ALIBABA CLOUD

# 阿里云

## 访问控制

## 常见问题

文档版本：20220422

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<br>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<br>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<br>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<br>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`<br>*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.RAM用户常见问题 05
2.RAM角色和STS Token常见问题 09
3.访问密钥常见问题 12
4.多因素认证（MFA）常见问题 13
5.存在RAM资源导致无法注销阿里云账号的问题 14

# 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： 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：使用默认域名登录。RAM用户的登录格式为 `<UserName>@<AccountAlias>.onaliyun.com` ，例如：username@company-alias.onaliyun.com。

  > **说明** RAM用户的登录账号为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。关于默认域名的更多信息，请参见基本概念和查看和修改默认域名。

- 方式二：使用账号别名登录。RAM用户的登录格式为 `<UserName>@<AccountAlias>` ，例如：username@company-alias。

  > **说明** `<UserName>` 为RAM用户名称， `<AccountAlias>` 为账号别名。关于账号别名的更多信息，请参见基本概念和查看和修改默认域名。

- 方式三：如果创建了域别名，也可以使用域别名登录。RAM用户的登录格式为 `<UserName>@<DomainAlias>` ，例如：username@example.com。

  > **说明** `<UserName>` 为RAM用户名称， `<DomainAlias>` 为域别名。关于域别名的更多信息，请参见基本概念和创建并验证域别名。

## 什么是默认域名和域别名？

阿里云为每个阿里云账号分配了一个默认域名，格式为： `<AccountAlias>.onaliyun.com` 。默认域名可作为RAM用户登录或单点登录（SSO）等场景下该阿里云账号的唯一标识符。关于如何设置默认域名，请参见查看和修改默认域名。

如果您持有公网上可以解析的域名，那么您可以使用该域名替代您的默认域名，该域名称为域别名。域别名就是指默认域名的别名。关于如何设置域别名，请参见创建并验证域别名。

> **说明** 域别名必须经过域名归属验证后才能使用。验证通过后，您可以使用域别名替代默认域名，用于所有需要使用默认域名的场景。

## 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用户分配该云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。

- 某些云产品在购买时需要使用或创建其他多种资源，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，还需要授予下表所示的对应权限。

| 操作 | 权限策略 |
| --- | --- |
| 使用快照创建ECS实例 | `ecs:DescribeSnapshots` |
| 同时创建并使用新的VPC | ○ `vpc:CreateVpc`<br>○ `vpc:CreateVSwitch` |
| 同时创建并使用新的安全组 | ○ `ecs:CreateSecurityGroup`<br>○ `ecs:AuthorizeSecurityGroup` |
| 指定实例角色 | ○ `ecs:DescribeInstanceRamRole`<br>○ `ram:ListRoles`<br>○ `ram:PassRole` |

| 操作 | 权限策略 |
| --- | --- |
| 使用Keypair | ○ `ecs:CreateKeyPair`<br>○ `ecs:DescribeKeyPairs` |
| 在专有宿主机上创建ECS实例 | `ecs:AllocateDedicatedHosts` |

> **说明**
> - 关于如何创建自定义策略，请参见创建自定义权限策略。
> - 关于如何为RAM用户授权，请参见为RAM用户授权。

## 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（用户权限策略、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用户无法查看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等云产品的实例信息。

## 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，需要根据具体云产品自定义权限策略。一般需要授予RAM用户购买该云产品所需要的权限以及支付订单的权限。

例如：RAM用户进行管理ECS续费的权限，请参见RAM用户采购云产品需要什么权限为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。更多信息，请参见资源组分账和标签分账概述。

## 为什么RAM授权后，没有立刻在云产品中生效？

RAM采用多地域（Region）、多可用区（AZ）部署的高可用架构，数据在不同的Region间复制，并遵从最终一致性。当您在RAM中进行授权后，RAM会将授权信息同步分发到全球各个Region以及AZ中，为各个云产品提供鉴权能力。当某个AZ或者Region发生宕机后，RAM高可用容灾机制会切换到其它可用的AZ。

授权信息分发机制需要一定的时间来确保授权生效。当您进行授权变更后，需要等待一定的时间，授权才能在云产品中生效。

RAM会保证授权数据的最终一致性。

# 2.RAM角色和STS Token常见问题

本文介绍了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。此类角色主要用于解决跨云服务授权访问问题。例如：ECS实例RAM角色就是这个类型，其可信实体为ECS服务。更多信息，请参见使用实例RAM角色访问其他云产品。
- **身份提供商**：允许可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:*:<account-id>:role/<role-name>"
        }
    ],
    "Version": "1"
}
```

> **说明**
>
> - 上述自定义策略中的 `Resource` 为角色ARN，其中，`<account-id>` 为阿里云账号ID，`<role-name>` 为RAM角色名称。关于如何查看角色ARN，请参见如何查看RAM角色的ARN。
> - 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，请参见为RAM用户授权。

## 如何查看RAM角色的ARN？

1. 登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 角色**。
3. 单击目标RAM角色名称。
4. 在**基本信息**区域，查看RAM角色ARN。

## 为什么使用STS时会报错？

如果一个RAM用户使用API、CLI或SDK调用AssumeRole获取STS Token时，出现如下报错信息：

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

问题原因和解决方法如下：

- 该RAM用户缺少允许STS扮演角色的权限策略：请为该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。
- RAM角色的信任策略不包含您正在使用的RAM用户，即RAM角色不允许该RAM用户扮演：请为RAM角色添加允许该RAM用户扮演的信任策略，详情请参见修改RAM角色的信任策略。

## STS服务调用次数是否有上限？

AssumeRole接口每分钟最多调用6000次，且一个阿里云账号及该账号下的RAM用户、RAM角色共用这6000次。

当请求量超过限制时，会返回以下报错信息：

- 错误信息

| 错误码 | 错误信息 |
| --- | --- |
| Throttling.Api | Request was denied due to api flow control. |
| Throttling.User | Request was denied due to user flow control. |
| Throttling | Request was denied due to flow control. |

- `302` 状态码

当出现以上报错信息时，请您减少并发调用次数。如果您的业务场景确实需要更高的并发调用次数，您可以提交工单申请配额。

## 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AssumeRole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AssumeRole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。更多信息，请参见设置角色最大会话时间。

## 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。

## STS Token发生泄露时如何处理？

如果您通过扮演RAM角色获取的安全令牌（STS Token）发生泄露，您可以按以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RAM角色的所有权限策略。

   具体操作，请参见为RAM角色移除权限。
3. 删除RAM角色。

   具体操作，请参见删除RAM角色。

   删除RAM角色后，所有通过扮演该RAM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。

## AccessKey包括哪些信息？

AccessKey包括AccessKey ID和AccessKey Secret：

- AccessKey ID：用于标识用户。
- AccessKey Secret：用于验证用户的密钥。AccessKey Secret必须保密。

## 创建AccessKey后，可以查看哪些信息？

创建AccessKey后，您可以再次查看AccessKey ID、状态、最后使用时间和创建时间等基本信息。更多信息，请参见查看访问密钥信息。

## 创建AccessKey后，能否再次查看AccessKey ID？

可以。

## 创建AccessKey后，能否再次查看AccessKey Secret？

RAM用户的AccessKey Secret只在创建时显示，创建后将不能再次查看。

## 如何判断AccessKey是否还在使用？

您可以通过控制台或API查看AccessKey的最后使用时间，以此判断AccessKey是否还在使用。具体如下：

- AccessKey管理页面

  阿里云账号（主账号）登录时，查看该阿里云账号AccessKey的最后使用时间。RAM用户登录时，查看该RAM用户AccessKey的最后使用时间。

- RAM控制台

  阿里云账号（主账号）或具有管理员权限的RAM用户登录时，查看所有RAM用户AccessKey的最后使用时间。具体操作，请参见查看访问密钥信息。

- GetAccessKeyLastUsed

  您可以调用该API查看阿里云账号（主账号）或RAM用户AccessKey的最后使用时间。

## 创建AccessKey后，能否修改AccessKey ID？

AccessKey ID不能修改。您只能禁用、启用或删除AccessKey。

## 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AccessKey Secret。

> **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.多因素认证（MFA）常见问题

本文为您介绍多因素认证（MFA）相关的一些常见问题。

## 在绑定MFA页面，输入两组安全码后，提示安全码错误，怎么办？

- MFA是基于时间的，您需要检查并确保移动端的时间不存在延迟或超前。
- 移动端MFA设备上的安全码会每隔30秒更新一次，您需要确保输入的是前后连续的两组安全码。
- 当前绑定页面打开时间过长，二维码（密钥）已过期，您需要刷新页面重新扫码。
- 如果多次打开MFA绑定页面并扫码，在移动端MFA设备上会显示相同的用户名，但实际安全码是不同的，这可能会导致验证失败。建议您在绑定前先检查移动端MFA设备，如果已存在相同用户名，则先删除再扫码，以避免混淆。
- 当您尝试以上方法后，仍然存在问题时，您可以提交工单，同时提供绑定出错的页面截图、绑定时移动端的时间截图、待绑定的账号和操作时间点等信息。

## 登录验证MFA时，提示验证失败，怎么办？

- MFA是基于时间的，您需要检查并确保移动端的时间不存在延迟或超前。
- 检查并确保当前输入的MFA安全码是当前账号的，且是最新的、未被使用过的。
- 如果当前的移动端MFA设备已与当前账号解绑，解绑后当前账号又重新绑定了其他移动端MFA设备，此时您需要确保从最新绑定的移动端MFA设备上获取MFA安全码。
- 尝试重新绑定MFA设备。分为以下两种情况：
  - 为阿里云账号重新绑定MFA设备。
    a. 解绑MFA设备。

       具体操作，请参见为阿里云账号停用多因素认证。

    b. 重新绑定MFA设备。

       具体操作，请参见为阿里云账号启用多因素认证。
  - 为RAM用户重新绑定MFA设备。

    如果当前RAM用户没有权限绑定MFA设备，则需要联系您的RAM管理员操作。

    a. 解绑MFA设备。

       具体操作，请参见为RAM用户停用多因素认证。

    b. 重新绑定MFA设备。

       具体操作，请参见为RAM用户启用多因素认证。
- 当您尝试以上方法后，仍然存在问题时，您可以提交工单，同时提供验证时移动端的时间截图、验证的账号和操作时间点等信息。

# 5.存在RAM资源导致无法注销阿里云账号的问题

注销阿里云账号前，需要删除该阿里云账号下的全部RAM资源。否则，会注销失败。

- 对于已经通过实名认证的阿里云账号，您可以通过RAM控制台或API，按以下操作删除账号下的自定义资源。
  - 删除全部RAM用户。

    具体操作，请参见删除RAM用户。
  - 删除全部RAM用户组。

    具体操作，请参见删除用户组。
  - 删除全部RAM角色。

    具体操作，请参见删除RAM角色。
  - 删除全部自定义策略。

    具体操作，请参见删除自定义权限策略。
  - 删除全部OAuth应用，包括自建的企业应用和外部的第三方应用。

    具体操作，请参见删除应用。
  - 删除全部身份提供商。

    具体操作，请参见删除SAML身份提供商。
  - 删除全部虚拟MFA设备。

    正常情况下，删除RAM用户时会同步删除该RAM用户绑定的虚拟MFA设备。但存在以下两种例外情况：
    - 通过RAM控制台为RAM用户启用虚拟MFA时，当进入了绑定虚拟MFA设备的页面（包括RAM管理员为RAM用户绑定和RAM用户自主绑定），但一直未完成绑定的情况下，会产生额外的虚拟MFA设备。
    - 通过CreateVirtualMFADevice API创建了虚拟MFA设备，但未绑定RAM用户。

    对于以上的例外情况，您可以先调用ListVirtualMFADevices API查询阿里云账号下存在的所有虚拟MFA设备，然后调用DeleteVirtualMFADevice API删除这些虚拟MFA设备。
  - 删除自定义的默认域名名称，将其修改为默认的账号ID。

    a. 查看账号ID。

    当您登录阿里云控制台后，您可以将鼠标悬停在右上角头像的位置，然后单击**安全设置**，查看账号ID。

    b. 修改默认域名名称为账号ID。

    具体操作，请参见查看和修改默认域名。
- 对于未通过实名认证的阿里云账号，原则上不能使用RAM。但因为一些跨服务授权场景可能导致该阿里云账号下实际存在RAM服务角色，您可以通过API或CLI删除该服务角色。

  下面以在 Cloud Shell 中的操作为例。

  i. 执行以下命令，查询账号下的RAM服务角色。

```
aliyun ram ListRoles
```

ii. 检查待删除的RAM服务角色是否为服务关联角色。

以“AliyunServiceRoleFor”开头的角色为服务关联角色，其余情况均为普通服务角色。

iii. 删除RAM服务角色。

- 对于服务关联角色，请按以下步骤进行删除。
  a. 执行以下命令，删除服务关联角色。

```
aliyun resourcemanager DeleteServiceLinkedRole --secure --force --RoleName $role_name
```

将 `$role_name` 替换为实际的角色名称。

  b. 执行以下命令，查看删除是否成功。

```
aliyun resourcemanager GetServiceLinkedRoleDeletionStatus --DeletionTaskId $task_id
```

将 `$task_id` 替换为上一步返回的 `DeletionTaskId` 。如果返回的 `Status` 为 `SUCCEEDED` ，表示删除成功。

- 对于普通服务角色，请执行以下命令进行删除。

```
aliyun ram DeleteRole --secure --force --RoleName $role_name --CascadingDelete true
```

将 `$role_name` 替换为实际的角色名称。

iv. 再次执行以下命令，查询账号下的全部RAM服务角色是否已被成功删除。

```
aliyun ram ListRoles
```