ALIBABA CLOUD

Alibaba Cloud

Resource Access Management

Policy Management

Document Version: 20220713

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.Policy overview 06

2.Policy models 08

3.View the basic information about a policy 10

4.Custom policies 11

4.1. Create a custom policy 11

4.2. Delete a custom policy 15

4.3. Modify the document and description of a custom policy 15

4.4. Manage custom policy versions 16

5.Manage policy references 17

6.Policy language 18

6.1. Policy elements 18

6.2. Policy structure and syntax 22

6.3. Policy evaluation process 25

6.4. Policy evaluation process of assuming a RAM role 29

7.Example policies 32

7.1. Overview of sample policies 32

7.2. Restart ECS instances 32

7.3. Access Alibaba Cloud resources by using a specific IP addr... 33

7.4. Access Alibaba Cloud in a specified period of time 34

7.5. Access Alibaba Cloud by using a specified method 35

7.6. Authorize a RAM user to manage MFA devices 36

7.7. Authorize a RAM user to manage AccessKey pairs 36

7.8. Manage a specified ECS instance 37

7.9. View ECS instances in a specific region 38

7.10. Manage ECS security groups within an Alibaba Cloud acc... 38

7.11. Manage information about all resources within an Alibab... 39

7.12. View information about all cloud resources within an Alib.. 39
7.13. Grant permissions across cloud services 40
7.14. Create a snapshot 41
7.15. Manage an OSS bucket 42
7.16. List and read resources in a bucket 43
7.17. Access OSS through specified IP addresses 44
7.18. Read data from a specified object in OSS 46
7.19. Access and list specified files through OSS CLI 47
7.20. Access a specified directory through the OSS console 48
7.21. Manage a resource group 49

1.Policy overview

This topic describes the permissions and policies of Alibaba Cloud. To grant different permissions to Resource Access Management (RAM) identities on Alibaba Cloud resources, you can attach different policies to the RAM identities.

Permission

Permissions are specified by a statement within a policy that allows or denies access to a specific Alibaba Cloud resource.

- An Alibaba Cloud account is the resource owner and controls all permissions.
  - Each Alibaba Cloud resource has only one owner. The owner must be an Alibaba Cloud account and has complete control over the resource.
  - The resource owner is not necessarily the resource creator. For example, if a RAM user has permission to create Alibaba Cloud resources, the resources created by this RAM user belong to the Alibaba Cloud account of the RAM user. The RAM user is the resource creator, but is not the resource owner.
- A RAM user has no permissions by default.
  - A RAM user is an identity that is used to manage resources. Before a RAM user can perform operations, the RAM user must be granted the required permissions by the Alibaba Cloud account. The required permissions must be granted by attaching one or more explicit allow policies.
  - A new RAM user can manage resources only after the RAM user is granted the required permissions.
- As a resource creator, a RAM user is not automatically granted the permissions on the created resources.
  - A RAM user can create resources after the RAM user is granted the required permissions.
  - To grant the RAM user the required permissions, the resource owner must attach one or more explicit allow policies to the RAM user.

Policy

A policy defines a set of permissions that are described based on the policy structure and syntax. A policy can accurately describe the authorized resource sets, authorized operation sets, and authorization conditions. For more information, see Policy structure and syntax.

In RAM, a policy is a resource entity that can be created, updated, deleted, and viewed. RAM supports the following two types of policies:

- **System Policy**: System policies are automatically created and upgraded by Alibaba Cloud and cannot be modified by users.
- **Custom Policy**: Custom policies are created, modified, and deleted by users to meet their business requirements.

You can attach one or more policies to RAM users, RAM user groups, or RAM roles. For more information, see Grant permissions to a RAM user, Grant permissions to a RAM user group and Grant permissions to a RAM role.

Policies attached to RAM identities

You can attach one or more policies to RAM identities to grant the identities the relevant permissions.

- The attached policies can be system policies or custom policies.

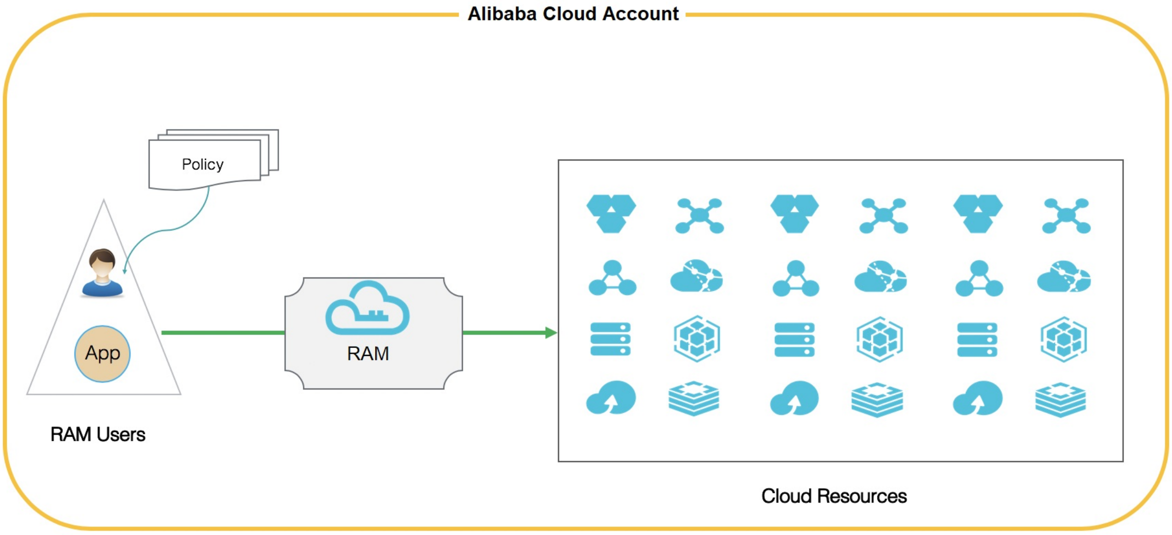
- If the attached policies are modified, the new policies automatically take effect. You do not need to attach the new policies to RAM identities.

2.Policy models

Alibaba Cloud allows you to grant RAM identities the permissions to manage the resources of an Alibaba Cloud account or a resource group. You can select a policy model from these two options based on your business requirements.

Manage the resources of an Alibaba Cloud account

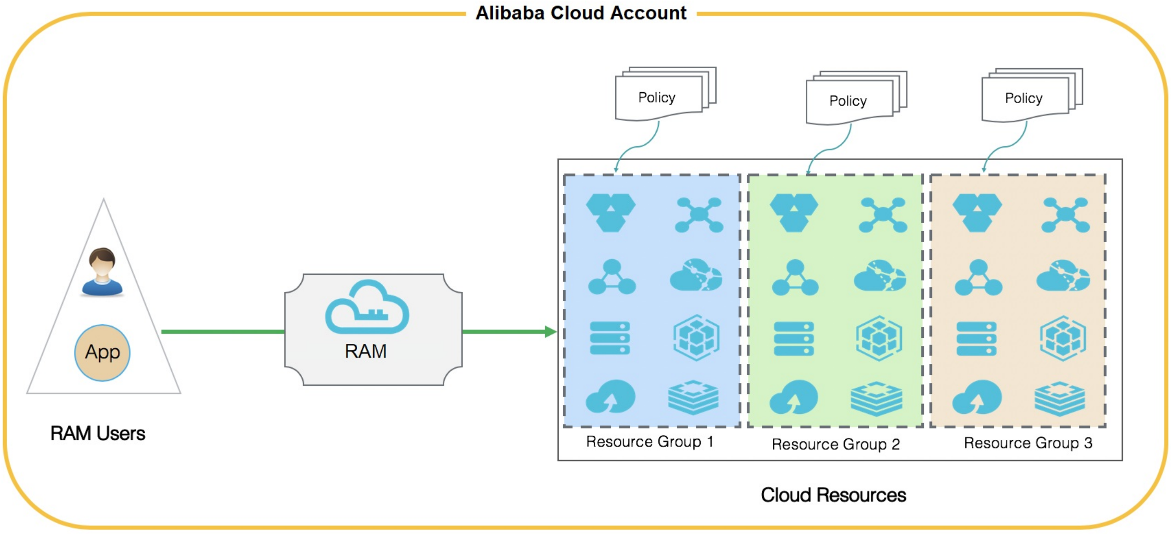
In this model, if you attach a policy to a RAM identity, all Alibaba Cloud resources of the Alibaba Cloud account are included in the scope of the policy permissions.



Manage the resources of a resource group

Resource Group authorization: In this model, if you attach a policy to a RAM identity, only the Alibaba Cloud resources of the resource group are included in the scope of the policy permissions.

Administrator: The RAM user that is attached with the `AdministratorAccess` system policy in a resource group is the administrator of the resource group. By default, the RAM user that creates the resource group is the administrator. The administrator can add RAM users to the resource group and grant permissions to the RAM users in the resource group.


Alibaba Cloud Account
Policy
Policy
Policy
App
RAM
RAM Users
Resource Group 1
Resource Group 2
Resource Group 3
Cloud Resources

3.View the basic information about a policy

This topic describes how to view the basic information about a policy, such as the policy name, policy type, and description.

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the **Policies** page, select a policy type from the **Policy Type** drop-down list.
4. Enter a policy name or description in the search box. Then, find the policy whose basic information you want to view and click its name. Fuzzy match is supported.
5. In the **Basic Information** section of the page that appears, view information such as **Policy Name**, **Note**, and **Policy Type**.

Related information

- GetPolicy
- ListPoliciesForUser
- ListPoliciesForGroup
- ListPoliciesForRole

4.Custom policies

4.1. Create a custom policy

This topic describes how to create a custom policy. Custom policies provide more fine-grained access control than system policies.

Methods to create a custom policy

- Create a custom policy on the Visual Editor Beta tab

  When you create a custom policy on the Visual Editor Beta tab, you need to select configuration items in the Effect, Service, Action, Resource, and Condition sections. Then, the system checks your configurations. This ensures the validity of the custom policy. On this tab, you can perform simple operations to create a custom policy.

- Create a custom policy on the JSON tab

  When you create a custom policy on the JSON tab, you must compile a policy document based on the syntax and structure of Resource Access Management (RAM) policies. On this tab, you can create a custom policy in a flexible manner. This method is suitable for users who are familiar with the syntax and structure of RAM policies.

- Create a custom policy by importing a policy template

  RAM provides policy templates that are created based on years of business practices and are suitable for common scenarios. For example, RAM provides policy templates that are applicable to system administrators, financial personnel, and network administrators. You need to only import an appropriate policy template and modify the template based on your business requirements. This way, you can create a custom policy in a convenient manner.

- Create a custom policy by importing a system policy

  You can import a system policy and modify the policy based on your business requirements. This way, you can create a custom policy in a convenient and efficient manner.

Create a custom policy on the Visual Editor Beta tab

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the **Policies** page, click **Create Policy**.
4. On the **Create Policy** page, click the **Visual Editor Beta** tab.
5. Configure the policy and click **Next: Edit Basic Information**.
   i. In the **Effect** section, select **Allow** or **Deny**.
   ii. In the **Service** section, select an Alibaba Cloud service.

   > **Note** The Alibaba Cloud services that you can select are displayed in the Service section.

   iii. In the **Action** section, select **All Actions** or **Specified Actions**.

   The system displays the actions that can be configured based on the Alibaba Cloud service you select in the previous step. If you select **Specified Actions**, you must select actions.

iv. In the **Resource** section, select **All Resources** or **Specified Resources**.

The system displays the resources that can be configured based on the actions you select in the previous step. If you select **Specified Resources**, you must click **Add Resource** to configure one or more Alibaba Cloud Resource Names (ARNs) of resources. You can also click **Match All** to select all resources for each action that you select.

> ? **Note** The resource ARNs that are required for an action are tagged with **Required**. We strongly recommend that you configure the resource ARNs that are tagged with Required. This ensures that the custom policy takes effect as expected.

v. (Optional)In the **Condition** section, click **Add Condition** to configure a condition.

Conditions include Alibaba Cloud common conditions and service-specific conditions. The system displays the conditions that can be configured based on the Alibaba Cloud service and the actions that you select. You need only to select a condition key and configure the Operator and Value parameters.

vi. Click **Add Statement** and repeat the preceding steps to configure multiple custom policy statements.

6. Configure the **Name** and **Note** parameters.
7. Check and optimize the document of the custom policy.
   - Basic optimization

     The system automatically optimizes the policy statement. The system performs the following operations during basic optimization:

     - Deletes unnecessary conditions.
     - Deletes unnecessary arrays.
   - (Optional)Advanced optimization

     You can move the pointer over **Optional: Advanced Optimize** and click **Perform**. The system performs the following operations during advanced optimization:

     - Splits resources or conditions that are incompatible with actions.
     - Narrows down resources.
     - Deduplicates or merges policy statements.
8. Click **OK**.

Create a custom policy on the JSON tab

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the **Policies** page, click **Create Policy**.
4. On the **Create Policy** page, click the **JSON** tab.
5. Enter the policy document and click **Next: Edit Basic Information**.

   For more information about the syntax and structure of RAM policies, see Policy structure and syntax.
6. Configure the **Name** and **Note** parameters.

7. Check and optimize the document of the custom policy.
    - Basic optimization

      The system automatically optimizes the policy statement. The system performs the following operations during basic optimization:

        - Deletes unnecessary conditions.
        - Deletes unnecessary arrays.
    - (Optional)Advanced optimization

      You can move the pointer over **Optional: Advanced Optimize** and click **Perform**. The system performs the following operations during advanced optimization:

        - Splits resources or conditions that are incompatible with actions.
        - Narrows down resources.
        - Deduplicates or merges policy statements.
8. Click **OK**.

Create a custom policy by importing a policy template

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the **Policies** page, click **Create Policy**.
4. On the **Create Policy** page, click **Import Policy Template** in the upper-right corner.
5. In the **Import Policy Template** dialog box, import the policy template that you want to use.
    i. Select a policy template.

       > **Note** The policy templates that are displayed in the RAM console prevail.

    ii. (Optional)Configure the parameters for the selected policy template.
    iii. Specify whether the policy document of the selected policy template overwrites the original policy document.
        - Overwrite: The policy document of the selected policy template overwrites the original policy document. This is the default value.
        - Append: The policy document of the selected policy template is appended to the end of the original policy document.
    iv. Click **Import**.
6. On the Visual Editor Beta tab or the JSON tab, view and modify the imported policy document and click **Next: Edit Basic Information**.

   By default, the imported policy template is displayed on the Visual Editor Beta tab. This way, you can view and modify the template in a visualized manner. You can also modify the template on the JSON tab.
7. Configure the **Name** and **Note** parameters.
8. Check and optimize the document of the custom policy.
    - Basic optimization

The system automatically optimizes the policy statement. The system performs the following operations during basic optimization:

- Deletes unnecessary conditions.
- Deletes unnecessary arrays.

- (Optional)Advanced optimization

  You can move the pointer over **Optional: Advanced Optimize** and click **Perform**. The system performs the following operations during advanced optimization:

  - Splits resources or conditions that are incompatible with actions.
  - Narrows down resources.
  - Deduplicates or merges policy statements.

9. Click **OK**.

Create a custom policy by importing a system policy

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the **Policies** page, click **Create Policy**.
4. On the **Create Policy** page, click **Import System Policy** in the upper-right corner.
5. In the **Import System Policy** dialog box, import a system policy.
   i. Select a system policy.
   ii. Specify whether the policy document of the selected system policy overwrites the original policy document.
      - Overwrite: The policy document of the selected system policy overwrites the original policy document.
      - Append: The policy document of the selected system policy is appended to the end of the original policy document. This is the default value.
   iii. Click **Import**.
6. On the Visual Editor Beta tab or the JSON tab, view and modify the policy document of the imported system policy and click **Next: Edit Basic Information**.

   By default, the imported system policy is displayed on the Visual Editor Beta tab. This way, you can view and modify the system policy in a visualized manner. You can also modify the system policy on the JSON tab.
7. Configure the **Name** and **Note** parameters.
8. Check and optimize the document of the custom policy.
   - Basic optimization

     The system automatically optimizes the policy statement. The system performs the following operations during basic optimization:

     - Deletes unnecessary conditions.
     - Deletes unnecessary arrays.
   - (Optional)Advanced optimization

You can move the pointer over **Optional: Advanced Optimize** and click **Perform**. The system performs the following operations during advanced optimization:

- Splits resources or conditions that are incompatible with actions.
- Narrows down resources.
- Deduplicates or merges policy statements.

9. Click **OK**.

Related information

- CreatePolicy

4.2. Delete a custom policy

This topic describes how to delete a custom policy. If permissions in a custom policy change or you no longer need the custom policy, you can delete the custom policy.

Prerequisites

The policy is not attached to a RAM user, a RAM user group, or a RAM role. If the policy is attached to a RAM user, a RAM user group, or a RAM role, you must detach the policy before you can delete the policy. For more information, see Manage policy references.

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the **Policies** page, find the policy that you want to delete and click **Delete** in the **Actions** column.
4. In the **Delete Custom Policy** message, click **OK**.

Related information

- DeletePolicy

4.3. Modify the document and description of a custom policy

This topic describes how to modify the document and description of a custom policy. You cannot modify the name of the custom policy.

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the **Policies** page, find the custom policy that you want to modify and click its name.
4. In the **Basic Information** section, click the edit icon to the right of **Note** to modify the description of the custom policy.
5. On the **Policy Document** tab, click **Modify Policy Document**.

6. Modify the policy document on the Visual Editor Beta tab or the JSON tab. You can also modify the description of the custom policy on the tabs. Then, click **Next**.

   For more information, see Create a custom policy.

7. Click **OK**.

Result

After the policy document is modified, a new version is generated for the custom policy and used as the current version.

Related information

- CreatePolicyVersion

4.4. Manage custom policy versions

This topic describes how to manage custom policy versions, such as how to view a policy version, set a policy version to the current policy version, and delete a policy version.

Context

Resource Access Management (RAM) allows you to manage the versions of custom policies.

- A custom policy has a maximum of five versions.
- If you modify a custom policy that has five versions, a version is created, and the earliest version that is not in use is deleted. You can also delete the versions that you no longer need.
- If a policy has more than one version, only the current version is active.
- The current version can be viewed but cannot be deleted.

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. In the **Policy Name** column on the Policies page, click the name of the policy that you want to manage.
4. On the page that appears, click the **Versions** tab. On this tab, you can view, specify, and delete policy versions.
   - To view a policy name, version, and its document, click **View** in the **Actions** column.
   - To set a policy version to the current policy version, click **Use This Version** in the **Actions** column.
   - To delete a policy version, click **Delete** in the **Actions** column. In the message that appears, click **OK**.

Related information

- SetDefaultPolicyVersion
- GetPolicyVersion
- ListPolicyVersions
- DeletePolicyVersion

5.Manage policy references

This topic describes how to manage policy references, such as how to view, create, and delete policy references.

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the **Policies** page, find the policy that you want to manage and click its name.
4. Click the **References** tab to manage the policy references.
   - You can view the details of a policy reference. The details include **Grant Permission On**, **Principal**, **Principal Type**, and **Attach Date**.
   - You can create a policy reference. To create a policy reference, click **Grant Permission**. In the Add Permissions panel, attach the policy to a Resource Access Management (RAM) user, a RAM user group, or a RAM role. Then, click OK.
   - You can delete a policy reference. To delete a policy reference, find the policy reference and click **Revoke Permission** in the **Actions** column. In the message that appears, click **OK**.

Related information

- ListEntitiesForPolicy

6.Policy language

6.1. Policy elements

This topic describes the elements of policies that are used in Resource Access Management (RAM) to define permissions. The elements are Effect, Action, Resource, and Condition.

Element	Description
Effect	Specifies whether a statement result is an explicit allow or an explicit deny. Valid values: Allow and Deny.
Action	Describes one or more API operations that are allowed or denied.
Resource	Specifies one or more objects that the statement covers.
Condition	Specifies the conditions that are required for a policy to take effect.

Effect

- Valid values are Allow and Deny.

> ? **Note** If policies that apply to a request include an Allow statement and a Deny statement, the Deny statement takes precedence over the Allow statement.

- Example: `"Effect": "Allow"`

Action

- Valid values are the names of operations from Alibaba Cloud services. This element can contain one or more values.

> ? **Note** In most cases, each Alibaba Cloud service has an exclusive set of API operations. For more information, see the documentation of each Alibaba Cloud service.

- Format: `<ram-code>:<action-name>`.
  - `ram-code`: the code that is used in RAM to indicate an Alibaba Cloud service. For more information, see the codes that are listed in the **RAM code** column in Services that work with RAM.
  - `action-name`: the name of one or more API operations in the service.
- Example: `"Action": ["oss:ListBuckets", "ecs:Describe*", "rds:Describe*"]`

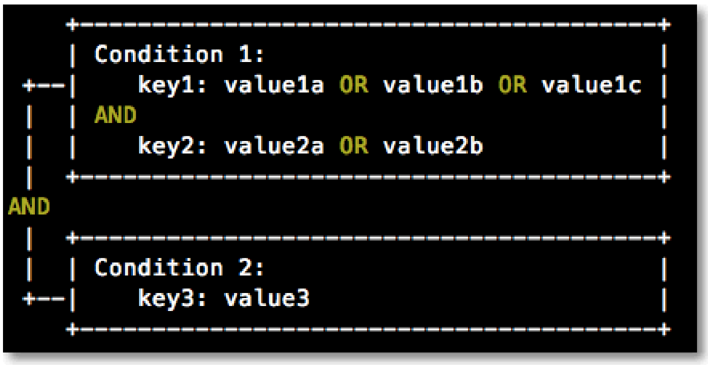
Resource

- Valid values are the Alibaba Cloud Resource Names (ARNs) of the resources. This element can contain one or more values.

- Format: `acs:<ram-code>:<region>:<account-id>:<relative-id>`, which complies with the format of ARNs.
  - `acs`: the acronym of Alibaba Cloud Service.
  - `ram-code`: the code that is used in RAM to indicate an Alibaba Cloud service. For more information, see the codes that are listed in the **RAM code** column in Services that work with RAM.
  - `region`: the information about a region. If the statement covers a global resource, leave this field empty. A global resource can be accessed without the need to specify a region. For more information, see Regions and zones.
  - `account-id`: the ID of the Alibaba Cloud account. For example, you can enter `123456789012****`.
  - `relative-id`: the identifier of the service-related resource. The meaning of this element varies based on services. The format of the relative-id element is similar to a file path. For example, `relative-id = "mybucket/dir1/object1.jpg"` indicates an Object Storage Service (OSS) object.
- Example: `"Resource": ["acs:ecs:*:*:instance/inst-001", "acs:ecs:*:*:instance/inst-002", "acs:oss:*:*:mybucket", "acs:oss:*:*:mybucket/*"]`

Condition

A condition block contains one or more conditions. Each condition consists of operators, keys, and values.



```
    +-----------------------------------+
    | Condition 1:                      |
+---|    key1: value1a OR value1b OR value1c |
|   | AND                               |
|   |    key2: value2a OR value2b       |
|   +-----------------------------------+
|
AND
|   +-----------------------------------+
|   | Condition 2:                      |
+---|    key3: value3                   |
    +-----------------------------------+
```

- Evaluation logic
  - You can specify one or more values for a condition key. If the value in a request matches one of the values, the condition is met.
  - A condition can have multiple keys that are attached to a single conditional operator. The condition of this type is met only if all requirements for the keys are met.
  - A condition block is met only if all of its conditions are met.
- Conditional operators

  Conditional operators can be classified into the following categories: string, number, date and time, Boolean, and IP address.

Category	Conditional operator

Category	Conditional operator
String	○ StringEquals ○ StringNotEquals ○ StringEqualsIgnoreCase ○ StringNotEqualsIgnoreCase ○ StringLike ○ StringNotLike
Number	○ NumericEquals ○ NumericNotEquals ○ NumericLessThan ○ NumericLessThanEquals ○ NumericGreaterThan ○ NumericGreaterThanEquals
Date and time	○ DateEquals ○ DateNotEquals ○ DateLessThan ○ DateLessThanEquals ○ DateGreaterThan ○ DateGreaterThanEquals
Boolean	Bool
IP address	○ IpAddress ○ NotIpAddress

- Condition keys
  - The format of common condition keys is `acs:<condition-key>` .

Common condition key	Category	Description
`acs:CurrentTime`	Date and time	The time at which a request is received by the web server. Specify the time in the ISO 8601 format. Example: `2012-11-11T23:59:59Z` .
`acs:SecureTransport`	Boolean	Specifies whether a secure channel is used to send a request. For example, a request can be sent over HTTPS.

Common condition key	Category	Description
`acs:SourceIp`	IP address	The IP address of the client that sends a request. Note If you specify only one value for the `acs:SourceIp` condition key, the value must be an IP address, such as 10.0.0.1. CIDR blocks such as 10.0.0.1/32 cannot be used.
`acs:MFAPresent`	Boolean	Specifies whether multi-factor authentication (MFA) is used during user logon.
`acs:PrincipalARN`	String	Specifies the identity of an object that performs an operation. The condition key can be used only in access control policies of resource directories. Example: `acs:ram:*:*:role/*resourcedirectory*` . Note You can specify an ARN only for a specified RAM role. The name can contain only lowercase letters. You can view the ARN of a RAM role on the role details page in the RAM console.

- The format of a condition key that is specific to an Alibaba Cloud service is `<ram-code>:<condition-key>` .

Condition key specific to an Alibaba Cloud service	Service	Category	Description
`ecs:tag/<tag-key>`	ECS	String	The tag key of Elastic Compute Service (ECS) resources. This key can be customized. **Note** <tag-key> indicates a tag key. Replace <tag-key> with the actual tag key.
`rds:ResourceTag/<tag-key>`	RDS	String	The tag key of ApsaraDB RDS resources. This key can be customized. **Note** <tag-key> indicates a tag key. Replace <tag-key> with the actual tag key.
`oss:Delimiter`	OSS	String	The delimiter that is used to categorize OSS object names.
`oss:Prefix`	OSS	String	The prefix of an OSS object name.

Related information

- Policy structure and syntax
- Overview of sample policies

6.2. Policy structure and syntax

This topic describes the structure and syntax that are used to create or update policies in Resource Access Management (RAM).

Conventions for policy syntax

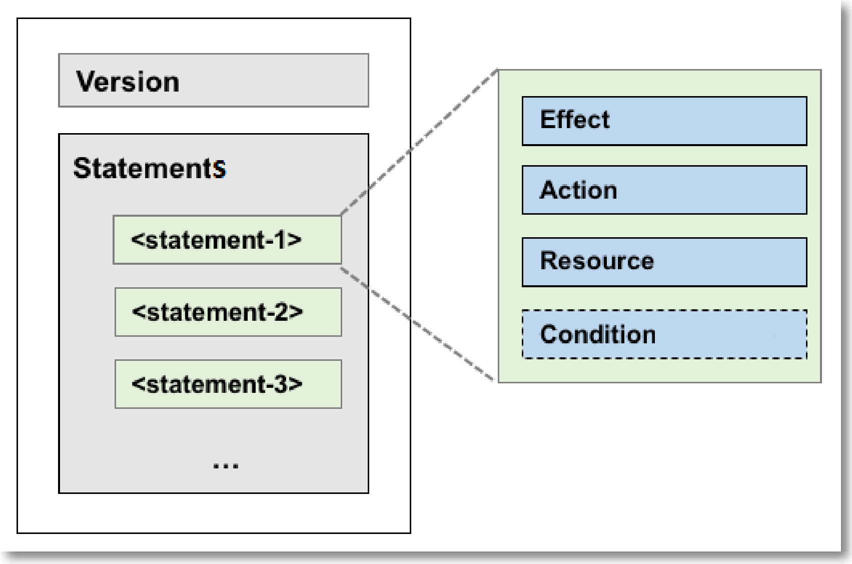
The following conventions are used for the policy syntax:

- Characters in a policy
  - The following characters are reserved JSON characters in the policy syntax: `{ } [ ] " , :`.
  - The following characters are special characters in the policy syntax: `= < > ( ) |`.
- Use of characters
  - If an element can have more than one value, you can perform one of the following operations:
    - Use a comma (,) as the delimiter to separate each value and an ellipsis (...) to describe the remaining values. Example: `[ <action_string>, <action_string>, ...]`.
    - Include only one value, Examples: `"Action": [<action_string>]` and `"Action": <action_string>`.
  - A question mark (?) that follows an element indicates that the element is optional. Example: `<condition_block?>`.
  - A vertical bar (|) between elements indicates multiple options. Example: `("Allow" | "Deny")`. Only one of the options can be used.
  - Strings are enclosed in double quotation marks ("). Example: `<version_block> = "Version" : ("1")`.

Policy structure

The policy structure includes the following components:

- The version number.
- A list of statements. Each statement contains the following elements: effect, action, resource, and condition. The condition element is optional.



Policy syntax

```
policy  = {
     <version_block>,
     <statement_block>
}
<version_block> = "Version" : ("1")
<statement_block> = "Statement" : [ <statement>, <statement>, ... ]
<statement> = {
    <effect_block>,
    <action_block>,
    <resource_block>,
    <condition_block?>
}
<effect_block> = "Effect" : ("Allow" | "Deny")
<action_block> = "Action" :
    ("*" | [<action_string>, <action_string>, ...])
<resource_block> = "Resource" :
    ("*" | [<resource_string>, <resource_string>, ...])
<condition_block> = "Condition" : <condition_map>
<condition_map> = {
  <condition_type_string> : {
      <condition_key_string> : <condition_value_list>,
      <condition_key_string> : <condition_value_list>,
      ...
  },
  <condition_type_string> : {
      <condition_key_string> : <condition_value_list>,
      <condition_key_string> : <condition_value_list>,
      ...
  }, ...
}
<condition_value_list> = [<condition_value>, <condition_value>, ...]
<condition_value> = ("String" | "Number" | "Boolean" | "Date and time" | "IP address")
```

The following list describes the policy syntax:

- Version: The current policy version is 1. The version cannot be changed.
- Statements: A policy can have multiple statements.
  - The effect of each statement can be either `Allow` or `Deny`.

    Note In a statement, both the Action and Resource elements can have multiple values.

  - Each statement can have its own conditions.

    Note A condition block can contain multiple conditions that have different operators.

- Permission precedence: You can attach multiple policies to a RAM user. If policies that apply to a request include an `Allow` statement and a `Deny` statement, the Deny statement takes precedence over the Allow statement.
- Element value:
  - If an element value is a sting, number, date, time, Boolean value, or an IP address, the value must

be enclosed in double quotation marks (").

- If an element value is a string, wildcard characters such as asterisks (`*`) and question marks (`?`) can be used.
    - An asterisk (`*`) indicates the number (which includes zero) of letters that you can use. For example, if the element value is `ecs:Describe*` , you can use all Elastic Compute Service (ECS) operations that start with `Describe` .
    - A question mark (`?`) indicates an allowed letter.

Policy syntax check

Policies are stored as JSON files. When you create or update a policy, RAM checks whether the JSON syntax is valid before the policy can be created or updated. You can also use tools such as JSON validators and editors to check whether policies meet JSON syntax standards. For more information about JSON syntax standards, see RFC 7159.

Related information

- Policy elements
- Overview of sample policies

6.3. Policy evaluation process

If a Resource Access Management (RAM) identity initiates a resource access request, a policy evaluation process is performed to determine whether to allow the request. The RAM identity is a RAM user or RAM role. The request can be initialized by using the Alibaba Cloud Management Console, API, or a CLI. This topic describes the policy evaluation process of Alibaba Cloud.

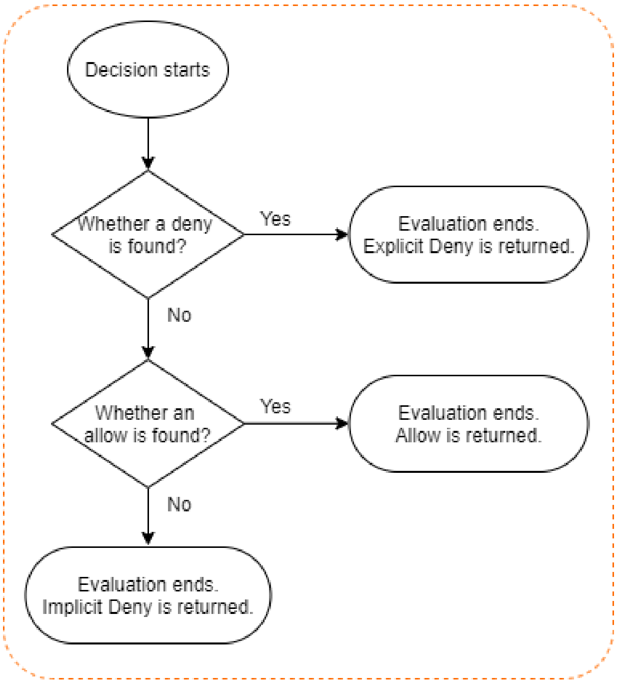
Overview

Alibaba Cloud provides multiple types of policies. A complete policy evaluation process includes the following steps:

1. Alibaba Cloud collects all types of policies that are involved in the access request. The policies include control policies, session policies, identity-based policies, and resource-based policies.
2. Alibaba Cloud evaluates policies in sequence. For more information, see the "Basic evaluation process" section of this topic. After Alibaba Cloud evaluates a policy, Alibaba Cloud decides whether to evaluate the next policy based on the decision. The evaluation continues until a final decision is obtained.

Basic evaluation process

All types of policies are evaluated based on the basic evaluation process, as shown in the following figure.


Decision starts
Whether a deny is found?
Yes
Evaluation ends. Explicit Deny is returned.
No
Whether an allow is found?
Yes
Evaluation ends. Allow is returned.
No
Evaluation ends. Implicit Deny is returned.

The basic evaluation process includes the following steps:

1. Alibaba Cloud first checks whether a policy that is involved in a request includes a Deny statement. This is because Deny statements take precedence over Allow statements in policy evaluation.
   - If the policy includes a Deny statement, the evaluation ends. Explicit Deny is returned.
   - If the policy does not include a Deny statement, the evaluation continues.
2. Alibaba Cloud checks whether the policy includes an Allow statement.
   - If the policy includes an Allow statement, the evaluation ends. Allow is returned.
   - If the policy does not include an Allow statement, the evaluation ends. Implicit Deny is returned.

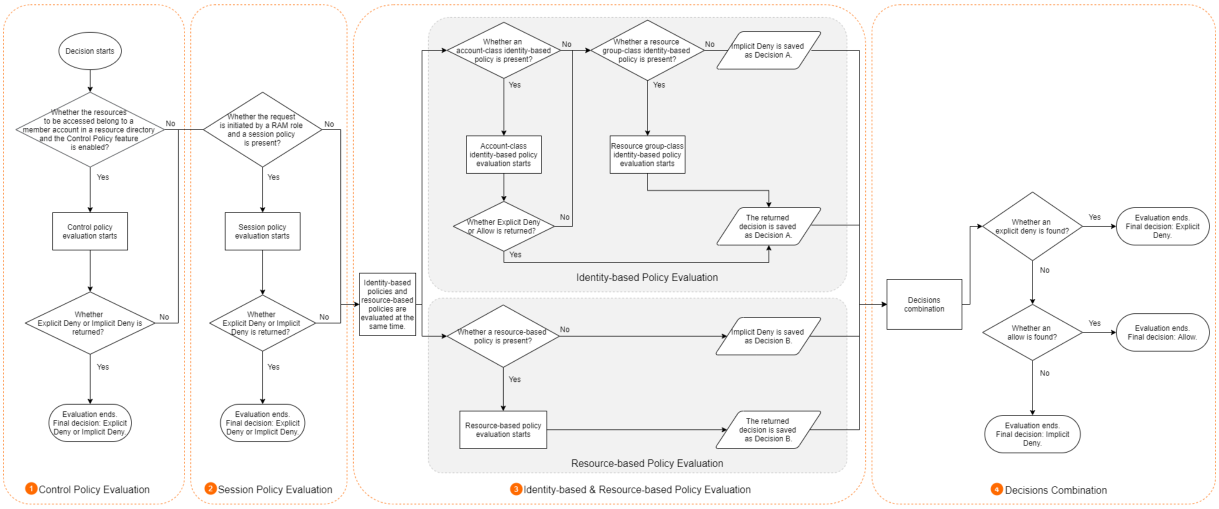
The following table describes the possible decisions.

Decision	Description
Allow	If a policy includes an Allow statement instead of a Deny statement, Allow is returned.
Explicit Deny	If a policy includes a Deny statement, Explicit Deny is returned. If the policy includes both a Deny statement and an Allow statement, the Deny statement takes precedence over the Allow statement. In this case, Explicit Deny is returned.
Implicit Deny	If a policy does not include an Allow statement or a Deny statement, Implicit Deny is returned. By default, all the requests initiated by a RAM identity are implicitly denied.

Standard evaluation process

The following figure shows how policies are evaluated and how a final decision is made.

> Note The majority of Alibaba Cloud services are separated based on Alibaba Cloud accounts. Some services allow access within the same account. Some services, such as Object Storage Service (OSS), allow access across accounts. The policy evaluation process applies to all cases.


Decision starts
Whether the resources to be accessed belong to a member account in a resource directory and the Control Policy feature is enabled?
No
Yes
Control policy evaluation starts
Whether Explicit Deny or Implicit Deny is returned?
No
Yes
Evaluation ends. Final decision: Explicit Deny or Implicit Deny.
1 Control Policy Evaluation
Whether the request is initiated by a RAM role and a session policy is present?
No
Yes
Session policy evaluation starts
Whether Explicit Deny or Implicit Deny is returned?
No
Yes
Evaluation ends. Final decision: Explicit Deny or Implicit Deny.
2 Session Policy Evaluation
Identity-based policies and resource-based policies are evaluated at the same time.
Whether an account-class identity-based policy is present?
No
Yes
Account-class identity-based policy evaluation starts
Whether Explicit Deny or Allow is returned?
No
Yes
Whether a resource group-class identity-based policy is present?
No
Yes
Resource group-class identity-based policy evaluation starts
Implicit Deny is saved as Decision A.
The returned decision is saved as Decision A.
Identity-based Policy Evaluation
Whether a resource-based policy is present?
No
Yes
Resource-based policy evaluation starts
Implicit Deny is saved as Decision B.
The returned decision is saved as Decision B.
Resource-based Policy Evaluation
3 Identity-based & Resource-based Policy Evaluation
Decisions combination
Whether an explicit deny is found?
Yes
Evaluation ends. Final decision: Explicit Deny.
No
Whether an allow is found?
Yes
Evaluation ends. Final decision: Allow.
No
Evaluation ends. Final decision: Implicit Deny.
4 Decisions Combination

A standard evaluation process includes the following steps:

1. **Control policy evaluation**

   Control policies allow you to manage the permission boundaries of the member accounts in a resource directory. If you want to access the resources of a member account in a resource directory and a control policy exists, Alibaba Cloud evaluates the control policy based on the basic evaluation process. For more information, see the "Basic evaluation process" section of this topic. Otherwise, this step is skipped.

   Alibaba Cloud decides whether to evaluate the next policy based on the decision:

   - If Explicit Deny or Implicit Deny is returned, the evaluation ends. The returned decision is the final decision.
   - If Allow is returned, the evaluation continues.

2. **Session policy evaluation**

   Session policies are policies that you pass as parameters when you programmatically create a temporary session for a RAM role. To programmatically create a role session, call the AssumeRole operation. If a RAM role initiates an access request and a session policy exists, Alibaba Cloud evaluates the session policy based on the basic evaluation process. For more information, see the "Basic evaluation process" section of this topic. Otherwise, this step is skipped.

   Alibaba Cloud decides whether to evaluate the next policy based on the decision:

   - If Explicit Deny or Implicit Deny is returned, the evaluation ends. The returned decision is the final decision.
   - If Allow is returned, the evaluation continues.

3. **Identity-based and resource-based policy evaluation**

   Identity-based policies and resource-based policies are evaluated at the same time. Decisions are temporarily saved and then combined at a later time.

   - **Identity-based policy evaluation**

For a RAM user, identity-based policies include the policies attached to the RAM usage and the policies inherited from the group to which the RAM user belongs. For a RAM role, identity-based policies are the policies attached to the RAM role. Identity-based policies are classified into account-class identity-based policies and resource group-class identity-based policies. The two classifications have different authorization granularities. During evaluation, account-class identity-based policies have a higher priority than resource group-class identity-based policies.

The following evaluation process is used to evaluate identity-based policies:

a. Alibaba Cloud checks whether the RAM identity that initiates the access request has an account-class identity-based policy.

- If an account-class identity-based policy exists, Alibaba Cloud evaluates the policy based on the basic evaluation process. For more information, see the "Basic evaluation process" section of this topic. Alibaba Cloud decides whether to evaluate the next policy based on the decision:
    - If Explicit Deny or Allow is returned, the evaluation ends. The returned decision is temporarily saved as Decision A.
    - If Implicit Deny is returned, the evaluation continues.
- If no account-class identity-based policies exist, the evaluation continues.

b. Alibaba Cloud checks whether the RAM identity that initiates the access request has a resource group-class identity-based policy.

- If a resource group-class identity-based policy exists, Alibaba Cloud evaluates the policy based on the basic evaluation process. For more information, see the "Basic evaluation process" section of this topic. The returned decision is temporarily saved as Decision A.
- If no resource group-class identity-based policies exist, Implicit Deny is saved as Decision A.

- **Resource-based policy evaluation**

  Alibaba Cloud checks whether the resources to be accessed have a resource-based policy.

  - If a resource-based policy exists, Alibaba Cloud evaluates the policy based on the basic evaluation process. For more information, see the "Basic evaluation process" section of this topic. The returned decision is temporarily saved as Decision B.
  - If no resource-based policies exist, Implicit Deny is saved as Decision B.

  > **Note** Alibaba Cloud provides bucket policies for OSS buckets and trust policies for RAM roles. If the resources to be accessed are not OSS buckets or RAM roles, this step is skipped. The returned decision of the identity-based policy is considered as the final decision.

4. **Combination of decisions**

   Alibaba Cloud combines Decision A and Decision B. The following logic is used to combine the decisions:

   - If an Explicit Deny decision is returned, the final decision is Explicit Deny. The evaluation ends.
   - If an Allow decision is returned, the final decision is Allow. The evaluation ends.
   - If neither an Explicit Deny nor an Allow decision is returned, the final decision is Implicit Deny. The evaluation ends.

> Note
>
> - Except for the preceding logic, the combination logic also depends on the cloud service to which the resources to be accessed belong. For information about exceptions, see Policy evaluation process of assuming a RAM role.
> - If the resources to be accessed belong to OSS, the bucket access control list (ACL) or object ACL are evaluated after policies are evaluated. For more information, see Authentication.

If the final decision is Allow, the request is allowed. If the final decision is Explicit Deny or Implicit Deny, the request is denied.

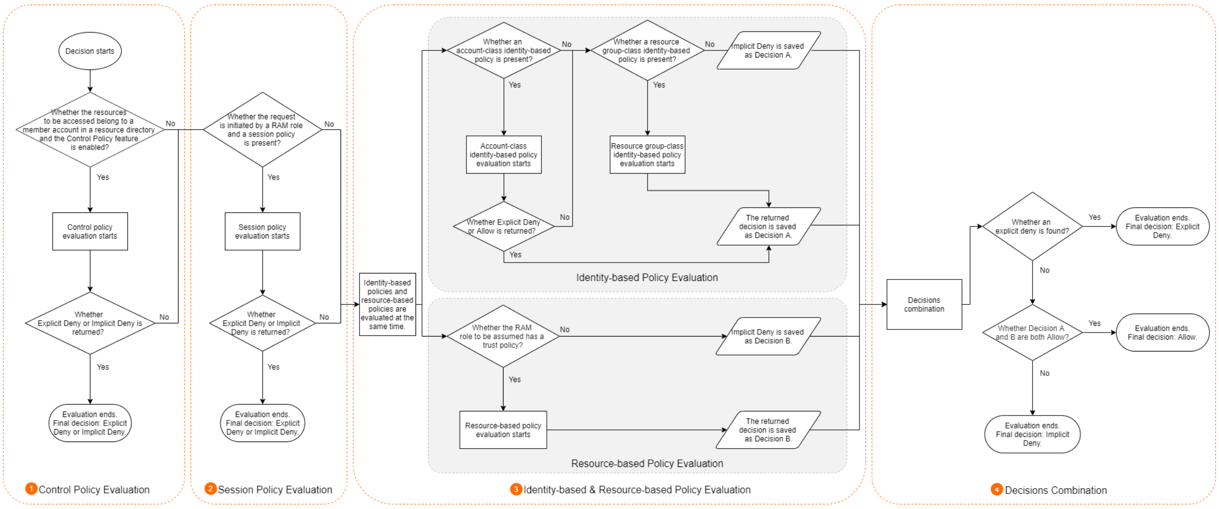
6.4. Policy evaluation process of assuming a RAM role

If a trusted entity attempts to assume a RAM role, a policy evaluation process is performed to determine whether to allow the request. The request can be initialized by using the Alibaba Cloud Management Console, API, or CLI. This topic describes the policy evaluation process that applies when you assume a Resource Access Management (RAM) role.

> Note The policy evaluation process of assuming a RAM role is the same as the Policy evaluation process except the decision combination process. If you are familiar with the Policy evaluation process, you only need to read the Decisions combination section of this topic.

If you create a role, you must specify a trusted entity for the role by adding a trust policy. In this case, trust policies take effect based on resources. If a trusted entity assumes a RAM role, the trusted entity must be granted required permissions. In this case, trust policies take effect based on identities.

When a trusted entity assumes a RAM role, the role is a resource to be accessed. Alibaba Cloud evaluates policies in sequence, as shown in the following figure.


Decision starts
Whether the resources to be accessed belong to a member account in a resource directory and the Control Policy feature is enabled?
No
Yes
Control policy evaluation starts
Whether Explicit Deny or Implicit Deny is returned?
No
Yes
Evaluation ends. Final decision: Explicit Deny or Implicit Deny.
1 Control Policy Evaluation
Whether the request is initiated by a RAM role and a session policy is present?
No
Yes
Session policy evaluation starts
Whether Explicit Deny or Implicit Deny is returned?
No
Yes
Evaluation ends. Final decision: Explicit Deny or Implicit Deny.
2 Session Policy Evaluation
Identity-based policies and resource-based policies are evaluated at the same time.
Whether an account-class identity-based policy is present?
No
Yes
Account-class identity-based policy evaluation starts
Whether Explicit Deny or Allow is returned?
No
Yes
Whether a resource group-class identity-based policy is present?
No
Yes
Implicit Deny is saved as Decision A.
Resource group-class identity-based policy evaluation starts
The returned decision is saved as Decision A.
Identity-based Policy Evaluation
Whether the RAM role to be assumed has a trust policy?
No
Yes
Implicit Deny is saved as Decision B.
Resource-based policy evaluation starts
The returned decision is saved as Decision B.
Resource-based Policy Evaluation
3 Identity-based & Resource-based Policy Evaluation
Decisions combination
Whether an explicit deny is found?
Yes
Evaluation ends. Final decision: Explicit Deny.
No
Whether Decision A and B are both Allow?
Yes
Evaluation ends. Final decision: Allow.
No
Evaluation ends. Final decision: Implicit Deny.
4 Decisions Combination

Alibaba Cloud evaluates multiple types of policies involved in the request based on the Basic evaluation process. A policy evaluation process consists of the following steps:

1. **Control policy evaluation**

Control policies allow you to manage the permission boundaries of the folders or member accounts in a resource directory. For example, the RAM role to be assumed belongs to a member account in a resource directory and the Control Policy feature is enabled. Alibaba Cloud evaluates the control policy based on the Basic evaluation process. Otherwise, this step is skipped.

Alibaba Cloud decides whether to evaluate the next policy based on the decision:

- If Explicit Deny or Implicit Deny is returned, the evaluation ends. The returned decision is the final decision.
- If Allow is returned, the evaluation continues.

2. **Session policy evaluation**

Session policies are policies that you pass as parameters when you programmatically create a temporary session for a RAM role. To programmatically create a role session, call the AssumeRole API operation. If a RAM role initiates an access request and a session policy is present, Alibaba Cloud evaluates the session policy based on the Basic evaluation process. Otherwise, this step is skipped.

> ⓘ **Note** If you implement role-based single sign-on (SSO), a session policy is absent. Therefore, this step is skipped.

Alibaba Cloud decides whether to evaluate the next policy based on the decision:

- If Explicit Deny or Implicit Deny is returned, the evaluation ends. The returned decision is the final decision.
- If Allow is returned, the evaluation continues.

3. **Identity-based and resource-based policy evaluation**

Identity-based policies and resource-based policies are evaluated at the same time. Decisions are temporarily saved for combination later.

- **Identity-based policy evaluation**

  For a RAM user, identity-based policies include the policies attached to the RAM user and the policies inherited from the group to which the RAM user belongs. For a RAM role, identity-based policies are the policies attached to the RAM role. Identity-based policies are divided into account-class identity-based policies and resource group-class identity-based policies, which have different authorization granularity. Account-class identity-based policies have a higher priority than resource group-class identity-based policies during evaluation.

  > ⓘ **Note** If you implement role-based SSO, the logon is not complete and an identity-based policy is absent. Therefore, this step is skipped. The returned decision of the resource-based policy is regarded as a final decision.

  The following evaluation process is used to evaluate identity-based policies:

a. Alibaba Cloud checks whether the RAM identity that initiates the access request has an account-class identity-based policy.

   - If an account-class identity-based policy is present, Alibaba Cloud evaluates the policy based on the Basic evaluation process. Alibaba Cloud decides whether to evaluate the next policy based on the decision:

     - If Explicit Deny or Allow is returned, the evaluation ends. The returned decision is temporarily saved as Decision A.

     - If Implicit Deny is returned, the evaluation continues.

   - If an account-class identity-based policy is absent, the evaluation continues.

b. Alibaba Cloud checks whether the RAM identity that initiates the access request has a resource group-class identity-based policy.

   - If a resource group-class identity-based policy is present, Alibaba Cloud evaluates the policy based on the Basic evaluation process. The returned decision is temporarily saved as Decision A.

   - If a resource group-class identity-based policy is absent, Implicit Deny is saved as Decision A.

- Resource-based policy evaluation

  Alibaba Cloud checks whether the RAM role to be assumed has a trust policy.

  - If a resource-based policy is present, Alibaba Cloud evaluates the policy based on the Basic evaluation process. The returned decision is temporarily saved as Decision B.

  - If a resource-based policy is absent, Implicit Deny is saved as Decision B.

4. Decisions combination

   Alibaba Cloud combines Decision A and Decision B. The combination logic is different from that of the standard Policy evaluation process. Only when Decision A and Decision B are both allowed, the request to assume a RAM role is allowed.

   The following combination logic is used to combine Decision A and Decision B:

   - If an explicit deny exists, the final decision is Explicit Deny.
   - If Decision A and Decision B are both allowed, the final decision is Allow. The evaluation ends.
   - In addition to the preceding two cases, the final decision is Implicit Deny. The evaluation ends.

7.Example policies

7.1. Overview of sample policies

This topic provides sample policies.

- Restart ECS instances
- Access Alibaba Cloud resources by using a specific IP address or CIDR block
- Access Alibaba Cloud in a specified period of time
- Access Alibaba Cloud by using a specified method
- Authorize a RAM user to manage MFA devices
- Authorize a RAM user to manage AccessKey pairs
- Manage a specified ECS instance
- View ECS instances in a specific region
- Manage ECS security groups within an Alibaba Cloud account
- Manage information about all resources within an Alibaba Cloud account except billing information
- View information about all cloud resources within an Alibaba Cloud account except billing information
- Grant permissions across cloud services
- Create a snapshot
- Manage an OSS bucket
- List and read resources in a bucket
- Access OSS through specified IP addresses
- Read data from a specified object in OSS
- Access and list specified files through OSS CLI
- Access a specified directory through the OSS console

7.2. Restart ECS instances

This topic uses an example policy to demonstrate how to authorize a RAM user to restart ECS instances.

The following policy indicates that the authorized RAM user can restart ECS instances. The ECS instances can be restarted only when MFA is enabled for the RAM user and the RAM user uses MFA to log on. In this case, the `acs:SecureTransport` condition key in the `Condition` element is set to `true` .

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

Note The `Condition` element applies only to the actions that are specified in the policy. You can set the `acs:MFAPresent` condition key to `true` or `false`.

7.3. Access Alibaba Cloud resources by using a specific IP address or CIDR block

This topic provides a sample policy that you can use to authorize your Resource Access Management (RAM) users. This policy allows RAM users to access Alibaba Cloud resources by using a specific IP address or Classless Inter-Domain Routing (CIDR) block.

In the following code, the RAM users can access Elastic Cloud Service (ECS) instances only by using 172.16.215.218 and 192.168.0.0/16.

You must specify `acs:SourceIp` in `Condition`, as shown in the following code.

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

Note

- `Condition` is applicable only to the actions that are specified in the policy.
- The value of `acs:SourceIp` in the preceding code is only for reference. You must specify the value based on your business requirements.

7.4. Access Alibaba Cloud in a specified period of time

This topic uses an example policy to demonstrate how to authorize a RAM user to access Alibaba Cloud in a specified period of time.

The following policy indicates that the authorized RAM user can only access Alibaba Cloud ECS before 17:00 on August 12, 2019 (UTC+8). In this case, the `acs:CurrentTime` condition key 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 only applies to the actions specified for the current policy. You can change the `2019-08-12T17:00:00+08:00` value as needed.

7.5. Access Alibaba Cloud by using a specified method

This topic uses an example policy to demonstrate how to authorize a RAM user to access Alibaba Cloud by using a specified method.

The following policy indicates that the authorized RAM user can only access Alibaba Cloud ECS through 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 only applies to the actions specified for the current policy. You can set the `acs:SecureTransport` condition key to `true` or `false` .

7.6. Authorize a RAM user to manage MFA devices

This topic describes how to authorize a Resource Access Management (RAM) user to manage multi-factor authentication (MFA) devices by using an example policy.

The following policy indicates that the authorized RAM user `alice` can enable and disable MFA devices.

```
{
   "Statement": [
       {
           "Action": [
               "ram:GetUserMFAInfo",
               "ram:BindMFADevice",
               "ram:UnbindMFADevice"
           ],
           "Resource": "acs:ram:*:*:user/alice",
           "Effect": "Allow"
       },
       {
           "Action": [
               "ram:CreateVirtualMFADevice",
               "ram:DeleteVirtualMFADevice"
           ],
           "Resource": "*",
           "Effect": "Allow"
       }
   ],
   "Version": "1"
}
```

If you want to authorize a specific RAM user in your Alibaba Cloud account to manage MFA devices, you can attach the policy to the RAM user. Unauthorized RAM users cannot manage MFA devices.

To authorize all the RAM users in your Alibaba Cloud account to manage MFA devices, perform the following steps: Log on to the RAM console. In the left-side navigation pane, choose Identities > Settings. On the Settings page, click Update RAM User Security Settings in the RAM User Security section. In the Update RAM User Security Settings panel, set **Manage MFA Devices** to **Allowed**. For more information, see Configure security policies for RAM users.

7.7. Authorize a RAM user to manage AccessKey pairs

This topic describes how to authorize a Resource Access Management (RAM) user to manage AccessKey pairs by using an example policy.

The following policy indicates that the authorized RAM user `alice` can update the status of, create, and delete AccessKey pairs.

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
      "ram:CreateAccessKey",
      "ram:ListAccessKeys",
      "ram:UpdateAccessKey",
      "ram:DeleteAccessKey"
      ],
      "Resource": "acs:ram:*:*:user/alice",
      "Effect": "Allow"
    }
  ]
}
```

If you want to authorize a specific RAM user in your Alibaba Cloud account to manage its own AccessKey pairs, you can attach the policy to the RAM user.

To authorize all the RAM users in your Alibaba Cloud account to manage their own AccessKey pairs, perform the following steps: Log on to the RAM console. In the left-side navigation pane, choose Identities > Settings. On the Settings page, click Update RAM User Security Settings in the RAM User Security section. In the Update RAM User Security Settings panel, set **Manage AccessKey** to **Allowed**. For more information, see Configure security policies for RAM users.

7.8. Manage a specified ECS instance

This topic uses an example policy to demonstrate how to authorize a RAM user to manage a specified ECS instance.

The following policy indicates that the authorized RAM user can view all ECS instances under an Alibaba Cloud account, but the user can manage only the `i-001` ECS instance.

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

? **Note** The `Describe*` element is required in the policy. Otherwise, the authorized RAM user cannot view instances in the console. However, the RAM user can manage the specified ECS instance through API operations, CLI, or ECS SDK.

7.9. View ECS instances in a specific region

This topic describes how to authorize a Resource Access Management (RAM) user to view Elastic Compute Service (ECS) instances in a specific region. A policy is used as an example in this topic.

The following policy indicates that the authorized RAM user can view ECS instances in the China (Qingdao) region, but cannot view disks or snapshots in this region.

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

? **Note** You can grant permissions on ECS instances to the RAM user based on the region and resource type. If you want to authorize a RAM user or role to view ECS instances in another region, you can change `cn-qingdao` in the `Resource` element to the ID of the required region. For more information about region IDs, see Regions and zones.

7.10. Manage ECS security groups within an Alibaba Cloud account

This topic describes how to authorize a Resource Access Management (RAM) user to manage Elastic Compute Service (ECS) security groups within an Alibaba Cloud account. This topic provides a policy as an example.

The following policy specifies that the authorized RAM user can manage ECS security groups within an Alibaba Cloud.

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

7.11. Manage information about all resources within an Alibaba Cloud account except billing information

This topic describes how to authorize a RAM user to manage information about all cloud resources within an Alibaba Cloud account except billing information. This topic provides a policy as an example.

The following policy specifies that the authorized RAM user can manage information about all cloud resources within an Alibaba Cloud account except billing information.

```
{
 "Statement": [{
   "Action": "*",
   "Effect": "Allow",
   "Resource": "*"
  },
  {
   "Action": [
    "bss:*",
    "bssapi:*",
    "efc:*"
   ],
   "Effect": "Deny",
   "Resource": "*"
  }
 ],
 "Version": "1"
}
```

7.12. View information about all cloud resources within an Alibaba Cloud account except billing information

This topic describes how to authorize a Resource Access Management (RAM) user to view information about all cloud resources within an Alibaba Cloud account except billing information. This topic provides a policy as an example.

The following policy specifies that the authorized RAM user can view information about all cloud resources within an Alibaba Cloud account except billing information.

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "*:Describe*",
                "*:List*",
                "*:Get*",
                "*:BatchGet*",
                "*:Query*",
                "*:BatchQuery*",
                "actiontrail:LookupEvents",
                "dm:Desc*",
                "dm:SenderStatistics*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
    {
            "Action": [
                "bss:*",
                "efc:*"
            ],
            "Effect": "Deny",
            "Resource": "*"
        }
    ]
}
```

7.13. Grant permissions across cloud services

If you want to authorize a cloud service to access resources of a different cloud service, you must grant permissions across these cloud services. This topic uses example policies to demostrate how to grant permissions across cloud services.

To grant permissions across cloud services, you can use policies of general authorization or fine-grained authorization.

- General authorization

  Authorized RAM users that belong to an Alibaba Cloud account can authorize a specific cloud service to access resources of other cloud services.

```
{
    "Statement": [
        {
            "Action": [
                "ram:CreateRole",
                "ram:AttachPolicyToRole"
            ],
            "Effect": "Allow",
            "Resource": [
                "*"
            ]
        }
    ],
    "Version": "1"
}
```

- Fine-grained authorization

  Authorized RAM users that belong to an Alibaba Cloud account can authorize a specific cloud service to access resources of another cloud service.

  > **Note** Compared with the policy of general authorization, the policy of fine-grained authorization specifies RAM roles and policy names. In this example, the RAM role is `aliyuncasdefaultrole`, and the system policy for SSL Certificates Service is `AliyunCASRolePolicy`.

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "ram:AttachPolicyToRole",
                "ram:CreateRole"
            ],
            "Resource": [
                "acs:ram:*:system:policy/AliyunCASRolePolicy",
                "acs:ram:*:*:role/aliyuncasdefaultrole"
            ],
            "Effect": "Allow"
        }
    ]
}
```

7.14. Create a snapshot

This topic uses an example policy to demonstrate how to authorize a RAM user to create a snapshot.

The following policy indicates that the authorized RAM user can create a snapshot by granting ECS administrator permissions and disk permissions. 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"
}
```

7.15. Manage an OSS bucket

This topic uses an example policy to demonstrate how to authorize a RAM user to manage an Object Storage Service (OSS) bucket.

The following policy indicates that the authorized RAM user can manage an OSS bucket named `myphotos` .

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

7.16. List and read resources in a bucket

This topic uses two example policies to demonstrate how to authorize a RAM user to list and read resources in a bucket.

- The following policy indicates that the authorized RAM user can list and read resources contained in the `myphotos` bucket by using Object Storage Service (OSS) SDKs or OSS CLI.

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

- The following policy indicates that the authorized RAM user can list and read resources contained in the `myphotos` bucket by using the OSS console.

> **Note** When you log on to the OSS console, the `ListBuckets`, `GetBucketAcl`, and `GetObjectAcl` API operations are automatically called to determine whether the bucket is public or private.

```
{
    "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/*"
        }
    ]
}
```

7.17. Access OSS through specified IP addresses

This topic uses an example policy to demonstrate how to access Object Storage Service (OSS) through specified IP addresses.

- The following policy indicates that the authorized RAM user can read data from the `myphotos` directory through an IP address in the `192.168.0.0/16` and `172.12.0.0/16` CIDR blocks.

```
{
    "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"]
                }
            }
        }
    ]
}
```

- The following policy indicates that the authorized RAM user cannot access OSS unless the IP address of the RAM user is in the `192.168.0.0/16` CIDR block.

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

```
{
    "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"]
                }
            }
        }
    ]
}
```

7.18. Read data from a specified object in OSS

This topic uses an example policy to demonstrate how to read data from a specified object in OSS.

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

```
myphotos[Bucket]
  ├── beijing
  │    ├── 2014
  │    └── 2015
  ├── hangzhou
  │    ├── 2013
  │    ├── 2014
  │    └── 2015
  └── qingdao
       ├── 2014
       └── 2015
```

The following policy indicates that the authorized RAM user can read data from the `myphotos/hangzhou/2015/` directory, but cannot list objects.

> ⓘ **Note** The RAM user knows the path of the object and can read data from the object. We recommend that you attach this policy to your applications.

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

7.19. Access and list specified files through OSS CLI

This topic uses an example policy to demonstrate how to access and list specified files through Object Storage Service (OSS) CLI.

The following policy indicates that the authorized RAM user can use OSS CLI to access the `myphotos/hangzhou/2015/` directory and list the files in this directory.

> ⓘ **Note** The RAM user does not know what files are stored in the directory, but can use OSS CLI or call API operations to obtain the directory information. We recommend that you attach this policy to your software developers.

```
{
    "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/*"
                }
            }
        }
    ]
}
```

7.20. Access a specified directory through the OSS console

This topic uses an example policy to demonstrate how to access a specified directory through the Object Storage Service (OSS) console.

The following policy indicates that the authorized RAM user can access the `myphotos/hangzhou/2015/` directory through the OSS console (similar to Windows File Manager).

> **Note** The RAM user can access the directory level by level.

```
{
    "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/*"
                    ]
                }
            }
        }
    ]
}
```

7.21. Manage a resource group

This topic describes how to authorize a Resource Access Management (RAM) user to manage a resource group by using an example policy.

The following policy allows the authorized RAM user to create and delete resource groups in Resource Management. The policy also allows the authorized RAM user to view and modify the basic information about resource groups in Resource Management.

```
{
    "Statement": [{
        "Action": "ram:*ResourceGroup*",
        "Effect": "Allow",
        "Resource": "*"
    }],
    "Version": "1"
}
```

> ? **Note** If you want to authorize a RAM user to perform more group-related operations, such as managing resources in a resource group, granting permissions to a resource group, or migrating resources across resource groups, you must attach other policies to the RAM user. For more information, see Resource Group.