ALIBABA CLOUD

Alibaba Cloud

访问控制

用户管理

文档版本：20220512

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.RAM用户概览

本文为您介绍RAM（Resource Access Management）用户的基本概念、使用流程、最佳实践和使用限制。

什么是RAM用户

RAM用户是RAM的一种实体身份类型，有确定的身份ID和身份凭证，它通常与某个确定的人或应用程序一一对应。RAM用户具备以下特点：

- RAM用户由阿里云账号（主账号）或具有管理员权限的其他RAM用户、RAM角色创建，创建成功后，归属于该阿里云账号，它不是独立的阿里云账号。
- RAM用户不拥有资源，不能独立计量计费，由所属的阿里云账号统一付费。
- RAM用户必须在获得授权后，才能登录控制台或使用API访问阿里云账号下的资源。
- RAM用户拥有独立的登录密码或访问密钥。
- 一个阿里云账号下可以创建多个RAM用户，对应企业内的员工、系统或应用程序。

您可以创建RAM用户并为其授权，实现不同RAM用户拥有不同资源访问权限的目的。当您的企业存在多用户协同访问资源的场景时，使用RAM可以按需为用户分配最小权限，避免多用户共享阿里云账号密码或访问密钥，从而降低企业的安全风险。

使用流程

1. 使用阿里云账号（主账号）或具有管理员权限的RAM用户、RAM角色登录RAM控制台。
2. 创建RAM用户。

   具体操作，请参见创建RAM用户。
3. 设置登录参数。

   虽然您可以为RAM用户同时设置控制台登录密码和API调用的访问密钥AK（AccessKey），但出于安全的考虑，建议您针对不同用途的RAM用户仅设置一种登录方式。例如：如果RAM用户代表的是应用程序，则需要通过API访问资源，您只需给它创建访问密钥。如果RAM用户代表的是员工，则需要通过控制台访问资源，您只需给它设置登录密码。具体设置方法如下：

   - 控制台登录

     您需要启用RAM用户控制台登录、设置RAM用户密码强度、设置或修改登录密码、按需启用多因素认证（MFA）。具体操作，请参见管理RAM用户登录设置、设置RAM用户密码强度、修改RAM用户登录密码和为RAM用户启用多因素认证。

     > **说明** 如果您启用了用户SSO，则可以不开启控制台登录，用户也能通过SSO方式登录到阿里云控制台。更多信息，请参见用户SSO概览。

   - API调用

     您需要为RAM用户创建访问密钥。具体操作，请参见为RAM用户创建访问密钥。
4. 为RAM用户授权。

   为不同的RAM用户授予不同的资源访问权限。具体操作，请参见为RAM用户授权。
5. 使用RAM用户登录控制台或使用访问密钥调用API。

   更多信息，请参见RAM用户登录阿里云控制台和API概览。

最佳实践

当企业拥有多种云资源时，使用RAM的身份管理与权限管理功能，实现用户分权及资源统一管理。更多信息，请参见用户管理与分权。

使用限制

关于RAM用户的使用限制，请参见使用限制。

2.基本操作

2.1. 创建RAM用户

RAM用户是RAM中的一种身份，对应某一个操作实体（运维操作人员或应用程序）。通过创建新的RAM用户并授权，RAM用户便可以访问相关资源。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击**创建用户**。
4. 在**创建用户**页面的**用户账号信息**区域，输入**登录名称**和**显示名称**。

   > **说明** 单击**添加用户**，可一次性创建多个RAM用户。

5. 在**访问方式**区域，选择访问方式。
   - **控制台访问**：设置控制台登录密码、重置密码策略和多因素认证策略。

     > **说明** 自定义登录密码时，密码必须满足密码复杂度规则。关于如何设置密码复杂度规则，请参见设置RAM用户密码强度。

   - **OpenAPI调用访问**：自动为RAM用户生成访问密钥（AccessKey），支持通过API或其他开发工具访问阿里云。

     > **说明** 为了保障账号安全，建议仅为RAM用户选择一种登录方式，避免RAM用户离开组织后仍可以通过访问密钥访问阿里云资源。

6. 单击**确定**。

后续步骤

- RAM用户创建成功后，可以使用RAM用户登录控制台。具体操作，请参见RAM用户登录阿里云控制台。
- 可以为RAM用户添加权限策略，使RAM用户具有资源的访问能力。具体操作，请参见为RAM用户授权。
- 可以将RAM用户添加到用户组，对RAM用户进行分类并授权。具体操作，请参见为用户组添加RAM用户。

相关文档

- CreateUser

2.2. 删除RAM用户

当不再需要某个RAM用户时，可以删除该RAM用户。删除RAM用户会删除对应的访问密钥、撤销RAM用户拥有的权限、解绑多因素认证设备和解绑钉钉账号。

前提条件

删除RAM用户前，请确保没有系统或应用程序正在以此用户身份运行，否则可能会导致业务故障。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击目标RAM用户**操作**列的**删除**。
4. 在**删除用户**对话框，仔细阅读删除影响，然后单击**我已知晓风险，确认删除**。

相关文档

- DeleteUser

2.3. 查看RAM用户基本信息

本文为您介绍如何查看RAM用户基本信息，包括登录名称、显示名称和UID等信息。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击目标RAM用户名称。
4. 在**用户基本信息**区域，查看**登录名称**、**显示名称**和**UID**等信息。

相关文档

- GetUser

2.4. 修改RAM用户基本信息

本文为您介绍如何修改RAM用户基本信息，包括用户名和显示名称等信息。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击目标RAM用户名称。
4. 在**用户基本信息**区域，单击**编辑基本信息**。
5. 在**编辑基本信息**面板，修改RAM用户基本信息，然后单击**确定**。

相关文档

- UpdateUser

3.登录管理

3.1. 管理RAM用户登录设置

本文为您介绍如何为RAM用户启用控制台登录、查看、修改或清空控制台登录设置。

启用控制台登录

您可以为RAM用户启用控制台登录，并设置登录密码等参数。

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户登录名称/显示名称**列，单击目标RAM用户名称。
4. 在**认证管理**页签下的**控制台登录管理**区域，单击**启用控制台登录**。
5. 在**修改登录设置**面板，设置控制台登录参数。
   - **控制台访问**：单击**开启**，启用RAM用户的控制台登录。
   - **设置密码**：按需设置RAM用户的控制台登录密码。

     > **说明** 设置完成后，请您妥善保管新密码。

   - **需要重置密码**：设置是否要求RAM用户下次登录时重置密码。
   - **MFA多因素认证**：设置是否要求RAM用户开启多因素认证。

     > **说明** 如果阿里云账号要求RAM用户开启多因素认证，RAM用户在登录时会直接进入多因素认证绑定流程。

6. 在**修改登录设置**对话框，单击**确定**。

查看控制台登录设置

启用控制台登录后，您可以查看控制台登录设置。

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户登录名称/显示名称**列，单击目标RAM用户名称。
4. 在**认证管理**页签下的**控制台登录管理**区域，查看控制台登录设置。
   - **控制台访问**：是否已开启控制台访问。
   - **上次登录控制台时间**：上一次登录控制台的时间。
   - **必须开启多因素认证**：是否登录时必须开启多因素认证（MFA）。
   - **下次登录重置密码**：是否下一次登录时必须重置密码。
   - **登录方式**：支持用户名密码登录方式。您可以将鼠标悬浮在图标上，单击链接直接登录或复制对应的登录地址。

修改控制台登录设置

为RAM用户启用控制台登录后，您可以按需修改控制台登录设置，例如：禁用控制台登录、修改登录密码等。

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户登录名称/显示名称**列，单击目标RAM用户名称。
4. 在**认证管理**页签下的**控制台登录管理**区域，单击**修改登录设置**。
5. 在**修改登录设置**面板，修改控制台登录参数。
   - **控制台访问**：单击**禁用**，禁用RAM用户的控制台登录。

     > **说明** 禁用后，您仍然可以修改RAM用户的登录设置，但不会生效。当再次单击**开启**时，登录设置才会生效。

   - **设置密码**：按需设置RAM用户的控制台登录密码。

     > **说明** 设置完成后，请您妥善保管新密码。

   - **需要重置密码**：设置是否要求RAM用户下次登录时重置密码。
   - **MFA多因素认证**：设置是否要求RAM用户开启多因素认证。

     > **说明** 如果阿里云账号要求RAM用户开启多因素认证，RAM用户在登录时会直接进入多因素认证绑定流程。

6. 在**修改登录设置**对话框，单击**确定**。

清空控制台登录设置

您可以一键清空RAM用户的控制台登录设置，同时禁用RAM用户的控制台登录。

> **注意** 登录设置如果被清空，将无法自动恢复，请您慎重操作。

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户登录名称/显示名称**列，单击目标RAM用户名称。
4. 在**认证管理**页签下的**控制台登录管理**区域，单击**清空登录设置**。
5. 在**清空登录设置**对话框，单击**确定**。

3.2. 设置RAM用户密码强度

为了保护账号安全，您可以编辑密码规则，包括密码长度、密码有效期和历史密码检查策略等。

背景信息

阿里云不会保存您的密码明文，只会保存SHA256哈希（Hash）且加盐（Salt）后的值，以确保密码不会被泄露给任何人。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 设置**。
3. 在**安全设置**页签下，单击**编辑密码规则**，配置相关参数。
   - **密码长度**：密码长度范围为8~32位。

     > **说明** 为了保护账号安全，建议至少设置8位以上的密码长度。

   - **密码中必须包含元素**：请根据需要勾选大写字母、小写字母、数字和符号。

     > **说明** 为了提高账号安全性，上述元素中，建议至少勾选2项以上。

   - **最少包含的不同字符数**：取值范围为0~8，默认值为0，表示不限制密码中的不同字符数量。
   - **密码中是否允许包含用户名**：根据需要选择**允许**或**不允许**。
     - **允许**：密码中可以包含用户名。
     - **不允许**：密码中不能包含用户名。
   - **密码有效期**：单位为天，取值范围为0~1095天，默认值为0，表示永不过期。

     > **说明** 重置密码将重置密码过期时间。

   - **密码过期后**：表示密码过期后是否仍可以登录，根据需要勾选**不可登录**或**不限制登录**。
     - **不可登录**：表示密码过期后，不能登录控制台。需要通过阿里云账号或具有管理员权限的RAM用户重置该RAM用户的密码后，才能正常登录。
     - **不限制登录**：表示密码过期后，RAM用户可以自行更改密码，然后正常登录。
   - **历史密码检查策略**：表示禁止使用前*N*次密码，取值范围为0~24。默认值为0，表示不启用历史密码检查策略。
   - **密码重试约束**：设置密码重试的次数，连续输入错误密码达到设定次数后，账号将被锁定一小时。取值范围为0~32。默认值为0，表示不启用密码重试约束。

     > **说明** 重置密码可清除尝试登录次数。

4. 单击**确定**。

执行结果

设置成功后，此密码规则适用于所有RAM用户。

相关文档

- SetPasswordPolicy

3.3. 修改RAM用户登录密码

阿里云账号可以定期为RAM用户修改登录密码以提高账号安全性。

操作步骤

1. 使用阿里云账号登录RAM控制台。

2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击目标RAM用户名称。
4. 在**认证管理**页签，单击**修改登录设置**。
5. 在**修改登录设置**面板的**设置密码**区域，修改登录密码。
   - 选择**保留当前密码**，表示不修改密码。
   - 选择**自动生成密码**，然后单击**确定**，会自动生成登录密码，请记录并妥善保管新密码。
   - 选择**自定义密码**，然后输入新的密码，最后单击**确定**。

   > **说明** 输入的新密码必须符合密码强度要求，更多信息，请参见设置RAM用户密码强度。

6. 单击**关闭**。

   > **说明** 如果阿里云账号允许RAM用户自主管理密码，RAM用户也可以登录控制台自行修改密码。

相关文档

- ChangePassword

3.4. 为RAM用户启用多因素认证

本文分别为您介绍如何为RAM用户启用虚拟MFA、U2F安全密钥这两种多因素认证设备的操作。启用多因素认证后，可以为您的账号提供更高的安全保护。

> **说明** 一个RAM用户只能启用一种MFA设备，不能同时启用虚拟MFA和U2F安全密钥。

启用虚拟MFA

前提条件

操作前，请在移动设备端下载并安装Google Authenticator应用。下载方式如下：

- iOS：在App Store中搜索Google Authenticator。
- Android：在应用市场中搜索Google Authenticator。

> **说明** Android系统的Google Authenticator还依赖外部二维码扫描组件，所以您还需要在应用市场中搜索并安装条行码扫描器。

启用方式

请根据实际情况，选择合适的方式启用虚拟MFA：

- 使用阿里云账号或RAM管理员在RAM控制台启用虚拟MFA。如下操作将以此为例进行介绍。
- 如果阿里云账号要求RAM用户启用多因素认证，那么RAM用户登录时会直接进入多因素认证绑定流程，请在**启用MFA设备**页面选择**虚拟MFA设备**，然后直接从第步开始操作。
- 如果阿里云账号允许RAM用户自主管理多因素认证设备，RAM用户也可以登录控制台启用虚拟MFA。将鼠标悬停在右上角头像的位置，先单击**安全信息管理**，然后在**控制台登录**页面的**虚拟MFA**页签下，单击**启用虚拟MFA**，最后直接从第步开始操作。

操作步骤

1. 阿里云账号或RAM管理员登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户登录名称/显示名称**列，单击目标RAM用户名称。
4. 单击**认证管理**页签，然后单击**虚拟MFA**页签。
5. 单击**启用虚拟MFA**。
6. 在移动设备端，添加虚拟MFA设备。

   > **说明** 如下以iOS系统上的Google Authenticator应用为例。

   i. 登录Google Authenticator应用。

   ii. 单击**开始使用**，选择合适的方式添加虚拟MFA设备。

   - 扫码添加（推荐）：单击**扫描二维码**，然后扫描从RAM控制台**扫码获取**页签下的二维码。
   - 手动添加：先单击**输入设置密钥**，然后填写从RAM控制台**手输信息获取**页签下的账号和密钥，最后单击**添加**。

7. 在RAM控制台，输入移动设备端显示的两组连续的动态验证码，然后单击**确定绑定**。

   > **说明** 您还可以设置是否允许RAM用户**保存MFA验证状态7天**，如果为允许，则RAM用户使用MFA登录时，可以选中**记住这台机器，7天内无需再次验证**，就可以在7天内免MFA验证。关于具体的设置方法，请参见设置RAM用户安全策略。

启用U2F安全密钥

启用方式

请根据实际情况，选择合适的方式启用U2F安全密钥：

- 使用阿里云账号或RAM管理员在RAM控制台启用U2F安全密钥。如下操作将以此为例进行介绍。
- 如果阿里云账号要求RAM用户开启多因素认证，那么RAM用户登录时会直接进入多因素认证绑定流程。请在**启用MFA设备**页面选择**U2F安全密钥**，然后直接从第步开始操作。
- 如果阿里云账号允许RAM用户自主管理多因素认证设备，RAM用户也可以登录控制台启用U2F安全密钥。将鼠标悬停在右上角头像的位置，先单击**安全信息管理**，然后在**控制台登录**页面的**U2F安全密钥**页签下，单击**启用U2F安全密钥**，最后直接从第步开始操作。

操作步骤

1. 阿里云账号或RAM管理员登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户登录名称/显示名称**列，单击目标RAM用户名称。
4. 单击**认证管理**页签，然后单击**U2F安全密钥**页签。
5. 单击**启用U2F安全密钥**。
6. 在**绑定U2F安全密钥**页面，绑定U2F安全密钥。

   > **说明** 进行以下操作前，您需要了解U2F的使用限制，请参见使用限制。

i. 将U2F安全密钥插入到计算机的USB端口。
ii. 轻按U2F安全密钥上的按钮。
iii. 在提示获取安全密钥的弹框中，单击**确定**。
iv. 当页面显示获取U2F密钥成功时，单击**确定绑定**。

后续步骤

绑定多因素认证设备后，RAM用户再次登录阿里云时，系统将要求输入两层安全要素：

1. 第一层安全要素：输入用户名和密码。
2. 第二层安全要素：输入虚拟MFA设备生成的验证码，或通过U2F安全密钥认证。

> 说明
> - 如果您要更换新的多因素认证设备，请先前往RAM控制台停用多因素认证，再绑定新的多因素认证设备。具体操作，请参见停用多因素认证。
> - 如果您在未停用多因素认证的状态下卸载了虚拟多因素认证设备或您的U2F安全密钥丢失，您将无法正常登录阿里云。此时您需要联系您的阿里云账号（主账号）或RAM管理员，前往RAM控制台帮您停用多因素认证，之后才能重新绑定。具体操作，请参见停用多因素认证。

相关文档

- BindMFADevice
- 多因素认证（MFA）常见问题

3.5. 为RAM用户创建访问密钥

访问密钥（AccessKey）是RAM用户的长期凭证。如果为RAM用户创建了访问密钥，RAM用户可以通过API或其他开发工具访问阿里云资源。

背景信息

为保证账号安全，强烈建议您给RAM用户创建访问密钥，不要给阿里云账号（主账号）创建访问密钥。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击目标RAM用户名称。
4. 在**用户AccessKey**区域，单击**创建AccessKey**。
5. 在**创建AccessKey**对话框，查看AccessKey ID和AccessKey Secret。
   您可以单击**下载CSV文件**，下载AccessKey信息。或者单击**复制**，复制AccessKey信息。
6. 单击**关闭**。

> 说明
> - AccessKey Secret只在创建时显示，不支持查询，请妥善保管。
> - 若AccessKey泄露或丢失，则需要创建新的AccessKey，最多可以创建2个AccessKey。

相关文档

- CreateAccessKey

3.6. RAM用户登录阿里云控制台

本文为您介绍RAM用户如何登录阿里云控制台，包括登录入口和操作步骤。

登录入口

RAM用户登录阿里云控制台的入口有以下几种：

- 通用登录地址
  - 在阿里云账号登录页面，单击**RAM用户登录**。

  - 直接访问阿里云控制台页面。
- 阿里云账号专属登录地址

  阿里云账号登录RAM控制台，在**概览**页的**账号管理**区域，获取RAM用户登录地址（例如：`https://signin.alibabacloud.com/example.onaliyun.com/login.htm`）。RAM用户使用该地址登录阿里云控制台。
- RAM用户专属登录地址

  在登录地址中使用`username`参数指定RAM用户名，登录过程中免输用户名，直接单击**下一步**输入密码即可。`username`使用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。例如：一个名为Alice@example.onaliyun.com的RAM用户可以使用`https://signin.alibabacloud.com/login.htm?username=Alice@example.onaliyun.com`登录阿里云控制台。

使用RAM用户名密码登录

以下操作以RAM用户使用通用登录地址登录阿里云控制台为例。

1. RAM用户登录阿里云控制台。
2. 在**RAM用户登录**页面，输入RAM用户名，单击**下一步**。
   - 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** `<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。

3. 输入RAM用户的登录密码，然后单击**登录**。
4. （可选）如果您开启了多因素认证（MFA），则需要输入虚拟MFA设备生成的验证码，或通过U2F安全密钥认证。

   更多信息，请参见多因素认证（MFA）和为RAM用户启用多因素认证。

4.授权管理

4.1. 为RAM用户授权

为RAM用户授权后，RAM用户可以访问相应的阿里云资源。本文为您介绍为RAM用户授权的几种方式。

方式一：在用户页面为RAM用户授权

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击目标RAM用户**操作**列的**添加权限**。
4. 在**添加权限**面板，为RAM用户添加权限。
   i. 选择授权应用范围。
      - **整个云账号**：权限在当前阿里云账号内生效。
      - **指定资源组**：权限在指定的资源组内生效。

      > **说明** 指定资源组授权生效的前提是该云服务已支持资源组。更多信息，请参见支持资源组的云服务。

   ii. 输入授权主体。

   授权主体即需要授权的RAM用户，系统会自动填入当前的RAM用户，您也可以添加其他RAM用户。

   iii. 选择权限策略。

   > **说明** 每次最多绑定5条策略，如需绑定更多策略，请分次操作。

5. 单击**确定**。
6. 单击**完成**。

方式二：在授权页面为RAM用户授权

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 > 授权**。
3. 在**授权**页面，单击**新增授权**。
4. 在**新增授权**页面，为RAM用户添加权限。
   i. 选择授权应用范围。
      - **整个云账号**：权限在当前阿里云账号内生效。
      - **指定资源组**：权限在指定的资源组内生效。

      > **说明** 指定资源组授权生效的前提是该云服务已支持资源组。更多信息，请参见支持资源组的云服务。

   ii. 输入授权主体。

   授权主体即需要授权的RAM用户。

iii. 选择权限策略。

> **说明** 每次最多绑定5条策略，如需绑定更多策略，请分次操作。

5. 单击**确定**。
6. 单击**完成**。

相关文档

- AttachPolicyToUser

4.2. 查看RAM用户的权限

本文为您介绍如何查看RAM用户的权限，包括查看RAM用户的个人权限和查看RAM用户继承用户组的权限。

查看RAM用户的个人权限

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击目标RAM用户名称。
4. 单击**权限管理**页签。
5. 在**个人权限**页签，查看RAM用户的个人权限。

查看RAM用户继承用户组的权限

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击目标RAM用户名称。
4. 单击**权限管理**页签。
5. 在**继承用户组的权限**页签，查看RAM用户继承用户组的权限。

4.3. 为RAM用户移除权限

当RAM用户不再需要某些权限或离开组织时，可以将这些权限移除。本文为您介绍移除RAM用户权限的几种方式。

方式一：在用户页面移除RAM用户的权限

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击目标RAM用户名称。
4. 单击**权限管理**页签，然后单击目标权限策略**操作**列的**移除权限**。
5. 单击**确定**。

方式二：在授权页面移除RAM用户的权限

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 > 授权**。

3. 在**授权**页面，单击目标RAM用户**操作**列的**移除授权**。
4. 单击**确定**。

相关文档

- DetachPolicyFromUser