阿里云
访问控制

用户组管理

文档版本：20190917

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。
*## *	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 用户组概述

访问控制（RAM）通过用户组对职责相同的 RAM 用户进行分类并授权，可以更加高效地管理 RAM 用户及其权限。

- 在 RAM 用户职责发生变化时，只需将其移动到相应职责的用户组下，不会对其他 RAM 用户产生影响。

  关于如何创建用户组，请参考：#unique_4。
- 当用户组的权限发生变化时，只需修改用户组的权限策略，即可应用到所有 RAM 用户。

  关于如何为用户组授权，请参考：#unique_5。

2 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. 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. 单击新建用户组，输入登录名称、显示名称和备注。
4. 单击确认。

后续步骤

可以为用户组添加一个或多个权限策略，详情请参考：#unique_7。

3 添加用户组成员

您可以为用户组添加一个或多个 RAM 用户。当 RAM 用户加入到用户组后，将拥有该用户组的所有权限。

操作步骤

1. 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. 在用户组名称/显示名称列表下，找到目标用户组。
4. 单击添加组成员，用户组名称会自动填入。
5. 在左侧名称列表下，勾选需要添加到当前用户组的 RAM 用户名称。

   说明:

   在右侧区域框，选择某个 RAM 用户名称并单击 ×，可撤销该操作。
6. 单击确定。

4 移出用户组成员

当某个 RAM 用户离开组织或权限发生变化时，您需要将该 RAM 用户从用户组中移出。

操作步骤

1. 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. 在用户组名称/显示名称列表下，单击目标用户组名称。
4. 在组成员管理页签下，找到目标 RAM 用户，单击移出用户组。
5. 单击确认。

5 查看用户组基本信息

本文为您介绍如何查看用户组基本信息，包括用户组名称、显示名称和备注。

操作步骤

1. 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. 在用户组名称/显示名称列表下，单击目标用户组名称。
4. 在组基本信息区域，可以查看用户组基本信息。

6 修改用户组基本信息

本文为您介绍如何修改用户组基本信息，包括用户组名称、显示名称和备注。

操作步骤

1. 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. 在用户组名称/显示名称列表下，单击目标用户组名称。
4. 在组基本信息区域，单击编辑基本信息。
5. 修改完成后，单击确认。

7 为用户组授权

本文为您介绍如何为用户组授权。为用户组授权后，用户组中的所有 RAM 用户将拥有该用户组的所有权限。

操作步骤

1. 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，输入用户组名称后，单击需要授权的用户组。
5. 在左侧权限策略名称列表下，单击需要授予用户组的权限策略。

   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。

8 为用户组移除权限

当用户组权限发生变化时，可以将这些权限移除。本文为您介绍如何移除用户组的权限。

操作步骤

1. 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. 找到目标用户组，单击移除授权。
4. 单击确认。

9 删除用户组

当不再需要某个用户组时，可以删除该用户组。删除用户组会将所有用户从用户组中移除并撤销用户组拥有的权限。

操作步骤

1. 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. 在用户组名称/显示名称列表下，找到目标用户组，单击删除。
4. 单击确认。

10 最佳实践

10.1 RAM企业上云安全实践

本文为您介绍当企业上云之后，通过RAM进行安全管控，帮助您实现简单管理账号、统一分配权限、集中管控资源，建立安全完善的资源控制体系。

前提条件

进行操作前，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。

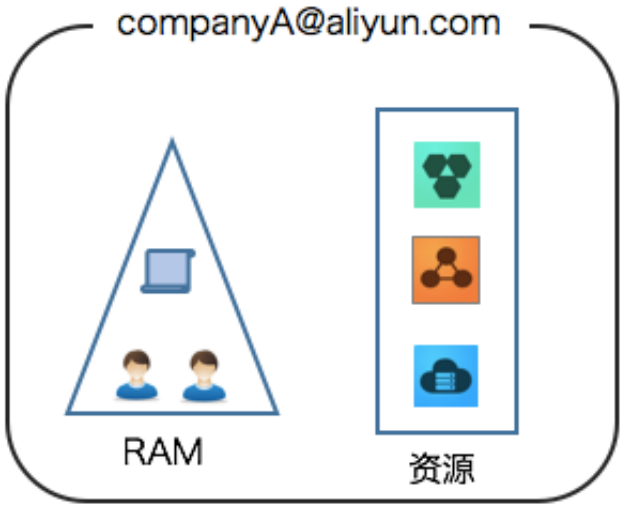
背景信息

某些公司使用RAM初期，对RAM的优势不够了解，也对云资源的安全管理要求不高。但是当初创企业成长为大型公司或大型企业客户迁移上云，组织结构更加复杂，对云资源的安全管理需求也更加强烈，需要建立安全完善的资源控制体系。

- 存在多用户协同操作，RAM用户分工不同，各司其职。
- 云账号不想与其他RAM用户共享云账号密钥，密钥泄露风险较大。
- RAM用户对资源的访问方式多种多样，资源泄露风险高。
- 某些RAM用户离开组织时，需要收回其对资源的访问权限。

解决方案

使用RAM，您可以创建、管理RAM用户，并可以控制这些RAM用户对资源的操作权限。当您的企业存在多用户协同操作资源时，使用RAM可以让您避免与其他用户共享云账号密钥，按需为用户分配最小权限，管理更加方便，权限更加明确，信息更加安全。



安全管理实施方案

- 创建独立的RAM用户

  企业只需使用一个云账号。通过RAM为名下的不同操作员创建独立的RAM用户，进行分权管理，不使用云账号进行日常运维管理。

  详情请参见#unique_17。

- 将控制台用户与API用户分离

  不建议给一个RAM用户同时创建用于控制台操作的登录密码和用于API操作的访问密钥。

  - 对于应用程序账号，只需要通过OpenAPI访问云资源，只需要给它创建访问密钥即可。
  - 对于员工账号，只需要通过控制台操作云资源，只需要设置登录密码即可。

  详情请参见#unique_17。

- 创建用户并进行分组

  当云账号下有多个RAM用户时，可以通过创建用户组对职责相同的RAM用户进行分类并授权。

  详情请参见创建用户组。

- 给不同用户组分配最小权限

  您可以使用系统策略为用户或用户组绑定合理的权限策略，如果您需要更精细粒度的权限策略，也可以选择使用自定义策略。通过为用户或用户组授予最小权限，可以更好的限制用户对资源的操作权限。

  详情请参见#unique_18。

- 为用户登录配置强密码策略

  您可以通过RAM控制台设置密码策略，如密码长度、密码中必须包含元素、密码有效期等。如果允许RAM用户更改登录密码，那么应该要求RAM用户创建强密码并且定期轮换登录密码或访问密钥。

  详情请参见#unique_19。

- 为云账号开启多因素认证

  开启多因素认证（Multi-factor authentication，MFA）可以提高账号的安全性，在用户名和密码之外再增加一层安全保护。启用MFA后，用户登录阿里云时，系统将要求输入两层安全要素：

  1. 第一安全要素：用户名和密码
  2. 第二安全要素：多因素认证设备生成的验证码

  详情请参见#unique_20。

- 为用户开启SSO单点登录功能

  开启SSO单点登录后，企业内部账号进行统一的身份认证，实现使用企业本地账号登录阿里云才能访问相应资源。

  详情请参见#unique_21。

- 不要为云账号创建访问密钥

  由于云账号对名下资源有完全控制权限，AccessKey与登录密码具有同样的权力，AccessKey用于程序访问，登录密码用于控制台登录。为了避免因访问密钥泄露带来的信息泄露，不建议您创建云账号访问密钥并使用该密钥进行日常工作。

  您可以通过为RAM用户创建访问密钥，使用RAM用户进行日常工作。

  详情请参见#unique_22。

- 使用策略限制条件来增强安全性

  要求用户必须使用安全信道（例如：SSL）、在指定时间范围或在指定源IP条件下才能操作指定的云资源。

  详情请参见#unique_23。

- 集中控制云资源

  阿里云默认云账号是资源的拥有者，掌握完全控制权。RAM用户对资源只有使用权，没有所有权。这一特性可以方便您对用户创建的实例或数据进行集中控制。

  - 当用户离开组织：只需要将对应的账号移除，即可撤销所有权限。
  - 当用户加入组织：只需创建新的账号，设置登录密码或访问密钥并为 RAM 用户授权。

  详情请参见#unique_24。

- 使用STS给用户授权临时权限

  STS （Security Token Service）是RAM的一个扩展授权服务，使用STS访问令牌可以给用户授予临时权限，您可以根据需要来定义访问令牌的权限和自动过期时间，可以让授权更加可控。

  详情请参见#unique_25。

操作结果

遵循最佳安全实践原则，企业上云之后，综合利用这些保护机制，建立安全完善的资源控制体系，可以更有效的保护账号及资产的安全。

更多信息

企业上云以后通过RAM进行运维划分，根据不同的职责，划分不同的运维人员，方便管理和控制。详情请参见#unique_26。