such as ECS instances, RDS instances, SLB instances, and OSS buckets. To ensure business and data security, this enterprise wants to only allow RAM users to access Alibaba Cloud resources by using the HTTPS method.

Solution

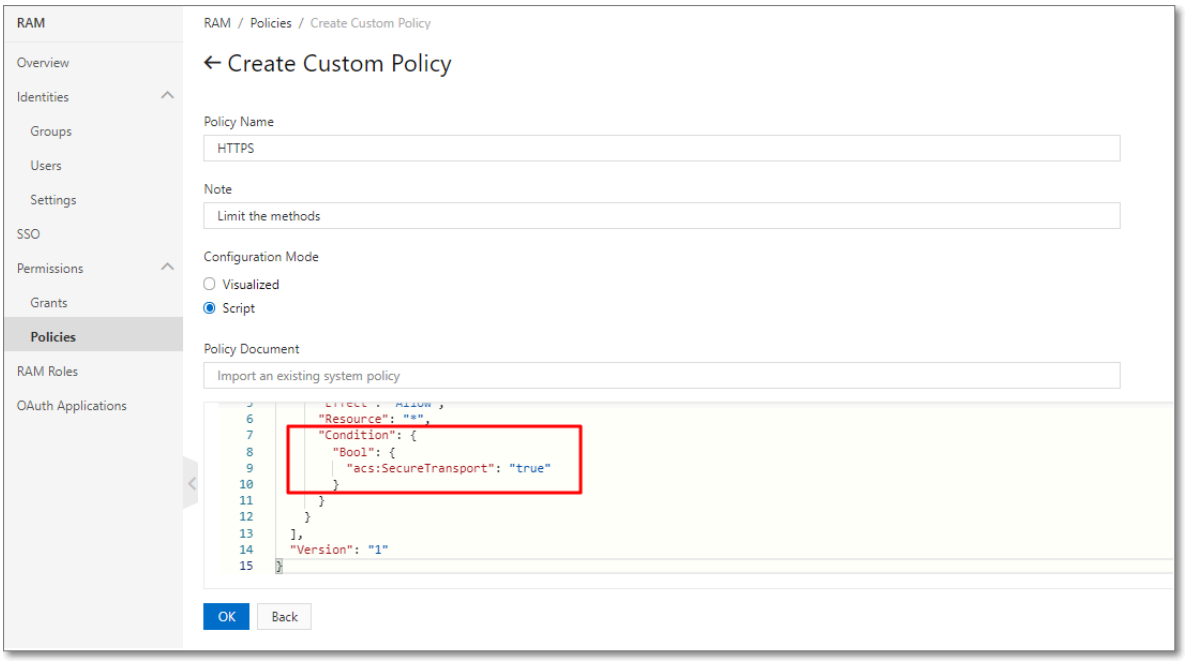
To only allow RAM users to access Alibaba Cloud resources by using the HTTPS method, create and attach a custom policy for the RAM users.

1. #unique_4.
2. Create a custom policy.
3. #unique_12.

Create a custom policy

1. In the left-side navigation pane, click Policies under Permissions.
2. On the Policies page, click Create Policy.
3. On the page that appears, specify the Policy Name and Note parameters.

4. Under Configuration Mode, select Script. Copy and paste the following sample script to the Policy Document area, and edit the script based on your business needs.



If the following policy is attached to a RAM user, the RAM user can only access ECS instances by using the HTTPS method. In this case, the `acs : SecureTran sport` parameter in `Condition` is set to `true` .

```
{
  " Statement ": [
    {
      " Action ": " ecs :*",
      " Effect ": " Allow ",
      " Resource ": "*",
      " Condition ": {
        " Bool ": {
          " acs : SecureTran  sport ": " true "
        }
      }
    }
  ],
  " Version ": " 1 "
}
```

Note:

The `Condition` setting only applies to the actions that are specified for the current policy. The valid values for the `acs : SecureTran sport` parameter include `true` and `false` .

5. Click OK.

5 Use RAM to manage permissions of O&M engineers

This topic describes how to use RAM to grant and then manage permissions of O&M engineers.

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.

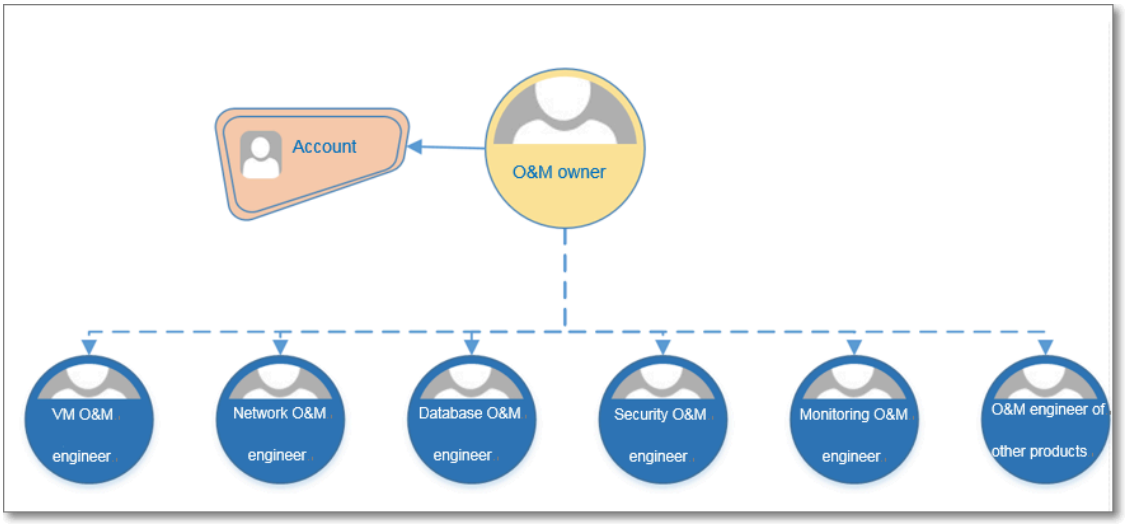
Context

Your company purchases several Alibaba Cloud products and deploys a number of application systems on the cloud, which brings greater O&M requirements.

- Different O&M owners are responsible for different Alibaba Cloud products.
- Different O&M engineers require different permissions to access, operate, and manage Alibaba Cloud resources.

Solution

You can categorize the O&M requirements by product to make them easier to manage . More specifically, you can set an O&M owner and assign different O&M engineers to different categories of requirements and attach your specified policies to these engineers, as shown in the following figure.



Example

This example describes how to set the RAM user `alice @ secloud . onaliyun . com` as the database O&M owner, so that the user can manage RDS and DTS.

1. Log on to the RAM console.
2. #unique_4.
3. In the User Logon Name/Display Name column, find the target RAM user.
4. Click Add Permissions.
5. In the Policy Name column, click `AliyunRDSF ullAccess` and `AliyunDTSF ullAccess` .
6. Click OK.
7. Click Finished.

 Note:
To grant other O&M permissions to the RAM user, see the policies described in the following table.

O&M owner	Policy	Description
O&M owner	AdministratorAccess	Grants the O&M owner the permission to manage all Alibaba Cloud resources.
VM O&M engineer	AliyunECSFullAccess	Grants the VM O&M engineer the permission to manage Elastic Compute Service (ECS).
	AliyunESSFullAccess	Grants the VM O&M engineer the permission to manage Elastic Scaling Service (ESS).
	AliyunSLBFullAccess	Grants the VM O&M engineer the permission to manage Server Load Balancer (SLB).
	AliyunNASFullAccess	Grants the VM O&M engineer the permission to manage Network Attached Storage (NAS).
	AliyunOSSFullAccess	Grants the VM O&M engineer the permission to manage Object Storage Service (OSS).

O&M owner	Policy	Description
	AliyunOTSFullAccess	Grants the VM O&M engineer the permission to manage Table Store (OTS).
Network O&M engineer	AliyunCDNFullAccess	Grants the network O&M engineer the permission to manage Content Delivery Network (CDN).
	AliyunCENFullAccess	Grants the network O&M engineer the permission to manage Cloud Enterprise Network (CEN).
	AliyunCommonBandwidthPackageFullAccess	Grants the network O&M engineer the permission to manage Internet Shared Bandwidth.
	AliyunEIPFullAccess	Grants the network O&M engineer the permission to manage Elastic IP (EIP).
	AliyunExpressConnectFullAccess	Grants the network O&M engineer the permission to manage ExpressConnect.
	AliyunNATGatewayFullAccess	Grants the network O&M engineer the permission to manage NAT Gateway.
	AliyunSCDNFullAccess	Grants the network O&M engineer the permission to manage Secure Content Delivery Network (SCDN).
	AliyunSmartAccessGatewayFullAccess	Grants the network O&M engineer the permission to manage Smart Access Gateway.
	AliyunVPCFullAccess	Grants the network O&M engineer the permission to manage Virtual Private Cloud (VPC).
	AliyunVPNGatewayFullAccess	Grants the network O&M engineer the permission to manage VPN Gateway.

O&M owner	Policy	Description
Database O&M engineer	AliyunRDSFullAccess	Grants the database O&M engineer the permission to manage Relational Database Service (RDS).
	AliyunDTSFullAccess	Grants the database O&M engineer the permission to manage Data Transmission Service (DTS).
Security O&M engineer	AliyunYundunFullAccess	Grants the security O&M engineer the permission to manage Alibaba Cloud Security.
Monitoring O&M engineer	AliyunActionTrailFullAccess	Grants the monitoring O&M engineer the permission to manage ActionTrail.
	AliyunARMSFullAccess	Grants the monitoring O&M engineer the permission to manage Application Real-Time Monitoring Service ARMS).
	AliyunCloudMonitorFullAccess	Grants the monitoring O&M engineer the permission to manage CloudMonitor.
	(Optional) ReadOnlyAccess	Optional. Grants the monitoring O&M engineer the read-only permission to all Alibaba Cloud resources.
	AliyunSupportFullAccess	Grants the monitoring O&M engineer the permission to manage Alibaba Cloud support systems.

6 Use RAM to manage user permissions and resources

This topic describes how to use RAM to manage user permissions and resources.

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.

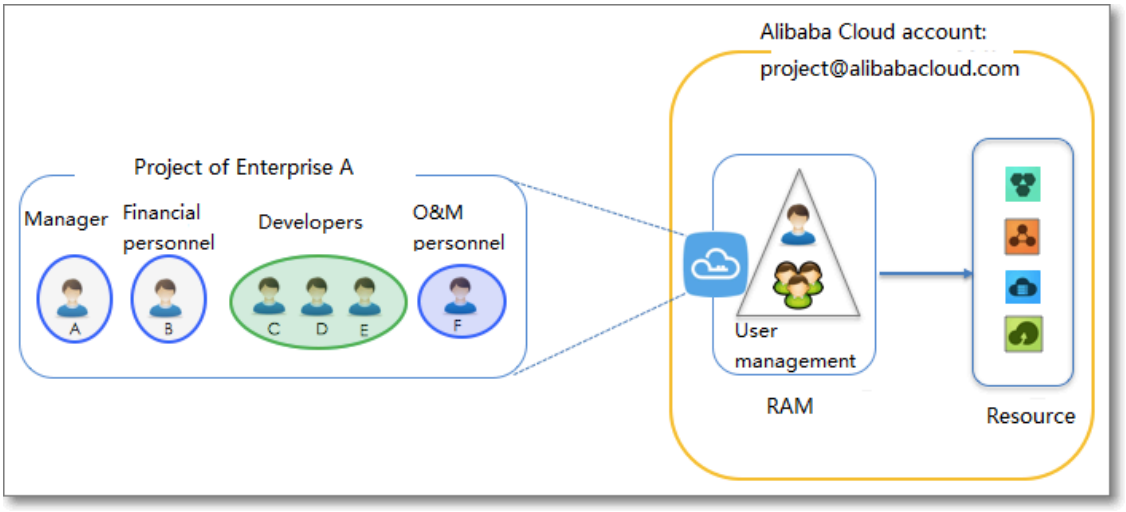
Scenario

Enterprise A has bought several types of Alibaba Cloud resources, such as ECS instances, RDS instances, SLB instances, and OSS buckets for a project. During this project, many employees need to perform operations on these cloud resources, but different employees require different permissions to complete different operations.

The requirements of Enterprise A are as follows:

- Employees do not share the Alibaba Cloud account to avoid mistaken disclosure of the account password or AccessKey pair.
- Independent RAM users are created for different employees and the RAM users are granted independent permissions.
- All operations of all RAM users can be audited by Enterprise A.
- The permissions of RAM users can be removed at any time, and users under an Alibaba Cloud account can be deleted by Enterprise A.
- Fees are not charged to each RAM user, but are instead charged to the correspond ing Alibaba Cloud account to which the RAM users belong.

Solution



- Set multi-factor authentication (MFA) for you Alibaba Cloud account to avoid risks associated with mistaken disclosure of the password. For more information, see #unique_8.
- Create RAM users for different employees (or applications) and set logon passwords or create AccessKey pairs. For more information, see #unique_4.
- If multiple RAM users require the same permissions, we recommend that you create a user group and add the corresponding users to this group. For more information, see #unique_5.
- Attach one or more system policies to the groups or users. For more information, see #unique_12 or #unique_22. For finer-grained permission management, you can create one or more custom policies and attach them to individual users or to a user group. For more information, see #unique_6.
- Remove permissions from groups or RAM users when they no longer need the permissions. For more information, see #unique_23 or #unique_24.

7 Use a temporary STS token to authorize a mobile app to access Alibaba Cloud resources

This topic describes how to use a temporary STS token of a RAM role to authorize a mobile app to access Alibaba Cloud resources.

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

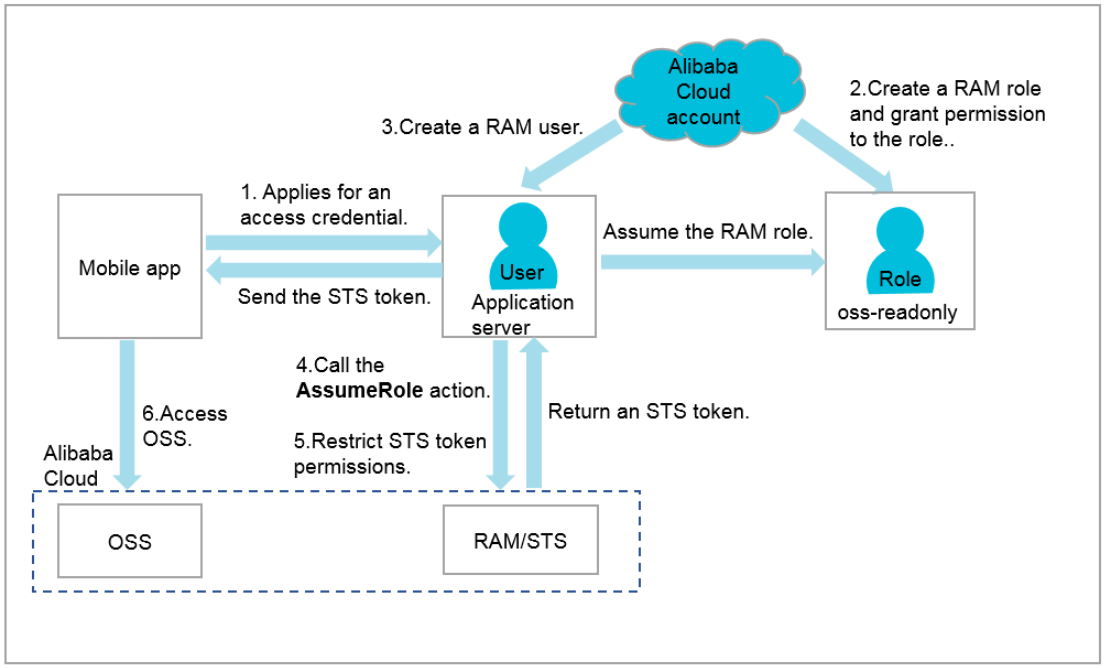
Enterprise A has developed a mobile app, which runs on users' own devices. Therefore, Enterprise A cannot manage these devices directly and wants to use Alibaba Cloud OSS so that the mobile app can upload data to or download data from OSS.

The requirements of Enterprise A are as follows:

- The app does not need to use an application server to transmit data. Instead, it can directly upload data to or download data from OSS.
- To maintain account security, Enterprise A will not save the AccessKey pair to the mobile app because mobile devices that run the app are not managed by Enterprise A directly.
- Security risks are minimized by granting the app temporary access credentials (by means of an STS token) that the app can then use to connect to OSS. The app can access OSS only for a specified duration.

Solution

Before you upload data to or download data from OSS, the mobile app must first apply for an access credential from the application server. The application server assumes a RAM role as a RAM user, calls the `AssumeRole` action of the STS API to obtain a temporary STS token, and then sends the STS token to the mobile app. After the STS token is sent, the mobile app uses the STS token to access OSS.



1. The mobile app applies for an access credential from the application server.
2. Enterprise A uses its Alibaba Cloud account to create a RAM role and grant relevant permissions to the role.

   For more information, see Create a RAM role and grant relevant permissions.
3. Enterprise A uses its Alibaba Cloud account to create a RAM user for the application server to assume the RAM role.

   For more information, see Create a RAM user and allow the user to assume a RAM role.
4. The application server calls the #unique_26 action of the STS API to obtain a temporary STS token of the RAM role.

   For more information, see Obtain the STS token of the RAM role.
5. The application server further limits the resource operation permissions of the temporary STS token when it assumes the role, to better manage the permissions of each app.

   For more information, see Restrict STS token permissions.
6. The mobile app uses the temporary STS token to upload data to or download data from OSS.

   For more information, see Use the STS token to access OSS.

Create a RAM role and grant relevant permissions

Assume that the Alibaba Cloud account ID of Enterprise A is `1234567890 12 ****`.

1. Enterprise A uses its Alibaba Cloud account to create a RAM role `oss - readonly` and selects Current Alibaba Cloud Account as the trusted account so that only RAM users under the Alibaba Cloud account can assume this role.

   For information about how to create a RAM role, see #unique_27.

   After creating the role, Enterprise A can view the role information on the basic information page.

   - In this example, the Alibaba Cloud Resource Name (ARN) of the role is `acs : ram :: 1234567890 12 ****: role / oss - readonly`.
   - The trust policy of the role (in which only RAM users under the current Alibaba Cloud account of Enterprise A can assume) is as follows:

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

2. Enterprise A uses its Alibaba Cloud account to attach the `AliyunOSSR eadOnlyAcc ess` policy (OSS read-only permission) to the role `oss - readonly`.

   For information about how to grant permission to a RAM role, see #unique_28.

Create a RAM user and allow the user to assume a RAM role

1. Enterprise A uses its Alibaba Cloud account to create a RAM user `appserver`.

   For information about how to create a RAM user, see #unique_4.

2. Enterprise A uses its Alibaba Cloud account to attach the `AliyunSTSA ssumeRoleA ccess` policy to the user `appserver` so that the user can assume a RAM role.

   For information about how to grant permission to a RAM user, see #unique_12.

Obtain the STS token of the RAM role

1. The application server uses the AccessKey pair of the RAM user to call the `AssumeRole` action of the STS API.

   > **Note:**
   > The AccessKey pair for the application server must be configured.

   The following is an example of how to use Alibaba Cloud CLI to call the `AssumeRole` action:

   ```
   $ aliyuncli sts AssumeRole -- RoleArn acs : ram ::
   1234567890 12 ****: role / oss - readonly -- RoleSessio nName
   client - 001
   {
       " AssumedRol eUser ": {
           " AssumedRol eId ": " 3915787525 73 ****: client - 001
   ",
           " Arn ": " acs : ram :: 1234567890 12 ****: role / oss -
   readonly / client - 001 "
       },
       " Credential s ": {
           " AccessKeyS ecret ": " 93ci2umK1Q KNEja6WGqi
   1Ba7Q2Fv9P wxZqtVF2Vy ****",
           " SecurityTo ken ": "********",
           " Expiration ": " 2016 - 01 - 13T15 : 02 : 37Z ",
           " AccessKeyI d ": " STS . F13GjskXTj k38dBY6YxJ t ****"
       },
       " RequestId ": " E1779AAB - E7AF - 47D6 - A9A4 - 53128708B6 CE
   "
   }
   ```

   > **Note:**
   > If the `Policy` parameter is left unspecified, the returned STS token has all the permissions of the RAM role `oss - readonly` .

2. The STS service sends the STS token to the application server. The STS token contains the following elements: `AccessKeyI d` , `AccessKeyS ecret` , and `SecurityTo ken` .

   > **Note:**
   > The validity period of the security token (`SecurityTo ken`) is determined. If the application requires a longer validity period, the application server must re-issue a new STS token, for example, issue one STS token every 1800 seconds.

Restrict STS token permissions

Enterprise A configures the `Policy` parameter to further restrict the permissions of the STS token.

For example, Enterprise A allows the STS token to access only `sample - bucket / 2015 / 01 / 01 /*. jpg` .

```
$ aliyuncli sts AssumeRole -- RoleArn acs : ram :: 1234567890
 12 ****: role / oss - readonly -- RoleSessio nName client - 002
 -- Policy "{\" Version \":\" 1 \", \" Statement \": [{\" Effect \":
\" Allow \", \" Action \":\" oss : GetObject \", \" Resource \":\" acs
 : oss :*:*: sample - bucket / 2015 / 01 / 01 /*. jpg \"}]}"
{
   " AssumedRol eUser ": {
       " AssumedRol eId ": " 3915787525 73 ****: client - 002 ",
       " Arn ": " acs : ram :: 1234567890 12 ****: role / oss -
 readonly / client - 002 "
   },
   " Credential s ": {
       " AccessKeyS ecret ": " 28Co5Vyx2X htTqj3RJgd ud4ntyzrSN
 dUvNygAj7x ****",
       " SecurityTo ken ": "********",
       " Expiration ": " 2016 - 01 - 13T15 : 03 : 39Z ",
       " AccessKeyI d ": " STS . FJ6EMcS1JL ZgAcBJSTDG 1 ****"
   },
   " RequestId ": " 98835D9B - 86E5 - 4BB5 - A6DF - 9D3156ABA5 67 "
}
```

Note:

The default validity period of the STS token is 3600 seconds (maximum limit). You can specify the `DurationSe conds` parameter to limit the STS token expiration time.

Use the STS token to access OSS

1. The application server sends the STS token to the mobile app.
2. The mobile app uses the STS token to access OSS.

   The following is an example of how to use Alibaba Cloud CLI and the STS token to access an OSS object:

```
 Configure the STS token syntax : aliyuncli oss Config
 -- host -- accessid -- accesskey -- sts_token
$ aliyuncli oss Config -- host oss . aliyuncs . com --
 accessid STS . FJ6EMcS1JL ZgAcBJSTDG 1 **** -- accesskey
 28Co5Vyx2X htTqj3RJgd ud4ntyzrSN dUvNygAj7x **** -- sts_token
   CAESnQMIAR KAASJgnzMz lXVyJn4KI + FsysaIpTGm 8ns8Y74HVE
 j0pOevO8ZW Xrnnkz4a4r BEPBAdFkh3 197GUspruj siU78Fkszx
 hnQPKkQKcy vPihoXqKvu ukrQ / Uoudk31KAJ Ez5o2EjlNU REcxWjRDRS
 ISMzkxNTc4 NzUyNTczOT cyODU0Kgpj bGllbnQtMD AxMKmZxIHB
 KjoGUnNhTU Q1Qn8KATEa egoFQWxsb3 cSJwoMQWN0 aW9uRXF1YW
 xzEgZBY3Rp b24aDwoNb3 NzOkdldE9i amVjdBJICg 5SZXNvdXJj
```

```
 ZUVxdWFscx  IIUmVzb3Vy  Y2UaLAoqYW  NzOm9zczoq  Oio6c2FtcG
 xlLWJ1Y2tl  dC8yMDE1Lz  AxLzAxLyou  anBnSgU0Mz  I3NFIFMjY4
 NDJaD0Fzc3  VtZWRSb2xl  VXNlcmAAah  IzOTE1Nzg3  NTI1NzM5Nz
 I4NTRyCWVj  cy1hZG1pbn  jgxt7Cj / bo ****
 Access   OSS
$  aliyuncli   oss   Get   oss :// sample - bucket / 2015 / 01 / 01
 / grass . jpg   grass . jpg
```

More information

#unique_29

#unique_30

#unique_31

#unique_32

8 Cross-account resource authorization and access

This topic describes how to use RAM roles to perform cross-account resource authorization and access.

Scenario

Account A and Account B represent two different enterprises (Enterprise A and Enterprise B, respectively). Enterprise A has bought various cloud resources (such as ECS instances, RDS instances, SLB instances, and OSS buckets) to support its business .

Requirement analysis

- Account A is the resource owner and wants to grant Account B the relevant permissions to perform operations on resources of Account A.
- Account B wants to further grant the permissions to its RAM users (employees or applications). If an employee of Account B joins or leaves Enterprise B, Account A cannot make any changes to the permissions.
- If Enterprise A or Enterprise B ends the agreement, Account A can remove the permissions of Account B at any time.

Solution

Use RAM roles to perform cross-account authorization and resource access.

- Account A creates a role in RAM, grants relevant permissions to the RAM role, and allows Account B to use this role.

  For more information, see Cross-account authorization.
- If an employee (that is, a RAM user) under Account B needs to use this role, Account B can grant permissions to this RAM user to perform operations on the resources of Account A.

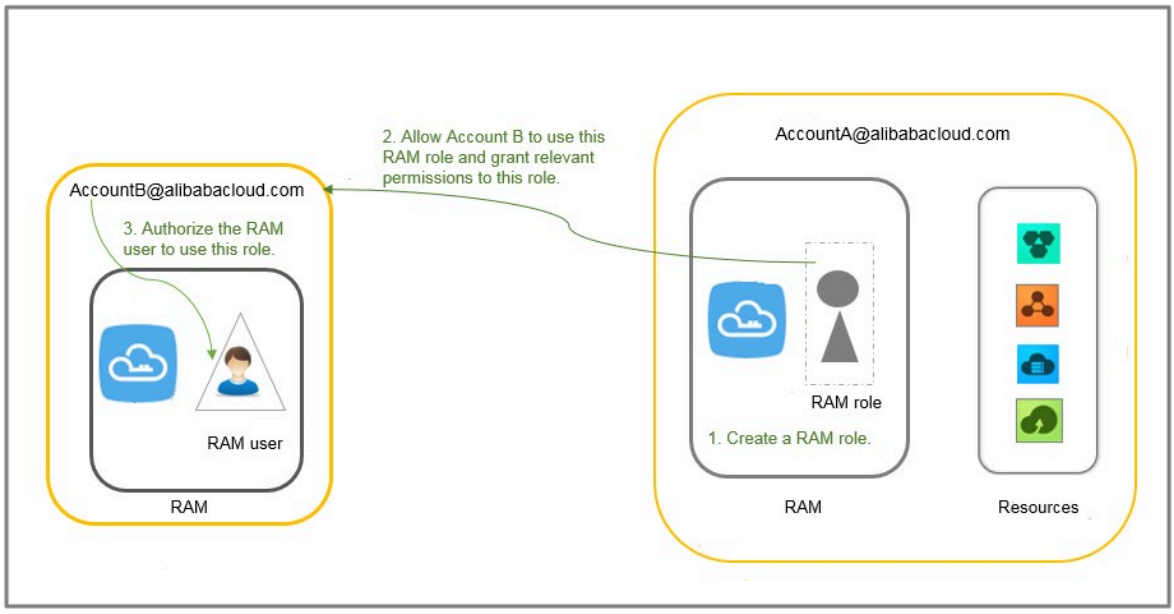
  For more information, see Cross-account resource access.
- If Enterprise A or Enterprise B ends the agreement, Account A can revoke the permissions of Account B. In this case, all RAM users of Account B lose the permissions associated with this role.

  For more information, see Removing cross-account authorization.

Cross-account authorization

The following figure shows how to use a RAM role to achieve cross-account authorization. In this example, Enterprise A (whose account ID is 11223344 and account alias is company-a) needs to grant ECS operation permissions to the employees of Enterprise B (whose account ID is 12345678 and account alias is company-b).

Figure 8-1: Use a RAM role to achieve cross-account authorization



1. Account A creates a RAM role (here, the role is named ecs-admin) and selects Other Alibaba Cloud Account (here, the account ID is 12345678) as a trusted entity.

   For more information, see #unique_37.

   After creating the role, Account A can view the role information on the Basic Information page.

   - In this example, the Alibaba Cloud Resource Name (ARN) of the role is as follows:

     ```
     acs : ram :: 11223344 : role / ecs - admin
     ```

   - The trust policy in the role (in which only RAM users under Account B can assume) is as follows:

     ```
     {
     " Statement ": [
     {
     ```

```
" Action ": " sts : AssumeRole ",
" Effect ": " Allow ",
" Principal ": {
  " RAM ": [
    " acs : ram :: 12345678 : root "
  ]
}
}
],
" Version ": " 1 "
}
```

2. Account A attaches the `AliyunECSF ullAccess` policy to the role ecs-admin.

   For more information, see #unique_38.

3. Account B creates a RAM user (here, the RAM user is named Alice) for its employee, sets a logon password for the RAM user, and attaches the `AliyunSTSA ssumeRoleA ccess` system policy for the RAM user to call the STS AssumeRole API.

Cross-account resource access

To allow RAM user Alice under Account B to access the ECS resources of Account A (through the Alibaba Cloud console), follow these steps:

1. Log on to the RAM console.

   During logon, enter the account alias company-b, RAM user name Alice, and password 123456.

2. Move the pointer over the account icon and click Switch Role.

   On the displayed page, enter company-a for Enterprise Alias/Default Domain Name and ecs-admin for Role Name.

> Note:
> After completing the preceding operations, the RAM user Alice can perform operations on the ECS resources of Account A.

Removing cross-account authorization

If Account A wants to remove the permission of using the role ecs-admin from Account B, the procedure is as follows:

1. Log on to the RAM console, click RAM Roles, and click the role name of ecs-admin.

2. Click the Trust Policy Management tab and delete `acs : ram :: 12345678 : root` .

Note:

Account A can also remove the permission of using the role ecs-admin from Account B by deleting the ecs-admin role on the RAM Roles page. However, the role cannot have any policies attached to it before being deleted.

9 Use RAM to authorize applications to access Alibaba Cloud resources

This topic describes how to use RAM to authorize applications to access Alibaba Cloud resources by obtaining the temporary STS token of a RAM role.

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

An enterprise has bought ECS instances and wants to deploy its applications in ECS. To allow the applications to access other Alibaba Cloud APIs by using access keys, the enterprise can use one of the following methods:

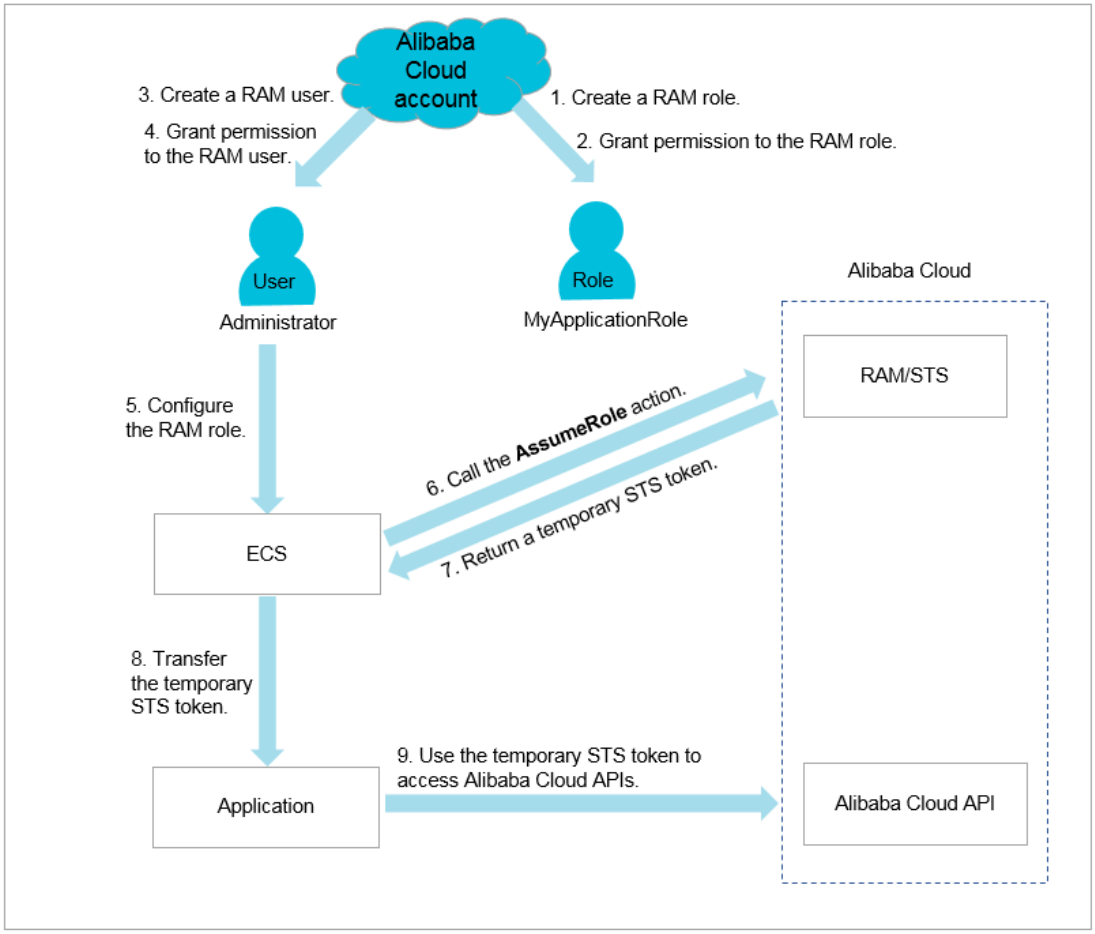
- Embed the access keys into the code.
- Save the access keys in the configuration files of the applications.

However, if the preceding methods are used, the following issues occur:

- Access key disclosure: If the access keys are embedded in the ECS instances in plaintext, they can be mistakenly disclosed to another user due to the sharing of a snapshot, or an image to create a shared image instance.
- O&M complexity: If the access keys are changed (due to access key rotation or changes to user identities), all instances and images need to be updated and redeployed because the access keys exist in the ECS instances. As a result, the management of instances and images is highly complex.

Solution

To resolve the preceding issues, the enterprise can combine ECS with the access control feature of RAM. Specifically, the administrator creates a RAM role for each ECS instance (that is, the operating environment of the applications) and grants each RAM role appropriate permissions. The applications can use the temporary STS token of the corresponding RAM role to call other Alibaba Cloud APIs.



Procedure

1. The enterprise uses its Alibaba Cloud account to create a RAM role (`MyApplicationRole`).

   > **Note:**
   > The preceding role is an Alibaba Cloud service in which ECS is selected as the trusted service.

   For information about how to create a RAM role, see #unique_40.

2. The enterprise uses its Alibaba Cloud account to grant relevant permissions to the RAM role.

   For information about how to grant permission to a RAM role, see #unique_28.

   > **Note:**
   > If the temporary STS token does not have corresponding permissions, the enterprise needs to attach related policies to the RAM role. After the policies attached to the RAM role are updated, the permissions associated with the

temporary STS token take effect immediately and the user does not need to restart the ECS instance.

3. The enterprise uses its Alibaba Cloud account to create a RAM user.

   For information about how to create a RAM user, see #unique_4.

4. The enterprise uses its Alibaba Cloud account to grant relevant permissions to the RAM user.

   - If the administrator and the RAM user have the same responsibilities, the `Administra torAccess` permission should be granted to the user.
   - If the administrator and the RAM user have different responsibilities, the `PassRole` permission should be granted to the user.

     The enterprise uses its Alibaba Cloud account to create a custom policy in the RAM console and attach the policy to the RAM user. The policy content is as follows:

```
{
   " Statement ": [
    {
      " Effect ": " Allow ",
      " Action ": " ram : PassRole ",
      " Resource ": " acs : ram :*:*: role / MyApplicat ionRole
 "// Replace  MyApplicat ionRole  with  the  name  of  your
   RAM  role .
    }
  ],
  " Version ": " 1 "
}
```

     Note:

     - Only authorized RAM users can configure RAM roles for ECS instances. In this way, the use of RAM roles is strictly controlled, which helps to prevent any abuse of permission usage.
     - Before a RAM user (for example, a RAM user that only has access to ECS and is not a RAM permission administrator) creates an ECS instance and configures a RAM role, ECS checks whether the RAM user has the `ram : PassRole` permission of the RAM role. If no permission is found, the RAM user cannot create an ECS instance.

     For information about how to create a custom policy, see #unique_6.

     For information about how to grant permission to a RAM user, see #unique_12.

5. The RAM user starts the ECS instance and then configures the RAM role.
6. ECS calls the `AssumeRole` action of the STS API to obtain the temporary STS token of the RAM role.

   > **Note:**
   > STS verifies the identity of ECS and the policies attached to the RAM role. If the verification succeeds, a temporary STS token is issued. If the verification fails, the request is denied.

   For information about how to use a RAM role by calling an STS API action, see Use the instance RAM role by calling APIs.
7. STS returns the temporary STS token to ECS.
8. ECS sends the temporary STS token to applications in the ECS instance by using the instance metadata.

   - In Linux, the temporary STS token and its validity period can be obtained by using the instance metadata. For more information, see Access other Alibaba Cloud APIs by using instance RAM roles.

     Request example:

     ```
     $  curl   http :// 100 . 100 . 100 . 200 / latest / meta - data /
      ram / security - credential  s / MyApplicat  ionRole
     ```

     Response example

     ```
     [ root @ local  ~]#  curl   http :// 100 . 100 . 100 . 200
      / latest / meta - data / ram / security - credential  s /
      MyApplicat  ionRole
     {
     " AccessKeyI  d " : " STS . J8XXXXXXXX  XX4 ",
     " AccessKeyS  ecret " : " 9PjfXXXXXX  XXXBf2XAW ",
     " Expiration " : " 2017 - 06 - 09T09 : 17 : 19Z ",
     " SecurityTo  ken " : " CAIXXXXXXX  XXXXwmBkle  CTkyI +",
     " LastUpdate  d " : " 2017 - 06 - 09T03 : 17 : 18Z ",
     " Code " : " Success "
     } cess "
     ```

```
}
```

- If the applications use an Alibaba Cloud SDK, the Alibaba Cloud SDK can obtain the STS token of the RAM role from the ECS instance metadata, and you do not need to configure any access key-related information in the SDK.

  For more information, see Configure a RAM role to access ECS instances without using an access key.

> Note:
> The applications can access Alibaba Cloud APIs when the temporary STS token is within the validity period. The STS token usually expires after one hour. ECS automatically refreshes the STS token before it expires.

9. The applications use the STS token to access Alibaba Cloud APIs.

What to do next

If Alibaba Cloud RAM does not meet all of your permission application requirements, you can use other Alibaba Cloud services, such as Function Compute and MaxCompute, that provide the access control features to authorize applications to access your Alibaba Cloud resources.

10 Use tags to authorize ECS instances by group

This topic describes how to use tags to authorize resources (such as ECS instances) by group so that RAM users can only view and operate on the tagged resources.

Scenario

You have 10 ECS instances. You want your dev team to manage 5 of them, and your ops team to manage the other 5. However, you want each team to see only their authorized resources (not the authorized resources of the other team).

Preparations

Make sure that you can log on to the RAM console by using your RAM account.

Solution

Create two RAM user groups, tag these two groups, and grant permissions to the groups.

- Tag five of them with the key as team and the value as dev.
- Tag the other five with the key as team and the value as ops.

Procedure

1. Log on to the ECS console, click Instances, and select the target instance. In the Actions column, choose More > Instance Settings > Edit Tag.
2. Click Create, enter the key and value, and click Confirm.
3. Log on to the RAM console, create two RAM user groups, and name the groups as dev and ops.

   For more information, see #unique_45.
4. Create RAM users and add the users to different user groups.

   For more information, see #unique_46.
5. Create two custom policies and attach them to different user groups.

   For more information, see #unique_47.

 Note:

After you attach a policy to a user group, the RAM users in this group inherit the relevant permissions.

In this example, the policy name of the dev user group is policyForDevTeam. The policy content is as follows:

```
{
    " Statement ": [
    {
        " Action ": " ecs :*",
        " Effect ": " Allow ",
        " Resource ": "*",
        " Condition ": {
            " StringEqua  ls ": {
                " ecs : tag / team ": " dev "
            }
        }
    },
    {
        " Action ": " ecs : DescribeTa  g *",
        " Effect ": " Allow ",
        " Resource ": "*"
    }
    ],
    " Version ": " 1 "
}
```

In the preceding policy,

- The `" Action ": " ecs :*"` element with "Condition" is used to filter the instances tagged as `" team ": " dev "`.
- The `" Action ": " ecs : DescribeTa  g *"` element is used to display all tags. When a user performs operations in the ECS console, the system displays all the tags for the user to select, and then filters the instances according to the tag key and value selected by the user.

 Note:
You can create the policy policyForOpsTeam according to the example and grant this policy to the ops user group.

Display authorized instances

1. Log on to the ECS console as a RAM user.

 Note:
After a user logs on to the ECS console, the system navigates to the ECS overview page by default. In this case, the number of the ECS instances displayed on the page is 0. To view relevant instances, click Instances.

2. Click Instances and click Tags next to the search box.

   Note:
   You need make sure that the region displayed in the console is the region to which the instances belong.

3. Move the pointer over Tag Key. The Tag Value list is displayed. Select a value, and the system then filters the corresponding instances.

What to do next

You can use the procedures described in this topic to tag and authorize security groups, disks, snapshots, and images by group.

Note:
Only custom images can be tagged.

11 Use tags to authorize RDS instances by group

This topic describes how to use tags to authorize resources (such as RDS instances) by group so that RAM users can only view and operate on the tagged resources.

Scenario

You have 10 RDS instances. You want your dev team to manage 5 of them, and your ops team to manage the other 5. However, you want each team to see only their authorized instances (not the authorized resources of the other team).

Preparations

For more information, see #unique_49.

The following is an example of the custom policy relevant to RDS:

```
{
  " Statement ": [
    {
      " Action ": " rds :*",
      " Effect ": " Allow ",
      " Resource ": "*",
      " Condition ": {
        " StringEqua  ls ": {
          " rds : ResourceTa  g / team ": " dev "
        }
      }
    },
    {
       " Action ": " rds : DescribeTa  g *",
       " Effect ": " Allow ",
       " Resource ": "*"
    }
  ],
  " Version ": " 1 "
}
```

In the preceding policy,

- The `" Action ": " rds :*"` element with "Condition" is used to filter the instances tagged as `" team ": " dev "`. The keyword of "Condition" is `rds : ResourceTa  g` .
- The `" Action ": " rds : DescribeTa  g *"` element is used to display all tags. When a user performs operations in the RDS console, the system displays all the tags for the user to select, and then filters the instances according to the tag key and value selected by the user.

What to do next

If the relevant permissions of a RAM user are missing after you have tagged RDS instances into groups and granted permissions, see #unique_50.

12 Manage ECS permissions by using RAM

This topic describes how to manage ECS permissions of RAM users by creating policies in RAM.

Common policies

The following table lists some common policies that can be created in RAM to manage ECS permissions.

Policy	Description
AliyunECSFullAccess	Grants a RAM user full management permissions for ECS instances.
AliyunECSReadOnlyAccess	Grants a RAM user read-only permission for ECS instances.

Note:
For more information about ECS permissions, see #unique_52.

Attach custom policies to RAM users

1. Create custom policies according to the subsequent ECS authorization examples.

   For more information, see #unique_53.
2. Locate the target policy and click the policy name.
3. On the References tab, click Grant Permission.
4. In the Principal field, enter the ID or name of the target RAM user.
5. Click OK.

Note:
You can also attach policies to a RAM user or a RAM user group as needed. For more information, see #unique_47.

ECS authorization examples

- Example 1: As a RAM administrator with multiple instances, authorize a user to operate on only two of your instances.

  The IDs of these two ECS instances are i-001 and i-002.

```
{
```

```
  " Statement ": [
    {
      " Action ": " ecs :*",
      " Effect ": " Allow ",
      " Resource ": [
                  " acs : ecs :*:*: instance / i - 001 ",
                  " acs : ecs :*:*: instance / i - 002 "
                  ]
    },
    {
      " Action ": " ecs : Describe *",
      " Effect ": " Allow ",
      " Resource ": "*"
    }
  ],
  " Version ": " 1 "
}
```

Note:

- The authorized RAM user can view all the ECS instances but can only operate on two of them.
- The `Describe *` element is required in a policy. If a policy does not contain the `Describe *` element, the authorized RAM user cannot view any instance in the console. However, the RAM user can operate on the two specified ECS instances by calling API actions, by using the CLI, or by using ECS SDKs.

- Example 2: As a RAM administrator, authorize a RAM user to view ECS instances in the Qingdao region, but do not allow them to view information about disks and snapshots.

  You can grant ECS permissions to the user by region and resource type.

```
{
  " Statement ": [
    {
      " Effect ": " Allow ",
      " Action ": " ecs : Describe *",
      " Resource ": " acs : ecs : cn - qingdao :*: instance /*"
    }
  ],
  " Version ": " 1 "
}
```

- Example 3: As a RAM administrator, authorize a RAM user to create snapshots.

  If a RAM user cannot create disk snapshots after being granted the ECS instance administrator permission, you must grant disk permissions to the user again. In this example, the ECS instance ID is inst-01 and the disk ID is dist-01.

```
{
  " Statement ": [
    {
```

```
      " Action ": " ecs :*",
      " Effect ": " Allow ",
      " Resource ": [
        " acs : ecs :*:*: instance / inst - 01 "
      ]
    },
    {
      " Action ": " ecs : CreateSnap  shot ",
      " Effect ": " Allow ",
      " Resource ": [
        " acs : ecs :*:*: disk / dist - 01 ",
        " acs : ecs :*:*: snapshot /*"
      ]
    },
    {
      " Action ": [
        " ecs : Describe *"
      ],
      " Effect ": " Allow ",
      " Resource ": "*"
    }
  ],
  " Version ": " 1 "
}
```

13 Manage OSS permissions by using RAM

This topic describes how to manage OSS permissions of RAM users by creating policies in RAM.

Common policies

The following table lists some common policies that can be created in RAM to manage OSS permissions.

Policy	Description
AliyunOSSFullAccess	Grants a RAM user full management permissions for OSS instances.
AliyunOSSReadOnlyAccess	Grants a RAM user read-only permission for OSS instances.

Note:
For more information about OSS permissions, see #unique_55.

Attach custom policies to RAM users

1. Create custom policies according to the subsequent OSS authorization examples.

   For more information, see #unique_6.
2. Locate the target policy and click the policy name.
3. On the References tab, click Grant Permission.
4. In the Principal field, enter the ID or name of the target RAM user.
5. Click OK.

Note:
You can also attach policies to a RAM user or a RAM user group as needed. For more information, see #unique_12and #unique_22.

OSS authorization examples

- Example 1: As a RAM administrator, authorize a user to fully manage an OSS bucket.

```
{
    " Version ": " 1 ",
    " Statement ": [
        {
```

```
            " Effect ": " Allow ",
            " Action ": " oss :*",
            " Resource ": [
                " acs : oss :*:*: myphotos ",
                " acs : oss :*:*: myphotos /*"
            ]
        }
    ]
}
```

- **Example 2: As a RAM administrator, authorize a user to list and read resources in an OSS bucket.**
  - **Authorize a RAM to list and read resources in an OSS bucket by using the OSS CLI or by using OSS SDKs. The name of the OSS bucket is `myphotos`.**

```
{
    " Version ": " 1 ",
    " Statement ": [
        {
            " Effect ": " Allow ",
            " Action ": " oss : ListObject  s ",
            " Resource ": " acs : oss :*:*: myphotos "
        },
        {
            " Effect ": " Allow ",
            " Action ": " oss : GetObject ",
            " Resource ": " acs : oss :*:*: myphotos /*"
        }
    ]
}
```

  - **Authorize a RAM user to operate on resources in the OSS console.**

Note:

When a RAM user logs on to the OSS console, the console calls the `ListBucket s`, `GetBucketA cl`, and `GetObjectA cl` actions to check whether the bucket is public.

```
{
    " Version ": " 1 ",
    " Statement ": [
        {
            " Effect ": " Allow ",
            " Action ": [
                    " oss : ListBucket  s ",
                    " oss : GetBucketS  tat ",
                    " oss : GetBucketI  nfo ",
                    " oss : GetBucketA  cl "
                    ],
            " Resource ": " acs : oss :*:*:*"
        },
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : ListObject  s ",
                " oss : GetBucketA  cl "
```

```
            ],
            " Resource ": " acs : oss :*:*: myphotos "
        },
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : GetObject ",
                " oss : GetObjectA  cl "
            ],
            " Resource ": " acs : oss :*:*: myphotos /*"
        }
    ]
}
```

- **Example 3: As a RAM administrator, authorize a RAM user to access OSS instances by using a specified IP address.**
  - **Add the following condition in the `Allow` element. This allows the IP address segments `192 . 168 . 0 . 0 / 16` and `172 . 12 . 0 . 0 / 16` to read data in `myphotos` .**

```
{
    " Version ": " 1 ",
    " Statement ": [
        {
            " Effect ": " Allow ",
            " Action ": [
                      " oss : ListBucket  s ",
                      " oss : GetBucketS  tat ",
                      " oss : GetBucketI  nfo ",
                      " oss : GetBucketA  cl "
                      ],
            " Resource ": [
                " acs : oss :*:*:*"
            ]
        },
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : ListObject  s ",
                " oss : GetObject "
            ],
            " Resource ": [
                " acs : oss :*:*: myphotos ",
                " acs : oss :*:*: myphotos /*"
            ],
            " Condition ":{
                " IpAddress ": {
                    " acs : SourceIp ": [" 192 . 168 . 0 . 0 / 16
 ", " 172 . 12 . 0 . 0 / 16 "]
                }
            }
        }
    ]
```

```
}
```

- Add the following condition in the `Deny` element. If the IP address of a RAM user is not within the `192 . 168 . 0 . 0 / 16` segment, the user cannot perform any operations on OSS instances.

```
{
    " Version ": " 1 ",
    " Statement ": [
        {
            " Effect ": " Allow ",
            " Action ": [
                    " oss : ListBucket  s ",
                    " oss : GetBucketS  tat ",
                    " oss : GetBucketI  nfo ",
                    " oss : GetBucketA  cl "
                    ],
            " Resource ": [
                " acs : oss :*:*:*"
            ]
        },
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : ListObject  s ",
                " oss : GetObject "
            ],
            " Resource ": [
                " acs : oss :*:*: myphotos ",
                " acs : oss :*:*: myphotos /*"
            ]
        },
        {
            " Effect ": " Deny ",
            " Action ": " oss :*",
            " Resource ": [
                " acs : oss :*:*:*"
            ],
            " Condition ":{
                " NotIpAddre  ss ": {
                    " acs : SourceIp ": [" 192 . 168 . 0 . 0 / 16
 "]
                }
            }
        }
    ]
}
```

Note:

A policy with the Deny command has a higher priority than the policy with the Allow command. Therefore, when a RAM user whose IP address is not within the `192 . 168 . 0 . 0 / 16` segment attempts to access data in `myphotos` , OSS notifies the user of having no permissions.

- **Example 4: Authorize a RAM user by OSS directory.**

  You have a photo bucket named myphotos. The bucket contains directories that indicate the places where the photos were taken. Each directory contains sub-directories that indicate the years when the photos were taken.

```
myphotos [ Bucket ]
  ├── beijing
  │    ├── 2014
  │    └── 2015
  ├── hangzhou
  │    ├── 2013
  │    ├── 2014
  │    └── 2015  // Grant   read - only   permission   on   this
directory   to   users .
  └── qingdao
       ├── 2014
       └── 2015
```

  You can grant read-only permission on the `myphotos / hangzhou / 2015 /` directory to a RAM user according to application scenarios and policy complexity. The following are examples of the application scenarios:

  - **Scenario 1: Authorize a RAM user to read files in the directory without them having to list the files.**

    In this scenario, the RAM user knows the complete paths of all files and can directly read the files by using the complete paths. Generally, a software system requires permission assignment for this.

```
{
    " Version ": " 1 ",
    " Statement ": [
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : GetObject "
            ],
            " Resource ": [
                " acs : oss :*:*: myphotos / hangzhou / 2015 /*"
            ]
        }
    ]
```

```
}
```

- **Scenario 2: Authorize a RAM user to access the `myphotos / hangzhou / 2015 /` directory and list files in the directory by using the OSS CLI.**

  Generally, software developers require such permission assignment. The developers do not know what files are available in a directory and can use the OSS CLI or API to directly obtain the directory information.

  In this scenario, the `ListObject s` permission is required.

```
{
    " Version ": " 1 ",
    " Statement ": [
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : GetObject "
            ],
            " Resource ": [
                " acs : oss :*:*: myphotos / hangzhou / 2015 /*"
            ]
        },
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : ListObject  s "
            ],
            " Resource ": [
                " acs : oss :*:*: myphotos "
            ],
            " Condition ":{
                " StringLike ":{
                    " oss : Prefix ":" hangzhou / 2015 /*"
                }
            }
        }
    ]
```

```
}
```

- **Scenario 3: Authorize a RAM user to access the `myphotos / hangzhou / 2015 /` directory by using the OSS console.**

  In this scenario, the RAM user uses a visual OSS client, such as Windows File Explorer, to access the `myphotos / hangzhou / 2015 /` directory from the root directory through levels of sub-directories.

  The following permissions are required:

  ■ **Permission to list all buckets**

  ■ **Permission to list directories under `myphotos`**

  ■ **Permission to list directories under `myphotos / hangzhou`**

```
{
    " Version ": " 1 ",
    " Statement ": [
        {
            " Effect ": " Allow ",
            " Action ": [
                    " oss : ListBucket  s ",
                    " oss : GetBucketS  tat ",
                    " oss : GetBucketI  nfo ",
                    " oss : GetBucketA  cl "
                    ],
            " Resource ": [
                " acs : oss :*:*:*"
            ]
        },
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : GetObject ",
                " oss : GetObjectA  cl "
            ],
            " Resource ": [
                " acs : oss :*:*: myphotos / hangzhou / 2015 /*"
            ]
        },
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : ListObject  s "
            ],
            " Resource ": [
                " acs : oss :*:*: myphotos "
            ],
            " Condition ": {
                " StringLike ": {
                    " oss : Delimiter ": "/",
                    " oss : Prefix ": [
                        "",
                        " hangzhou /",
                        " hangzhou / 2015 /*"
                    ]
                }
```

```
                }
            }
        ]
}
```

14 Manage RDS permissions by using RAM

This topic describes how to manage RDS permissions of RAM users by creating policies in RAM.

Common policies

The following table lists some common policies that can be created in RAM to manage RDS permissions.

Policy	Description
AliyunRDSFullAccess	Grants a RAM user full management permissions for RDS instances.
AliyunRDSReadOnlyAccess	Grants a RAM user read-only permission for RDS instances.

Note:
For more information about RDS permissions, see #unique_57.

Attach custom policies to RAM users

1. Create custom policies according to the subsequent RDS authorization examples.

   For more information, see #unique_53.
2. Locate the target policy and click the policy name.
3. On the References tab, click Grant Permission.
4. In the Principal field, enter the ID or name of the target RAM user.
5. Click OK.

Note:
You can also attach policies to a RAM user or a RAM user group as needed. For more information, see #unique_47.

RDS authorization examples

- Example 1: As a RAM administrator with multiple instances, authorize a user to operate on only two of your instances.

  The IDs of these two RDS instances are i-001 and i-002.

```
{
```

```
  " Statement ": [
    {
      " Action ": " rds :*",
      " Effect ": " Allow ",
      " Resource ": [
                  " acs : rds :*:*: dbinstance / i - 001 ",
                  " acs : rds :*:*: dbinstance / i - 002 "
                  ]
    },
    {
      " Action ": " rds : Describe *",
      " Effect ": " Allow ",
      " Resource ": "*"
    }
  ],
  " Version ": " 1 "
}
```

Note:

- The authorized RAM user can view all the RDS instances but can only operate on two of them.
- The `Describe *` element is required in a policy. If a policy does not contain the `Describe *` element, the authorized RAM user cannot view any instance in the console. However, the RAM user can operate on the two specified RDS instances by calling API actions, by using the CLI, or by using RDS SDKs.

- Example 2: As a RAM administrator, authorize a user to access data in the Alibaba Cloud Data Management System (DMS).
  - Authorize a RAM user to access a specified RDS instance.

```
{
  " Statement ": [
    {
      " Action ": " dms : LoginDatab  ase ",
      " Effect ": " Allow ",
      " Resource ": " acs : rds :*:*: dbinstance / rds783a063
 9ks5k7 ****"
    }
  ],
  " Version ": " 1 "
}
```

Note:
You need to replace `rds783a063  9ks5k7 ****` with the ID of the RDS instance to be accessed.

  - Authorize a RAM user to access all RDS instances.

```
{
  " Statement ": [
```

```
    {
      " Action ": " dms : LoginDatab  ase ",
      " Effect ": " Allow ",
      " Resource ": " acs : rds :*:*:*"
    }
  ],
  " Version ": " 1 "
}
```

15 Manage SLB permissions by using RAM

This topic describes how to manage SLB permissions of RAM users by creating policies in RAM.

Common policies

The following table lists some common policies that can be created in RAM to manage SLB permissions.

Policy	Description
AliyunSLBFullAccess	Grants a RAM user full management permissions for SLB instances.
AliyunSLBReadOnlyAccess	Grants a RAM user read-only permission for SLB instances.

Note:
For more information about SLB permissions, see #unique_59.

Attach custom policies to RAM users

1. Create custom policies according to the subsequent SLB authorization examples.

   For more information, see #unique_53.
2. Locate the target policy and click the policy name.
3. On the References tab, click Grant Permission.
4. In the Principal field, enter the ID or name of the target RAM user.
5. Click OK.

Note:
You can also attach policies to a RAM user or a RAM user group as needed. For more information, see #unique_47.

SLB authorization examples

- Example 1: As a RAM administrator with multiple instances, authorize a user to operate on only two of your instances.

  The IDs of these two SLB instances are i-001 and i-002.

```
{
```

```
  " Statement ": [
    {
      " Effect ": " Allow ",
      " Action ": " slb :*",
      " Resource ": [
                  " acs : slb :*:*: loadbalanc  er / i - 001 ",
                  " acs : slb :*:*: loadbalanc  er / i - 002 "
                  ]
    },
    {
      " Effect ": " Allow ",
      " Action ": " slb : Describe *",
      " Resource ": "*"
    }
  ],
  " Version ": " 1 "
}
```

Note:

- The authorized RAM user can view all the SLB instances but can only operate on two of them.
- The `Describe *` element is required in a policy. If a policy does not contain the `Describe *` element, the authorized RAM user cannot view any instance in the console. However, the RAM user can operate on the two specified SLB instances by calling API actions, by using the CLI, or by using SLB SDKs.

- Example 2: As a RAM administrator, authorize a user to add ECS instances to an SLB instance. The ID the SLB instance is i-001.

```
{
  " Statement ": [
    {
      " Effect ": " Allow ",
      " Action ": " slb : AddBackend  Servers ",
      " Resource ": [" acs : slb :*:*: loadbalanc  er / slb - 001 "]
    },
    {
      " Effect ": " Allow ",
      " Action ": " slb : AddBackend  Servers ",
      " Resource ": [" acs : ecs :*:*: instance / i - 001 "]
    },
    {
        " Effect ": " Allow ",
        " Action ": " slb : DescribeLo  adBalancer  s ",
        " Resource ": " acs : slb :*:*: loadbalanc  er /*"
    }
  ],
  " Version ": " 1 "
}
```

Note:

After you have granted the SLB management permission to a RAM user according to the policy described in example 1, you also need to grant the following permissions to the user so that the user can add or remove ECS instances, or set the weight of ECS instances as needed:

- The permission for SLB resources
- The permission for ECS resources

- Example 3: As a RAM administrator, authorize a user to perform any ECS-related operations on a specified SLB instance.

```
{
  " Statement ": [
    {
      " Effect ": " Allow ",
      " Action ": " slb :*",
      " Resource ": [
                  " acs : slb :*:*: loadbalanc  er / i - 001 ",
                  " acs : slb :*:*: loadbalanc  er / i - 002 "
                  ]
    },
    {
      " Effect ": " Allow ",
      " Action ": " slb : Describe *",
      " Resource ": "*"
    },
    {
      " Effect ": " Allow ",
      " Action ": " slb :*",
      " Resource ": " acs : ecs :*:*:*"
    }
  ],
  " Version ": " 1 "
}
```

 Note:

The preceding policy allows a RAM user to manage two specified SLB instances (IDs: i-001 and i-002) and perform all ECS-related operations on these two SLB instances, for example, add ECS instances to these two SLB instances and set the weight of ECS.

16 Manage CDN permissions by using RAM

This topic describes how to manage CDN permissions of RAM users by creating policies in RAM.

Common policies

The following table lists some common policies that can be created in RAM to manage CDN permissions.

Policy	Description
AliyunCDNFullAccess	Grants a RAM user full management permissions for CDN instances.
AliyunCDNReadOnlyAccess	Grants a RAM user read-only permission for CDN instances.

Note:
For more information about CDN permissions, see #unique_61.

Authorize a RAM user to perform the read-only, cache refresh, and push operations on CDN instances

1. Create a custom policy.

```
{
  " Version ": " 1 ",
  " Statement ": [
    {
      " Action ": [
        " cdn : Describe *",
        " cdn : PushObject  Cache ",
        " cdn : RefreshObj  ectCaches "
      ],
      " Resource ": " acs : cdn :*:*:*",
      " Effect ": " Allow "
    }
  ]
}
```

   For more information, see #unique_53.
2. Locate the target policy and click the policy name.
3. On the References tab, click Grant Permission.
4. In the Principal field, enter the ID or name of the target RAM user.

5. Click OK.

Note:

You can also attach policies to a RAM user or a RAM user group as needed. For more information, see #unique_47.

17 Record RAM operations by using ActionTrail

This topic describes how to record operations of an Alibaba Cloud account or a RAM user on resources by using ActionTrail.

View RAM operations by using ActionTrail

1. Log on to the ActionTrail console.
2. On the History Search page, use the Filter drop-down list to search for the target event.
3. Click the event, then click View event.

Operations recorded by ActionTrail

ActionTrail can record the following RAM operations:

- Logon information of an Alibaba Cloud account or a RAM user. For more information, see #unique_63.
- Operations in the RAM console. The following is an example of a recorded operation event:

```
{
    " apiVersion ":" 2015 - 05 - 01 ",
    " eventId ":" 2cc52dee - d8d2 - 40c2 - 8de0 - 3a2cf1df ****",
    " eventName ":" DeleteGrou  p ",
    " eventSourc  e ":" ram . aliyuncs . com ",
    " eventTime ":" 2015 - 11 - 03T13 : 41 : 49Z ",
    " eventType ":" ApiCall ",
    " eventVersi  on ":" 1 ",
    " requestId ":" 9AE24F49 - C52C - 4F0F - BCF9 - 9A4B8C22B1  47
 ",
    " requestPar  ameters ":{
        " GroupName ":" grp1 ",
    },
    " serviceNam  e ":" Ram ",
    " sourceIpAd  dress ":" 42 . 120 . XX . XX ",
    " userAgent ":" AliyunCons  ole ",
    " userIdenti  ty ":{
        " type ":" ram - user ",
        " principalI  d ":" 2741806465  4829 ****",
        " accountId ":" 1234567890  12 ****",
        " userName ":" Alice ",
        " sessionCon  text ":{
            " sessionAtt  ributes ":{
                " creationDa  te ":" 2015 - 11 - 03T13 : 41 : 48Z ",
                " mfaAuthent  icated ":" true "
            }
        }
    }
}
```

- RAM and STS API calls for resource creation, change, and deletion. The following is an example of a recorded event:

```
{
    " apiVersion ": " 2015 - 05 - 01 ",
    " eventId ": " 234ef3c7 - 8938 - 4bd7 - bb80 - 11754b7b ****",
    " eventName ": " CreateGrou  p ",
    " eventSourc  e ": " ram . aliyuncs . com ",
    " eventTime ": " 2016 - 01 - 04T08 : 58 : 50Z ",
    " eventType ": " ApiCall ",
    " eventVersi  on ": " 1 ",
    " recipientA  ccountId ": " 43274 ",
    " requestId ": " 1485748C - DB62 - 4693 - AB7E - 4BA3F3A970  E1
 ",
    " requestPar  ameters ": {
        " Comments ": " this   is   a   test   group ",
        " GroupName ": " grp1 "
    },
    " serviceNam  e ": " Ram ",
    " sourceIpAd  dress ": " 42 . 120 . XX . XX ",
    " userAgent ": " aliyuncli / 2 . 0 . 6 ",
    " userIdenti  ty ": {
        " type ": " ram - user ",
        " principalI  d ": " 2741806465  4829 ****",
        " accountId ": " 43274 ",
        " accessKeyI  d ": " f6Iz ******** EI4d ",
        " userName ": " Alice "
    }
}
```

What to do next

For more information about operation records, see #unique_64.

18 Authorize RAM users to use ActionTrail resources

This topic describes how to authorize RAM users to use ActionTrail resources by using system policies or custom policies.

Before you begin

1. View the ActionTrail API actions and their descriptions. For more information, see #unique_66.
2. View the RAM policy structure and syntax. For more information, see #unique_17.

Procedure

1. Create a RAM user.

   For more information, see #unique_67.
2. Grant permission to the RAM user.
   - You can grant required permissions to the RAM user by attaching one or more system policies according to the subsequent ActionTrail-related system policies.

     For more information, see #unique_47.
   - You can grant fine-grained permissions to the RAM user by creating custom policies according to the subsequent authorization examples.

     For more information, see #unique_53.

ActionTrail-related system policies

The following table lists the system policies that are commonly used in ActionTrail.

Table 18-1: System policies

System policy	Description
AliyunActionTrailFullAccess	Grants a RAM user full management permissions for ActionTrail resources.
AliyunActionTrailReadOnlyAccess	Grants a RAM user read-only permission for ActionTrail resources.

Authorization examples

- **Example 1: As a RAM administrator, grant a user read-only permission.**

```
{
    " Version ": " 1 ",
    " Statement ": [{
        " Effect ": " Allow ",
        " Action ": [
            " actiontrai  l : LookupEven  ts ",
            " actiontrai  l : Describe *",
            " actiontrai  l : Get *"
        ],
        " Resource ": "*"
    }]
}
```

- **Example 2: As a RAM administrator, grant a user read-only permission when they log on from a specified IP address.**

```
{
    " Version ": " 1 ",
    " Statement ": [{
        " Effect ": " Allow ",
        " Action ": [
            " actiontrai  l : LookupEven  ts ",
            " actiontrai  l : Describe *",
            " actiontrai  l : Get *"
        ],
        " Resource ": "*",
        " Condition ":{
            " IpAddress ": {
                " acs : SourceIp ": " 42 . 120 . XX . X / 24 "
            }
        }
    }]
}
```