

Alibaba Cloud Resource Access Management Policy Management

Issue: 20190917

Legal disclaimer

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

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

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

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

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK.
Courier font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>switch {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Policy overview.....	1
2 Policy models.....	3
3 View basic information about a policy.....	5
4 Custom policies.....	6
4.1 Create a custom policy.....	6
4.2 Modify a custom policy.....	6
4.3 Manage policy versions.....	7
4.4 Delete a custom policy.....	8
5 Manage policy references.....	9
6 Policy language.....	10
6.1 Policy elements.....	10
6.2 Policy structure and grammar.....	14
6.3 Policy check rules.....	18
7 Best practices.....	24
7.1 Use RAM to maintain security of your Alibaba Cloud resources.....	24

1 Policy overview

You can manage access in Alibaba Cloud by creating policies and attaching them to RAM identities (RAM users, RAM user groups, or RAM roles) or Alibaba Cloud resources. A policy, when associated with an identity or an Alibaba Cloud resource, defines their permissions.

Permission

A statement within a policy that allows or denies access to a particular Alibaba Cloud resource.

- An Alibaba Cloud account (resource owner) controls all permissions.
 - Each Alibaba Cloud resource has only one owner. The owner must be an Alibaba Cloud account and has full resource control permissions.
 - 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 RAM user's Alibaba Cloud account. The RAM user is the resource creator, but is not the resource owner.
- By default, a RAM user has no permissions.
 - A RAM user is an operator and must be granted explicit permission before performing any operations.
 - A new RAM user has no operation permissions by default, and cannot perform operations on Alibaba Cloud resources through the console or APIs until being granted permission.
- A resource creator (RAM user) is not automatically granted permissions for the created resources.
 - A RAM user can create resources if the user is granted the resource creation permission.
 - However, the RAM user is not automatically granted any permissions for the created resources, unless the resource owner explicitly grants permission to the user.

Policy

A set of permissions that are described by using policy structure and grammar. It can accurately describe the authorized resource sets, operation sets, and authorization

conditions a user can be granted with. For information about structures and grammars supported by RAM, see [#unique_4](#).

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

- **System policy:** System policies are created by Alibaba Cloud and cannot be modified by users. The policies are automatically upgraded by Alibaba Cloud.
- **Custom policy:** If no system policy meets your requirements, you can create a custom policy as needed. You can also modify and delete a custom policy as needed.
-

You can attach one or more policies to RAM users, RAM user groups, or RAM roles. For more information, see [#unique_5](#), [#unique_6](#), and [#unique_7](#).

Policies attached to RAM identities

You can attach one or more policies to RAM identities to grant necessary permissions to them.

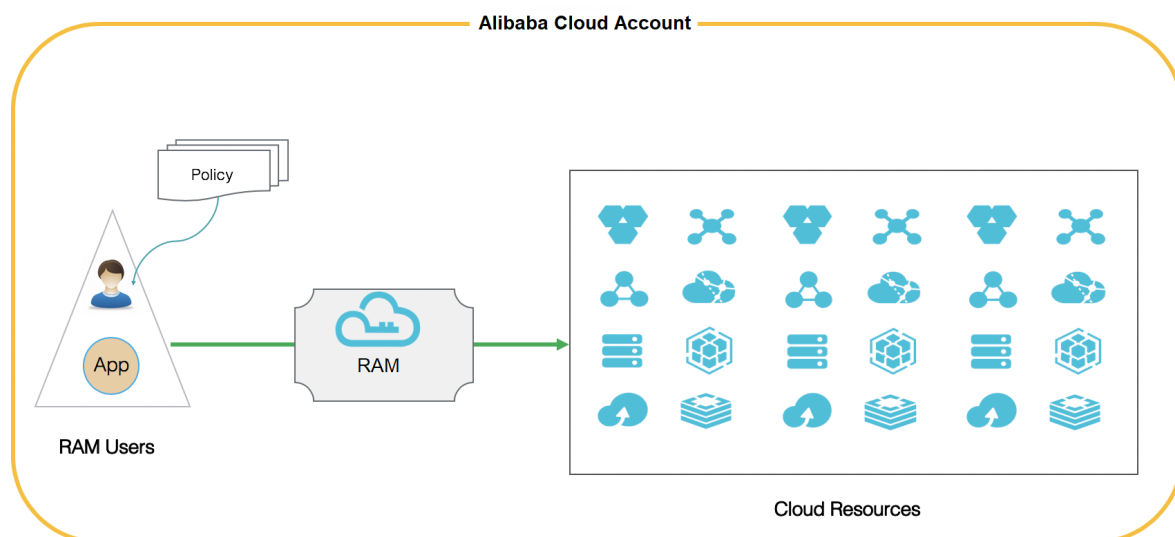
- The attached policy can be either a system policy or a custom policy.
- If the attached policy is updated, the updates to the policy automatically take effect, and you do not need to attach the policy again.

2 Policy models

Alibaba Cloud allows you to grant permission for an Alibaba Cloud account or for a resource group. You can select an appropriate model according to your specific requirements.

Grant permission for an Alibaba Cloud account

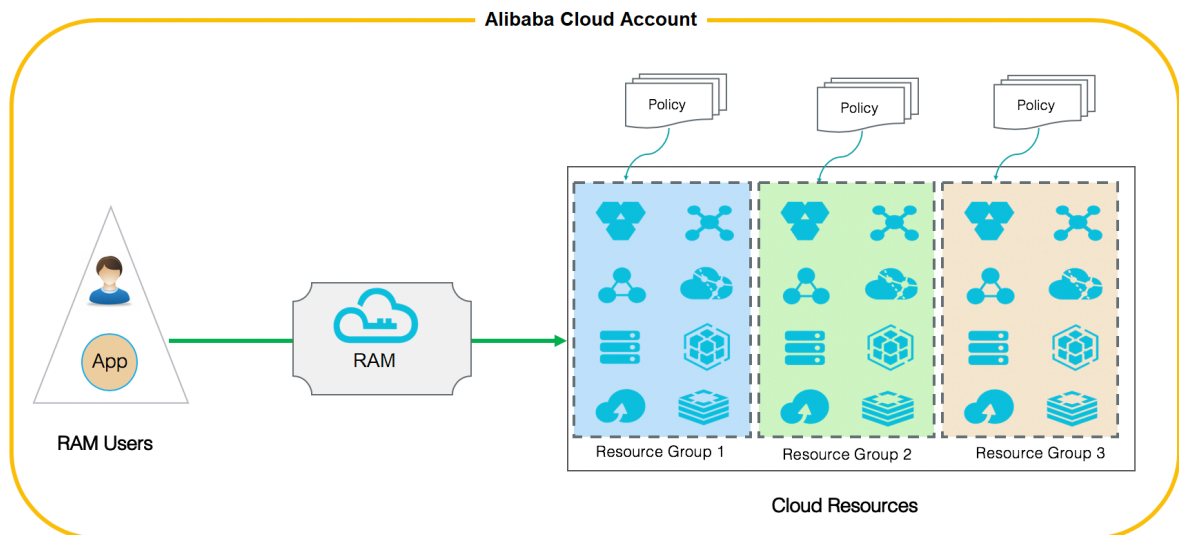
Granting permission for an Alibaba Cloud account means that when you attach a policy to a RAM identity, all Alibaba Cloud resources under the account are included within the scope of the policy permissions.



Grant permission for a target resource group

Granting permission for a resource group means that when you attach a policy to a RAM identity, only the Alibaba Cloud resources within the target resource group are included within the scope of the policy permissions.

In detail, the RAM user with the `AdministratorAccess` system policy in a resource group is called administrator. By default, the resource group creator is assigned as administrator. The administrator is the entity that can add RAM users to the resource group and grant permission to the users in the resource group.



3 View basic information about a policy

This topic describes how to view basic information about a policy, such as the policy name, policy type, and the number of times the policy is referenced.

Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Policies.
3. Enter a policy name or description in the search box.
4. From the Policy Type drop-down list, select System Policy or Custom Policy.



Note:

System policies can be viewed but cannot be modified, whereas custom policies can be created and modified.

4 Custom policies

4.1 Create a custom policy

This topic describes how to create a custom policy. Custom policies provide more precise control than system policies.

Prerequisites

Before you create a custom policy, we recommend that you read about the basic structure and grammar of a policy. For more information, see [#unique_4](#).

Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Policies.
3. Click Create Policy.
4. Enter a policy name and description.
5. Set the configuration mode.
 - If you set the configuration mode to Visualized, click Add Statement and configure the permission effect, actions, and resources as prompted.
 - If you set the configuration mode to Script, edit the policy according to [policy structure and grammar](#).
6. Click OK.

4.2 Modify a custom policy

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

Context

You may have the following requirements when modifying a policy:

- You still want to use the old policy after a period of time.
- You want to restore a previous policy version if the current version has incorrect modifications.

Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Policies.
3. From the Policy Type drop-down list, select Custom Policy.
4. In the Policy Name column, click the name of the target custom policy.



Note:

System policies and custom policies are available for use in Alibaba Cloud Resource Access Management (RAM). System policies can be viewed but cannot be modified, whereas custom policies can be created and modified.

5. On the Policy Document tab, click Modify Policy Document.



Note:

For information about how to modify a policy document, see [#unique_4](#).

6. Click OK.



Note:

After the modifications are completed, a new custom policy is automatically generated and used as a default policy.

4.3 Manage policy versions

This topic describes how to manage policy versions, such as viewing a policy version, setting the default policy version, and deleting a policy version.

Context

- You can retain multiple versions for a policy.
- If you reach the maximum number of policy versions allowed, we recommend that you delete versions you no longer need to save space.
- Even if a policy has multiple versions, only one version is active. The active version is known as the default version.
- The default version can be viewed but cannot be deleted.

Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Policies.

3. In the Policy Name column, click the name of the target policy.
4. On the Versions tab, you can:
 - Click View to view the policy version and the policy document.
 - Click Use This Version to set the policy version to the default version.
 - Click Delete to delete the policy version.

4.4 Delete a custom policy

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

Prerequisites

- The policy has only one version, that is, the default version. If multiple versions exist, you must delete all of the versions except the default one.
- The policy is not referenced (that is, attached to a RAM user, RAM user group, or RAM role). If the policy is currently being referenced, remove related permissions in the policy. For more information, see [#unique_15](#).

Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Policies.
3. From the Policy Type drop-down list, select Custom Policy.
4. In the Policy Name column, find the target custom policy and click Delete.
5. Click OK.

5 Manage policy references

This topic describes how to manage policy references, such as viewing and deleting policy references.

Procedure

1. Log on to the [RAM console](#).
2. Choose Permissions > Policies.
3. In the Policy Name column, click the name of the target policy.
4. On the References tab, you can:
 - View the permission principal, the principal type, and actions.
 - Click Revoke Permission to delete the policy reference, that is, remove permission from a principal.

6 Policy language

6.1 Policy elements

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

Elements

Element	Description
Effect	<p>Specifies whether the statement results in an allow or an explicit deny.</p> <p>Valid values: <code>Allow</code> <code>Deny</code></p>
Action	<p>Describes the specific API action or actions that will be allowed or denied.</p>
Resource	<p>Specifies the object or objects that the statement covers.</p>
Condition	<p>Specifies when a policy takes effect.</p>

How to use a policy element

- Effect



Note:

If policies that apply to a request include an `Allow` statement and a `Deny` statement, the `Deny` statement trumps the `Allow` statement.

Example: `"Effect": "Allow"`

- Action



Note:

In most cases, each Alibaba Cloud service has its own set of API actions. For more information, see [#unique_19](#).

Format: < service - name >:< action - name >

- **service - name** : the name of an Alibaba Cloud service
- **action - name** : **service** : the name of a relevant API action

Example: " Action ": [" oss : ListBucket s ", " ecs : Describe *", " rds : Describe *"]

• Resource

Format: acs :< service - name >:< region >:< account - id >:< relative - id >

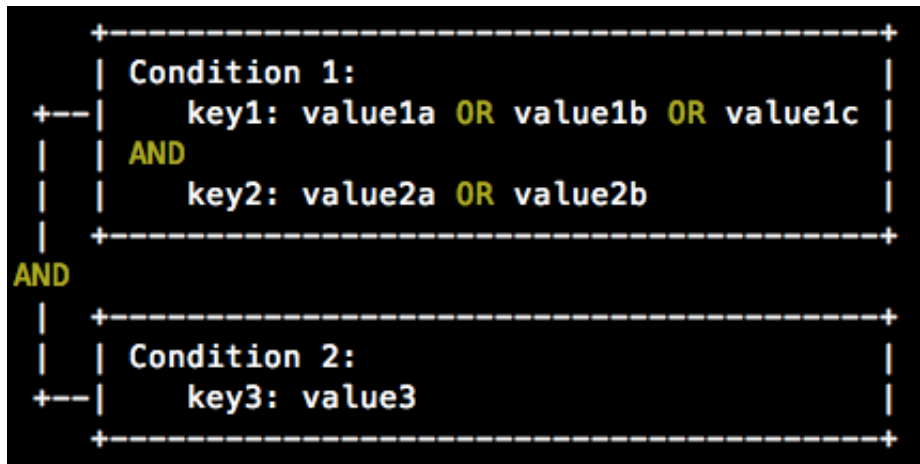
- **acs** : the abbreviation of Alibaba Cloud Service
- **service - name** : the name of an Alibaba Cloud service
- **region** : the region information. If this element is not supported, use an asterisk (*).
- **account - id** : the Alibaba Cloud account ID, such as 1234567890 12 ****. If no ID is required or available, it can be replaced with an asterisk (*).
- **relative - id** : service-related resource description. Its meaning is specified by a specific Alibaba Cloud service. The **relative - id** element is similar to 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 multiple conditions, and each condition can contain multiple key-value pairs.

Figure 6-1: Condition block



- Unless otherwise specified, all keys can have multiple values. When conditions are evaluated, if the condition value matches any of the corresponding values, the condition is satisfied.
- A condition is satisfied only if multiple conditions of the same action type are all satisfied.
- A condition block is satisfied only if all of its conditions are satisfied.

Action type

The following types of actions are supported: string, numeric, date and time, Boolean, and IP address.

Action type	Supported type
String	<ul style="list-style-type: none"> - StringEquals - StringNotEquals - StringEqualsIgnoreCase - StringNotEqualsIgnoreCase - StringLike - StringNotLike

Action type	Supported type
Numeric	<ul style="list-style-type: none"> - NumericEquals - NumericNotEquals - NumericLessThan - NumericLessThanEquals - NumericGreaterThan - NumericGreaterThanEquals
Date and time	<ul style="list-style-type: none"> - DateEquals - DateNotEquals - DateLessThan - DateLessThanEquals - DateGreaterThan - DateGreaterThanEquals
Boolean	Bool
IP address	<ul style="list-style-type: none"> - IpAddress - NotIpAddress

Condition key

- The format of common condition keys is as follows:

```
acs :< condition - key >
```

Condition key	Type	Description
acs : CurrentTime	Date and time	The date and time when the web server receives a request. This key is defined in ISO 8601 format, for example, 2012 - 11 - 11T23 : 59 : 59Z .
acs : SecureTransport	Boolean	Indicates whether a secure channel, such as HTTPS, is used to send a request.
acs : SourceIp	IP address	The IP address of the client that sends a request.

Condition key	Type	Description
<code>acs : MFAPresent</code>	Boolean	Indicates whether multi-factor authentication (MFA) is used during user logon.

- The format of Alibaba Cloud service-related condition keys is as follows:

```
< service - name > : < condition - key >
```

Condition key	Alibaba Cloud service	Type	Description	
<code>ecs : tag / < tag - key ></code>	ECS	String	The tag-key pair for ECS. This key can be customized.	
<code>rds : ResourceTag / < tag - key ></code>	RDS	String	The tag-key pair for RDS. This key can be customized.	
<code>oss : Delimiter</code>	OSS	String	The separator used by OSS to group object names.	
<code>oss : Prefix</code>	OSS	String	The prefix of an OSS object name.	

6.2 Policy structure and grammar

This topic describes the structure and grammar used to create or update policies in Alibaba Cloud Resource Access Management (RAM).

Conventions used in a policy grammar

The conventions used in a policy grammar are as follows:

- Characters in a policy:

- The following characters are JSON tokens and are included in policies:

`{ } [] " , :`

- The following characters are special characters in the grammar and are not included in policies:

`= < > () |`

- Use of characters:

- If an element allows multiple values, you can:

- Use a comma (,) as the delimiter to separate each value, and an ellipses (...) to describe the remaining values. For example, [`< action_str ing >`, `< action_str ing >`, ...].

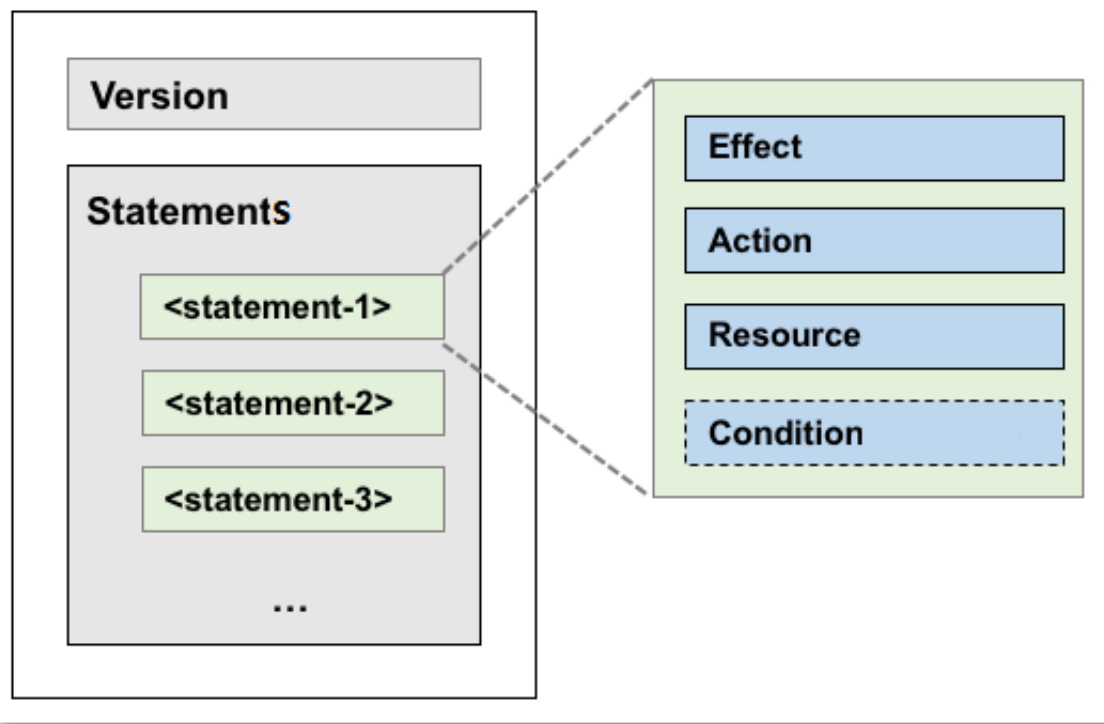
- Include only one value, for example, " Action ": [`< action_str ing >`] and " Action ": `< action_str ing >`.

- A question mark (?) following an element indicates that the element is optional, for example, `< condition_ block ?>`.
- A vertical bar (|) between elements indicates alternatives, for example, (" Allow " | " Deny ").
- Elements that must be text strings are enclosed in double quotation marks (""), for example, `< version_block > = " Version " : (" 1 ")`.

Policy structure

The policy structure includes the version number and a list of statements.

Each statement contains the following elements: effect, action, resource, and condition. The condition element is optional.



Policy grammar

```

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 " | " NotAction " ) :
    ( "*" | [ < action_string >, < action_string >, ... ] )
< resource_block > = ( " Resource " | " NotResource " ) :
    ( "*" | [ < 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:

- The current policy version is 1.
- The policy can have multiple statements.
 - Each statement can be either `Allow` or `Deny` .

**Note:**

In a statement, both the action and resource elements can have multiple values.

- Each statement supports its own conditions.

**Note:**

A condition block can contain multiple conditions with different action types and logical combinations of these conditions.

- 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 trumps the `Allow` statement.
- Element value:
 - If an element value is a number or Boolean, it must be enclosed by using double quotation marks (") such as strings.
 - If an element value is a string, characters such as the asterisk (*) and question mark (?) can be used for fuzzy matching.
 - The asterisk (*) indicates any number (including zero) of allowed characters. For example, `ecs : Describe *` indicates all ECS actions starting with `Describe` .
 - The question mark (?) indicates one allowed character.

Policy format check

Policies are stored in RAM as JSON documents. When you create or update a policy, RAM first checks whether the JSON format is correct.

- For more information about the JSON grammar standards, see [RFC 7159](#).
- We recommend that you use tools such as JSON validators and editors to verify your policies to meet JSON grammar standards.


6.3 Policy check rules



This topic describes the policy check rules to help you better understand RAM policies.

Check rules

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

RAM determines whether to allow access according to the rules described in the following table.

Access type	Rules
Alibaba Cloud account	<p>The Alibaba Cloud account is the resource owner and can access all Alibaba Cloud resources under the account.</p> <div> Note: Some Alibaba Cloud services, such as Log Service, support cross-account ACL authorization. If ACL authorization is successful, access is allowed even the Alibaba Cloud account is not the resource owner.</div>

Access type	Rules
RAM user	<ul style="list-style-type: none"> • The Alibaba Cloud account has attached a policy with explicit allow effect to the RAM user. • The Alibaba Cloud account to which the RAM user belongs has permission to access specific Alibaba Cloud resources. <div data-bbox="842 589 1434 871">  Note: By default, a RAM user does not have any permissions to access Alibaba Cloud resources. The user can access Alibaba Cloud resources only when both of the preceding rules are met. </div> <p>For information about how to check the permissions of a RAM user, see Policy check rules for RAM users.</p>
RAM role	<ul style="list-style-type: none"> • The STS token of the RAM role has the required permissions. <p>For more information about RAM role STS tokens, see #unique_22</p> <ul style="list-style-type: none"> • The Alibaba Cloud account has attached a policy with explicit allow effect to the RAM role. • The Alibaba Cloud account to which the RAM role belongs has permission to access specific Alibaba Cloud resources. <div data-bbox="842 1608 1434 1890">  Note: By default, a RAM role does not have any permissions to access Alibaba Cloud resources. The role can access Alibaba Cloud resources only when all the preceding rules are met. </div> <p>For information about how to check the permissions of a RAM role, see Policy check rules for RAM roles.</p>

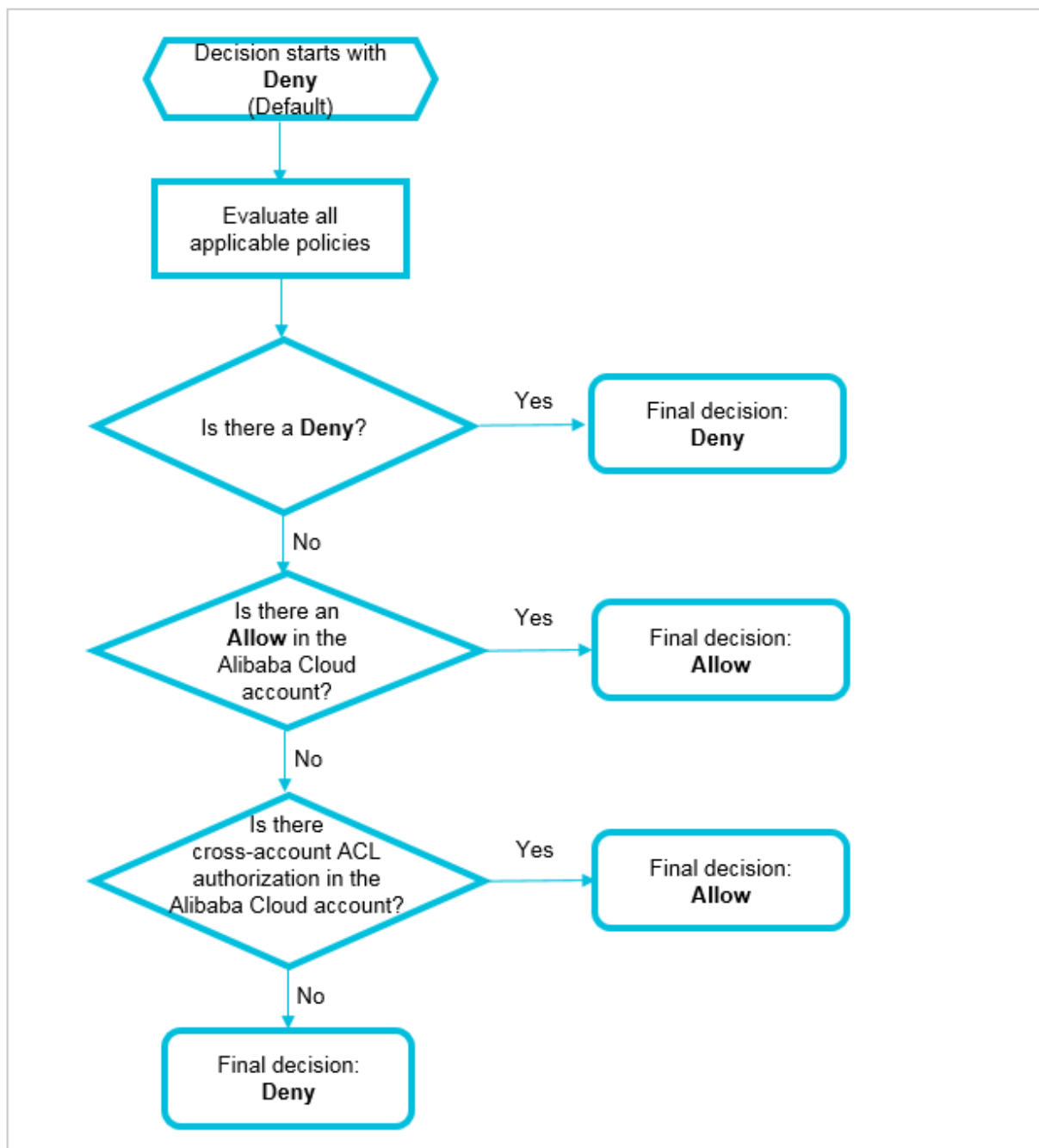
Policy check rules for RAM users

By default, RAM users do not have resource access permissions unless they have been granted explicit permission by the Alibaba Cloud account.



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 trumps the **Allow** statement.

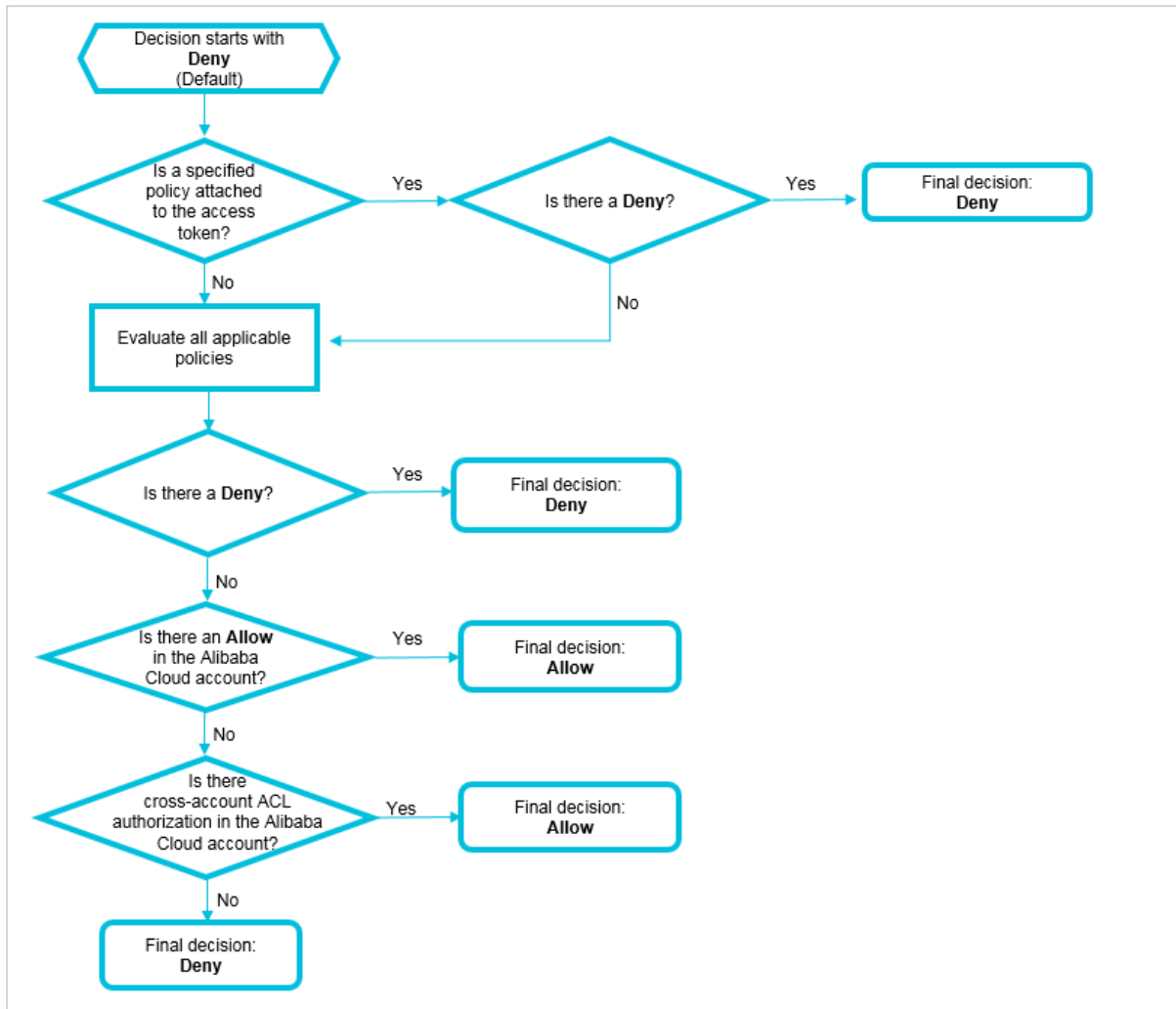


When you access Alibaba Cloud resources as a RAM user, the system checks the policies as follows:

1. Whether the policy attached to the RAM user has a `Deny` statement:
 - If yes, access is denied.
 - If no, go to the next step.
2. Whether the policy 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. Whether the Alibaba Cloud account of the RAM user has cross-account ACL authorization:
 - 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 and calling the [#unique_23](#) action. The `Policy` parameter specifies the resource access permission or permissions.



When you access Alibaba Cloud resources as a RAM role, the system checks the policies as follows:

1. 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. Whether the policy attached to the RAM role has a **Deny** statement:

- If yes, access is denied.
- If no, go to the next step.

3. Whether the policy 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. Whether the Alibaba Cloud account of the RAM role has cross-account ACL authorization:

- If yes, access is allowed.
- If no, access is denied.

7 Best practices

7.1 Use RAM to maintain security of your Alibaba Cloud resources

This topic describes how to use RAM to apply access and security settings to your Alibaba Cloud resources so that you can better manage access permissions with fine-grained access control.

Prerequisites

An Alibaba Cloud account is created. If not, create one before proceeding. To create an Alibaba Cloud account, click [Create a new Alibaba Cloud account](#).

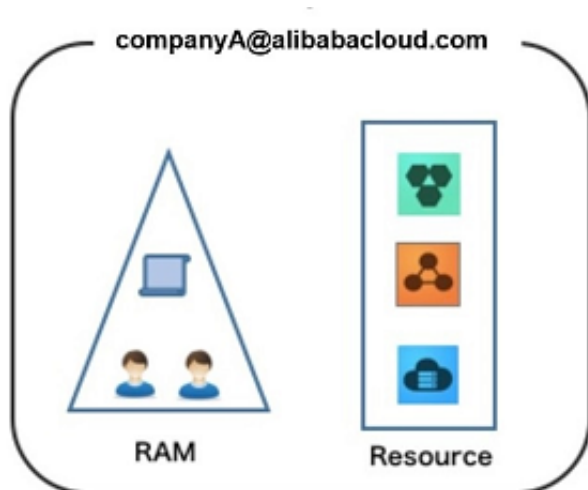
Scenario

When you migrate your business resources to the cloud, the traditional organizational structures and previous management methods of your resources may no longer meet your requirements. As a result, the migration of your resources may create higher security management issues as follows:

- The responsibilities of the RAM users are not clear.
- The Alibaba Cloud account owner does not want to share the access key with RAM users due to security risks involved.
- RAM users can access resources by using different methods, which is not unified and may mistakenly cause security risks.
- The resource access permissions of RAM users need to be frequently recalled when the users no longer require these permissions.

Solution

To resolve the preceding issues, you can use RAM to create RAM users and grant resource access permissions to RAM users. Specifically, you can use RAM to separate the access key of your Alibaba Cloud account from RAM users and grant minimum permissions to users as needed to maintain the security of your resources.



Security management solution

- Create independent RAM users.

An enterprise needs only one Alibaba Cloud account. As a best practice, the Alibaba Cloud account is not used for daily tasks. However, multiple RAM users can be created under the account, and granted the necessary access permissions to resources as needed.

For more information, see [#unique_26](#).

- Separate console users from API users.

We recommend that you do not create a logon password for console operations and an access key for API operations for a RAM user at the same time.

- To allow an application to access cloud resources only through APIs, you only need to create an access key for the application.
- To allow an employee to operate on cloud resources only through the console, you only need to set a logon password for the employee.

For more information, see [#unique_26](#).

- Create RAM users and group them.

If your Alibaba Cloud account has multiple RAM users, you can group RAM users with same responsibilities and grant permissions to the group as needed.

For more information, see [#unique_27](#).

- Grant the minimum permissions to different RAM user groups.

You can attach proper system policies to RAM users or user groups as needed.

You can also create custom policies for fine-grained permission management. In

this way, by granting the minimum permissions to different RAM users and user groups, you can better manage the RAM users' operations on the cloud resources.

For more information, see [#unique_28](#).

- Configure strong password policies.

You can configure password policies with custom conventions regarding the minimum length, mandatory characters, and validation period, for RAM users in the RAM console. If a RAM user is allowed to change their logon password, the user must create a strong logon password and rotate the password or access key on a regular basis.

For more information, see [#unique_29](#).

- Enable an MFA device for your Alibaba Cloud account.

You can enable a multi-factor authentication (MFA) device for your Alibaba Cloud account to enhance the account security. When you log on to Alibaba Cloud with MFA enabled, the system requires the following two security factors:

1. Your username and password
2. Verification code provided by the MFA device

For more information, see [#unique_30](#).

- Enable SSO for RAM users.

After Single Sign On (SSO) is enabled, all the internal accounts of your enterprise will be authenticated. Then, users can log on to Alibaba Cloud to access corresponding resources only by using an internal account.

For more information, see [#unique_31](#).

- Do not share the access key of your Alibaba Cloud account.

Your Alibaba Cloud account has full control permissions over resources under it, and its access keys have the same permissions as logon passwords. However, access keys are used for programmatic access whereas logon passwords are used to log on to the console. Therefore, to avoid information leaks due to misuse of an access key, we recommend that you do not share or use the access key of your Alibaba Cloud account.

Instead, create a RAM user and grant this user the relevant permissions.

For more information, see [#unique_32](#).

- Specify operation conditions to enhance security.

You can specify the operational conditions that a RAM user must meet before they can use your cloud resources. For example, you can specify that the RAM user must use a secure channel (such as SSL), use a specified source IP address, or operate within a specified period of time.

For more information, see [#unique_33](#).

- Manage permissions of your cloud resources.

By default, all your resources are under your Alibaba Cloud account. A RAM user can use the resources but do not own the resources. This allows you to easily manage the instances or data created by RAM users.

- For an existing RAM user that you no longer require, you can remove all of its corresponding permissions by simply removing the RAM user account.
- For a RAM user that requires a permission, you need to first create the RAM user, set the logon password or access key for it, and then grant the RAM user the relevant permissions as needed.

For more information, see [#unique_5](#).

- Use STS to grant temporary permissions to RAM users.

The Security Token Service (STS) is an extended authorization service of RAM. You can use STS to grant temporary permissions to RAM users and specify the permission and automatic expiration time of the tokens as needed.

For more information, see [#unique_22](#)

Result

After migrating your services to the cloud, you can use the preceding solutions to ensure you manage your cloud-based resources effectively and keep your Alibaba Cloud account and all business assets secure.

What to do next

You can use RAM to categorize your O&M requirements and assign tasks to different engineers as needed. For more information, see [#unique_34](#).