Alibaba Cloud

访问控制

常见问题

文档版本：20200708

法律声明

通用约定

格式	说明	样例
	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。	**禁止:** 重置操作将丢失用户配置数据。
	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。
	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。
	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。	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

法律声明..I
通用约定..I
1 RAM用户常见问题.. 1
2 RAM角色和STS Token常见问题.. 5
3 访问密钥常见问题.. 8
4 利用标签对RDS实例分组授权的常见问题.................................10

1 RAM用户常见问题

本文介绍了RAM用户常见问题，包括登录、费用和权限等问题。

RAM用户登录地址和登录方式是什么？

RAM用户登录地址如下： RAM用户登录地址。

> **说明：**
> 通过登录RAM控制台，在**概览**页可以快速查询登录RAM用户登录地址。当您使用此地址登录时，系统会为您自动填写默认域名，您只需补齐RAM用户名称即可。

RAM用户登录方式有以下几种：

- 方式一：`<$username>@<$AccountAlias>.onaliyun.com`。例如：`username@company-alias.onaliyun.com`。

  > **说明：**
  > RAM用户登录账号为UPN（User Principal Name）格式，即RAM控制台用户列表中所见的用户登录名称。<$username>为RAM用户名称，<$AccountAlias>.onaliyun.com为默认域名。

- 方式二：`<$username>@<$AccountAlias>`。例如：`username@company-alias`。

  > **说明：**
  > <$username>为RAM用户名称，<$AccountAlias>为账号别名。

- 方式三：如果创建了域别名，也可以使用域别名登录，格式为：`<$username>@<$DomainAlias>`。

  > **说明：**
  > <$username>为RAM用户名称，<$DomainAlias>为域别名。

什么是默认域名和域别名？

关于**默认域名**和**域别名**的概念，请参见#unique_4。

查看并管理**默认域名**和**域别名**的操作步骤如下：

1. 使用阿里云账号或具有RAM管理权限的RAM用户登录RAM控制台。
2. 在左侧导航栏的**人员管理**菜单下，单击**设置**。
3. 在**高级设置**页签下，可以查看并管理**默认域名**和**域别名**。

RAM用户采购云产品需要什么权限？

- 如需采购按量付费的云产品，一般只需给RAM用户分配该产品的创建实例或创建资源的权限即可。
- 如需采购包年包月的云产品，还需要额外授予支付订单的权限，即授予用户AliyunBSSOrderAccess的权限策略。
- 有些产品在购买时需要连带使用或创建多种资源，这种情况下需要RAM用户具备相应资源的读取或创建权限。

  以下以创建ECS实例为例，说明具体需要的权限。

  如下权限策略表示RAM用户可以从实例启动模板创建ECS实例：

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "ecs:DescribeLaunchTemplates",
        "ecs:CreateInstance",
        "ecs:RunInstances",
        "ecs:DescribeInstances",
        "ecs:DescribeImages",
        "ecs:DescribeSecurityGroups"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "vpc:DescribeVpcs",
        "vpc:DescribeVSwitches"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

  如果需要RAM用户在创建ECS实例过程中使用或创建其他资源，根据资源类型不同，还需要授予以下各类权限。

  说明：

  - 关于如何创建自定义策略，请参见#unique_5。
  - 关于如何为RAM用户授权，请参见#unique_6。

操作	权限策略
使用快照创建ECS实例	ecs:DescribeSnapshots

操作	权限策略
同时创建并使用新的VPC	- vpc:CreateVpc - vpc:CreateVSwitch
同时创建并使用新的安全组	- ecs:CreateSecurityGroup - ecs:AuthorizeSecurityGroup
指定实例角色	- ecs:DescribeInstanceRamRole - ram:ListRoles - ram:PassRole
使用Keypair	- ecs:CreateKeyPair - ecs:DescribeKeyPairs
在专有宿主机上创建ECS实例	ecs:AllocateDedicatedHosts

为什么RAM用户被授权后依然无访问权限？

- 请确认RAM用户的权限策略是否正确。
- 请检查RAM用户的自定义策略（个人权限策略、加入用户组的权限策略）是否对相关资源或操作设置了`"Effect": "Deny"`。

  例如：RAM用户拥有只读访问云服务器ECS的权限：`AliyunECSReadOnlyAccess`，但如果同时也拥有如下权限策略，根据RAM的Deny优先原则，该RAM用户不可以查看ECS资源。

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

为什么RAM用户没有权限仍然可以操作？

例如：RAM用户没有ECS的`AliyunECSFullAccess`或者`AliyunECSReadOnlyAccess`系统策略，也没有添加任何自定义策略，但可以查看实例列表。

- 请检查RAM用户所在的用户组权限策略中是否存在允许RAM用户操作的相应权限。
- 请确认当前已经被授权给RAM用户的其他权限策略中是否包含了相关权限。

  例如：云监控的系统权限策略为AliyunCloudMonitorFullAccess，此权限包括查看ECS实例列表的权限：`"ecs:DescribeInstances"`，查看RDS实例列表的权限：`"rds:DescribeDBInstances"`和

查看SLB实例列表的权限"slb:DescribeLoadBalancer"等。当AliyunCloudMonitorFullAccess被授权给RAM用户后，该RAM用户便有权限查看ECS、RDS和SLB等产品的实例信息。

怎样授权RAM用户单独管理续费？

目前续费管理没有统一的权限策略，需要根据具体产品自定义权限策略。一般需要授权给RAM用户购买该产品所需要的权限以及支付订单的权限。

例如：RAM用户进行ECS的续费管理所需权限，请参见RAM用户采购云产品需要什么权限给RAM用户授权，同时需要授予AliyunBSSOrderAccess权限策略。

RAM用户使用资源所产生的费用怎么计算？

- RAM用户使用资源所产生的费用由其所属的阿里云账号承担。
- RAM用户可以自动享有阿里云账号享有的折扣，无需特殊设置。
- 消费额度、信用额度和独立付款方式等财务相关属性均为阿里云账号内的全局设置，影响所有RAM用户。不支持为某个RAM用户单独设置。
- RAM用户可以被授权进行充值操作，充值后的金额归属于阿里云账号。
- RAM用户或RAM用户组不能作为独立的财务单元出账单。 若有阿里云账号内的分账需求，推荐您使用资源管理服务，详情请参见#unique_7。

2 RAM角色和STS Token常见问题

本文介绍了一些RAM角色和STS Token的常见问题，为您提供说明和指导。

RAM角色有几种类型？

根据RAM可信实体的不同，RAM支持以下三种类型的角色：

- **阿里云账号**
- **阿里云服务**
- **身份提供商**

三种类型的RAM角色分别可以被谁扮演？

- **阿里云账号**：允许RAM用户所扮演的角色。扮演角色的RAM用户可以属于自己的阿里云账号，也可以属于其他阿里云账号。此类角色主要用来解决跨账号访问和临时授权问题。
- **阿里云服务**：允许云服务所扮演的角色。特别的是，ECS实例RAM角色也属于这个类型，其可信实体为ECS服务，详情请参见#unique_9。此类角色主要用于授权云服务代理您进行资源操作。
- **身份提供商**：允许受信身份提供商下的用户所扮演的角色。此类角色主要用于实现与阿里云的SSO。

能否指定RAM用户具体可以扮演哪个RAM角色？

您也可以通过创建自定义策略指定RAM用户具体可以扮演的RAM角色。策略示例如下所示：

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Resource": "acs:ram:*:$accountId:role/$roleName"
    }
  ],
  "Version": "1"
}
```

说明：

- 上述自定义策略中的Resource为角色ARN，关于如何查看角色ARN，请参见如何查看RAM角色的ARN。其中，$accountId为阿里云账号ID，$roleName为RAM角色名称。
- 将上述自定义策略授权给RAM用户，便可以指定具体可以扮演的RAM角色。关于如何为RAM用户授权，请参见#unique_6。

如何查看RAM角色的ARN？

1. 登录RAM控制台。

2. 在**RAM角色管理**页签下，单击目标RAM角色名称。
3. 在**基本信息**区域下查看角色ARN。

为什么使用STS时会报错？

使用Java SDK生成STS Token时，报错信息如下所示：

```
Error message: You are not authorized to do this action. You should be authorized by RAM.
```

出现上述现象是因为进行授权的RAM用户没有相应的权限，因此使用时系统会报错。

请为RAM用户添加系统策略（AliyunSTSAssumeRoleAccess）或自定义策略，详情请参见能否指定RAM用户具体可以扮演哪个RAM角色。

STS服务调用次数是否有上限？

AssumeRole接口调用次数限制：一个主账号及主账号下的RAM用户、RAM角色共用100QPS。当请求量超过100时，超出部分会报错，报错信息如下：

```
Request was denied due to user flow control
```

STS Token的权限限制是什么？

STS Token的权限：指定角色的权限与调用#unique_10接口时所设置的Policy的交集。

> **说明：**
> 若在调用**AssumeRole**接口时不设置**Policy**参数，则返回的STS Token将拥有指定角色的所有权限。

STS Token的有效期是多久？

STS Token的有效期最小值为900秒，最大值为角色最大会话时间设置的值，默认值为3600秒。

> **说明：**
> - 您可以通过#unique_10接口的**DurationSeconds**参数来限制STS Token的有效期。
> - 您可以通过控制台或API设置角色最大会话时间，详情请参见#unique_11。

STS获取的多个Token是否同时有效？

STS Token在过期之前都是有效的，无论是否创建了新的STS Token。

STS Token发生泄漏时如何处理？

如果您通过扮演角色获取的安全令牌（STS Token）发生泄漏，您可以按如下步骤回收所有已经颁发的STS Token。

1. 使用阿里云账号登录RAM控制台。
2. 移除角色的所有权限策略。详情请参见#unique_12。
3. 删除角色。详情请参见#unique_13。

   删除角色后，所有通过扮演该角色获取的且未过期的STS Token都将立即失效。

如果您还需要使用该角色，您可以重新创建同名角色并授权相同的权限策略，使用新创建的角色继续完成您的任务。

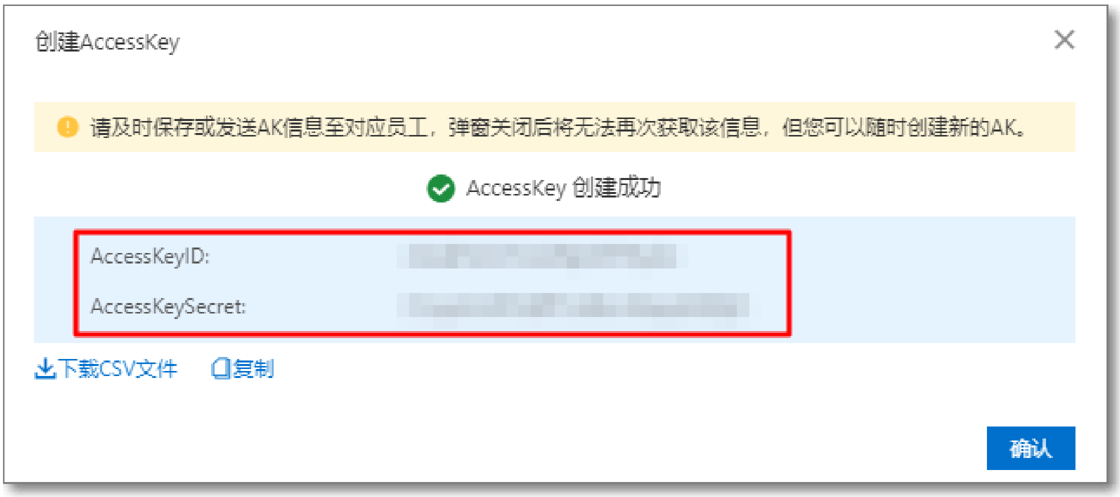
3 访问密钥常见问题

本文为您介绍访问密钥（AccessKey）相关的一些常见问题。

首次创建AccessKey的页面包含哪些信息？

首次创建AccessKey将会出现以下信息：

- AccessKey ID
- AccessKeySecret

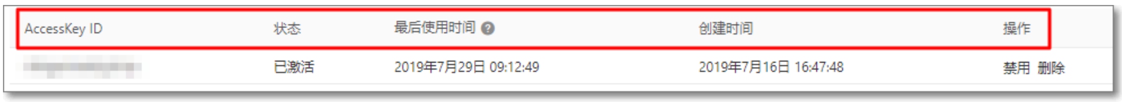


创建AccessKey后，可以查看哪些信息？

创建AccessKey后，您可以再次查询AccessKey的基本信息。详情请参见#unique_15。

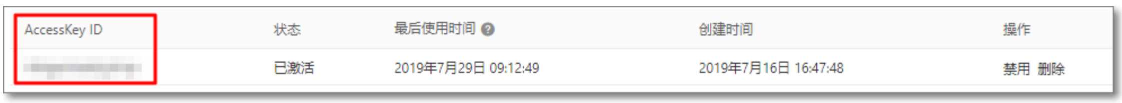
说明：

此时只能查看AccessKey ID、状态、最后使用时间和创建时间等基本信息。



创建AccessKey后，能否再次查看AccessKey ID？

创建AccessKey后，您仍可以再次查询AccessKey ID。

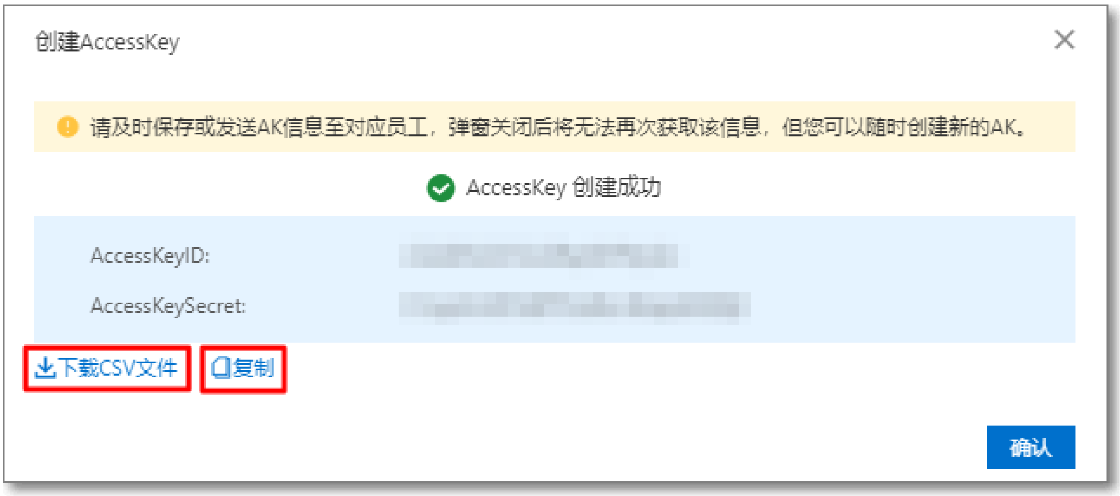


创建AccessKey后，能否再次查看AccessKeySecret？

AccessKeySecret只在首次创建时显示，不提供后续查询，请在创建AccessKey时及时保存。

如何查看AccessKeySecret？

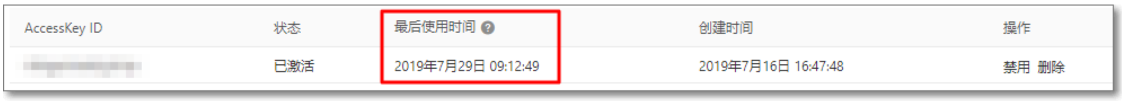
首次创建AccessKey时，可以手动将AccessKey信息保存到本地。



- 单击**下载CSV文件**可以将包含**Status**、**AccessKey ID**和**AccessKeySecret**的表格下载到本地。
- 单击**复制**可以将**AccessKey ID**和**AccessKeySecret**保存到本地。

如何判断AccessKey是否还在使用？

您可以通过查看AccessKey的最后使用时间来确认AccessKey的使用情况。



创建AccessKey后，能否修改AccessKey ID？

AccessKey ID不能修改，只能**禁用**、**激活**和**删除**。

AccessKey删除后能否恢复？

已经删除的AccessKey是无法恢复的，包括AccessKey ID和AccessKeySecret。

说明:

删除AccessKey需慎重，在使用中的AccessKey一旦删除，可能会造成您的应用系统故障。

4 利用标签对RDS实例分组授权的常见问题

本文介绍了利用标签对RDS实例分组授权后，如果RAM用户无法正常使用，如何进行错误排查。

问题现象

利用标签对RDS实例分组授权后，RAM用户登录**RDS控制台**，控制台首页提示无权操作。

解决方案

1. 请确保标签已被加到正确的实例上。
2. 请确保权限策略与实例上的标签键、标签值完全一样。

    说明：

    RDS的标签键值不可以使用大写字母，若输入大写字母在保存时会被自动转换成小写字母。
3. 请确保登录到**RDS控制台**的RAM用户已被授权了期望的权限策略。
4. 请确保控制台展示的当前地域是期望地域。
5. 请确保已选中相应标签值，此时系统才可以过滤出相应资源。
6. RAM用户登录**RDS控制台**后，控制台会提示无权限，请关掉错误提示。

    说明：

    具体提示为：您没有指定资源的操作权限，请先对资源进行授权操作。这是因为控制台默认展示所有资源，而当前RAM用户并没有查看所有资源的权限，所以会报错。