ALIBABA CLOUD

Alibaba Cloud

弹性容器实例

安全

文档版本：20220511

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.弹性容器实例服务关联角色

本文为您介绍弹性容器实例服务关联角色AliyunServiceRoleForECI以及如何删除服务关联角色。

背景信息

弹性容器实例服务关联角色AliyunServiceRoleForECI是ECI在某些情况下，为了完成自身的某个功能，需要获取其他云服务的访问权限而提供的RAM角色。更多关于服务关联角色的信息，请参见服务关联角色。

AliyunServiceRoleForECI应用场景

在创建ECI实例和镜像缓存的过程中，ECI需要访问云服务器ECS、专有网络VPC、容器镜像服务ACR、日志服务SLS和负载均衡SLB的资源时，可以通过自动创建的弹性容器实例服务关联角色AliyunServiceRoleForECI获取访问权限。

AliyunServiceRoleForECI权限说明

弹性容器实例服务关联角色AliyunServiceRoleForECI对应的角色权限策略为AliyunServiceRolePolicyForECI，包含的云服务访问权限如下：

```
{
    "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":[
```

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

删除AliyunServiceRoleForECI

如果您需要删除弹性容器实例服务关联角色AliyunServiceRoleForECI，请先通过控制台或者OpenAPI删除依赖该服务关联角色的ECI资源，包括ECI实例和镜像缓存。删除ECI实例和镜像缓存后，您可以删除AliyunServiceRoleForECI。具体操作，请参见删除RAM角色。

2.为RAM用户授权

默认情况下，您可以使用阿里云账号完整操作该账号下的ECI资源，但如果您使用的是RAM用户，则需要进行授权，RAM用户才可以操作ECI资源。本文介绍如何为RAM用户进行授权。

前提条件

已创建RAM用户。具体操作，请参见创建RAM用户。

背景信息

为RAM用户授权时，您可以根据使用需求为其授予相应的权限策略。ECI相关的权限如下：

- AliyunECIReadOnlyAccess

  只读访问ECI资源的权限。默认提供的系统权限策略，包含的权限如下：

  - eci:Describe*：获取ECI相关资源列表
  - eci:List*：获取ECI相关资源列表
  - ecs:DescribeSecurityGroups：获取安全组列表
  - vpc:DescribeVSwitches：获取交换机列表
  - vpc:DescribeVpcs：获取VPC列表

- AliyunECIFullAccess

  管理ECI资源的权限。默认提供的系统权限策略，包含的权限如下：

  - eci：ECI相关资源的所有操作权限
  - ecs:DescribeSecurityGroups：获取安全组列表
  - vpc:DescribeVSwitches：获取交换机列表
  - vpc:DescribeVpcs：获取VPC列表
  - vpc:DescribeEipAddresses：获取EIP列表

- 在ECI控制台操作时所需的其它权限

  如果您需要使用ECI控制台进行操作，则除了AliyunECIFullAccess默认的权限外，还需要以下权限：

  - ram:ListRoles：获取实例的RAM角色
  - nas:DescribeFileSystems：获取NAS文件系统列表
  - oss:ListBuckets：获取OSS Bucket列表
  - vpc:DescribeCommonBandwidthPackages：获取共享带宽包列表
  - cr:GetRepoList：获取镜像仓库列表
  - cr:GetRepoTags：获取镜像Tag
  - cr:GetImageManifest：获取镜像详情
  - cr:SearchRepo：搜索镜像仓库

操作步骤

1. 使用阿里云账号登录RAM控制台。

2. 如果想要为RAM用户授予在控制台操作ECI资源的权限，您需要创建对应的自定义权限策略。
   i. 在左侧导航栏选择**权限管理>权限策略**。
   ii. 单击**创建权限策略**。
   iii. 选择**脚本编辑**页签，复制以下脚本到策略内容中，然后单击**下一步**。

```
{
    "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. 输入策略名称，单击**确定**。
3. 根据需要为RAM用户添加权限。
   i. 在左侧导航栏选择**身份管理>用户**。
   ii. 找到待授权的RAM用户，单击对应操作列中的**添加权限**。

iii. 在**添加权限**面板，完成相关配置。

相关配置说明如下表所示。

参数	描述
授权范围	根据需要选择权限的生效范围： ■ 整个云账号：在当前阿里云账号内生效。 ■ 指定资源组：在指定的资源组内生效。
授权主体	需要授权的RAM用户。系统将自动填入您选择的RAM用户，您也可以手动添加其它用户。
选择权限	根据需要选择对应的权限。常见场景如下： ■ 只查看ECI资源：在系统策略中选择AliyunECIReadOnlyAccess。 ■ 通过openAPI操作ECI资源：在系统策略中选择AliyunECIFullAccess。 ■ 通过控制台操作ECI资源：在系统策略中选择AliyunECIFullAccess，在自定义策略中选择第2步创建的自定义策略。

iv. 单击**确定**。

v. 确认授权应用范围和权限策略，然后单击**完成**。

3.通过资源组实现RAM用户鉴权

创建ECI资源时，您可以指定所属的资源组，以便对资源进行分组管理。本文介绍如何通过资源组控制RAM用户的权限，实现RAM用户只能操作特定资源组内的ECI资源。

背景信息

资源组是在阿里云账号下进行资源分组管理的一种机制，可以帮助您解决单个阿里云账号内的资源分组和授权管理的问题。资源组的使用说明如下：

- 一个资源组可以包含不同地域的云资源。例如：资源组A中可以包含华北2（北京）地域的实例和华东1（杭州）地域的实例。
- 同一个账号内不同资源组中，相同地域的资源可以进行关联。例如：资源组A中华北2（北京）地域的实例可以加入到资源组B中华北2（北京）地域的VPC内。
- 资源组会继承RAM用户的全局权限，即：如果您授权RAM用户管理所有的阿里云资源，那么阿里云账号下所有的资源组都会在该RAM用户中显示出来。

应用场景

每个ECI资源（ECI实例、镜像缓存）必须且只能属于一个资源组。创建ECI资源时，您可以指定资源组，如果没有指定资源组，则该资源将加入到默认资源组中。

> **说明**
>
> 目前不支持修改ECI资源的资源组，即ECI资源只能在创建的时候加入指定的资源组或默认资源组，在删除的时候自动从资源组中移出。

您可以将不同用途的ECI资源分别加入到多个资源组中，并为每个资源组设置不同的RAM用户作为管理员，从而实现分组、分权管理ECI资源。

例如：如果您的ECI实例分别用于生产环境和测试环境，您可以将ECI实例分别加入到生产资源组和测试资源组中，授权RAM用户A可以操作生产资源组中的ECI实例，授权RAM用户B可以操作测试资源组中的ECI实例。配置完成后，当产品进行测试时，由RAM用户B操作测试资源组中的ECI实例。当产品需要上线时，由RAM用户A对生产资源组中的ECI实例进行操作。两套环境由不同的RAM用户进行管理，可以很好地控制权限，避免不必要的误操作。

配置流程

按以下场景为示例，创建多个资源组对ECI资源进行分组，并授权RAM用户只能操作特定资源组的ECI资源：

- 新增两个资源组：生产资源组、测试资源组。
- 新增两个RAM用户：RAM用户A具备生产环境的AliyunECIFullAccess权限，RAM用户B具备测试环境的AliyunECIFullAccess权限。

  > **说明**
  >
  > AliyunECIFullAccess是RAM提供的系统策略，包含操作ECI资源的所有权限。

配置流程如下：

1. 创建两个资源组。具体操作，请参见创建资源组。
2. 创建两个RAM用户。具体操作，请参见创建RAM用户。

3. 分别为两个资源组设置对应的RAM用户作为管理员。具体操作，请参见添加RAM身份并授权。

   授权时，授权主体请输入RAM用户，权限可以选择AliyunECIFullAccess权限。

4. 指定资源组创建ECI实例。
   - 如果通过弹性容器实例售卖页创建，请在**其他设置（选填）**页面指定资源组。
   - 如果调用CreateContainerGroup创建，请传入资源组ID（ResourceGroupId）。

预期结果

按配置流程配置分组、分权管理ECI实例后，预期结果如下：

- 在弹性容器实例控制台上，RAM用户只能查看和操作有权限的资源组中的ECI资源。
- 调用各API接口时，RAM用户只能查看和操作有权限的资源组中的ECI资源。例如：
  - CreateContainerGroup

    创建ECI实例时，必须要传入正确的资源组ID，才可以通过鉴权；如果没有传入资源组ID，或者传入的资源组ID不正确，则鉴权不通过。

    > **说明**
    >
    > 如果RAM用户具备默认资源的权限，则无需传入资源组ID，ECI实例将默认将加入到默认资源组中。

  - DescribeContainerGroups

    查询ECI实例信息时，必须要传入正确的资源组ID，才可以通过鉴权；如果没有传入资源组ID，或者传入的资源组ID不正确，则鉴权不通过。

    > **说明**
    >
    > 如果传入的ECI实例ID与资源组ID不匹配，即ECI实例不属于该资源组时，即使资源组ID正确，也无法查看ECI实例的信息。

  - DescribeContainerLog

    查询ECI实例的日志时，无需传入资源组ID，系统将自动检索ECI实例所属的资源组并进行鉴权。

  - DeleteContainerGroup

    删除ECI实例时，无需传入资源组ID，系统将自动检索ECI实例所属的资源组并进行鉴权。

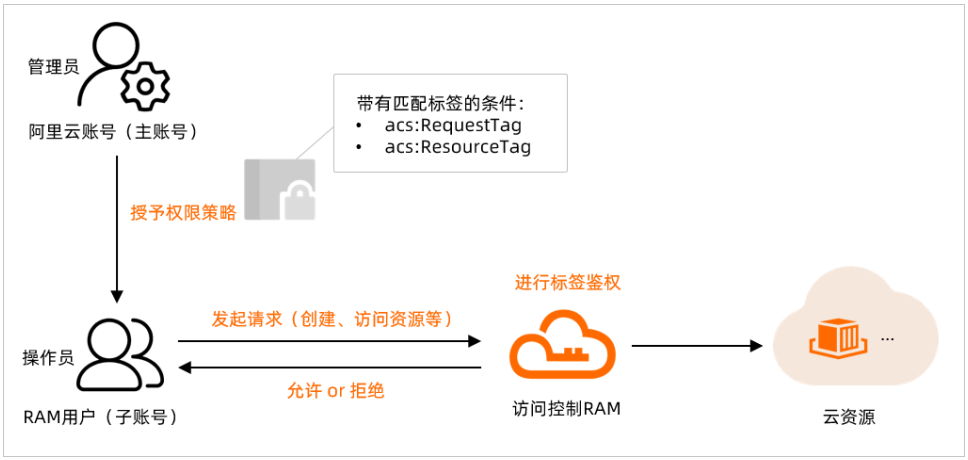
4.通过标签实现RAM用户鉴权

本文介绍如何基于标签控制RAM用户权限，实现不同的用户可以拥有不同云资源的访问和操作权限。

背景信息

标签可用于标识云资源，实现分类管理资源；访问控制RAM可基于权限策略，控制云资源的访问和操作权限。结合标签和RAM，将标签作为权限策略的匹配条件，可以实现云资源精细化权限管理。

基于标签控制RAM用户权限（即标签鉴权）的逻辑如下：



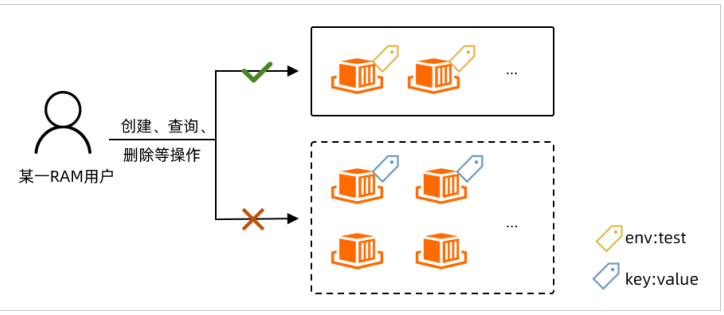
> **说明**
>
> 支持绑定标签的ECI资源包括ECI实例、镜像缓存和虚拟节点；仅支持在创建或者更新ECI资源时为其绑定标签。更多信息，请参见使用标签管理ECI实例。

配置示例

示例场景说明

本文以下述场景作为示例，说明如何实现标签鉴权。

假设您需要控制某一RAM用户只能操作特定（假设绑定了 `env:test` 标签）的ECI资源，如下图：



具体需求包括：

- 需求1：不允许创建不带标签的ECI资源，仅当创建时为ECI资源绑定 `env:test` 标签才可以创建成功。
- 需求2：只允许操作自身创建（即绑定 `env:test` 标签）的ECI资源，不允许操作其它ECI资源。

- 需求3：查询ECI资源时，只允许查看自身创建（即绑定 `env:test` 标签）的ECI资源。

步骤一：配置自定义权限策略并授权

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏选择**权限管理>权限策略管理**。
3. 在**权限策略管理**页面，单击**创建权限策略**。
4. 完成自定义策略配置。
   i. 选择**脚本编辑**页签。
   ii. 单击右上角的**导入系统策略**，在弹出的对话框中选择AliyunECIFullAccess，单击**导入**。

   AliyunECIFullAccess为系统默认的管理ECI资源的权限，包括操作ECI资源、查询相关资源（安全组、VPC等资源）、创建ECI服务关联角色等权限。
   iii. 修改权限策略内容，然后单击**下一步：编辑基本信息**。

> **说明**
>
> 权限策略是一组访问权限的集合。结构包括版本号和授权语句列表，每条授权语句包括授权效果（Effect）、操作（Action）、资源（Resource）以及条件（Condition，可选项）。更多信息，请参见权限策略语法和结构和权限策略基本元素。

在权限策略的 `Condition` 中，您可以增加需要匹配标签的条件来限制操作权限。支持的标签条件关键字如下：

标签条件关键字	说明
`acs:RequestTag`	限制在请求中必须传入特定的标签。 如果API请求中没有标签参数，则不能使用 `acs:RequestTag` ，否则会导致鉴权失败。
`acs:ResourceTag`	限制指定的资源必须包含特定的标签。 如果API请求中没有资源ID参数，则不能使用 `acs:ResourceTag` ，否则会导致鉴权失败。

> **说明**
>
> 设计权限策略时，您可以根据各操作接口特性（API请求是否需要指定资源ID、是否支持传入标签），结合实际业务需求，来设置 `acs:RequestTag` 或 `acs:ResourceTag` 。更多信息，请参见API接口鉴权说明。

根据示例场景中的需求，设计权限策略如下：

需求	权限策略

不允许创建不带标签的ECI资源，仅当创建时为ECI资源绑定 `env:test` 标签才可以创建成功	<pre>{
	"Effect": "Allow",
	"Action": "eci:Create*",
	"Resource": "*",
	"Condition": {
	"StringEquals": {
	"acs:RequestTag/env": "test"
	}
	}
	}</pre>

只允许操作绑定了env:test标签的ECI资源，不允许操作其它资源	<pre>{
	"Effect": "Allow",
	"Action": "eci:*",
	"Resource": "*",
	"Condition": {
	"StringEquals": {
	"acs:ResourceTag/env": "test"
	}
	}
	}</pre>

查询ECI资源时，只允许查看绑定了env:test标签的ECI资源。	<pre>{
	"Effect": "Allow",
	"Action": "eci:Describe*",
	"Resource": "*",
	"Condition": {
	"StringEquals": {
	"acs:RequestTag/env": "test"
	}
	}
	}</pre>

结合AliyunECIFullAccess已有的权限策略，完整权限策略示例如下：

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

> **说明**
>
> 如果您通过OpenAPI操作ECI资源，则使用AliyunECIFullAccess的权限即可；如果您通过ECI控制台操作ECI资源，则除了AliyunECIFullAccess的权限外，还需添加额外权限。更多信息，请参见为RAM用户授权。

iv. 输入权限策略名称，单击**确定**。

5. 将自定义权限策略授予RAM用户。
   i. 在左侧导航栏选择**人员管理>用户**。
   ii. 创建RAM用户。

   请根据自身管理需求创建相应的RAM用户。具体操作，请参见创建RAM用户。如果已有RAM用户，可跳过该步骤。

   iii. 为RAM用户授权。

   为RAM用户授予新创建的自定义权限策略，具体操作，请参见为RAM用户授权。

步骤二：验证权限策略是否生效

1. 使用RAM用户登录OpenAPI平台。
2. 测试权限策略是否生效。

   以ECI实例为例进行测试：

   - 创建ECI实例
     - 设置了 `env:test` 标签，则可以创建。
     - 没有设置标签或者设置了其它标签，则无法创建，提示没有权限。
   - 删除ECI实例
     - 删除的实例绑定了 `env:test` 标签，则可以删除。
     - 删除的实例没有绑定 `env:test` 标签，则无法删除，提示没有权限。
   - 查询ECI实例
     - 指定实例（该实例绑定了 `env:test` 标签）但没有设置标签，则查询出指定实例的信息。
     - 指定实例（该实例没有绑定 `env:test` 标签），则查询结果为空。
     - 没有指定实例，仅设置 `env:test` 标签，则查询出带有 `env:test` 标签的所有实例信息。
     - 没有指定实例也没有设置标签，则查询结果为空。

API接口鉴权说明

为某一RAM用户授予含有标签鉴权的权限策略后，该RAM用户调用各API接口时的鉴权情况如下表所示：

接口	鉴权说明
CreateContainerGroup、CreateImageCache等创建接口	该类接口无需指定资源ID，则匹配 `acs:RequestTag` ： • 没有传入标签，或者传入的标签不包含授权标签，则鉴权不通过。 • 传入完全匹配的标签，或者传入的标签包含了授权标签，则鉴权通过。
DescribeContainerGroups、DescribeImageCaches等查询接口	该类接口按需指定资源ID或传入标签，则匹配 `acs:ResourceTag` 或 `acs:RequestTag` ： • 传入资源ID和标签，如果指定资源绑定的标签能够匹配 `acs:ResourceTag` ，或者传入的标签能够匹配 `acs:RequestTag` ，则鉴权通过，反之则鉴权不通过。 • 传入资源ID，没有传入标签，如果指定资源绑定的标签能够匹配 `acs:ResourceTag` ，则鉴权通过，反之则鉴权不通过。 • 没有传入资源ID，传入标签，如果传入的标签能够匹配 `acs:RequestTag` ，则鉴权通过，反之则鉴权不通过。 • 没有传入资源ID，也没有传入标签，则鉴权不通过。 **说明** 查询接口在鉴权不通过时，返回结果为空，并不会报错。
UpdateContainerGroup、UpdateImageCache等更新接口	该类接口必须指定资源ID，则匹配 `acs:ResourceTag` ： • 不传入标签，如果指定资源绑定的标签能够匹配，则鉴权通过，反之则鉴权不通过。 • 传入标签（即更新标签），如果指定资源绑定的标签能够匹配，且同时具备所传入标签的权限，则鉴权通过，反之则鉴权不通过。 **说明** 更新标签时，RAM用户需要分别具有更新前后的标签权限。即授权时，需要授予用户两个自定义权限策略，分别包含更新前后的标签条件限制。
RestartContainerGroup、ExecContainerCommand等其它操作接口	该类接口必须指定资源ID，则匹配 `acs:ResourceTag` ： • 如果指定资源绑定的标签不能匹配，则鉴权不通过。 • 如果指定资源绑定的标签能够匹配，则鉴权通过。

5.通过API使用实例RAM角色

实例RAM角色允许您将一个角色关联到ECI实例，在实例内部基于STS（Security Token Service）临时凭证访问其他云产品的API。本文介绍如何通过API创建、授权实例RAM角色，并将该角色授予给ECI实例。

应用场景

ECI实例上部署的应用程序在云产品通信中，通过云账号或者RAM用户的AccessKey访问阿里云其他云产品（例如OSS、VPC、RDS等）的API。为了方便和快速地调用，部分用户直接把AccessKey固化在实例中，例如直接写在配置文件中。这种方式存在权限过高、泄露信息和难以维护等问题。实例RAM角色能够避免此类问题。

RAM角色是一种具备某些权限的虚拟用户，可以被ECI实例扮演，从而使得ECI实例获得相应的权限。使用RAM角色，无需在实例中保存AccessKey，通过修改RAM角色的权限即可变更ECI实例的权限，在使用上安全便捷。更多关于RAM角色的信息，请参见RAM角色概览。

使用流程

使用实例RAM角色的步骤如下：

1. 创建实例RAM角色

   调用CreateRole创建实例RAM角色，设置允许扮演该角色的可信实体为ECI服务（受信服务为ECS）。

2. 授权实例RAM角色

   根据需要调用CreatePolicy创建权限策略，然后调用AttachPolicyToRole将该权限策略授予给实例RAM角色。

3. （可选）授权RAM用户使用实例RAM角色

   如果您使用RAM用户创建ECI实例并指定实例RAM角色，则必须先授权RAM用户可以使用实例RAM角色。

4. 为ECI实例授予实例RAM角色

   调用CreateContainerGroup创建ECI实例，通过RamRoleName参数为ECI实例授予实例RAM角色，使得ECI实例获得对应的权限。一个ECI实例只能授予一个实例RAM角色。

5. （可选）获取临时授权Token

   为ECI实例授予了实例RAM角色后，如果需要在ECI实例内部部署的应用程序中访问云产品的API，您需要通过实例元数据获取实例RAM角色的临时授权Token。

创建实例RAM角色

调用CreateRole可以创建一个实例RAM角色。具体参数信息，请参见CreateRole。

您可以自定义设置RoleName来指定角色名（假设为ECIRamRoleTest），然后按如下策略文本设置AssumeRolePolicyDocument。

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

授权实例RAM角色

1. 调用CreatePolicy创建一个自定义权限策略。

   调用时，需设置以下参数：

   - PolicyName：权限策略名称（假设为ECIRamRoleTestPolicy）。
   - PolicyDocument：权限策略内容。

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

   更多信息，请参见CreatePolicy。

2. 调用AttachPolicyToRole为RAM角色添加权限策略。

   调用时，需设置以下参数：

   - PolicyName：指定权限策略名称，例如ECIRamRoleTestPolicy。
   - PolicyType：权限策略类型，配置为Custom，表示是自定义权限策略。
   - RoleName：指定RAM角色，例如ECIRamRoleTest。

   更多信息，请参见AttachPolicyToRole。

授权RAM用户使用实例RAM角色

如果您使用RAM用户，则必须先授权RAM用户具备该实例RAM角色的 `ram:PassRole` 权限，RAM用户才可以使用实例RAM角色。 `ram:PassRole` 权限决定RAM用户能否直接执行角色策略赋予的权限。

1. 使用阿里云账号（或者具备管理权限的RAM用户）登录RAM控制台。
2. 授权RAM用户使用实例RAM角色。

   授权时，请创建以下自定义权限策略，并将其授权给RAM用户。其中，ECIRamRoleTest为要授权的 `ram:PassRole` 权限的实例RAM角色。具体操作，请参见为RAM用户授权。

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

为ECI实例授予实例RAM角色

调用CreateContainerGroup创建ECI实例时，可以通过RamRoleName参数来指定RAM角色。更多信息，请参见CreateContainerGroup。

> **说明**
>
> 一个ECI实例只能授予一个实例RAM角色。如果ECI实例已有RAM角色，则会报错提示您不能附加新的角色。

获取临时授权Token

您可以获得实例RAM角色的临时授权Token，该临时授权Token可以执行实例RAM角色的权限和资源，并且该临时授权Token会自动周期性地更新。

执行以下命令可以检索名为ECIRamRoleTest的实例RAM角色的临时授权Token。

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

返回结果中获得临时授权Token。返回示例如下：

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