ALIBABA CLOUD

Alibaba Cloud

Elastic Container Instance

Security

Document Version: 20220617

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.Elastic Container Instance service-linked role

This topic describes the AliyunServiceRoleForECI service-linked role for Elastic Container Instance and how to delete the service-linked role.

Background information

AliyunServiceRoleForECI is the service-linked role for Elastic Container Instance. This role is a Resource Access Management (RAM) role that is defined for Elastic Container Instance to access other Alibaba Cloud services in specific scenarios. For more information about service-linked roles, see Service-linked roles.

AliyunServiceRoleForECI scenarios

When you create an elastic container instance or an image cache, if Elastic Container Instance needs to access resources of Elastic Compute Service (ECS), Virtual Private Cloud (VPC), Container Registry (ACR), Log Service (SLS), or Server Load Balancer (SLB), you can use the automatically created AliyunServiceRoleForECI role to obtain the access permissions.

AliyunServiceRoleForECI permissions

The permission policy attached to the AliyunServiceRoleForECI role is AliyunServiceRolePolicyForECI that contains the following access permissions on cloud services:

```
{
    "Version":"1",
    "Statement":[
        {
            "Action":[
                "ecs:CreateNetworkInterfacePermission",
                "ecs:DeleteNetworkInterfacePermission",
                "ecs:CreateNetworkInterface",
                "ecs:DescribeNetworkInterfaces",
                "ecs:AttachNetworkInterface",
                "ecs:DetachNetworkInterface",
                "ecs:DeleteNetworkInterface",
                "ecs:DescribeSecurityGroups"
            ],
            "Resource":"*",
            "Effect":"Allow"
        },
        {
            "Action":[
                "vpc:DescribeVSwitches",
                "vpc:DescribeVpcs",
                "vpc:AssociateEipAddress",
                "vpc:UnassociateEipAddress",
                "vpc:DescribeEipAddresses",
                "vpc:AllocateEipAddress",
                "vpc:ReleaseEipAddress",
                "vpc:AddCommonBandwidthPackageIp",
                "vpc:RemoveCommonBandwidthPackageIp",
```

```
                "vpc:TagResources"
            ],
            "Resource":"*",
            "Effect":"Allow"
        },
        {
            "Action":[
                "cr:Get*",
                "cr:List*",
                "cr:PullRepository"
            ],
            "Resource":"*",
            "Effect":"Allow"
        },
        {
            "Action":[
                "log:CreateProject",
                "log:GetProject",
                "log:CreateLogStore",
                "log:GetLogStore",
                "log:CreateMachineGroup",
                "log:CreateConfig",
                "log:GetConfig",
                "log:ApplyConfigToGroup",
                "log:GetAppliedConfigs",
                "log:CreateIndex",
                "log:TagResources"
            ],
            "Resource":"*",
            "Effect":"Allow"
        },
        {
            "Action":[
                "slb:DescribeLoadBalancers",
                "slb:RemoveBackendServers"
            ],
            "Resource":"*",
            "Effect":"Allow"
        },
        {
            "Action":"ram:DeleteServiceLinkedRole",
            "Resource":"*",
            "Effect":"Allow",
            "Condition":{
                "StringEquals":{
                    "ram:ServiceName":"eci.aliyuncs.com"
                }
            }
        }
    ]
}
```

Delete AliyunServiceRoleForECI

If you want to delete the AliyunServiceRoleForECI service-linked role, you must delete the Elastic Container Instance resources related to the role, such as elastic container instances and image caches, by using the Elastic Container Instance console or calling operations. You can delete AliyunServiceRoleForECI after you delete the related elastic container instances and image caches. For more information, see Delete a RAM role.

2.Grant permissions to RAM users

By default, you can use an Alibaba Cloud account or a Resource Access Management (RAM) user to manage Elastic Container Instance resources. However, when a RAM user is created for an Alibaba Cloud account, the RAM user does not have permissions to manage the resources within the Alibaba Cloud account. You must grant the required permissions to the RAM user before you can use it to manage Elastic Container Instance resources. This topic describes how to grant permissions to a RAM user.

Prerequisites

A RAM user is created. For information about how to create a RAM user, see Create a RAM user.

Background information

You can attach a policy to a RAM user to grant the user permissions. The following permissions related to Elastic Container Instance can be granted:

- AliyunECIReadOnlyAccess

  Grants read-only permissions on Elastic Container Instance resources. This is a default system policy and contains the following permissions:

  - eci:Describe*: the permissions to query Elastic Container Instance resources
  - eci:List*: the permissions to query Elastic Container Instance resources
  - ecs:DescribeSecurityGroups: the permissions to query security groups
  - vpc:DescribeVSwitches: the permissions to query vSwitches
  - vpc:DescribeVpcs: the permissions to query virtual private clouds (VPCs)

- AliyunECIFullAccess

  Grants permissions to manage Elastic Container Instance resources. This is a default system policy and contains the following permissions:

  - eci: all permissions to manage Elastic Container Instance resources
  - ecs:DescribeSecurityGroups: the permissions to query security groups
  - vpc:DescribeVSwitches: the permissions to query vSwitches
  - vpc:DescribeVpcs: the permissions to query VPCs
  - vpc:DescribeEipAddresses: the permissions to query elastic IP addresses (EIPs)

- Other permissions to perform operations in the Elastic Container Instance console

  If you want to perform operations in the Elastic Container Instance console, you must have the following permissions in addition to the default permissions granted by the AliyunECIFullAccess policy:

  - ram:ListRoles: the permissions to query RAM roles of instances
  - nas:DescribeFileSystems: the permissions to query Apsara File Storage NAS file systems
  - oss:ListBuckets: the permissions to query Object Storage Service (OSS) buckets
  - vpc:DescribeCommonBandwidthPackages: the permissions to query EIP bandwidth plans

- cr:GetRepoList: the permissions to query image repositories
- cr:GetRepoTags: the permissions to query tags of images in a repository
- cr:GetImageManifest: the permissions to query manifest information about an image
- cr:SearchRepo: the permissions to search for image repositories

Procedure

1. Log on to the RAM console by using your Alibaba Cloud account.
2. If you want to grant a RAM user permissions to manage Elastic Container Instance resources in the Elastic Container Instance console, you must create corresponding custom policies.
   i. In the left-side navigation pane, choose **Permissions > Policies**.
   ii. On the Policies page, click **Create Policy**.
   iii. On the **JSON** tab, copy the following script to the policy content, and then click **Next Step**.

```
{
    "Statement": [
        {
            "Action": "ram:ListRoles",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "nas:DescribeFileSystems",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "oss:ListBuckets",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "vpc:DescribeCommonBandwidthPackages",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "cr:GetRepoList",
                "cr:GetRepoTags",
                "cr:GetImageManifest",
                "cr:SearchRepo"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ],
    "Version": "1"
}
```

   iv. Enter a policy name in the Name field and click **OK**.

3. Grant permissions to the RAM user based on your needs.
   i. In the left-side navigation pane, choose **Identities > Users**.
   ii. Find the RAM user to which you want to grant permissions and click **Add Permissions** in the Actions column.
   iii. In the **Add Permissions** panel, configure parameters to attach policies to the RAM user.

   The following table describes the parameters.

Parameter	Description
Authorized Scope	The authorization scope. ■ Alibaba Cloud Account: Permissions take effect on the current Alibaba Cloud account. ■ Specific Resource Group: Permissions take effect on a specific resource group.
Principal	The RAM user to which you want to grant permissions. The selected RAM user is automatically entered in the Principal field. You can also specify another RAM user.
Select Policy	The policies that you want to attach to the RAM user. Select policies that fit your needs. ■ If you want the RAM user only to view Elastic Container Instance resources, select the AliyunECIReadOnlyAccess system policy. ■ If you want the RAM user to manage Elastic Container Instance resources by calling API operations, select the AliyunECIFullAccess system policy. ■ If you want the RAM user to manage Elastic Container Instance resources by using the Elastic Container Instance console, select the AliyunECIFullAccess system policy and the custom policy that you created in Step 2.

   iv. Click **OK**.
   v. Confirm the authorization scope and the policies and click **Complete**.

3.Use resource groups to control the permissions of a RAM user

When you create Elastic Container Instance resources, you can specify a resource group for each resource. This allows you to manage resources by group. This topic describes how to grant RAM users the permissions on resource groups. Then, the RAM users can manage only resources in the resource groups on which they have permissions.

Background information

You can use resource groups to categorize and manage resources in your Alibaba Cloud account. This simplifies the resource and permission management of your Alibaba Cloud account. Take note of the following items when you use resource groups:

- A resource group can contain cloud resources from different regions. For example, Resource Group A can contain instances from the China (Beijing) and China (Hangzhou) regions.
- If resources that belong to different resource groups in the same account are located within the same region, these resources can be correlated with each other. For example, an instance in the China (Beijing) region of Resource Group A can be added to the virtual private cloud (VPC) in the China (Beijing) region of Resource Group B.
- Resource groups inherit the global permissions of a RAM user. For example, if you authorize a RAM user to manage all Alibaba Cloud resources, the RAM user can see all the resource groups that belong to the Alibaba Cloud account.

Scenarios

Elastic Container Instance resources contain elastic container instances and image caches. Each Elastic Container Instance resource must belong to only one resource group. When you create an Elastic Container Instance resource, you can specify a resource group for the resource. If no resource group is specified, the resource is added to the default resource group.

> **Note**
>
> You can add an Elastic Container Instance resource to a specified resource group or the default resource group only when you create the resource. You cannot modify the resource group after it is specified. After you delete a resource, the resource is automatically removed from the resource group.

You can add Elastic Container Instance resources that are used for different purposes to specific resource groups. Then you can specify different RAM users as administrators for these resource groups to manage resources in a decentralized manner.

For example, if you have one elastic container instance for the production environment and the other instance for the test environment, you can add the two instances to their respective resource groups in the production and test environments. Then, you can authorize RAM User A to perform operations on the instance in the resource group of the production environment and RAM User B to perform operations on the other instance in the resource group of the test environment. To test a product, RAM User B performs operations on the instance in the resource group of the test environment. To launch a product, RAM User A performs operations on the instance in the resource group of the production environment. The two environments are managed by different RAM users. This facilitates permission control and helps avoid misoperations.

Procedure

The following scenario is used as an example: Two resource groups are created to group Elastic Container Instance resources and RAM users are authorized to perform operations on the resources in specific resource groups.

- Two resource groups are created. One is created for the production environment, and the other is created for the test environment.
- Two RAM users are created. RAM User A has the AliyunECIFullAccess permission on the production environment, and RAM User B has the AliyunECIFullAccess permission on the test environment.

  > **Note**
  >
  > AliyunECIFullAccess is a system policy provided by Resource Access Management (RAM) and contains all permissions to perform operations on Elastic Container Instance resources.

The procedure is as follows:

1. Create two resource groups. For more information, see Create a resource group.
2. Create two RAM users. For more information, see Create a RAM user.
3. Specify each RAM user as an administrator for only a resource group. For more information, see Add RAM authorization.

   When you grant permissions to the two RAM users, select the AliyunECIFullAccess permission.
4. Create an elastic container instance with its resource group specified.
   - If you create an elastic container instance on the instance buy page in the Elastic Container Instance console, specify a resource group on the **Other settings (optional)** page.
   - If you create an elastic container instance by calling the CreateContainerGroup operation, pass ResourceGroupId to specify the resource group ID.

Expected results

The expected results are as follows:

- In the Elastic Container Instance console, the RAM user can only view and perform operations on the elastic container instance in the resource group on which the user has permissions.
- If a RAM user calls an operation, the RAM user can only view and perform operations on the elastic container instance in the resource group on which the RAM user has permissions. The following operations are used as examples:

- CreateContainerGroup

  To create an elastic container instance, the RAM user must specify the resource group ID for authentication. If no resource group ID is specified or the specified resource group ID is incorrect, the authentication fails.

  > **Note**
  >
  > If the RAM user has permissions on the default resource group, the RAM user does not need to specify the resource group ID. The elastic container instance is added to the default resource group by default.

- DescribeContainerGroups

  To query the information about elastic container instances, the RAM user must specify the resource group ID for authentication. If no resource group ID is specified or the specified resource group ID is incorrect, the authentication fails.

  > **Note**
  >
  > If the ID of the specified elastic container instance does not match the resource group ID, the elastic container instance does not belong to the resource group. In this case, the RAM user cannot view the information about the elastic container instance even if the resource group ID is correct.

- DescribeContainerLog

  To query the logs of an elastic container instance, the RAM user does not need to specify the resource group ID. The system automatically retrieves the resource group to which the elastic container instance belongs and authenticates the request.

- DeleteContainerGroup

  To delete an elastic container instance, the RAM user does not need to specify the resource group ID. The system automatically retrieves the resource group to which the elastic container instance belongs and authenticates the request.

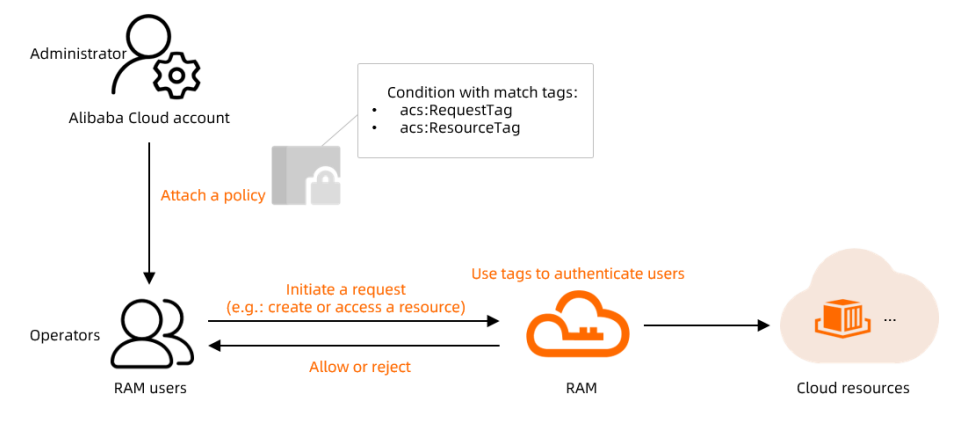
4.Use tags to authenticate a RAM user

This topic describes how to use tags to manage the permissions of a RAM user. This topic also describes how to use tags to authenticate the RAM user.

Background information

Tags are used to identify and categorize cloud resources. Resource Access Management (RAM) manages the access and operation permissions of RAM users on cloud resources based on permission policies. You can specify multiple tags in each policy and attach one or more policies to a RAM user. If you want to manage the permissions of RAM users on resources, you can create custom policies that contain tags to implement fine-grained permission management of resources.

The following figure shows how to use tags to authenticate RAM users.

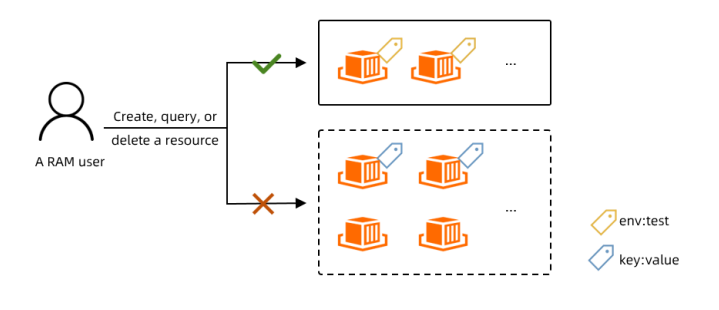


> **Note**
>
> You can bind tags to Elastic Container Instance resources, such as elastic container instances, image caches, and virtual nodes (VNodes). You can bind tags to resources only when you create or update resources. For more information, see Use tags to manage elastic container instances.

Example

Scenario

For example, you want to grant a RAM user the permissions only on the Elastic Container Instance resources to which the `env:test` tag is bound, as shown in the following figure:



You must meet the following specific requirements:

- Requirement 1: The RAM user can create only Elastic Container Instance resources to which the `env:test` tag is bound.
- Requirement 2: The RAM user can operate only the Elastic Container Instance resources to which the `env:test` tag is bound.
- Requirement 3: The RAM user can view only the Elastic Container Instance resources to which the `env:test` tag is bound.

Step 1: Create a custom policy and attach the policy to the RAM user

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. Configure the parameters to create a custom policy.
   i. On the Create Policy page, click the **JSON** tab.
   ii. Click **Import System Policy** in the upper-right corner. In the dialog box that appears, select AliyunECIFullAccess and click **Import**.

   AliyunECIFullAccess is the default policy that is used to manage Elastic Container Instance resources. AliyunECIFullAccess contains the permissions to operate Elastic Container Instance resources, query resources such as security groups and virtual private clouds (VPCs), and create the service-linked role for Elastic Container Instance.
   iii. Modify the policy document and click **Next: Edit Basic Information**.

> **Note**
>
> A policy contains a set of permissions. The structure of a policy consists of a version number and a list of authorization statements. Each statement contains the following elements: effect, action, resource, and condition. The condition element is optional. For more information, see Policy structure and syntax and Policy elements.

You can specify authentication tags in the `condition` element of a policy to restrict the operation permissions of the RAM user. The following table describes the tag keywords that can be specified in the condition element.

Tag keyword	Description
`acs:RequestTag`	To use the tag keyword in the authentication process, you must specify a tag in the API request. If the API request does not contain a parameter that specifies the tag and you use the `acs:RequestTag` tag keyword, the authentication fails.
`acs:ResourceTag`	To use the tag keyword in the authentication process, you must specify a resource to which a tag is bound in the API request. If the API request does not contain a parameter that specifies the resource ID and you use the `acs:ResourceTag` tag keyword, the authentication fails.

> **Note**
>
> When you configure a policy, you can use the `acs:RequestTag` or `acs:ResourceTag` tag keyword based on the attributes of the API operation and your business requirements. The attributes of an API operation include whether the API request contains parameters that separately specify the resource ID and the tag. For more information, see Authenticate a RAM user when the RAM user initiates an API request.

You can configure the following policies to meet your business requirements in the preceding scenario:

Requirement	Policy

The RAM user can create only Elastic Container Instance resources to which the `env:test` tag is bound.	<pre>{
	"Effect": "Allow",
	"Action": "eci:Create*",
	"Resource": "*",
	"Condition": {
	"StringEquals": {
	"acs:RequestTag/env": "test"
	}
	}
	}</pre>

Requirement	Policy

The RAM user can operate only the Elastic Container Instance resources to which the env:test tag is bound.	<pre>{
	"Effect": "Allow",
	"Action": "eci:*",
	"Resource": "*",
	"Condition": {
	"StringEquals": {
	"acs:ResourceTag/env": "test"
	}
	}
	}</pre>

The RAM user can view only the Elastic Container Instance resources to which the env:test tag is bound.	<pre>{
	"Effect": "Allow",
	"Action": "eci:Describe*",
	"Resource": "*",
	"Condition": {
	"StringEquals": {
	"acs:RequestTag/env": "test"
	}
	}
	}</pre>

The following example shows a full policy that combines the existing permissions of AliyunECIFullAccess.

```
{
 "Version": "1",
 "Statement": [{
   "Effect": "Allow",
   "Action": "eci:Create*",
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "acs:RequestTag/env": "test"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": "eci:*",
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "acs:ResourceTag/env": "test"
    }
   }
  },
```

```
  {
   "Effect": "Allow",
   "Action": "eci:Describe*",
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "acs:RequestTag/env": "test"
    }
   }
  },
  {
   "Action": [
    "ecs:DescribeSecurityGroups"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "vpc:DescribeVSwitches",
    "vpc:DescribeVpcs",
    "vpc:DescribeEipAddresses"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "ram:CreateServiceLinkedRole",
   "Resource": "*",
   "Effect": "Allow",
   "Condition": {
    "StringEquals": {
     "ram:ServiceName": [
      "eci.aliyuncs.com",
      "vnode.eci.aliyuncs.com"
     ]
    }
   }
  }
 ]
}
```

> **Note**
>
> If you want the RAM user to operate Elastic Container Instance resources by calling API operations, you must grant the RAM user the permissions in the AliyunECIFullAccess policy. If you want the RAM user to operate Elastic Container Instance resources by using the Elastic Container Instance console, you must grant the RAM user the permissions in the AliyunECIFullAccess policy and other permissions from existing policies. For more information, see Grant permissions to RAM users.

iv. Enter a name for the policy and click **OK**.

5. Attach the custom policy to the RAM user.
   i. In the left-side navigation pane, choose **Identities > Users**.
   ii. Create a RAM user.

   Create a RAM user based on your management requirements. For more information, see Create a RAM user. If you already created a RAM user, skip this step.
   iii. Attach the policy to the RAM user.

   Attach the custom policy that you created to the RAM user. For more information, see Grant permissions to a RAM user.

Step 2: Check whether the policy is in effect

1. Log on to the OpenAPI Explorer console as a RAM user.
2. Check whether the policy is in effect.

   An elastic container instance is used in the following tests:

   - Create an elastic container instance
     - If you bind the `env:test` tag to an instance, the instance can be created.
     - If you do not bind the env:test tag to the instance or you bind another tag to the instance, the instance cannot be created. You are prompted that you do not have the permission to create the instance.
   - Delete an elastic container instance
     - If the `env:test` tag is bound to the instance that you want to delete, the instance can be deleted.
     - If the `env:test` tag is not bound to the instance that you want to delete, the instance cannot be deleted. You are prompted that you do not have the permission to delete the instance.
   - Query an elastic container instance
     - If you specify an instance to which the `env:test` tag is bound in the request but you do not specify a tag, the specified instance is queried.
     - If you specify an instance to which the `env:test` tag is not bound in the request, the query result is empty.
     - If you do not specify an instance but you specify the `env:test` tag in the request, all instances to which the `env:test` tag is bound are queried.
     - If you do not specify an instance or a tag, the query result is empty.

Authenticate a RAM user when the RAM user initiates an API request

The following table describes how the system authenticates a RAM user after a policy that contains an authentication tag is attached to the RAM user and the RAM user initiates an API request.

API operation	Authentication description
API operations that are used to create resources, such as CreateContainerGroup and CreateImageCache	You do not need to specify a resource ID in the requests to call these API operations. The system checks whether the authentication tag specified in the policy matches the `acs:RequestTag` tag keyword. • If you do not specify a tag in the requests or if the tag that you specify does not match the authentication tag, the authentication fails. • If you specify a tag that exactly matches the authentication tag or if the tag that you specify contains the authentication tag, the authentication succeeds.
API operations that are used to query resources, such as DescribeContainerGroups and DescribeImageCaches	To call these API operations, you must specify a resource ID or a tag in the requests based on the requirements of the API operations. The system checks whether the authentication tag specified in the policy matches the `acs:ResourceTag` or `acs:RequestTag` tag keyword. • If you specify a resource ID and a tag in the requests and the tag that is bound to the specified resource matches the `acs:ResourceTag` tag keyword, or the specified tag matches the `acs:RequestTag` tag keyword, the authentication succeeds. • If you specify a resource ID but you do not specify a tag in the requests and the tag that is bound to the specified resource matches the `acs:ResourceTag` tag keyword, the authentication succeeds. • If you specify a tag but you do not specify a resource ID in the requests and the specified tag matches the `acs:RequestTag` tag keyword, the authentication succeeds. • If you do not specify a resource ID or a tag in the requests, the authentication fails. **Note** For API operations that are used to query resources, the system returns an empty result and does not report an error if the authentication fails.

API operation	Authentication description
API operations that are used to update resources, such as UpdateContainerGroup and UpdateImageCache	You must specify a resource ID in the requests to call these API operations. The system checks whether the authentication tag specified in the policy matches the `acs:ResourceTag` tag keyword. • If you do not specify a tag in the requests and the tag that is bound to the specified resource matches the acs:ResourceTag tag keyword, the authentication succeeds. • If you specify a tag in the requests, which is used as the new tag of the resource after the resource is updated, and the tag that is bound to the specified resource matches the acs:ResourceTag tag keyword and the specified tag, the authentication succeeds. **Note** To update tags, the RAM user must have the permissions that are specified in the original and new tags. You must attach the following two custom policies to the RAM user: a policy that contains the original tag and a policy that contains the new tag.
Other API operations that are used to perform other operations on resources, such as RestartContainerGroup and ExecContainerCommand	You must specify a resource ID in the requests to call these API operations. The system checks whether the authentication tag specified in the policy matches the `acs:ResourceTag` tag keyword. • If the tag that is bound to the specified resource does not match the acs:ResourceTag tag keyword, the authentication fails. • If the tag that is bound to the specified resource matches the acs:ResourceTag tag keyword, the authentication succeeds.

5.Use an instance RAM role by calling API operations

You can bind an instance Resource Access Management (RAM) role to an elastic container instance. Then, applications on the elastic container instance can access APIs of other cloud services by using a temporary security token service (STS) token. This topic describes how to create an instance RAM role, attach a policy to the role, and then assign the role to an elastic container instance by calling API operations.

Scenarios

Applications on elastic container instances can use an AccessKey pair of an Alibaba Cloud account or a RAM user to access the APIs of other Alibaba Cloud services such as Object Storage Service (OSS), Virtual Private Cloud (VPC), and ApsaraDB RDS. To call API operations in an efficient manner, some users specify AccessKey pairs in an elastic container instance. For example, the users write AccessKey pairs in the configuration file of the elastic container instance. However, this method may cause issues such as information leakage and complex maintenance. This method may also cause unnecessary permissions to be granted. You can use instance RAM roles to prevent similar issues.

A RAM role is a virtual user that has specific permissions. When an elastic container instance assumes a RAM role, the instance has the permissions of the RAM role. You do not need to save the AccessKey pair of the RAM role in the elastic container instance. If you want to modify the permissions of an elastic container instance, you need only to modify the permissions of the RAM role. This way, operations are simplified and issues such as information leakage are prevented. For more information about RAM roles, see RAM role overview.

Procedure

To use an instance RAM role, perform the following operations:

1. Create an instance RAM role

   You can call the CreateRole operation to create an instance RAM role. In the configuration file, you must set the trusted service to ECS to allow an elastic container instance to assume the RAM role.

2. Attach a policy to the RAM role

   You can call the CreatePolicy operation to create a policy, and then call the AttachPolicyToRole operation to attach the policy to the instance RAM role.

3. (Optional) Authorize a RAM user to use the instance RAM role

   Before you use a RAM user to create an elastic container instance and assign an instance RAM role to the instance, you must authorize the RAM user to use the instance RAM role.

4. Assign the instance RAM role to an elastic container instance

   When you call the CreateContainerGroup operation to create an elastic container instance, you can use the RamRoleName parameter to assign the instance RAM role to the elastic container instance. This way, the instance obtains the permissions of the RAM user. An elastic container instance can assume only one instance RAM role.

5. (Optional) Obtain a temporary access token

After you assign an instance RAM role to an elastic container instance, you must obtain a temporary access token if you want to access the APIs of other Alibaba Cloud services from applications on the elastic container instance. The temporary access token is granted by the instance RAM role and is displayed in the instance metadata.

Create an instance RAM role

You can call the CreateRole operation to create an instance RAM role. For information about the parameters, see CreateRole.

You can use the RoleName parameter to specify a role name. The ECIRamRoleTest name is used in the example. Then, configure AssumeRolePolicyDocument based on the following code.

```
{
"Statement": [
{
  "Action": "sts:AssumeRole",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "ecs.aliyuncs.com"
    ]
  }
}
],
"Version": "1"
}
```

Attach a policy to the RAM role

1. Call the CreatePolicy operation to create a custom policy.

   Configure the following parameters in the request:

   - PolicyName: the name of the policy. The ECIRamRoleTestPolicy name is used in the example.
   - PolicyDocument: the details about the policy.

     ```
     {
          "Statement": [
              {
              "Action": [
                  "oss:Get*",
                  "oss:List*"
              ],
              "Effect": "Allow",
              "Resource": "*"
              }
          ],
          "Version": "1"
      }
     ```

   For more information, see CreatePolicy.

2. Call the AttachPolicyToRole operation to attach the policy to the RAM role.

   Configure the following parameters in the request:

- PolicyName: the name of the policy. The ECIRamRoleTestPolicy name is used in the example.
- PolicyType: the type of the policy. Set this parameter to Custom.
- RoleName: the name of the RAM role. The ECIRamRoleTest name is used in the example.

For more information, see AttachPolicyToRole.

Authorize a RAM user to use the instance RAM role

If you want a RAM user to use an instance RAM role, you must grant the `ram:PassRole` permission of the instance RAM role to the RAM user. If the RAM user does not have the `ram:PassRole` permission, the RAM user cannot exercise the permissions that are specified in role policies.

1. Log on to the RAM console by using a RAM user that has administrator permissions or by using an Alibaba Cloud account.
2. Authorize the RAM user to use the instance RAM role.

   To authorize the RAM user to use the instance RAM role, create the following custom policy and attach the policy to the RAM user. ECIRamRoleTest is the name of the RAM role. The `ram:PassRole` permission of the RAM role is to be granted to the RAM user. For more information, see Grant permissions to a RAM user.

```
{
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ram:PassRole",
      "Resource": "acs:ram:*:*:role/ECIRamRoleTest"
    }
  ],
  "Version": "1"
}
```

Assign the instance RAM role to an elastic container instance

When you call the CreateContainerGroup operation to create an elastic container instance, you can use the RamRoleName parameter to specify the RAM role.

> **Note**
>
> An elastic container instance can assume only one instance RAM role. If an instance RAM role is assigned to an instance, an error message appears when you attempt to assign another instance RAM role to the instance.

Obtain a temporary access token

You can obtain a temporary access token from the instance RAM role. The token is automatically updated on a regular basis and allows you to exercise the permissions and use the resources of the instance RAM role.

Run the following command to query the temporary access token of the ECIRamRoleTest RAM role:

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

The command output contains the temporary access token. The following code provides an example of the command output.

```
{
"AccessKeyId" : "STS.J8XXXXXXXXX4",
"AccessKeySecret" : "9PjfXXXXXXXXXBf2XAW",
"Expiration" : "2021-06-09T09:17:19Z",
"SecurityToken" : "CAIXXXXXXXXXXXwmBkleCTkyI+",
"LastUpdated" : "2021-06-09T03:17:18Z",
"Code" : "Success"
}
```