阿里云
访问控制

用户管理

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 RAM用户概览

RAM用户是RAM的一种实体身份类型，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。

- 一个云账号下可以创建多个RAM用户，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号统一控制和付费。
- RAM用户归属于云账号，只能在所属云账号的空间下可见，而不是独立的云账号。
- RAM用户必须在获得云账号的授权后才能登录控制台或使用API操作云账号下的资源。

当企业有多种云资源时，使用RAM的授权管理功能，可以实现用户分权及资源统一管理。详情请参见#unique_4。

2 创建 RAM 用户

RAM 用户是 RAM 中的一种身份。 RAM 用户对应某一个操作实体，如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. 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. 单击新建用户，输入登录名称和显示名称。

   
   说明:
   单击添加用户，可一次性创建多个 RAM 用户。
4. 在访问方式区域下，选择控制台密码登录或编程访问。
   - 控制台密码登录：可以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。
   - 编程访问：将会自动为 RAM 用户创建访问密钥（AccessKey）。RAM 用户可以通过 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。
5. 单击确认。

后续步骤

- 可以选择为用户添加到一个或多个组，对 RAM 用户进行分类并授权。详情请参考：#unique_6。
- 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。详情请参考：为 RAM 用户授权。

3 查看 RAM 用户基本信息

本文为您介绍如何查看 RAM 用户基本信息，包括用户名、显示名称和 UID 等信息。

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。
3. 在用户登录名称/显示名称列表下，单击目标 RAM 用户名称。
4. 在用户基本信息区域，可以查看用户基本信息。

4 修改 RAM 用户基本信息

本文为您介绍如何修改 RAM 用户基本信息，包括用户名和显示名称等信息。

操作步骤

1. 登录 RAM 控制台。
2. 单击人员管理 > 用户。
3. 在用户登录名称/显示名称列表下，单击目标 RAM 用户名称。
4. 在用户基本信息区域，单击编辑基本信息。
5. 修改完成后，单击确认。

5 为 RAM 用户授权

为 RAM 用户授权后，用户可以访问相应的阿里云资源。本文为您介绍如何为 RAM 用户授权。

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 RAM 用户名称或 ID 后，单击需要授权的 RAM 用户。

   说明:

   可以输入用户的 ID 或名称进行模糊搜索。
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。

6 为 RAM 用户移除权限

当 RAM 用户不再需要某些权限或离开组织时，可以将这些权限移除。本文为您介绍如何移除 RAM 用户的权限。

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 RAM 用户，单击移除授权。
4. 单击确认。

7 RAM用户登录控制台

本文为您介绍RAM用户如何登录RAM控制台，包括登录地址和登录方式。

操作步骤

1. RAM用户登录RAM控制台。

   > 说明:
   > 云账号登录RAM控制台，在概览页可以快速查询登录RAM用户登录地址。

2. 输入RAM用户登录名称，单击下一步。

   - 方式一：使用默认域名登录。RAM用户登录格式为`<$username>@<$AccountAlias>.onaliyun.com`，例如：username@company-alias.onaliyun.com。

     > 说明:
     > RAM用户登录账号为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用户登录密码，单击登录。

8 删除 RAM 用户

当不再需要某个 RAM 用户或 RAM 用户离开组织时，可以删除该 RAM 用户。删除 RAM 用户会删除对应的访问密钥，解绑多因素认证设备并撤销 RAM 用户拥有的权限。

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。
3. 在用户登录名称/显示名称列表下，找到目标 RAM 用户，单击删除。
4. 单击确认。

说明:

删除 RAM 用户需要谨慎操作。如果有业务系统正在以此用户身份运行，那么可能会导致客户的业务故障。

9 最佳实践

9.1 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。

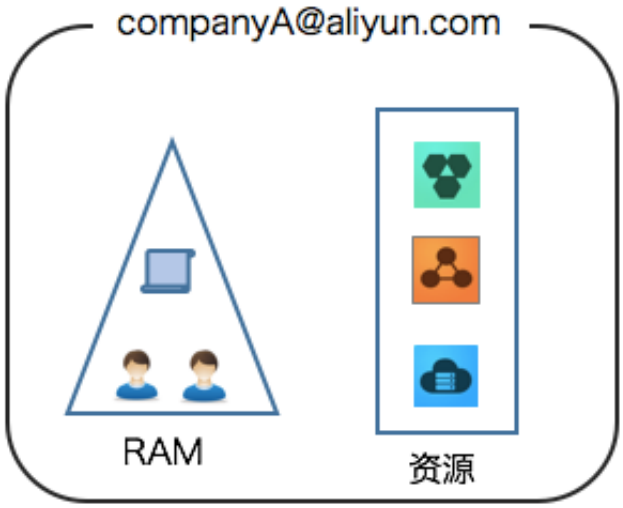
背景信息

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_15。

- 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_15。

- 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#unique_16。

- 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_17。

- 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_18。

- 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_19。

- 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_20。

- 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_21。

- 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_22。

- 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_23。

- 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_24。

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_25。

9.2 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

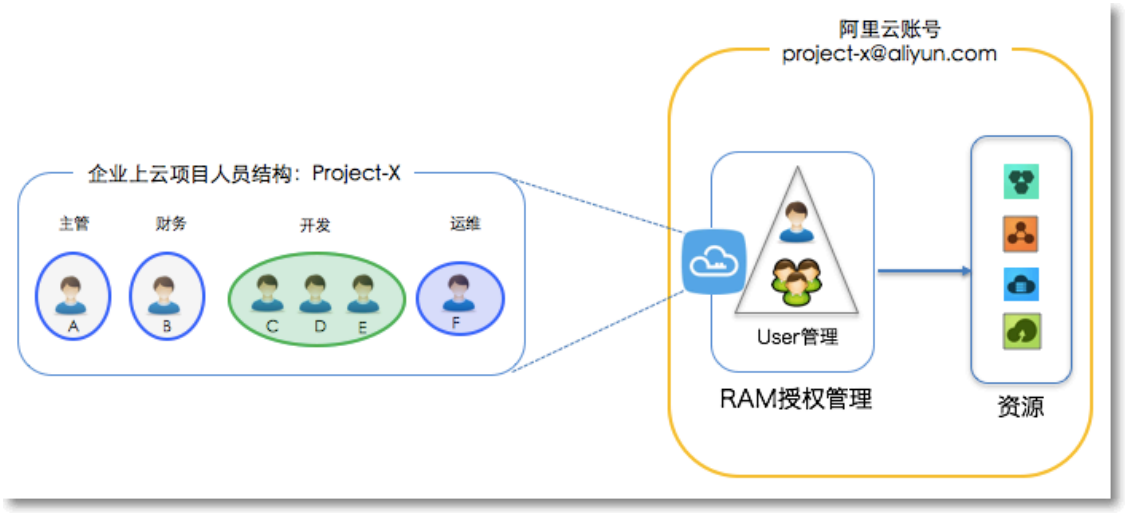
企业A的某个项目（Project-X）上云，购买了多种阿里云资源，例如：ECS实例、RDS实例、SLB实例和OSS存储空间等。项目里有多个员工需要操作这些云资源，由于每个员工的工作职责不同，需要的权限也不同。

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#unique_27。
- 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#unique_15。
- 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#unique_28。
- 为RAM用户或用户组添加一条或多条系统策略。详情请参见#unique_23或#unique_29。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#unique_30。
- 为不需要权限的RAM用户或用户组移除权限。详情请参见#unique_31或#unique_32。

10 常见问题

10.1 RAM用户常见问题

本文介绍了在使用RAM用户过程中的常见问题，包括登录、费用和权限等问题，为您提供说明和指导。

RAM用户登录地址在哪里?

RAM用户登录地址如下： RAM用户登录地址。

> 说明:
> 通过登录RAM控制台，在概览页可以快速查询登录RAM用户登录地址。当您使用此地址登录时，系统会为您自动填写默认域名，您只需补齐RAM用户名称即可。

RAM用户的登录有以下几种方式:

- 方式一：`<$username>@<$AccountAlias>.onaliyun.com`。例如：`username@company-alias.onaliyun.com`。

  > 说明:
  > RAM用户登录账号为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：`<$username>@<$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，格式为：`<$username>@<$DomainAlias>`。

  > 说明:
  > <$username>为RAM用户名称，<$DomainAlias>为域别名。

关于RAM用户的登录地址和登录方式，请参见#unique_35。

什么是默认域名、账号别名和域别名?

关于默认域名、账号别名和域别名的概念，请参见#unique_36。

- 使用云账号或具有RAM管理权限的RAM用户登录RAM控制台。
- 在左侧导航栏的人员管理菜单下，单击设置。
- 在高级设置页签下，可以查看并管理默认域名、账号别名和域别名。

RAM用户采购云产品需要什么权限?

- 如需采购按量付费的云产品，一般只需给RAM用户分配该产品的创建实例或类似权限即可。
- 如需采购包年包月的云产品，还需要额外授予支付订单的权限，即授予用户`AliyunBSSOrderAccess`的权限策略。
- 有些产品在购买时需要连带使用或创建多种资源，这种情况下需要RAM用户具备相应资源的读取或创建权限。

  以下以创建ECS实例为例，说明具体需要的权限。

  如下权限策略表示RAM用户具有从控制台、使用API或从实例启动模板创建ECS实例的能力：

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "ecs:DescribeLaunchTemplates",
        "ecs:CreateInstance",
        "ecs:RunInstances",
        "ecs:DescribeInstances",
        "ecs:DescribeImages",
        "ecs:DescribeSecurityGroups"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "vpc:DescribeVpcs",
        "vpc:DescribeVSwitches"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

  如果需要RAM用户在创建ECS实例过程中使用或创建其他资源，根据资源类型不同，还需要授予以下各类权限。

  说明：

  - 关于如何创建自定义策略，请参见#unique_17。

- 关于如何为RAM用户授权，请参见为 RAM 用户授权。

操作	权限策略
使用快照创建ECS实例	ecs:DescribeSnapshots
同时创建并使用新的VPC	- vpc:CreateVpc - vpc:CreateVSwitch
同时创建并使用新的安全组	- ecs:CreateSecurityGroup - ecs:AuthorizeSecurityGroup
指定实例角色	- ecs:DescribeInstanceRamRole - ram:ListRoles - ram:PassRole
使用Keypair	- ecs:CreateKeyPair - ecs:DescribeKeyPairs
在专有宿主机上创建ECS实例	ecs:AllocateDedicatedHosts

为什么RAM用户被授权后依然无访问权限?

- 请确认RAM用户的权限策略是否正确。
- 请检查RAM用户的自定义策略（个人权限策略、加入用户组的权限策略）是否对相关资源或操作设置了"Effect": "Deny"。

  例如：RAM用户拥有只读访问云服务器ECS的权限：AliyunECSReadOnlyAccess ，但如果同时也拥有如下权限策略：

```
{
  "Statement": [
    {
      "Action": "ecs:*",
      "Effect": "Deny",
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

说明:

根据RAM的Deny优先原则，该RAM用户不可以查看ECS资源。

为什么RAM用户没有权限仍然可以操作?

例如：RAM用户没有ECS的`FullAccess`或者`ReadOnly`系统策略，也没有添加任何自定义策略，但可以查看实例列表。

- 请检查RAM用户所在的用户组权限策略中是否存在允许RAM用户操作的相应权限。
- 请确认当前已经被授权给RAM用户的其他权限策略中是否包含了相关权限。

  例如：云监控的系统权限策略为`AliyunCloudMonitorFullAccess`，此权限包括查看ECS实例列表的权限：`"ecs:DescribeInstances"`，查看RDS实例列表的权限：`"rds:DescribeDBInstances"`和查看SLB实例列表的权限`"slb:DescribeLoadBalancer"`等。当`AliyunCloudMonitorFullAccess`被授权给RAM用户后，该RAM用户便有权限查看ECS、RDS和SLB等产品的实例信息。

怎样授权RAM用户单独管理续费?

目前续费管理没有统一的权限策略，需要根据具体产品自定义权限策略。一般需要授权给RAM用户购买该产品所需要的权限以及支付订单的权限。

例如：RAM用户进行ECS的续费管理所需权限，请参见RAM用户采购云产品需要什么权限?给RAM用户授权，同时需要授予`AliyunBSSOrderAccess`权限策略。

RAM用户使用资源所产生的费用怎么计算?

- RAM用户使用资源所产生的费用由其所属的云账号承担。
- RAM用户可以自动享有云账号享有的折扣，无需特殊设置。
- 消费额度、信用额度和独立付款方式等财务相关属性均为云账号内的全局设置，影响所有RAM用户。不支持为某个RAM用户单独设置。
- RAM用户可以被授权进行充值操作，充值后的金额归属于云账号。
- RAM用户或RAM用户集合不能作为独立的财务单元出账单。 若有云账号内的分账需求，请提交工单由售后人员提供解决方案。