访问控制

最佳实践

最佳实践

本文分别从 **登录验证**、**账号授权**、**权限分配** 三方面 提供 RAM 的操作建议，帮助您更有效地使用 RAM 进行用户身份管理和资源访问控制。

登录验证

为根账户和 RAM 用户启用 MFA

- 建议您 为根账户绑定 MFA（Multi-factor authentication，多因素认证），每次使用根账户时都强制使用多因素认证。
- 如果您创建了 RAM 用户，并且给用户授予了高风险操作权限（比如，停止虚拟机，删除存储桶），那么建议您 给 RAM 用户绑定 MFA。

为用户登录配置强密码策略

- 如果您 允许子用户更改登录密码，那么应该要求他们创建强密码并且定期轮换。
- 您可以通过 RAM 控制台 设置密码策略，如最短长度、是否需要非字母字符、必须进行轮换的频率等等。

定期轮转用户登录密码和访问密钥

- 建议您或 RAM 用户要定期轮换登录密码或访问密钥。 在您不知情的时候，如果出现凭证泄露，那么凭证的使用期限也是受限制的。
- 您可以通过 设置密码策略 来强制 RAM 用户轮换登录密码或访问密钥的周期。

账号授权

遵循最小授权原则

最小授权原则是安全设计的基本原则。当您需要 给 RAM 用户授权 时，请授予刚好满足他工作所需的权限，而不要过度授权。

比如，在您的组织中，如果 Developers 组员（或者一个应用系统）的工作职责只需要读取 OSS 存储桶里的数据，那么就只给这个组（或应用系统）授予 OSS 资源的只读权限，而不要授权 OSS 资源的所有权限，更不要授予对所有产品资源的访问权限。

使用策略限制条件来增强安全性

建议您给用户授权时 设置策略限制条件，这样可以增强安全性。

比如，授权用户 Alice 可以关停 ECS 实例，限制条件是 Alice 必须在指定时间、并且您公司网络中执行该操作。

及时撤销用户不再需要的权限

当一个用户由于工作职责变更而不再使用权限时，您应该及时 将用户的权限撤销。撤销方法请参考 给 RAM 用户授权 中的 后续操作。

这样，如果在不知情的时候，当用户的访问凭证泄露时对您带来的安全风险最小。

权限分配

不要为根账户创建访问密钥

由于根账户对名下资源有完全控制权限，所以为了避免因访问密钥泄露所带来的灾难性损失，不建议您创建根账号访问密钥并使用该密钥进行日常工作。

使用群组给 RAM 用户分配权限

在 给 RAM 用户授权 时，除了对 RAM 用户直接绑定授权策略，更方便的做法是创建与人员工作职责相关的群组（如admins、developers、accounting等），为每个群组绑定合适的授权策略，然后把用户加入这些群组。群组内的所有用户共享相同的权限。

这样，如果您需要修改群组内所有人的权限，只需在一处修改即可。当您的组织人员发生调动时，您只需更改用户所属的群组即可。

将用户管理、权限管理与资源管理分离

在使用 RAM 时，您应该考虑创建不同的 RAM 用户，其职责分别是 RAM 用户管理、RAM 权限分配，以及各产品的资源操作管理。一个好的分权体系应该支持权力制衡，尽可能地降低安全风险。

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。通常只给员工创建登录密码，给系统或应用程序只创建访问密钥。

阿里云主账号相当于您的所有云资源管控的 root 账号。一旦主账号的登录密码或 API 访问密钥丢失或泄露，将会对您的企业造成不可估量的损失。

那么，在使用阿里云服务时，如何保护您的主账号安全呢？请参考本文提供的主账号安全实践若干原则。

原则 1：给主账号开启多因素认证

- 给主账号开启多因素认证(MFA)，不要与他人共享 MFA 设备。
- 给授予特权操作的 RAM 用户也开启多因素认证。特权操作通常指管理用户、授权、停止/释放实例、修改实例配置、删除数据等。

原则 2：不要使用主账号进行日常运维管理操作

- 给员工 创建 RAM 用户账号 进行日常的运维管理操作。
- 为财务人员创建独立的 RAM 用户账号。
- 创建独立的 RAM 用户账号来作为 RAM 管理员。

原则 3：不要为主账号创建 AccessKey

AccessKey 与登录密码具有同样的特权，AccessKey 用于程序访问，登录密码用于控制台登录。由于 AccessKey 通常以明文形式保存在配置文件中，泄露的风险更高。

给所有的应用系统 配置 RAM 用户身份，并在 给 RAM 用户授权 时遵循最小授权原则。

原则 4：使用带 IP 限制条件的授权策略进行授权

授予所有的特权操作 必须受 IP 条件限制（acs:SourceIp）。

那么，即使 RAM 用户的登录密码或 AccessKey 泄露，只有攻击者没有渗透进入您的可信网络，那么攻击者也无能为力。

原则 5：使用带 MFA 限制条件的授权策略进行授权

授予所有的特权操作 必须受 MFA 条件限制（acs:MFAPresent）。

那么，即使 RAM 用户的登录密码或 AccessKey 泄露，只要 MFA 设备没有丢失，攻击者也无能为力。

更多限制条件，请参考 Policy 语法结构。

没有绝对的安全，只有最佳的实践。只有遵循最佳安全实践原则，综合利用这些保护机制，相信可以极大提高对您的账号资产的保护。

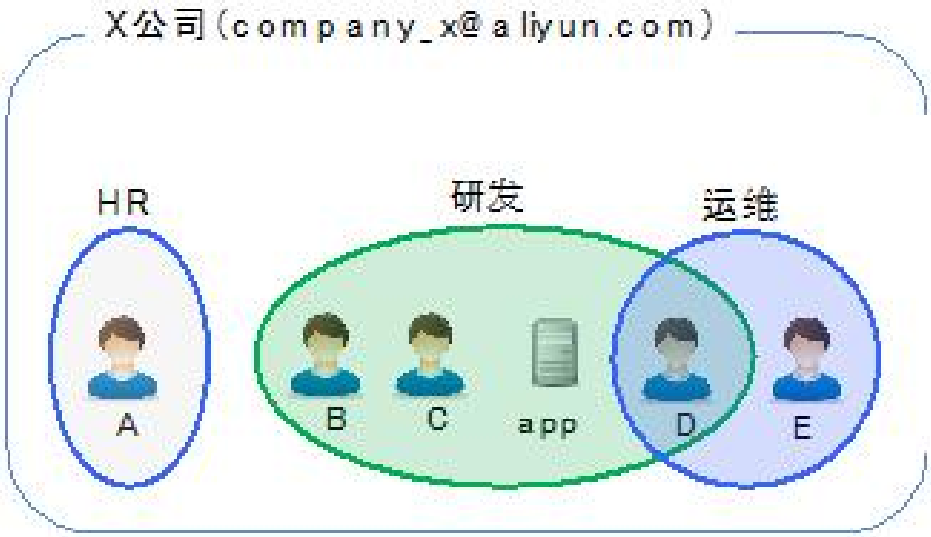
在创业之初，企业对云资源的安全管理要求不高，可以接受使用一个访问密钥(AccessKey)来操作所有资源。但随着时间推移，初创企业成长为大型的公司，或是大型企业客户迁移上云，他们的组织结构更加复杂，对云资源的安全管理需求非常强烈。

本文从企业管理者视角，以企业上云后面临严峻的资源访问控制需求出发，通过场景模拟，介绍如何通过 RAM 一步步建立安全完善的资源控制体系。

场景描述

假设您是 X 公司的管理者。当初您为 X 公司注册了云账号(company-x@aliyun.com)，并购买了基础设施服务 ECS、RDS 和 OSS。自从公司上云之后，业务发展迅猛，团队不断壮大，云资源越来越多。但是资源操作和管理都是使用一个大账号所带来的安全问题越来越突出。

假设 X 公司组织结构如下图所示。一共有 HR、研发和运维三个部门。HR 只能管人，研发人员只能使用资源，而运维人员可以管理资源（比如启停虚拟机）。



实践步骤

下面我们看看如何使用 RAM 来帮助您逐步实现对资源访问的安全管理。

第1步：给主账号开启多因素认证

考虑到之前您可能已经将主账号密码与他人分享，密码泄露的可能性较高。强烈建议您 给主账号开通多因素认证（Multi-Factor Authentication, MFA）。

阿里云账号支持标准的虚拟 MFA，它是一种可以安装在移动设备（如智能手机、智能手表）上的应用程序，使用起来非常方便。当您在账号中心启用虚拟 MFA 功能之后，在您登录阿里云平台时，除了校验用户名和密码（第一安全要素），系统还会要求您提供由虚拟 MFA 应用程序所产生的动态安全码（第二安全要素）。多重要素结合起来可以为您的账户提供更高的安全保护。

第2步：创建用户并给用户分组

根据上述的组织结构，您需要分别给员工 A、B、C、D、E 分别创建不同的 用户账号，再给应用 app 创建一个用户账号。然后创建三个 用户组 分别对应 HR、研发和运维组，再将不同用户添加到合适的组中去（注意用户 D 是同时属于研发组和运维组）。

进一步，根据不同用户的需要，分别为 在用户属性上设置登录密码或访问密钥。

- 对于应用 app 而言，它只可能通过 OpenAPI 访问云资源，所以只需要给它创建访问密钥即可。
- 而对于员工而言，如果只需要通过控制台操作云资源，那么就只给他设置登录密码即可。

再进一步，考虑到运维操作一般都是特别敏感，您可能会担心运维人员的账号密码泄露会带来巨大的风险，那么您可以 为这些账号设置登录时强制多因素认证，而且可以将账号密码和多因素认证设备交给不同的人员分开保管，这样可以做到必须两人同时在场时才能完成某些操作。

第3步：给不同用户组分配最小权限

RAM 提供了多种 系统授权策略模板 供您选择使用。比如，您需要给运维组授予对 ECS、RDS 的所有操作权限，给研发组授予对 ECS、RDS 的只读操作权限以及对 OSS的所有操作权限，给 HR 组授予对 RAM 用户管理操作权限。

如果您觉得 RAM 默认提供的系统授权策略模板对资源的控制粒度不够精细，那么您也可以在 RAM 中 自定义授权策略模板。自定义授权策略可以支持非常精细的访问控制粒度，比如精确定义 API 操作名称和资源实例名称；也可以支持多种条件限制操作表达式用于实现对资源操作方式的灵活控制，比如限制操作者的源 IP 地址。自定义授权策略可以满足用户对资源访问控制粒度的诸多苛刻需求，从而满足用户对“最小授权（只授予满足用户需要的最小权限）”的完美实施。

举个条件授权的例子，如果您担心研发人员密钥泄露而导致公司的 OSS 数据泄露到公司外部，那么您可以在给研发组授权访问 OSS 数据时附加限制条件，比如要求必须在公司（使用 acs:SourceIP 条件表达式）并且在上班时间段（使用acs:CurrentTime 条件表达式）才能操作 OSS 。

第4步：员工换岗、入职与离职的处理

当员工从一个岗位换到另一个岗位之后，您只需要将对应的用户账号从一个组移到另一个组，仅此而已。如果有员工入职，那么只需为新员工创建新的用户账号，设置登录密码或访问密钥，然后 添加到相应的用户组。如果是离职，那么只需在 RAM 控制台中执行用户删除操作即可，RAM 会自动删除用户的所有访问权限。

第5步：使用 STS 给临时用户授权

有时存在一些用户（人或应用程序），他们并不经常访问您的云资源，只是偶尔需要访问一次，我们称这些用户为“临时用户”。您可以通过 STS (Security Token Service，它是 RAM 的一个扩展授权服务) 来为这些用户颁发访问令牌。颁发令牌时，您可以根据需要来定义令牌的权限和自动过期时间。

使用 STS 访问令牌给临时用户授权的好处是让授权更加可控。您不必为临时用户创建一个 RAM 用户账号及密钥，因为 RAM 用户密钥都是长期有效的，但临时用户并不需要长期的资源访问。

此外，您也可以授权允许一个 RAM 用户使用 STS 服务颁发访问令牌，以实现对 RAM 用户的进一步分权。

第6步：让主账号“好好休息”

当您的员工和应用系统都开始使用 RAM 用户账号之后，您将不必再使用主账号去做日常工作了。为了降低主账号泄露的风险，建议您不要为主账号创建访问密钥，并且将主账号密码和多因素认证设备都放在公司的保险柜里，让它“好好休息”。

通过以上步骤，您可以体验到 RAM 丰富的资源控制能力，并可根据企业实际需求，制定适用的资源控制策略，协调好企业用户对上云资源的灵活访问控制。