ALIBABA CLOUD

Alibaba Cloud

Resource Access Management

Tutorials

Document Version: 20210112

Alibaba Cloud

Legal disclaimer

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

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

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

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Use RAM to manage permissions of O&M engineers

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

Prerequisites

An Alibaba Cloud account is created. To create an Alibaba Cloud account, visit the account registration page.

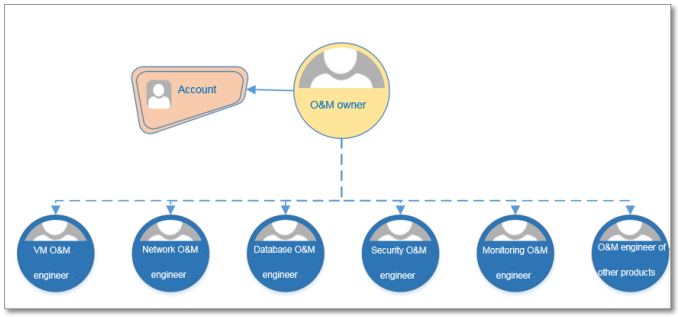
Context

A company has purchased multiple Alibaba Cloud services and deployed its application systems on the cloud. This results in the following O&M requirements:

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

Solution

The company can set an O&M owner, assign different O&M engineers to different O&M requirements, and then attach specified policies to these engineers.



Procedure

This section uses an example to describe how to set a RAM user as the database O&M owner. In this example, the RAM user is `alice@secloud.onaliyun.com`. The RAM user can then manage ApsaraDB for RDS and Data Transmission Service (DTS).

1. Log on to the RAM console with an Alibaba Cloud account.
2. Create a RAM user.
3. In the **User Logon Name/Display Name** column, find the RAM user.
4. Click **Add Permissions** in the **Actions** column. In the **Add Permissions** pane, the **Principal** field is automatically filled in.
5. In the **Authorization Policy Name** column, click `AliyunRDSFullAccess` and `AliyunDTSFullAccess`.
6. Click **OK**.
7. Click **Finished**.

> **Note** The following table describes the policies that you can use to grant other O&M permissions to the RAM user.

O&M owner	Policy	Description
O&M owner	AdministratorAccess	Permissions to manage all Alibaba Cloud resources.
VM O&M engineer	AliyunECSFullAccess	Permissions to manage Elastic Compute Service (ECS).
	AliyunESSFullAccess	Permissions to manage Auto Scaling (ESS).
	AliyunSLBFullAccess	Permissions to manage Server Load Balancer (SLB).
	AliyunNASFullAccess	Permissions to manage Apsara File Storage NAS.
	AliyunOSSFullAccess	Permissions to manage Object Storage Service (OSS).
	AliyunOTSFullAccess	Permissions to manage Tablestore.
Network O&M engineer	AliyunCDNFullAccess	Permissions to manage Alibaba Cloud CDN.
	AliyunCENFullAccess	Permissions to manage Cloud Enterprise Network (CEN).
	AliyunCommonBandwidthPackageFullAccess	Permissions to manage EIP Bandwidth Plan.
	AliyunEIPFullAccess	Permissions to manage Elastic IP Address (EIP).
	AliyunExpressConnectFullAccess	Permissions to manage Express Connect.
	AliyunNATGatewayFullAccess	Permissions to manage NAT Gateway.
	AliyunSCDNFullAccess	Permissions to manage Secure Content Delivery Network (SCDN).
	AliyunSmartAccessGatewayFullAccess	Permissions to manage Smart Access Gateway.
	AliyunVPCFullAccess	Permissions to manage Virtual Private Cloud (VPC).
	AliyunVPNGatewayFullAccess	Permissions to manage VPN Gateway.

O&M owner	Policy	Description
Database O&M engineer	AliyunRDSFullAccess	Permissions to manage ApsaraDB for RDS.
	AliyunDTSFullAccess	Permissions to manage Data Transmission Service (DTS).
Security O&M engineer	AliyunYundunFullAccess	Permissions to manage Alibaba Cloud Security.
Monitoring O&M engineer	AliyunActionTrailFullAccess	Permissions to manage ActionTrail.
	AliyunARMSFullAccess	Permissions to manage Application Real-Time Monitoring Service (ARMS).
	AliyunCloudMonitorFullAccess	Permissions to manage Cloud Monitor.
	ReadOnlyAccess	Permissions to read all Alibaba Cloud resources. This policy is optional.
	AliyunSupportFullAccess	Permissions to manage Ticket Management.

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

This topic describes how to use Resource Access Management (RAM) to limit the IP addresses that are used to access Alibaba Cloud resources. This ensures a higher level of data security.

Prerequisites

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, visit the account registration page.
- You have a basic knowledge of policy elements, structure, and syntax before you create a custom policy. For more information, see Policy elements and Policy structure and syntax.

Context

An enterprise has purchased multiple types of Alibaba Cloud resources, such as Elastic Compute Service (ECS) instances, ApsaraDB for RDS instances, Server Load Balancer (SLB) instances, and Object Storage Service (OSS) buckets. To ensure business and data security, this enterprise requires RAM users to access Alibaba Cloud resources only from the IP addresses of the enterprise intranet.

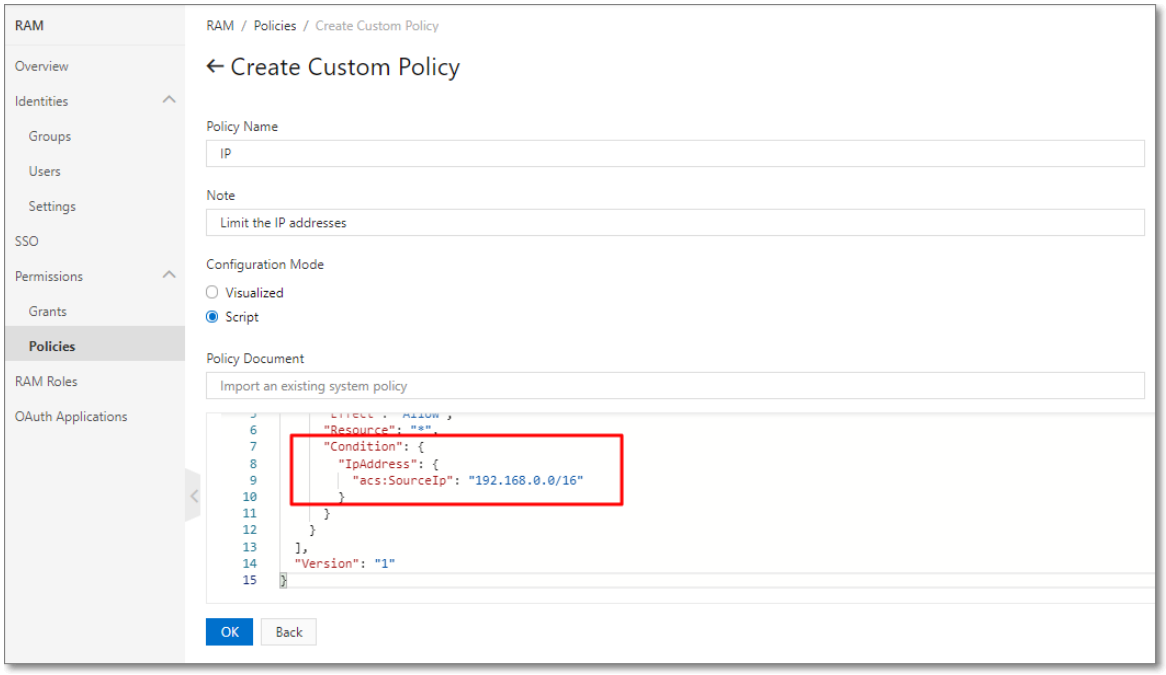
Solution

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

1. Create a RAM user. For more information, see Create a RAM user.
2. Create a custom policy. For more information, see Create a custom policy.
3. Attach the policy to the RAM user. For more information, see Grant permissions to a RAM user.

Create a custom policy

1. Log on to the RAM console. In the left-side navigation pane, click **Policies** under **Permissions**.
2. On the Policies page, click **Create Policy**.
3. On the Create Custom Policy page, set the **Policy Name** and **Note** parameters.
4. In the **Configuration Mode** section, select **Script**. Copy and paste the following sample script to the Policy Document section, and then edit the script based on your business requirements.



If the following policy is attached to a RAM user, the RAM user can access ECS instances only from IP addresses in the 192.168.0.0/16 CIDR block. This is because the value of the `acs:SourceIp` key in the `Condition` element is `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` element applies only to the actions that are specified in the policy. You can change the `192.168.0.0/16` CIDR block to an IP address or CIDR block in your intranet.

5. Click **OK**.

3.Use RAM to limit the time of access to Alibaba Cloud resources

This topic describes how to use Resource Access Management (RAM) to limit the time of access to Alibaba Cloud resources. This ensures a higher level of data security.

Prerequisites

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, visit the account registration page.
- You have a basic knowledge of policy elements, structure, and syntax before you create a custom policy. For more information, see Policy elements and Policy structure and syntax.

Context

An enterprise has purchased multiple types of Alibaba Cloud resources, such as Elastic Compute Service (ECS) instances, ApsaraDB for RDS instances, Server Load Balancer (SLB) instances, and Object Storage Service (OSS) buckets. To ensure business and data security, this enterprise requires RAM users to access Alibaba Cloud resources only during working hours.

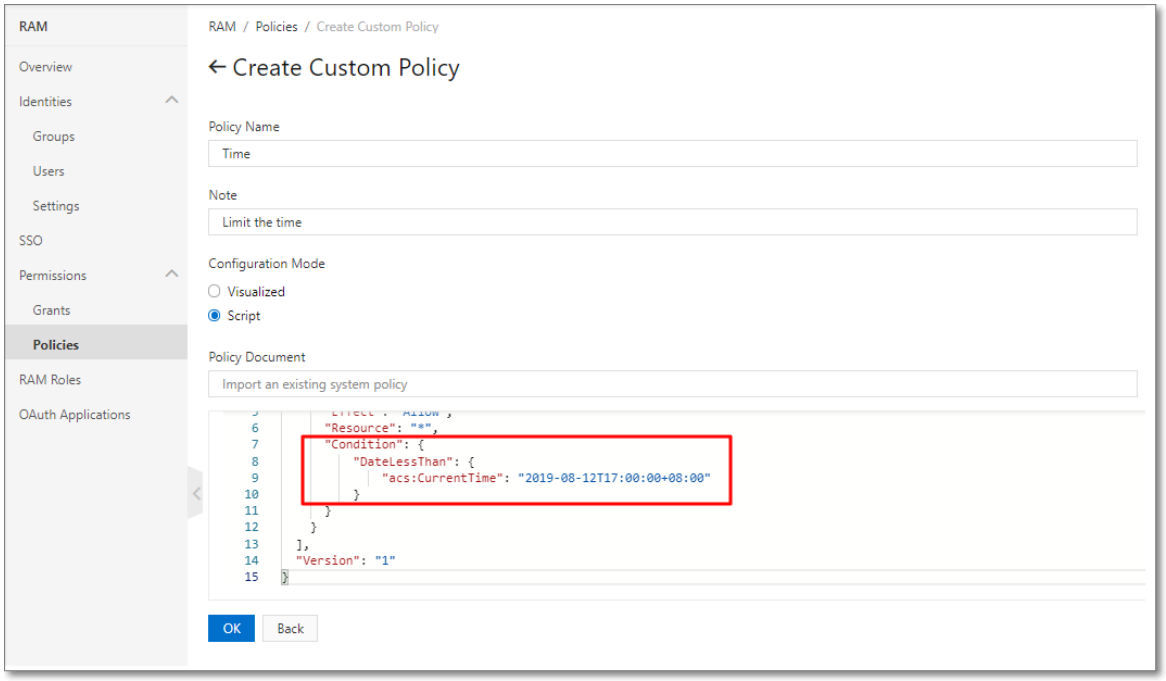
Solution

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

1. Create a RAM user. For more information, see Create a RAM user.
2. Create a custom policy. For more information, see Create a custom policy.
3. Attach the policy to the RAM user. For more information, see Grant permissions to a RAM user.

Create a custom policy

1. Log on to the RAM console. In the left-side navigation pane, click **Policies** under **Permissions**.
2. On the Policies page, click **Create Policy**.
3. On the Create Custom Policy page, set the **Policy Name** and **Note** parameters.
4. In the **Configuration Mode** section, select **Script**. Copy and paste the following sample script to the Policy Document section, and then edit the script based on your business requirements.



If the following policy is attached to a RAM user, the RAM user can access ECS instances only before 17:00 on August 12, 2019 (UTC+8). This is because the value of the `acs:CurrentTime` key in the `Condition` element is `2019-08-12T17:00:00+08:00`.

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

> **Note** The `Condition` element applies only to the actions that are specified in the policy. You can change the `2019-08-12T17:00:00+08:00` value based on your business requirements.

5. Click **OK**.

4.Use RAM to limit the methods of access to Alibaba Cloud resources

This topic describes how to use RAM to limit the methods of access to Alibaba Cloud resources. This ensures a higher level of data security.

Prerequisites

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, visit the account registration page.
- You have a basic knowledge of policy elements, structure, and syntax before you create a custom policy. For more information, see Policy elements and Policy structure and syntax.

Context

An enterprise has purchased multiple types of Alibaba Cloud resources, such as Elastic Compute Service (ECS) instances, ApsaraDB for RDS instances, Server Load Balancer (SLB) instances, and Object Storage Service (OSS) buckets. To ensure business and data security, this enterprise requires RAM users to access Alibaba Cloud resources only over HTTPS.

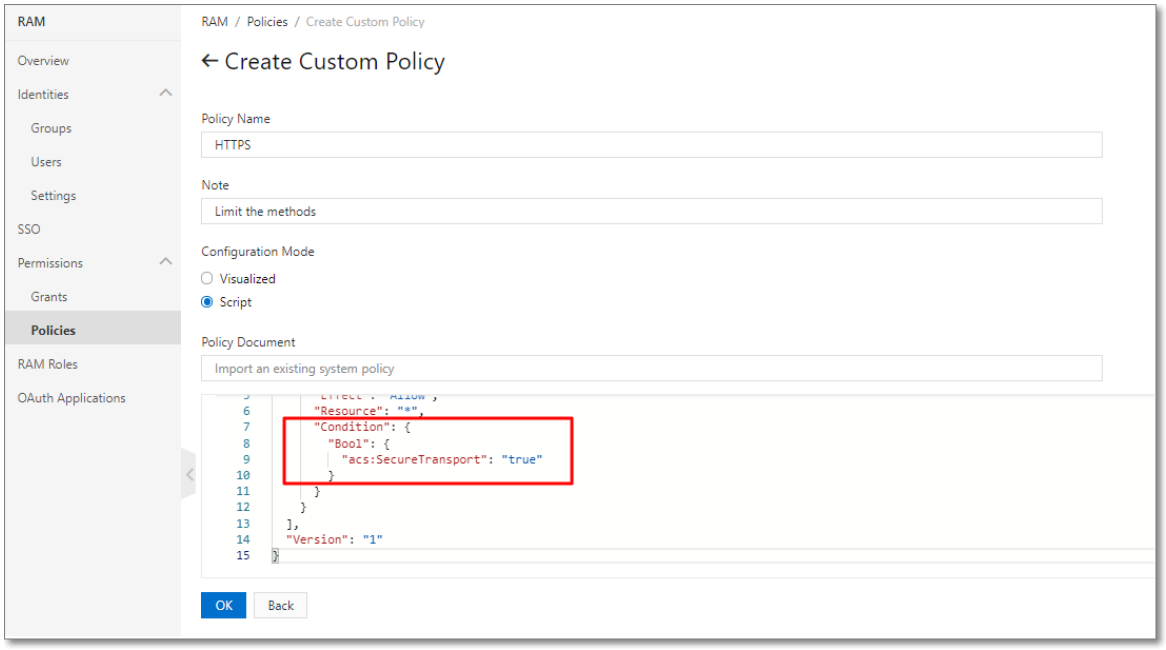
Solution

To allow a RAM user to access Alibaba Cloud resources only over HTTPS, create a custom policy and attach the policy to the RAM user.

1. Create a RAM user. For more information, see Create a RAM user.
2. Create a custom policy. For more information, see Create a custom policy.
3. Attach the policy to the RAM user. For more information, see Grant permissions to a RAM user.

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 Create Custom Policy page, set the **Policy Name** and **Note** parameters.
4. In the **Configuration Mode** section, select **Script**. Copy and paste the following sample script to the Policy Document section, and then edit the script based on your business requirements.



If the following policy is attached to a RAM user, the RAM user can access ECS instances only over HTTPS. This is because the value of the `acs:SecureTransport` key in the `Condition` element is `true`.

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

> **Note** The `Condition` element applies only to the actions that are specified in the policy. The valid values of the `acs:SecureTransport` key are `true` and `false`.

5. Click **OK**.

5.Allow only MFA-enabled RAM users to access cloud resources

This topic describes how to allow only Resource Access Management (RAM) users that have multi-factor authentication (MFA) enabled to access Alibaba Cloud resources, such as Elastic Compute Service (ECS) instances.

Prerequisites

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, visit the account registration page.
- A RAM user is created. For more information, see Create a RAM user.
- You have a basic knowledge of policy elements, structure, and syntax before you create a custom policy. For more information, see Policy elements and Policy structure and syntax.

Step 1: Enable MFA for a RAM user

1. Log on to the RAM console with the Alibaba Cloud account.
2. In the left-side navigation pane, click **Users** under **Identities**.
3. In the **User Logon Name/Display Name** column, click the name of the RAM user.
4. On the **Authentication** tab, click **Enable the Virtual MFA Device**.
5. On a mobile device, download and log on to the Google Authenticator app.
6. On the mobile device, open the app and scan the QR code.
7. Enter the two successive security codes that are obtained from the app and click **Enable**.

> **Note** For more information about how to use MFA, see Enable an MFA device for a RAM user.

Step 2: 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 Create Custom Policy page, set the **Policy Name** and **Note** parameters.
4. In the **Configuration Mode** section, select **Script**.
5. Copy and paste the following sample script to the Policy Document text box, and then edit the script based on your business requirements.

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

The policy indicates that only MFA-enabled RAM users can use the console to access ECS resources. This is because the value of the `acs:MFAPresent` key in the `Condition` element is `true`.

You can modify the policy to limit the access from RAM users to other cloud resources based on your business requirements.

6. Click **OK**.

Step 3: Attach the policy to the RAM user

1. In the left-side navigation pane, click **Users** under **Identities**.
2. In the **User Logon Name/Display Name** column, find the RAM user.
3. In the Actions column, click **Add Permissions**. In the Add Permissions pane, the Principal field is automatically filled in.
4. In the **Authorization Policy Name** column, click the custom policy that you created in Step 2.
5. Click **OK**.
6. Click **Complete**.

6.Use an STS token for authorizing a mobile app to access Alibaba Cloud resources

STS tokens are security credentials that have a limited validity period. This topic describes how to use a Security Token Service (STS) token of a Resource Access Management (RAM) role for authorizing a mobile app to access Alibaba Cloud resources.

Prerequisites

An Alibaba Cloud account is created. To create an Alibaba Cloud account, visit the account registration page.

Context

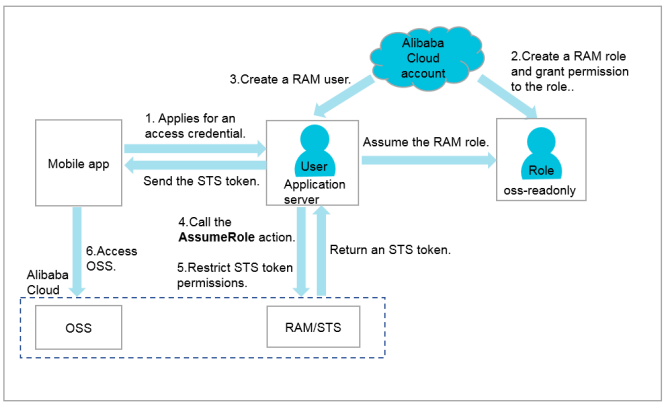
An enterprise has developed a mobile app and purchased Object Storage Service (OSS). The mobile app runs on mobile devices. These mobile devices are not controlled by the enterprise. The enterprise must grant the necessary permissions to the mobile app. The mobile app can then upload data to and download data from OSS.

The enterprise has the following requirements:

- Direct data transmission: The mobile app directly uploads data to or downloads data from OSS. The application server of the enterprise does not need to transfer data between the mobile app and OSS.
- Security control: AccessKey pairs are not saved on mobile devices. Mobile devices are controlled by app users and cannot provide trusted operating environments.
- Risk control: Security risks are minimized. During direct access to OSS, each app client is authorized based on the principle of least privilege and the access duration is under strict control.

Solution

Before a mobile app directly uploads data to or downloads data from OSS, the mobile app requests an STS token from the application server. After the application server receives the request, the server calls the AssumeRole STS API operation as a RAM user. If the call succeeds, the application receives an STS token and forwards the STS token to the mobile app. The mobile app can then use the STS token to access OSS.



1. The mobile app requests an STS token from the application server.

2. The enterprise uses its Alibaba Cloud account to create a RAM role and grant the necessary permissions to the role. For more information, see Create a RAM role and grant the necessary permissions to the role.
3. The enterprise uses its Alibaba Cloud account to create a RAM user for the application server and allows 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 AssumeRole STS API operation to obtain an STS token of the RAM role. For more information, see Obtain an STS token of the RAM role.
5. The application server can request an STS token whose permissions are fewer than those that are granted to the RAM role. In this way, the application server controls the access from the mobile app to OSS. For more information, see Request an STS token whose permissions are fewer than those of the RAM role.
6. The mobile app uses the STS token to directly 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 the necessary permissions to the role

The ID of the Alibaba Cloud account that is used by the enterprise in this section is `123456789012****`.

1. The enterprise uses its Alibaba Cloud account to create a RAM role named `oss-readonly`. **Alibaba Cloud Account** is selected as the trusted entity type.

   > **Note** When the RAM role is created, **Current Alibaba Cloud Account** is selected as the trusted account. This ensures that only RAM users under the account can assume the RAM role.

   For more information, see Create a RAM role for a trusted Alibaba Cloud account.

   After the RAM role is created, the enterprise can view the information of the role on the basic information page.

   - In this example, the Alibaba Cloud Resource Name (ARN) of the RAM role is `acs:ram::123456789012****:role/oss-readonly`.
   - The following policy is attached to the RAM role:

     > **Note** This policy indicates that only RAM users under the Alibaba Cloud account of the enterprise can assume the RAM role.

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

2. The enterprise uses its Alibaba Cloud account to attach the `AliyunOSSReadOnlyAccess` policy (OSS read-only permission) to the RAM role `oss-readonly`.

   For more information, see Grant permissions to a RAM role.

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

1. The enterprise uses its Alibaba Cloud account to create a RAM user named `appserver`.

   For more information, see Create a RAM user.

2. The enterprise uses its Alibaba Cloud account to attach the `AliyunSTSAssumeRoleAccess` policy to the RAM user. The RAM user can then assume the RAM role.

   For more information, see Grant permissions to a RAM user.

Obtain an STS token of the RAM role

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

   > **Note** The AccessKey pair of the RAM user rather than the Alibaba Cloud account must be used.

   The following example shows how to use Alibaba Cloud CLI to call the AssumeRole operation:

```
$ aliyuncli sts AssumeRole --RoleArn acs:ram::123456789012****:role/oss-readonly --RoleSessionName client-001
{
  "AssumedRoleUser": {
    "AssumedRoleId": "391578752573****:client-001",
    "Arn": "acs:ram::123456789012****:role/oss-readonly/client-001"
  },
  "Credentials": {
    "AccessKeySecret": "93ci2umK1QKNEja6WGqi1Ba7Q2Fv9PwxZqtVF2Vy****",
    "SecurityToken": "********",
    "Expiration": "2016-01-13T15:02:37Z",
    "AccessKeyId": "STS.F13GjskXTjk38dBY6YxJt****"
  },
  "RequestId": "E1779AAB-E7AF-47D6-A9A4-53128708B6CE"
}
```

> **Note** In this example, the returned STS token has all permissions of the RAM role `oss-readonly` because the `Policy` parameter is unspecified. The application server can also request an STS token whose permissions are fewer than those of the RAM role. For more information, see Request an STS token whose permissions are fewer than those of the RAM role.

2. The STS service sends the STS token to the application server. The STS token contains the following elements: `AccessKeyId`, `AccessKeySecret`, and `SecurityToken`.

> **Note** The STS token (`SecurityToken`) is valid only for a short period of time. If the mobile app requires access to OSS for a long period of time, the application server can request a new STS token at a regular basis, for example, every 1,800 seconds.

Request an STS token whose permissions are fewer than those of the RAM role

In practice, we recommend that you specify the `Policy` parameter to grant the STS token fewer permissions than those that are granted to the RAM role. Ensure that the principle of least privilege is applied. The following example shows how to specify the Policy parameter.

In this example, the returned STS token has only the permissions to access objects that match the `sample-bucket/2015/01/01/*.jpg` pattern.

```
$ aliyuncli sts AssumeRole --RoleArn acs:ram::123456789012****:role/oss-readonly --RoleSessionName client-002 --Policy "{\"Version\":\"1\", \"Statement\": [{\"Effect\":\"Allow\", \"Action\":\"oss:GetObject\", \"Resource\":\"acs:oss:*:*:sample-bucket/2015/01/01/*.jpg\"}]}"
{
  "AssumedRoleUser": {
    "AssumedRoleId": "391578752573****:client-002",
    "Arn": "acs:ram::123456789012****:role/oss-readonly/client-002"
  },
  "Credentials": {
    "AccessKeySecret": "28Co5Vyx2XhtTqj3RJgdud4ntyzrSNdUvNygAj7x****",
    "SecurityToken": "********",
    "Expiration": "2016-01-13T15:03:39Z",
    "AccessKeyId": "STS.FJ6EMcS1JLZgAcBJSTDG1****"
  },
  "RequestId": "98835D9B-86E5-4BB5-A6DF-9D3156ABA567"
}
```

Note The default and maximum validity period of the STS token is 3,600 seconds. The enterprise can specify the `DurationSeconds` parameter to shorten the validity period of the STS token.

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 example shows how to use Alibaba Cloud CLI and the STS token to access an OSS object:

   ```
   The syntax that is used to specify the STS token: aliyuncli oss Config --host  --accessid  --accesskey  --sts_token
   $ aliyuncli oss Config --host oss.aliyuncs.com --accessid STS.FJ6EMcS1JLZgAcBJSTDG1**** --accesskey 28Co5Vyx2XhtTqj3RJgdud4ntyzrSNdUvNygAj7x**** --sts_token CAESnQMIARKAASJgnzMzlXVyJn4KI+FsysaIpTGm8ns8Y74HVEj0pOevO8ZWXrnnkz4a4rBEPBAdFkh3197GUsprujsiU78FkszxhnQPKkQKcyvPihoXqKvuukrQ/Uoudk31KAJEz5o2EjlNUREcxWjRDRSISMzkxNTc4NzUyNTczOTcyODU0KgpjbGllbnQtMDAxMKmZxIHBKjoGUnNhTUQ1Qn8KATEaegoFQWxsb3cSJwoMQWN0aW9uRXF1YWxzEgZBY3Rpb24aDwoNb3NzOkdldE9iamVjdBJICg5SZXNvdXJjZUVxdWFscxIIUmVzb3VyY2UaLAoqYWNzOm9zczoqOio6c2FtcGxlLWJ1Y2tldC8yMDE1LzAxLzAxLyouanBnSgU0MzI3NFIFMjY4NDJaD0Fzc3VtZWRSb2xlVXNlcmAAahIzOTE1Nzg3NTI1NzM5NzI4NTRyCWVjcy1hZG1pbnjgxt7Cj/bo****
   Access OSS:
   $ aliyuncli oss Get oss://sample-bucket/2015/01/01/grass.jpg grass.jpg
   ```

Related information

- Set up direct data transfer for mobile apps
- Set up upload callback for mobile apps
- Access OSS with a temporary access credential provided by STS

7.Use RAM for authorizing applications to access Alibaba Cloud resources

This topic describes how to use a temporary STS token of a RAM role for authorizing applications to access Alibaba Cloud resources.

Prerequisites

An Alibaba Cloud account is created. To create an Alibaba Cloud account, visit the account registration page.

Context

An enterprise has purchased Elastic Compute Service (ECS) instances and wants to deploy its applications on these ECS instances.

To allow the applications to use AccessKey pairs for calling API operations of other Alibaba Cloud services, the enterprise can use one of the following methods:

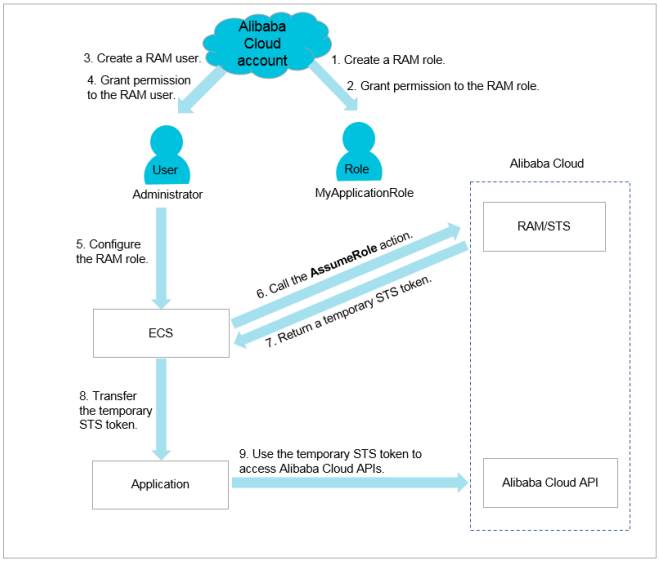
- Include the AccessKey pairs in application code.
- Save the AccessKey pairs in the configuration files of the applications.

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

- AccessKey pair disclosure: If AccessKey pairs are stored in the ECS instances in plaintext, the AccessKey pairs may be disclosed by the sharing of snapshots and images or by ECS instances created from images.
- Complex O&M: The AccessKey pairs are stored in the ECS instances. If the AccessKey pairs are changed due to AccessKey pair rotations or user identity changes, all ECS instances and images must be updated and redeployed. This increases the difficulty in managing the ECS instances and images.

Solution

To resolve the preceding issues, the enterprise can use an integrated feature of RAM to control the permissions of ECS instances. This feature allows the enterprise to create a RAM role for each ECS instance and grant the required permissions to each RAM role. The applications can use the temporary STS token of the corresponding RAM role to call Alibaba Cloud API operations.



Procedure

1. The enterprise creates a RAM role named MyApplicationRole.

   > **Note** **Alibaba Cloud Service** is selected as the trusted entity and **Elastic Compute Service** is selected as the trusted service. This allows ECS to assume the RAM role and then access Alibaba Cloud resources.

   For more information, see Create a RAM role for a trusted Alibaba Cloud service.

2. The enterprise grants the required permissions to the RAM role.

   For more information, see Grant permissions to a RAM role.

   > **Note** If the temporary STS token lacks specific permissions, the enterprise must assign required policies to the RAM role. After the policies are assigned, the permissions that are attached to the temporary STS token take immediate effect without the need to restart the corresponding ECS instance.

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

   For more information, see Create a RAM user.

4. The enterprise grants the required permissions to the RAM user.
   - If the RAM user has the same responsibilities as an administrator, the `AdministratorAccess` permission policy must be attached to the RAM user.
   - If the responsibilities of the RAM user are different from those of an administrator, the permission on the `PassRole` operation must be granted to the RAM user.

     The enterprise creates a custom policy in the RAM console and attaches the custom policy to the RAM user. The custom policy is as follows:

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

> **Note**
>
> - Only authorized RAM users can create RAM roles for ECS instances. This prevents against abuse of RAM roles.
> - When a RAM user who has access only to ECS attempts to create an ECS instance and configure a RAM role, ECS checks whether the RAM user has the `ram:PassRole` permission on the RAM role. If the RAM user does not have the permission, the ECS instance fails to be created.

For more information, see Grant permissions to a RAM user.

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

   > **Note** The STS service 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 more information, see Use an instance RAM role by calling API operations.
7. STS returns the temporary STS token to ECS.
8. ECS includes the temporary STS token in the metadata of the ECS instance, and sends the metadata to the application deployed on the ECS instance.
   - In a Linux system, applications can query the instance metadata to obtain a temporary STS token and its validity period. For more information, see Use RAM roles to access other Alibaba Cloud services.

     Sample request:

     ```
     $ curl http://100.100.100.200/latest/meta-data/ram/security-credentials/MyApplicationRole
     ```

     Sample response:

```
[root@local ~]# curl http://100.100.100.200/latest/meta-data/ram/security-credentials/MyApplicationRole
{
"AccessKeyId" : "STS.J8XXXXXXXXX4",
"AccessKeySecret" : "9PjfXXXXXXXXBf2XAW",
"Expiration" : "2017-06-09T09:17:19Z",
"SecurityToken" : "CAIXXXXXXXXXXwmBkleCTkyI+",
"LastUpdated" : "2017-06-09T03:17:18Z",
"Code" : "Success"
}
```

- If the applications use an Alibaba Cloud SDK, the SDK can obtain the temporary STS token of the RAM role from the ECS instance metadata. No AccessKey pair-related configurations are required in the SDK. For more information, see Configure RamRole to achieve non-AK access to ECS instances.

  > **Note** The applications can call Alibaba Cloud API operations when the temporary STS token is valid. The temporary STS token expires after one hour. Before the temporary STS token expires, it is refreshed by ECS.

9. The applications use the temporary STS token to call Alibaba Cloud API operations.

> **Note** Applications deployed on other Alibaba Cloud services such as Function Compute and MaxCompute can also use temporary STS tokens of RAM roles to call Alibaba Cloud API operations.

8.Use a RAM role to grant permissions across Alibaba Cloud accounts

This topic describe how to use a Resource Access Management (RAM) role to grant permissions across Alibaba Cloud accounts. Two enterprises (Enterprise A and Enterprise B) are used as examples. To authorize Enterprise B to access specified resources of Enterprise A, Enterprise A can create and assign a RAM role to Enterprise B. Then, Enterprise B can assume the RAM role and access the specified resources.

Prerequisites

An alias is set for your Alibaba Cloud account. For more information, see Manage the default domain name.

Context

An enterprise (Enterprise A) has purchased multiple types of Alibaba Cloud resources, such as ECS instances, RDS instances, SLB instances, and OSS buckets. Enterprise A wants to authorize Enterprise B to access specified resources of Enterprise A.

Enterprise A has the following requirements:

- Enterprise A only serves as a cloud resource owner. Enterprise A can authorize Enterprise B to maintain, monitor, and manage specified cloud resources of Enterprise A.
- If an employee joins or leaves Enterprise B, Enterprise B does not need to change permissions. Enterprise B can grant fine-grained permissions on cloud resources of Enterprise A to its RAM users (employees or applications).
- If the agreement between Enterprise A and Enterprise B ends, Enterprise A can revoke the permissions from Enterprise B based on business requirements.

Solution

In this example, Enterprise A needs to authorize employees of Enterprise B to manage ECS resources of Enterprise A. Enterprise A has an Alibaba Cloud account named Account A and Enterprise B has an Alibaba Cloud account named Account B.

- The ID of Account A is `123456789012****` and the account alias is `company-a`.
- The ID of Account B is `134567890123****` and the account alias is `company-b`.

1. Enterprise A uses Account A to create a RAM role, grants the required permissions to the RAM role, and then authorizes Account B to assume this role.

   For more information, see Grant permissions across Alibaba Cloud accounts.

2. If an employee (a RAM user) under Account B needs to assume this role, Account B can grant the required permissions to the RAM user. Then, the RAM user assumes the RAM role to access the resources of Account A.

   For more information, see Access resources across Alibaba Cloud accounts.

3. If the agreement between Enterprise A and Enterprise B ends, Enterprise A can revoke the permissions from Account B. Then, all RAM users of Account B no longer have the permissions of the RAM role.

For more information, see Revoke permissions across Alibaba Cloud accounts.

Grant permissions across Alibaba Cloud accounts

1. Enterprise A uses Account A to create a RAM role named `ecs-admin`. **Alibaba Cloud Account** is selected as the trusted entity type.

   > **Note** When the RAM role is created, **Other Alibaba Cloud Account** is selected and `1345678901234567****` is specified as the trusted Alibaba Cloud account. This ensures that RAM users under Account B can assume the RAM role.

   For more information, see Create a RAM role for a trusted Alibaba Cloud account.

   After the RAM role is created, Enterprise A can view information about the RAM role on the basic information page.

   - In this example, the Alibaba Cloud Resource Name (ARN) of the RAM role is `acs:ram::1234567890123****:role/ecs-admin`.
   - The following policy is attached to the RAM role:

     > **Note** This policy indicates that RAM users of Account B can assume the RAM role.

     ```
     {
     "Statement": [
     {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
       "RAM": [
        "acs:ram::134567890123****:root"
       ]
      }
     }
     ],
     "Version": "1"
     }
     ```

2. Enterprise A uses Account A to attach the `AliyunECSFullAccess` policy to the RAM role `ecs-admin`.

   For more information, see Grant permissions to a RAM role.

3. Enterprise B uses Account B to create a RAM user named `Alice`.

   For more information, see Create a RAM user.

4. Enterprise B uses Account B to set the logon password of the RAM user to `123456****` and attach the `AliyunSTSAssumeRoleAccess` system policy to the RAM user. This allows the RAM user to assume the RAM role.

For more information, see Grant permissions to a RAM user.

Access resources across Alibaba Cloud accounts

After Enterprise A uses Account A to grant required permissions to Account B, the RAM user `Alice` of Account B can access ECS resources of Account A by assuming the RAM role. An employee of Enterprise B can perform the following steps to assume the RAM role as a RAM user:

1. Log on to the RAM console as the RAM user named Alice.

   > **Note** On the logon page, you must enter the account alias `company-b`, username `Alice`, and password `123456****`.

   For more information, see Log on to the console as a RAM user.

2. Move the pointer over the profile picture and click **Switch Role**.

   > **Note** On the page that appears, you must enter the account alias `company-a` and role name `ecs-admin`.

   For more information, see Assume a RAM role.

Revoke permissions across Alibaba Cloud accounts

Enterprise A can use Account A to revoke the permission to assume the RAM role `ecs-admin` from Account B. Enterprise A can perform the following steps to revoke the permission to assume the RAM role:

1. Log on to the RAM console with Account A.
2. In the left-side navigation pane, click **RAM Roles**.
3. In the RAM Role Name column, click the RAM role `ecs-admin`.
4. On the **Trust Policy Management** tab, click **Edit Trust Policy**. In the pane that appears, delete `"acs:ram::134567890123****:root"`.

   > **Note** Enterprise A can also use Account A to delete the RAM role **ecs-admin**. This revokes the permissions of the RAM role from Account B. Before the RAM role is deleted, the policies attached to the RAM role must be detached. For more information, see Remove permissions from a RAM role.

9.Use RAM to create and authorize resource groups

This topic describes how to use RAM to create and authorize resource groups in Alibaba Cloud. After you create and authorize resource groups, you can manage your own members, permissions, and resources by group.

Prerequisites

An Alibaba Cloud account is created. To create an Alibaba Cloud account, visit the account registration page.

Context

A gaming company is developing three gaming projects. Each project requires multiple types of cloud resources. The company has an Alibaba Cloud account and more than 100 Elastic Compute Service (ECS) instances under this account.

The requirements of the company are as follows:

- Independent project management: Project managers can manage their own project members and the permissions that the project members require to access cloud resources.
- Separate bills: The financial department of the company requires that each project receives separate bills.
- A shared bottom-layer network: The company requires a shared bottom-layer network for its cloud resources.

The company has the following optional solutions:

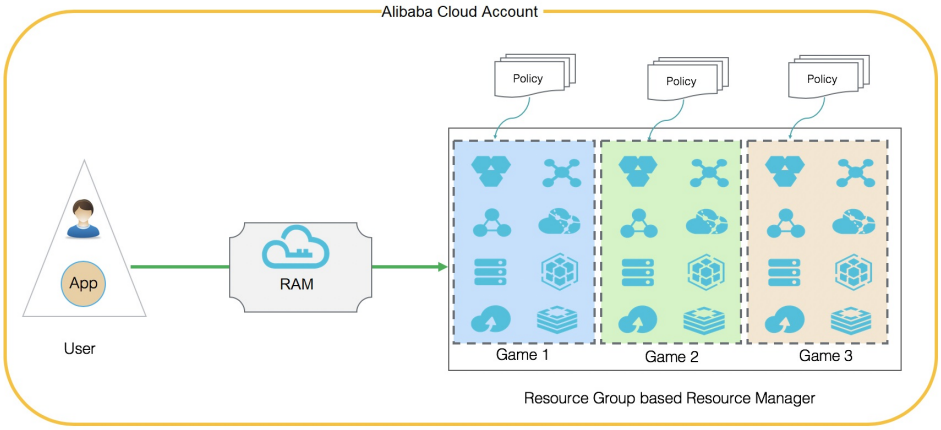
- Multi-account solution
  - This solution supports independent project management. The company creates three Alibaba Cloud accounts (one account for each project) and assigns one project manager for each account. Then, project managers can manage their own project members and access permissions of each member.
  - This solution supports separate bills. The accounts receive separate bills by default. The consolidated billing feature provided by Alibaba Cloud for multiple accounts can be used to consolidate the bills and invoices.
  - This solution does not support a shared bottom-layer network. The resources of different accounts are isolated between different networks. Virtual private clouds (VPCs) under the accounts can be connected through peering connections. However, this incurs higher management costs.
- Single-account solution (with tagged resources)
  - This solution does not support independent project management. The company can tag its cloud resources by group, but project managers cannot manage their own members and access permissions of each member.
  - This solution supports separate bills. The company can tag its cloud resources by project. Then, each project can receive separate bills.

- This solution supports a shared bottom-layer network. The company can use tag-based RAM policies to authorize RAM users to access a group of resources. The company does not need to pay for peering connections established between different networks because these resources belong to the same account.

- Resource group-based management solution
  - This solution supports independent project management. Each resource group has an administrator. Administrators can manage their own group members and access permissions of each member.
  - This solution supports separate bills. Alibaba Cloud provides the consolidated billing feature that allows resource groups to receive separate bills.
  - This solution supports a shared bottom-layer network. Resource groups belong to the same account and can share a VPC. The cost of peering connections is eliminated.

Solution

The resource group-based management solution can meet all requirements of the company. By using this solution, the company only needs to use one Alibaba Cloud account to create three resource groups that correspond to the three projects.



1. Create three RAM users: `alice@secloud.onaliyun.com`, `bob@secloud.onaliyun.com`, and `charlie@secloud.onaliyun.com`.

   For more information, see Create a RAM user.

   > **Note** The following steps use the RAM user Alice as an example. The steps demonstrate how to set a RAM user as a resource group administrator.

2. Log on to the Resource Management console.
3. In the left-side navigation pane, click **Resource Group**. On the **Resource Group** page, click **Create Resource Group**.
4. Specify the **Resource Group Name** and **Display Name** parameters, and then click **OK**.

   > **Note** Create three resource groups: Game1, Game2, and Game3.

5. Find the target resource group, and click **Manage Permission** in the **Actions** column.
6. On the **Permissions** tab, click **Grant Permission**.

7. In the **Principal** field, enter Alice, and then select the RAM user from the auto-complete results.
8. In the **Authorization Policy Name** column, click `AdministratorAccess`.
9. Click **OK**.
10. Click **Complete**.

> **Note** Repeat the preceding steps to set Bob and Charlie as resource group administrators.

Result

Alice, Bob, and Charlie are the respective resource group administrators of Game1, Game2, and Game3. The administrators have the following permissions:

- After an administrator logs on to the ECS console, the administrator can view the respective resource group. The administrator can also create and manage ECS instances.
- After an administrator logs on to the Resource Management console, the administrator can add RAM users and grant resource access permissions to RAM users.

10.Use tags to grant access to a group of ECS instances

This topic describes how to use tags to grant Resource Access Management (RAM) users access to a group of Elastic Compute Service (ECS) instances. After authorization, RAM users can view and manage only the tagged resources.

Prerequisites

An Alibaba Cloud account is created. To create an Alibaba Cloud account, visit the account registration page.

Context

Assume that you have 10 ECS instances. You want to authorize the developer team to manage five instances and the operator team to manage the other five. However, you want each team to view and manage only the authorized instances.

In this case, you must create two RAM user groups that are named developer and operator.

You must create two RAM custom policies that are named policyForDevTeam and policyForOpsTeam.

You must create the following tags:

- A tag that is attached to five ECS instances. The tag key is team and the tag value is dev.
- A tag that is attached to the other five ECS instances. The tag key is team and the tag value is ops.

Procedure

1. Log on to the ECS console by using your Alibaba Cloud account. In the ECS console, create tags and attach the tags to your ECS instances.
   i. Log on to the ECS console.
   ii. In the upper-left corner, select a region.
   iii. In the left-side navigation pane, choose **Instances & Images > Instances**. On the Instances page, find the ECS instance to which you want to attach a tag.
   iv. Move the pointer over the icon in the **Tag** column, and click **Edit Tags** in the tooltip that appears.
   v. Click **Create**.
   vi. Enter the tag key and tag value in the fields that appear, and then click **Confirm**.

   Repeat the preceding steps to attach the `team:dev` tag to five ECS instances and attach the `team:ops` tag to the other five ECS instances.
2. Log on to the RAM console by using your Alibaba Cloud account and create two user groups that are named developer and operator.

   For more information, see Create a RAM user group.
3. Create RAM users and add each RAM user to the corresponding user group.

   For more information, see Create a RAM user and Add a RAM user to a RAM user group.
4. Create two custom policies that are named policyForDevTeam and policyForOpsTeam. Attach the

policyForDevTeam policy to the developer group and attach the policyForOpsTeam policy to the operator group.

For more information, see Create a custom policy and Grant permissions to a RAM user group.

> **Note** After you attach a policy to a user group, the RAM users in the group have the permissions that are included in the policy.

The policyForDevTeam policy is defined by using the following script:

```
{
  "Statement": [
  {
    "Action": "ecs:*",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "ecs:tag/team": "dev"
      }
    }
  },
  {
    "Action": "ecs:DescribeTag*",
    "Effect": "Allow",
    "Resource": "*"
  }
  ],
  "Version": "1"
}
```

The policyForOpsTeam policy is defined by using the following script:

```
{
  "Statement": [
  {
    "Action": "ecs:*",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "ecs:tag/team": "ops"
      }
    }
  },
  {
    "Action": "ecs:DescribeTag*",
    "Effect": "Allow",
    "Resource": "*"
  }
  ],
  "Version": "1"
}
```

Each policy consists of two statements:

- The statement that includes the `"Action": "ecs:*"` `condition` grants RAM users access to the ECS instances to which the `team:dev` or `team:ops` tag is attached.
- The statement that includes `"Action": "ecs:DescribeTag*"` authorizes RAM users to view all ECS tags. After a RAM user logs on to the ECS console, all existing tags are displayed. The RAM user must select an authorized tag key and tag value to view the instances to which the selected tag is attached.

Verify the authorization

1. Log on to the ECS console as a RAM user.
2. In the upper-left corner, select the region.
3. In the left-side navigation pane, choose **Instances & Images > Instances**.
4. On the Instances page, click **Tags** next to the search box.
5. Move the pointer over a tag key. The list of tag values is displayed. Select a tag value. Then, only the ECS instances to which the tag is attached are displayed in the instance list. For example, a RAM user in the developer user group can view the list of ECS instances to which the `team:dev` tag is attached.

Related operations

You can use the procedure that is described in this topic to grant access to other ECS instances by group. The ECS resources include block storage devices, snapshots, images, security groups, elastic network interfaces (ENIs), dedicated hosts, and Secure Shell (SSH) key pairs.

11.Use tags to grant access to a group of ApsaraDB for RDS instances

This topic describes how to use tags to grant Resource Access Management (RAM) users access to a group of ApsaraDB for RDS instances. After authorization, RAM users can view and manage only the tagged resources.

Prerequisites

An Alibaba Cloud account is created. To create an Alibaba Cloud account, visit the account registration page.

Scenario

Assume that you have 10 ApsaraDB for RDS instances. You want to authorize the developer team to manage five instances and the operator team to manage the other five. However, you want each team to view and manage only the authorized instances.

Procedure

The procedure for using tags to grant access to ApsaraDB for RDS instances by group is the same as that for using tags to grant access to ECS instances by group. For more information, see Use tags to grant access to a group of ECS instances.

However, you must use a custom policy that includes the permissions on ApsaraDB for RDS instances. The following script is an example policy that you can use to authorize the developer team:

```
{
 "Statement": [
  {
   "Action": "rds:*",
   "Effect": "Allow",
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "rds:ResourceTag/team": "dev"
    }
   }
  },
  {
   "Action": "rds:DescribeTag*",
   "Effect": "Allow",
   "Resource": "*"
  }
 ],
 "Version": "1"
}
```

The policy consists of two statements:

- The statement that includes the `"Action": "rds:*"` `condition` grants RAM users access to the ApsaraDB for RDS instances to which the `team:dev` tag is attached. The `Condition` key in this statement is `rds:ResourceTag`.
- The statement that includes the `"Action": "rds:DescribeTag*"` condition authorizes RAM users to view all tags. After a RAM user logs on to the ApsaraDB for RDS console, all existing tags are displayed. The RAM user must select the value of an authorized tag key to view the instances to which the tag is attached.

FAQ

If permission errors occur after you use tags to grant RAM users access to a group of ApsaraDB for RDS instances, check whether the following conditions are met:

- The tag is attached to the instances.
- The tag keys and values that are specified in the policies have the same keys and values as the tags that are attached to the instances.

  > **Note** The keys and values of tags in ApsaraDB for RDS cannot contain uppercase letters. If you enter uppercase letters when you add a tag, ApsaraDB for RDS converts the uppercase letters into lowercase letters.

- The required policy is attached to the RAM users that are logged on.

- The region selected in the ApsaraDB for RDS console is the region to which the instances belong.
- The corresponding tag value to filter the instances is selected.

> **Note** If a RAM user logs on to the ApsaraDB for RDS console, the console returns the message "You do not have permission to perform this operation." Close the error message. This message appears because all ApsaraDB for RDS instances are displayed by default. However, the RAM user is not authorized to view all ApsaraDB for RDS resources.

12.Use RAM to manage ECS permissions

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

Prerequisites

- An Alibaba Cloud account is created. If not, create one before proceeding. To create an Alibaba Cloud account, click account registration page.
- You have a basic understanding of the following common policies:
  - AliyunECSFullAccess: grants a RAM user the permissions to manage ECS instances.
  - AliyunECSReadOnlyAccess: grants a RAM user the read-only permission on ECS instances.
- You have a basic understanding of ECS permissions. For more information, see Authentication rules.

Attach a custom policy to a RAM user

1. Create a custom policy based on ECS authorization examples.

   For more information, see Create a custom policy.
2. On the **Policies** page, click the name of the policy.
3. On the **References** tab, click **Grant Permission**.
4. In the dialog box that appears, enter the name or ID of the RAM user in the **Principal** field. Then, select the RAM user from the auto-complete results.
5. Click **OK**. Click **Finished**.

> **Note** For more information, see Grant permissions to a RAM user and Grant permissions to a RAM user group.

ECS authorization examples

- Example 1: Authorize a RAM user to manage two specified ECS instances.

  To authorize a RAM user to manage the ECS instances i-001 and i-002 in your Alibaba Cloud account, use the following sample script:

```
{
 "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 ECS instances but can manage only the specified two ECS instances.
> - The `Describe*` element is required in the policy. Otherwise, the authorized RAM user cannot view instances in the console. However, the RAM user can manage the two specified ECS instances by calling API operations or using the CLI or SDK.

- Example 2: Authorize a RAM user to view ECS instances in the China (Qingdao) region, but do not allow the RAM user to view information about disks and snapshots.

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

> **Note** You can grant ECS permissions to the RAM user by region and resource type. If you want to authorize a RAM user to view ECS instances in another region, you can replace `cn-qingdao` in `Resource` with the ID of the region. For a list of region IDs, see .

- Example 3: 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 RAM user. 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:CreateSnapshot",
   "Effect": "Allow",
   "Resource": [
    "acs:ecs:*:*:disk/dist-01",
    "acs:ecs:*:*:snapshot/*"
   ]
  },
  {
   "Action": [
    "ecs:Describe*"
   ],
   "Effect": "Allow",
   "Resource": "*"
  }
 ],
 "Version": "1"
}
```

13.Use RAM to manage OSS permissions

This topic describes how to manage Object Storage Service (OSS) permissions of a RAM user by using RAM. In the RAM console, you can create custom policies and attach them to a RAM user.

Prerequisites

- An Alibaba Cloud account is created. If not, create one before proceeding. To create an Alibaba Cloud account, click account registration page.
- You have a basic understanding of the following common system policies:
  - AliyunOSSFullAccess: grants a RAM user the permissions to manage OSS buckets.
  - AliyunOSSReadOnlyAccess: grants a RAM user the read-only permission on OSS buckets.
- You have a basic understanding of OSS permissions. For more information, see Overview.

Attach a custom policy to a RAM user

1. Create a custom policy based on OSS authorization examples.

   For more information, see Create a custom policy.
2. On the **Policies** page, click the name of the policy.
3. On the **References** tab, click **Grant Permission**.
4. In the dialog box that appears, enter the name or ID of the RAM user in the **Principal** field. Then, select the RAM user from the auto-complete results.
5. Click **OK**. Click **Finished**.

> **Note** For more information, see Grant permissions to a RAM user and Grant permissions to a RAM user group.

OSS authorization examples

- Example 1: Authorize a RAM user to manage a bucket named `myphotos`.

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

- Example 2: Authorize a RAM user to list and read resources in a bucket.
  - To authorize a RAM user to list and read resources in a bucket named `myphotos` by using the OSS SDK or OSS CLI, use the following sample script:

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

- To authorize a RAM user to use the OSS console to list and read resources in a bucket named myphotos, use the following sample script:

  > **Note** When a RAM user logs on to the OSS console, the `ListBuckets`, `GetBucketAcl`, and `GetObjectAcl` API operations are called to check whether the bucket is public.

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
            "oss:ListBuckets",
            "oss:GetBucketStat",
            "oss:GetBucketInfo",
            "oss:GetBucketTagging",
            "oss:GetBucketAcl"
            ],
      "Resource": "acs:oss:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "oss:ListObjects",
        "oss:GetBucketAcl"
      ],
      "Resource": "acs:oss:*:*:myphotos"
    },
    {
      "Effect": "Allow",
      "Action": [
        "oss:GetObject",
        "oss:GetObjectAcl"
      ],
      "Resource": "acs:oss:*:*:myphotos/*"
    }
  ]
}
```

- Example 3: Authorize a RAM user to use a specified IP address to access an OSS bucket.

- Add an IP address condition to the `Allow` element. This allows a RAM user to read data from the `myphotos` bucket by using an IP address in the `192.168.0.0/16` or `172.12.0.0/16` CIDR block.

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
            "oss:ListBuckets",
            "oss:GetBucketStat",
            "oss:GetBucketInfo",
            "oss:GetBucketTagging",
            "oss:GetBucketAcl"
            ],
      "Resource": [
        "acs:oss:*:*:*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "oss:ListObjects",
        "oss:GetObject"
      ],
      "Resource": [
        "acs:oss:*:*:myphotos",
        "acs:oss:*:*:myphotos/*"
      ],
      "Condition":{
        "IpAddress": {
          "acs:SourceIp": ["192.168.0.0/16", "172.12.0.0/16"]
        }
      }
    }
  ]
}
```

- Add an IP address condition to the `Deny` element. If the IP address of a RAM user is not in the `192.168.0.0/16` CIDR block, the RAM user cannot access or manage the myphotos bucket.

```
{
```

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
            "oss:ListBuckets",
            "oss:GetBucketStat",
            "oss:GetBucketInfo",
            "oss:GetBucketTagging",
            "oss:GetBucketAcl"
            ],
      "Resource": [
        "acs:oss:*:*:*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "oss:ListObjects",
        "oss:GetObject"
      ],
      "Resource": [
        "acs:oss:*:*:myphotos",
        "acs:oss:*:*:myphotos/*"
      ]
    },
    {
      "Effect": "Deny",
      "Action": "oss:*",
      "Resource": [
        "acs:oss:*:*:*"
      ],
      "Condition":{
        "NotIpAddress": {
          "acs:SourceIp": ["192.168.0.0/16"]
        }
      }
    }
  ]
}
```

> **Note** A policy with the Deny command has a higher priority than a policy with the Allow command. When a RAM user attempts to read data from the `myphotos` bucket, but the IP address is not in the `192.168.0.0/16` CIDR block, OSS notifies the RAM user of having no permissions.

- Example 4: Authorize a RAM user to read data from an OSS directory.

  In this example, the bucket that stores photos is named `myphotos`. The bucket contains directories that indicate the location where the photos were captured. Each directory contains subdirectories that indicate the years when the photos were captured.

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

  You can use different policies to grant read-only permissions on the `myphotos/hangzhou/2015/` directory to a RAM user based on specific scenarios. The following examples describe three typical scenarios:

- Scenario 1: Authorize a RAM user to read data from objects in the directory, but do not authorize the RAM user to list objects.

  In this scenario, the RAM user can use the full path to read object data. We recommend that you attach this policy to your applications.

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

- Scenario 2: Authorize a RAM user to use the OSS CLI to access the `myphotos/hangzhou/2015/` directory and list objects in the directory.

  In this scenario, the RAM user can use the OSS CLI or call API operations to read data from the directory. We recommend that you use this policy to grant the relevant permissions to your software developers.

  In this scenario, the `ListObjects` permission is required.

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

- Scenario 3: Authorize a RAM user to use the OSS console to access the directory.

  In this scenario, the RAM user can use a visual OSS client (for example, Windows File Explorer) to access the `myphotos/hangzhou/2015/` directory.

  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:ListBuckets",
        "oss:GetBucketStat",
        "oss:GetBucketInfo",
        "oss:GetBucketTagging",
        "oss:GetBucketAcl"
        ],
  "Resource": [
    "acs:oss:*:*:*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "oss:GetObject",
    "oss:GetObjectAcl"
  ],
  "Resource": [
    "acs:oss:*:*:myphotos/hangzhou/2015/*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "oss:ListObjects"
  ],
  "Resource": [
    "acs:oss:*:*:myphotos"
  ],
  "Condition": {
    "StringLike": {
      "oss:Delimiter": "/",
      "oss:Prefix": [
        "",
        "hangzhou/",
        "hangzhou/2015/*"
      ]
    }
  }
```

```
    }
  ]
}
```

14.Use RAM to manage ApsaraDB for RDS permissions

This topic describes how to manage ApsaraDB for RDS permissions of a RAM user by using RAM. In the RAM console, you can create custom policies and attach them to a RAM user.

Prerequisites

- An Alibaba Cloud account is created. If not, create one before proceeding. To create an Alibaba Cloud account, click account registration page.
- You have a basic understanding of the following common system policies:
  - AliyunRDSFullAccess: grants a RAM user the permissions to manage RDS instances.
  - AliyunRDSReadOnlyAccess: grants a RAM user the read-only permission on RDS instances.
- You have a basic understanding of RDS permissions. For more information, see RAM authorization.

Attach a custom policy to a RAM user

1. Create a custom policy based on RDS authorization examples.
2. On the **Policies** page, click the name of the policy.
3. On the **References** tab, click **Grant Permission**.
4. In the dialog box that appears, enter the name or ID of the RAM user in the **Principal** field. Then, select the RAM user from the auto-complete results.
5. Click **OK**. Click **Finished**.

> **Note** For more information, see Grant permissions to a RAM user and Grant permissions to a RAM user group.

RDS authorization examples

- Example 1: Authorize a RAM user to manage two specified RDS instances.

  To authorize a RAM user to manage the RDS instances i-001 and i-002 in your Alibaba Cloud account, use the following sample script:

```
{
 "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 RDS instances but can manage only the specified two RDS instances.
> - The `Describe*` element is required in the policy. Otherwise, the authorized RAM user cannot view instances in the console. However, the RAM user can manage the two specified RDS instances by calling API operations or using the CLI or SDK.

- Example 2: Authorize a RAM user to access Data Management (DMS).

- To authorize a RAM user to log on to a specified RDS instance, use the following sample script:

```
{
 "Statement": [
  {
   "Action": "dms:LoginDatabase",
   "Effect": "Allow",
   "Resource": "acs:rds:*:*:dbinstance/rds783a0639ks5k7****"
  }
 ],
 "Version": "1"
}
```

> **Note** You must replace `rds783a0639ks5k7****` with the ID of the RDS instance.

- To authorize a RAM user to log on to all RDS instances, use the following sample script:

```
{
 "Statement": [
  {
   "Action": "dms:LoginDatabase",
   "Effect": "Allow",
   "Resource": "acs:rds:*:*:*"
  }
 ],
 "Version": "1"
}
```

15.Use RAM to manage SLB permissions

This topic describes how to manage Server Load Balancer (SLB) permissions of a Resource Access Management (RAM) user by using RAM policies.

Prerequisites

An Alibaba Cloud account is created. To create an Alibaba Cloud account, visit the account registration page.

Context

- The following common system policies are used in the RAM console to manage SLB permissions:
  - AliyunSLBFullAccess: grants a RAM user all permissions on SLB instances.
  - AliyunSLBReadOnlyAccess: grants a RAM user the read-only permission on SLB instances.
- For more information about SLB permissions, see Authorize a RAM user.

Attach a custom policy to a RAM user

1. Create a custom policy based on Examples of SLB permission policies.

   For more information, see Create a custom policy.
2. On the Policies page, click the name of the policy.
3. On the page that appears, click the **References** tab. On this tab, click **Grant Permission**.
4. In the Add Permissions pane, enter the logon name or display name of the RAM user in the **Principal** field, and select the RAM user from the auto-complete results.
5. Click **OK**.
6. Click **Finish**.

> **Note** For more information, see Grant permissions to a RAM user and Grant permissions to a RAM user group.

Examples of SLB permission policies

- Example 1: Authorize a RAM user to manage two specified SLB instances.

  To authorize a RAM user to manage the SLB instances `i-001` and `i-002` in your Alibaba Cloud account, use the following policy:

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

> **Note**
>
> - The authorized RAM user can view all SLB instances. However, the RAM user can manage only the specified two SLB instances.
> - The policy must contain the `Describe*` element. Otherwise, the authorized RAM user cannot view instances in the console. However, the RAM user can manage the two specified SLB instances by calling API operations or using the CLI or SDK.

- Example 2: Authorize a RAM user to add an ECS instance as a backend server of the SLB instance `slb-001`. The ID of the ECS instance is `i-001`.

```
{
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "slb:AddBackendServers",
   "Resource": ["acs:slb:*:*:loadbalancer/slb-001"]
  },
  {
   "Effect": "Allow",
   "Action": "slb:AddBackendServers",
   "Resource": ["acs:ecs:*:*:instance/i-001"]
  },
  {
   "Effect": "Allow",
   "Action": "slb:DescribeLoadBalancers",
   "Resource": "acs:slb:*:*:loadbalancer/*"
  }
 ],
 "Version": "1"
}
```

Note You must grant both of the following two permissions to a RAM user. Otherwise, the RAM user cannot add or remove ECS instances or set the weights of ECS instances.

- Permissions on SLB instances
- Permissions on ECS instances

- Example 3: Authorize a RAM user to perform ECS-related operations on a specified SLB instance.

```
{
  "Statement": [{
      "Effect": "Allow",
      "Action": "slb:*",
      "Resource": [
        "acs:slb:*:*:loadbalancer/i-001",
        "acs:slb:*:*:loadbalancer/i-002"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "slb:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ecs:DescribeInstances",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "slb:*",
      "Resource": [
        "acs:ecs:*:*:instance/i-instance001",
        "acs:ecs:*:*:instance/i-instance002"
      ]
    }
  ],
  "Version": "1"
}
```

Note This policy allows the RAM user to manage two SLB instances `i-001` and `i-002`, including to perform all ECS-related operations on the SLB instances. For example, the RAM user can add the ECS instances `i-instance001` and `i-instance002` as backend servers of the two SLB instances and set the weights of the ECS instances. After this policy is attached to the RAM user, the RAM user can view the ECS instance list when selecting ECS instances.

16.Use RAM to manage Alibaba Cloud CDN permissions

This topic describes how to manage Alibaba Cloud content delivery network (CDN) permissions of RAM users by creating policies in RAM.

Prerequisites

- An Alibaba Cloud account is created. If not, create one before proceeding. To create an Alibaba Cloud account, click account registration page.
- You have a basic understanding of the following common system policies:
  - AliyunCDNFullAccess: grants a RAM user full management permissions for Alibaba Cloud CDN.
  - AliyunCDNReadOnlyAccess: grants a RAM user read-only permissions for Alibaba Cloud CDN.
- You have a basic understanding of Alibaba Cloud CDN permissions. For more information, see API authentication rules.

Procedure

1. Create a custom policy.

```
{
 "Version": "1",
 "Statement": [
  {
   "Action": [
    "cdn:Describe*",
    "cdn:PushObjectCache",
    "cdn:RefreshObjectCaches"
   ],
   "Resource": "acs:cdn:*:*:*",
   "Effect": "Allow"
  }
 ]
}
```

> **Note** The preceding custom policy indicates that RAM users are authorized to perform CDN read-only, cache refresh, and preload operations. You can modify the policy content to grant different permissions to RAM users. For more information about how to use the `Action` or `Resource` elements, see Policy elements.

2. Find the target policy and click the policy name.
3. On the **References** tab, click **Grant Permission**.
4. In the **Principal** field, enter the name of the target RAM user, and then select the corresponding

user.

5. Click **OK**.

> **Note** For more information, see Grant permissions to a RAM user and Grant permissions to a RAM user group.

17.Use RAM to manage VPC permissions

This topic describes how to manage Virtual Private Cloud (VPC) permissions of a RAM user by using RAM. In the RAM console, you can create custom policies and attach them to the RAM user.

Prerequisites

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, visit the account registration page.
- You have a basic knowledge of the following system policies that are used in the RAM console to manage VPC permissions:
  - AliyunVPCFullAccess: grants all permissions on VPCs to a RAM user.
  - AliyunVPCReadOnlyAccess: grants the read-only permissions on VPCs to a RAM user.
- You have a basic knowledge of VPC permissions. For more information, see RAM user authorization.

Attach a custom policy to a RAM user

1. Log on to the RAM console by using an Alibaba Cloud account.
2. Create a custom policy. For more information, see Create a custom policy and Examples of VPC permission policies.
3. On the **Policies** page, click the name of the policy.
4. On the page that appears, click the **References** tab. On this tab, click **Grant Permission**.
5. In the **Add Permissions** pane, enter the logon name or display name of the RAM user in the **Principal** field, and select the RAM user from the auto-complete results.
6. Click **OK**.
7. Click **Complete**.

> **Note** You can also attach existing policies to a RAM user or RAM user group. For more information, see Grant permissions to a RAM user and Grant permissions to a RAM user group.

Examples of VPC permission policies

- Example 1: Authorize a RAM user to manage all VPCs.

  To authorize a RAM user to manage all of the VPCs that belong to the Alibaba Cloud account 1234567, use the following policy:

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vpc:*"
      ],
      "Resource": [
        "acs:vpc:*:1234567:*/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:*Describe*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

- Example 2: Authorize a RAM user to manage VSwitches.

  To authorize a RAM user to manage the VSwitches of the VPCs in the China (Qingdao) region, use the following policy. After the policy is attached to the RAM user, the RAM user can create, delete, associate, or disassociate subnet routes for the VSwitches of the VPCs in the China (Qingdao) region. The RAM user can also view the VSwitches in other regions.

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

- Example 3: Authorize a RAM user to manage the route tables and route entries in a specified region.

  To authorize a RAM user to manage only the VPCs in the China (Hangzhou) region, use the following policy. After the policy is attached to the RAM user, the RAM user can add or delete route entries, create subnet routes, and associate subnet routes with VSwitches in the China (Hangzhou) region. The RAM user can also view the cloud products in other regions.

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:*Describe*"
      ],
      "Resource": [
        "*"
```

```
      ],
      "Condition": {}
    },
    {
      "Effect": "Allow",
      "Action": [
        "slb:*Describe*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {}
    },
    {
      "Effect": "Allow",
      "Action": [
        "rds:*Describe*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {}
    },
    {
      "Effect": "Allow",
      "Action": [
        "vpc:*Describe*",
        "vpc:*RouteEntry*",
        "vpc:*RouteTable*"
      ],
      "Resource": [
"acs:vpc:cn-hangzhou:11111111:*/*"
      ],
      "Condition": {}
    }
  ]
}
```

- Example 4: Authorize a RAM user to add or delete route entries in a specified route table.

  To authorize a RAM user to add or delete route entries in a specified route table, use the following policy:

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vpc:*RouteEntry*"
      ],
      "Resource": [
        "acs:vpc:cn-qingdao:*:routetable/vtb-m5e64ujkb7xn5zlq0xxxx"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "vpc:*Describe*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:*Describe*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

18.View RAM operation records in the ActionTrail console

This topic describes how to view RAM operation records of a RAM user in the ActionTrail console. ActionTrail can record operations performed by Alibaba Cloud accounts and RAM users under the accounts. You can view records of operations performed by all RAM users under your Alibaba Cloud account.

Prerequisites

An Alibaba Cloud account is created. If not, create one before proceeding. To create an Alibaba Cloud account, click account registration page.

Procedure

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. Enter the username, select an **Event Type** and **Time**, and then click **Search**.

   > **Note** You can also search for the target event by specifying the **Event Name**, **Resource Type**, **Resource Name**, and **AccessKeyId**.

4. Find the target event, and then click **+**.
5. Click **View Event**.

Operations recorded by ActionTrail

ActionTrail can record the following RAM operations. For more information, see ActionTrail event log reference.

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

```
{
  "apiVersion":"2015-05-01",
  "eventId":"2cc52dee-d8d2-40c2-8de0-3a2cf1df****",
  "eventName":"DeleteGroup",
  "eventSource":"ram.aliyuncs.com",
  "eventTime":"2015-11-03T13:41:49Z",
  "eventType":"ApiCall",
  "eventVersion":"1",
  "requestId":"9AE24F49-C52C-4F0F-BCF9-9A4B8C22B147",
  "requestParameters":{
    "GroupName":"grp1",
  },
  "serviceName":"Ram",
  "sourceIpAddress":"42.120.XX.XX",
  "userAgent":"AliyunConsole",
  "userIdentity":{
    "type":"ram-user",
    "principalId":"27418064654829****",
    "accountId":"123456789012****",
    "userName":"Alice",
    "sessionContext":{
      "sessionAttributes":{
        "creationDate":"2015-11-03T13:41:48Z",
        "mfaAuthenticated":"true"
      }
    }
  }
}
```


- RAM and STS API operations called to create, change, or delete resources. The following is an example of a recorded API operation:

```
{
  "apiVersion": "2015-05-01",
  "eventId": "234ef3c7-8938-4bd7-bb80-11754b7b****",
  "eventName": "CreateGroup",
  "eventSource": "ram.aliyuncs.com",
  "eventTime": "2016-01-04T08:58:50Z",
  "eventType": "ApiCall",
  "eventVersion": "1",
  "recipientAccountId": "4****",
  "requestId": "1485748C-DB62-4693-AB7E-4BA3F3A970E1",
  "requestParameters": {
    "Comments": "this is a test group",
    "GroupName": "grp1"
  },
  "serviceName": "Ram",
  "sourceIpAddress": "42.120.XX.XX",
  "userAgent": "aliyuncli/2.0.6",
  "userIdentity": {
    "type": "ram-user",
    "principalId": "27418064654829****",
    "accountId": "4****",
    "accessKeyId": "f6Iz********EI4d",
    "userName": "Alice"
  }
}
```

19.Authorize RAM users to use ActionTrail

This topic describes how to create custom policies to grant permissions to RAM users so that they can log on to the ActionTrail console and use the corresponding ActionTrail resources.

Prerequisites

- An Alibaba Cloud account is created. If not, create an Alibaba Cloud account first.
- View the supported ActionTrail API operations and RAM permission policies. For more information, see RAM account authentication.

Procedure

1. Create a RAM user.
2. Create a custom policy.

   You can create custom policies to grant permissions to RAM users based on the following examples of permission policies.
3. Grant permissions to a RAM user.

Examples of permission policies

- Example 1: Grant read-only permissions to a RAM user.

```
{
  "Version": "1",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "actiontrail:LookupEvents",
      "actiontrail:Describe*",
      "actiontrail:Get*"
    ],
    "Resource": "*"
  }]
}
```

- Example 2: Grant read-only permissions to a RAM user when the RAM user logs on from a specified IP address.

```
{
  "Version": "1",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "actiontrail:LookupEvents",
      "actiontrail:Describe*",
      "actiontrail:Get*"
    ],
    "Resource": "*",
    "Condition":{
      "IpAddress": {
        "acs:SourceIp": "42.120.XX.X/24"
      }
    }
  }]
}
```