ALIBABA CLOUD

Alibaba Cloud

访问控制

快速入门

文档版本：20201010

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.入门概述

当企业接入阿里云，需要通过访问控制（RAM）进行安全管控。本文为您介绍一系列入门操作，方便您快速上手和使用。

前提条件

请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。

入门操作

- 为了保护账号安全，请先设置安全策略。请参见设置RAM用户安全策略。
- RAM用户对应某一个操作实体，如运维操作人员或应用程序，您可以创建RAM用户进行日常管理。请参见创建RAM用户。
- 通过创建用户组对职责相同的RAM用户进行分类并授权，从而更好的管理用户。请参见创建用户组。
- 为创建好的RAM用户授权后，RAM用户便可以访问相应的阿里云资源。请参见为RAM用户授权。
- 如果系统策略不能满足您的需求，可以通过创建自定义策略满足细粒度的要求，从而实现更灵活的权限管理。请参见创建自定义策略。
- 基础操作配置完成后，RAM用户便可以登录控制台访问相应阿里云资源并进行日常工作。请参见RAM用户登录控制台。

更多信息

您可以通过RAM学习路径图快速了解RAM，学习相关的基础操作，并利用丰富的API、SDK包和便捷工具进行二次开发。

2.设置RAM用户安全策略

阿里云账号可以通过修改RAM用户安全设置更好的管理RAM用户的权限。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏的**人员管理**菜单下，单击**设置**。
3. 在**安全设置**页签下，单击**修改RAM用户安全设置**，配置相关参数。
   - **保存MFA登录状态7天**：表示是否允许RAM用户登录时保存多因素认证设备登录状态，有效期为7天，默认为不允许。
   - **自主管理密码**：表示是否允许RAM用户修改密码。
   - **自主管理AccessKey**：表示是否允许RAM用户管理访问密钥。
   - **自主管理多因素设备**：表示是否允许RAM用户绑定或解绑多因素认证设备。
   - **登录Session过期时间**：表示RAM用户登录有效期，单位为小时。

     > 说明 通过切换角色或角色SSO登录控制台时，登录会话有效期也会受到**登录Session过期时间**的限制，即最终的登录会话有效期将不会超过此参数设置的值。详情请参见使用RAM角色、角色SSO的SAML响应。

   - **登录掩码设置**：登录掩码决定哪些IP地址会受到登录控制台的影响。默认为空字符串，不限制登录IP。如果设置了登录掩码，使用密码登录或单点登录（SSO）时会受到影响，但使用访问密钥发起的API访问不受影响。
4. 单击**确定**。

   > 说明 设置成功后，此规则适用于所有RAM用户。

相关文档

- SetSecurityPreference

3.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. 在左侧导航栏的**人员管理**菜单下，单击**用户**。
3. 单击**创建用户**。

   > **说明** 单击**添加用户**，可一次性创建多个RAM用户。

4. 输入**登录名称**和**显示名称**。
5. 在**访问方式**区域下，选择**控制台访问**或**编程访问**。
   - **控制台访问**：完成对登录安全的基本设置，包括自动生成或自定义登录密码、是否要求下次登录时重置密码以及是否要求开启多因素认证。

     > **说明** 自定义登录密码时，密码必须满足您在**人员管理** > **设置**中设置的密码复杂度规则。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。

   - **编程访问**：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

- 可以为用户添加一个或多个权限策略，使RAM用户具有资源的访问能力。详情请参见为RAM用户授权。
- RAM用户创建成功后，可以使用RAM用户登录控制台。详情请参见RAM用户登录控制台。
- 可以将RAM用户添加到一个或多个RAM用户组，对RAM用户进行分类并授权。详情请参见添加用户组成员。

相关文档

- CreateUser

4.创建用户组

若云账号下有多个RAM用户，通过创建用户组对职责相同的RAM用户进行分类并授权，从而更好的管理用户及其权限。

操作步骤

1. 云账号登录RAM控制台。
2. 在左侧导航栏的**人员管理**菜单下，单击**用户组**。
3. 单击**创建用户组**。
4. 输入**用户组名称**、**显示名称**和**备注**。
5. 单击**确定**。

后续步骤

可以为用户组添加一个或多个权限策略，详情请参见为用户组授权。

相关文档

- CreateGroup

5.创建自定义策略

如果系统策略无法满足您的需求，您可以通过创建自定义策略实现精细化权限管理。

前提条件

创建自定义策略前，需要先了解权限策略语言的基本结构和语法，请参见权限策略语法和结构。

操作步骤

1. 云账号登录RAM控制台。
2. 在左侧导航栏的**权限管理**菜单下，单击**权限策略管理**。
3. 单击**创建权限策略**。
4. 输入**策略名称**和**备注**。
5. **配置模式**选择**可视化配置**或**脚本配置**。
   - 若选择**可视化配置**：单击**添加授权语句**，根据界面提示，对权限效力、操作名称和资源等进行配置，然后单击**确定**。
   - 若选择**脚本配置**，请参考权限策略语法和结构编辑策略内容。
6. 单击**确定**。

相关文档

- CreatePolicy

6.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

您可以在用户页面下为RAM用户授权。

1. 云账号登录RAM控制台。
2. 在左侧导航栏的**人员管理**菜单下，单击**用户**。
3. 在**用户登录名称/显示名称**列表下，找到目标RAM用户。
4. 单击**添加权限**，被授权主体会自动填入。
5. 在左侧**权限策略名称**列表下，单击需要授予RAM用户的权限策略。

   > **说明** 在右侧区域框，选择某条策略并单击×，可撤销该策略。

6. 单击**确定**。
7. 单击**完成**。

方式二

您可以在授权页面下为RAM用户授权。

1. 云账号登录RAM控制台。
2. 在左侧导航栏的**权限管理**菜单下，单击**授权**。
3. 单击**新增授权**。
4. 在**被授权主体**区域下，输入RAM用户名称或ID后，单击需要授权的RAM用户。
5. 在左侧**权限策略名称**列表下，单击需要授予RAM用户的权限策略。

   > **说明** 在右侧区域框，选择某条策略并单击×，可撤销该策略。

6. 单击**确定**。
7. 单击**完成**。

相关文档

- AttachPolicyToUser

7.RAM用户登录控制台

本文为您介绍RAM用户如何登录阿里云控制台，包括登录地址和登录方式。

背景信息

- 默认域名、账号别名、域别名的概念，请参见基本概念。
- 阿里云账号登录RAM控制台后，在人员管理 > 设置 > 高级设置中查看默认域名和域别名。

操作步骤

1. RAM用户登录阿里云控制台。

   > 说明 阿里云账号登录RAM控制台，在概览页可以快速查询RAM用户的登录地址。

2. 输入RAM用户的登录名称，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 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。

   - 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。

   - 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。

3. 输入RAM用户的登录密码，单击登录。