

ALIBABA CLOUD

阿里云

性能测试
访问控制

文档版本：20220425

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、特殊性或惩罚性的损害，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。未经阿里云和/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 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <code>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>switch {active stand}</code>

目录

1. 访问控制概述	05
2. 借助RAM用户实现分权	06
3. 借助RAM角色实现跨云账号访问资源	08

1. 访问控制概述

借助访问控制RAM (Resource Access Management) 的RAM用户，您可以实现权限分割的目的，按需为子账号赋予不同权限，并避免因暴露阿里云账号（主账号）密钥造成的安全风险。

应用场景

以下是需用到访问控制RAM的典型场景。

- 借助RAM用户实现分权

企业A因为项目上云，购买了多种阿里云产品，例如：ECS实例、RDS实例、SLB实例、OSS存储空间等。项目里有多个员工需要操作这些云资源，但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：

- 出于安全或信任的考虑，企业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独立账号。
- 用户账号只能在授权的前提下操作资源。企业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。
- 不需要对用户账号进行独立的计量计费，所有开销都由企业A来承担。

RAM的授权管理功能支持用户分权及资源统一管理，可以解决企业A的上述诉求。

- 借助RAM角色实现跨账号访问资源

云账号A和云账号B分别代表不同的企业。A购买了多种云资源来开展业务，例如：ECS实例、RDS实例、SLB实例、OSS存储空间等。

- A希望能专注于业务系统，而将云资源运维、监控、管理等任务授权给B。
- B还可以进一步将A的资源访问权限分配给B的某一个或多个员工，B可以精细控制其员工对资源的操作权限。
- 如果A和B的这种运维合同关系终止，A随时可以撤销对B的授权。

RAM角色支持跨账号授权及资源访问控制，可以满足上述诉求。

更多信息

- [借助RAM用户实现分权](#)
- [借助RAM角色实现跨云账号访问资源](#)

2. 借助RAM用户实现分权

借助访问控制RAM (Resource Access Management) 的RAM用户，您可以实现权限分割，按需为RAM用户赋予不同权限，并避免因暴露阿里云账号（主账号）密钥造成的安全风险。

前提条件

- 开通PTS
- 开通RAM

背景信息

出于安全考虑，您可以为阿里云账号（主账号）创建RAM用户，并根据需要为这些RAM用户赋予不同的权限，这样就能在不暴露主账号密钥的情况下，实现让RAM用户各司其职的目的。

在本文中，假设企业A希望让部分员工处理日常运维工作，则企业A可以创建RAM用户，并为RAM用户赋予相应权限，此后员工即可使用这些RAM用户登录控制台。

操作步骤

1. 创建RAM用户。

首先需要使用阿里云账号（主账号）登录RAM控制台并创建RAM用户。

- 登录RAM控制台，在左侧导航栏选择身份管理 > 用户，并在用户页面上单击创建用户。
- 在创建用户页面的用户账号信息区域中，输入登录名称和显示名称。

说明 登录名称中允许使用英文字母、数字、英文句号(.)、下划线(_)和短划线(-)，长度不超过64个字符。显示名称不可超过24个字符或汉字。

- （可选）如需一次创建多个用户，则单击+添加用户，并重复上一步操作。
- 在访问方式区域中，选中控制台访问，设置自动生成默认密码或自定义登录密码、登录时是否要求重置密码，以及是否开启MFA多因素认证，并单击确定。
- 在手机验证对话框中单击获取验证码，并输入收到的手机验证码，然后单击确定。

创建的RAM用户显示在用户页面上。

后续步骤

为RAM用户授予PTS控制台权限

RAM用户默认对PTS控制台不具备任何操作权限。若想使RAM用户拥有PTS控制台的操作权限（包括只读权限和读写权限），您需要使用阿里云账号（主账号）登录PTS控制台，并在应用权限管理页面为目标RAM用户授予相应权限。具体操作，请参见[管理账号权限](#)。

创建和删除服务关联角色

当PTS检测到您没有授予PTS访问您的云资源权限时，会提示您授权PTS自动创建一个服务关联角色（AliyunServiceRoleForPts），允许PTS拥有对您云资源相应的访问权限。

- 角色名称：AliyunServiceRoleForPts
- 角色权限策略：AliyunServiceRolePolicyForPts
- 角色权限说明：允许PTS拥有对您云资源相应的访问权限，包括ACK、ECS、ENI、RDS、SLB、VPC等。

如果您需要删除AliyunServiceRoleForPts，请在[RAM控制台](#)删除此服务关联角色。

② **说明** 删除服务关联角色后会影响您VPC网络的压测和云产品（包括RDS、ECS、SLB等）数据的获取，若删除角色后仍需使用到VPC或云监控功能，系统会提示您创建服务关联角色。更多关于创建和删除服务关联角色的信息，请参见[服务关联角色](#)。

3. 借助RAM角色实现跨云账号访问资源

使用企业A的阿里云账号创建RAM角色并为该角色授权，并将该角色赋予企业B，即可实现使用企业B的阿里云账号或其RAM用户访问企业A的阿里云资源的目的。

背景信息

假设企业A购买了多种云资源来开展业务，并需要授权企业B代为开展部分业务，则可以利用RAM角色来实现此目的。RAM角色是一种虚拟用户，没有确定的身份认证密钥，需要被一个受信的实体用户扮演才能正常使用。为了满足企业A的需求，可以按照以下流程操作：

1. 企业A创建RAM角色。
2. 企业A为该RAM角色添加权限。
3. 企业B创建RAM用户。
4. 企业B为RAM用户添加AliyunSTSAssumeRoleAccess权限。
5. 企业B的RAM用户通过控制台访问企业A的资源。

可以为RAM角色添加的应用发现服务权限策略为：AliyunPTSSFullAccess，即PTS的完整权限。

步骤一：企业A创建RAM角色

首先需要使用企业A的阿里云账号登录RAM控制台并创建RAM角色。

1. 登录RAM控制台，在左侧导航栏选择身份管理 > 角色，然后单击创建角色。
2. 在弹出的创建角色面板中执行以下操作并单击完成。
 - i. 选择可信实体类型为阿里云账号，单击下一步。
 - ii. 在角色名称文本框内输入角色名称。

 说明 角色名称中允许使用英文字母、数字和短划线（-），长度不超过64个字符。

- iii. 选择信任的云账号为其他云账号，并在文本框内输入企业B的云账号，然后单击完成。

步骤二：企业A为该RAM角色添加权限

新创建的角色没有任何权限，因此企业A必须为该角色添加权限。

1. 在RAM控制台左侧导航栏中选择身份管理 > 角色。
2. 在角色页面上单击目标角色操作列中的添加权限。
3. 在添加权限面板的选择权限区域框中，通过关键字搜索需要添加的权限策略，并单击权限策略将其添加至右侧的已选择列表中，然后单击确定。

 说明 可添加的权限参见背景信息部分。

4. 在添加权限面板中，查看授权信息，并单击完成。

步骤三：企业B创建RAM用户

接下来要使用企业B的阿里云账号登录RAM控制台并创建RAM用户。

1. 登录RAM控制台，在左侧导航栏中选择身份管理 > 用户，并在用户页面上单击创建用户。
2. 在创建用户页面的用户账号信息区域框中，输入登录名称和显示名称。

② 说明 登录名称中允许使用小写英文字母、数字、半角句号(.)、下划线(_)和半角连接号(-)，长度不超过64个字符。显示名称不超过128个字符或汉字。

3. (可选) 如需一次创建多个用户，则单击**+添加用户**，并重复上一步。
4. 在**访问方式**区域框中，选中**控制台访问**或**OpenAPI 调用访问**，并单击**确定**。

② 说明 为提高安全性，请仅选择一种访问方式。

- 如果选中**控制台访问**，则完成进一步设置，包括自动生成默认密码或自定义登录密码、登录时是否要求重置密码，以及是否开启MFA多因素认证。
- 如果选中**OpenAPI 调用访问**，则RAM会自动为RAM用户创建AccessKey (API访问密钥)。

② 说明 出于安全考虑，RAM控制台只提供一次查看或下载AccessKey Secret的机会，即创建AccessKey时，因此请务必将AccessKey Secret记录到安全的地方。

步骤四：企业B为RAM用户添加权限

企业B必须为其阿里云账号下的RAM用户添加**AliyunSTSAssumeRoleAccess**权限，RAM用户才能扮演企业A创建的RAM角色。

1. 在**RAM控制台**左侧导航栏中选择**身份管理 > 用户**。
2. 在**用户**页面上找到需要授权的用户，单击操作列中的**添加权限**。
3. 在**添加权限**面板的**选择权限**区域框中，通过关键字搜索**AliyunSTSAssumeRoleAccess**权限策略，并单击该权限策略将其添加至右侧的**已选择**列表中，然后单击**确定**。
4. 在**添加权限**面板中，查看授权信息，并单击**完成**。

后续步骤

完成上述操作后，企业B的RAM用户即可按照以下步骤登录控制台访问企业A的云资源。

1. 在浏览器中打开**RAM用户登录入口**。
2. 在**RAM用户登录**页面上，输入RAM用户登录名称，单击**下一步**，并输入RAM用户密码，然后单击**登录**。

② 说明 RAM用户登录名称的格式为 `<$username>@<$AccountAlias>` 或 `<$username>@<$AccountAlias>.onaliyun.com`。 `<$AccountAlias>` 为账号别名，如果没有设置账号别名，则默认值为阿里云账号的ID。

3. 在阿里云控制台页面上，将鼠标指针移到右上角头像，并在浮层中单击**切换身份**。
4. 在**阿里云 - 角色切换**页面，输入企业A的企业别名或默认域名，以及角色名，然后单击**提交**。
5. 对企业A的阿里云资源执行操作。