ALIBABA CLOUD

阿里云

访问控制
最佳实践

文档版本：20211231

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.企业上云安全实践

当企业上云之后，RAM可以帮助您实现简单管理账号、统一分配权限、集中管控资源，从而建立安全、完善的资源控制体系。

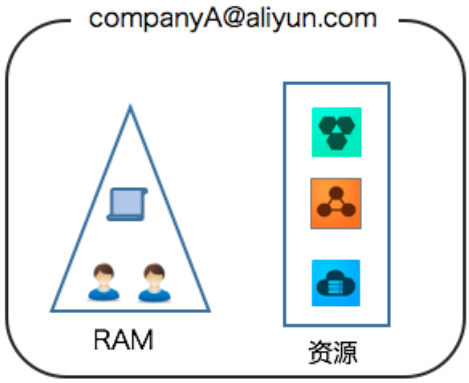
背景信息

某些企业使用RAM初期，对RAM的优势不够了解，也对资源的安全管理要求不高。然而，当初创企业成长为大型企业或大型企业客户迁移上云后，组织结构更加复杂，对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。
- 阿里云账号不想与其他RAM用户共享阿里云账号访问密钥（AccessKey），访问密钥泄露风险较大。
- 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阿里云账号访问密钥，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。



安全管理原则

- **创建独立的RAM用户**

  企业只需使用一个阿里云账号。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，不使用阿里云账号进行日常运维管理。

  具体操作，请参见创建RAM用户。

- **将控制台用户与API用户分离**

  不建议为一个RAM用户同时创建用于控制台操作的登录密码和用于API调用的访问密钥。具体如下：

  - 应用程序账号：只需要通过API访问资源，创建访问密钥即可。
  - 员工账号：只需要通过控制台操作资源，设置登录密码即可。

  具体操作，请参见创建RAM用户。

- **创建RAM用户并进行分组**

  当阿里云账号下有多个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。

  具体操作，请参见创建用户组。

- **为不同用户组分配最小权限**

您可以使用系统策略或自定义策略为RAM用户或用户组授权。自定义策略可以满足您精细化授权的需求。通过为RAM用户或用户组授予最小权限，可以更好地限制RAM用户对资源的操作权限。

> **说明** 当业务场景比较简单时，您可以直接创建RAM用户并为其授权。当业务场景越来越复杂，RAM用户数量越来越多时，推荐您将相同职责的RAM用户添加到用户组，然后为用户组授权，以此降低管理的复杂性。

具体操作，请参见创建自定义权限策略和为用户组授权。

- **为RAM用户配置强密码策略**

  您可以通过RAM控制台设置密码策略，例如：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。

  具体操作，请参见设置RAM用户安全策略。

- **为阿里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，再次登录阿里云时，系统将要求输入两层安全要素：

  i. 第一层安全要素：用户名和密码。
  ii. 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。

  具体操作，请参见为阿里云账号启用多因素认证。

- **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并访问阿里云资源。

  更多信息，请参见SSO概览。

- **不要为阿里云账号创建访问密钥**

  访问密钥用于API调用访问，登录密码用于控制台访问，两者具有同样的权限。由于阿里云账号对名下资源有完全控制权限，为了避免因访问密钥泄露带来的安全风险，不建议您为阿里云账号创建访问密钥并使用该访问密钥进行日常工作。

  您可以为RAM用户创建访问密钥，使用RAM用户进行日常工作。

  具体操作，请参见为RAM用户创建访问密钥。

- **使用权限策略条件来增强安全性**

  您可以在自定义权限策略中设置条件，实现在指定时间范围或指定IP等条件满足时才能访问某资源。

  更多信息，请参见权限策略基本元素。

- **集中控制资源**

  默认阿里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。具体如下：

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

  具体操作，请参见为RAM用户授权。

- **使用RAM角色进行临时授权**

  RAM角色不具备永久身份凭证，可以通过STS获取可以自定义时效和访问权限的临时身份凭证（STS Token），然后使用STS Token访问阿里云资源。

  更多信息，请参见什么是STS。

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，可以更有效地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。更多信息，请参见通过RAM管控多运维人员的权限 。

2.用户管理与分权

当企业有多种云资源时，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。

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 。

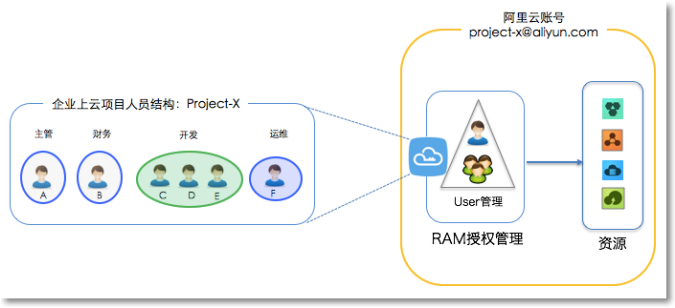
背景信息

企业A的某个项目（Project-X）上云，购买了多种阿里云资源，例如：ECS实例、RDS实例、SLB实例和OSS存储空间等。项目里有多个员工需要操作这些云资源，由于每个员工的工作职责不同，需要的权限也不同。

企业A希望能够达到以下要求：

- 企业A不希望多员工共享同一个云账号，共享云账号可能导致密码或访问密钥泄露。
- 企业A希望能给员工创建独立账号（操作员账号）并独立分配权限，做到责权一致。
- 企业A希望用户账号只能在授权的前提下操作资源，所有用户账号的所有操作行为可审计。
- 企业A希望随时可以撤销用户账号身上的权限，也可以随时删除其创建的用户账号。
- 企业A不需要对用户账号进行独立的计量计费，所有发生的费用统一计入云账号账单。

解决方案



- 为云账号设置多因素认证，避免因云账号密码泄露导致风险。详情请参见 为阿里云账号启用多因素认证 。
- 为不同员工（应用系统）创建RAM用户，并按需设置登录密码或创建访问密钥。详情请参见 创建RAM用户。
- 如果有多个员工的职责相同，建议创建用户组，并将用户添加到用户组。详情请参见 创建用户组 。
- 为RAM用户或用户组添加一条或多条系统策略。详情请参见 为RAM用户授权 或为用户组授权 。如果需要更细粒度的授权，可以创建自定义策略并为RAM用户或用户组进行授权。详情请参见创建自定义权限策略。
- 为不需要权限的RAM用户或用户组移除权限。详情请参见 为RAM用户移除权限 或为用户组移除权限 。