



应用配置管理 ACM 访问控制

文档版本: 20210923



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。

- 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。
- 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。
- 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。	
▲ 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。	大意 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 <i>,</i> 不是 用户必须了解的内容。	⑦ 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 listinstanceid
[] 或者 [alb]	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 {act ive st and}

目录

1.访问权限控制	05
2.RAM用户	10
3.RAM角色	14
4.通过ECS实例RAM角色访问ACM	17
5.利用RAM角色实现跨账号访问ACM	20

1.访问权限控制

本文以将单个命名空间授权给某个RAM用户为例,介绍如何使用ACM的访问权限控制功能。

迁移到MSE Nacos

ACM进入下线状态,所有配置管理相关的需求由MSE中的Nacos承接(ACM独享版,更好的安全和稳定性)。您需要在ACM控制台导出配置,然后在MSE控制台导入之前导出的配置即可完成迁移。具体操作,请参见将应用配置从ACM迁移到MSE Nacos。

背景信息

以往,当一个RAM用户(或角色)被授予AliyunACMFullAccess授权策略时,即拥有ACM的完全操作权限, 包括对所有配置和所有命名空间的读写权限。由于RAM用户之间的配置并未隔离,因误操作或恶意操作造成 的损失就可能会被放大,并造成严重后果。更重要的是,由于对所有授权用户可见,数据库账号密码等敏感 配置面临着泄露的安全风险。

现在,ACM提供了更细粒度的权限控制,您可以按需为用户分配最小权限,达到为不同用户(或角色)授予 不同资源操作权限的目的。对应RAM的授权策略,可以分为操作(Action)维度和资源(Resource)维度。

操作 (Action)

- 读:可以读取Resource所指定范围的配置,以及读取命名空间基本信息,对应的RAM授权策略Action为 a cms:R 。
- 写:可以增加、删除和修改Resource所指定范围的配置,但无法增加、删除和修改命名空间,对应的RAM 授权策略Action为 acms:₩ 。
- 完全权限:可以读写Resource所指定范围的配置,并读取命名空间基本信息。当Resource为*时,也可以增加、删除和修改命名空间,对应的RAM授权策略Action为 acms:*。

资源 (Resource)

授权资源的定义规则为 acs:\${service-name}:\${region-id}:\${resource-owner-id}:\${resourcetype}/\${namespace_id}/\${resource-name} 。

- 所有资源:对应的RAM授权策略Resource为 *。
- 单个命名空间:例如命名空间为 1ca01ca0-11b0-1e01-0df1-d1010101bc10 ,则对应的RAM授权策略 Resource为 *:*:*:cfg/1ca01ca0-11b0-1e01-0df1-d1010101bc10 。
- 单个命名空间下的某个Group:例如命名空间为 1ca01ca0-11b0-1e01-0df1-d1010101bc10, Group为 DEF AULT GROUP,则对应的RAM授权策略Resource为 *:*:*:cfg/1ca01ca0-11b0-1e01-0df1-d1010101bc10/DE FAULT_GROUP。
- 单个命名空间下的某个Group的特定配置项:例如命名空间为 1ca01ca0-11b0-1e01-0df1d1010101bc10, Group为 DEFAULT GROUP,配置项的Datald为 com.alibaba.acm.test,则对应的RAM 授权策略Resource为 *:*:*:cfg/1ca01ca0-11b0-1e01-0df1-d1010101bc10/DEFAULT_GROUP/com.alibaba.ac m.test。

步骤一: 创建RAM自定义授权策略

- 1. 登录RAM控制台。
- 2. 在左侧导航栏的权限管理菜单下,单击权限策略管理。
- 3. 在授权策略管理页面左上角单击创建权限策略。
- 4. 在新建自定义权限策略页面,选择配置模式为脚本配置。
- 5. 在策略内容输入框内输入自定义的授权策略名称、备注和策略内容,并单击确定。

例如,要为命名空间 1ca01ca0-11b0-1e01-0df1-d1010101bc10 配置读写权限,请在**策略内容**文本框中 输入以下内容:

```
{
    "Version": "1",
    "Statement": [
    {
        "Action": [
        "acms:*"
    ],
        "Resource": "*:*:*:cfg/1ca01ca0-11b0-1e01-0df1-d1010101bc10",
        "Effect": "Allow"
    }
]
}
```

⑦ 说明 关于创建RAM自定义授权策略的详细步骤,请参考创建自定义策略。

步骤二: 创建RAM用户并授权

- 1. 在左侧导航栏,选择身份管理 > 用户。
- 2. 在用户页面,单击创建用户。
- 3. 在创建用户页面的用户账号信息区域, 输入登录名称和显示名称。

⑦ 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,选择编程访问,然后单击确定。 在用户信息页面会显示创建用户的AccessKey ID和AccessKeySecret,请记录下来供后续步骤使用 并妥善保管。
- 5. 在用户页面,单击目标RAM用户操作列的添加权限。
- 6.
- 7. 在权限策略名称右侧的输入框内, 输入步骤一: 创建RAM自定义授权策略中生成的策略名称。
- 8. 单击确定,然后关闭右侧面板。

步骤三:登录RAM用户并验证权限

- 1. 返回到RAM控制台。
- 2. 在概览页面上单击账号管理区域的登录链接,并以您新建的用户登录。
- 3. 访问ACM控制台,验证当前可以操作的只有刚刚设置授权策略中的命名空间。

更多示例

1. 授予单个命名空间(例如 1ca01ca0-11b0-1e01-0df1-d1010101bc10)的只读权限。

```
{
    "Version": "1",
    "Statement": [
    {
        "Action": [
            "acms:R"
    ],
        "Resource": "*:*:*:cfg/1ca01ca0-11b0-1e01-0df1-d1010101bc10",
        "Effect": "Allow"
    }
]
}
```

2. 授予单个命名空间(例如 1ca01ca0-11b0-1e01-0df1-d1010101bc10)中单个Group(例如 DEFAULT_GR OUP)的读写权限。

```
{
    "Version": "1",
    "Statement": [
    {
        "Action": [
            "acms:*"
    ],
        "Resource": "*:*:*:cfg/1ca01ca0-11b0-1e01-0df1-d1010101bc10/DEFAULT_GROUP",
        "Effect": "Allow"
    }
}
```

3. 授予单个命名空间(例如 1ca01ca0-11b0-1e01-0df1-d1010101bc10)中多个Group(例如 DEFAULT_GR OUP、 DEFAULT_GROUP_1)的只读权限。

```
{
    "Version": "1",
    "Statement": [
    {
        "Action": [
        "acms:R"
    ],
        "Resource": [
            "*:*:*:cfg/lca0lca0-11b0-1e01-0df1-d1010101bc10/DEFAULT_GROUP",
            "*:*:*:cfg/lca0lca0-11b0-1e01-0df1-d1010101bc10/DEFAULT_GROUP_1"
        ],
        "Effect": "Allow"
    }
]
```

4. 授予单个命名空间(例如1ca01ca0-11b0-1e01-0df1-d1010101bc10)中某个Group(例如 DEFAULT_GROUP)下特定配置项(com.alibaba.acm.test)只读权限。

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
               "acms:R"
            ],
            "Resource": "*:*:*:cfg/lca01ca0-11b0-1e01-0df1-d1010101bc10/DEFAULT_GROUP/com.alibaba.ac
m.test",
            "Effect": "Allow"
        }
    ]
```

```
}
```

5. 授予所有命名空间中单个Group(例如DEFAULT_GROUP)的读写权限。

```
{
    "Version": "1",
    "Statement": [
    {
        "Action": [
        "acms:*"
    ],
        "Resource": [
            "*:*:*::cfg/*/DEFAULT_GROUP"
    ],
    "Effect": "Allow"
}
]
```

6. 授予单个Region (例如杭州 cn-hangzhou) 单个命名空间 (例如 1ca01ca0-11b0-1e01-0df1-d1010101bc 10) 的读写权限。

```
{
    "Version": "1",
    "Statement": [
    {
        "Action": [
        "acms:*"
    ],
        "Resource": [
            "*:*:cn-hangzhou:*:cfg/1ca01ca0-11b0-1e01-0df1-d1010101bc10"
        ],
        "Effect": "Allow"
    }
]
```

备注

- 只有当授权策略操作(Action)为 acms:* 并且资源(Resource)为 * 时,被授予该授权策略的用户 (或角色)才能增加、删除和修改命名空间。
- 由于存在缓存机制,授权策略的添加和修改会延迟生效,但通常都会在10秒内生效。

• 通过ECS实例RAM角色访问ACM时,授予如上所述授权策略,同样可以实现细粒度的权限控制。

相关文档

通过ECS实例RAM角色访问ACM

2.RAM用户

ACM支持阿里云访问控制RAM的账户体系。借助RAM用户,云账户(主账户)可以避免与其他用户共享账户 密钥,并按需为RAM用户分配最小权限,实现各司其职的高效管理。

迁移到MSE Nacos

ACM进入下线状态,所有配置管理相关的需求由MSE中的Nacos承接(ACM独享版,更好的安全和稳定性)。您需要在ACM控制台导出配置,然后在MSE控制台导入之前导出的配置即可完成迁移。具体操作,请参见将应用配置从ACM迁移到MSE Nacos。

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(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用户登录控制台或调用API。

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。
- 2. 在用户页面上单击新建用户,在用户账号信息区域输入用户的登录名称和显示名称。

↓ 注意 登录名称必须在云账户内保持唯一。

如需创建多个用户,则单击**添加用户**,并输入**登录名称和显示名称**。 新建用户页面



3. 在**访问方式**区域选择控制台密码登录,然后按需设置控制台密码、要求重置密码和多因素认证,并 单击确定。

完成以上步骤后,一个可以登录控制台的RAM用户就创建成功了。

为RAM用户授权

RAM授权的粒度是ACM服务级别,即RAM授权表示允许用户拥有ACM的所有权限。RAM授权或者解除授权只能在RAM控制台上操作。

- 1. 登录RAM控制台, 在左侧导航栏中选择人员管理 > 用户。
- 2. 在用户页面上单击目标用户操作列中的授权。

添加权限					×
被授权主体					
test@	5.onaliyun.com ×				
选择权限					
系统权限策略 🛛 🗸	AliyunACMFullAccess	۵	Q	已选择(1)	清除
权限策略名称	备注			AliyunACMFullAccess	×
AliyunACMFullAccess	管理应用配置管理(ACM	们的权限			
					1
備足取消					

3. 在添加权限对话框左侧的系统权限策略中找到AliyunACMFullAccess策略,并单击该策略,然后单击确定。

⑦ 说明 如果还使用到ACM的加解密配置功能,则还需要为用户添加AliyunKMSCryptoAccess授权策略。

为RAM用户解除授权

- 1. 登录RAM控制台,在左侧导航栏中选择人员管理 > 用户。
- 2. 在用户管理页面上单击目标用户的用户登录名称/显示名称,然后单击权限管理页签。
- 3. 在个人权限子页签的表格中,单击操作列中的移除权限。
- 4. 在移除权限对话框中单击确认。

授权解除后, RAM用户无权登录ACM。

删除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。
- 2. 在用户页面上单击目标用户操作列中的删除。
- 3. 在删除用户对话框中单击确认。

使用RAM用户登录ACM控制台

- 1. 使用云账户登录RAM控制台,在左侧导航栏中选择概览。
- 2. 在账号管理区域单击用户登录地址链接。

账号管理	
主账号	
用户登录地址	
https://signin.aliyun.com/	onaliyun.com/login.htm (] 复制
域别名	

3. 在**阿里云-RAM用户登录**页面上按照提示输入登录用户名称,单击下**一步**,然后输入密码并单击登录。

子用户登录
登录用户名称
RAM用户新版登录格式: <子用户名称 > @ <企业别名 > 例 如:username@company-alias
下一步

4. 在子用户用户中心页面上,单击互联网中间件类目下的应用配置管理进入ACM控制台。

相关文档

- 访问权限控制
- RAM角色
- 基本概念

3.RAM角色

ACM支持阿里云访问控制RAM的账户体系。借助RAM角色,可实现访问其他云账户的ACM资源的目的。

迁移到MSE Nacos

ACM进入下线状态,所有配置管理相关的需求由MSE中的Nacos承接(ACM独享版,更好的安全和稳定性)。您需要在ACM控制台导出配置,然后在MSE控制台导入之前导出的配置即可完成迁移。具体操作,请参见将应用配置从ACM迁移到MSE Nacos。

创建RAM角色

- 1. 登录RAM控制台, 在左侧导航栏中选择RAM角色管理。
- 2. 在RAM角色管理页面上单击新建RAM角色。
- 3. 在新建RAM角色对话框中的执行以下操作并单击确定。
 - i. 在RAM角色类型区域按需选择:
 - 用户RAM角色:受信云账户(当前云账户或其他云账户)下的RAM用户可以通过扮演用户角色 来访问您的云资源。
 - 服务RAM角色: 受信云服务(例如ECS云服务器)可以通过扮演用户角色来访问您的云资源。
 - ii. 根据上一步的选择执行相应操作:
 - 如果选择**用户RAM角色**,则在**选择云账号**区域选择**当前云账号**,或者选择**其他云账号**并在文本框内输入其账户ID。
 - 如果选择**服务RAM角色**,则在选择受信服务下拉框中选择一种云服务。
 - iii. 在RAM角色名称文本框内输入RAM角色名称。

为RAM角色授权

新创建的角色没有任何权限,因此需要为该角色授权。

- 1. 登录RAM控制台, 在左侧导航栏中选择RAM角色管理。
- 2. 在RAM角色管理页面上单击目标角色操作列中的添加权限。

添加权限				\times
被授权主体				
test@	un.com X			
选择权限				
系统权限策略 > Aliyun	ACMFullAccess	© Q	已选择(1)	清除
权限策略名称	备注		AliyunACMFullAccess ×	
AliyunACMFullAccess	管理应用配置管理(ACM)的权限			
确定取消				

- 3. 在添加权限对话框左侧的系统权限策略中找到AliyunACMFullAccess策略,并单击该策略,然后单击确定。
 - 如果还使用到ACM的加解密配置功能,则还需要为用户添加AliyunKMSCryptoAccess授权策略。

为RAM角色解除授权

- 1. 登录RAM控制台,在左侧导航栏中选择RAM角色管理。
- 2. 在RAM角色管理页面上单击目标角色的RAM角色名称。
- 3. 在RAM角色授权策略页签上的表格中,单击操作列中的移除权限。
- 4. 在移除权限对话框中单击确认。

授权解除后, RAM用户无权登录ACM。

删除RAM角色

- 1. 登录RAM控制台, 在左侧导航栏中选择RAM角色管理。
- 2. 在RAM角色管理页面上单击目标角色操作列中的删除RAM角色。
- 3. 在删除RAM角色对话框中单击确认。

相关文档

- 访问权限控制
- > 文档版本: 20210923

- 利用RAM角色实现跨账号访问ACM
- RAM用户
- 基本概念

4.通过ECS实例RAM角色访问ACM

如果借助ECS实例RAM角色,则无需配置AccessKey(AK)即可访问ACM,从而提高安全性。

迁移到MSE Nacos

ACM进入下线状态,所有配置管理相关的需求由MSE中的Nacos承接(ACM独享版,更好的安全和稳定性)。您需要在ACM控制台导出配置,然后在MSE控制台导入之前导出的配置即可完成迁移。具体操作,请参见将应用配置从ACM迁移到MSE Nacos。

背景信息

以往,如果部署在ECS实例中的应用程序需要访问ACM,必须将AccessKey以配置文件或其他形式保存在ECS 实例中,这在一定程度上增加了AccessKey管理的复杂性,并且降低了AccessKey的保密性。创建AccessKey 的具体操作,请参见获取AccessKey(文档将在2021年9月30日下线)。

现在,借助ECS实例RAM角色,您可以将RAM角色和ECS实例关联起来,然后将RAM角色名称告知ACM SDK(1.0.8及以上版本),此后无需配置AccessKey即可访问ACM。另外,借助RAM(访问控制),您可以通 过角色和授权策略实现不同实例对ACM具有不同访问权限的目的。例如,如果配置只读策略,关联了该角色 的ECS就只能读取ACM的配置,而无法新增或修改ACM配置。

前提条件

您已成功创建ECS实例,且ECS实例的网络环境为专有网络(VPC)。

步骤一: 创建RAM角色并配置授权策略

- 1. 云账号登录RAM控制台。
- 2. 在左侧导航栏,单击RAM角色管理。
- 3. 单击创建RAM角色,选择可信实体类型为阿里云服务,单击下一步。
- 4. 选择角色类型, 输入角色名称和备注, 选择受信服务为云服务器, 然后单击完成。
- 5. 在RAM角色名称列,找到刚创建的RAM角色。
- 6. 在操作列单击添加权限。
- 7. 在**添加权限**对话框中,通过关键词搜索授权策略 AliyunACMFullAccess ,并单击该授权策略将其添加至 右侧的**已选授**列表,然后单击**确定**。

⑦ 说明 如果需要用到加解密配置功能,则还要添加 AliyunKMSCryptoAdminAccess 授权策略。

此时,该角色已具备ACM的所有操作权限。

步骤二:为ECS实例授予该RAM角色

- 1. 登录ECS控制台,单击左侧导航栏的实例。
- 2. 单击实例列表中目标ECS实例操作栏的更多 > 实例设置 > 授予/收回RAM角色。

实例列表	■产品动态 ⑦	ECS控制台操作指南 C 创建实例 批量操作
检查到安全组中包含允许对特定端口进行不受限制访问的规则,存在潜在高危风险。	. 查看洋情	
▼ 选择实例属性项搜索,或者输入关键字识别搜索	Q 标签	修改实例属性 注
实例ID/名称 标签 监控 可用区 IP地址	状态 → 网络类型 → 配置	授予/收回RAM角色 操作
□ ◆ ◆ ★ 东京可用区A	(公) ① 运行中 专有网络 1 vCPU 1 GB (I/O优化) ecs.xr4.small 1Mbps (建復)	编辑标签 连接帮助 更改实例则格 更多√ 词签信主机部署 购买相同配置
□ 启动 停止 重启 重置实例密码 续费 按量付	费转包年包月 释放设置 更多▲ 共	调整实例所属部署集 实例状态 有1 保存为启动模板 实例设置
		密码/密钥 🕨
		资源变配 ▶
		磁曲和鏡像
		运堆和诊断

- 3. 在授予/收回RAM角色对话框中选择RAM角色为步骤一创建的RAM角色。
 - ⑦ 说明 若您还未创建RAM角色,请单击创建RAM角色进行创建。

授予/收回RAM角色 🕐 P	RAM实例角色授权	×
操作类型:	● 授予	
操作说明:	实例绑定RAM角色将授予实例该角色所拥有的所有权限,请 谨慎操作。	
*RAM角色:	请选择	
	确定	取消

步骤三:将RAM角色名称告知ACM SDK并访问配置

将RAM角色名称告知ACM SDK(版本1.0.8及以上)方法有两种:通过JVM参数设置和通过代码传参设置。

⑦ 说明 JVM参数设置方式优先级高于代码传参方式。

- 通过JVM参数设置:
 - 格式: -Dram.role.name=\$ramRoleName
 - 示例: -Dram.role.name=ECS-RAM
- 通过代码传参设置:

import java.util.Properties; import com.alibaba.edas.acm.ConfigService; import com.alibaba.edas.acm.exception.ConfigException; //示例代码,仅用于示例测试public class ACMTest { public static void main(String[] args) { try { Properties properties = new Properties(); // endpoint可以从ACM控制台 "命名空间详情"或 "示例代码"中获取properties.put("endpoint", "\$end point"); // namespace可以从ACM控制台 "命名空间详情" 或 "示例代码"中获取properties.put("namespace", "\$ namespace"); // 刚刚新建并绑定到ECS实例的RAM角色名称,如 "ECS-RAM" properties.put("ramRoleName", "\$ramRo leName"); ConfigService.init(properties); // 主动获取配置String content = ConfigService.getConfig("\${dataId}", "\${group}", 6000); System.out.println(content); } catch (ConfigException e) { e.printStackTrace(); } } }

更多信息

- Access Key (AK)
- RAM (访问控制)
- 创建可信实体为阿里云服务的RAM角色
- 使用实例RAM角色访问其他云产品
- ACM Java Native SDK概述

5.利用RAM角色实现跨账号访问ACM

使用企业A的阿里云主账号创建RAM角色、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的主账号或其RAM用户访问企业A的ACM资源的目的。

迁移到MSE Nacos

ACM进入下线状态,所有配置管理相关的需求由MSE中的Nacos承接(ACM独享版,更好的安全和稳定性)。您需要在ACM控制台导出配置,然后在MSE控制台导入之前导出的配置即可完成迁移。具体操作,请参见将应用配置从ACM迁移到MSE Nacos。

跨账号授权流程

假设企业A(账号ID为11223344,企业别名为Company-a)需要将ACM操作权限授予企业B(账号ID为 12345678,企业别名为Company-b)的员工C,则授权流程为:

- 1. 步骤一: 企业A创建角色
- 2. 步骤二:企业A为该角色授权
- 3. 步骤三:企业B创建RAM用户
- 4. 步骤四:企业B为RAM用户授权
- ⑦ 说明 关于企业别名的详细信息,请参见创建并验证域别名。

步骤一:企业A创建角色

- 1. 使用企业A的云账户登录RAM控制台,在左侧导航栏中选择RAM角色管理。
- 2. 在RAM角色管理页面上单击创建RAM角色。
- 3. 在创建RAM角色对话框中执行以下操作并单击确定。
 - i. 在选择类型区域选择阿里云账号,单击下一步。
 - ii. 输入角色名称文本框内输入需授权的云帐户。

在本示例中, 输入acm-admin。

iii. 选择**其他云账号**,并输入需授权的云帐户,单击完成。

在本示例中,输入企业B的账号ID 12345678。

步骤二:企业A为该角色授权

新创建的角色没有任何权限,因此企业A必须为该角色授权。在本示例中,企业A要将授权策略AliyunACMFullAccess分配给该角色,从而使该角色能够访问ACM资源。

- 1. 登录RAM控制台, 在左侧导航栏中选择RAM角色管理。
- 2. 在RAM角色管理页面上单击目标角色操作列中的添加权限。
- 3. 在添加权限对话框左侧的系统权限策略中找到AliyunACMFullAccess策略,并单击该策略,然后单击确定。

test@	5.onaliyu	in.com ×				
选择权限						
系统权限策略 🛛 🗸	AliyunA	ACMFullAccess	8	Q	已选择(1)	7
权限策略名称		备注			AliyunACMFullAccess	×
AliyunACMFullAccess		管理应用配置管理(ACM)的权限				

② 说明 如果还使用到ACM的加解密配置功能,则还需要为用户添加AliyunKMSCryptoAccess授权策略。

↓ 注意 此步骤将授予ACM的全部访问权限。如果希望授予单个命名空间的特定权限,请参见访问权限。
限控制。

步骤三:企业B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。
- 2. 在用户页面上单击创建用户,在用户账号信息区域输入用户的登录名称和显示名称。

↓ 注意 登录名称必须在云账户内保持唯一。

如需创建多个用户,则单击添加用户,并输入登录名称和显示名称。

新建用户页面



3. 在**访问方式**区域选择控制台密码登录,然后按需设置控制台密码、要求重置密码和多因素认证,并 单击确定。

完成以上步骤后,一个可以登录控制台的RAM用户就创建成功了。

步骤四:企业B为RAM用户授权

- 1. 登录RAM控制台, 在左侧导航栏中选择人员管理 > 用户。
- 2. 在用户页面上单击目标用户操作列中的添加授权。
- 3. 在**添加权限**对话框左侧的**系统策略**中找到AliyunSTSAssumeRoleAccess策略,并单击该策略,然后单击确定。

步骤五:使用企业B的RAM用户跨账号访问资源

- 1. 使用云账户登录RAM控制台, 在左侧导航栏中选择概览。
- 2. 在账号管理区域单击用户登录地址链接。

账号管理
主账号
用户登录地址
https://signin.aliyun.com/
域别名

3. 在**阿里云-RAM用户登录**页面上按照提示输入登录用户名称,单击**下一步**,然后输入密码并单击登 **录**。

子用户登录
登录用户名称
RAM用户新版登录格式: <子用户名称>@ <企业别名> 例 如:username@company-alias
T-1E

- 4. 在子用户用户中心页面上, 单击互联网中间件类目下的应用配置管理进入ACM控制台。
- 5. 登录成功后,将鼠标指针移到右上角头像,并在浮层中单击**切换身份**。
- 6. 在**阿里云 角色切换**页面, 输入企业A的企业别名Company-a(或默认域名) 和角色名acm-admin, 然后单击**切换**。
- 7. 对企业A的ACM资源执行操作。

相关文档

- RAM用户
- RAM角色
- 创建并验证域别名