访问控制

产品简介

产品简介

访问控制服务(RAM)简介

什么是RAM？

RAM (Resource Access Management) 是阿里云为客户提供的用户身份管理与访问控制服务。使用RAM，您可以创建、管理用户账号（比如员工、系统或应用程序），并可以控制这些用户账号对您名下资源具有的操作权限。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，从而降低您的企业信息安全风险。

RAM需求场景

- 企业子账号管理与分权

企业A购买了多种云资源（如ECS实例/RDS实例/SLB实例/OSS存储桶/...），A的员工需要操作这些云资源，比如有的负责购买，有的负责运维，还有的负责线上应用。由于每个员工的工作职责不一样，需要的权限也不一样。出于安全或信任的考虑，A不希望将云账号密钥直接透露给员工，而希望能给员工创建相应的用户账号。用户账号只能在授权的前提下操作资源，不需要对用户账号进行独立的计量计费，所有开销都算在A的头上。当然，A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。

- 不同企业之间的资源操作与授权管理

A和B代表不同的企业。A购买了多种云资源（如ECS实例/RDS实例/SLB实例/OSS存储桶/...）来开展业务。A希望能专注于业务系统，而将云资源运维监控管理等任务委托或授权给企业B。当然，企业B可以进一步将代运维任务分配给B的员工。B可以精细控制其员工对A的云资源操作权限。如果A和B的这种代运维合同终止，A随时可以撤销对B的授权。

- 针对不可信客户端App的临时授权管理

企业A开发了一款移动App，并购买了OSS服务。移动App需要上传数据到OSS（或从OSS下载数据），A不希望所有App都通过AppServer来进行数据中转，而希望让App能直连OSS上传/下载数据。由于移动App运行在用户自己的终端设备上，这些设备并不受A的控制。出于安全考虑，A不能将访问密钥保存到移动App中。A希望将安全风险控制到最小，比如，每个移动App直连OSS时都必须使用最小权限的访问令牌，而且访问时效也要很短（比如30分钟）。

RAM设计思路

RAM允许在一个云账号下创建并管理多个用户身份，并允许给单个身份或一组身份分配不同的授权策略(Policy)，从而实现不同用户拥有不同的云资源访问权限。

RAM用户身份是指任意的通过控制台或OpenAPI操作阿里云资源的人、系统或应用程序。为了支持多种应用场景的身份管理，RAM支持两种不同的用户身份类型：RAM-User和RAM-Role。 RAM-User是一种实体身份，有确定的身份ID和身份认证密钥，它通常与某个确定的人或应用程序一一对应。 RAM-Role是一种虚拟身份，有确定的身份ID，但没有确定的身份认证密钥。RAM-Role需要与某个实体身份进行关联之后才能被使用。一个RAM-Role可以与多种实体身份关联，比如可以与当前云账号下的RAM-User关联，与其它云账号下的RAM-User关联，与阿里云服务(EMR/MTS/...)关联，与外部实体身份（如企业本地账号）关联。

RAM允许在云账号下创建并管理多个授权策略，每个授权策略本质上是一组权限的集合。管理员可以将一个或多个授权策略分配给RAM用户（包括RAM-User和RAM-Role）。RAM授权策略语言可以表达精细的授权语义，可以指定对某个API-Action和Resource-ID授权，也可以支持多种限制条件（源IP、访问时间、多因素认证等）。

云账户 vs RAM用户

1. 从归属关系上看，云账户与RAM用户是一种主子关系。云账户是阿里云资源归属、资源使用计量计费的基本主体。RAM用户只能存在于某个云账户下的RAM实例中。RAM用户不拥有资源，在被授权操作时所创建的资源归属于主账户；RAM用户不拥有账单，被授权操作时所发生的费用也计入主账户账单。
2. 从权限角度看，云账户与RAM用户是一种root与user的关系（类比Linux系统）。Root对资源拥有一切操作控制权限，而user只能拥有被root所授予的某些权限，而且root在任何时刻都可以撤销user身上的权限。

RAM产品功能

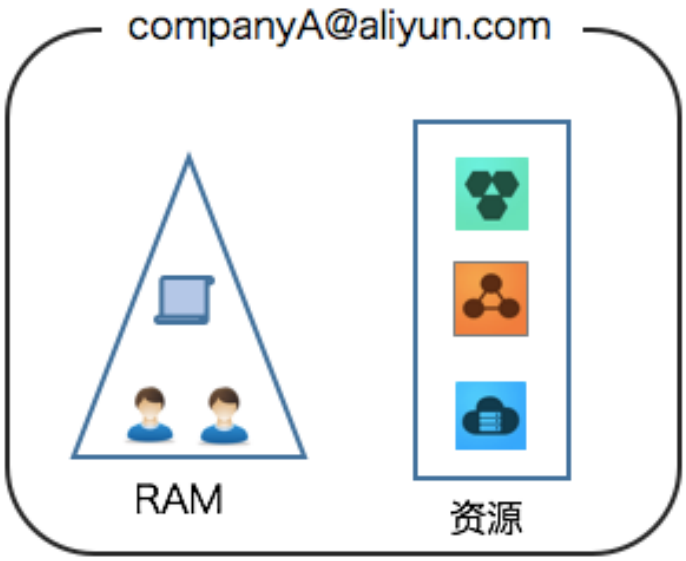
RAM包括下列功能：

- 集中控制RAM用户及其密钥 —— 可以在云账号下创建并管理用户及其访问密钥，并可以为用户绑定/解绑多因素认证设备
- 集中控制RAM用户的访问权限 —— 可以为每个用户或用户组绑定一个或多个授权策略，限制用户对指定资源的操作权限
- 集中控制RAM用户的资源访问方式 —— 可以要求用户必须使用安全信道（如SSL）、指定时间范围、以及在指定源IP条件下才能操作指定的云资源
- 集中控制RAM角色与外部账号的身份联盟管理 —— 可以使用RAM角色与外部身份系统（比如您的企业本地域账号、您的App用户账号）进行关联，满足直接使用外部身份登录到一个RAM角色身份访问阿里云控制台或API。
- 集中控制云资源 —— 可以对用户创建的实例或数据进行集中控制。当用户离开您的组织时，这些实例或数据仍然受您的完全控制。
- 统一账单 —— 云账户将收到包括所有RAM用户的资源操作所发生的费用的单一账单

RAM与企业级云资源管理

需求说明（如下图所示）：

- 您的企业只需使用一个云账号(比如companyA@aliyun.com)
- 所有资源都归属于该云账号的名下，云账号是资源的Owner（掌握完全控制权的人），也是账单的支付者
- 通过RAM为您名下的操作员（对资源进行运维管控操作）创建独立的用户账号并进行授权管理
- 用户账号不拥有资源（对其所创建的资源默认没有访问权限），只能操作被授权的资源
- 用户账号操作所发生费用都计入主账号名下，不支持用户账号的独立计量计费



适用具有如下特点的企业场景：

- 希望很简单就能管理每个操作人员（或应用）的账号及权限
- 不需要分别核算每个操作人员（或应用）的成本和费用

基本概念

云账户（主账户）

云账户是阿里云资源归属、资源使用计量计费的基本主体。当用户开始使用阿里云服务时，首先需要注册一个云账户。云账户为其名下所拥有的资源付费，并对其名下所有资源拥有完全权限。默认情况下，资源只能被属主（ResourceOwner）所访问，任何其他用户访问都需要获得属主的显式授权。所以从权限管理的角度来看

，云账户就是操作系统的 root 或 Administrator，所以我们有时称它为“**根账户**”或“**主账户**”。

云账户别名

每个云账户可以在 RAM 中为自己设置一个全局唯一的别名。别名主要用于 RAM 用户登录以及成功登录后的显示名。比如，云账号 admin@abc.com 为自己设置一个别名为 abc.com，那么其名下的 RAM 用户 alice 成功登录后，显示名就是 alice@abc.com。

RAM 用户

RAM 允许在一个云账户下创建多个 RAM 用户（可以对应企业内的员工、系统或应用程序）。RAM 用户不拥有资源，没有独立的计量计费，这些用户由所属云账户统一控制和付费。RAM 用户是归属于云账户，只能在所属云账户的空间下可见，而不是独立的云账户。RAM 用户必须在获得云账户的授权后才能登录控制台或使用 API 操作云账户下的资源。

RAM 用户有两种身份类型：**RAM-User** 和 **RAM-Role**。RAM-User 类型是一种实体身份类型，有确定的身份 ID 和身份凭证，它通常与某个确定的人或应用程序一一对应。RAM-Role 类型是一种虚拟身份类型，它没有确定的身份凭证，它必须关联到某个实体身份上才能使用。

RAM-Role 与 Textbook-Role（教科书式角色）的差异

i. （相同点）RAM-Role 和 Textbook-Role 都可以绑定一组权限集。
ii. （不同点）RAM-Role 是一种虚拟身份或影子账号，它有独立的身份 ID，除了绑定权限之外，还需要指定演员列表（Roleplayers），它主要用于解决与身份联盟（Identity Federation）相关的问题。Textbook-Role 通常只表示一组权限的集合，它不是身份，主要用于简化授权管理。

RAM-Role 的扮演与切换

i. 从登录身份切换到角色身份（SwitchRole）：一个实体用户（比如 RAM-User）登录到控制台后，可以选择“切换到某个角色”，前提是这个实体用户已经被关联了角色。每次只能切换进入某一种角色。当用户从“登录身份”进入“角色身份”时，用户只能使用“角色身份”上所绑定的权限，而“登录身份”上绑定的权限会被屏蔽。如果需要使用“登录身份”的权限，那么需要从“角色身份”切换回到“登录身份”。
ii. 从实体身份通过程序调用方式扮演角色（AssumeRole）：如果一个实体用户（比如 RAM-User）关联了某个 RAM-Role，那么该用户可以使用访问密钥（AccessKey）来调用 STS 服务的 AssumeRole 接口来获得这个 RAM-Role 的一个临时访问密钥。临时访问密钥有过期时间和受限制的访问权限（不会超过该角色所绑定的权限集），通常用于解决临时授权问题。

身份凭证（Credential）

身份凭证是用于证明用户真实身份的凭据，它通常是指登录密码或访问密钥（Access Key）。身份凭证是秘密

信息，用户必须保护好身份凭证的安全。

登录名/密码（Password）您可以使用登录名和密码登入阿里云控制台，查看订单、账单或购买资源，并通过控制台进行资源操作。

访问密钥（AccessKey）您可以使用访问密钥构造一个 API 请求（或者使用云服务 SDK）来操作资源。

多因素认证多因素认证（Multi-Factor Authentication, MFA）是一种简单有效的最佳安全实践方法，它能够在用户名和密码之外再额外增加一层安全保护。启用 MFA 后，用户登录阿里云网站时，系统将要求输入用户名和密码（第一安全要素），然后要求输入来自其MFA设备的可变验证码（第二安全要素）。这些多重要素结合起来将为您的账户提供更高的安全保护。

资源（Resource）

资源是云服务呈现给用户与之交互的对象实体的一种抽象，如 OSS 存储桶或对象，ECS 实例等。

我们为每个资源定义了一个全局的阿里云资源名称（Aliyun Resource Name, ARN）。格式如下：

```
acs:<service-name>:<region>:<account-id>:<resource-relative-id>
```

格式说明：

- acs: 它是 Alibaba Cloud Service 的首字母缩写，表示阿里云的公有云平台
- service-name: 阿里云提供的 Open Service 的名字，如 ecs, oss, odps 等
- region: 地区信息。如果不支持该项，可以使用通配符“*”号来代替
- account-id: 账号 ID，比如 1234567890123456
- resource-relative-id: 与 service 相关的资源描述部分，其语义由具体 service 指定。以 OSS 为例，” acs:oss::1234567890123456:sample_bucket/file1.txt” 表示公有云平台 OSS 资源，OSS 对象名称是 sample_bucket/file1.txt，对象的 Owner 是 1234567890123456。

权限（Permission）

权限是允许（Allow）或拒绝（Deny）一个用户对某种资源执行某种操作。

操作可以分为两大类：**资源管控操作**和**资源使用操作**。资源管控操作是指云资源的生命周期管理及运维管理操作，比如 ECS 的实例创建、停止、重启等，OSS 的 Bucket 创建、修改、删除等。资源使用操作是指使用资源的核心功能，比如 ECS 实例操作系统中的用户操作，OSS Bucket 的数据上传/下载。资源管控所面向的用户一般是资源购买者或您组织内的运维员工，资源使用所面向的用户则是您组织内的研发员工或应用系统。

对于弹性计算和数据库产品，资源管控操作可以通过 RAM 来管理，而资源使用操作是在每个产品的实例内进行管理，比如ECS 实例操作系统的权限控制，MySQL 数据库提供的权限控制。单对于存储类产品，如 OSS, Table Store等，资源管控操作和资源使用操作都可以通过 RAM 来管理。

授权策略（Policy）

授权策略是描述权限集的一种简单语言规范。RAM 支持的语言规范请参见 授权策略语言。

RAM 支持两种类型的授权策略：云平台管理的**系统访问策略**和客户管理的**自定义访问策略**。对于阿里云管理的系统访问策略，用户只能使用，不能修改，阿里云会自动完成系统访问策略的版本更新。对于客户管理的自定义访问策略，用户可以自主创建和删除，策略版本由客户自己维护。

应用场景

企业子账号管理与分权

场景概述：企业A购买了多种云资源（如ECS实例/RDS实例/SLB实例/OSS存储桶/...），A的员工需要操作这些云资源，比如有的负责购买，有的负责运维，还有的负责线上应用。由于每个员工的工作职责不一样，需要的权限也不一样。出于安全或信任的考虑，A不希望将云账号密钥直接透露给员工，而希望能给员工创建相应的用户账号。用户账号只能在授权的前提下操作资源，不需要对用户账号进行独立的计量计费，所有开销都算在A的头上。当然，A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。

不同企业之间的资源操作与授权管理

场景概述：A和B代表不同的企业。A购买了多种云资源（如ECS实例/RDS实例/SLB实例/OSS存储桶/...）来开展业务。A希望能专注于业务系统，而将云资源运维监控管理等任务委托或授权给企业B。当然，企业B可以进一步将代运维任务分配给B的员工。B可以精细控制其员工对A的云资源操作权限。如果A和B的这种代运维合同终止，A随时可以撤销对B的授权。

针对不可信客户端App的临时授权管理

场景概述：企业A开发了一款移动App，并购买了OSS服务。移动App需要上传数据到OSS（或从OSS下载数据），A不希望所有App都通过AppServer来进行数据中转，而希望让App能直连OSS上传/下载数据。由于移动App运行在用户自己的终端设备上，这些设备并不受A的控制。出于安全考虑，A不能将访问密钥保存到移动App中。A希望将安全风险控制到最小，比如，每个移动App直连OSS时都必须使用最小权限的访问令牌，而且访问时效也要很短（比如30分钟）。

支持RAM的云服务列表

所有阿里云服务都会与RAM集成。查阅目前支持哪些服务与RAM集成，请参考支持RAM的云服务