ALIBABA CLOUD

阿里云

智能顾问

访问控制

文档版本：20220415

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
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 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	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。	`switch {active|stand}`

目录

1.访问控制概述

借助访问控制 RAM 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。

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 的某个项目（Project-X）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，由于每个员工的工作职责不同，需要的权限也不一样。企业 A 希望能够达到以下要求：

- 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独立账号。
- 用户账号只能在授权的前提下操作资源。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 A 来承担。
- 针对以上需求，可以借助 RAM 的授权管理功能实现用户分权及资源统一管理。

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。

- 企业 A 希望能专注于业务系统，而将云资源运维、监控、管理等任务授权给企业 B。
- 企业 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。
- 针对以上需求，可以借助 RAM 角色实现跨账号授权及资源访问的控制。

借助 RAM 服务角色实现动态访问云服务

如果您购买了 ECS 实例，并且打算在 ECS 中部署企业的应用程序，而这些应用程序需要使用 Access Key 访问其他云服务 API，那么有两种做法：

- 将 Access Key 直接嵌入代码。
- 将 Access Key 保存在应用程序的配置文件中。

然而，这两种做法会带来两个问题：

- 保密性问题：如果 Access Key 以明文形式存在于 ECS 实例中，则可能随着快照、镜像及镜像创建出来的实例被泄露。
- 运维难问题：由于 Access Key 存在于实例中，如果要更换 Access Key（例如周期性轮转或切换用户身份），那么需要对每个实例和镜像进行更新并重新部署，这会增加实例和镜像管理的复杂性。

ECS 服务结合 RAM 提供的访问控制能力，允许给每一个 ECS 实例（即用户应用程序的运行环境）配置一个拥有合适权限的 RAM 角色身份，应用程序通过获取该角色身份的动态令牌来访问云服务 API。

智能顾问的权限策略

Advisor 支持的系统权限策略为：

- AliyunAdvisorFullAccess：管理智能顾问（Advisor）的权限，包含编辑/设置操作权限。

- AliyunAdvisorReadOnlyAccess：只读访问智能顾问（Advisor）的权限。

更多信息

- [RAM主子账号授权]
- 什么是RAM

2.RAM主子账号授权

借助访问控制 RAM 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。

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

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。Advisor 支持借助 RAM 用户实现分权，即为该子账号开启控制台登录权限，并按需授予以下权限。

- AliyunAdvisorFullAccess：管理智能顾问（Advisor）的权限，包含编辑/设置操作权限。
- AliyunAdvisorReadOnlyAccess：只读访问智能顾问（Advisor）的权限。

前提条件

- 开通 RAM。
- [开通Advisor]。

步骤一：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。

1. 登录 RAM 控制台，在左侧导航栏中选择**人员管理 > 用户**，并在用户页面上单击**新建用户**。
2. 在**新建用户**页面的**用户账号信息**区域框中，输入**登录名称**和**显示名称**。

说明：登录名称中允许使用小写英文字母、数字、“.”、“_”和“-”，长度不超过 128 个字符。显示名称不可超过 24 个字符或汉字。

1. （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。
2. 在**访问方式**区域框中，勾选**控制台密码登录（推荐使用）**或**编程访问**，并单击确定。

说明： 为提高安全性，请仅勾选一种访问方式。

- 如果勾选**控制台密码登录**，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。
- 如果勾选**编程访问**，则 RAM 会自动为 RAM 用户创建 AccessKey（API 访问密钥）。

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

1. 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。

步骤二：为 RAM 用户添加权限

在使用 RAM 用户之前，需要为其添加相应权限。

1. 在 RAM 控制台左侧导航栏中选择**人员管理 > 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。

1. 在**添加权限**的**授权结果**页面上，查看授权信息摘要，并单击**完成**。

后续步骤

使用阿里云账号（主账号）创建好 RAM 用户后，即可将 RAM 用户的登录名称及密码或者 AccessKey 信息分发给其他用户。其他用户可以按照以下步骤使用 RAM 用户登录 Advisor 控制台。

1. 在浏览器中打开 RAM 用户登录入口 https://signin.aliyun.com/login.htm。
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。

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（主账号）的 ID。

1. 在**子用户用户中心**页面上单击**智能顾问**，即可访问只能顾问控制台。

3.Advisor服务关联角色

本文介绍Advisor服务关联角色AliyunServiceRoleForAdvisor以及如何删除该角色。

背景信息

Advisor服务关联角色AliyunServiceRoleForAdvisor是Advisor为了完成自身的某个功能，需要获取其他云服务的访问权限而提供的RAM角色。更多关于服务关联角色的信息请参见服务关联角色。

应用场景

Advisor需要访问负载均衡SLB（Server Load Balancer）、专有网络VPC（Virtual Private Cloud）、云服务器ECS（Elastic Compute Service）等云服务的资源时，可通过自动创建的Advisor服务关联角色AliyunServiceRoleForAdvisor获取访问权限。

权限说明

AliyunServiceRoleForAdvisor具备的云服务的访问权限如下所示，更多权限说明请参见权限策略管理。

- ECS的访问权限

```
{
    "Action": [
        "ecs:DescribeInstances",
        "ecs:DescribeTags",
        "ecs:DescribeDisks",
        "ecs:DescribeRegions",
        "ecs:DescribeInstanceMonitorData",
        "ecs:DescribeDiskMonitorData",
        "ecs:ValidateSecurityGroup",
        "ecs:DescribeCommands",
        "ecs:DescribeDisksFullStatus",
        "ecs:DescribeDeploymentSets",
        "ecs:DescribeAccountAttributes",
        "ecs:DescribeNetworkInterfaces",
        "ecs:DescribeSecurityGroups",
        "ecs:DescribeAccountAttributes",
        "ecs:DescribeDedicatedHosts",
        "ecs:DescribeDedicatedHostAutoRenew",
        "ecs:DescribeSecurityGroupAttribute"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
```

- SLB的访问权限

```
{
    "Action": [
        "slb:DescribeLoadBalancers",
        "slb:DescribeRegions",
        "slb:DescribeLoadBalancerAttribute",
        "slb:DescribeHealthStatus",
        "slb:DescribeLoadBalancerTCPListenerAttribute",
        "slb:DescribeLoadBalancerUDPListenerAttribute",
        "slb:DescribeLoadBalancerHTTPListenerAttribute",
        "slb:DescribeLoadBalancerHTTPSListenerAttribute"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
```

- VPC的访问权限

```
{
    "Action": [
         "vpc:DescribeVpcs",
        "vpc:DescribeVSwitches",
        "vpc:DescribeEipAddresses",
        "vpc:DescribeRegions",
        "vpc:DescribeEipMonitorData",
        "vpc:DescribePhysicalConnections"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
```

删除Advisor服务关联角色

删除AliyunServiceRoleForAdvisor会影响Advisor获取数据，请谨慎操作。删除AliyunServiceRoleForAdvisor的操作步骤如下。

1. 登录RAM控制台，在左侧导航栏中单击**RAM角色管理**。
2. 在**RAM角色管理**页面的搜索框中，输入**AliyunServiceRoleForAdvisor**，自动搜索到名称为AliyunServiceRoleForAdvisor的RAM角色。
3. 在右侧**操作**列，单击**删除**。
4. 在**删除RAM角色**对话框，单击**确定**。

恢复服务关联角色

若删除服务关联角色后仍需使用到云资源，系统会提示您创建服务关联角色。登录Advisor控制台，根据提示完成授权。

常见问题

问：为什么我的RAM用户无法自动创建AliyunServiceRoleForAdvisor?

答：您需要拥有指定的权限才能自动创建或删除AliyunServiceRoleForAdvisor。因此，在RAM用户无法自动创建AliyunServiceRoleForAdvisor时，您需为其添加以下权限策略。

```
{
    "Statement": [
        {
            "Action": [
                "ram:CreateServiceLinkedRole"
            ],
            "Resource": "acs:ram:*:主账号ID:role/*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": [
                        "advisor.aliyuncs.com"
                    ]
                }
            }
        }
    ],
    "Version": "1"
}
```

说明 请将*主账号ID*替换为您实际的阿里云账号（主账号）ID。