

阿里云 访问控制

用户指南

文档版本：20180929

法律声明

阿里云提醒您在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 。
<code>courier</code> 字体	命令。	执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid Instance_ID</code>
[]或者[a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ }或者{a b}	表示必选项，至多选择一个。	<code>swich {stand slave}</code>

目录

法律声明.....	I
通用约定.....	I
1 身份管理.....	1
1.1 用户.....	1
1.2 组.....	5
1.3 角色.....	6
2 授权管理.....	18
2.1 权限与授权策略.....	18
2.2 授权策略管理.....	19
2.3 授权.....	24
2.4 操作资源.....	26
3 云产品授权.....	28

1 身份管理

1.1 用户

用户，是 RAM 中的一种身份；它对应某一个操作实体，如操作员或应用程序。如果有新的用户或应用程序访问您的云资源，您需要创建 RAM 用户并授权其访问相关资源。一般操作步骤如下：

1. 使用云账号（或拥有 RAM 操作权限的 RAM 用户）登录到 RAM 控制台。
2. 创建 RAM 用户，并将此用户添加到一个或多个组。
3. 为用户（或其所属的组）添加一个或多个授权策略。
4. 设置用户密钥。如果用户是通过控制台进行操作，则需为用户设置登录密码；如果用户是通过 API 进行调用，则需为用户创建 API 访问密钥（AccessKey）。
5. 如果用户需要使用特权操作（如停止虚拟机），那么可以为用户设置多因素认证（MFA），并要求用户必须使用 MFA 口令才能登录到阿里云控制台。
6. 向用户提供登录 URL、用户名及密码。

基本设置

- [设置企业别名](#)
- [设置密码策略](#)
- [设置登录限制](#)

设置企业别名

1. 在 RAM 控制台选择设置 > 企业别名设置 > 编辑企业别名。
2. 输入企业别名，并单击确定。

设置密码策略

操作步骤如下：

1. 在 RAM 控制台选择设置 > 密码强度设置。
2. 按照页面提示，配置密码长度、字符格式、有效期、重试约束策略等规则，然后单击保存修改，使规则生效。



说明：

一旦设置成功，此密码策略适用于所有 RAM 用户。

设置登录限制

1. 在RAM控制台选择设置 > 子用户安全设置。
2. 在子用户安全设置子页，配置相关参数。
3. 单击保存修改。

创建 RAM 用户

操作步骤如下：

1. 在RAM控制台选择 用户管理 > 新建用户。
2. 按照页面提示，输入用户信息，然后单击确定。

创建 RAM 用户后，您可以根据使用需求执行如下操作：

- [设置登录密码](#)
- [创建访问密钥#AK#](#)
- [设置 MFA](#)

设置登录密码

为需要通过控制台进行操作的用户设置登录密码，操作步骤如下：

1. 在RAM控制台用户管理页面，找到需要设置登录密码的用户（可使用用户名进行模糊查询），然后单击其用户名或其操作列下的管理按钮。
2. 在用户详情页面，单击启用控制台登录。

图 1-1: 设置登录密码



3. 在弹出的对话框中，为用户设置初始密码，并可以指定用户下次登录成功后必须更换密码。

创建访问密钥 (AK)

为需要通过 API 进行调用的用户创建访问密钥 (AK)，操作步骤如下：

1. 在RAM控制台用户管理页面，找到需要创建 AccessKey 的用户（可使用用户名进行模糊查询），然后单击其用户名或其操作列下的管理按钮。
2. 在用户详情页面，单击创建 AccessKey。

3. 在弹出的对话框中，查看新建的 AK 信息，并可选择保存 AK 信息。



说明：

- AK 信息只会在创建时显示，请您妥善保管。为安全起见，RAM 不提供 AK 信息查询。
- 如果 AK 泄露或丢失，则需要创建新的 AK。

设置 MFA

多因素认证 (Multi-Factor Authentication, MFA) 是一种简单有效的最佳安全实践，它能够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，系统将要求输入用户名和密码 (第一安全要素)，然后要求输入来自其虚拟 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。

虚拟 MFA 设备是产生一个 6 位数字验证码的应用程序，它遵循基于时间的一次性密码 (TOTP) 标准 ([RFC 6238](#))。此应用程序可在移动硬件设备上运行 (例如智能手机)。

设置 MFA 的操作步骤如下：

1. 在 RAM 控制台用户管理页面，找到需要创建 AccessKey 的用户 (可使用用户名进行模糊查询)，然后单击其用户名或其操作列下的管理按钮。
2. 在用户详情页面，单击启用虚拟 MFA 设备，启动 [设置 MFA#可选#](#) 流程。

图 1-2: 设置 MFA

多因素认证设备			
类型	简介	启用状态	操作
虚拟 MFA 设备	遵循 TOTP 标准算法来产生 6 位数字验证码的应用程序	未启用	启用虚拟 MFA 设备

RAM 用户登录

登录入口

RAM 用户和云账号的登录入口不同，RAM 用户不能通过云账户登录页面进行登录。

请登录 RAM 控制台在概览子页查询登录链接)。

登录信息

RAM 用户登录需提供企业别名、子用户名称和密码。

其中，企业别名就是您在 RAM 初始设置 中设置的企业别名。如果没有设置企业别名，默认的企业别名就是您的云账号 ID（可在账号管理 > 安全设置中查询）。



说明：

RAM 用户默认是没有任何访问权限的。如果没有被授权，即使能登入控制台，也无法进行任何操作。关于如何为 RAM 用户授权，请参考[授权](#)。

删除 RAM 用户



说明：

删除用户需要谨慎操作！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。

操作步骤如下：

1. 在RAM控制台单击左侧的用户管理，进入用户管理页面。
2. 找到您要删除的RAM用户，在对应的操作区域单击删除。

图 1-3: 删除RAM用户

用户名/显示名	备注	创建时间	操作
[Redacted]		2017-12-28 14:54:35	管理 授权 删除 加入组

3. 在弹出的删除用户对话框中，勾选关联删除子用户AccessKey并撤销子用户权限复选框，然后单击确定按钮。

图 1-4: 确认删除



1.2 组

对云账号下有多个 RAM 用户的情况，建议您通过创建群组对职责相同的 RAM 用户进行分类并[授权](#)，从而更好的管理用户及其权限。这样做的好处是：

- 在具体用户职责发生变化时，只需将其移动到相应职责的群组下，不会对其他用户产生影响。
- 当群组的权限发生变化时，只需修改群组的授权策略，即可应用到所有用户身上。

本文主要介绍如下操作流程：

- [创建群组](#)
- [管理组成员](#)
- [重命名群组](#)
- [删除群组](#)
- [为群组授权](#)

创建群组

操作步骤如下：

1. 在[RAM控制台首页](#)选择群组管理 > 新建群组。
2. 输入群组名称，并单击确定。

管理组成员

操作步骤如下：

1. 在[RAM控制台首页](#)单击 群组管理。
2. 进入群组管理页面，单击操作列下的管理，可以管理组成员。
 - 添加组成员：
 1. 在群组列表中找到要管理的群组（可使用组名称进行模糊查询），单击其操作列下的编辑组成员。
 2. 从左列中选择要添加到组中的用户（可使用关键字查询），单击向右箭头将其添加到右侧已选列下；选择右侧已选列下的用户，单击向左箭头可撤销选择。
 3. 选择完成后单击确定。
 - 删除组成员：
 1. 在群组列表中找到要管理的群组（可使用组名称进行模糊查询），单击群组名称。

2. 在组成员管理区域，单击要删除用户的操作列下的移除出组按钮，可将其从当前群组中删除。

重命名群组

操作步骤如下：

1. 在[RAM控制台首页](#)单击群组管理。
2. 在群组列表中找到要重命名的群组（可使用组名称进行模糊查询），单击其组名称或其操作列下的管理，进入群组详情页面。
3. 单击编辑基本信息。
4. 输入组名称并点击确定。

删除群组

操作步骤如下：

1. 在[RAM控制台首页](#)单击群组管理。
2. 在群组列表中找到要删除的群组（可使用组名称进行模糊查询），单击其操作列下的删除。



说明：

如果群组中包含组成员或者有绑定的授权策略，则需选中强制解除关联关系后才能删除群组。

为群组授权

关于如何为群组授权，请参考[授权](#)。

1.3 角色

角色，与用户一样，都是 RAM 中使用的身份。与 RAM 用户相比，RAM 角色是一种虚拟用户，它没有确定的身份认证密钥，且需要被一个受信的实体用户扮演才能正常使用。

本文详细解释了角色的[概念](#)和[应用场景](#)，帮助您正确理解；也介绍了 RAM 角色的[类型](#)、[创建方法](#)和[使用方法](#)，指导您正确实践。



说明：

如果没有特别说明，文中出现的角色都是指 RAM 角色。

理解 RAM 角色

RAM 角色 (RAM-Role) 是一种虚拟用户 (或影子账号)，它是 RAM 用户类型的一种。

图 1-5: RAM角色



- RAM 角色不同于教科书式角色 (Textbook-Role)。教科书式角色 (或传统意义上的角色) 是指一组权限集合, 类似于 RAM 里的授权策略 (Policy)。如果一个用户被赋予了这种角色, 也就意味着该用户被赋予了一组权限, 然后该用户就能访问被授权的资源。
- RAM 角色作为虚拟用户, 它有确定的身份, 可以被赋予一组授权策略 (Policy), 但它没有确定的身份认证密钥 (登录密码或 AccessKey)。

虚拟用户 vs 实体用户: 虚拟用户与实体用户的区别在于是否能被直接身份认证:

- 实体用户拥有确定的登录密码或 AccessKey, 比如云账号、RAM-User 账号、云服务账号。
- 虚拟用户没有确定的认证密钥, 比如 RAM-Role。
- 相比于 RAM 用户, 在使用方法上 RAM 角色需要被一个授信的实体用户扮演, 扮演成功后实体用户将获得 RAM 角色的临时安全令牌, 使用这个临时安全令牌就能以角色身份访问被授权的资源。

使用须知

RAM-Role 必须与一种实体用户身份联合起来才能使用。

图 1-6: 使用RAM角色



- 如果一个实体用户要想使用被赋予的某个 RAM 角色，实体用户必须先以自己身份登录，然后执行 切换到角色 操作将自己从 实体身份 切换到 角色身份。



说明：

当切换到角色身份后，将只能执行该角色身份被授权的所有操作，而登录时实体身份所对应的访问权限被隐藏。

- 如果用户希望从 角色身份 回到 实体身份，那么只需执行 切回登录身份 操作。



说明：

此时将拥有实体身份所对应的访问权限，而不再拥有角色身份所拥有的权限。

相关概念

与 RAM 角色相关的概念间关系释义如下图所示：

图 1-7: RAM角色相关概念



相关概念的具体释义见下表：

名称	释义
RoleARN	<p>RoleARN 是角色的全局资源描述符，用来指定具体角色。</p> <ul style="list-style-type: none"> RoleARN 遵循阿里云 ARN 的命名规范。比如，某个云账号下的 devops 角色的 ARN 为：<code>acs:ram::1234567890123456:role/samplerole</code>。 创建角色后，可在其角色详情页查看其 Arn。
受信演员	<p>角色的受信演员是指可以扮演角色的实体用户身份。</p> <ul style="list-style-type: none"> 创建角色时必须指定受信演员，角色只能被受信的演员扮演。 受信演员可以是受信的云账号，或者受信服务。

名称	释义
授权策略	一个角色可以绑定一组授权策略 (Policy)。没有绑定授权策略的角色也可以存在,但不能使用。
扮演角色	扮演角色 (AssumeRole) 是实体用户获取角色身份的安全令牌的方法。一个实体用户通过调用 AssumeRole 的 API 可以获得角色的安全令牌,使用安全令牌可以访问云服务 API。
切换身份	切换身份 (SwitchRole) 是在控制台中实体用户从当前登录身份切换到角色身份的方法。 <ul style="list-style-type: none"> 一个实体用户登录到控制台之后,可以切换到被许可扮演的某一种角色身份,然后以角色身份操作云资源。切换到角色身份后,原实体用户身份的访问权限将被屏蔽。 用户不需要使用角色身份时,可以从角色身份切换回原来的登录身份。
角色令牌	角色令牌是角色身份的一种临时访问密钥。角色身份没有确定的访问密钥,当一个实体用户要使用角色时,必须通过扮演角色来获取对应的角色令牌,然后使用角色令牌来调用阿里云服务 API。

RAM 角色应用场景

RAM 角色主要用于解决委托其他云账号及其下 RAM 用户操作您所控制的资源、委托云服务操作您所控制的资源。

跨账号的资源操作与授权管理

场景概述：企业 A 和企业 B 代表不同的企业。企业 A 购买了多种云资源 (如 ECS 实例/ RDS 实例/ SLB 实例/ OSS 存储空间/...) 来开展业务。

需求说明	解决方案
企业 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。	云账号 A 在 RAM 中创建一个角色,给角色授予合适的权限,并允许云账号 B 使用该角色。

需求说明	解决方案
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。	如果云账号 B 下的某个员工 (RAM 用户) 需要使用该角色, 那么云账号 B 可以自主进行授权控制。代运维操作时, 账号 B 下的 RAM 用户将使用被授予的角色身份来操作账号 A 的资源。
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。	如果账号 A 与账号 B 的合作终止, A 只需要撤销账号 B 对该角色的使用。一旦账号 B 对该角色的使用权限被撤销, 那么 B 下的所有 RAM 用户对该角色的使用权限将被自动撤销。

临时授权移动 app 客户端直接操作您所控制的资源

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); 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。

需求说明	解决方案
企业 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。	<ul style="list-style-type: none"> 云账号 A 在 RAM 中创建一个角色, 给角色授予合适的权限, 并允许 appServer (以 RAM 用户身份运行) 使用该角色。 当 app 需要直连 OSS 上传/下载数据时, appServer 可以使用角色, 获取角色的一个临时安全令牌并传送给 app, app 就可以使用临时安全令牌直接访问 OSS API。
企业 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)。	如果需要更精细地控制每个 app 的权限, appServer 可以在使用角色时进一步限制临时安全令牌的资源操作权限, 比如, 不同 app 用户只能操作不同的子目录, 那么 appServer 在使用角色时就可以进行这种限制。

委托云服务操作您的云资源

场景概述: 企业 A 购买了云服务器 ECS, 并在其中部署了一款应用程序; 应用程序需要访问 A 的 OSS 存储空间。通常情况下,

- 云账号 A 要将其 AccessKey (AK) 保存在应用程序的配置文件中, 并在定期更换 AK 时修改应用程序的配置文件。

- 在进行多地域一致性部署时，AK 会随镜像以及使用镜像创建的实例扩散出去；这种情况下，当 A 需要更换 AK 时，就需要逐台更新和重新部署实例与镜像。

需求说明	解决方案
<ul style="list-style-type: none"> 安全性考虑，A 不希望其应用程序通过 AK 取得其 API 操作的完整权限，希望应用程序以临时凭证访问其他产品的 API。 操作性考虑，A 不希望在应用程序端更新 AK，也不希望在多地域维护 AK。 	<p>使用 RAM 服务角色：</p> <ul style="list-style-type: none"> 云账号 A 在 RAM 中创建一个 ECS 服务角色（只允许 ECS 实例扮演），给角色授予合适的权限（如 OSS 的只读权限），并将该服务角色关联其 ECS 实例。 在连接 ECS 实例后，通过访问 ECS 实例元数据获取服务角色的 STS 临时身份凭证；ECS 中的应用程序使用该临时身份凭证访问 OSS。



说明：

其他场景如授权 EMR 操作客户的 ECS，函数计算 FC 操作客户的 OSS，媒体转码 MTS 操作用户的 OSS 数据等需要跨产品相互调用的场景，都可使用 RAM 服务角色授权操作。参考 [创建服务角色](#) 查看 RAM 提供的所有服务角色类型及场景。

关于RAM的PassRole权限

为了限制一个服务能代表你做什么操作，你需要给这个服务配置一个RAM角色，该服务将会以对应RAM角色的身份去执行相关操作，并且受限于管理员对RAM角色的授权。比如，你可以给ECS实例配置一个RAM角色，ECS实例里的应用程序就能获取对应RAM角色的身份令牌去访问阿里云服务API。

当一个RAM用户为云服务配置RAM角色时，这个RAM用户必须要拥有对该RAM角色的PassRole权限。云服务在收到RAM角色配置的请求时，会强制检查RAM用户是否拥有指定RoleArn的 ram:PassRole 权限。这样做能确保只有被授权用户才能为云服务配置RAM角色，而不会导致RAM角色的权限被滥用。

RAM 角色类型

RAM 支持以下两种类型的角色：

- 用户角色：**允许 RAM 用户所扮演的角色。扮演角色的 RAM 用户可以属于自己云账号，也可以是属于其他云账号。用户角色主要用来解决跨账号访问和临时授权问题。
- 服务角色：**允许云服务所扮演的角色。服务角色主要用于授权云服务代理您进行资源操作。

创建 RAM 角色

通过RAM 控制台来创建 RAM 角色包含以下步骤：

1. 选择角色类型
2. 选择受信的演员身份
3. 填写角色名称
4. 给角色绑定授权策略

创建用户角色

操作步骤如下：

1. 登录到[RAM 控制台](#)。
2. 在左侧导航栏单击角色管理。
3. 单击右上角新建角色。
4. 在选择角色类型子页，单击用户角色。
5. 在填写类型信息子页，选择受信云账号，如下图所示：

图 1-8: 填写类型信息

- 若创建的角色是给您自己名下的 RAM 用户使用（比如授权移动 app 客户端直接操作 OSS 资源），请选择当前云账号为受信云账号。
- 若创建的角色是给其他云账号名下的 RAM 用户使用（比如跨账号的资源授权），请选择其他云账号，并在受信云账号 ID 中填写其他云账号的 ID。

6. 在配置角色基本信息子页，输入角色名称和备注后，单击 **创建**。
7. 创建成功。成功创建角色后，角色没有任何权限，单击**授权**可直接为该角色授权（**编辑授权策略**），授权方法请参考**授权**。

至此，您已完成用户角色的创建。

返回 RAM 控制台，在角色管理页面找到新创建的角色（可使用角色名进行模糊查询），单击其角色名称或其对应操作列下的**管理**，可以查看相应的角色详情，如下图所示：

图 1-9: 角色基本信息



创建服务角色

操作步骤如下：

1. 在RAM控制台左侧导航栏单击**角色管理**。
2. 单击右上角**新建角色**。
3. 在选择角色类型子页，单击**服务角色**。可用的服务角色包括：
 - MTS 多媒体转码服务，用于将 OSS Bucket 设置为 MTS 任务的数据源时，创建以 MTS 为受信服务的角色，并使用 MTS 服务扮演该角色访问 OSS 中的数据。
 - OAS 归档存储服务，用于将 OSS Bucket 设置为归档存储服务的数据源时，创建以归档存储为受信服务的角色，并使用归档存储服务扮演该角色访问 OSS 中的数据
 - LOG 日志服务，用于将日志服务收集的日志导入 OSS 时，创建以日志服务为受信服务的角色，并使用日志服务扮演该角色将数据写入 OSS。

- ApiGateway API 网关服务，用于将函数服务设置为 API 网关的后端服务时，创建以 API 网关服务为受信服务的角色，并使用 API 网关扮演该角色调用函数服务。
 - ECS 云服务器，用于授权 ECS 服务访问您在其他云服务中的云资源。
4. 在填写类型信息子页，选择受信服务。
 5. 在配置角色基本信息子页，输入角色名称和备注后，单击创建。
 6. 创建成功。成功创建角色后，角色没有任何权限，单击授权可直接为该角色授权（编辑授权策略），授权方法请参考[授权](#)。

至此，您已完成服务角色的创建。

返回 RAM 控制台，在角色管理页面找到新创建的角色（可使用角色名进行模糊查询），单击其角色名称或其对应操作列下的管理，可以查看相应的角色详情。

使用 RAM 角色

RAM 角色需通过 RAM 用户身份来扮演（**AssumeRole**）使用，不允许受信云账号以自己身份扮演角色。因此，受信云账号必须通过创建一个 RAM 用户账号，并授予该 RAM 用户账号的 AssumeRole 权限，然后以 RAM 用户身份去扮演角色。

操作步骤：

1. 创建一个 RAM 用户，并为该用户创建 AccessKey 或设置登录密码。
2. 给该 RAM 用户授权，授权时添加系统授权策略：AliyunSTSAssumeRoleAccess。

操作控制台

使用角色身份进行控制台操作的步骤如下：

1. RAM 用户登录控制台。
2. 在右上角账号菜单下，选择切换身份。

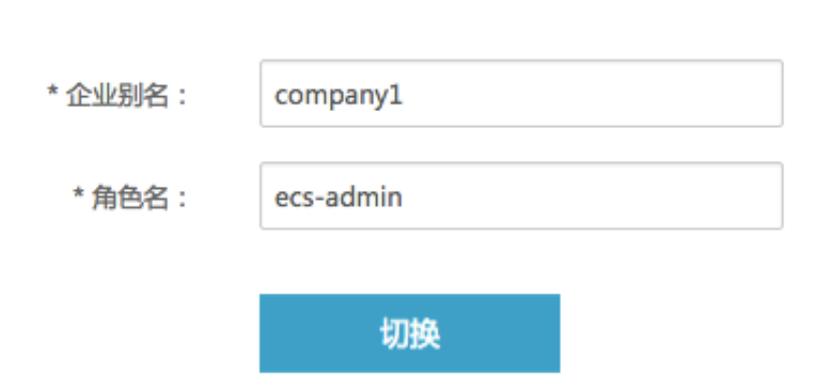
例如，company2（企业别名）下的 RAM 用户 zhangsan 登录控制台之后，控制台右上角会显示该用户的身份信息，如下图所示：

图 1-10: 身份信息



单击切换身份，进入角色切换的页面，选择相应的企业别名和角色名（假设当前用户已被授权允许扮演 company1（企业别名）下的 ecs-admin 角色），单击切换。

图 1-11: 切换角色



切换成功后，将以角色身份访问控制台。此时控制台右上角将显示角色身份（即当前身份）和登录身份。

图 1-12: 角色切换成功



3. 在扮演角色身份时，选择 返回登录身份可以切换回登录身份。

访问云服务 API

当 RAM 用户被授予 AssumeRole 权限之后，可以使用其 AccessKey 调用安全令牌服务(STS) 的 AssumeRole 接口，以获取某个角色的临时安全令牌。关于 AssumeRole API 的调用方法，请参考 [AssumeRole](#)。

2 授权管理

2.1 权限与授权策略

阿里云使用权限来描述内部身份（如用户、用户组、角色）对具体资源的访问能力。权限指在某种条件下允许 (**Allow**) 或拒绝 (**Deny**) 对某些资源执行某些操作。权限的载体是授权策略，授权策略是一组访问权限的集合。

本文梳理了阿里云权限与授权策略的相关属性，帮助您正确理解和使用它们。

权限

- 主账户（资源 Owner）控制所有权限
 - 每个资源有且仅有一个属主（资源 Owner）。该属主必须是云账户，是对资源付费的人，对资源拥有完全控制权限。
 - 资源属主不一定是资源创建者。比如，一个 RAM 用户被授予创建资源的权限，该用户创建的资源归属于主账户，该用户是资源创建者但不是资源属主。
- RAM 用户（操作员）默认无任何权限
 - RAM 用户代表的是操作员，其所有操作都需被显式授权。
 - 新建 RAM 用户默认没有任何操作权限，只有在被授权之后，才能通过控制台和 API 操作资源。
- 资源创建者（RAM 用户）不会自动拥有对所创建资源的任何权限
 - 如果 RAM 用户被授予创建资源的权限，用户将可以创建资源。
 - 但是 RAM 用户不会自动拥有对所创建资源的任何权限，除非资源 Owner 对他有显式的授权。

授权策略

授权策略（Policy）是用 [Policy语法结构](#) 所描述的一组权限，它可以精确地描述被授权的资源集、操作集以及授权条件。当授权策略中既有 Allow 又有 Deny 的授权语句时，遵循 **Deny** 优先的原则。

在 RAM 中，访问策略是一种资源实体，用户可以创建、更新、删除和查看访问策略。RAM 支持以下两种授权策略：

- **系统访问策略**：由阿里云创建和管理的一组常用的权限集，比如对 ECS 的只读权限、对 ECS 的完全权限等；用户只能使用而不能修改。
- **自定义访问策略**：由用户自己创建和管理的权限集，是对系统访问策略的扩展和补充。

系统访问策略所描述的权限粒度较粗，如果用户需要更精细的授权描述，比如精确控制对某个 ECS 实例的权限或添加授权条件限制，则需要用户创建自定义授权策略。

给 RAM 用户授权

给 RAM 用户授权，指给用户、用户组或角色绑定一个或多个授权策略。

- 绑定的授权策略可以是系统授权策略也可以是自定义授权策略。
- 如果绑定的授权策略被更新，更新后的授权策略自动生效，无需重新绑定授权策略。

2.2 授权策略管理

授权策略是一组权限的集合，它以阿里云定义的 **Policy 基本元素** 来描述。通过给用户或群组附加授权策略，用户或群组中的所有用户就能获得授权策略中指定的访问权限。

RAM 支持两种类型的授权策略：**系统授权策略**和 **自定义授权策略**。本文系统介绍了授权策略的管理方法，具体包括：[查看](#)系统授权策略，以及[创建](#)、[修改](#)和[删除](#)自定义授权策略。

系统授权策略

系统授权策略是阿里云提供的一组通用授权策略，主要针对不同产品的 **只读权限** 或 **所有权限**。对于阿里云提供的这组授权策略，

- 用户只能用于授权，而不能编辑和修改。
- 阿里云会自动进行更新或修改。

查看系统授权策略

如果要查看阿里云支持的所有系统授权策略，请登录到 RAM控制台，并进入授权策略管理页面，在系统授权策略子页下，通过系统授权策略列表查看或搜索。

自定义授权策略

由于系统授权策略的授权粒度比较粗，如果这种粗粒度授权策略不能满足您的需要，那么您可以创建自定义授权策略。比如，您想控制对某个具体的 ECS 实例的操作权限，或者您要求访问者的资源操作请求必须来自于指定的 IP 地址，您必须使用自定义授权策略才能满足这种细粒度要求。

应用场景

如果您有更细粒度的授权需求，比如授权用户 bob 只能对 `oss://sample_bucket/bob/` 下的所有对象执行只读操作，而且限制 IP 来源必须为您的公司网络 (通过搜索引擎查询“我的IP”可以获知您的公司网络 IP 地址)，那么您可以通过创建自定义授权策略来进行访问控制。

创建自定义授权策略

在创建自定义授权策略时，您需要了解授权策略语言的基本结构和语法，相关内容的详细描述请参考 [Policy 语法结构](#)。

操作步骤

在了解授权策略语言之后，您通过 RAM 控制台可以很方便地创建满足上述需求的自定义授权策略。

1. 登录到 [RAM 控制台](#)。
2. 单击策略管理 > 自定义授权策略。
3. 单击新建授权策略，打开新建授权策略弹窗，如下图所示：

图 2-1: 新建授权策略



4. 选择一个模板 (这里选择 AliyunOSSReadOnlyAccess)，我们可以基于该模板进行 Policy 编辑，如下图所示：

图 2-2: 编辑授权策略



我们修改了自定义的授权策略名称，备注和策略内容。上图策略内容中的选中部分是我们新增的细粒度授权限制内容。

代码样例如下所示：

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "oss:Get*",
        "oss:List*"
      ],
      "Effect": "Allow",
      "Resource": "acs:oss:*:*:samplebucket/bob/*",
      "Condition": {
        "IpAddress": {
          "acs:SourceIp": "127.0.27.1"
        }
      }
    }
  ]
}
```

5. 单击新建授权策略，完成新建自定义授权策略。

后续操作

如果将这个自定义的授权策略附加给用户 bob，那么 bob 对 `oss://samplebucket/bob/` 下的对象有只读操作权限，且限制条件是必须从您的公司网络（假设为 121.0.27.1）进行访问。

具体操作请参考[授权](#)。

修改自定义授权策略

当用户的权限发生变更时，比如新增或撤销权限，您需要修改授权策略。当您修改授权策略时可能会遇到以下问题：

- 希望一段时间后，老的授权策略还能继续使用。
- 修改完成后，您发现授权策略修改错了，需要回滚。

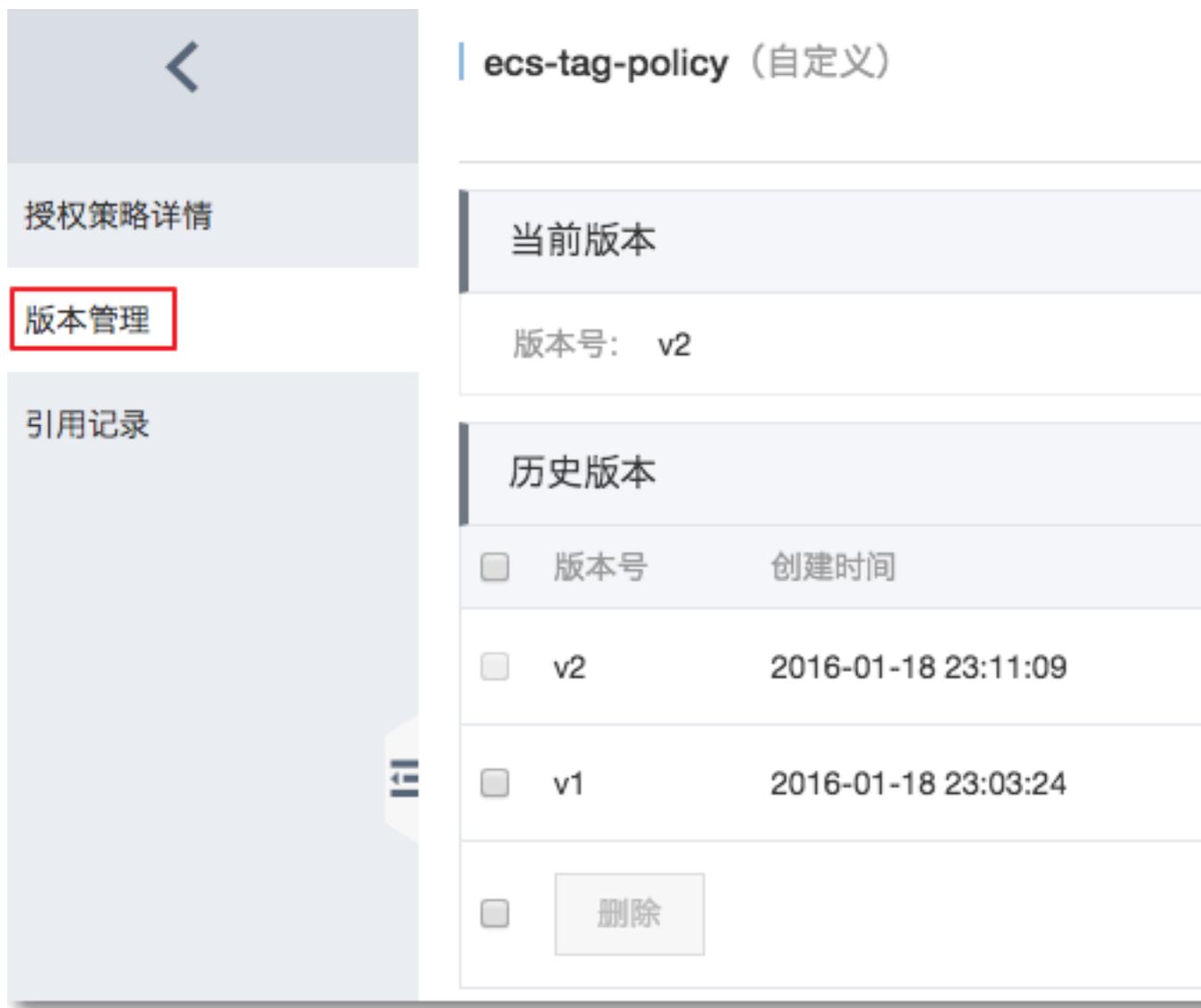
授权策略具备版本管理机制，用于解决在使用中存在的问题：

- 您可以为一个授权策略保留多个版本。
- 如果超出限制，您需要自主删除不需要的版本。
- 对于一个存在多版本的授权策略，只有一个版本是活跃的，即默认版本。

操作步骤

1. 在RAM控制台单击策略管理 > 自定义授权策略。
2. 通过 授权策略名称（可使用关键字查询）找到需要管理的授权策略，单击其名称或对应操作列下的查看。
3. 在左侧导航栏单击版本管理。

图 2-3: 版本管理



4. 如上图所示，在版本管理页面，您可以：

- 选择查看所有历史版本的策略内容。
- 将非默认版本策略设为当前版本（即默认版本）。
- 选择删除非默认版本策略。

删除自定义授权策略

您可以创建多个自定义授权策略，每个策略也可以维护多个版本。当您不再需要自定义授权策略时，您应该将授权策略删除。

前提

在删除某个授权策略前，应保证：

- 当前授权策略不存在多版本，只有一个默认版本。若该授权策略存在多个版本，您必须先删除除默认版本之外的所有版本。
- 当前授权策略未被引用（即附加给用户、用户组或角色）。若该授权策略已被引用，您可以：
 - 在该授权策略的引用记录中解除授权。
 - 还可以选择在删除过程中强制解除关联关系。

操作步骤

1. 在RAM控制台单击策略管理 > 自定义授权策略。
2. 通过授权策略名称（可使用关键字查询）找到需要删除的授权策略，单击其对应操作列下的删除。
3. 确认删除授权策略，可选择勾选强制解除关联关系（该策略有被引用记录时强制删除引用关系）。

至此，您已成功删除一条自定义授权策略。

2.3 授权

在 RAM 中，授权指将一个或多个授权策略附加到用户、用户组或角色的过程。其中，

- 给用户或用户组授权，用于对当前云账号下的 RAM 用户授权。
- 给角色授权，既用于对当前云账号下的 RAM 用户授权，也用于对其他云账号下的 RAM 用户或服务角色授权；不同的是，被授权的对象需要扮演角色以获取角色的身份与权限。

给用户或用户组授权

在对当前云账号下的 RAM 用户授权时，您可选择给具体用户授权，也可以向用户所在用户组授权。区别在于给用户组授权会应用到用户组下所有用户，便于对资源访问需求类似的用户（创建并添加到同一组别中）进行统一授权。

给用户授权

操作步骤如下：

1. 登录到[RAM控制台](#)。
2. 单击用户管理。

3. 通过用户名/显示名找到需要授权的用户（可使用模糊查询），单击其对应操作列下的授权按钮。
4. 在编辑个人授权策略页面，
 - 从左侧可选授权策略名称中找到需要授予当前用户的权限（可使用关键字查询），选中该策略，并单击右向箭头，可将该策略添加到右侧已选授权策略名称下。
 - 在右侧已选授权策略名称下，选择某条策略，并单击左向箭头，可撤销该策略。
5. 添加完授权策略后，单击确认，完成授权。

至此，您已完成给用户授权。

给用户组授权

操作步骤如下：

1. 登录到[RAM控制台](#)。
2. 单击群组管理。
3. 通过组名称找到需要授权的用户组（可使用模糊查询），单击其对应操作列下的授权按钮。
4. 在编辑群组授权策略页面，
 - 从左侧可选授权策略名称中找到需要授予当前群组的权限（可使用关键字查询），选中该策略，并单击右向箭头，可将该策略添加到右侧已选授权策略名称下。
 - 在右侧已选授权策略名称下，选择某条策略，并单击左向箭头，可撤销该策略。
5. 添加完授权策略后，单击确认，完成授权。

至此，您已完成给用户组授权。

给角色授权

新建角色时，可以选择新建用户角色（包括以当前云账号、其他云账号为受信云账号）或服务角色，并需选择相应的受信云账号或云服务（即允许其使用所创建的角色来访问您的云资源）。

- 对当前云账号用户角色授权，则当前云账号下的 RAM 用户可扮演角色并访问被授权的云资源。
- 对其他云账号用户角色授权，则指定的其他云账号下的 RAM 用户可扮演角色并访问被授权的云资源。
- 对服务角色授权，则受信的云服务可扮演角色并访问被授权的云资源。

操作步骤如下：

1. 登录到[RAM控制台](#)。

2. 单击角色管理。
3. 通过角色名找到需要授权的角色（可使用模糊查询），单击其对应操作列下的 **授权** 按钮。
4. 在编辑角色授权策略页面，
 - 从左侧 **可选授权策略名称** 中找到需要授予当前角色的权限（可使用关键字查询），选中该策略，并单击右向箭头，可将该策略添加到右侧 **已选授权策略名称** 下。
 - 在右侧 **已选授权策略名称** 下，选择某条策略，并单击左向箭头，可撤销该策略。
5. 添加完授权策略后，单击确认，完成授权。

至此，您已完成给角色授权。

2.4 操作资源

经授权后，RAM 用户可以通过控制台或 API 访问相关资源，也可以通过登录控制台后切换身份，或调用 `AssumeRole` 获取角色令牌（STS）以扮演相关角色，以角色身份操作相关资源。

RAM 用户登录控制台操作资源

RAM 用户登录需要使用独立的登录 URL（可以在 RAM 控制台查看），登录时使用主账号别名、用户名和密码登录控制台后，登录成功后可以操作被授权的资源。如果用户点击了没有授权的操作，一般会报告“没有操作权限”的错误。

如果 RAM 用户被许可扮演角色，

- 在 RAM 用户登录控制台之后，可以通过切换身份操作将当前登录身份切换到角色身份，并使用角色身份的权限来操作资源；
- 通过 **返回登录身份** 操作从角色身份返回到当前登录身份，以使用原登录身份操作资源。

关于使用角色的更多内容请参考[角色](#)。

应用程序调用云服务 API 操作资源

如果您的应用程序需要调用云服务 API，您需要为应用程序创建一个 RAM 用户账号并授予合适的权限，给 RAM 用户创建 `AccessKey`，应用程序使用该 `AccessKey` 来调用云服务 SDK 或 API。

通过客户端工具操作云资源

某些云服务提供了易用的客户端工具，这些工具支持使用 RAM 用户 `AccessKey` 来操作云资源。

下面以 OSS 服务为例，假设 RAM 用户获得了某个 Bucket 的访问授权，那么可以使用 OSS 客户端工具 `ossbrowser` 来访问指定的 Bucket。

操作步骤如下：

1. 打开 ossbrowser，在账号和密码处分别输入 RAM 用户的 AccessKeyId 和 AccessKeySecret。

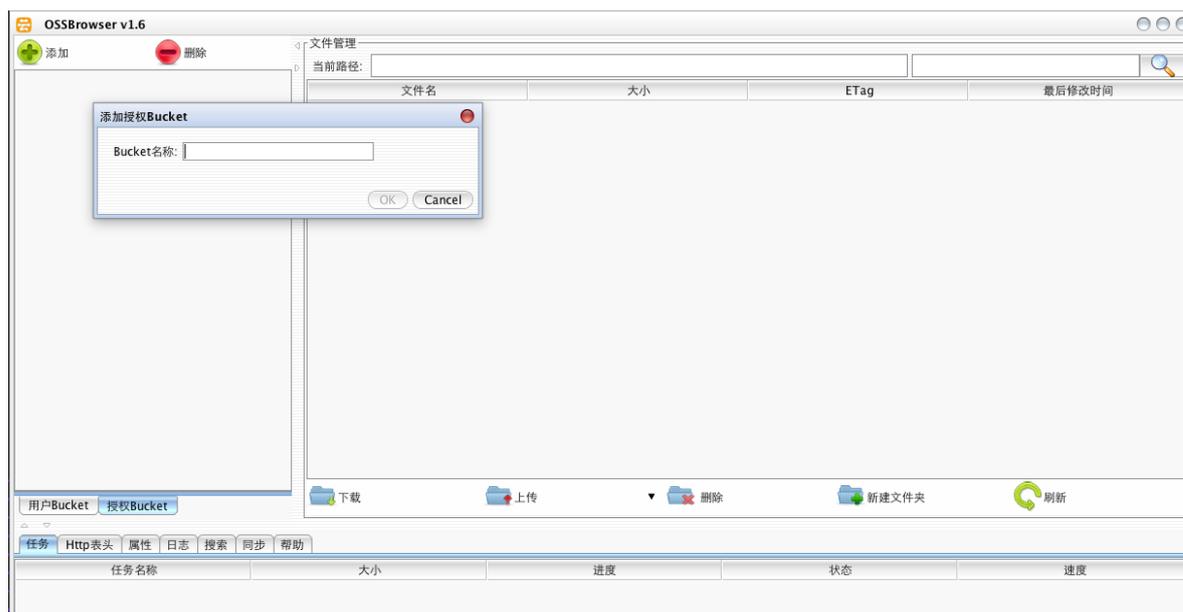
如下图所示：

图 2-4: 登录



2. 登录后进入 ossbrowser 界面，选择授权Bucket标签，点击添加即可添加一个授权 Bucket。如下图所示：

图 2-5: 添加授权Bucket



然后您就可以操作被授权 Bucket 的内容。

3 云产品授权
