阿里云
访问控制

常见问题

文档版本：20190919

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
	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，恢复业务所需时间约10分钟。
	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。	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。	单击 确定。
`courier 字体`	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	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。	`swich` *{stand | slave}*

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

本文介绍了在使用RAM用户过程中的常见问题，包括登录、费用和权限等问题，为您提供说明和指导。

RAM用户登录地址在哪里?

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用户的登录有以下几种方式：

- 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。

关于RAM用户的登录地址和登录方式，请参见#unique_4。

什么是默认域名、账号别名和域别名?

关于默认域名、账号别名和域别名的概念，请参见#unique_5。

- 使用云账号或具有RAM管理权限的RAM用户登录RAM控制台。
- 在左侧导航栏的人员管理菜单下，单击设置。

- 在高级设置页签下，可以查看并管理默认域名、账号别名和域别名。

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类似权限即可。
- 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用户具有从控制台、使用API或从实例启动模板创建ECS实例的能力：

```
{
  "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_6。
  - 关于如何为RAM用户授权，请参见#unique_7。

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：

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

说明:

根据RAM的Deny优先原则，该RAM用户不可以查看ECS资源。

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FullAccess或者ReadOnly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云账号承担。
- RAM用户可以自动享有云账号享有的折扣，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云账号。
- RAM用户或RAM用户集合不能作为独立的财务单元出账单。 若有云账号内的分账需求，请提交工单由售后人员提供解决方案。

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云账号，也可以属于其他云账号。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，如何查看角色ARN请参见如何查看RAM角色的ARN? 其中，`$accountId`为云账号ID，`$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_10。

如何查看RAM角色的ARN?

您可以登录RAM控制台，在RAM角色管理页签下，单击目标RAM角色名称，在基本信息区域下查看角色ARN。

为什么使用STS时会报错?

STS使用Java SDK生成临时账号密码报错的信息如下所示：

```
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?

STS服务有流控限制：100QPS。超过流控会被限制。

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_11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的有效期为900秒~3600秒，默认值为3600秒。

> **说明:**
> 您可以在调用#unique_11接口时设置`DurationSeconds`参数来限制STS token的有效时间。

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。

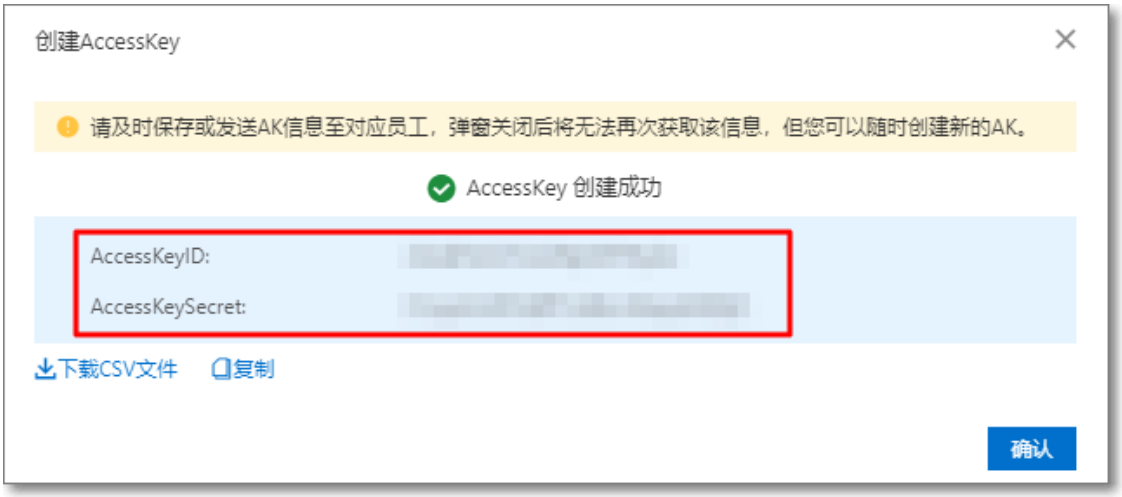
3 访问密钥常见问题

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：

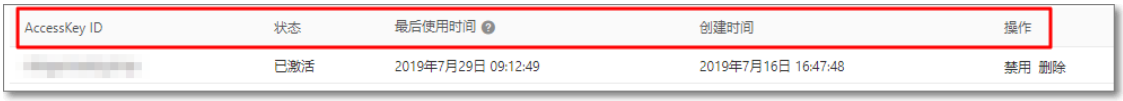
- AccessKey ID
- AccessKeySecret



创建AccessKey后，可以查看哪些信息？

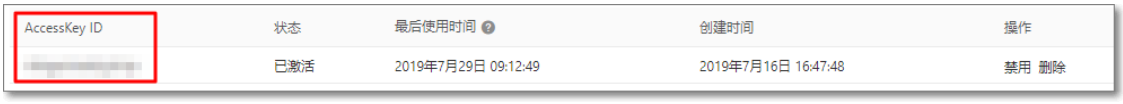
创建AccessKey后，您可以再次查询AccessKey的基本信息。详情请参见#unique_13。

> **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。

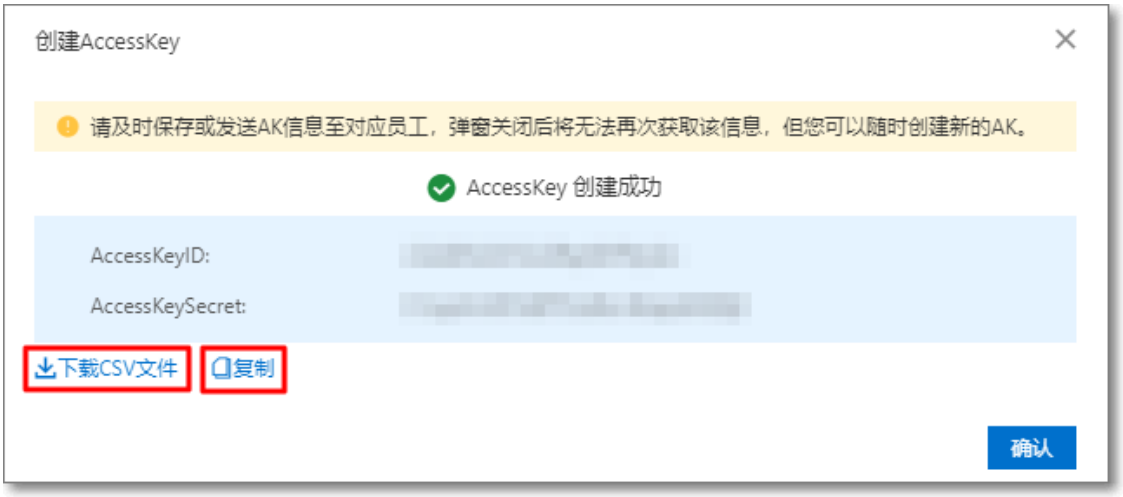


创建AccessKey后，能否再次查看AccessKeySecret？

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。

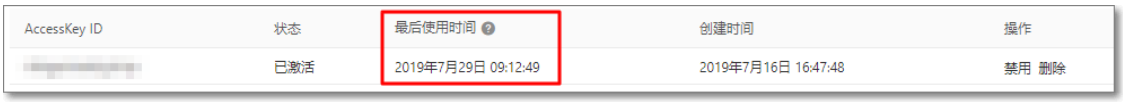


- 单击下载CSV文件可以将包含Status、AccessKey ID和AccessKeySecret的表格下载到本地。
- 单击复制可以将AccessKey ID和AccessKeySecret保存到本地。

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。

> **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。