ALIBABA CLOUD

Alibaba Cloud

Resource Access Management
Policy Management

Document Version: 20200910

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.Policy overview

You can manage the access in Alibaba Cloud by creating polices and attaching them to RAM identities (RAM users, RAM user groups, or RAM roles) or Alibaba Cloud resources. When a policy is associated with an identity or an Alibaba Cloud resource, the policy defines the permissions of the identity or resource.

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.

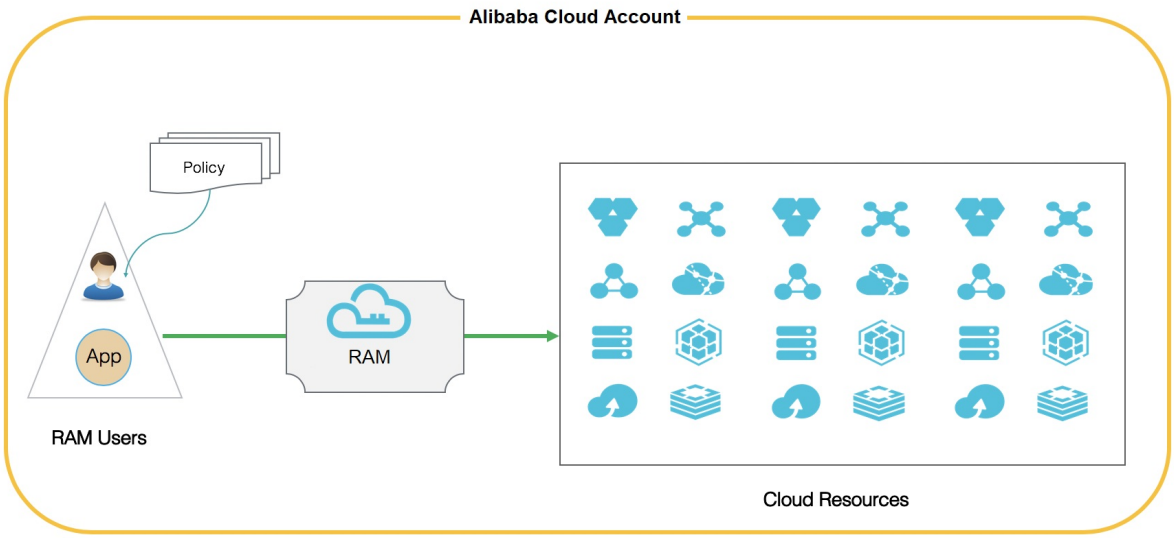
- The attached policies can be system policies or custom policies.
- If the attached policies are modified, the new policies automatically take effect. You do not need to attach the new policies to RAM identities.

2.Policy models

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

Manage the resources of an Alibaba Cloud account

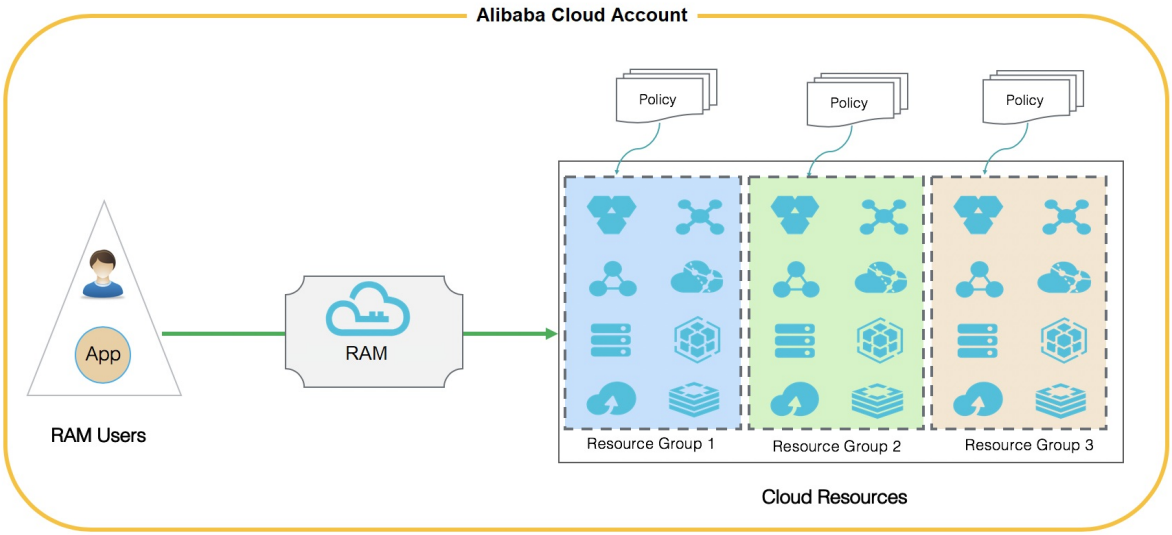
In this model, if you attach a policy to a RAM identity, all Alibaba Cloud resources under the Alibaba Cloud account are included in the scope of the policy permissions.



Manage the resources of a target resource group

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

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, description, and references.

Procedure

1. Log on to the RAM console with an Alibaba Cloud account.
2. In the left-side navigation pane, click **Policies** under **Permissions**.
3. From the **Policy Type** drop-down list, select **System Policy** or **Custom Policy**.
4. Enter a policy name or description into the search box, and click  .

> **Note** You can enter keywords for fuzzy matching.

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 finer-grained access control than system policies.

Prerequisites

You have a basic knowledge of the policy elements, structure, and syntax. For more information, see Policy structure and syntax.

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **Policies** under **Permissions**.
3. On the **Policies** page, click **Create Policy**.
4. On the page that appears, specify the **Policy Name** and **Note** parameters.
5. In the **Configuration Mode** section, select **Visualized** or **Script**.
   - If you select **Visualized**, click **Add Statement**. In the dialog box that appears, specify the permission effect, actions, and resources.
   - If you select **Script**, edit the policy in the **Policy Document** section. For more information, see Policy structure and syntax.
6. Click **OK**.

Related information

- CreatePolicy

4.2. Modify a custom policy

This topic describes how to modify a custom policy. If the permissions of a RAM user are changed, you must modify the corresponding policy attached to the RAM user.

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **Policies** under **Permissions**.
3. In the **Policy Name** column, click the name of the target custom policy.

   > **Note** System policies and custom policies are available in Alibaba Cloud Resource Access Management (RAM). System policies can be viewed but cannot be modified. However, custom policies can be created, viewed, and modified.

4. On the **Policy Document** tab, click **Modify Policy Document** and modify the policy document based on your business needs.

> Note For information about how to modify a policy document, see Policy structure and syntax.

5. Click OK.

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

Related information

- CreatePolicyVersion

4.3. Manage custom policy versions

This topic describes how to manage custom policy versions, including how to view a policy version, specify the default policy version, and delete a policy version.

Context

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

Procedure

1. Log on to the RAM console with an Alibaba Cloud account.
2. In the left-side navigation pane, click **Policies** under **Permissions**.
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 version and its document, click **View** in the Actions column.
   - To specify a policy version as the default 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

4.4. Delete a custom policy

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

Prerequisites

- The policy has only one version, which is the default version. If more than one version exists, delete all versions except the default version.
- The policy is not referenced, which means that the policy is not attached to a RAM user, RAM user group, or RAM role. If the policy is being referenced, delete the references to the policy. For more information, see Manage policy references.

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **Policies** under **Permissions**.
3. On the **Policies** page, select **Custom Policy** from the **Policy Type** drop-down list.
4. Find the target custom policy in the **Policy Name** column and click **Delete** in the Actions column.
5. In the message that appears, click **OK**.

Related information

- DeletePolicy

5.Manage policy references

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

Procedure

1. Log on to the RAM console by using an Alibaba Cloud account.
2. In the left-side navigation pane, click **Policies** under **Permissions**.
3. In the **Policy Name** column, click the name of the target policy.
4. Click the **References** tab. On this tab, you can view or delete references.
   - You can view the reference details, including the principal and principal type.
   - You can delete a reference. To do this, click **Revoke Permission** in the **Actions** column, and then click **OK** in the message that appears.

Related information

- ListEntitiesForPolicy

6.Policy language

6.1. Policy elements

This topic describes the elements of policies that are used to define permissions in Alibaba Cloud Resource Access Management (RAM).

Elements

Element	Description
Effect	Specifies whether the statement results in an explicit allow or an explicit deny. Valid values: Allow and Deny.
Action	Describes one or more 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.

Rules for using policy elements

- 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

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

  > **Note** In most cases, each Alibaba Cloud service has its own set of API operations. For more information, see Alibaba Cloud services that support RAM.

  Syntax: `<service-name>:<action-name>`

  - `service-name`: the name of an Alibaba Cloud service
  - `action-name: service`: one or more API operation names from the service

  Example: `"Action": ["oss:ListBuckets", "ecs:Describe*", "rds:Describe*"]`

- Resource

  This element specifies one or more objects that the statement covers.

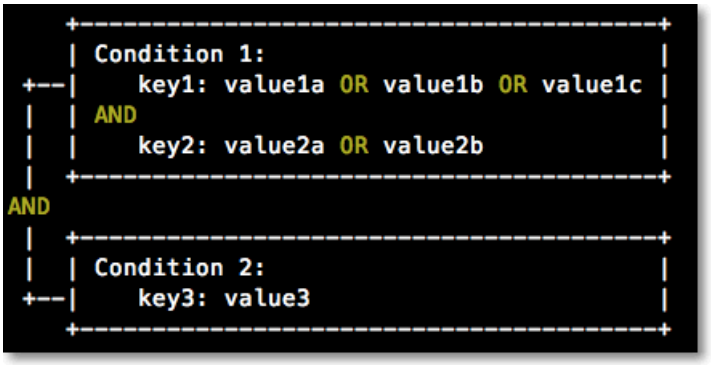
Syntax: `acs:<service-name>:<region>:<account-id>:<relative-id>`. The syntax is the same as the format of an Alibaba Cloud Resource Name (ARN).

- `acs`: the abbreviation of Alibaba Cloud Service, which indicates the public cloud of Alibaba Cloud.
- `service-name`: the name of an Alibaba Cloud service.
- `region`: the region information. If this element is not supported, use the asterisk (`*`) wildcard character.
- `account-id`: the Alibaba Cloud account ID, for example, `123456789012****`. If no ID is required or available, use an asterisk (`*`).
- `relative-id`: the identifier of the service-related resource. The meaning of this element varies by service. The value of the relative-id element can be a file path. For example, `relative-id = "mybucket/dir1/object1.jpg"` indicates an OSS object.

Example: `"Resource": ["acs:ecs:*:*:instance/inst-001", "acs:ecs:*:*:instance/inst-002", "acs:oss:*:*:mybucket", "acs:oss:*:*:mybucket/*"]`

- Condition

  A condition block can contain one or more conditions, and each condition consists of a condition operator, key, and value.



  Evaluation logic:

  - You can specify one or more values for a condition key. If the value in a request matches any of the values, the condition is met.
  - You can specify one or more condition keys for a single condition operator in a condition. The condition is met only if all the requirements for the keys are met.
  - A condition block is met only if all of its conditions are met.

  Condition operators:

  The condition operators are grouped into the following categories: string, numeric, date and time, Boolean, and IP address.

Category	Condition operator

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

Condition keys:

- The syntax of a common condition key is `acs:<condition-key>`.

Common condition key	Category	Description
`acs:CurrentTime`	Date and time	The time when the web server receives a request. Specify the time in the ISO 8601 standard, for 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.
`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` key, the value must be an IP address, for example, 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.

- The syntax of a condition key that is specific to an Alibaba Cloud service is `<service-name>:<condition-key>`.

Condition key specific to an Alibaba Cloud service	Alibaba Cloud service	Category	Description
`ecs:tag/<tag-key>`	ECS	String	The tag key for the ECS resource. This key can be customized.
`rds:ResourceTag/<tag-key>`	RDS	String	The tag key for the RDS resource. This key can be customized.
`oss:Delimiter`	OSS	String	The delimiter that is used to categorize object names.
`oss:Prefix`	OSS	String	The prefix of object names.

6.2. Policy structure and syntax

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

Conventions used in policy syntax

The following conventions are used in the policy syntax:

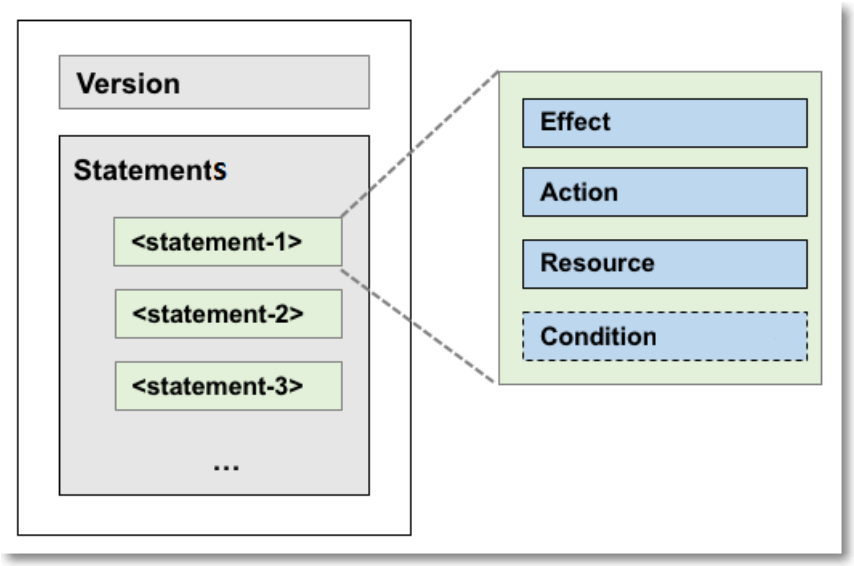
- Characters in a policy
  - The following characters are JSON tokens in the policy syntax: `{ } [ ] " , :`.
  - The following characters are special characters in the policy syntax: `= < > ( ) |`.
- Use of characters
  - If an element can have more than one value, you can perform one of the following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

- Strings are enclosed in double quotation marks ("), for 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. For more information about the elements, see Policy elements.



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")
```

Description:

- Version: The current policy version is 1. The version cannot be changed.
- Statement: The policy can have multiple statements.
  - The effect of each statement can be `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 with different operators and logical combinations of these conditions.

- 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 number or Boolean value, it must be enclosed in double quotation marks ("). This is the same method that is used for strings.
  - If an element value is a string, characters such as the asterisk (`*`) and question mark (`?`) can be used for fuzzy match.
    - The asterisk (`*`) indicates a number (including zero) of allowed characters. For example, `ecs:Describe*` indicates all ECS API operations that start with `Describe` .
    - `?` indicates an allowed character.

Policy syntax check

Policies are stored in RAM as JSON files. When you create or edit a policy, RAM first checks whether the JSON syntax is valid.

- For more information about JSON syntax standards, visit RFC 7159.
- We recommend that you use tools such as JSON validators and editors to check whether policies meet JSON syntax standards.

6.3. Policy check rules

This topic describes the policy check rules of RAM to provide a better understanding of RAM policies.

Policy check rules

You can access Alibaba Cloud resources by using an Alibaba Cloud account, or as an authorized RAM user or RAM role.

RAM determines whether to allow access based on the following rules.

Access type	Rule

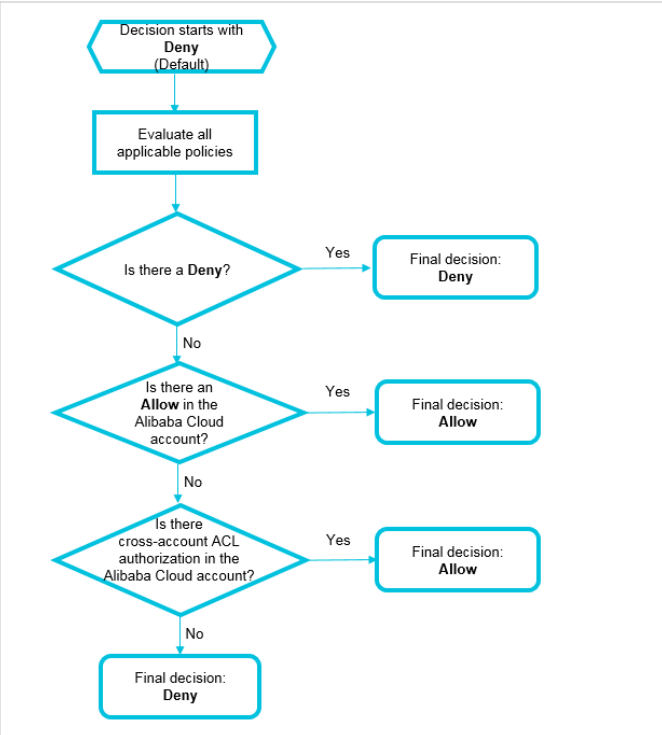
Access type	Rule
Alibaba Cloud account	The Alibaba Cloud account is the resource owner and can access all the Alibaba Cloud resources under the account. Note Some Alibaba Cloud services, such as Log Service, support cross-account access based on the access control list (ACL) authorization. If an Alibaba Cloud account is authorized by using the ACL, access is allowed even if the Alibaba Cloud account is not the resource owner.
RAM user	• The Alibaba Cloud account has attached an explicit allow policy to the RAM user. • The Alibaba Cloud account to which the RAM user belongs has permission to access the resources specified in the policy. • The Alibaba Cloud account to which the RAM user belongs is authorized by using the ACL for cross-account access. Note By default, a RAM user does not have permission to access Alibaba Cloud resources. A RAM user can access Alibaba Cloud resources only when the preceding rules are met. For more information, see Policy check rules for RAM users.

Access type	Rule
RAM role	• The STS token of the RAM role contains the required permissions. For more information, see What is STS? • The Alibaba Cloud account has attached an explicit allow policy to the RAM role. • The Alibaba Cloud account to which the RAM role belongs has permission to access the resources specified in the policy. • The Alibaba Cloud account to which the RAM user belongs is authorized by using the ACL for cross-account access. Note By default, a RAM role does not have permission to access Alibaba Cloud resources. A RAM role can access Alibaba Cloud resources only when the preceding rules are met. For more information, see Policy check rules for RAM roles.

Policy check rules for RAM users

By default, a RAM user does not have permissions. A RAM user can access resources only after an Alibaba Cloud account grants the required permissions to the RAM user. The required permissions must be granted by attaching one or more explicit allow policies to the RAM user.

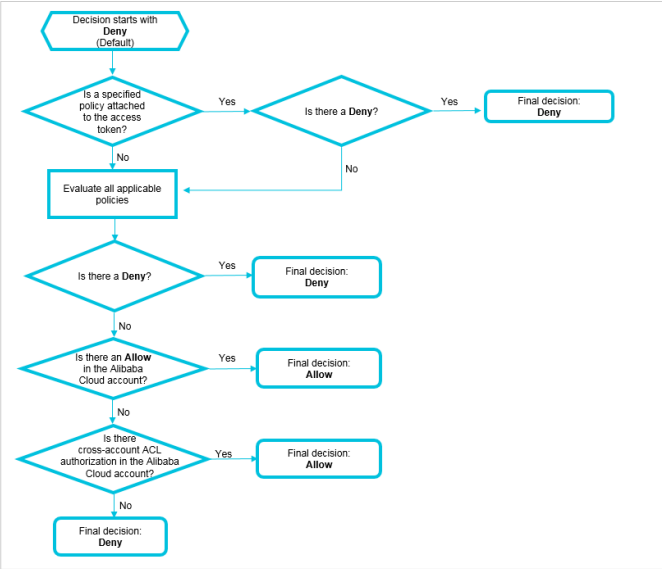
Note A policy can contain Allow and Deny statements. If policies that apply to a request include an Allow statement and a Deny statement, the Deny statement prevails.



1. The system checks whether the policy that is attached to a RAM user has a Deny statement.
   - If yes, access is denied.
   - If no, go to the next step.
2. The system checks whether the policy that is attached to the Alibaba Cloud account of the RAM user has an Allow statement.
   - If yes, access is allowed.
   - If no, go to the next step.
3. The system checks whether the Alibaba Cloud account of the RAM user is authorized by using the ACL for cross-account access.
   - If yes, access is allowed.
   - If no, access is denied.

Policy check rules for RAM roles

You can access Alibaba Cloud resources as a RAM role by using an STS token. To do this, you can call the AssumeRole API operation where the Policy request parameter specifies the resource access permissions.



1. The system checks whether a policy is attached to the STS token.
   - If a policy is attached to the STS token, the system checks whether the policy has a Deny statement.
     - If yes, access is denied.
     - If no, the system checks the policy attached to the RAM role.
   - If no policy is attached to the STS token, the system checks the policy attached to the RAM role.
2. The system checks whether the policy that is attached to the RAM role has a Deny statement.
   - If yes, access is denied.
   - If no, go to the next step.
3. The system checks whether the policy that is attached to the Alibaba Cloud account of the RAM role has an Allow statement.
   - If yes, access is allowed.
   - If no, go to the next step.
4. The system checks whether the Alibaba Cloud account of the RAM role is authorized by using the ACL for cross-account access.
   - If yes, access is allowed.
   - If no, access is denied.

7.Example policies

7.1. 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`.

7.2. Access Alibaba Cloud through a specified CIDR block

This topic uses a sample policy to demonstrate how to authorize a RAM user to access Alibaba Cloud through a specified CIDR block.

The following policy indicates that the authorized RAM user can access ECS instances only from IP addresses in the 192.168.0.0/16 CIDR block.

In this case, the `acs:SourceIp` condition key in the `Condition` element is set to `192.168.0.0/16`.

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

Note The `Condition` element only applies to the actions specified for the current policy. You can replace the `192.168.0.0/16` CIDR block with the CIDR block of your private network.

7.3. 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.

7.4. 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`.

7.5. Manage MFA

This topic uses an example policy to demonstrate how to authorize a RAM user to manage multi-factor authentication (MFA).

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"
}
```

Note For information about how to authorize a RAM user to manage MFA through the RAM console, see Set security policies for RAM users.

7.6. Manage AccessKey pairs

This topic uses an example policy to demonstrate how to authorize a RAM user to manage AccessKey pairs.

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

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

You can attach the policy to RAM users if you need to authorize the RAM users to manage their own AccessKey pairs. Unauthorized RAM users cannot manage their AccessKey pairs.

To allow all RAM users under the Alibaba Cloud account to manage their own AccessKey pairs, perform the following steps: Log on to the RAM console and choose **Identities** > **Settings** > **Update RAM User Security Settings**. In the pane that appears, select **Allowed** under **Manage AccessKey**. For more information, see Set security policies for RAM users.

7.7. 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.

7.8. View ECS instances in a specified region

This topic uses a sample policy to demonstrate how to authorize a RAM user to view ECS instances in a specified region.

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 ECS permissions to the RAM user by 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 target region. For a list of region IDs, see .

7.9. Manage ECS security groups under an Alibaba Cloud account

This topic uses an example policy to demonstrate how to authorize a RAM user to manage ECS security groups under an Alibaba Cloud account.

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

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

7.10. Manage information of all resources under an Alibaba Cloud account except billing information

This topic uses an example policy to demonstrate how to authorize a RAM user to manage information of all resources under an Alibaba Cloud account except billing information.

The following policy indicates that the authorized RAM user can manage information of all resources under an Alibaba Cloud account except billing information.

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

7.11. View information of all cloud resources under an Alibaba Cloud account except billing information

This topic uses an example policy to demonstrate how to authorize a RAM user to view information of all cloud resources under an Alibaba Cloud account except billing information.

The following policy indicates that the authorized RAM user can view information of all cloud resources under 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": "*"
    }

  ]
}
```

7.12. Grant permissions across cloud services

This topic uses two example policies to demonstrate how to grant permissions across cloud services.

Granting permissions across cloud services refers to authorizing a cloud service to access resources of another cloud service. To grant permissions across cloud services, you can use general authorization and precise authorization.

- General authorization: Authorized RAM users under an Alibaba Cloud account can grant permissions across cloud services.

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

- Precise authorization: Authorized RAM users under an Alibaba Cloud account can only authorize Alibaba Cloud SSL Certificates Service to access resources of other cloud services.

  > **Note** Compared with the policy of general authorization, the policy of precise authorization specifies a RAM role and policy name. In this example, the RAM role is `AliyunCASDefaultRole` and the system policy of Alibaba Cloud SSL Certificates Service is `AliyunCASRolePolicy`.

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

7.13. 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"
}
```

7.14. 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/*"
      ]
    }
  ]
}
```

7.15. 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/*"
    }
  ]
}
```

7.16. 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"]
          }
        }
      }
    ]
}
```

7.17. 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/*"
      ]
    }
  ]
}
```

7.18. 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/*"
        }
      }
    }
  ]
}
```

7.19. 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/*"
```

```
            ]
          }
        }
      }
    ]
}
```