访问控制

快速入门

快速入门

本文介绍了 RAM 的一般操作步骤，旨在帮助您使用 RAM 创建子用户，对子用户授权，并使用子用户登录系统。

快速入门流程

使用 访问控制 RAM 的一般操作步骤如下：

1. 设置 MFA（可选）
2. RAM 初始设置
3. 创建 RAM 用户
4. 创建自定义授权策略（可选）
5. 给 RAM 用户授权
6. RAM 用户登录控制台

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。

此外，常用的 MFA 应用程序还有 Google Authenticator，您可以自主选择安装使用。关于 Google Authenticator 安装问题，请参考 Google Authenticator 安装及使用指导。

下文以 阿里云 App 为例来描述操作步骤，使用其他 MFA 应用程序的步骤与此类似。

操作步骤

使用阿里云主账号登录到账号管理下 安全设置 页面。

在 **虚拟MFA** 菜单下，点击 **设置** 进入启用虚拟 MFA 设备绑定流程。

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。

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。

注意：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。

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：

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：

登录控制台时先输入登录用户名和密码。

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：

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。

在 RAM 控制台中您可以设置您的 **企业别名**、您的 **RAM 用户登录密码强度**、您的 **RAM 用户安全设置**。

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

登录到 **阿里云 RAM 控制台**。

点击左侧导航栏中的 **设置**。

点击 **企业别名设置**，进入子页面。

点击 **编辑企业别名**，进入编辑页面。

5. 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

登录到 阿里云 RAM 控制台。

点击左侧导航栏中的 **设置**。

在 **密码强度设置** 子页面配置密码策略。

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 用户安全设置

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

登录到 阿里云 RAM 控制台。

点击左侧导航栏中的 **设置**。

点击 **子用户安全设置**，进入子页面。

在子页面勾选需要的安全策略。

完成配置后，点击 **保存修改**。

至此， 您已完成 RAM 用户安全设置。

在创建 RAM 用户前，确保您已完成 RAM 初始设置，配置了您的企业别名，及 RAM 用户的登录密码策略及安全策略。

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

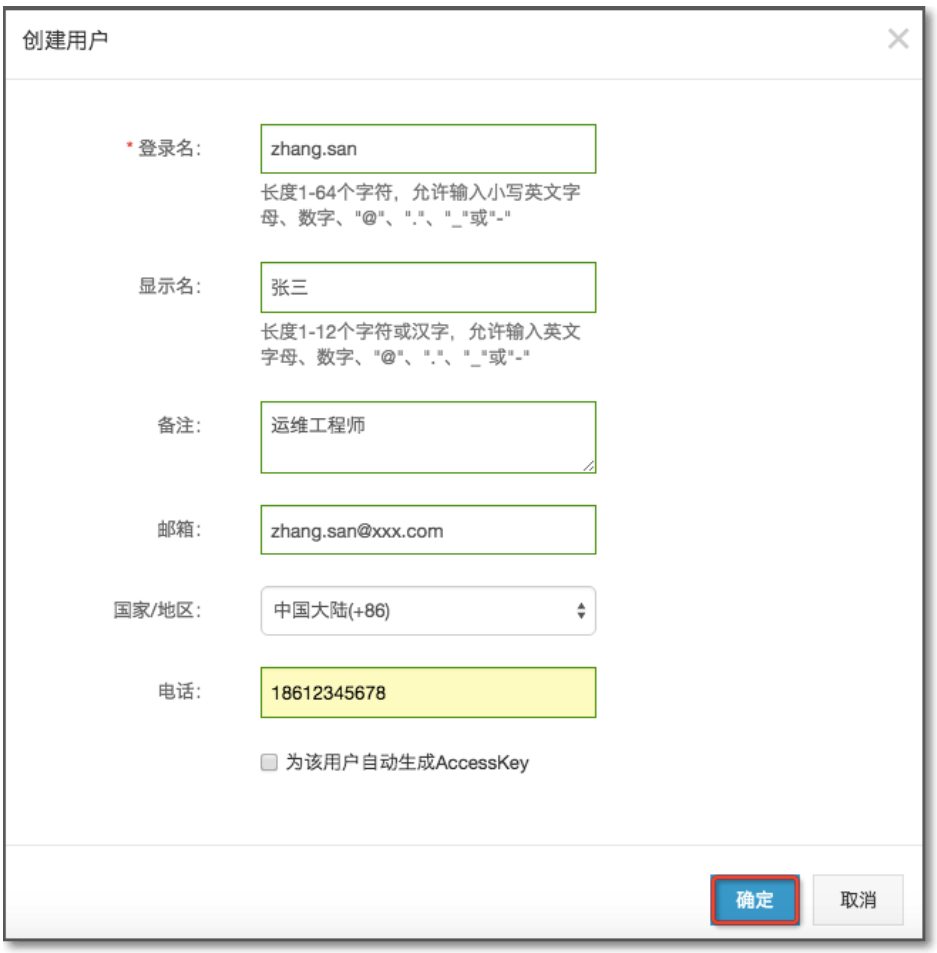
执行以下步骤创建 RAM 用户。

登录到 阿里云 RAM 控制台。

点击左侧导航栏中的 **用户管理**。

点击右上角 **新建用户**，进入创建用户页面。

输入用户信息后，点击 **确认**。



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。

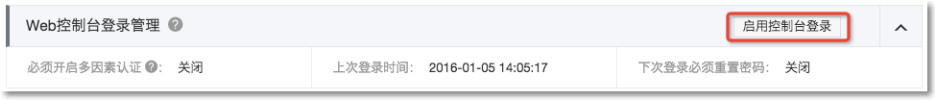
操作步骤

登录到 阿里云 RAM 控制台。

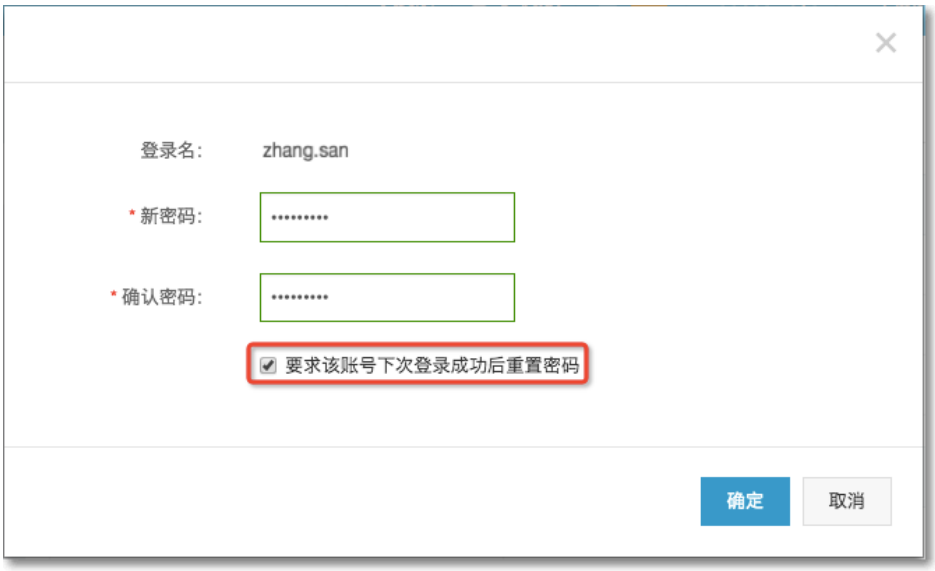
点击左侧导航栏中的 **用户管理**。

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。

在 **Web控制台登录管理** 下，点击 **启用控制台登录**。



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。



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

登录到 阿里云 RAM 控制台。

点击左侧导航栏中的 **用户管理**。

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。

在 **用户AccessKey** 子页下，点击 **创建AccessKey**。

新建 Accesskey 成功后，点击保存 **保存AK信息**。

注意：

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 给 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。

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://sample_bucket/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。

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 授权策略语言描述。

RAM 最细可以支持各产品 API 粒度的授权，即 Policy 中的 Action 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 RAM 支持的云服务。

操作步骤

登录到 阿里云 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。

点击 **新建授权策略**，进入 **创建授权策略** 页面。

选择权限策略模板。

注意：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。如本文我们以 具体 OSS 桶下资源的只读权限为例，这里选择 AliyunOSSReadOnlyAccess （账号下所有 OSS 资源的只读权限）作为模板。

基于选择的模板，编辑 Policy。

这里修改了授权策略名称，备注和策略内容。上图策略内容中的选中部分是新增的细粒度授权限制内容。其代码样例为：

```
{
"Version": "1",
"Statement": [
{
"Effect": "Allow",
"Action": [
"oss:Get*",
"oss:List*"
],
"Resource": [
"acs:oss:*:*:samplebucket/bob/*"
]
"Condition": {
"IpAddress": {
"acs:SourceIp": "127.0.27.1"
}
}
}
]
}
```

策略内容编辑完成后，点击 **新建授权策略** 完成创建。

至此，您已完成自定义授权策略的创建。

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。

- 给 RAM 用户授权，请参照 给 RAM 用户授权。

在对 RAM 用户进行授权时，你可以选择直接向具体 RAM 用户授权，也可以给用户所属的用户组授权，两种方法都可以达到授予 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，它可以满足用户的粗粒度授权需求。比如，授权某个 RAM 用户可以管理订单（AliyunBSSFullAccess），或管理 ECS 资源(AliyunECSFullAccess)，或者管理所有子用户及其权限(AliyunRAMFullAccess)，等等。

您可以在 RAM 授权策略管理 查看 RAM 所支持的所有系统授权策略。

如果这些授权策略不满足您的需要，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。

直接给 RAM 用户授权

通过 AttachPolicyToUser 直接给 RAM 用户授权。

操作步骤

登录到 阿里云 RAM 控制台。

点击左侧导航栏中的 **用户管理**。

选择需要授权的用户（可通过 **登录名** 进行搜索），并点击其用户菜单下的 **授权** 按钮，进入 **编辑个人授权策略** 页面。

也可以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，并选择 **用户授权策略** > **编辑授权策略**。

添加需要的授权策略（可按关键词进行搜索），并点击 **确认**。

从左侧 **可选授权策略** 下选择需要的策略，点击右向箭头（即授权）将其添加到 **已选授权策略** 中。

反之，通过左向箭头可将右侧 **已选授权策略** 取消。

至此，您已完成直接给 RAM 用户授权。

给用户所属的用户组授权

通过 AttachPolicyToGroup 来给用户所属用户组进行授权。

使用该方法时，需要保证待授权用户在待授权的用户组中。为此，需要先创建用户组，并将待授权用户添加到相应用户组。

操作步骤

登录到 阿里云 RAM 控制台。

点击左侧导航栏中的 **群组管理**。

点击 **新建群组**。

输入 **组名称** 和 **备注**，并点击 **确认**，完成群组创建。

创建群组后，可通过以下任意一种方式将用户添加到相应群组中：

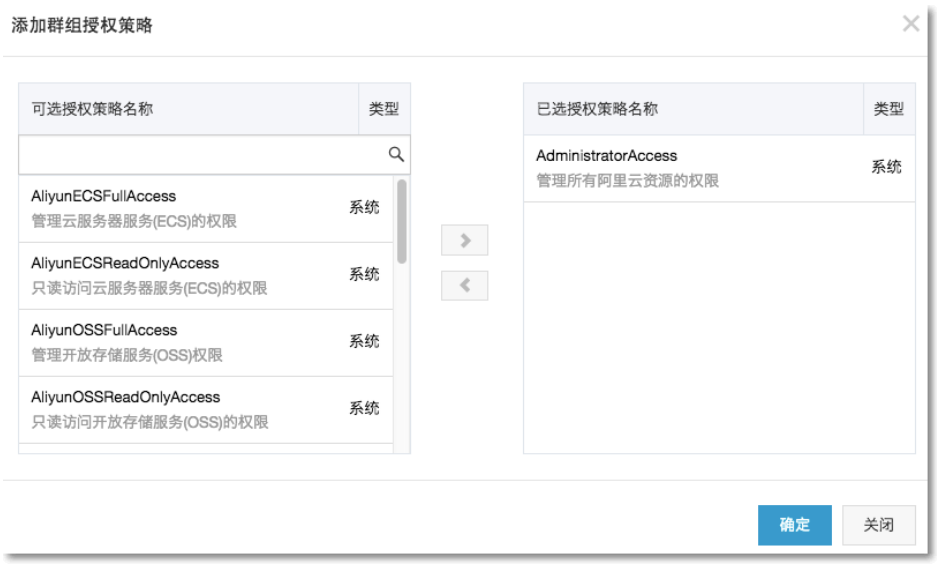
在 **群组管理** 页面，选择对应群组菜单下 **编辑组成员**。

在 **用户管理** 页面，选择对应用户菜单下 **加入组**。

具体操作方法类似于 直接给 RAM 用户授权- 步骤 4 中的 **添加需要的授权策略**。

用户添加到群组后，在 **群组管理** 页面，选择对应群组菜单下 **授权** 按钮。

添加需要的授权策略（可按关键词进行搜索），并点击 **确认**。



操作方法类似于 直接给 RAM 用户授权- 步骤 4 中的 **添加需要的授权策略**。

至此，您已完成给用户所属用户组授权。

后续操作

> 对于直接授予 RAM 用户的权限，可前往 **用户详情** > **用户授权策略** 下 **查看权限** 或 **解除授权**。
>
> 对于授予 RAM 用户所在用户组的权限，可前往 **群组详情** > **群粗授权策略管理** 下，**查看权限** 或 **解除授权**。

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

RAM 用户需要使用如下登录入口进行登录：https://signin.aliyun.com/login.htm （用户可登录 RAM 控制台，在概览页中查看 RAM 用户的登录入口链接）。

登录信息

RAM 登录时需要提供 **企业别名**、**子用户名称** 和 **子用户密码**。

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（在 **账号管理** > **安全设置** 中可以查看当前的登录云账号 ID）。

限制

限制项	限制值
用户总数	100
组总数	50
每个用户可以加入的组	5
每个用户允许创建AccessKey	2
每个用户可绑定MFA数	1
虚拟 MFA 设备数	100
自定义授权策略数	200
自定义策略版本数	5
附加给用户的授权策略数	5

附加给组的授权策略数	5
用户名字符数	64
组名字符数	64
授权策略名称字符数	128
角色名称字符数	64
角色数	100
别名字符数	3-64
自定义授权策略字符数	2048