Alibaba Cloud
Elastic Container Instance

Security

Issue: 20200525

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 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 contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

Style	Description	Example
	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.
	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.
	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.
	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]`

Style	Description	Example
{} or {a|b}	This format is used for a required value, where only one item can be selected.	switch {active|stand}

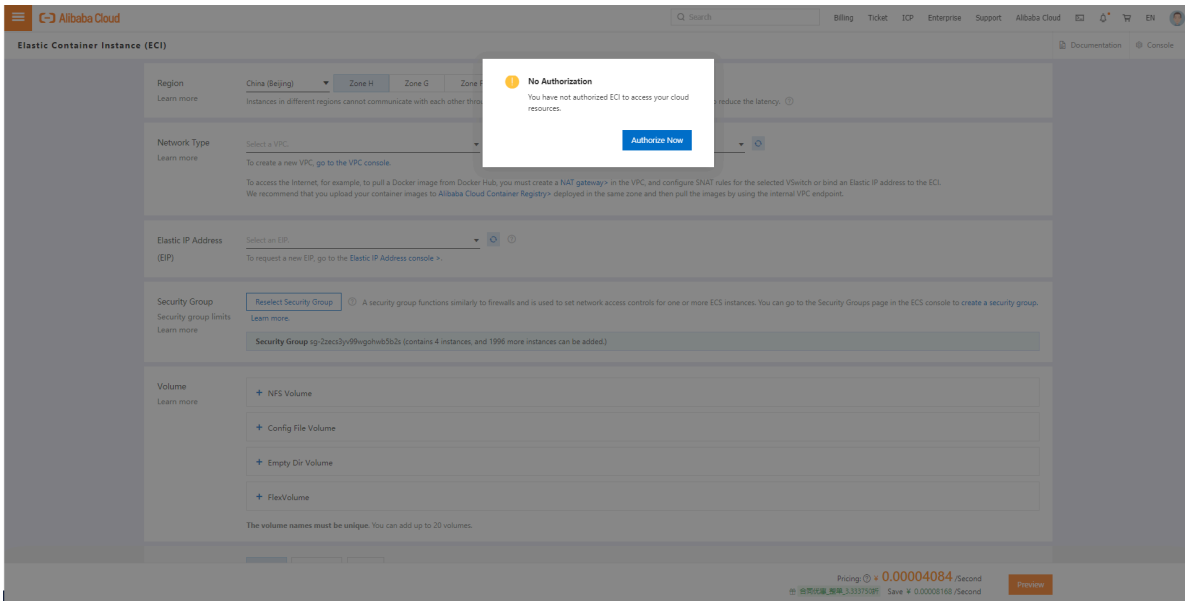
Contents

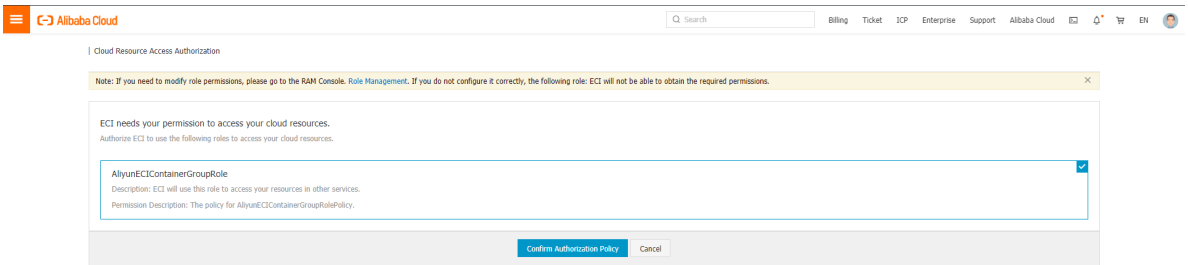
1 Authorize a RAM role

When you enable Elastic Container Instances (ECIs), grant the default role of AliyunECIContainerGroupRole to the service account. ECIs can call Elastic Compute Service (ECS), Virtual Private Cloud (VPC), and other services only when this default role is correctly granted.

Authorize a role

1. If you log on to the ECI console and you have not granted the default role to the service account, the following message is displayed. Click **Authorize** and then click **Confirm Authorization Policy**.





Notice:

The default role permissions have been set for ECIs. You can go to the RAM roles page to modify the role permissions. Incorrect configurations may cause ECIs to fail to obtain the required permissions.

2. After you complete the authorization, refresh the ECI console.

   To view detailed policy information about AliyunECIContainerGroupRole, you can log on to the RAM console.

Permissions granted to AliyunECIContainerGroupRole

The default role AliyunECIContainerGroupRole has permissions to perform the following actions.

ECS actions

Action	Description
ecs:CreateNetworkInterfacePermission	Create Elastic Network Interface (ENI) permissions
ecs:DeleteNetworkInterfacePermission	Delete ENI permissions
ecs:CreateNetworkInterface	Create an ENI
ecs:DescribeNetworkInterfaces	Query an ENI
ecs:AttachNetworkInterface	Attach an ENI to an instance
ecs:DetachNetworkInterface	Detach an ENI from an instance
ecs:DeleteNetworkInterface	Delete an ENI
ecs:DescribeSecurityGroups	Query security group information

VPC actions

Action	Description
vpc:DescribeVSwitches	Query VSwitches in a VPC
vpc:DescribeVpcs	Query VPCs
vpc:AssociateEipAddress	Attach an Elastic IP address
vpc:DescribeEipAddresses	Query Elastic IP addresses

Image repository actions

Action	Description
cr:Get*	Query the image information of ECS instances.

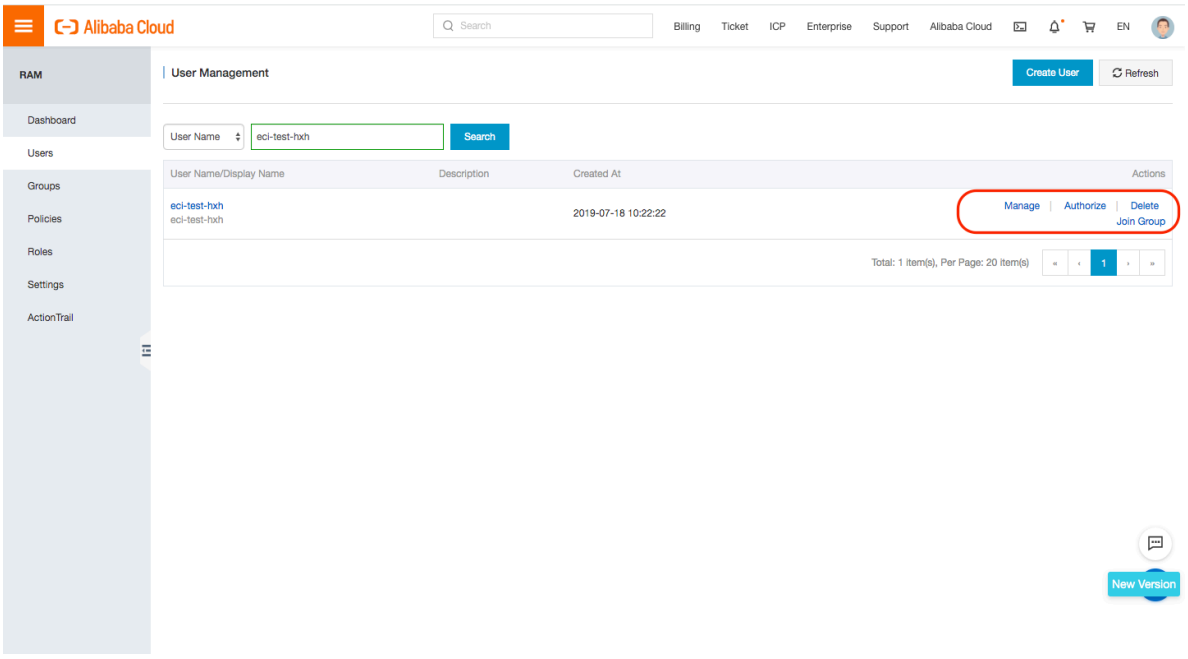
Action	Description
cr:List*	Query the image list information of ECS instances.
cr:PullRepository	Pull images from a repository.

2 Grant permissions to a RAM user

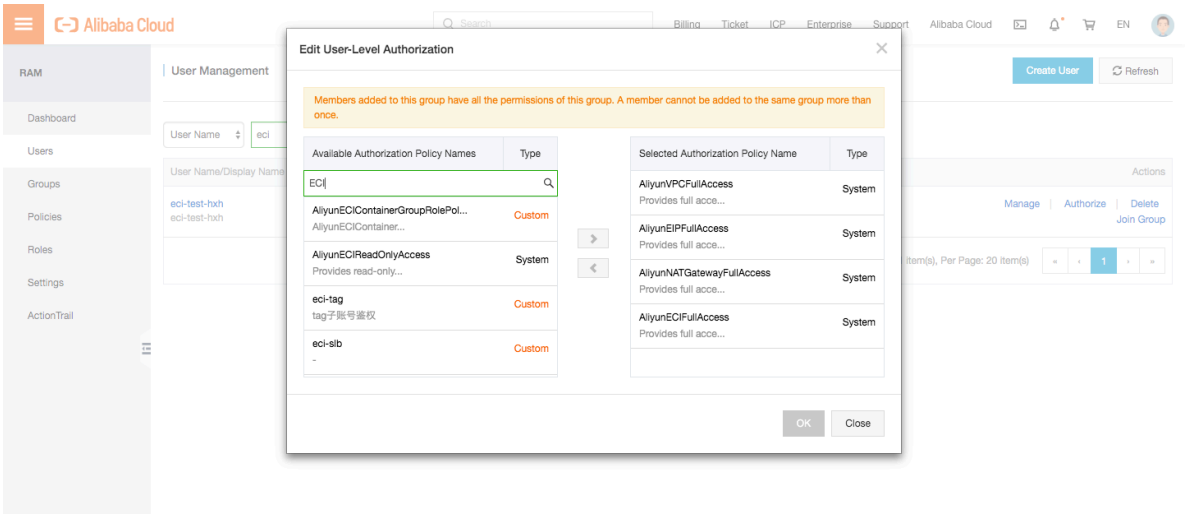
This topic describes how to authorize a Resource Access Management (RAM) user to use the features of Elastic Container Instance (ECI).

You can use an Alibaba Cloud account or a RAM user to manage ECI resources. However, when a RAM user is created, it has no permissions to manage the resources of the Alibaba Cloud account. Therefore, you need to grant permissions to the RAM user before you use it to manage ECI resources.

1. Log on to the RAM console.
2. Check whether you have RAM users on the **Overview** page of the RAM console. If you do not have any RAM users, create one. For more information, see Create a RAM user .
3. If you have RAM users, click **Users** in the left-side navigation pane of the RAM console . On the page that appears, find the target RAM user to which you want to grant permissions, as shown in the following figure.

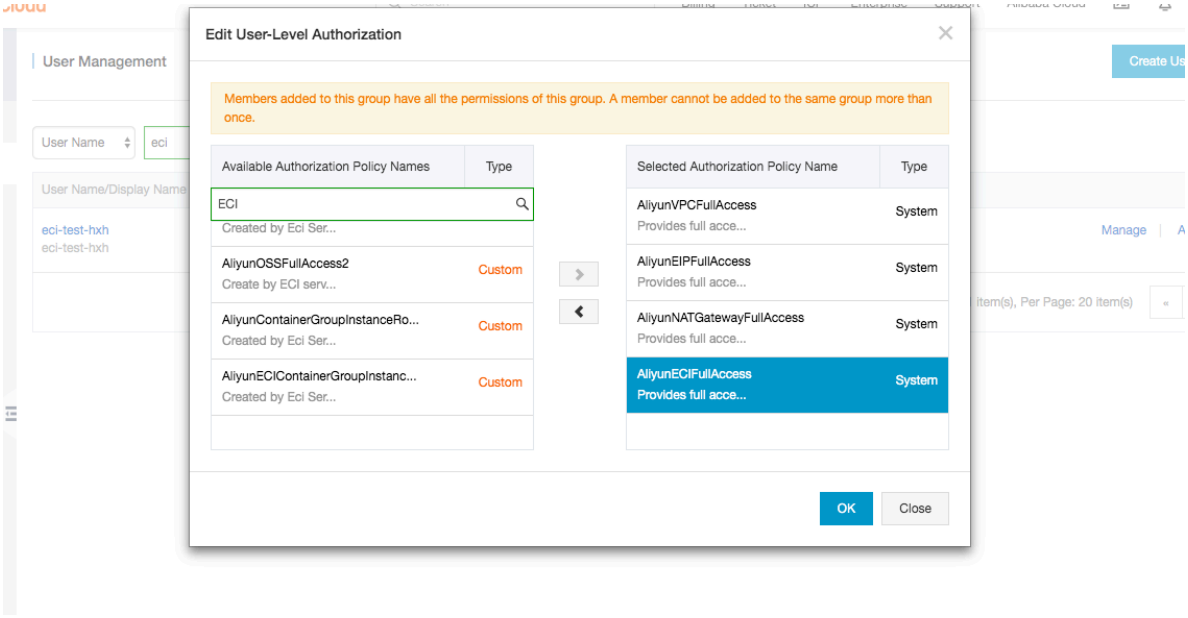


4. Click **Add Permissions** in the Actions column. The **Add Permissions** pane appears, as shown in the following figure.



5. In the **Add Permissions** pane, enter a keyword in the Select Policy search box to search for ECI authorization policies. Select an authorization policy as required to add it to the **Selected** section, as shown in the following figure.

   - To grant ECI read/write permissions to the RAM user, select **AliyuECIFullAccess**.
   - To grant ECI read-only permissions to the RAM user, select **AliyunECIReadOnlyAccess**.



6. Click **OK**.

3 Use resource groups for authentication

Resource group

A resource group is a set of resources owned by end users. You can use resource groups to manage resources in Alibaba Cloud services such as Elastic Compute Service (ECS), ApsaraDB for RDS, Server Load Balancer (SLB), and Elastic Container Instance (ECI).

With resource groups, you can divide resources based on their purposes and manage user permissions.

For example, a company purchases cloud resources by using an Alibaba Cloud account. Some of these resources are used for test environments and some are used for production environments. In this case, resources for different purposes can be added to separate resource groups.

This topic describes how to use ECI resource groups to manage the permissions of RAM users.

Benefits

If you do not use resource groups, you can use an Alibaba Cloud account to grant all ECI-related permissions to RAM users. These include the create, modify, and delete permissions on all ECIs under the Alibaba Cloud account. In this case, a conflict may occur because the resources of each RAM user may need to be isolated. However, if you use resource groups, you can restrict the permissions of a RAM user to a single resource group. The RAM user can only manage resources in the resource group, but not resources outside the resource group.

Authentication rules for API operations

CreateContainerGroup

Alibaba Cloud account

An Alibaba Cloud account has the highest level of permissions. If you call the CreateContainerGroup operation by using an Alibaba Cloud account, you can create an ECI and add it to any resource group under the account. If you do not specify a resource group ID, the newly created ECI is added to the default resource group by default.

RAM user

If the permissions of a RAM user are restricted to a single resource group, and you want to create an ECI as the RAM user, you must specify the resource group ID when creating the ECI. However, if the resource group that the RAM user is restricted to use is the default resource group, you do not need to specify the resource group ID. In this case, the created ECI is added to the default resource group. If you specify a resource group ID, the system verifies the resource group ID.

If the permissions of the RAM user are not restricted to a resource group, you can add the ECI to the default resource group.

DescribeContainerGroups

Alibaba Cloud account

An Alibaba Cloud account has the highest level of permissions. If you call the DescribeContainerGroups operation by using an Alibaba Cloud account, the information about all ECIs under the account is returned by default. The operation is not restricted by resource groups.

However, if you specify a resource group ID as a filtering condition, the information about all matching ECIs in the resource group is returned. Only Alibaba Cloud accounts have such permission.

RAM user

If the permissions of a RAM user are restricted to a resource group, you must specify the resource group when you query ECIs. Otherwise, the authentication fails. The query will not be performed until the resource group is verified. The ECIs whose information is returned belong to the specified resource group.

DescribeContainerLog

Alibaba Cloud account

An Alibaba Cloud account has the highest level of permissions. If you call the DescribeContainerLog operation by using an Alibaba Cloud account, you can query the container logs of any ECI under the account.

RAM user

If you call the DescribeContainerLog operation as a RAM user, you are not required to specify the resource group ID. If the requested ECI is under any resource group, the system checks whether the RAM user has permissions on the resource group. You can proceed with the operation only if the authentication succeeds. This prevents unauthorized operations.

DeleteContainerGroup

Alibaba Cloud account

An Alibaba Cloud account has the highest level of permissions. If you call the DeleteContainerGroup operation by using an Alibaba Cloud account, you can delete any ECI under the account.

RAM user

If you call the DeleteContainerGroup operation as a RAM user, you are not required to specify the resource group ID. If the requested ECI is under any resource group, the system checks whether the RAM user has permissions on the resource group. You can proceed with the operation only if the authentication succeeds. This prevents unauthorized operations.

Resource lifecycle management

ECI does not allow users to modify resource groups. Resources can be added to the specified resource group or default resource group only when they are created. When resources are deleted, they are automatically removed from the resource group.

Common scenarios

Assume that the following three resource groups exist under an Alibaba Cloud account: default resource group, test_a, and test_b.

The following two RAM users exist under the Alibaba Cloud account: test and test2. The former has full permissions to the test_a resource group. The latter has full permissions to the default resource group.

CreateContainerGroup

Alibaba Cloud account

- If you call the CreateContainerGroup operation by using the Alibaba Cloud account and do not specify the resource group ID, the created ECI is added to the default resource group.
- If you call the CreateContainerGroup operation by using the Alibaba Cloud account and specify a valid resource group ID, the created ECI is added to the specified resource group.
- If you call the CreateContainerGroup operation by using the Alibaba Cloud account and specify an invalid resource group ID, the created ECI is added to the default resource group.

RAM user

- If you call the CreateContainerGroup operation as the test RAM user and do not specify the resource group ID, the authentication fails.
- If you call the CreateContainerGroup operation as the test RAM user and specify an invalid resource group ID, the authentication fails.
- If you call the CreateContainerGroup operation as the test2 RAM user and do not specify the resource group ID, the created ECI is added to the default resource group.
- If you call the CreateContainerGroup operation as the test RAM user and specify a valid resource group ID, the created ECI is added to the specified resource group.

DescribeContainerGroups

Alibaba Cloud account

- If you call the DescribeContainerGroups operation by using the Alibaba Cloud account and do not specify the resource group ID, the information about all ECIs under the account is returned.
- If you call the DescribeContainerGroups operation by using the Alibaba Cloud account and specify a valid resource group ID, the information about the ECIs in the specified resource group is returned.
- If you call the DescribeContainerGroups operation by using the Alibaba Cloud account and specify an invalid resource group ID, an empty response is returned.

RAM user

- If you call the DescribeContainerGroups operation as the test RAM user and do not specify the resource group ID, the authentication fails.
- If you call the DescribeContainerGroups operation as the test RAM user and specify an invalid resource group ID, the authentication fails.
- If you call the DescribeContainerGroups operation as the test RAM user and specify a valid resource group ID, the information about the ECIs in the specified resource group is returned.
- If you call the DescribeContainerGroups operation as the test RAM user and specify a valid resource group ID, but the requested ECI is not in the resource group, an empty response is returned.

DescribeContainerLog

Alibaba Cloud account

- If you call the DescribeContainerLog operation by using the Alibaba Cloud account, you can retrieve the container logs of any ECI in the default resource group.
- If you call the DescribeContainerLog operation by using the Alibaba Cloud account, you can retrieve the container logs of any ECI in the test_a resource group.

RAM user

- If you call the DescribeContainerLog operation as the test RAM user to query the container logs of an ECI in the resource group owned by the test account, the authentica tion succeeds.
- If you call the DescribeContainerLog operation as the test RAM user to query the container logs of an ECI in a resource group that is not owned by the test account, the authentication fails.

DeleteContainerGroup

Alibaba Cloud account

- If you call the DeleteContainerGroup operation by using the Alibaba Cloud account, you can delete any ECI in the default resource group.
- If you call the DeleteContainerGroup operation by using the Alibaba Cloud account, you can delete any ECI in the test_a resource group.

RAM user

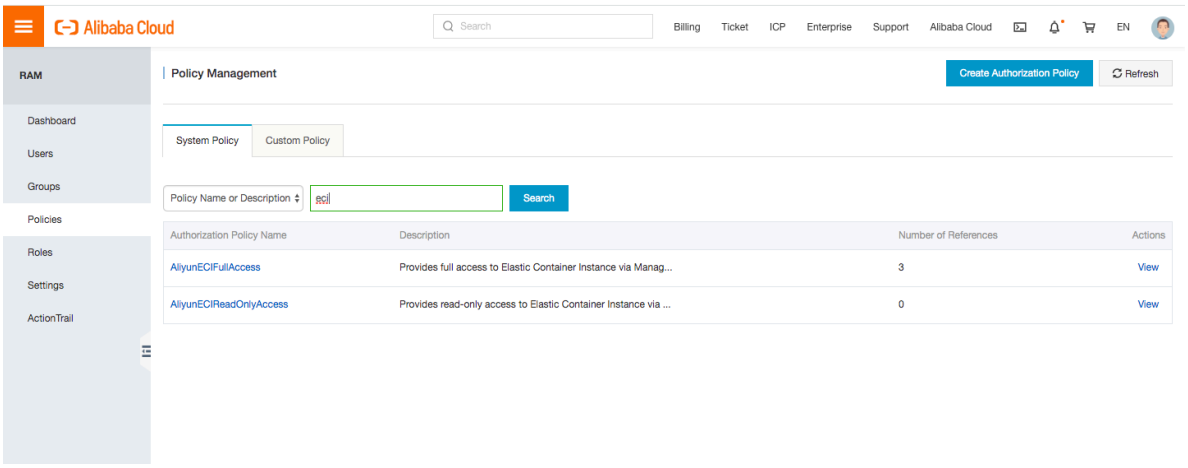
- If you call the DeleteContainerGroup operation as the test RAM user to delete an ECI in the resource group owned by the test RAM user, the authentication succeeds.
- If you call the DeleteContainerGroup operation as the test RAM user to delete an ECI in a resource group that is not owned by the test RAM user, the authentication fails.

4 Authenticate RAM users based on tags

Elastic Container Instance (ECI) allows you to manage resources by using resource groups and manage permissions of Resource Access Management (RAM) users based on resource groups. Now, ECI supports a new authentication method for RAM users, that is, tag-based authentication.

Procedure

1. Log on to the RAM console. In the left-side navigation pane, click Policies. On the page that appears, set Policy Type to System Policy and enter ECI in the search box.



Click AliyunECIFullAccess. The following code appears:

```
"Version": "1",
"Statement": [
  {
    "Action": "eci:*",
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "ecs:DescribeSecurityGroups"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "vpc:DescribeVSwitches",
      "vpc:DescribeVpcs",
      "vpc:DescribeEipAddresses"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }
]
```

```
}
```

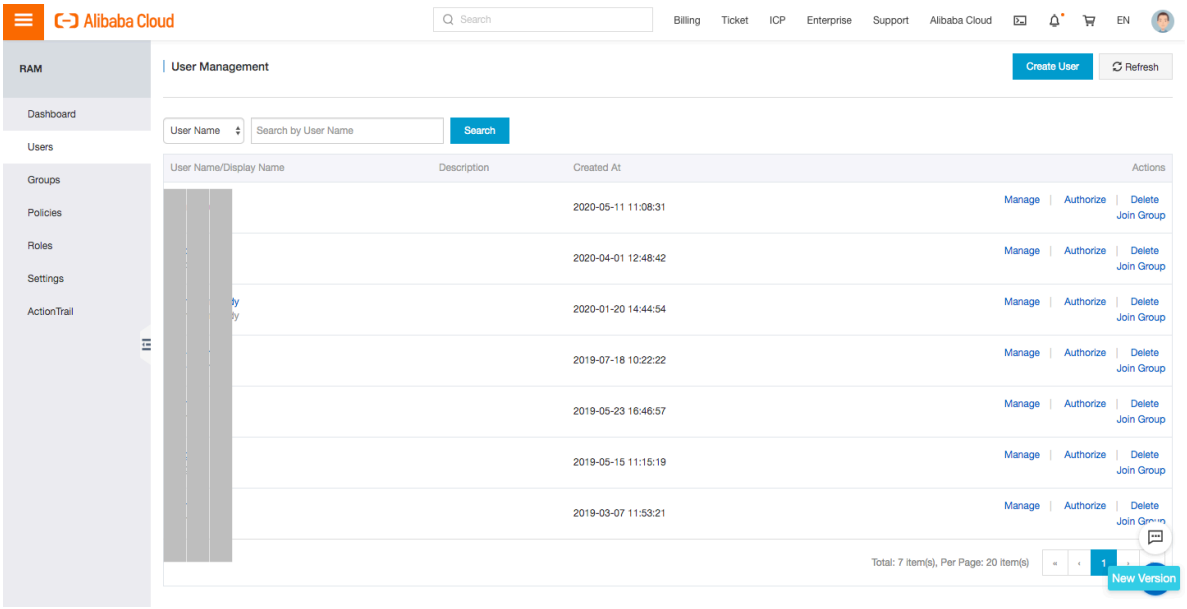
The preceding code displays ECI full permissions generated by the system.

2. On the Policies page, click Create Policy. On the page that appears, set Configuration Mode to Script, enter ECI in the search box, and then select AliyunECIFullAccess. The relevant code appears. Modify the code as shown in the following example:

```
{
 "Version": "1",
 "Statement": [
  {
   "Action": "eci:*",
   "Resource": "*",
   "Effect": "Allow",
   "Condition": {
    "StringEquals": {
     "eci:tag/name": "liumi",
     "eci:tag/env": "test"
    }
   }
  },
  {
   "Action": [
    "ecs:DescribeSecurityGroups"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "vpc:DescribeVSwitches",
    "vpc:DescribeVpcs",
    "vpc:DescribeEipAddresses"
   ],
   "Resource": "*",
   "Effect": "Allow"
  }
 ]
}
```

The preceding code adds tag conditions to the AliyunECIFullAccess policy. The RAM user to which this policy is applied can only manage the resources that meet the following requirements: name=liumi and env=test. You can change the tags based on your business requirements. After the authorization policy is applied, the RAM user has full permissions to the ECI resources that have the specified tags. The RAM user cannot manage the ECI resources that have tags other than those specified.

3. To apply the policy to a RAM user, click Users in the left-side navigation pane. Find the target RAM user that you want to set the tag permissions for in the list, or create a new RAM user.



Click Add Permissions in the Actions column. In the Add Permissions pane that appears , set Select Policy to Custom Policy and select the authorization policy that you have created.

Common scenarios

Taking the RAM user in the preceding steps as an example, the expected results are as follows:

CreateContainerGroup

- If you call the CreateContainerGroup operation and do not specify tags, the authentica tion fails.
- If you call the CreateContainerGroup operation and specify tags that do not match the authorized tags, the authentication fails.
- If you call the CreateContainerGroup operation and specify tags that match the authorized tags, the authentication succeeds.
- If you call the CreateContainerGroup operation and specify tags that contain the authorized tags, the authentication succeeds.

RestartContainerGroup

- If you call the RestartContainerGroup operation by using the Alibaba Cloud account and specify tags that do not match the authorized tags, the authentication fails.

- If you call the RestartContainerGroup operation by using the Alibaba Cloud account and specify tags that match the authorized tags, the authentication succeeds.
- If you call the RestartContainerGroup operation as the RAM user and specify tags that match the authorized tags, the authentication succeeds.

ExportContainerGroupTemplate

- If you call the ExportContainerGroupTemplate operation by using the Alibaba Cloud account and specify tags that do not match the authorized tags, the authentication fails.
- If you call the ExportContainerGroupTemplate operation by using the Alibaba Cloud account and specify tags that match the authorized tags, the authentication succeeds.
- If you call the ExportContainerGroupTemplateoperation as the RAM user and specify tags that match the authorized tags, the authentication succeeds.

ExecContainerCommand

- If you call the ExecContainerCommand operation by using the Alibaba Cloud account and specify tags that do not match the authorized tags, the authentication fails.
- If you call the ExecContainerCommand operation by using the Alibaba Cloud account and specify tags that match the authorized tags, the authentication succeeds.
- If you call the ExecContainerCommand operation as the RAM user and specify tags that match the authorized tags, the authentication succeeds.

DescribeContainerLog

- If you call the DescribeContainerLog operation by using the Alibaba Cloud account and specify tags that do not match the authorized tags, the authentication fails.
- If you call the DescribeContainerLog operation by using the Alibaba Cloud account and specify tags that match the authorized tags, the authentication succeeds.
- If you call the DescribeContainerLog operation as the RAM user and specify tags that match the authorized tags, the authentication succeeds.

DescribeContainerGroups

- When you call the DescribeContainerGroups operation, if you do not specify tags and you specify a resource ID whose tags do not match the authorized tags, the authentica tion fails.
- When you call the DescribeContainerGroups operation, if you do not specify tags and you specify a resource ID whose tags match the authorized tags, the authentication succeeds.

- When you call the DescribeContainerGroups operation, if you specify tags that do not match the authorized tags and you do not specify a resource ID, the authentication fails.
- When you call the DescribeContainerGroups operation, if you specify tags that match the authorized tags and you do not specify a resource ID, the authentication succeeds.
- When you call the DescribeContainerGroups operation, if you specify both tags and a resource ID, the specified tags are used only as filtering conditions, and the tags of the resource ID are used for authentication.
- When you call the DescribeContainerGroups operation, if you do not specify tags or a resource ID, the authentication fails even if you specify other filtering conditions. In this case, you need to specify tags in the console.

Notice:

Note: If the authentication fails, the operation returns an empty result instead of an error.

UpdateContainerGroup

- When you call the UpdateContainerGroup operation, If you update an ECI whose tags do not match the authorized tags, the authentication fails.
- When you call the UpdateContainerGroup operation, if you update an ECI whose tags match the authorized tags and you do not update the tags, the authentication succeeds.
- When you call the UpdateContainerGroup operation, if you update an ECI whose tags match the authorized tags, you update the tags, and you have no permissions to the new tags, the authentication fails.
- When you call the UpdateContainerGroup operation, if you update an ECI whose tags match the authorized tags, you update the tags, and you have permissions to the new tags, the authentication succeeds.

This is a complicated situation.

If you want to update tags, you must ensure that you have the permissions on the existing and updated tags. How do you ensure that you have the required permissions?

The following two examples show the possible methods.

Example 1: Add two tags to the existing permissions.

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "eci:*",
      "Resource": "*",
      "Effect": "Allow",
```

```
    "Condition": {
     "StringEquals": {
      "eci:tag/name": "liumi",
      "eci:tag/env": "test",
      "eci:tag/name": "liumi2",
      "eci:tag/env": "pre"
     }
    }
   },
   {
    "Action": [
     "ecs:DescribeSecurityGroups"
    ],
    "Resource": "*",
    "Effect": "Allow"
   },
   {
    "Action": [
     "vpc:DescribeVSwitches",
     "vpc:DescribeVpcs",
     "vpc:DescribeEipAddresses"
    ],
    "Resource": "*",
    "Effect": "Allow"
   }
  ]
}
```

This method is not recommended because it reduces the scope of permissions and causes tag mismatch. We recommend that you use the following method.

Example 2: Add separate permissions to the RAM user.

```
{
 "Version": "1",
 "Statement": [
  {
   "Action": "eci:*",
   "Resource": "*",
   "Effect": "Allow",
   "Condition": {
    "StringEquals": {
     "eci:tag/name": "liumi2",
     "eci:tag/env": "pre"
    }
   }
  },
  {
   "Action": [
    "ecs:DescribeSecurityGroups"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "vpc:DescribeVSwitches",
    "vpc:DescribeVpcs",
    "vpc:DescribeEipAddresses"
   ],
   "Resource": "*",
   "Effect": "Allow"
```

```
    }
  ]
}
```