阿里云
访问控制

快速入门

文档版本：20180930

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。
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。	`swich` *`{stand | slave}`*

目录

1 概述

本文介绍访问控制（RAM）的一般操作步骤：

1. 设置 *MFA*#可选#
2. *RAM* 初始设置
3. 创建 *RAM* 用户
4. 创建 *RAM* 用户组#可选#
5. 创建自定义授权策略#可选#
6. 为 *RAM* 用户授权
7. *RAM* 用户登录控制台

2 RAM 初始设置

在 RAM 控制台中您可以设置您的企业别名、 *RAM* 用户的登录密码强度以及*RAM* 用户安全策略。

设置您的企业别名

为您的云账号设置一个 RAM 企业别名，好处是能让 RAM 用户更容易记住登录入口。

由于安全原因，RAM 用户的登录入口不同于主账号的登录入口。RAM 用户登录时，需要提供主账号的 RAM 企业别名、RAM 用户名和 RAM 用户登录密码。

操作步骤

1. 在RAM控制台点击左侧导航栏中的设置。
2. 点击企业别名设置，进入子页面。
3. 点击编辑企业别名，进入编辑页面。

图 **2-1:** 编辑企业别名

4. 输入企业别名，并点击确认。

至此，您已完成企业别名的设置。登录到阿里云控制台后，将鼠标悬置在导航菜单右上角的账号名上，即可在悬浮窗口中查看当前账号的企业别名。

设置 RAM 用户的登录密码强度

在 RAM 中，您可以统一指定所有 RAM 用户的密码登录强度，那么在用户重置密码时将要求不得低于您设置的密码强度。

操作步骤

1. 在RAM控制台点击左侧导航栏中的设置。
2. 在密码强度设置 子页面配置密码策略。

图 2-2: 设置密码强度

3. 完成配置后，点击保存修改。

至此，您已完成 RAM 用户登录密码强度的设置。

设置 RAM 用户安全策略

在 RAM 中，您可以指定 RAM 用户必须设置多因素认证(MFA)。一旦设置 MFA，您还可以统一指定是否允许登录时在其登录设备上保存 MFA 登录状态(保存7天)。此外，您可以进一步指定是否允许子用户自主管理密码、AccessKey及多因素认证设备。

操作步骤

1. 在RAM控制台点击左侧导航栏中的设置。
2. 点击子用户安全设置，进入子页面。
3. 在子页面勾选需要的安全策略。

图 2-3: 子用户安全设置

4. 完成设置后，点击保存修改。

至此， 您已完成 RAM 用户安全设置。

3 设置 MFA（可选）

本文介绍了在 RAM 控制台开启 MFA（Multi-factor authentication，多因素认证）以及使用 MFA 进行登录的方法，帮助您使用 MFA 提高账号安全性。

为主账号开启多因素认证

主账号对其名下的资源拥有完全控制权限，一旦云账号登录密码泄露，账号下的资产将面临极大的威胁。为了降低风险，我们强烈建议您给主账号绑定多因素认证。

前提条件

您需要在智能手机终端上安装虚拟 MFA 应用程序以完成下述操作，推荐您使用阿里云 App。

下文以 阿里云 App 为例来描述操作步骤。

操作步骤

1. 使用阿里云主账号登录到账号管理下 安全设置 页面。
2. 在虚拟**MFA** 菜单下，点击**设置** 进入启用虚拟 MFA 设备绑定流程。
3. 通过邮箱验证、手机验证或密保问题完成身份验证，进入**启用虚拟MFA设备**页面，如下图所示。

图 **3-1:** 身份验证

4. 在手机中打开阿里云 **App**，选择**+** > **扫码添加**进行扫码。扫码完成后会自动添加用户，阿里云 App 会显示您当前账号的动态口令，每30秒更新一次。

图 **3-2:** 动态口令

说明：

如果您的智能设备不支持扫码功能，那么您也可以选择**手输信息获取**，在 MFA 应用程序中以手动输入 MFA 密钥的方式进行配置。

5. 在**启用虚拟MFA设备** 页面中输入 MFA 应用中显示的连续两组动态口令，然后单击**确定启用**。如下图所示：

图 **3-3:** 启用虚拟**MFA**设备

至此，您已成功启用 MFA 设备。

开启 **MFA** 后的登录过程

在开启 MFA 后，只有完成两步验证后，您才能登录到阿里云。操作步骤如下：

1. 登录控制台时先输入登录用户名和密码。
2. 校验密码成功后，还需您提供虚拟 MFA 设备的动态安全验证码，如下图所示：

图 3-4: 验证动态安全验证码

在您的手机阿里云 App 应用中，获取并输入登录账号的动态验证码，即可正常登录到阿里云。

4 创建 RAM 用户

在创建 RAM 用户前，确保您已完成*RAM* 初始设置。

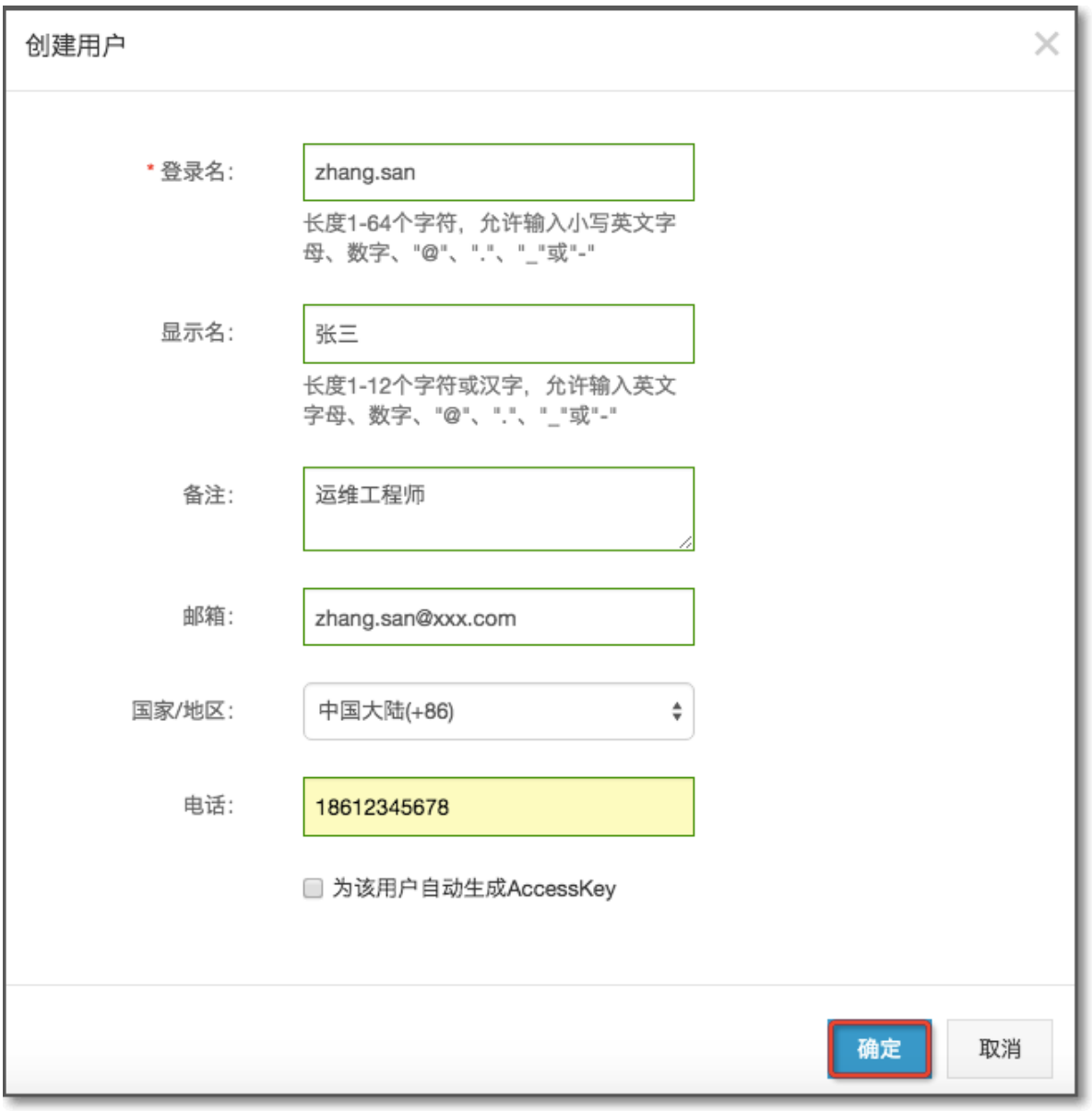
本文将指导您创建一个 RAM 用户，并根据用户的使用需求，分别为用户设置登录密码（如果该用户需要登录控制台），或 AccessKey（如果用户需要以程序方式调用云服务 API）。

创建 RAM 用户

执行以下步骤创建 RAM 用户：

1. 在RAM控制台点击左侧导航栏中的用户管理。
2. 点击右上角新建用户，进入创建用户页面。
3. 输入用户信息后，点击确认。

图 **4-1:** 创建用户



至此，您已完成 RAM 用户创建。

为用户设置登录密码

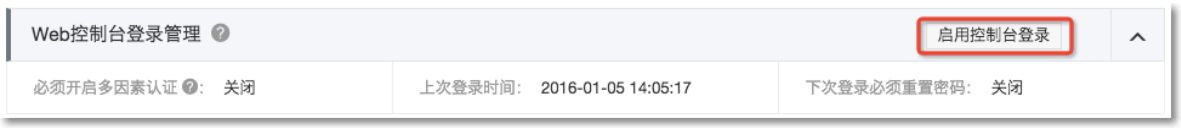
对于已创建的 RAM 用户，如果该用户需要登录到控制台，则应为其配置登录密码。

操作步骤

1. 在RAM控制台点击左侧导航栏中的用户管理。
2. 选择需要设置密码的用户（可通过登录名 进行搜索），并点击该用户名或其用户菜单下的管理按钮，进入用户详情页。

3. 在**Web**控制台登录管理下，点击启用控制台登录。

   图 **4-2:** 启用控制台登录



4. 在弹窗中为用户设置初始密码，并可以指定用户登录时必须更换密码。

   图 **4-3:** 设置登录密码

至此，您已为 RAM 用户设置登录密码。

- 如需使用 RAM 子账号登录进行测试，请参照*RAM* 用户登录控制台。

- 如需对 RAM 子账号登录密码进行管理，请执行步骤 1~3，并在**Web控制台登录管理** 下，选择**重置密码**或者**关闭控制台登录**。

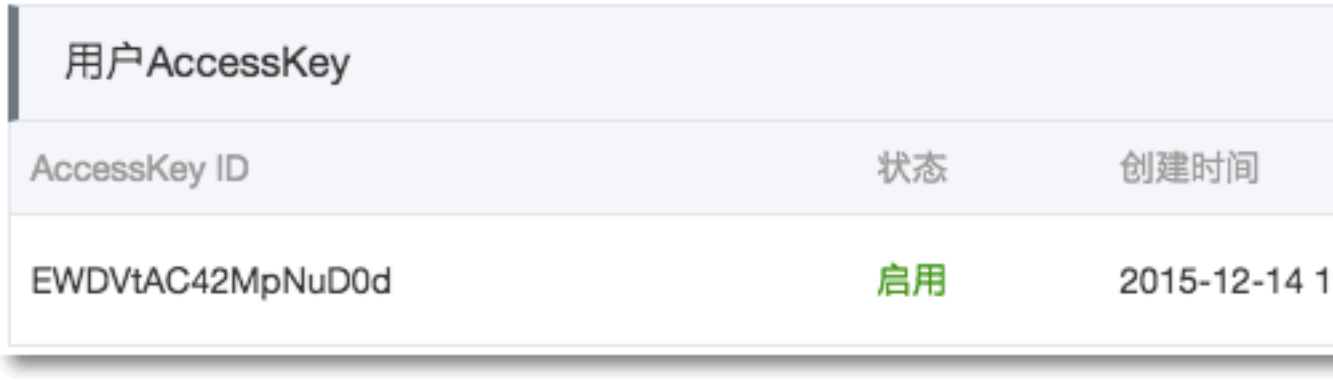
为用户创建**AK**

对于已创建的 RAM 用户，如果该用户需要以程序方式调用云服务 API，则应为其创建 AccessKey（AK）。

操作步骤

1. 在RAM控制台点击左侧导航栏中的**用户管理**。
2. 选择需要设置密码的用户（可通过登录名进行搜索），并点击该用户名或其用户菜单下的管理按钮，进入用户详情页。
3. 在用户**AccessKey**子页下，点击创建**AccessKey**。

   图 **4-4:** 创建**AccessKey**



4. 新建 Accesskey 成功后，点击保存保存**AK**信息。

   说明：

   - AccessKeySecret 只会在 AK 创建时提供查看或下载，为了安全考虑，后续不会提供 AccessKeySecret 的再次查看或下载功能。
   - 如果 AK 丢失，您只能重新创建 AK。新创建的 AK 与原来的 AK 都是代表相同的用户身份，同一个 RAM 用户的不同 AK 在使用上是完全等效的。
   - 建议您为应用程序周期性更换 AK，避免因为 AK 泄露导致风险。

至此，您已为 RAM 用户创建 AccessKey。如需对用户的 AK 进行管理，请执行步骤 1~3，然后在用户**AccessKey**子页下，选择**禁用**或**删除**已创建的 AccessKey。

后续操作

对于已创建的 RAM 用户，在正常使用前，需要根据其职责对其进行访问资源授权。

- 给 RAM 用户授权，请参照 为 *RAM* 用户授权。
- 创建粒度精细的自定义的授权策略，请参照创建自定义授权策略#可选#创建自定义授权策略。

5 创建 RAM 用户组（可选）

操作步骤

1. 在RAM控制台单击群组管理 > 新建群组。

   图 5-1: 新建群组

2. 在新建群组 对话框中，输入组名称（必填）和备注（选填），然后单击确定。

6 创建自定义授权策略（可选）

目前，阿里云提供了多种系统授权策略可供用户选择使用。这些授权策略仅仅提供了粗粒度的访问控制能力，比如某个云产品级别的只读权限或所有权限。

如果您有更细粒度的授权需求，比如授权用户 bob 只能对 `oss://samplebucket/bob/` 下的所有对象执行只读操作，而且限制 IP 来源必须为您的公司网络(可以通过搜索引擎查询“我的 IP”来获知您的公司网络 IP 地址)，那么您可以通过创建自定义授权策略来进行访问控制。

本文以上述用户 bob 为例，介绍了创建自定义授权策略的方法，帮助您更好地理解和使用 RAM 进行精细粒度的访问控制。

日志组的限制为：最大 4096 条日志，或 10MB 空间。

前提条件

在创建自定义授权策略时，您需要了解授权策略语言的基本结构和语法，请参考*Policy* 语法结构。

RAM 最细可以支持各产品 API 粒度的授权，即授权策略中的操作权限可以精细到每个 API 操作。在创建自定义授权策略前，您需要了解有关产品所支持的授权粒度和授权方法，具体请参考支持 *RAM* 的云服务。

操作步骤

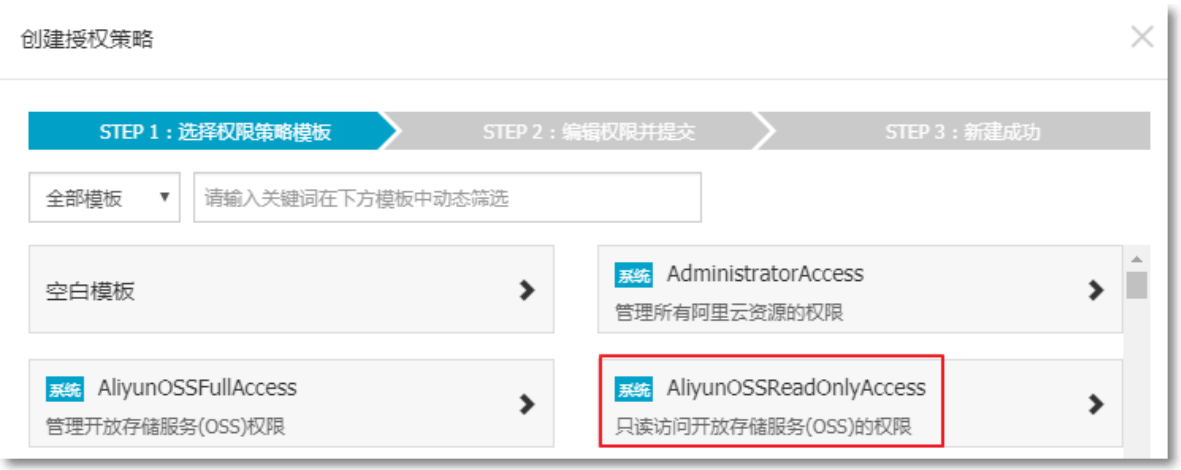
1. 在RAM控制台点击左侧导航栏中的策略管理。在策略管理页面，可通过系统授权策略和自定义授权策略子页，分别查看已有的系统和自定义策略。

图 6-1: 自定义授权策略

2. 点击新建授权策略，进入创建授权策略页面。
3. 选择权限策略模板。

> 说明：
> 可以选择空白模板，但推荐使用类似的已有系统策略作为模板进行编辑。此处以 AliyunOSSReadOnlyAccess（账号下所有 OSS 资源的只读权限）作为模板。

图 6-2: 创建授权策略



4. 基于选择的模板，编辑授权策略。
5. 策略内容编辑完成后，点击新建授权策略。

图 6-3: 新建授权策略

此处修改了授权策略名称、备注和策略内容。上图策略内容中的高亮显示部分是新增的细粒度授权限制内容，其代码样例为：

```json
{
"Version": "1",
"Statement": [
{
"Effect": "Allow",
"Action": [
"oss:Get*",
"oss:List*"
],
"Resource": [
"acs:oss:*:*:samplebucket/bob/*"
],
"Condition": {
"IpAddress": {
"acs:SourceIp": "121.0.27.1"
}
}
}
]
}
```

```
```

后续操作

接下来只需将本文创建的策略授权给用户 bob，则 bob 会拥有对 `oss://samplebucket/bob/` 下的对象的只读操作权限，且限制条件是必须从您的公司网络（假设为121.0.27.1）进行访问。

为 RAM 用户授权，请参考为 *RAM* 用户授权。

7 为 RAM 用户授权

为 RAM 用户授权有两种方法：

- 直接为 *RAM* 用户授权
- 为用户所属的用户组授权

以上两种方法均可达到授予 RAM 用户相关资源访问权限的目的。

背景知识

系统授权策略是 RAM 提供的一组通用授权策略，可满足粗粒度授权需求。比如，授权某个 RAM 用户管理订单（AliyunBSSFullAccess），管理 ECS 资源(AliyunECSFullAccess)，或管理所有子用户及其权限(AliyunRAMFullAccess)。

您可以在授权策略管理查看 RAM 支持的所有系统授权策略。

如果这些授权策略均无法满足需求，您可以自定义粒度更精细的授权策略，具体请参考创建自定义授权策略#可选#。

直接为 RAM 用户授权

通过 AttachPolicyToUser 直接为 RAM 用户授权。

操作步骤

1. 在RAM控制台单击左侧导航栏中的用户管理。
2. 找到待授权用户（可按用户名 搜索），并单击此用户对应的授权按钮。
3. 在编辑个人授权策略对话框中，添加授权策略（可按关键词搜索），并单击确定。
   - 从左侧可选授权策略名称 列表中选择您需要的策略，单击向右箭头（即授权）将其添加到已选授权策略名称列表中。
   - 反之，单击向左箭头可取消选择已选授权策略名称列表中的策略。

图 7-1: 编辑个人授权策略

为用户所属的用户组授权

通过 AttachPolicyToGroup 为用户所属的用户组授权。

使用此方法前，请确保待授权用户已经在待授权用户组中。

操作步骤

1. 在RAM控制台单击左侧导航栏中的群组管理。
2. 找到待授权用户所属的用户组，单击此用户组对应的授权按钮。
3. 在编辑群组授权策略对话框中，添加授权策略（可按关键词搜索），并单击 确定。

后续操作

- 对于直接授予 RAM 用户的权限，可前往用户授权策略子页面的个人授权策略页签 查看权限或解除授权。
- 对于授予 RAM 用户所属用户组的权限，可前往群组授权策略管理子页面查看权限或解除授权。

8 RAM 用户登录控制台

RAM 用户和云账号有不同的登录入口。本文介绍 RAM 用户的登录入口和登录所需信息。

登录入口

请登录*RAM*控制台后，在**概览**子页查询登录链接）。

登录信息

RAM 用户登录需提供企业别名、子用户名称和密码。

其中，企业别名就是您在*RAM* 初始设置中设置的企业别名。如果没有设置企业别名，默认的企业别名就是您的云账号 ID（可在**账号管理 > 安全设置**中查询）。

9 业务限制

限制项	限制值
用户总数	100
组总数	50
每个用户可加入的组数	5
每个用户可创建的 AccessKey 个数	2
每个用户可绑定的 MFA 个数	1
虚拟 MFA 设备数	100
自定义授权策略数	200
自定义授权策略版本数	5
为用户添加的授权策略数	5
为组添加的授权策略数	5
用户名的字符数	64
组名的字符数	64
授权策略名称的字符数	128
角色名称的字符数	64
角色数	100
别名的字符数	3-64
自定义授权策略的字符数	2048