ALIBABA CLOUD

Alibaba Cloud

Resource Access Management

Tutorials

Document Version: 20220530

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 Resource Access Management (RAM) to grant permissions to O&M engineers and manage the permissions.

Context

An enterprise has purchased multiple Alibaba Cloud services and deployed its application systems on the cloud. This poses the following O&M requirements:

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

Solution

The enterprise can create RAM users and attach different policies to the RAM users to meet different O&M requirements.

O&M engineer	Policy	Description
Cloud O&M engineers	AdministratorAccess	Permissions to manage all Alibaba Cloud resources.
VM O&M engineers	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 (NAS).
	AliyunOSSFullAccess	Permissions to manage Object Storage Service (OSS).
	AliyunOTSFullAccess	Permissions to manage Tablestore (OTS).
	AliyunCDNFullAccess	Permissions to manage Alibaba Cloud CDN (CDN).
	AliyunCENFullAccess	Permissions to manage Cloud Enterprise Network (CEN).
	AliyunCommonBandwidthPackageFullAccess	Permissions to manage EIP Bandwidth Plan.
	AliyunEIPFullAccess	Permissions to manage Elastic IP Address (EIP).

O&M engineer	Policy	Description
Network O&M engineers	AliyunExpressConnectFullAccess	Permissions to manage Express Connect.
	AliyunNATGatewayFullAccess	Permissions to manage NAT Gateway (NAT).
	AliyunSCDNFullAccess	Permissions to manage Secure CDN (SCDN).
	AliyunSmartAccessGatewayFullAccess	Permissions to manage Smart Access Gateway.
	AliyunVPCFullAccess	Permissions to manage Virtual Private Cloud (VPC).
	AliyunVPNGatewayFullAccess	Permissions to manage VPN Gateway.
Database O&M engineers	AliyunRDSFullAccess	Permissions to manage ApsaraDB RDS.
	AliyunDTSFullAccess	Permissions to manage Data Transmission Service (DTS).
Security O&M engineers	AliyunYundunFullAccess	Permissions to manage all Alibaba Cloud Security services.
Monitoring O&M engineers	AliyunActionTrailFullAccess	Permissions to manage ActionTrail.
	AliyunARMSFullAccess	Permissions to manage Application Real-Time Monitoring Service (ARMS).
	AliyunCloudMonitorFullAccess	Permissions to manage CloudMonitor.
	ReadOnlyAccess	Permissions only to read all Alibaba Cloud resources.
	AliyunSupportFullAccess	Permissions to manage Ticket Management.

Procedure

This example describes how to set the RAM user `alice@secloud.onaliyun.com` as a database O&M engineer. Then, the RAM user can manage ApsaraDB RDS and DTS.

1. Log on to the RAM console by using your Alibaba Cloud account.
2. Create a RAM user named `alice@secloud.onaliyun.com`.

   For more information, see Create a RAM user.
3. Attach the `AliyunRDSFullAccess` and `AliyunDTSFullAccess` policies to the RAM user `alice@secloud.onaliyun.com`.

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

You can repeat to to create other RAM users and attach policies to the RAM users so that the RAM users can manage different cloud services.

2.Use RAM to limit the IP addresses that are allowed to access Alibaba Cloud resources

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

Prerequisites

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. The resources include Elastic Compute Service (ECS) instances, ApsaraDB RDS instances, Server Load Balancer (SLB) instances, and Object Storage Service (OSS) buckets. To ensure business and data security, the enterprise requires users to access Alibaba Cloud resources only from specific IP addresses, such as the IP addresses of the internal network of the enterprise.

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

Step 1: Create a custom policy

1.
2.
3.
4.
5.
6. Enter the policy document and click **Next Step**.

   The following policy document specifies that the RAM users can access ECS instances only by using `192.168.0.0/16` and `172.16.215.218`. In this case, the `acs:SourceIp` condition key in the `Condition` element is set to `192.168.0.0/16` and `172.16.215.218`.

```
{
  "Statement": [
    {
      "Action": "ecs:*",
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "IpAddress": {
          "acs:SourceIp":[
          "192.168.0.0/16",
          "172.16.215.218"
         ]
        }
      }
    }
  ],
  "Version": "1"
}
```

> **Note** The `Condition` element applies only to the actions specified for the current policy. You can replace 192.168.0.0/16 and 172.16.215.218 with the IP address or CIDR block of your network.

7.
8.
9.

Step 2: Create a RAM user

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click **Create User**.
4. In the **User Account Information** section of the **Create User** page, configure the **Logon Name** and **Display Name** parameters.

   > **Note** You can click **Add User** to create multiple RAM users at a time.

5. In the **Access Mode** section, select an access mode.
   - **Console Access**: If you select this option, you must complete the logon security settings. These settings specify whether to use a system-generated or custom logon password, whether the password must be reset upon the next logon, and whether to enable multi-factor authentication (MFA).

     > **Note** If you select Custom Logon Password in the Console Password section, you must specify a password. The password must meet the complexity requirements. For more information about the complexity requirements, see Configure a password policy for RAM users.

   - **OpenAPI Access**: If you select this option, an AccessKey pair is automatically created for the

RAM user. The RAM user can call API operations or use other development tools to access Alibaba Cloud resources.

> **Note** To ensure the security of the Alibaba Cloud account, we recommend that you select only one access mode for the RAM user. This prevents the RAM user from using an AccessKey pair to access Alibaba Cloud resources after the RAM user leaves the organization.

6. Click **OK**.

Step 3: Attach the policy to the RAM user

Attach the policy that you created in Step 1 to the RAM user that you created in Step 2.

3.Use RAM to limit the period of time in which users are allowed to access Alibaba Cloud resources

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

Prerequisites

Context

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

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

Step 1: Create a custom policy

1.
2.
3.
4.
5. Enter the policy document and click **Next Step**.

   The following policy indicates that the authorized RAM user can access Alibaba Cloud ECS only before 17:00 on August 12, 2019 (UTC+8). In this case, the `acs:CurrentTime` parameter in the `Condition` element is set to `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 specified for the current policy. You can change the value `2019-08-12T17:00:00+08:00` based on your business requirements.

6.
7.
8.

Step 2: Create a RAM user

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click **Create User**.
4. In the **User Account Information** section of the **Create User** page, configure the **Logon Name** and **Display Name** parameters.

   > **Note** You can click **Add User** to create multiple RAM users at a time.

5. In the **Access Mode** section, select an access mode.
   - **Console Access**: If you select this option, you must complete the logon security settings. These settings specify whether to use a system-generated or custom logon password, whether the password must be reset upon the next logon, and whether to enable multi-factor authentication (MFA).

     > **Note** If you select Custom Logon Password in the Console Password section, you must specify a password. The password must meet the complexity requirements. For more information about the complexity requirements, see Configure a password policy for RAM users.

   - **OpenAPI Access**: If you select this option, an AccessKey pair is automatically created for the RAM user. The RAM user can call API operations or use other development tools to access Alibaba Cloud resources.

     > **Note** To ensure the security of the Alibaba Cloud account, we recommend that you select only one access mode for the RAM user. This prevents the RAM user from using an AccessKey pair to access Alibaba Cloud resources after the RAM user leaves the organization.

6. Click **OK**.

Step 3: Attach the policy to the RAM user

Attach the policy that you created in Step 1 to the RAM user that you created in Step 2.

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

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

Prerequisites

Context

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

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

Step 1: Create a custom policy

1.
2.
3.
4.
5. Enter the policy document and click **Next Step**.

   If the following policy is attached to a RAM user, the RAM user can access ECS instances only over HTTPS. In this case, the `acs:SecureTransport` condition key in the `Condition` element is set to `true`.

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

   Note The `Condition` element applies only to the actions specified for the current policy. The valid values of the `acs:SecureTransport` parameter are `true` and `false`.

6.

7.
8.

Step 2: Create a RAM user

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click **Create User**.
4. In the **User Account Information** section of the **Create User** page, configure the **Logon Name** and **Display Name** parameters.

   > **Note** You can click **Add User** to create multiple RAM users at a time.

5. In the **Access Mode** section, select an access mode.
   - **Console Access**: If you select this option, you must complete the logon security settings. These settings specify whether to use a system-generated or custom logon password, whether the password must be reset upon the next logon, and whether to enable multi-factor authentication (MFA).

     > **Note** If you select Custom Logon Password in the Console Password section, you must specify a password. The password must meet the complexity requirements. For more information about the complexity requirements, see Configure a password policy for RAM users.

   - **OpenAPI Access**: If you select this option, an AccessKey pair is automatically created for the RAM user. The RAM user can call API operations or use other development tools to access Alibaba Cloud resources.

     > **Note** To ensure the security of the Alibaba Cloud account, we recommend that you select only one access mode for the RAM user. This prevents the RAM user from using an AccessKey pair to access Alibaba Cloud resources after the RAM user leaves the organization.

6. Click **OK**.

Step 3: Attach the policy to the RAM user

Attach the policy that you created in Step 1 to the RAM user that you created in Step 2.

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

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

Prerequisites

- You have basic knowledge of the policy elements, structure, and syntax before you create a custom policy. For more information, see Policy elements and Policy structure and syntax.
- The Google Authenticator app is downloaded and installed on your mobile device. You can use one of the following methods to download the Google Authenticator app:
  - For iOS, download the Google Authenticator app from the App Store.
  - For Android, download the Google Authenticator app from your preferred app store.

> **Note** For Android, you must download and install a quick response (QR) code scanner from an app store for the Google Authenticator app to identify QR codes.

Step 1: Create a custom policy

1.
2.
3.
4.
5. Enter the policy document and click **Next Step**.

   The following policy indicates that only MFA-enabled RAM users can access ECS resources by using the Alibaba Cloud Management Console. The `acs:MFAPresent` condition key in the `Condition` element is set to `true`.

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

> **Note** The `Condition` element applies only to the actions specified for the current policy. You can also modify the policy to limit the access from RAM users to other cloud resources based on your business requirements.

6.
7.
8.

Step 2: Create a RAM user

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click **Create User**.
4. In the **User Account Information** section of the **Create User** page, configure the **Logon Name** and **Display Name** parameters.

   > **Note** You can click **Add User** to create multiple RAM users at a time.

5. In the **Access Mode** section, select an access mode.
   - **Console Access**: If you select this option, you must complete the logon security settings. These settings specify whether to use a system-generated or custom logon password, whether the password must be reset upon the next logon, and whether to enable multi-factor authentication (MFA).

     > **Note** If you select Custom Logon Password in the Console Password section, you must specify a password. The password must meet the complexity requirements. For more information about the complexity requirements, see Configure a password policy for RAM users.

   - **OpenAPI Access**: If you select this option, an AccessKey pair is automatically created for the RAM user. The RAM user can call API operations or use other development tools to access Alibaba Cloud resources.

     > **Note** To ensure the security of the Alibaba Cloud account, we recommend that you select only one access mode for the RAM user. This prevents the RAM user from using an AccessKey pair to access Alibaba Cloud resources after the RAM user leaves the organization.

6. Click **OK**.

Step 3: Attach the policy to the RAM user

Attach the policy that you created in Step 1 to the RAM user that you created in Step 2.

Step 4: Enable MFA for the RAM user

Enable MFA for the RAM user that you created in Step 2.

1. Log on to the RAM console by using your Alibaba Cloud account or a RAM user that has administrative rights.

2. In the left-side navigation pane, choose **Identities > Users**.
3. In the **User Logon Name/Display Name** column, click the username of the RAM user for which you want to enable a virtual MFA device.
4. On the page that appears, click the **Authentication** tab. Then, click the **Virtual MFA Device** tab.
5. Click **Enable Virtual MFA Device**.
6. On your mobile device, enable a virtual MFA device.

   > **Note** The following example shows how to enable a virtual MFA device in the Google Authenticator app on your mobile device that runs iOS.

   i. Open the Google Authenticator app.

   ii. Click **Get started** and select one of the following methods to enable a virtual MFA device:

   - Tap **Scan a QR code** in the Google Authenticator app. Then, scan the QR code that is displayed on the **Scan the code.** tab in the RAM console. This method is recommended.
   - Tap **Enter a setup key**. Then, enter the account and key that you obtained from the **QR Information** tab in the RAM console, and tap **Add**.

7. In the RAM console, enter the two consecutive verification codes that are displayed in the Google Authenticator app. Then, click **Confirm Bind**.

   > **Note** 您还可以设置是否允许RAM用户**保存MFA验证状态7天**，如果为允许，则RAM用户使用MFA登录时，可以选中**记住这台机器，7天内无需再次验证**，就可以在7天内免MFA验证。关于具体的设置方法，请参见Configure security policies for RAM users。

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

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.

Context

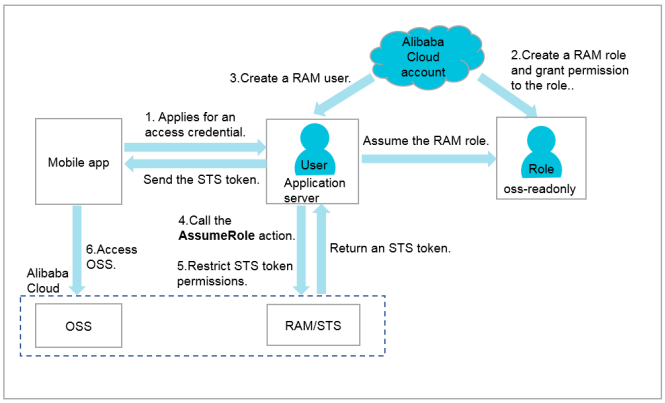
An enterprise develops a mobile app and activates Object Storage Service (OSS). The mobile app runs on mobile devices. These mobile devices are not controlled by the enterprise. The enterprise must grant the necessary permissions to the mobile app. Then, the mobile app can upload data to and download 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 can directly upload data to or download data from OSS, the mobile app must apply for an access credential from the application server. After the application server receives the request, the server uses a RAM user identity to call the STS AssumeRole operation. If the call succeeds, the application receives an STS token and forwards the STS token to the mobile app. Then, the mobile app can 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 attaches the required policies to the role.

   For more information, see Create a RAM role and attach the required policies 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 STS AssumeRole 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 that has fewer permissions than the policies attached to the RAM role. This way, the application server controls the access from the mobile app to OSS.

   For more information, see Request an STS token that has fewer permissions than the policies attached to 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 attach the required policies 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, the **Current Alibaba Cloud Account** is selected as the trusted account. This ensures that only RAM users that belong to 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 about 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 that belong to 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 to

the RAM role `oss-readonly`. The AliyunOSSReadOnlyAccess policy indicates the read-only permissions on OSS.

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. Then, the RAM user can 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 STS AssumeRole 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:

   - Sample request

     ```
     aliyuncli sts AssumeRole --RoleArn acs:ram::123456789012****:role/oss-readonly --Role
     SessionName client-001
     ```

   - Sample response

     ```
     {
          "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 policies of the RAM role `oss-readonly` because the `Policy` parameter is unspecified. The application server can also request an STS token that has fewer permissions than the policies attached to the RAM role. For more information, see Request an STS token that has fewer permissions than the policies attached to 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 must request a new STS token on a regular basis. For example, the application server can request a new STS token every 1,800 seconds.

Request an STS token that has fewer permissions than the policies attached to the RAM role

In actual scenarios, we recommend that you specify the `Policy` parameter to grant the STS token with fewer permissions than the policies that are attached to the RAM role. Follow the principle of least privilege. The following example shows how to specify the Policy parameter:

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

- Sample request

```
aliyuncli sts AssumeRole --RoleArn acs:ram::123456789012****:role/oss-readonly --RoleSess
ionName client-002 --Policy "{\"Version\":\"1\", \"Statement\": [{\"Effect\":\"Allow\", \
"Action\":\"oss:GetObject\", \"Resource\":\"acs:oss:*:*:sample-bucket/2015/01/01/*.jpg\"}
]}"
```

- Sample response

```
{
    "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 validity period of the STS token is 3,600 seconds. The enterprise can specify the `DurationSeconds` parameter to limit the validity period of the STS token. The maximum validity period of the STS token is 3,600 seconds.

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:

   - Specify the STS token

     Syntax: `aliyuncli oss Config --host --accessid --accesskey --sts_token` .

```
aliyuncli oss Config --host oss.aliyuncs.com --accessid STS.FJ6EMcS1JLZgAcBJSTDG1****
--accesskey 28Co5Vyx2XhtTqj3RJgdud4ntyzrSNdUvNygAj7x**** --sts_token CAESnQMIARKAASJg
nzMzlXVyJn4KI+FsysaIpTGm8ns8Y74HVEj0pOevO8ZWXrnnkz4a4rBEPBAdFkh3197GUsprujsiU78Fkszxh
nQPKkQKcyvPihoXqKvuukrQ/Uoudk31KAJEz5o2EjlNUREcxWjRDRSISMzkxNTc4NzUyNTczOTcyODU0Kgpjb
GllbnQtMDAxMKmZxIHBKjoGUnNhTUQ1Qn8KATEaegoFQWxsb3cSJwoMQWN0aW9uRXF1YWxzEgZBY3Rpb24aDw
oNb3NzOkdldE9iamVjdBJICg5SZXNvdXJjZUVxdWFscxIIUmVzb3VyY2UaLAoqYWNzOm9zczoqOio6c2FtcGx
lLWJ1Y2tldC8yMDE1LzAxLzAxLyouanBnSgU0MzI3NFIFMjY4NDJaD0Fzc3VtZWRSb2xlVXNlcmAAahIzOTE1
Nzg3NTI1NzM5NzI4NTRyCWVjcy1hZG1pbnjgxt7Cj/bo****
```

- Access OSS

```
aliyuncli oss Get oss://sample-bucket/2015/01/01/grass.jpg
```

Related information

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

7.Use RAM to authorize applications to access Alibaba Cloud resources

This topic describes how to use a Security Token Service (STS) token of a Resource Access Management (RAM) role to authorize applications to access Alibaba Cloud resources.

Context

An enterprise has purchased Elastic Compute Service (ECS) instances and wants to deploy applications on these ECS instances. The applications need to use AccessKey pairs to call the operations of other Alibaba Cloud services.

In this case, the enterprise can use one of the following methods:

- Includes the AccessKey pairs in application code.
- Saves the AccessKey pairs in the configuration files of the applications.

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

- AccessKey pair disclosure: If AccessKey pairs are stored in the ECS instances in plaintext, the AccessKey pairs may be disclosed after snapshots and images are shared or ECS instances are 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 difficulties in managing the ECS instances and images.

Solution

To resolve the preceding issues, the enterprise can use RAM to manage the permissions of ECS instances. RAM is a resource access control service that allows the enterprise to assign a RAM role that is attached with specific policies to each ECS instance. The applications can use an STS token of the specific RAM role to call Alibaba Cloud operations.

Process

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 access Alibaba Cloud resources.

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

2. The enterprise attaches the required policies to the RAM role.

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

   > **Note** If the STS token cannot grant the required permissions, the enterprise can attach policies to the RAM role based on business requirements. After the policies are attached, the permissions that are attached to the STS token immediately take effect without requiring you to restart the specific 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 attaches the required policies to the RAM user.
   - If the RAM user has the same responsibilities as an administrator, the `AdministratorAccess` policy must be attached to the RAM user.
   - If the RAM user has different responsibilities from those of an administrator, the enterprise must create the following custom policy in the RAM console and attach the policy to the RAM user:

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

> **Note**
>
> - Only authorized RAM users can configure RAM roles for ECS instances. This prevents the abuse of RAM roles.
> - When a RAM user that can only manage ECS instances attempts to create an ECS instance and configure a RAM role, ECS checks whether the RAM user is allowed to perform the `ram:PassRole` action on the RAM role. If the RAM user is not allowed, the ECS instance fails to be created.

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

5. The RAM user that is created in Step assigns the RAM role that is created in Step to a specific ECS instance.

   For more information, see Step 3: Attach the RAM role to an ECS instance.

6. ECS includes the STS token in the metadata of the ECS instance and sends the metadata to the application that is deployed on the ECS instance.
   - In a Linux system, applications can query the instance metadata to obtain an 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/MyApplicationRo
le
```

     Sample response

```
{
    "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 automatically obtain the STS token of the RAM role from the ECS instance metadata. No AccessKey pair-related configurations are required in the SDK.

  > **Note** In most cases, an STS token is valid for one hour. The applications can call Alibaba Cloud operations when the STS token is valid. Before the STS token expires, the token is updated by ECS.

7. The applications use the STS token to call Alibaba Cloud operations.

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

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

This topic describes 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 account alias is configured for your Alibaba Cloud account. For more information, see View and modify the default domain name.

Context

Enterprise A has purchased multiple types of Alibaba Cloud resources, such as Elastic Compute Service (ECS) instances, ApsaraDB RDS instances, Server Load Balancer (SLB) instances, and Object Storage Service (OSS) buckets. Enterprise A wants to authorize Enterprise B to access specified resources of Enterprise A.

Enterprise A has the following requirements:

- Enterprise A serves only 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 A does not need to change permissions. Enterprise B can grant its RAM users fine-grained permissions on cloud resources of Enterprise A. The RAM user credentials can be assigned to either employees or applications.
- If the agreement between Enterprise A and Enterprise B ends, Enterprise A can revoke the permissions from Enterprise B.

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 of Enterprise B needs to use a RAM user to assume this role, Enterprise B can use Account B to 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, the 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 that is 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 `1345678901234****` is specified as the trusted Alibaba Cloud account. This ensures that RAM users that belong to 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::1345678901234****: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` 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 the 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 Alibaba Cloud Management Console as a RAM user.

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

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

1. Log on to the RAM console by using Account A.
2. In the left-side navigation pane, choose **Identities > Roles**.
3. In the Role Name column of the page that appears, click the RAM role `ecs-admin`.
4. On the **Trust Policy Management** tab, click **Edit Trust Policy**. In the panel 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 Revoke permissions from a RAM role.

9.Use RAM to create and authorize resource groups

This topic describes how to use Resource Access Management (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.

Context

A gaming enterprise is developing three gaming projects. Each project requires various cloud resources. The enterprise has an Alibaba Cloud account and more than 100 Elastic Compute Service (ECS) instances that belong to the Alibaba Cloud account.

The enterprise has the following requirements:

- 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 enterprise requires that each project receives separate bills.
- Shared bottom-layer network: The enterprise requires a shared bottom-layer network for its cloud resources.

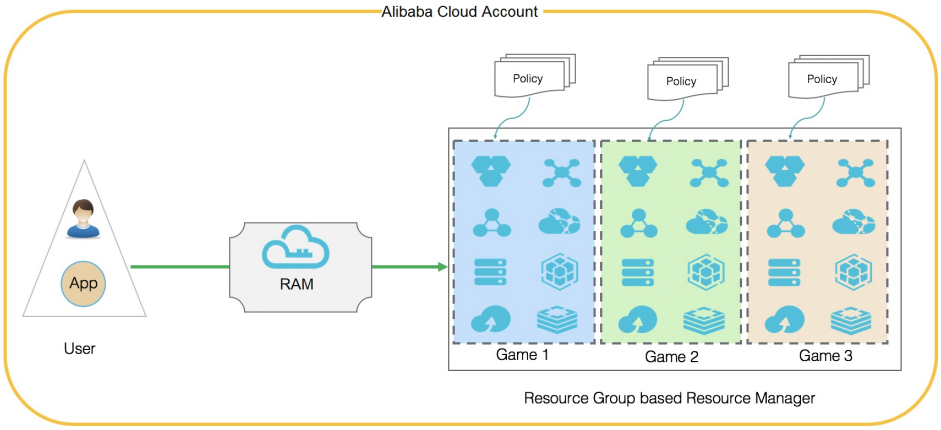
The enterprise has the following optional solutions:

- Multi-account solution
  - This solution supports independent project management. The enterprise 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. By default, each Alibaba Cloud account receives separate bills. The enterprise can use the consolidated billing feature provided by Alibaba Cloud to consolidate the bills and invoices of the multiple Alibaba Cloud accounts.
  - This solution does not support a shared bottom-layer network. The resources of different accounts are isolated between different networks. Virtual private clouds (VPCs) of the accounts can be connected by using peering connections. However, this leads to higher management costs.
- Single-account solution (with tagged resources)
  - This solution does not support independent project management. The enterprise 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 enterprise can tag its cloud resources by project. Then, each project can receive separate bills.
  - This solution supports a shared bottom-layer network. The enterprise can use tag-based RAM policies to authorize RAM users to access a group of resources. These resources belong to the same Alibaba Cloud account, and the enterprise does not need to pay for peering connections.
- 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 Alibaba Cloud account and can share a VPC. The enterprise does not need to pay for peering connections. This helps reduce management costs.

Solution

The resource group-based management solution can meet all requirements of the enterprise. This solution allows the enterprise to create three resource groups that correspond to the three projects by using one Alibaba Cloud account.



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 show how to specify a RAM user as a resource group administrator. The RAM user Alice is used as an example.

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. In the **Create Resource Group** panel, specify **Resource Group Name** and **Display Name**, and click **OK**.

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

5. Find a resource group that you created and click **Manage Permission** in the **Actions** column.
6. On the **Permissions** tab of the page that appears, click **Grant Permission**.
7. In the **Principal** field of the **Grant Permission** panel, enter `Alice@secloud.onaliyun.com`.
8. In the Authorization Policy Name column of the Select Policy section, click `AdministratorAccess`.
9. Click **OK**.
10. Click **Complete**.

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

Result

Alice, Bob, and Charlie are the 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 resource group on which the administrator has permissions. The administrator can also create and manage ECS instances.
- After an administrator logs on to the Resource Management console, the administrator can manage the RAM users, RAM user groups, and RAM roles in a resource group on which the administrator has permissions.

10.Use a resource group to manage an ECS instance

This topic describes how to add an Elastic Compute Service (ECS) instance to a resource group and authorize a Resource Access Management (RAM) user to view and manage the ECS instance in the resource group.

Procedure

In this example, the RAM user Alice is authorized to view and manage only the ECS instance i-001. You can add the ECS instance to a resource group and grant the permissions on the resource group to Alice.

1. Log on to the RAM console and create a RAM user named Alice.

   For more information, see Create a RAM user.

2. Log on to the Resource Management console and create a resource group named ECS-Admin.

   For more information, see Create a resource group.

3. In the Resource Management console, add the ECS instance i-001 to the resource group ECS-Admin.

   You can use one of the following methods to add the ECS instance to the resource group:

   - Add the ECS instance to the resource group when you create the instance. For more information, see Create an instance by using the wizard.
   - Move the ECS instance to the resource group. For more information, see Transfer resources across resource groups.

4. In the RAM console, grant the required permissions to Alice.

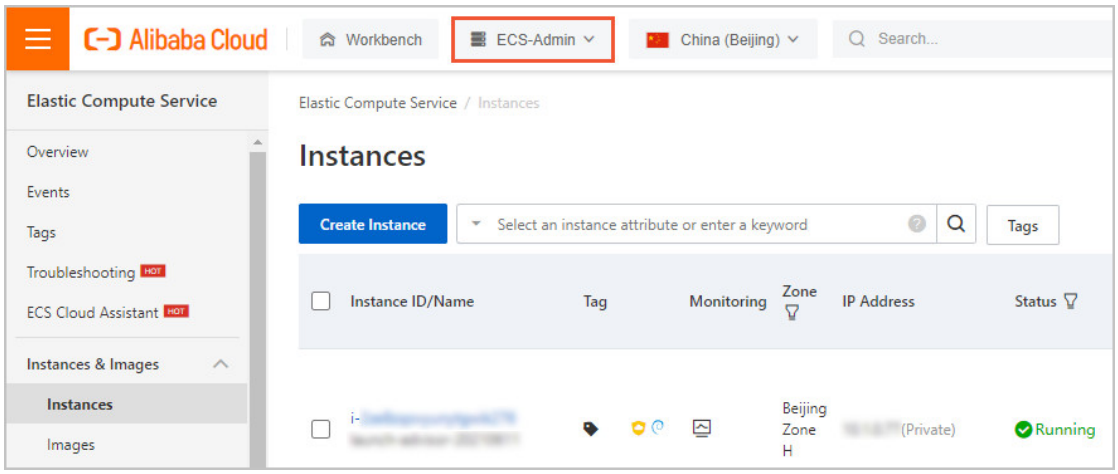
   In this step, set Authorization Scope to Specific Resource Group, enter ECS-Admin in the field below, enter Alice in the Principal field, and then select the system policy AliyunECSFullAccess. For more information, see Grant permissions to a RAM user.

   > **Note** If you want to authorize Alice only to view the ECS instance, select the system policy AliyunECSReadOnlyAccess in this step.

5. Log on to the ECS console and view and manage the ECS instance.

   i. In the left-side navigation pane, choose **Instances & Images > Instances**.

ii. In the top navigation bar, select the resource group ECS-Admin.



iii. On the Instances page, view the information about the instance and manage the instance.

11.Use tags to grant access to ECS instances by group

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

Context

In this example, you have 10 ECS instances. You want to authorize the developer team to manage 5 instances and the operator team to manage the other 5 instances. However, you want each team to view only the instances that you authorize each team to manage.

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

You can create a custom policy named policyForDevTeam and another custom policy named policyForOpsTeam.

You must create the following tags:

- A tag that is added to five ECS instances. The tag key is team and the tag value is dev.
- A tag that is added 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 add the tags to your ECS instances.
   i. Log on to the ECS console.
   ii. In the left-side navigation pane, choose **Instances & Images > Instances**.
   iii. In the upper-left corner of the top navigation bar, select a region.
   iv. On the **Instances** page, find a specific instance, move the pointer over the icon in the **Tag** column, and then click **Edit Tags**.
   v. In the **Edit Tags** dialog box, click **Create**.
   vi. Enter the tag key and tag value in the fields that appear and click **Confirm**.
   vii. Click **OK**.

   Repeat the preceding steps to add the `team:dev` tag to five ECS instances and add 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 user group.
3. Create RAM users and add each RAM user to a RAM 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. 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 RAM user group, the RAM users in the RAM user 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 parts:

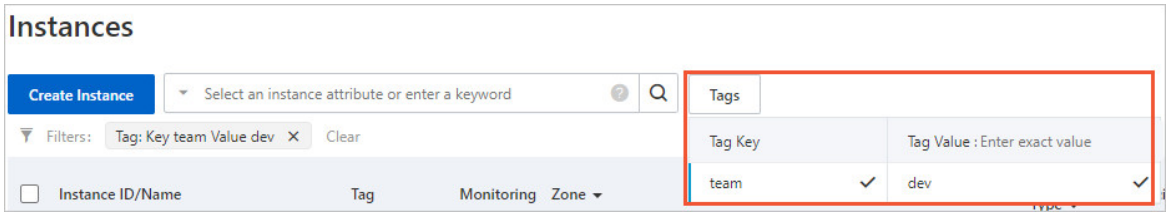
- The `"Action":"ecs:*"` part that includes `Condition` specifies the ECS instances to which the `team:dev` or `team:ops` tag is added.

- The `"Action": "ecs:DescribeTag*"` part authorizes RAM users to query all tags in ECS. After a RAM user logs on to the ECS console, all existing tags are displayed. The RAM user must select the value of an authorized tag key to view the ECS instances to which the tag is added.

Verify the authorization

1. Log on to the ECS console as a RAM user.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the upper-left corner of the top navigation bar, select the region.
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 added 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 added.



> **Note** A RAM user can view the ECS instances to which a tag is added only after the RAM user selects the tag. Otherwise, the RAM user cannot view the ECS instances to which the tag is added.

References

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 SSH key pairs.

12.Use tags to grant access to ApsaraDB RDS instances by group

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

Background information

In this example, you have 10 ApsaraDB RDS instances. You want to authorize the developer team to manage 5 instances and the operator team to manage the other 5 instances. However, you want each team to view only the instances that you authorize each team to manage.

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

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

You must create the following tags:

- A tag that is added to five ApsaraDB RDS instances. The tag key is team and the tag value is dev.
- A tag that is added to the other five ApsaraDB RDS instances. The tag key is team and the tag value is ops.

Procedure

The procedure in which tags are used to grant access to ApsaraDB RDS instances by group is the same as the procedure in which tags are used to grant access to ECS instances by group. For more information, see Use tags to grant access to ECS instances by group.

You must create the following two custom policies to authorize the teams:

- The policy policyForDevTeam for the RAM user group developer

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

- The policy policyForOpsTeam for the RAM user group operator

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

Each policy consists of two parts:

- The `"Action":"rds:*"` part that includes `Condition` specifies the ApsaraDB RDS instances to which the `team:dev` or `team:ops` tag is added.
- The `"Action": "rds:DescribeTag*"` part authorizes RAM users to query all tags in ApsaraDB RDS. After a RAM user logs on to the ApsaraDB RDS console, all existing tags are displayed. The RAM user must select the value of a tag key to view the ApsaraDB RDS instances to which the tag is added.

FAQ

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

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

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

- The required policy is attached to the RAM users.
- The region selected in the ApsaraDB RDS console is the region where the ApsaraDB RDS instances reside.
- The corresponding tag value to filter the instances is selected.

> **Note** If a RAM user logs on to the ApsaraDB 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 RDS instances are displayed by default. However, the RAM user is not authorized to view all ApsaraDB RDS resources.

13.Use RAM to manage ECS permissions

This topic describes how to manage Elastic Compute Service (ECS) permissions of Resource Access Management (RAM) users. In the RAM console, you can create custom policies and attach them to the RAM users.

Context

- Before you manage the ECS permissions of RAM users, take note of the following system policies:
  - AliyunECSFullAccess: grants a RAM user the permissions to manage ECS instances.
  - AliyunECSReadOnlyAccess: grants a RAM user the read-only permission on ECS instances.

  If the system policies cannot meet your business requirements, you can create custom policies.
- Before you manage the ECS permissions of RAM users, take note of the ECS permissions. For more information, see Authentication rules.

Procedure

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 and Policy examples.
3. Attach the custom policy to the RAM user.

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

Policy 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. If you want the authorized RAM user to view and manage only the specified two ECS instances, you can add the ECS instances to a resource group and authorize the RAM user to view and manage the ECS instances in the resource group. For more information, see Use a resource group to manage an ECS instance.
- `Describe*` is required in the policy. Otherwise, the authorized RAM user cannot view ECS instances in the ECS console. However, the RAM user can manage the two specified ECS instances by calling API operations or using a 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 If you want to authorize a RAM user to view ECS instances in a different region, you can replace `cn-qingdao` in the `Resource` element with the ID of the region. For more information about region IDs, see Regions and zones.

- Example 3: Authorize a RAM user to create snapshots.

If a RAM user cannot create disk snapshots after the RAM user is granted administrative rights on the ECS instance, 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"
}
```

14.Use RAM to manage OSS permissions

This topic describes how to manage Object Storage Service (OSS) permissions of Resource Access Management (RAM) users. In the RAM console, you can create custom policies and attach them to the RAM users.

Context

- Before you manage OSS permissions of RAM users, take note of the following system policies:
  - AliyunOSSFullAccess: grants a RAM user the permissions to manage OSS buckets.
  - AliyunOSSReadOnlyAccess: grants read-only permissions on OSS buckets.

  If the system policies cannot meet your business requirements, you can create custom policies.
- Before you manage OSS permissions of RAM users, take note of the OSS permissions. For more information, see Overview.

Procedure

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 and Policy examples.
3. Attach the policy to the RAM user.

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

Policy 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` 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 specific 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 that the RAM user does not have the required 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 multiple folders that are named based on the location where the photos were captured. Each folder contains subfolders that are named based on the years when the photos were captured.

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

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

- Scenario 1: Authorize a RAM user to read data from objects in the folder, 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/` folder and list objects in the folder.

  In this scenario, the RAM user can use the OSS CLI or call operations to read data from the folder. We recommend that you use this policy to grant related 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 folder.

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

  The following permissions are required:

  - Permission to list all `buckets`
  - Permission to list folders under `myphotos`
  - Permission to list folders 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/*"
                    ]
                }
            }
        }
    ]
}
```

15.Use RAM to manage ApsaraDB RDS permissions

This topic describes how to manage ApsaraDB RDS permissions of Resource Access Management (RAM) users. In the RAM console, you can create custom policies and attach them to the RAM users.

Context

- Before you manage the ApsaraDB RDS permissions of RAM users, take note of the following system policies:
  - AliyunRDSFullAccess: grants a RAM user the permissions to manage ApsaraDB RDS instances.
  - AliyunRDSReadOnlyAccess: grants read-only permissions on ApsaraDB RDS instances.

  If the system policies cannot meet your business requirements, you can create custom policies.
- Before you manage the ApsaraDB RDS permissions of RAM users, take note of the ApsaraDB RDS permissions. For more information, see Use RAM for resource authorization.

Procedure

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 and Policy examples.
3. Attach the policy to the RAM user.

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

Policy examples

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

  To authorize a RAM user to manage the ApsaraDB 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 ApsaraDB RDS instances but can manage only the specified two ApsaraDB RDS instances.
> - The `Describe*` element is required in the policy. Otherwise, the authorized RAM user cannot view instances in the ApsaraDB RDS console. However, the RAM user can manage the two specified ApsaraDB 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 specific ApsaraDB 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 ApsaraDB RDS instance.

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

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

16.Use RAM to manage SLB permissions

This topic describes how to manage Server Load Balancer (SLB) permissions of Resource Access Management (RAM) users. In the RAM console, you can create custom policies and attach the policies to the RAM users.

Context

- Before you manage the SLB permissions of RAM users, take note of the following system policies:
  - AliyunSLBFullAccess: grants a RAM user the permissions to manage SLB instances.
  - AliyunSLBReadOnlyAccess: grants read-only permissions on SLB instances.

  If the system policies cannot meet your business requirements, you can create custom policies.
- Before you manage the SLB permissions of RAM users, take note of the SLB permissions. For more information, see Authorize a RAM user.

Procedure

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 and Policy examples.
3. Attach the policy to the RAM user.

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

Policy examples

- Example 1: Authorize a RAM user to manage two specific 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 sample script:

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

- Example 2: Authorize a RAM user to add an Elastic Compute Service (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** After you grant a RAM user permissions to manage an SLB instance based on the policy described in Example 1, you must also grant the following two permissions to the RAM user. Otherwise, the RAM user cannot add or remove ECS instances or configure 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 specific 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** The preceding policy allows the RAM user to manage SLB instances `i-001` and `i-002`. Then, the RAM user can 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 specified SLB instances and configure 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 the user selects ECS instances.

17.Use RAM to manage CDN permissions

This topic describes how to manage Alibaba Cloud CDN (CDN) permissions of Resource Access Management (RAM) users. In the RAM console, you can create custom policies and attach them to the RAM users.

Context

- Before you manage the CDN permissions of RAM users, take note of the following system policies:
  - AliyunCDNFullAccess: grants a RAM user the permissions to manage CDN.
  - AliyunCDNReadOnlyAccess: grants a RAM user the read-only permission on CDN.

  If the system policies cannot meet your business requirements, you can create custom policies.
- Before you manage the CDN permissions of RAM users, take note of the CDN permissions. For more information, see RAM authorization.

Procedure

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.

   The following 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.

   ```
   {
     "Version": "1",
     "Statement": [
       {
         "Action": [
           "cdn:Describe*",
           "cdn:PushObjectCache",
           "cdn:RefreshObjectCaches"
         ],
         "Resource": "acs:cdn:*:*:*",
         "Effect": "Allow"
       }
     ]
   }
   ```
3. Attach the policy to the RAM user.

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

18.Use RAM roles to manage VPC permissions

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

Context

- Before you manage the VPC permissions of RAM users, take note of the following system policies:
  - AliyunVPCFullAccess: grants a RAM user the permissions to manage VPCs.
  - AliyunECSReadOnlyAccess: grants read-only permissions on VPCs.

  If the system policies cannot meet your business requirements, you can create custom policies.
- Before you manage the VPC permissions of RAM users, take note of the VPC permissions. For more information, see RAM user authorization.

Procedure

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 and Policy examples.
3. Attach the policy to the RAM user.

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

Policy examples

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

  To authorize a RAM user to manage all VPCs in your Alibaba Cloud account 1234567, use the following sample script:

```
{
    "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 the vSwitches in a VPC.

  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 only 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 routes in a specific region.

  To authorize a RAM user to manage all VPCs in the China (Hangzhou) region, use the following sample script. The RAM user belongs to your Alibaba Cloud account 1234567. After the RAM user is authorized, the RAM user can add or delete routes, create subnet routes, and associate vSwitches in this region. The RAM user can only view the cloud services 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:1234567:*/*"
            ],
            "Condition": {}
        }
    ]
}
```

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

  To authorize a RAM user to add or delete routes in a specific 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": [
                "*"
            ]
        }
    ]
}
```

19.Authorize RAM users to use ActionTrail

This topic shows you how to create custom policies to grant permissions to the RAM users within your Alibaba Cloud account. Then, you can log on to the ActionTrail console as one of these RAM users and use ActionTrail resources.

Context

- Take note of the following system policies before you authorize RAM users to use ActionTrail:
  - AliyunActionTrailFullAccess: full permissions on ActionTrail
  - AliyunActionTrailReadOnlyAccess: read-only permissions on ActionTrail

  If the preceding system policies cannot meet your requirements, you can create custom policies as needed.
- You must view the supported ActionTrail API operations and the RAM policies related to ActionTrail before the authorization. For more information, see RAM account authentication.

Procedure

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 and Examples of policies.
3. Grant the required permissions to the RAM user.

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

Examples of policies

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

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

- Example 2: Grant read-only permissions on ActionTrail to a RAM user and allow the RAM user to access ActionTrail only 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"
            }
        }
    }]
}
```

20.View RAM operation events in the ActionTrail console

ActionTrail can track and record Resource Access Management (RAM) operation events that are performed by using Alibaba Cloud accounts, RAM users, and RAM roles. This topic describes how to view RAM operation events in the ActionTrail console.

Context

ActionTrail can track and record the following RAM operation events:

- IMS
- STS
- Logons as a RAM user

For more information about the fields in operation events, see Management event log reference.

Procedure

1. Log on to the ActionTrail console.
2. In the left-side navigation pane, click **Event Detail Query**.
3. In the top navigation bar, select a region from the drop-down list. The region is where the event that you want to query occurred.
4. On the **Query Event Details** page, select **Service Name** from the drop-down list.
5. Enter **Ram** in the field and click the

   icon.
6. Find the event that you want to query and move the pointer over the event name in the **Event Name** column to view the event details.
7. (Optional)To query the code of an event, click the plus sign (+) to the left of the event that you want to query and click **Event Detail**.