# IAM 5.0 最佳实践

**文档版本** 01

**发布日期** 2025-11-05

**华为云计算技术有限公司**

### 商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

### 注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

## 华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

# 目 录



# 1 安全使用 IAM

## 通过 IAM 身份中心集中管理人机用户并使用联邦认证

华为云的用户可以是管理员、开发者、使用应用程序的用户（例如，业务分析师，数据分析师等），他们使用CLI、控制台或者是客户端应用程序访问华为云，他们通常位于企业或者组织的内部。有时，他们也可能是企业或组织外部的用户。这些用户必须有身份凭证才能访问华为云。推荐使用**IAM 身份中心**管理这些用户，这样带来的好处是：

- 可以对用户进行集中管理，企业或组织成员的变动只通过一个系统完成，减少维护成本。
- 用户认证凭据的集中管理，不需要在许多单独的系统中创建或维护密码。
- 减少身份系统的数量，通过一个身份提供商管理所有用户。
- 便于审计，单一的身份源会使审计变得容易。

## 机机用户通过 IAM 委托或信任委托的临时访问密钥访问华为云

使用临时访问密钥是一个好的安全实践，因为它们的生命周期有限，并且会自动过期，所以临时凭证不需要进行轮转，也不需要在不需要它们时进行注销。推荐使用IAM委托或者信任委托的的方式给机机账号颁发临时凭证，而不是IAM用户的永久访问密钥。

## 不将访问密钥嵌入到代码中

当您使用API、CLI、SDK等开发工具来访问云服务时，请勿直接将访问密钥嵌入到代码中，减少访问密钥被泄露的风险。

## 创建单独的 IAM 用户

如果有任何人需要访问您账号中的资源，请不要将账号的密码共享给他们，而是在您的账号中给他们创建单独的IAM用户并分配相应的权限，同时，建议您不要直接使用账号访问华为云，而是为自己创建一个IAM用户，并授予该用户管理权限，以使用该IAM用户代替账号进行日常管理工作，保护账号的安全。

## 合理设置访问方式

您可以通过不同的方式访问华为云，在IAM新版控制台创建的IAM用户，具体访问方式取决于IAM用户的凭证类型。如果您在创建IAM用户时设置了控制台密码，则该IAM用

户可以通过控制台方式来访问华为云；如果给IAM用户创建了访问密钥，则该IAM用户可以通过编程方式来访问华为云。在IAM旧版控制台创建的IAM用户，则需要对**访问方式**进行显示设置，可以在创建IAM用户时或者创建后从用户列表进入IAM用户的安全设置中进行设置。

## 开启虚拟 MFA 功能

Multi-Factor Authentication（简称MFA）是一种非常简单的安全实践方法，建议您给账号以及您账号中的IAM用户开启MFA功能，它能够在用户名和密码之外再额外增加一层保护。启用MFA后，用户登录控制台时，系统将要求用户输入用户名和密码（第一安全要素），以及来自其MFA设备的验证码（第二安全要素）。这些多重要素结合起来将为您的账号和资源提供更高的安全保护。

MFA设备目前包含虚拟MFA和安全密钥两种。虚拟MFA是能产生6位数字认证码的应用程序，此类应用程序可在移动硬件设备（包括智能手机）上运行，非常方便。安全密钥是基于FIDO协议的双因素认证，华为云当前支持基于FIDO协议的硬件设备和Windows Hello的安全密钥。

## 设置强密码策略

在IAM控制台设置强密码策略，例如密码最小长度、密码中同一字符连续出现的最大次数、密码不能与历史密码相同，保证用户使用复杂程度高的强密码。

## 设置敏感操作

设置敏感操作后，如果您或者您账号中的用户进行敏感操作时，例如删除资源、生成访问密钥等，需要输入密码和验证码进行验证，避免误操作带来的风险和损失。

## 定期修改身份凭证

如果您不知道自己的密码或访问密钥是否已泄露，定期进行修改可以将不小心泄露的风险降至最低。

- 定期轮换密码可以通过设置密码有效期策略进行，您以及您账号中的用户在设置的时间内必须修改密码，否则密码将会失效，IAM会在密码到期前15天开始提示用户修改密码。
- 轮换访问密钥可以通过创建两个访问密钥进行，将两个访问密钥作为一主一备，一开始先使用主访问密钥一，一段时间后，使用备访问密钥二，然后在控制台删除主访问密钥一，并重新生成一个访问密钥，在您的应用程序中定期轮换使用。

## 删除不需要的身份凭证

对于仅需要登录控制台的IAM用户，不需要使用访问密钥，请不要给他们创建，或者及时删除访问密钥。您还可以通过账号中IAM用户的“最近一次登录时间”，来判断该用户的凭证是否已经属于不需要的范畴，对于长期未登录的用户，请及时修改他们的身份凭证，包括修改密码和删除访问密钥，您还可以设置“账号停用策略”来控制长期未使用的账号到期自动停用。

## 开通云审计服务

您可以通过云审计服务（Cloud Trace Service，CTS）对IAM的关键操作事件进行收集、存储和查询，用于安全分析、合规审计、资源跟踪和问题定位等。为了方便查看IAM的关键操作事件，例如创建用户、删除用户等，建议您开启云审计服务。

## 遵循最佳实践保护账号身份凭证

账号是您华为云资源归属、资源使用计费的主体，对其所拥有的资源及云服务具有完全的访问权限。请您像保护个人隐私数据一样保护账号的身份凭证。

- 请勿为账号创建访问密钥

  密码与访问密钥（AK/SK）都是账号的身份凭证，具有同等效力，密码用于登录界面控制台，是您必须具备的身份凭证，访问密钥用于使用开发工具进行编程调用，是第二个身份凭证，为辅助性质，非必须具备。为了提高账号安全性，建议您仅使用密码登录控制台即可，不要给账号创建第二个身份凭证（访问密钥），避免因访问密钥泄露带来的信息安全风险。

- 保护您的账号身份凭证，不允许未经授权使用账号

  加强账号身份凭证的保护，请勿泄露您的密码，多因子认证、AK/SK，严格限制需要通过账号身份凭据进行认证的业务范围。

- 使用强密码来加强访问保护

  推荐使用密码工具生成强密码，请勿将密码设置为您的账号名或者是邮箱地址。

- 开启多因素认证

  强烈建议为账号开启多因素认证。

- 尽可能使用多人审批进行账号的登录

  推荐使用多人审批，防止一个人可以同时使用密码和多因子认证进行账号登录。例如，可以通过设置一组有权限访问密码的管理员和另一组有权限访问多因子认证的管理员，必须通过至少两个人的审批才能进行账号登录。

- 监控账号的权限以及使用情况

  建议通过华为云审计服务（CTS）监控账号的使用情况，如发现异常活动请及时进行安全审计与防范。

## 授予最小权限

最小权限原则是标准的安全建议，您可以使用IAM提供的系统权限，或者自己创建自定义策略或身份策略，给账号中的用户仅授予刚好能完成工作所需的权限，通过最小权限原则，可以帮助您安全地控制用户对华为云资源的访问。

同时，建议为使用API、CLI、SDK等开发工具访问云服务的IAM用户，授予自定义策略或身份策略，通过精细的权限控制，减小因访问密钥泄露对您的账号造成的影响。

- 将管理员使用的IAM用户和程序用的IAM用户区分开。
- 管理员使用的IAM用户，建议使用身份联邦，密码在企业线下身份系统。
- 程序使用IAM用户，授予程序需要访问的API对应的权限，禁止登录控制台（避免保存密码）。
- 禁止重要数据资产的下载和删除权限被授权，或针对重要数据的下载（部分敏感数据的查询）和删除权限，仅授予几个重要的IAM用户（联邦用户），这些用户的密码禁止分享，杜绝账号密码泄露带来的影响。

## 使用 IAM 策略或身份策略中的条件进一步限制访问权限

推荐使用IAM策略或身份策略进一步限制访问权限，例如，您可以编写一个策略或身份策略来限制只允许特定的IAM用户执行特定的操作。有关更多信息，请参阅**IAM权限管理**。

## 移除（或不生成）账号根用户访问密钥

保护账号的最佳方法之一是不为账号根用户设置访问密钥。除非必须具有账号根用户访问密钥（这种情况很少见），否则建议不要生成根用户访问密钥。最佳实践是在华为云IAM身份中心中创建一个管理用户来执行日常管理任务。有关如何在 IAM 身份中心中创建管理用户的信息，请参见**IAM 身份中心快速入门**。

如果您已经拥有并在使用账号的根用户访问密钥，建议您执行以下操作：找到您当前在应用程序中使用访问密钥的位置，然后使用IAM用户访问密钥替换根用户访问密钥，最后再禁用并移除根用户访问密钥。

## 控制访问密钥的使用

作为最佳实践，我们建议工作负载使用**临时安全凭证**来访问华为云，如果一定要使用永久访问密钥，我们建议向拥有永久访问密钥的IAM用户授权时遵循最小权限原则，并启用多因素认证（MFA）。

例如，您正在进行一些短期的测试，并选择使用IAM用户的永久访问密钥来运行工作负载，我们建议您使用条件键来进一步限制用户的权限。在这种情况下，您可以创建有时限的身份策略附加在IAM用户身上，使用户的权限在指定时间后过期；或者如果您是从安全网络运行工作负载，可以使用限制IP的身份策略。

- **为IAM用户配置限时策略**
  a. 管理员登录**统一身份认证服务新版控制台**。
  b. 在左侧导航窗格中，选择“身份策略”。
  c. 单击右上方的“创建自定义身份策略”，输入策略名称，策略配置方式选择JSON视图。
  d. 在“策略内容”区域中输入以下策略，将 g:CurrentTime 条件键的值替换为所需的到期时间。

```
{
   "Version": "5.0",
   "Statement": [{
      "Effect": "Deny",
      "Action": [
         "*"
      ],
      "Condition": {
         "DateGreaterThan": {
            "g:CurrentTime": [
               "2025-07-15T08:53:13Z"
            ]
         }
      }
   }]
}
```

  该策略使用Deny效果来限制在指定日期后对所有资源执行所有操作。DateGreaterThan运算符用于比较当前的时间是否大于您设置的时间。
  e. 选择确定，返回身份策略页面。在选择策略身份搜索框，输入刚才创建的策略名称，选择对应身份策略，单击“附加”，将对应身份策略附加到指定IAM用户身上。

  附加身份策略后，身份策略将显示在用户的权限选项卡上。当前时间大于或等于该身份策略中指定的时间时，用户就无法再访问华为云资源。请务必让开发人员了解您为这些用户权限指定的到期日期。

- **为IAM用户配置IP限制策略**
  a. 管理员登录**统一身份认证服务新版控制台**。

b. 在左侧导航窗格中，选择“身份策略”。

c. 单击右上方的“创建自定义身份策略”，输入策略名称，策略配置方式选择JSON视图。

d. 在“策略内容”区域中，将以下IAM策略复制到 JSON 编辑器，并根据需要更改对应公网IP地址或范围。您可以使用斜杠标记指定单个IP地址或IP地址范围。有关更多信息，请参阅**g:SourceIp条件键**。

```
{
   "Version": "5.0",
   "Statement": [{
         "Effect": "Deny",
         "Action": [
            "*"
         ],
         "Resource": [
            "*"
         ],
         "Condition": {
            "NotIpAddress": {
               "g:SourceIp": [
                  "xx.xx.xx.0/32"
               ]
            },
            "BoolIfExists": {
               "g:ViaService": [
                  "false"
               ]
            }
         }
      },
      {
         "Effect": "Deny",
         "Action": [
            "*"
         ],
         "Resource": [
            "*"
         ],
         "Condition": {
            "NotIpAddress": {
               "g:SourceIp": [
                  "xx.xx.xx.0/32"
               ]
            },
            "StringEquals": {
               "g:CalledViaFirst": "service.console",
               "g:CalledViaLast": "service.console"
            }
         }
      }
   ]
}
```

该策略使用Deny效果来限制在指定IP外对所有资源执行所有操作。NotIpAddress运算符指指定IP地址或者IP范围之外的所有IP地址。

e. 选择“确定”，返回身份策略页面。在选择策略身份搜索框，输入刚才创建的策略名称，选择对应身份策略，单击“附加”，将对应身份策略附加到指定IAM用户身上。

您还可以将以下策略作为服务控制策略 (SCP) 应用于华为云中的多个账号，我们建议您使用条件键g:PrincipalUrn让该策略仅适用于受此SCP约束的账号中的IAM用户：

```
{
   "Version": "5.0",
   "Statement": [{
         "Effect": "Deny",
         "Action": [
```

```
            "iam:*:*"
         ],
         "Resource": [
            "*"
         ],
         "Condition": {
            "NotIpAddress": {
               "g:SourceIp": [
                  "xx.xx.xx.0/32"
               ]
            },
            "BoolIfExists": {
               "g:ViaService": [
                  "false"
               ]
            },
            "StringMatch": {
               "g:PrincipalUrn": [
                  "iam::<account-id>:user:<user-name>"
               ]
            }
         }
      },
      {
         "Effect": "Deny",
         "Action": [
            "iam:*:*"
         ],
         "Resource": [
            "*"
         ],
         "Condition": {
            "NotIpAddress": {
               "g:SourceIp": [
                  "xx.xx.xx.0/32"
               ]
            },
            "StringEquals": {
               "g:CalledViaFirst": "service.console",
               "g:CalledViaLast": "service.console"
            },
            "StringMatch": {
               "g:PrincipalUrn": [
                  "iam::<account-id>:user:<user-name>"
               ]
            }
         }
      }
   ]
}
```

# 2 根用户最佳实践

您在华为云注册的账号天然具有账号下所有资源的最大操作权限，该身份叫做根用户，您可以使用账号名+密码登录华为云，也可以使用账号名+和账号同名的用户名+密码登录华为云。根用户的凭证泄露后将影响整个账号下所有的资源和数据，请妥善保管根用户的凭证。我们强烈建议您注册账号后，创建用户并加入admin用户组，使该用户作为管理员用户管理其他身份并分配权限，避免直接使用根用户的身份执行任何非必要的操作。

## 妥善保管根用户的密码

为了保护根用户的安全，请妥善保管根用户的凭证，包括密码、访问密钥和MFA验证设备，避免与他人共享，并仅在必需的情况下才使用根用户的凭证。

## 为根用户设置强密码

建议您为根用户设置高复杂度的强密码，例如：

- 密码长度至少为8位以上字符。
- 至少包含以下字符中的2种：大写字母、小写字母、数字、特殊字符。
- 避免使用账号名或邮箱作为密码。

## 使用多重身份验证（MFA）保护您的根用户登录安全

因为根用户天然具有账号下所有资源的最大操作权限，所以强烈建议您为根用户绑定MFA验证设备，并开启登录二次验证。

- 若您的账号是未升级华为账号的华为云账号，可以在IAM控制台中“用户 > 根用户（描述为企业管理员的用户）> 安全设置 > 多因素认证设备 > 添加MFA设备”中绑定MFA设备，此时会自动开启登录保护。华为云账号的根用户当前仅支持虚拟MFA和基于FIDO身份验证协议和Windows Hello的安全密钥作为登录二次验证方式。
- 若您的华为云账号已升级为华为账号，将不支持在“安全设置”页面绑定MFA设备，请在“华为账号中心>账号与安全>安全验证>双重验证”中单击“开启”，输入验证信息，开启登录保护。华为账号的根用户当前仅支持手机、邮箱和虚拟MFA作为登录二次验证方式。

## 使用多人审批进行根用户登录

为了在根用户的密码和MFA以外再增加一层安全防护，建议您将根用户的MFA设备和密码分配给不同的人进行保管，确保根用户每次登录必须经过多人的许可审批。

## 不给根用户创建访问密钥

账号是您华为云资源归属、资源使用计费的主体，对其所拥有的资源及云服务具有完全的访问权限。账号中根用户的密码与访问密钥（AK/SK）都是账号的身份凭证，具有同等效力，密码用于登录界面控制台，是您必须具备的身份凭证，访问密钥用于使用开发工具进行编程调用，是第二个身份凭证，为辅助性质，非必须具备。为了提高账号安全性，建议您仅使用密码登录控制台即可，不要给根用户创建第二个身份凭证（访问密钥），避免因访问密钥泄露带来的信息安全风险。

## 保护组织中组织管理账号和组织成员账号的根用户

当您使用Organizations服务进行多账号管理时，组织管理账号和组织成员账号的根用户也需要进行以上的安全措施进行防护。

## 在 Organizations 服务中使用服务控制策略（SCP）限制根用户的行为

您可以在Organizations服务中使用SCP限制根用户的访问，例如拒绝组织中所有成员账号的根用户操作ECS实例，详细信息请参见**SCP配置示例**。

## 自动评估根用户设置是否合规

Config服务对根用户合规情况进行检测，您可以使用Config服务检测**根用户存在可使用的访问密钥**，还可以检测**根用户开启MFA认证**。

如果您对根用户存在安全方面的疑问，也可以通过官网提交工单或拨打400服务热线（4000-955-988或950808）方式反馈。

# 3 通过 IAM 对多运维人员进行权限设置

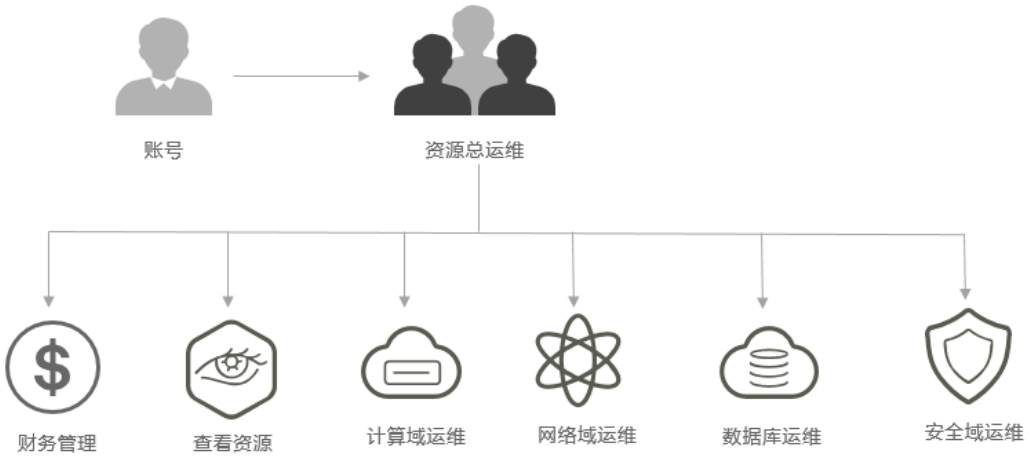
## 方案概述

A公司在华为云中购买了多种资源，公司中有多个职能团队，这些职能团队需要使用一种或者多种资源，因此涉及到多运维人员权限设置需求，通过IAM的身份策略功能可以实现该需求。

## 资源规划

根据A公司中员工所负责的不同职能，将员工划分为以下七个团队。

**图 3-1** 权限设置模型




- 资源总运维：负责管理公司所有资源的团队。
- 财务管理：负责管理公司财务的团队。
- 查看资源：负责查看并监控所有资源使用情况的团队。
- 计算域运维：负责计算域运维的团队。
- 网络域运维：负责网络域运维的团队。
- 数据库运维：负责数据库运维的团队。
- 安全域运维：负责安全域运维的团队。

通过**表1**，给公司中不同的职能团队设置不同的权限，可以实现各团队之间权限隔离，各司其职。如需了解华为云所有云服务的系统权限，请参见：**系统身份策略**。

**表 3-1** 团队权限说明

| 职能团队 | 需要授予的策略 | 权限说明 |
| --- | --- | --- |
| 资源总运维 | AdministratorAccessPolicy | 所有服务的所有权限。 |
| 财务管理 | BILLINGFullAccessPolicy | 费用中心、账号中心、成本中心、企业中心、消息中心的所有执行权限。 |
| 查看资源 | ReadOnlyPolicy | 所有服务的只读权限。 |
| 计算域运维 | ECSFullPolicy | 弹性云服务器（ECS）的所有执行权限，包括购买ECS的权限，仅拥有该权限的用户不能查看ECS以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。 |
| | CCEFullPolicy | 云容器引擎（CCE）的所有执行权限，包括购买CCE的权限，仅拥有该权限的用户不能查看CCE以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。 |
| | ASFullPolicy | 弹性伸缩（AS）的所有执行权限，包括购买AS的权限，仅拥有该权限的用户不能查看AS以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。 |

| 职能团队 | 需要授予的策略 | 权限说明 |
| --- | --- | --- |
| 网络域运维<br>数据库运维<br>安全领域运维 | VPCFullAccessPolicy<br>ELBFullAccessPolicy<br>RDSFullAccessPolicy<br>DDSFullAccessPolicy<br>DDMFullAccessPolicy<br>Anti-DDoSFullAccessPolicy<br>AADFullAccessPolicy<br>KMSFullAccessPolicy | 虚拟私有云（VPC）的所有执行权限，包括购买VPC的权限，仅拥有该权限的用户不能查看VPC以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。<br>弹性负载均衡（ELB）的所有执行权限，包括购买ELB的权限，仅拥有该权限的用户不能查看ELB以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。<br>云数据库（RDS）的所有执行权限，包括购买RDS的权限，仅拥有该权限的用户不能查看RDS以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。<br>文档数据库服务（DDS）的所有执行权限，包括购买DDS的权限，仅拥有该权限的用户不能查看DDS以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。<br>分布式数据库中间件的所有执行权限。<br>Anti-DDoS流量清洗服务的所有执行权限。<br>DDoS高防服务的所有执行权限。<br>KMS的所有权限策略，包括购买KMS的权限，仅拥有该权限的用户不能查看KMS以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。 |

根据以上职能团队的划分，资源规划情况包含以下内容：

**表 3-2** 资源规划

| 资源 | 资源名称 | 资源说明 | 数量 |
| --- | --- | --- | --- |
| 管理员账号 | Company-A | A公司用于管理资源和权限所创建的账号。 | 1 |
| IAM用户组 | 网络域运维 | A公司根据团队职能需要划分为七个用户组，此处仅以创建用户组“网络域运维”为例。 | 1 |
| IAM用户 | James、Alice | 此处仅以创建IAM用户“James”和“Alice”为例。 | 2 |

| 资源 | 资源名称 | 资源说明 | 数量 |
| --- | --- | --- | --- |
| 权限 | VPC FullAccess、ELB FullAccess | 根据上表可知，需要为“网络域运维”用户组配置两个权限。 | 2 |

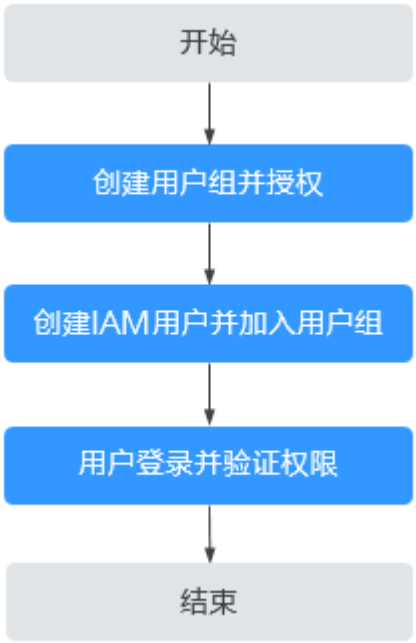
**说明**

因为统一身份认证服务为免费服务，因此此最佳实践中不涉及费用。

## 操作流程

IAM通过用户组功能实现用户的授权。本文档以A公司将一个员工配置为网络域运维负责人为例，介绍如何通过IAM实现多运维人员权限设置需求，流程如**图2 操作流程**所示。如果需要将员工配置为其他运维负责人，请参考**表1 团队权限说明**，为相关负责人授予相应的系统身份策略。

**图 3-2** 操作流程




### 步骤一：创建用户组并授权

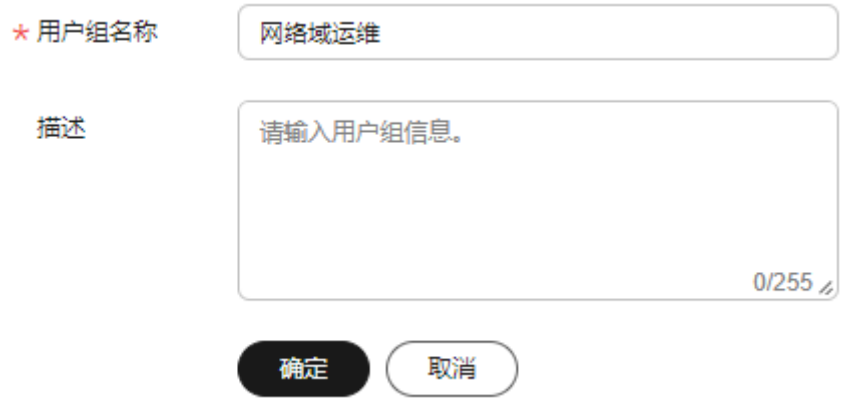
1. A公司管理员登录并进入华为云控制台。
2. 在控制台页面中将鼠标移动至右上角的用户名，选择“统一身份认证”。
3. 在统一身份认证服务的左侧导航空格中，单击“用户组”>“创建用户组”。

**图 3-3** 创建用户组

4. 在“创建用户组”界面，输入“用户组名称”为“网络域运维”，单击“确定”。用户组名称只能包含中文、大小写字母、数字、空格或特殊字符(-_)。

**图 3-4** 输入名称




5. 单击新建用户组右侧的“授权”。

**图 3-5** 授权

6. 在搜索框中搜索“VPCFullAccessPolicy”和“ELBFullAccessPolicy”，勾选并单击“确定”。

**图 3-6** 勾选权限


7. 单击“确定”，完成对“网络域运维”用户组的授权。创建成功的用户组将会展示在用户组列表中。

   可以单击“网络域运维”用户组的名称，在“授权记录”页签下查看已授予的权限。

**步骤二：创建IAM用户并加入用户组**

1. A公司管理员在统一身份认证服务，左侧导航中，选择“用户”。
2. 在用户页面，单击右上角“创建用户”。

**图 3-7** 创建用户

3. 配置用户James和Alice的基本信息

   在“创建用户”界面填写“用户名”、“描述”和“管理控制台访问”，并设置密码。

**图 3-8** 配置用户信息


4. 单击“下一步”，将IAM用户James、Alice加入到上一步中创建的“网络域运维”用户组。

**图 3-9** 加入用户组


5. 单击“创建创建用户”，IAM用户创建完成，此时可以下载登录密码。

**图 3-10** 创建成功


步骤3：IAM用户登录并验证权限

IAM用户登录有多种方式，如下步骤仅讲述其中一种，更多登录方式请参见：**登录华为云**。

1. IAM用户James或Alice在华为云登录页面，单击右下角的“IAM用户登录”。
2. 在“IAM用户登录”页面，输入A公司账号名Company-A、IAM用户名及用户密码。
   - 账号名为该IAM用户所属账号的名称。

– 用户名和密码为账号在IAM创建用户时输入的用户名和密码。

**图 3-11** IAM 用户登录


3. 登录成功后，IAM用户进入华为云控制台。
4. 在“服务列表”中选择虚拟私有云VPC、弹性负载均衡ELB，可以进入这些服务的主页面并进行管理操作，权限配置成功。
5. 在“服务列表”中选择除以上服务外的任一服务，系统提示权限不足，权限配置成功。

# 4 使用信任委托实现跨账号的资源授权与管理

A公司和B公司是华为云注册的企业用户，分别拥有自己单独的账号。本文主要介绍当A账号希望将部分资源委托给B账号时，使用IAM的信任委托功能来实现跨账号的资源授权与管理（A账号为委托方，B账号为被委托方）。

## 企业需求

- A账号在华为云购买了多种资源，为了专注自己的业务领域，希望将VPC资源委托给B账号进行代运维。
- B账号希望将A账号委托的资源分配给公司中一个或多个员工（IAM用户），进行精细的权限管理。
- 如果合作关系发生变更，A账号希望随时可以修改或撤销对B账号的授权。

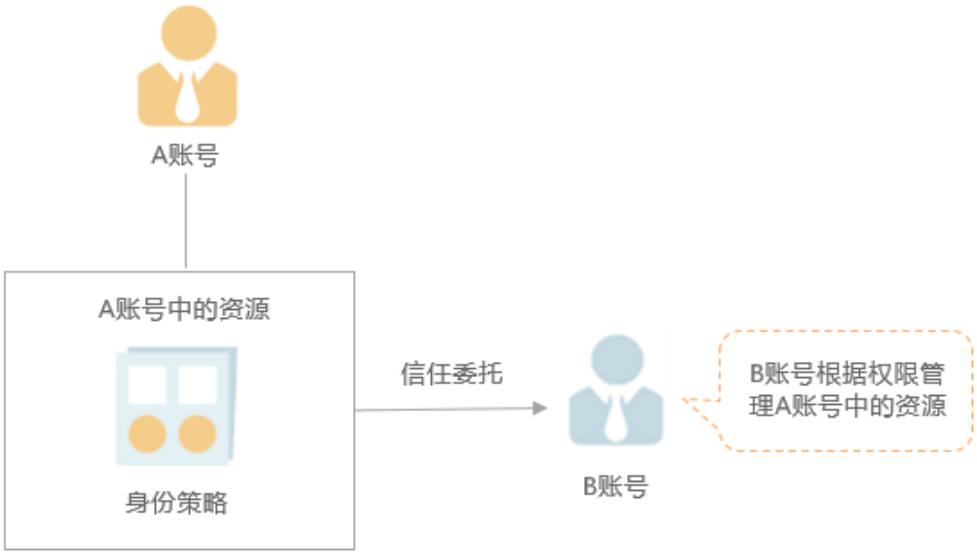
## 解决方案

针对以上企业需求，可以使用IAM的信任委托功能来实现跨账号的资源授权与管理。

- A账号在IAM控制台创建一个信任委托，指定信任委托的信任主体为B账号，并将需要代运维的资源授权给这个信任委托。
- B账号进一步授权，将A账号委托的资源分配给账号下专职管理信任委托的IAM用户，让IAM用户帮助管理。
- 当合作关系发生变更时，A账号随时可以修改或者删除这个信任委托，B账号以及账号下可以管理该信任委托的用户对该信任委托的使用权限将自动修改或者撤销。

**图 4-1** 跨账号授权模型




## 委托方跨账号授权

以A账号将VPC资源委托给B账号进行代运维为例，说明委托方进行跨账号授权的操作方法。

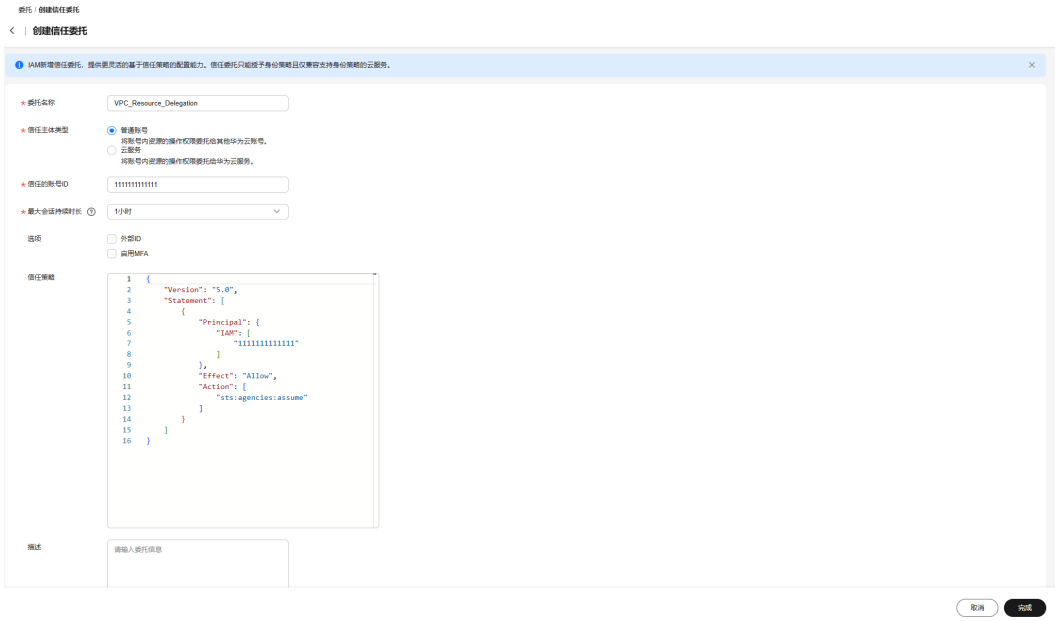
**步骤1** A账号登录华为云，在统一身份认证服务中，单击“委托”。

**步骤2** 在“委托”页面，单击“创建信任委托”，设置“委托名称”，例如“VPC_Resource_Delegation”。

**步骤3** “信任主体类型”选择“普通账号”，在“信任的账号ID”中填入B公司的账号ID。

**步骤4** 设置“最大会话持续时长”。

**图 4-2** 创建信任委托



**步骤5** 选择是否使用“外部ID”。被委托方的外部ID需要唯一，不可以与其他被委托方的外部ID重复。外部ID可以是只有您和被委托方所熟知的任何标识符。例如，您和被委托方之间可以使用发票号等，但不要使用可以猜测的信息，如被委托方的姓名或电话号码。选择使用“外部ID”，系统会将外部ID添加至信任策略中，信任策略会检查外部ID，能够确保被委托方执行了正确的操作。注意：使用了“外部ID”之后，将无法在IAM控制台切换该信任委托，因为IAM控制台切换时不会帮您传递“外部ID”，此时被委托方可以使用**AssumeAgency API**携带“外部ID”后进行切换该信任委托。

**步骤6** 选择是否“启用MFA”。

启用MFA后，在登录验证页面被委托方必须需要输入MFA设备中的验证码进行二次认证，之后才能在控制台中切换该信任委托。

**步骤7** 信任策略区域将会展示当前信任策略的内容，如需编辑请在创建后修改信任委托。

**步骤8** 填写“描述”信息，单击“完成”。

**步骤9** 在授权的确认弹窗中，单击“立即授权”。

**步骤10** 选择权限“VPCFullAccessPolicy”，单击“确定”。

委托创建完成，委托列表中显示新创建的信任委托。

**说明**

当合作关系发生变更时，A账号可以在委托列表中，单击“修改”，修改信任委托的信任账号、权限等。

**----结束**

## 被委托方跨账号管理

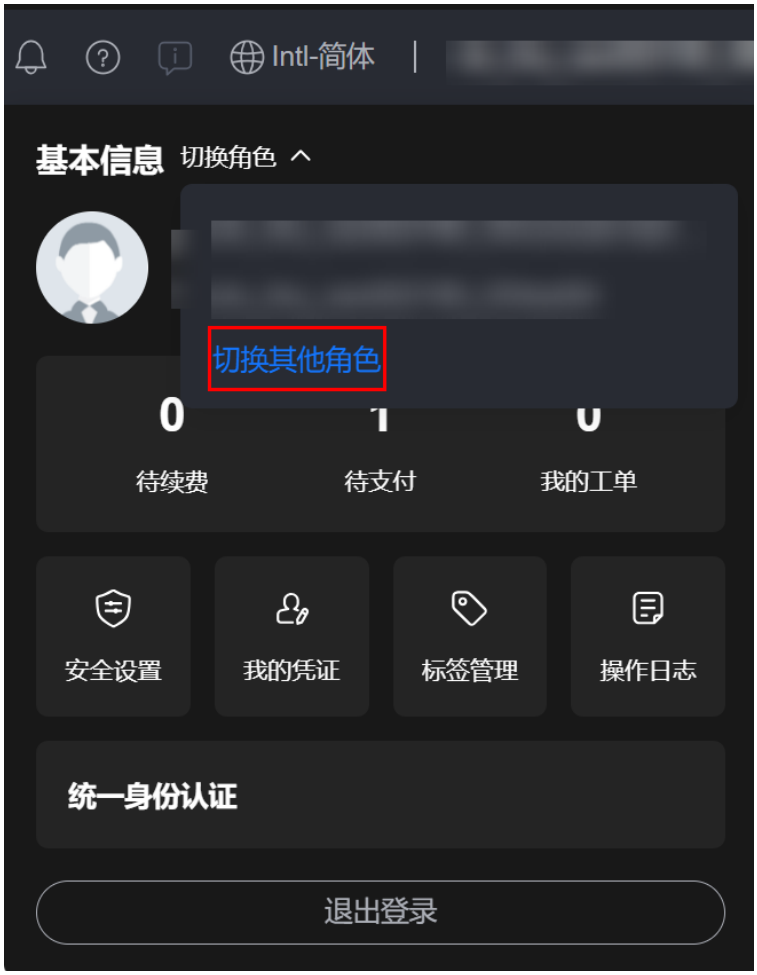
当A账号与B账号创建委托关系后，即B账号为被委托方，B账号通过切换信任委托的方法（控制台中是在切换角色页面进行切换信任委托），可以切换到A账号中，管理委托方授权的资源。B账号需要提前获取A账号的名称以及所创建的信任委托名称。

**步骤1** B账号登录华为云，进入控制台。

**步骤2** 鼠标移动至右上方的用户名，选择“切换角色”。选择角色切换记录或单击其他切换指定的信任委托。

**图 4-3** 切换角色




**步骤3** 在“切换角色”页面中，输入委托方的账号名称以及委托名称，同时也可以直接单击切换历史记录直接切换。

**注意**

输入委托方的账号名称之后，只会列举出委托方委托给您的普通委托，而不会列举出信任委托，您需要手动输入名称进行切换。

**图 4-4** 输入信任委托名称


**步骤4** 单击“确定”，B账号切换至委托方A账号中，直接对A账号的VPC资源进行管理。

**----结束**

## 被委托方分配委托权限

以B账号将信任委托分配给IAM用户进行管理为例，实现分配信任委托以及对信任委托进行精细授权。信任委托权限分配完成后，B账号中的IAM用户通过切换信任委托的方式，可以切换到A账号中，管理委托方授权的资源。

B账号需要提前获取委托公司的账号名称、所创建的信任委托名称。

**步骤1** 创建用户组。

1. B账号在统一身份认证服务左侧导航窗格中，单击“用户组”。
2. 在“用户组”界面中，单击“创建用户组”。
3. 输入“用户组名称”，例如“委托管理”。
4. 单击“确定”。

**步骤2** 创建自定义身份策略。

1. 在身份策略界面，单击“创建自定义身份策略”。
2. 策略名称输入“AssumeAgencies”。
3. “策略配置方式”选择“JSON视图”。
4. 在“策略内容”区域，填入以下内容：在自定义身份策略中，设置用户仅能管理指定ID的信任委托，不能管理其他信任委托。

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "sts:agencies:assume"
        ],
        "Resource": [
            "iam::<account-a-id>:agency:VPC_Resource_Delegation"
        ]
    }]
}
```

**说明**

<account-a-id>需要替换为委托方的账号ID，需要提前向委托方获取，其他内容不需修改，直接拷贝即可。

**步骤3** 为用户组授权。

1. 返回用户组列表，用户组列表中显示新创建的用户组。
2. 单击新建用户组右侧的“授权”，进入授权界面。
3. 选择上一步创建的自定义身份策略，单击“下一步”，单击“确定”，授权完成。

**图 4-5** 授权


**步骤4** 创建用户并加入用户组。

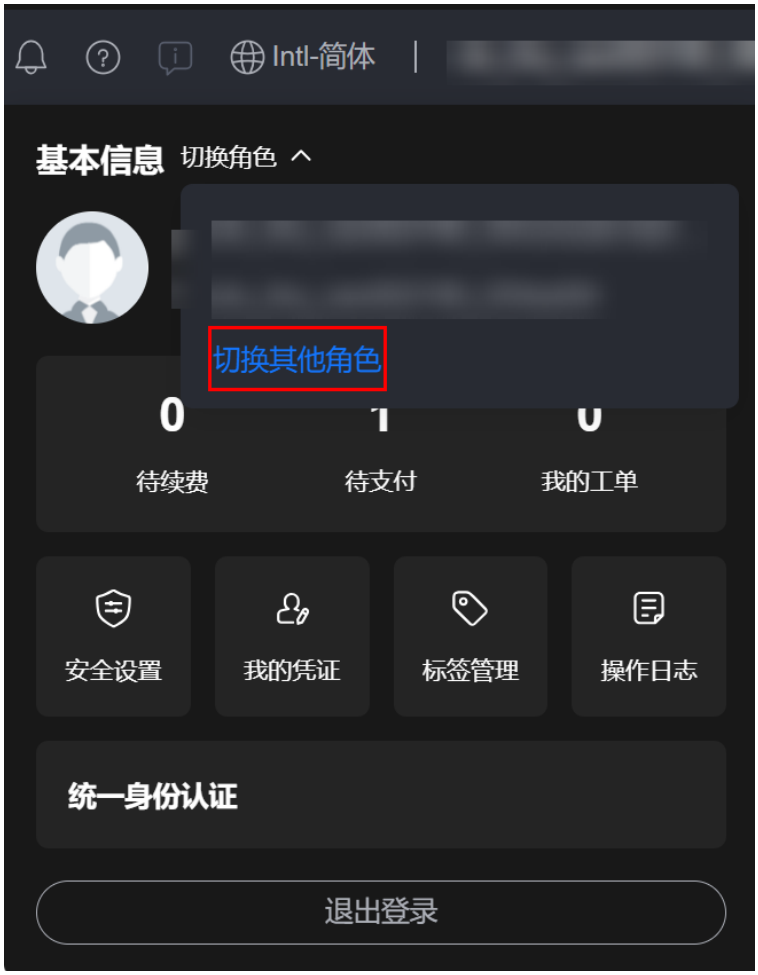
1. B账号在统一身份认证服务左侧导航窗格中，单击“用户”。
2. 在“用户”界面，单击“创建用户”。
3. 在“创建用户”界面，输入“用户名”和“描述”。
4. 打开“管理控制台访问”，选择“创建IAM用户”。
5. “密码设置 选择“自定义创建”，输入自定义密码，并勾选“首次登录时设置”，单击“下一步”。
6. 在“权限配置”页面，选择**步骤1**中创建的用户组“委托管理”，单击“创建用户”。

**步骤5** 切换角色。

1. 使用**步骤4**创建的IAM用户，通过“IAM用户登录”方式，登录华为云。登录方法，请参见：**IAM用户登录**。
2. IAM用户在控制台页面，光标移动到右上方用户名右侧的下拉框“切换角色”。选择角色切换记录或单击“切换其他角色”切换指定的信任委托。

**图 4-6** IAM 用户切换角色




3. IAM用户在“切换角色”页面中，输入委托方的账号名称和委托名称。
4. 单击“确定”，切换至委托方账号中。B账号中的IAM用户便可以A账号中的资源进行操作管理。

**----结束**

# 5 使用标签控制对 IAM 用户的资源访问权限

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。标签即是一种属性，您可以将标签绑定到IAM资源（IAM主体中的IAM用户与信任委托作为客体被其他主体访问时也是一种IAM资源）或者其他的华为云资源上。您可以定义以标签作为条件键的身份策略，这样在对华为云资源访问时可以通过对身份策略进行较少的改动来实现业务的增长。ABAC策略比传统的RBAC策略更加灵活，因为后者需要您列出每个单独的资源。有关ABAC的更多信息及其相对于传统RBAC策略的优势，请参阅**基于属性的ABAC权限管理**。

本教程将向您说明如何创建一个具有主体标签（Principal Tag）的IAM用户，并创建一个身份策略绑定给该IAM用户，这条身份策略的作用是限制该IAM用户只能访问具有与该主体标签相匹配的资源标签（Resource Tag）的资源。

## 操作说明

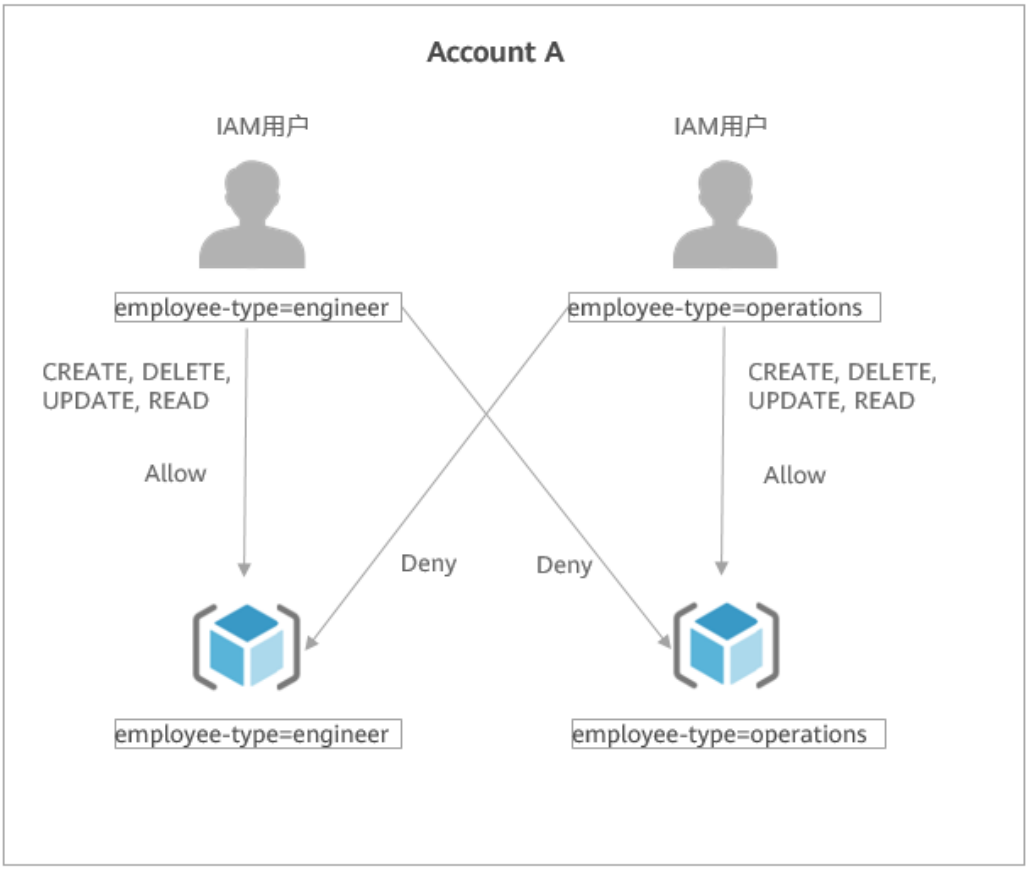
您是一名经验丰富的IAM管理员，您对IAM用户、信任委托和身份策略的创建、管理都非常熟悉。您希望确保您公司工程师团队和运维团队成员能够只访问其所需要的资源，并且后续会有更多类型的成员加入，您需要一个随着公司发展而扩展的身份策略。您选择使用主体标签和资源标签来编写该身份策略。支持资源标签的云服务列表见**支持身份策略与信任委托的云服务列表**中的“ABAC(基于标签的鉴权)”列。

您可以为您的工程师团队成员和运维团队成员分别绑定以下标签：

- employee-type=engineer（工程师团队成员）
- employee-type=operations（运维团队成员）

在本章节中，您将标记每个IAM用户、每个信任委托，并编写身份策略，将身份策略绑定到IAM用户上以达到前面所述的目的。编写的身份策略允许IAM用户对其可访问的资源进行创建、删除、更新、读取操作。




## 步骤一：给 IAM 用户添加标签

**步骤1** 管理员进入**统一身份认证服务新版控制台**，在左侧导航栏选择“用户”页签。

**步骤2** 单击工程师团队IAM用户employee-user的名称，进入用户详情页，选择“标签”页签。

**步骤3** 单击左上角的“添加标签”。

**步骤4** 在弹窗中设置标签的键为employee-type和值为engineer。


**----结束**

## 步骤二：为资源添加标签

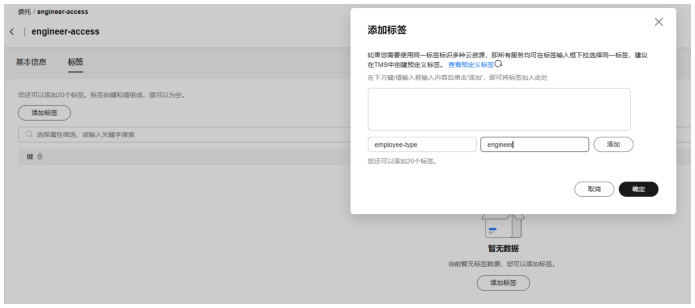
以信任委托为例（当以信任委托会话发起访问时，信任委托是IAM主体，此时它的标签是主体标签；当以IAM主体访问信任委托时，信任委托是IAM资源，此时它的标签是资源标签。）

**步骤1** 管理员进入**统一身份认证服务新版控制台**，在左侧导航栏选择“委托”页签。

**步骤2** 单击工程师团队IAM用户employee-user可访问的信任委托的名称，进入信任委托engineer-access详情页，选择“标签”页签。

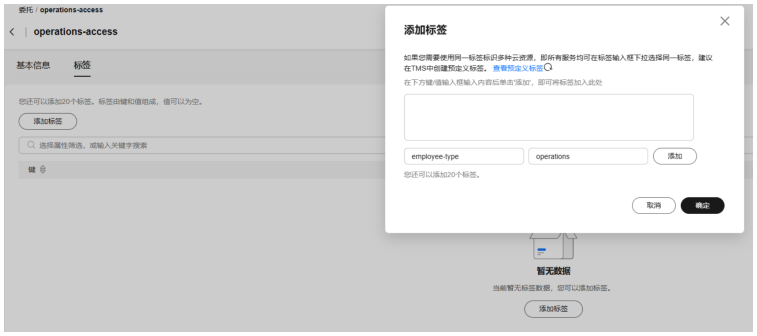
**步骤3** 单击左上角的“添加标签”。

**步骤4** 在弹窗中设置标签的键为employee-type和值为engineer。 单击“确定”。




**步骤5** 返回信任委托列表，单击运维团队operations可访问的信任委托的名称，进入信任委托operations-access详情页，选择“标签”页签。

**步骤6** 在弹窗中设置标签的键为employee-type和值为operations。 单击“确定”。




**----结束**

## 步骤三：创建自定义身份策略

**步骤1** 管理员进入**统一身份认证服务新版控制台**，在左侧导航栏选择“身份策略”页签。

**步骤2** 单击右上角“创建自定义身份策略”。

**步骤3** 输入身份策略名称为“engineer-access-policy”。

**步骤4** 策略配置方式选择“JSON视图”。配置以下身份策略，表示当主体标签和所访问的资源标签相等时允许访问。

```
{
  "Version": "5.0",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
```

```
            "iam:agencies:getV5"
        ],
        "Condition": {
            "StringEquals": {
                "g:ResourceTag/employee-type": [
                    "${g:PrincipalTag/employee-type}"
                ]
            }
        }
    }]
}
```

**步骤5** 单击“确定”。完成身份策略创建。

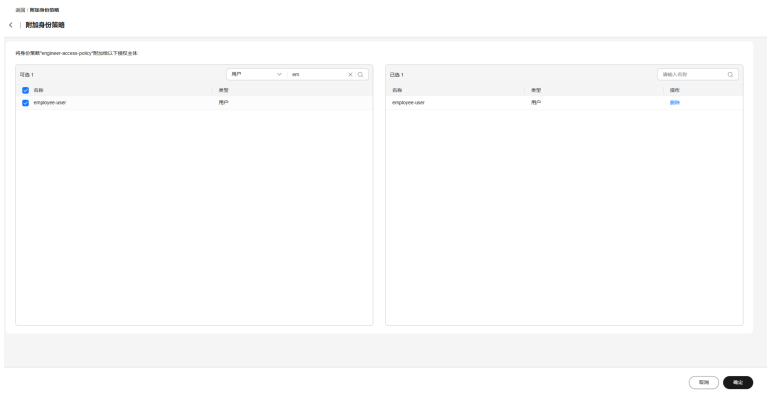
**----结束**

## 步骤四：将身份策略附加至授权主体

**步骤1** 管理员进入**统一身份认证服务新版控制台**，在左侧导航栏选择“身份策略”页签。

**步骤2** 勾选**步骤三**中创建的身份策略，单击身份策略列表上方的“附加”。

**步骤3** 勾选**步骤一**添加标签的工程师团队IAM用户employee-user，单击“确定”。



**----结束**

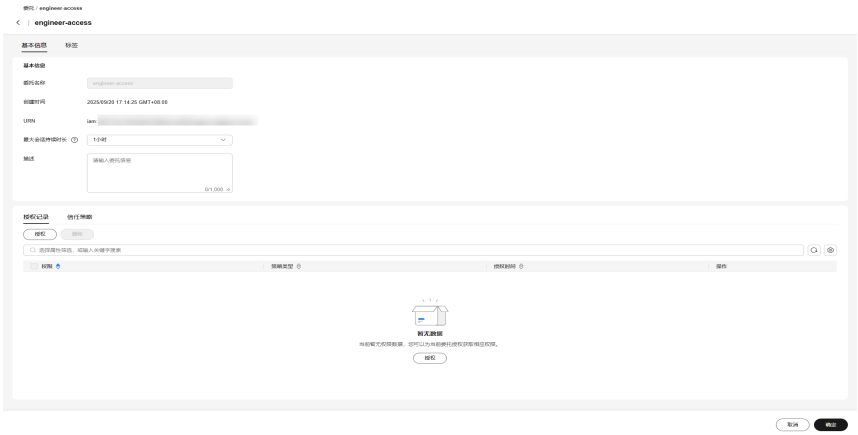
## 步骤五：验证结果

**步骤1** 除了为工程师团队IAM用户employee-user附加**步骤三**中创建的身份策略，还需要为其附加一个能够列举所有委托的身份策略（用于IAM控制台查看委托和信任委托的列表，如果仅进行API访问则不需要附加该身份策略）。

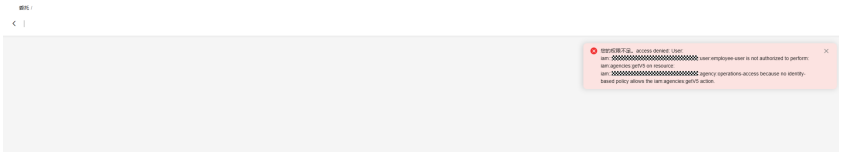
**步骤2** 工程师团队IAM用户employee-user分别查看信任委托engineer-access和信任委托operations-access。

- 查看信任委托engineer-access时，可以查看到信任委托详情。这是由于employee-user的主体标签与engineer-access的资源标签相同，符合身份策略的内容。




- 查看信任委托operations-access时，提示权限不足。这是由于employee-user的主体标签与operations-access的资源标签不同。



**----结束**

## 后续操作

如果该公司后续新增成员，则不需要修改已经编写好的身份策略，只需要给新增的成员和这些成员可访问的资源添加相应的标签即可。