云运维中心

常见问题

文档版本	01
发布日期	2025-09-11

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 产品咨询

1.1 云运维中心权限如何配置?

问题描述

如何快速配置云运维中心权限。

解决方法

1. 管理员登录**IAM控制台**。
2. 管理员在用户列表中，单击新建的用户，右侧的“授权”。

图 1-1 IAM 用户授权

3. 授权模型选择“**角色授权**”。

图 1-2 选择授权模型

4. 授权方式选择“直接给用户授权（适用于企业项目授权）”，根据需要分配“COC FullAccess”或“COC ReadOnlyAccess”策略，策略详情可查看**COC权限管理**。

图 1-3 分配 COC 策略

说明

如已有包含云运维中心策略的群组，可选择"继承所选用户组的策略"方式授权，可参考**IAM用户授权**。

5. 选择授权范围方案，指定企业项目资源。
6. 完成授权。

图 1-4 完成授权

1.2 如何通过企业项目进行权限控制

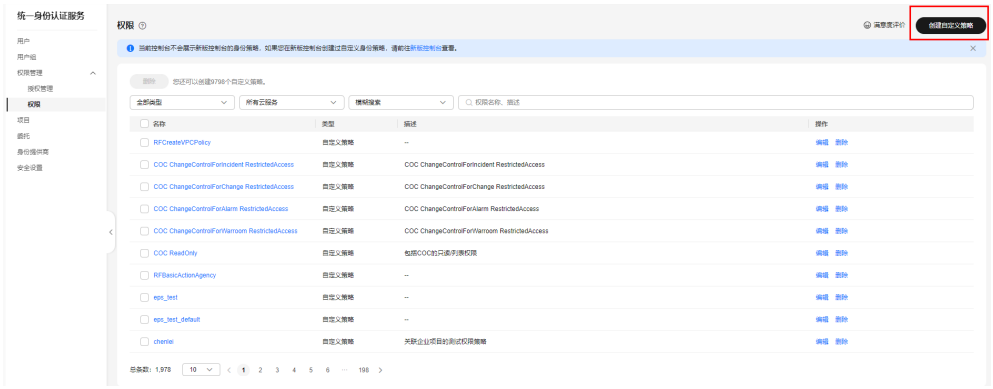
问题描述

如何通过企业项目进行云运维中心的权限控制。

解决方法

1. 管理员登录**IAM控制台**。
2. 管理员在权限管理-权限中，单击“创建自定义策略”。

图 1-5 创建自定义策略



3. 设置策略内容，选择允许“云服务操作中心”，并选择要进行企业项目鉴权的操作。单击“确定”完成创建。

图 1-6 设置策略内容-1

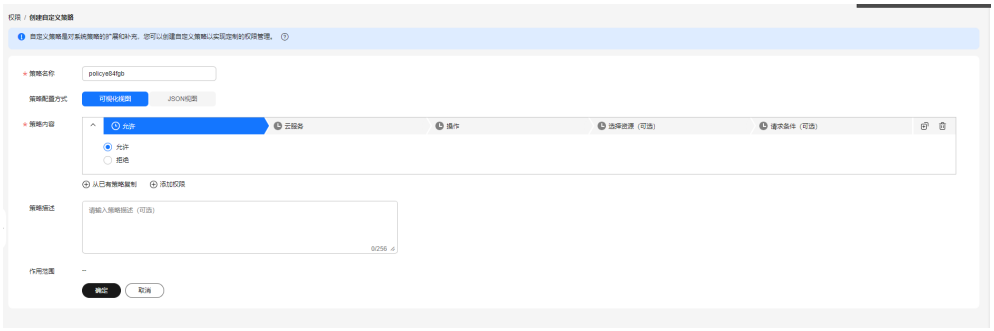


图 1-7 设置策略内容-2

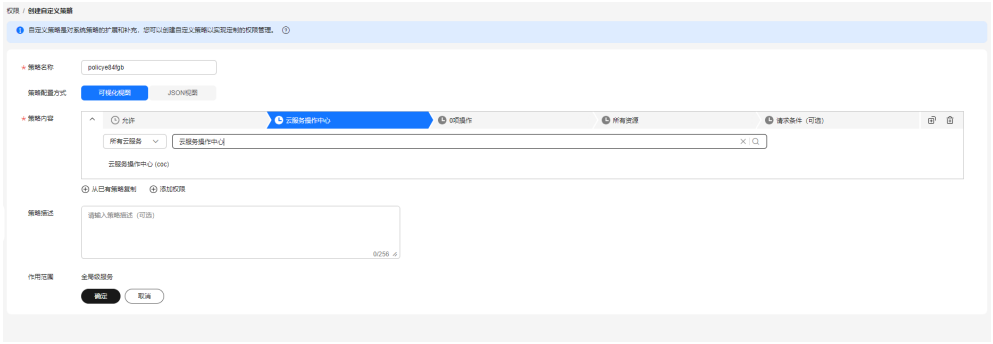
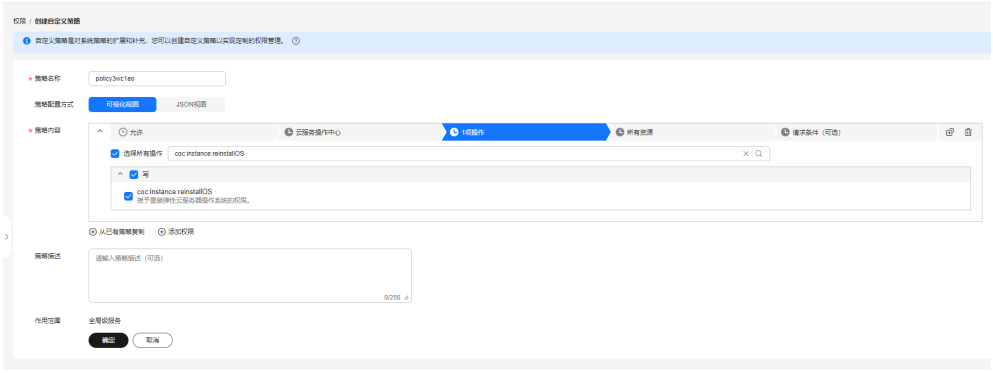


图 1-8 设置策略内容-3



说明

云运维中心当前仅有部分操作支持按照企业项目授权，可以参考**表1**创建自定义策略。

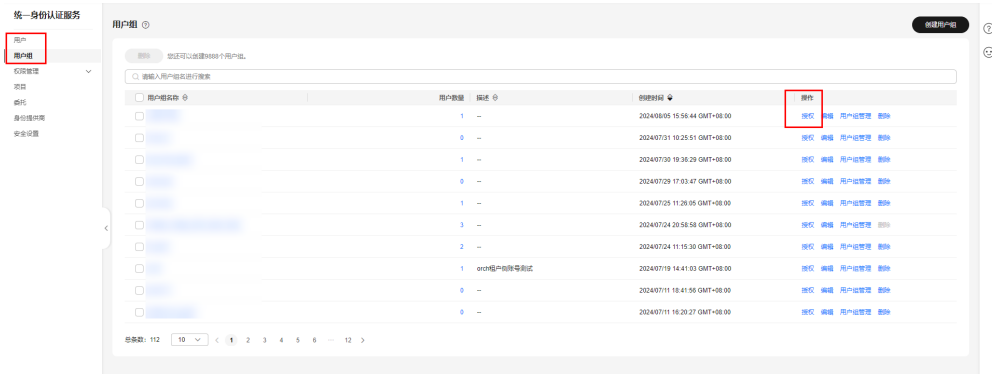
表 1-1 支持企业项目鉴权的操作

操作	描述
coc:instance:reinstallOS	授予重装弹性云服务器操作系统的权限。

操作	描述
coc:instance:changeOS	授予切换弹性云服务器操作系统的权限。
coc:instance:start	授予启动云服务器的权限。
coc:instance:reboot	授予重启云服务器的权限。
coc:instance:stop	授予关闭云服务器的权限。
coc:instance:startRDSInstance	授予启用RDS实例的权限。
coc:instance:stopRDSInstance	授予停止RDS实例的权限。
coc:instance:restartRDSInstance	授予重启RDS实例的权限。
coc:instance:scanOSCompliance	授予服务器操作系统补丁扫描的权限。
coc:instance:installPatches	授予为弹性云服务器安装补丁的权限。
coc:instance:executeDocument	授予在弹性云服务器上执行文档的权限。
coc:schedule:create	授予创建定时任务列表的权限。
coc:schedule:update	授予更新定时任务的权限。

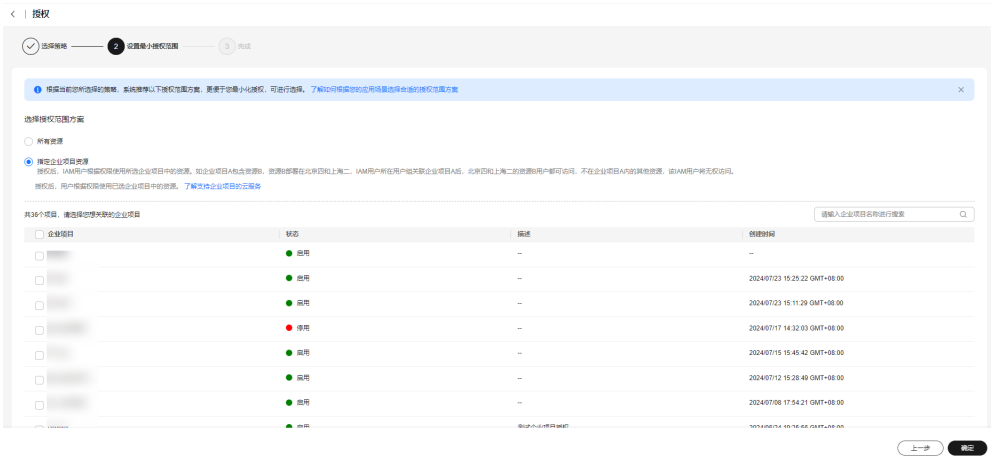
4. 管理员选择用户或用户组，进行授权。

图 1-9 选择对象进行授权



5. 选择步骤3中创建的自定义策略，在设置最小授权范围时，指定企业项目资源，完成企业项目授权。

图 1-10 按照企业项目授权



1.3 如何创建委托?

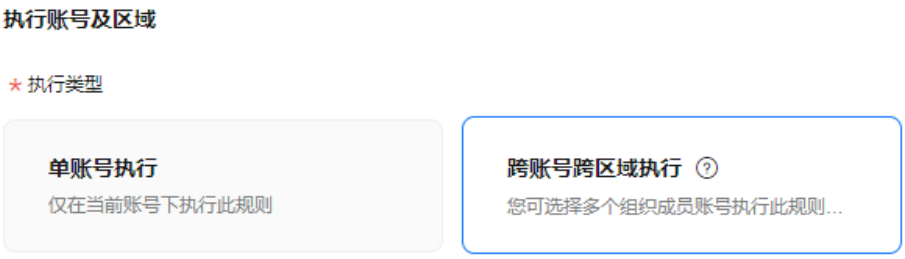
背景

若您的企业组织存在多个租户账号，您可以使用COC的跨账号能力在创建CES告警规则、执行作业等场景通过一个账号完成多账号多区域的运维任务配置和下发，在此过程中，您需要创建和使用相应的委托。

本章节将以跨账号创建CES告警规则场景为例，详述如何创建相关委托。

COC服务“总览 > 快速配置中心 > 云服务配置”板块使用跨账号配置功能，如下图示例。

图 1-11 配置跨账号功能



委托功能说明

跨账号功能的使用需要两个委托：组织管理员委托和执行账号委托。

- 组织管理员委托：组织管理员或组织内COC服务委托管理员（以下统称管理员）创建并信任COC服务的委托。委托用于支持COC服务切换到管理员身份，即允许COC服务以管理员身份执行必要的管理任务。
- 执行账号委托：执行账号（组织中的成员租户）信任COC服务和管理员的委托，必须是IAM 5.0版本的信任委托。委托用于支持管理员切换到执行账号身份进行作业工单创建以及跨账号实际目的操作。

  示例：

假设您正在使用华为云的COC服务进行跨账号操作，您需要创建一个执行账号委托，以便COC服务可以以管理员的身份执行以下操作：

- 在执行账号中创建一个新的SMN主题。
- 向该SMN主题添加订阅，以便接收告警通知。
- 在执行账号中创建CES告警规则，以便监控和触发告警。

同时，该委托还应允许管理员切换至执行账号身份，以便创建作业工单。这确保了管理员能够在执行账号中执行必要的管理任务，同时保持操作的灵活性和安全性。

执行账号委托信任策略内容：

```
{
 "Version": "5.0",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ces:alarms:create"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "smn:topic:create",
    "smn:topic:subscribe"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "sts:agencies:assume",
    "sts::setSourceIdentity",
    "sts::tagSession"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "coc:instance:executeDocument",
    "coc:job:action",
    "coc:job:get",
    "coc:job:list"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "iam:projects:list"
   ]
  }
 ]}
```

说明

- 委托需要支持的操作就代表了委托的授权。
- 当前创建CES告警规则中包含了告警通知功能，通知功能受限于周边服务对外开放能力，故当前仅开放了主题订阅一种通知方式。
- 在配置CES告警规则参数时，通知主题是依托于登录的管理员租户（组织管理员或组织COC服务委托管理员）拥有的通知主题进行选择的，服务不支持提前查询执行账号（目标跨账号租户）拥有的通知主题，故在执行快速配置工单时，服务会为执行账号创建与配置CES告警规则参数时选择的管理员租户的通知主题具有相同订阅方式（订阅方式中welink、飞书、钉钉因为订阅方式特殊，不会自动添加到新创建的主题订阅中）相同名称的主题。通知根据通知数量等情形可能存在收费，因此请使用跨账号创建CES告警规则的用户注意，如不需要发送通知功能，可在配置CES告警规则时关闭发送通知功能。

注意事项

组织管理员委托和执行账号委托的创建，均基于跨账号操作的两个租户（委托租户和被委托租户）属于同一组织的前提条件。

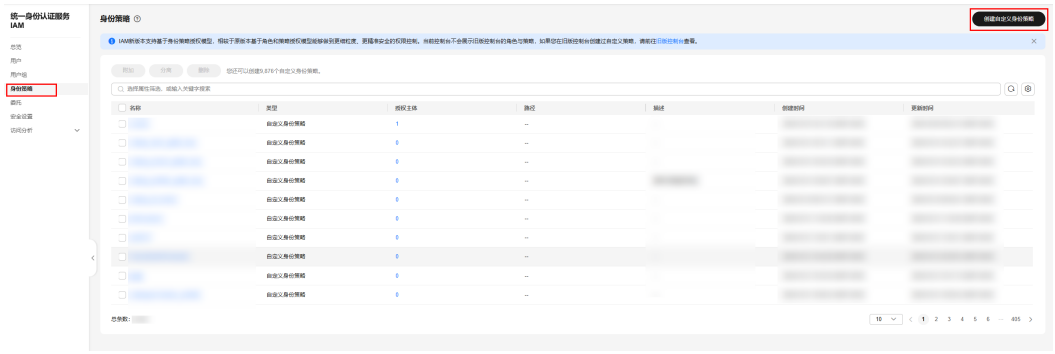
组织管理员委托

步骤1 使用组织管理员租户账号登录**IAM控制台**。

步骤2 单击“体验新版控制台”，进入新版控制台。

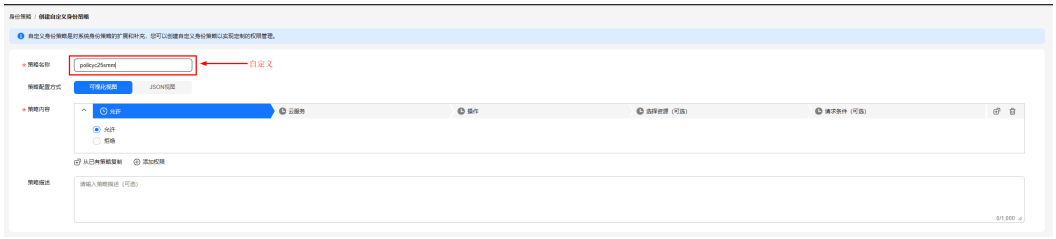
步骤3 在左侧菜单栏单击“身份策略”，进入“身份策略”列表页，单击右上角“创建自定义身份策略”，为委托创建授权策略。

图 1-12 创建授权策略



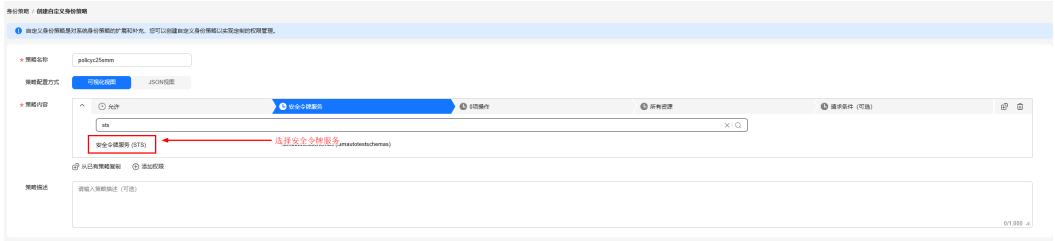
步骤4 进入身份策略创建页面，填写“策略名称”。

图 1-13 自定义身份策略名称



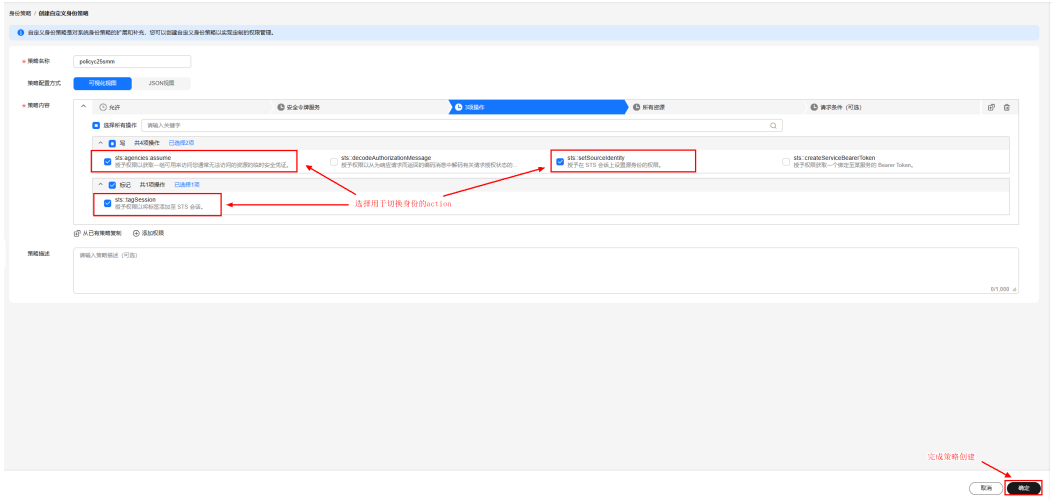
步骤5 在“策略内容”中单击“云服务”，搜索“安全令牌服务”，选中后跳转至操作选择区。

图 1-14 选择云服务



步骤6 在操作选择区分别搜索“sts:agencies:assume”、“sts::tagSession”、“sts::setSourceIdentity”三个action，勾选后，单击页面右下角“确定”，用于切换身份的策略即创建成功。

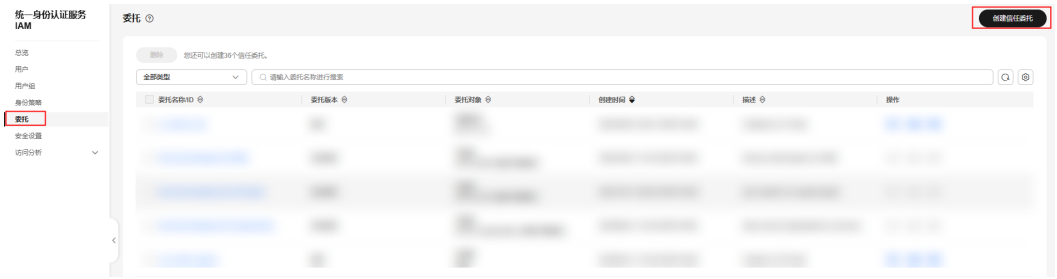
图 1-15 完成切换身份的身份策略创建



步骤7 在左侧菜单栏单击“委托”，进入“委托”列表页。

步骤8 单击右上角“创建信任委托”，进入创建信任委托页面。

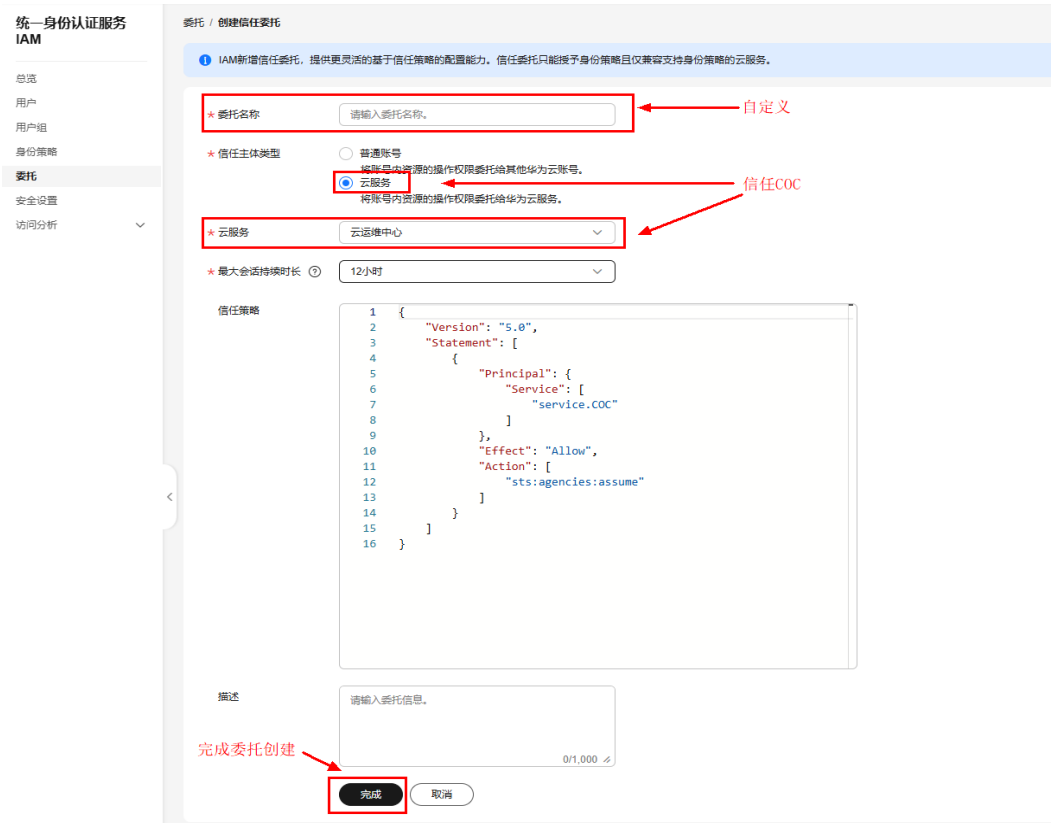
图 1-16 创建信任委托



步骤9 自定义“委托名称”，信任主体类型选择“云服务”，云服务选择“云运维中心”，最大会话持续时长推荐选择“12小时”。

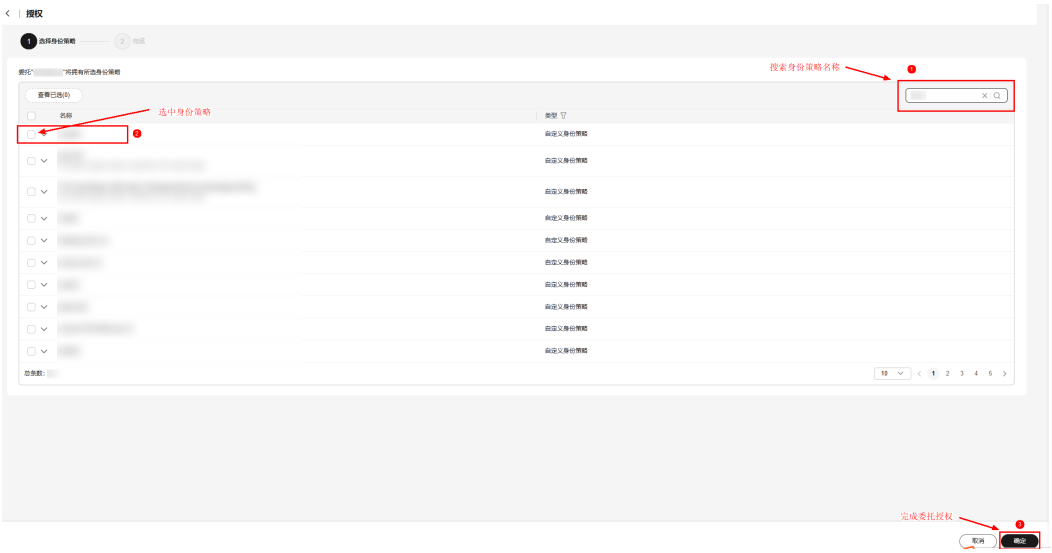
步骤10 单击页面最下方的“完成”，即完成委托创建，之后单击弹窗中的“立即授权”，进入委托授权页面。

图 1-17 完成信任委托创建



步骤11 在授权列表右上角搜索**步骤4**中创建的策略名称，选中，单击“确定”，即完成授权。

图 1-18 委托授权



----结束

执行账号委托

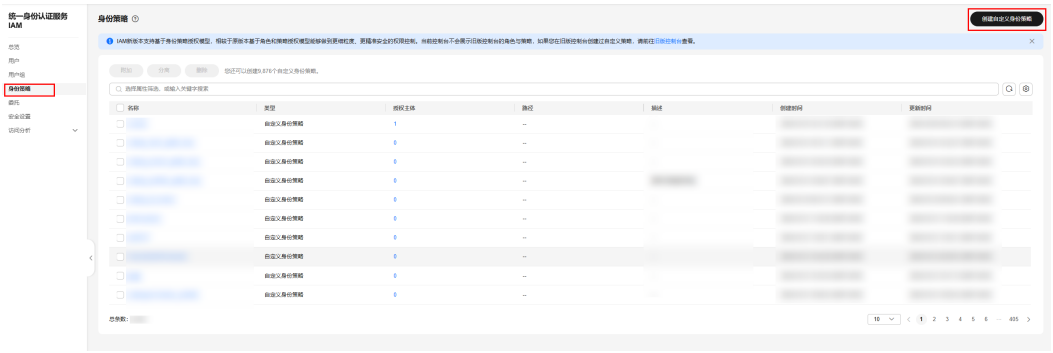
步骤1 以组织成员租户（执行账号）身份登录**IAM控制台**。

步骤2 单击“体验新版控制台”，进入新版控制台。

步骤3 在左侧菜单栏单击“身份策略”，进入“身份策略”列表页。

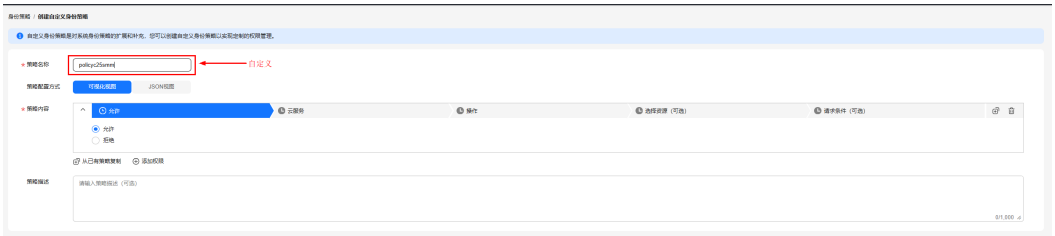
步骤4 单击右上角“创建自定义身份策略”，为委托创建授权策略、

图 1-19 创建授权策略



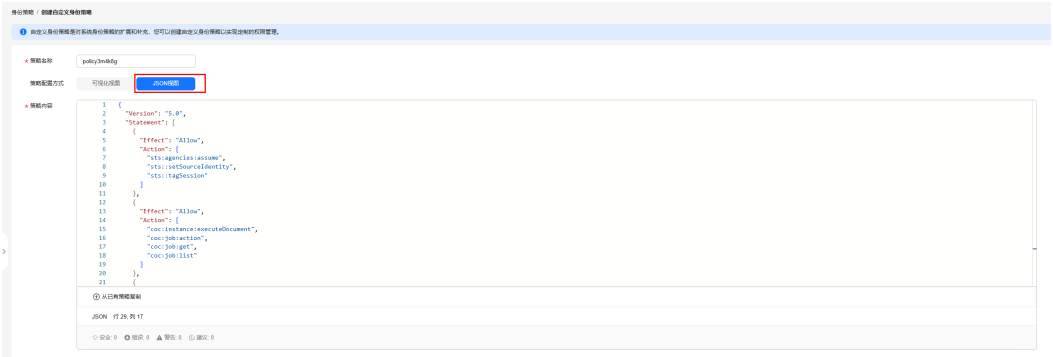
步骤5 进入身份策略创建页面，填写“策略名称”。

图 1-20 自定义身份策略名称



步骤6 “策略配置方式”选择“JSON视图”，在输入框中填写以下策略内容。

图 1-21 自定义策略内容



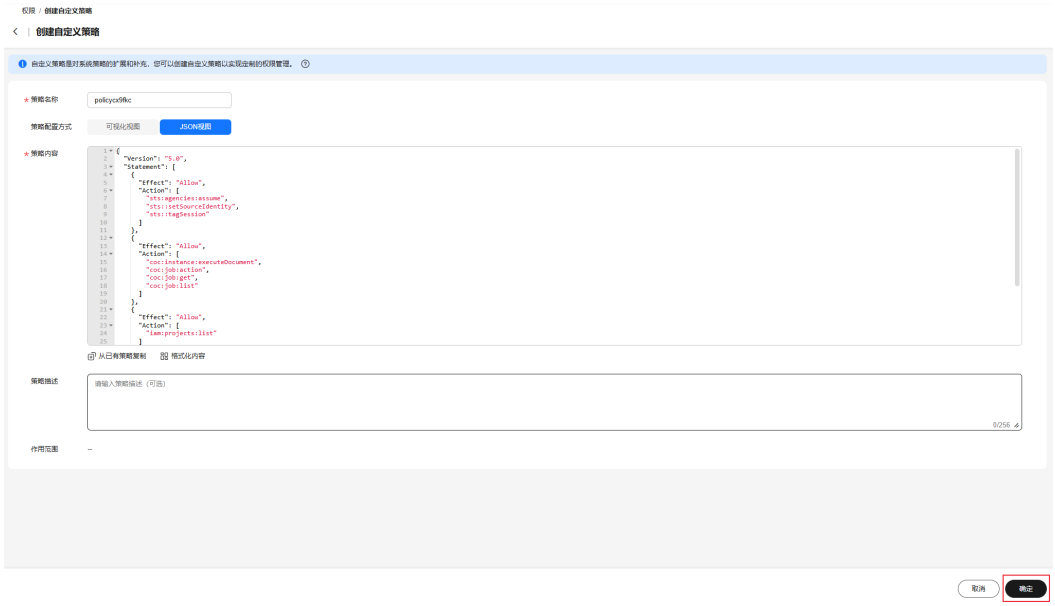
```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sts:agencies:assume",
        "sts::setSourceIdentity",
        "sts::tagSession"
      ]
```



```
  },
  {
    "Effect": "Allow",
    "Action": [
      "coc:instance:executeDocument",
      "coc:job:action",
      "coc:job:get",
      "coc:job:list"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:projects:list"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "smn:topic:create",
      "smn:topic:subscribe"
    ]
  }
 ]
}
```

步骤7 单击页面右下角“确定”，完成执行租户委托的身份策略创建。

图 1-22 执行租户委托身份策略创建



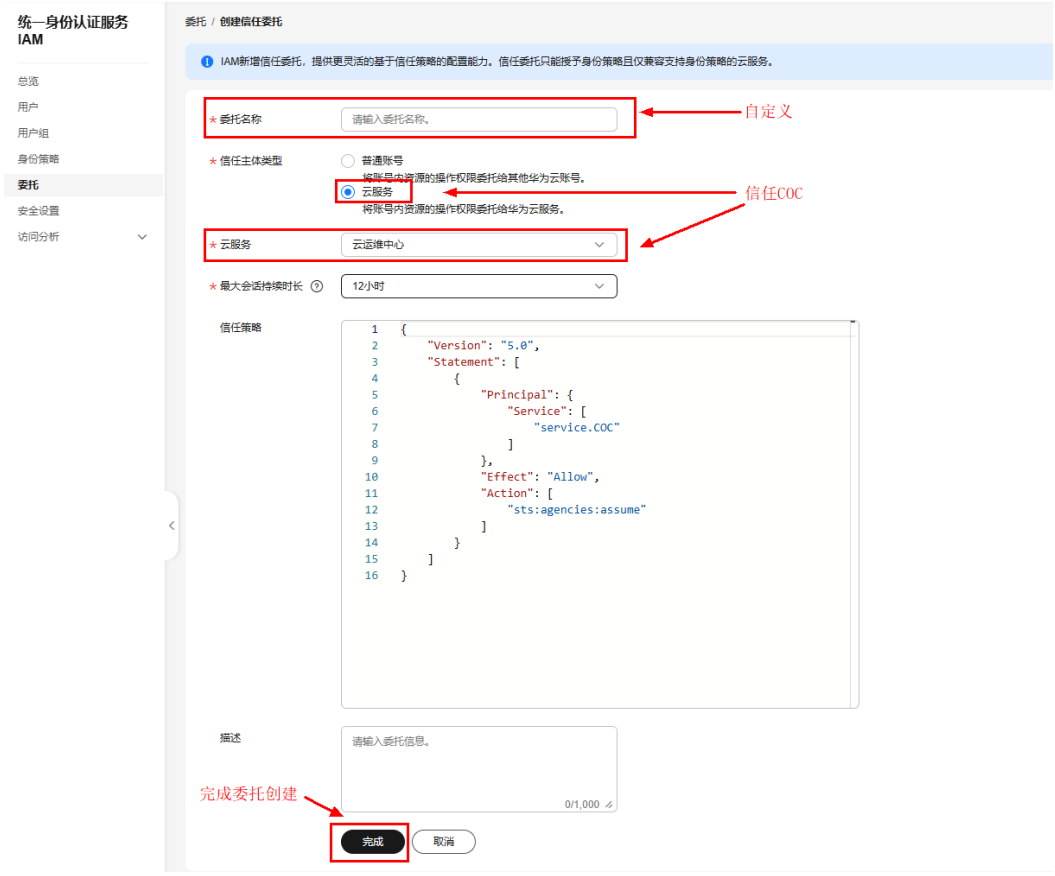
步骤8 在IAM新版控制台页面左侧菜单栏单击“委托”，进入“委托”列表

步骤9 单击页面右上角“创建信任委托”，创建执行账号委托组织管理员权限的委托身份。

- 自定义“委托名称”。
- 信任主体类型选择“云服务”。
- 云服务选择“云运维中心”。
- 最大会话持续时长推荐选择“12小时”。

步骤10 单击页面最下方的“完成”，即完成委托创建。

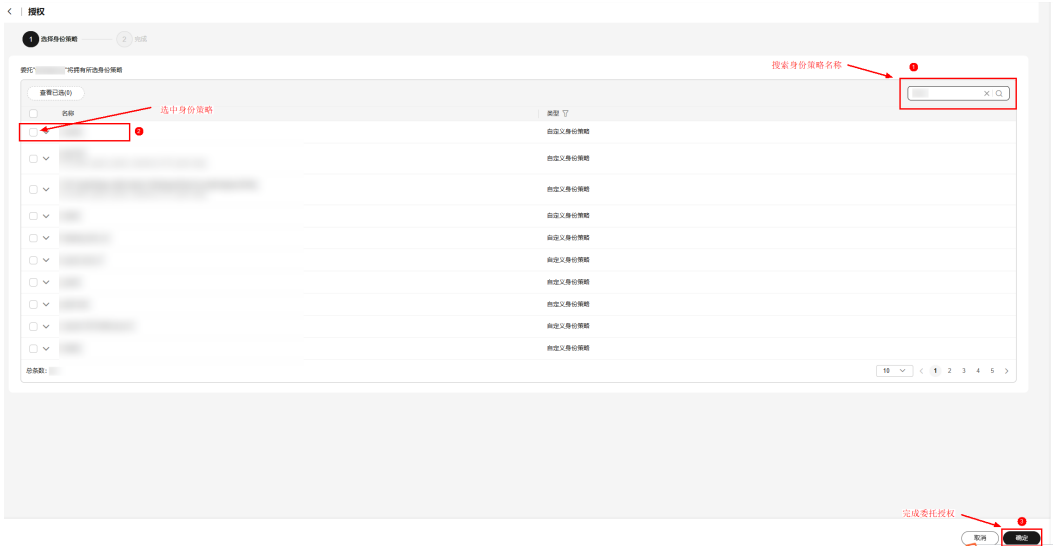
图 1-23 创建委托



步骤11 单击弹窗中的“立即授权”，进入委托授权页面。

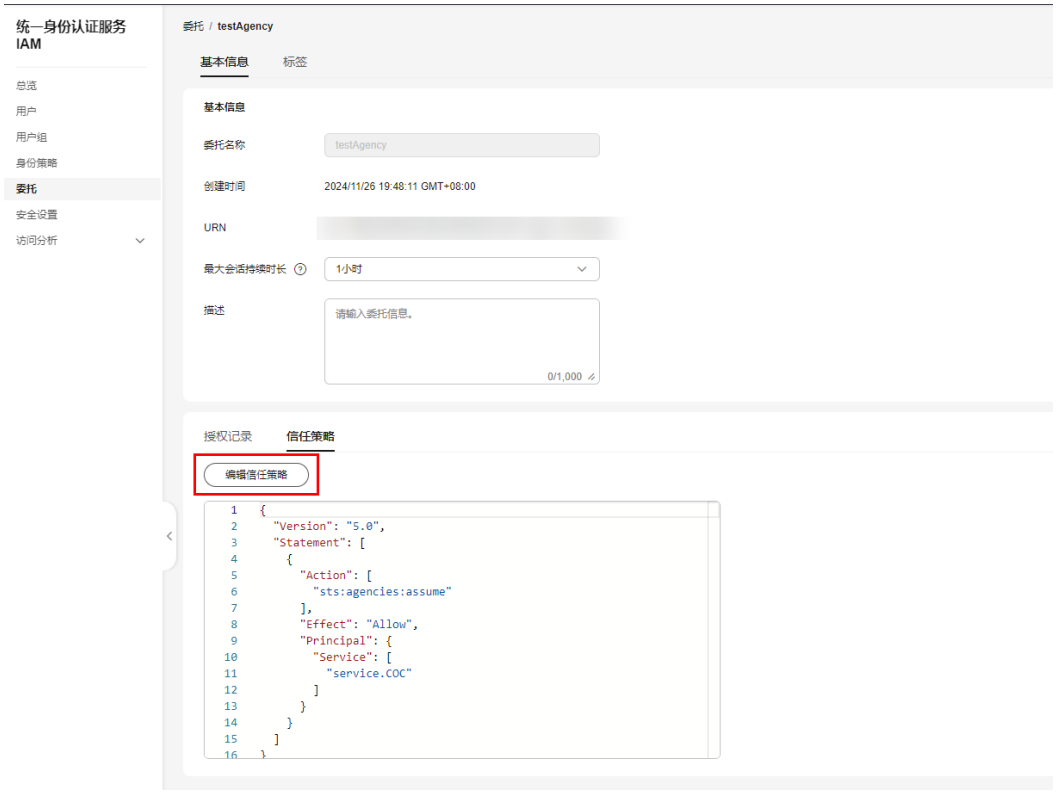
步骤12 在授权列表右上角搜索**步骤5**中创建的策略名称，选中，单击“确定”，即完成授权。

图 1-24 委托授权



步骤13 之后在“委托”列表页找到**步骤9**-**步骤12**创建的委托，单击该委托一栏右侧“操作”列中的“编辑”按钮，进入委托编辑页面；

图 1-25 编辑执行租户委托的信任策略 1

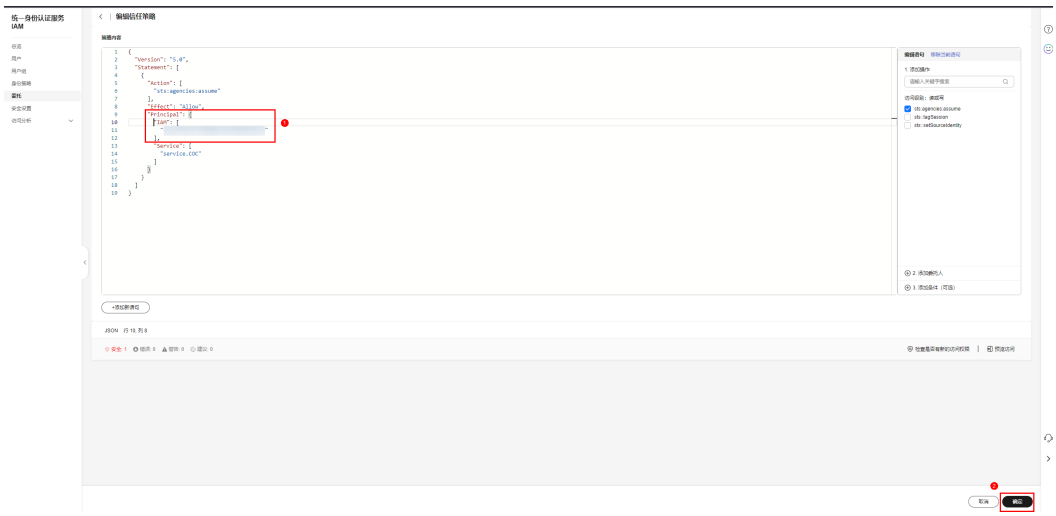


步骤14 在“信任委托”tab页单击“编辑信任策略”，在Pricipal中添加以下json数据：

```
"IAM": [
        "${目标组织管理员租户的租户ID}"
    ],
```

步骤15 单击右下角的“确定”按钮，信任策略编辑完成，继续单击页面右下角的“确定”按钮，执行账户信任COC同时信任组织管理员的委托即创建完成。

图 1-26 编辑执行租户委托的信任策略 2



----结束

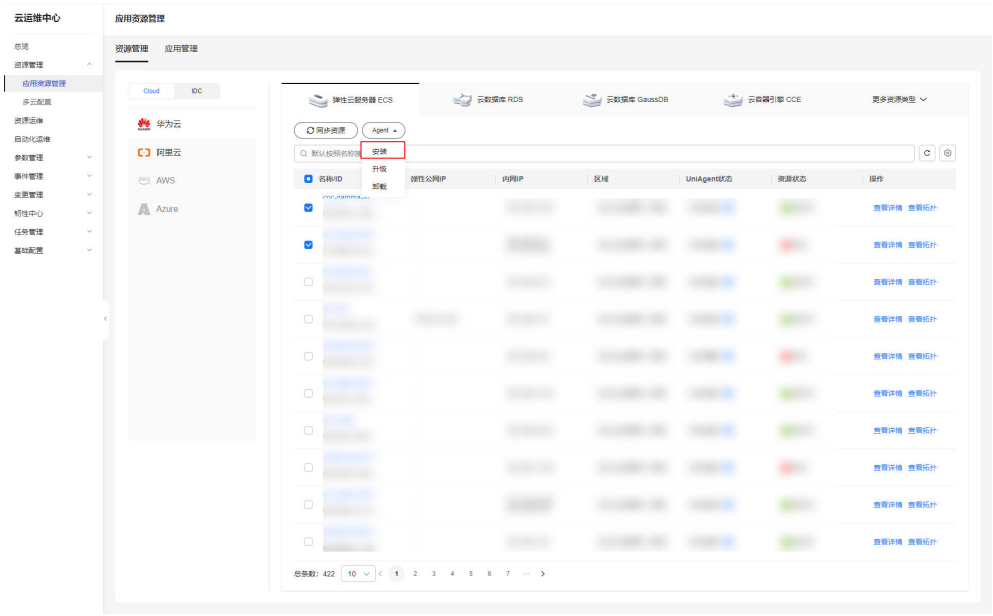
2 资源管理常见问题

2.1 首次安装 UniAgent 如何操作?

步骤1 登录**云运维中心**。

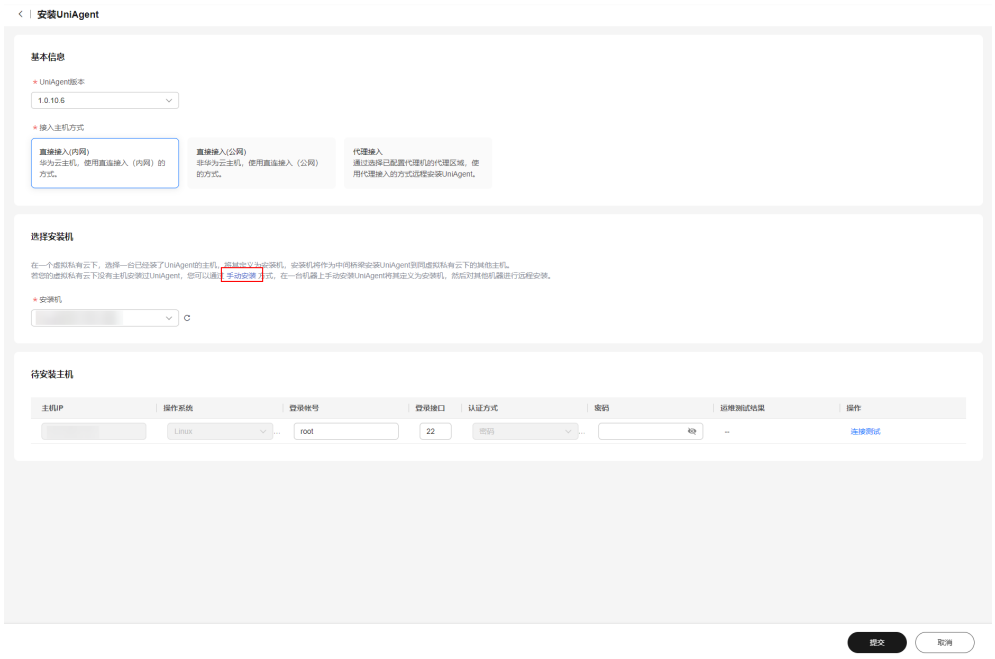
步骤2 在左侧菜单栏单击“**应用资源管理**”，进入“资源管理”页面，选中首台未安装过UniAgent的机器。

图 2-1 安装 UniAgent



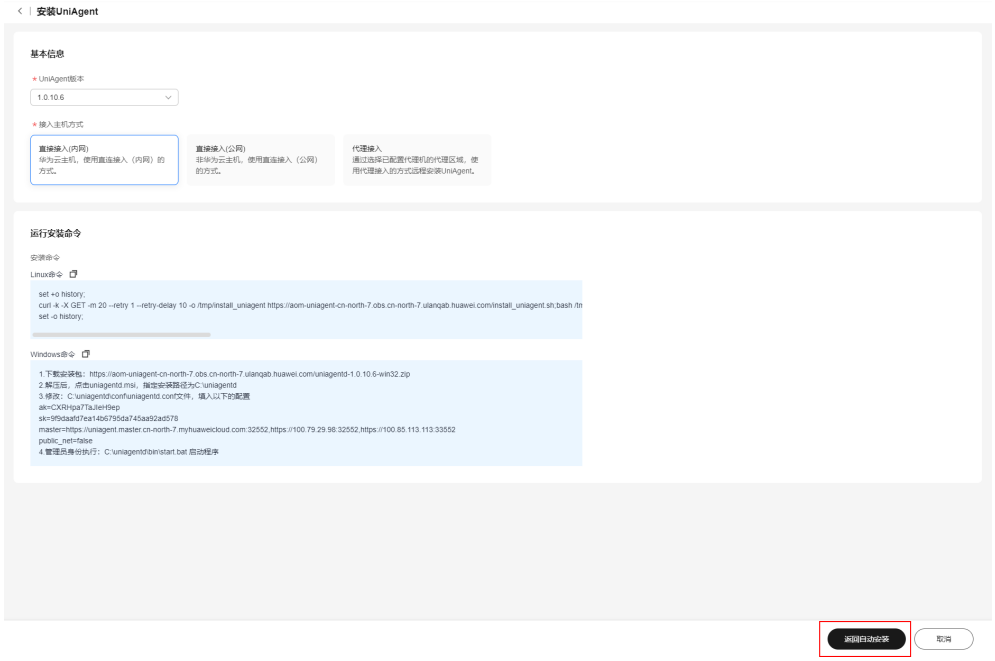
步骤3 在跳转的安装UniAgent页面中，单击 “**手动安装**”。

图 2-2 安装 UniAgent 页面



步骤4 根据页面的运行安装命令进行手动安装UniAgent。

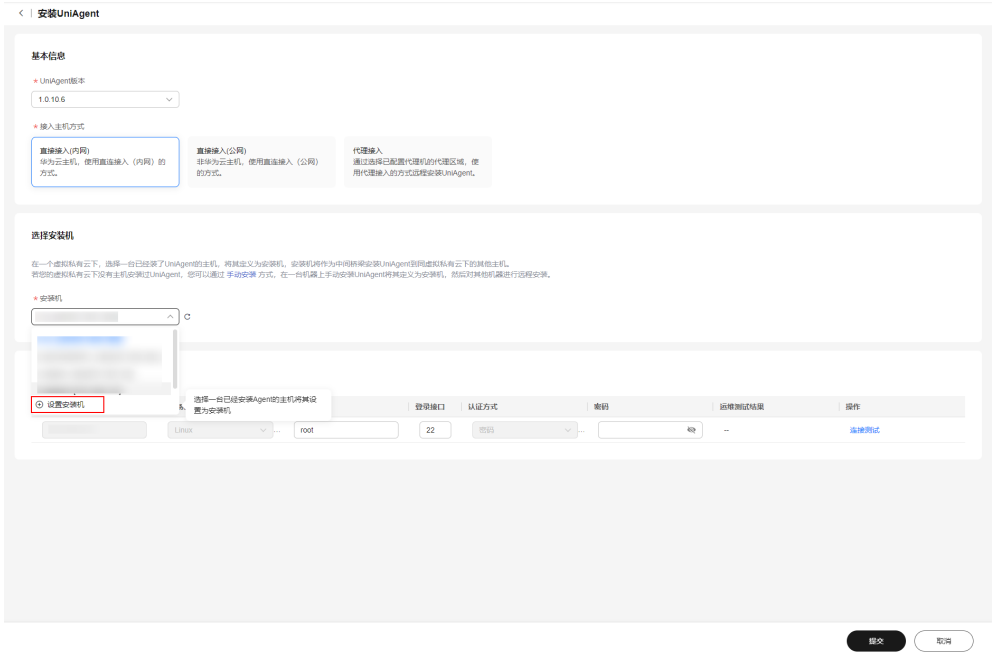
图 2-3 “手动安装 UniAgent”页面



步骤5 UniAgent安装完成后，单击 “**返回自动安装**”。

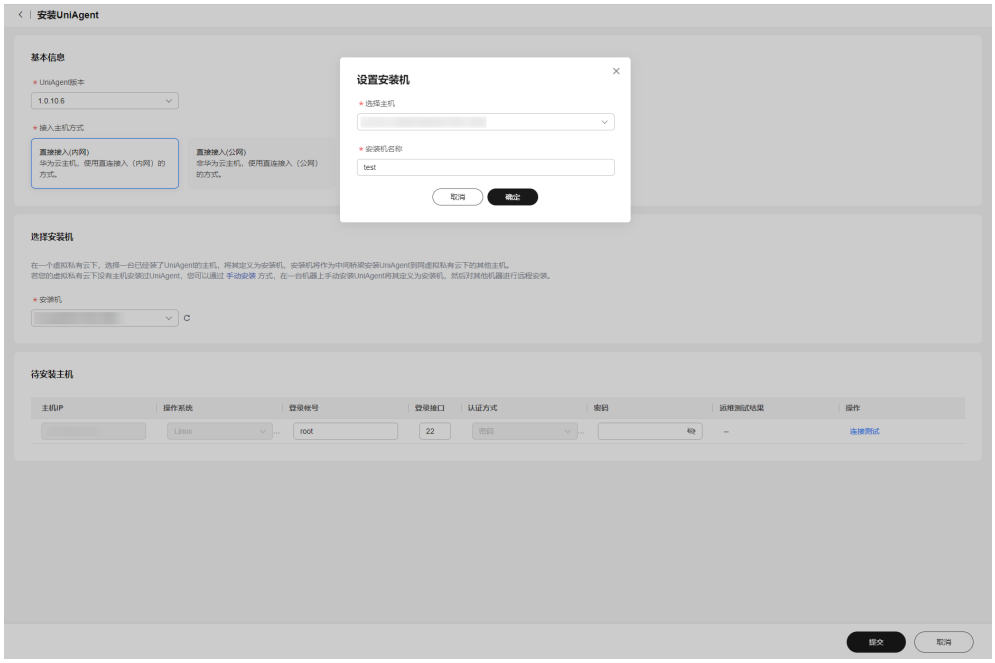
步骤6 单击“**设置安装机**”，设置刚才完成UniAgent安装的机器为安装机。

图 2-4 设置安装机



步骤7 在弹框中填写设置安装机相关信息，单击“**确认**”。

图 2-5 确定安装机



----结束

2.2 如果资源无法在资源管理页面中查询到，如何处理?

问题描述

在资源管理页面中查询不到对应的资源。

问题定位

资源未同步到COC平台，不能在资源管理页面对资源进行管理。

解决方案

在资源管理页面中进行同步资源。具体操作详见**同步资源**。

2.3 无法找到应用管理层级说明页面?

问题描述

在应用管理页面，没有找到应用管理层级说明。

问题定位

指导说明已隐藏。

解决方案

在“应用管理”页面，单击右上角的“操作指引”，取消隐藏即可展示操作指引。

图 2-6 隐藏指引

图 2-7 取消隐藏

3 补丁管理常见问题

3.1 补丁基线不生效?

问题描述

补丁基线创建后不生效。

问题定位

补丁基线未设置为默认基线。

解决方案

在使用补丁管理扫描或修复功能前，请确认创建的补丁基线已经设置为默认基线并且使用场景正确。

3.2 补丁基线中安装规则基线与自定义基线的区别?

在企业补丁管理体系中，安装规则基线与自定义基线是补丁基线的两种核心类型，二者围绕 “补丁筛选逻辑” 和 “修复目标版本” 形成明确差异，分别适配不同的补丁管理需求，具体区别如下：

核心定位与设计目标

- 安装规则基线：定位为“标准化、自动化的通用补丁管理方案”，设计目标是帮助用户快速筛选符合通用安全或功能需求的补丁，无需关注具体补丁名称与版本细节，适用于追求高效、统一补丁升级的场景。
- 自定义基线：定位为“精细化、场景化的专属补丁管理方案”，设计目标是满足用户对特定补丁版本的精准管控需求，允许用户自主定义补丁范围与目标版本，适用于需严格控制版本兼容性的场景。

补丁筛选能力差异

- 安装规则基线：聚焦 “基于补丁基本信息的批量筛选”，用户无需手动指定具体补丁，而是通过预设规则圈定补丁范围。支持的筛选维度包括补丁类型（如安全

补丁、功能补丁、bug修复补丁）、补丁等级（如高危、中危、低危）、发布时间（如近30天发布的补丁）、适用系统版本（如CentOS7、Ubuntu 20.04）等。例如，用户可设置 “筛选近15天发布的Linux系统高危安全补丁”，系统会自动匹配所有符合该规则的补丁，无需逐一勾选。

- 自定义基线：聚焦 “基于补丁名称与版本的精准筛选”，用户需手动定义具体的补丁标识与版本范围。操作时，用户可直接输入补丁包名称（如“kernel-devel”“openssl”），并指定对应的版本号（如“kernel-devel-3.10.0-1160.el7.x86_64”、“openssl-1.0.2k-25.el7_9.x86_64”），系统仅会将用户明确指定的补丁纳入基线范围。例如，用户可针对“openssl”补丁，仅选择“1.0.2k-25.el7_9”版本，排除其他更高或更低版本的补丁。

补丁修复逻辑差异

- 安装规则基线：遵循 “最新版本优先” 的修复逻辑，旨在将系统补丁更新至当前可用的最新合规版本。当检测到主机存在不合规补丁（即未安装符合筛选规则的补丁，或已安装补丁版本低于最新版本）时，系统会自动从补丁库中获取对应补丁的最新版本，将不合规补丁直接升级至该最新版本。例如，若筛选规则为 “高危安全补丁”，且某主机 “openssl” 当前版本为“1.0.2k-20.el7”，而最新高危修复版本为“1.0.2k-25.el7_9”，系统会自动将其升级至“1.0.2k-25.el7_9”。
- 自定义基线：遵循 “指定版本优先” 的修复逻辑，严格按照用户定义的版本完成补丁升级。当检测到主机补丁不合规（即未安装用户指定版本的补丁，或已安装版本与指定版本不一致）时，系统不会自动选择最新版本，而是精准匹配用户在基线中设定的目标版本，将不合规补丁升级或降级至该指定版本。例如，用户在自定义基线中指定“openssl”版本为“1.0.2k-20.el7”，即使补丁库中存在更新的 “1.0.2k-25.el7_9” 版本，系统也仅会将主机“openssl” 补丁修复至“1.0.2k-20.el7”，确保版本与用户需求完全一致。

3.3 补丁工单日志中出现 all mirrors were tried 异常如何处理?

问题描述

补丁工单日志中出现all mirrors were tried异常。

问题定位

一般由网络原因引发。

解决方案

确认机器网络是否能和机器上所配置的补丁源联通，或机器网络是否出现异常。

3.4 机器无法选择?

问题描述

创建补丁扫描时，添加实例，无法选择对应资源。

问题定位

资源状态异常，或者未安装UniAgent。

解决方案

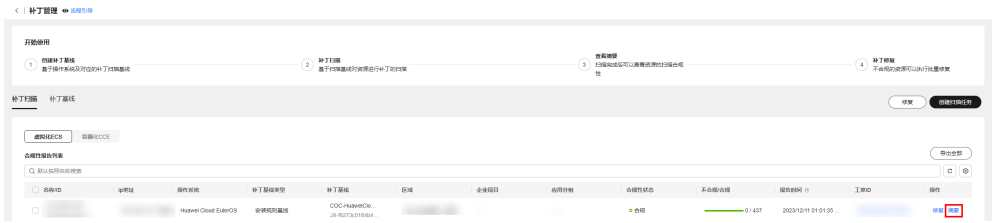
请确认机器状态是否正确，资源状态为运行中且UniAgent状态为运行中。

UniAgent安装可参考**安装UniAgent**。

3.5 补丁修复后合规性报告仍然为不合规如何处理?

步骤1 单击修复后生成的合规性报告摘要。

图 3-1 合规性报告摘要



步骤2 查看不合规的补丁状态，根据状态不同查看不同解决方案。

表 3-1 不同合规性状态的解决方案

不合规状态	解决方案
失败	查看生成此合规性报告的补丁工单日志，根据失败的日志解决此问题。
已安装待重启	补丁已安装修复，待机器重启后生效，机器重启后扫描即可解决不合规问题。
已拒绝	在补丁基线中拒绝了此补丁，合规性报告中显示为已拒绝，若需要取消拒绝，请到补丁基线中编辑相应基线。

----结束

3.6 补丁操作出现 lsb_release not found 异常如何处理?

问题描述

补丁操作出现lsb_release not found异常。

解决方案

请确认ECS实例上有是否有lsb_release命令包。

- 若没有，则安装相应命令包。
- 若ECS实例上有lsb_release命令包，则确认使用的UniAgent版本是否高于1.1.0版本，若高于1.1.0则降UniAgent版本为1.1.0以下重试。

4 自动化运维常见问题

4.1 审批人无法接收通知?

问题描述

审批人无法接收通知信息。

原因分析

审批人没有在人员管理配置任何消息通知渠道。

解决方案

消息渠道配置请参考：**如何使用人员管理**。

4.2 自定义脚本参数输入值无效?

问题描述

自定义脚本参数输入值提示无效。

解决方案

请排查输入的自定义脚本参数是否满足如下规则：

- 参数值长度为1-1024位。
- 可以包含大写字母、小写字母、数字以及特殊字符(_-/.*?:",=+@\[{]})和空格。
- 禁止出现连续‘.’。

4.3 实例无法选择?

问题描述

执行自动化运维时实例无法选择。

解决方案

实例需要安装UniAgent才能执行自动化运维。

安装UniAgent请参考：**安装UniAgent**。

4.4 如何在不重启实例的情况下重置密码?

在云资源（如ECS、BMS）管理中，若需重置主机账号密码且避免实例重启（防止业务中断），可通过COC提供的账号重置公共脚本实现，该方案无需重启实例即可完成密码更新，当前支持ECS与BMS两种资源类型，具体操作逻辑如下：

⚠ 注意

您在COC中执行公共脚本时，需要选择实例，而能够选择到实例的前提条件为：

您的资源实例信息已经同步到COC中，具体操作指导请见：**同步资源**；

您的资源实例已经安装UniAgent且UniAgent运行正常、状态为“运行中”；

在实例上安装UniAgent，需要您提供实例的管理员账号密码，若您的资源实例未安装UniAgent且您已忘记密码，则无法安装UniAgent、导致无法执行重置密码的公共脚本，请知悉！

以ECS Linux实例重置root账号密码为例：

步骤1 登录**云运维中心**。

步骤2 在左侧导航栏选择“资源运维 > 自动化运维”。

步骤3 在“日常运维”模块单击“脚本管理”。

步骤4 在“公共脚本”页签，在脚本列表中选择 “管理员账号重置密码”，单击操作列“执行”。

步骤5 输入新密码（需符合平台密码复杂度要求，如8-30位字符，包含大写字母、数字及特殊符号）。

步骤6 添加目标ECS实例。

步骤7 单击 “确定”，系统会将脚本远程下发至实例并自动运行，过程中无需登录实例终端。

脚本执行完成后，可直接使用新密码通过SSH工具登录实例，实例全程保持运行状态，无重启动作。

----结束

4.5 在账号管理中查看密码，提示没有权限如何处理?

问题描述

在账号管理中执行密码查看操作时，页面提示用户无查看密码权限，如下图所示。

原因分析

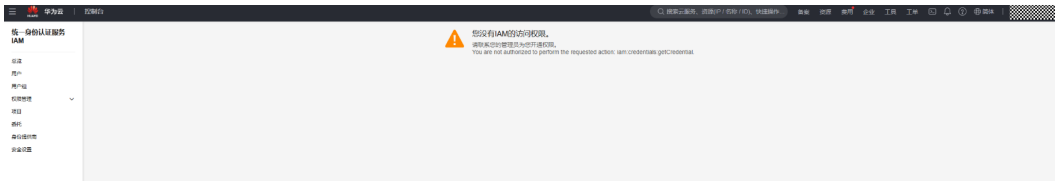
查看密码通常涉及到两个主要步骤：获取加密的密码和解密密码。这两个步骤分别需要coc:account:getPassword和kms:dek:decrypt权限。因此，在查看密码前，请确保用户当前登录账号已获取对应授权。

解决方案

步骤1 登录**IAM控制台**。

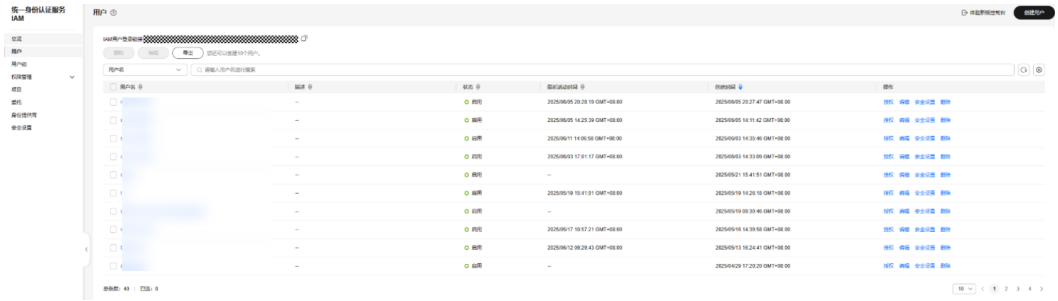
若无IAM访问权限，请联系管理员处理。

图 4-1 无 IAM 访问权限



步骤2 在左侧导航栏选择“用户”，进入用户列表页面。

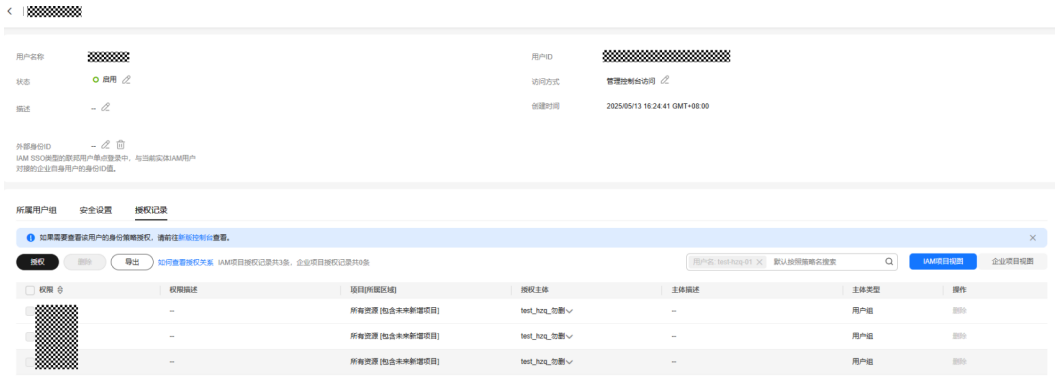
图 4-2 查看用户列表



步骤3 在用户列表中单击待查看的用户名称，进入用户详情页面。

步骤4 选择授权记录页签，查看当前用户所有授权。

图 4-3 查看用户授权记录



步骤5 单击权限名称查看详情，在策略内容中确认Action列表中是否包含coc:account:getPassword和kms:dek:decrypt权限。

图 4-4 确认权限

步骤6 如果当前账号缺少所需权限，请联系账号管理员，在IAM中为登录用户申请coc:account:getPassword和kms:dek:decrypt权限。

具体操作可参见**创建用户组并授权**。

----结束

5 批量操作常见问题

5.1 批量 ECS 资源切换镜像报错如何处理?

问题描述

批量ECS资源切换镜像报错"code":"Ecs.0021","message":"Failed to check Cinder quotas because the number of Gigabytes exceeded the upper limit."或CreateRootVolumeTask-fail: call evs api - create volume fail :{"error_msg":"volume gigabytes exceeded volume gigabytes quota!","common_error_code":"CMM.3141","error_code":"EVS.1042"}

解决方案

用户云硬盘配额不足，需要申请扩大云硬盘配额，具体操作详见**申请扩大云硬盘资源配额**。

6 参数管理常见问题

6.1 参数管理的页面权限说明

权限设计

- 访问参数列表页：需要list权限: coc:parameter:list。
- 获取参数详情：需要get权限：coc:parameter:get。
- 删除参数：需要操作类权限：coc:parameter:delete。
- 创建参数：需要操作类权限：coc:parameter:create。
- 更新参数：需要操作类权限：coc:parameter:update。
- 资源类权限（具体到某一个region下 && 某一个租户的一个参数）：coc:*:*:parameter:name（第一个*代表所有regionID，第二个*所有租户，name代表参数名称）。

常见问题

资源类权限决定您可以访问哪些数据，操作类权限是对您有的资源类权限进行操作。

- 如果您可以访问某个参数，但是您访问不了列表页，代表您缺少coc:parameter:list权限。
- 如果您找不到指定的参数，需要确认是否有该参数的权限。
- coc:service-name:region:account-id:resource-type:resource-path这个是资源类权限的结构，*代表该层级所有权限，添加资源类权限需要按照这个格式填写。

6.2 引用参数中心的参数和目标实例是否可跨 Region?

基于安全生产规则要求，引用“参数中心”的参数和“目标实例”不允许跨Region。

例如：

执行脚本时“脚本入参”选择“参数中心”，参数的区域为“华北-北京四”，则在添加“目标实例”时，区域也需要选择“华北-北京四”，否则会报错，无法执行脚本。

图 6-1 引用参数中心

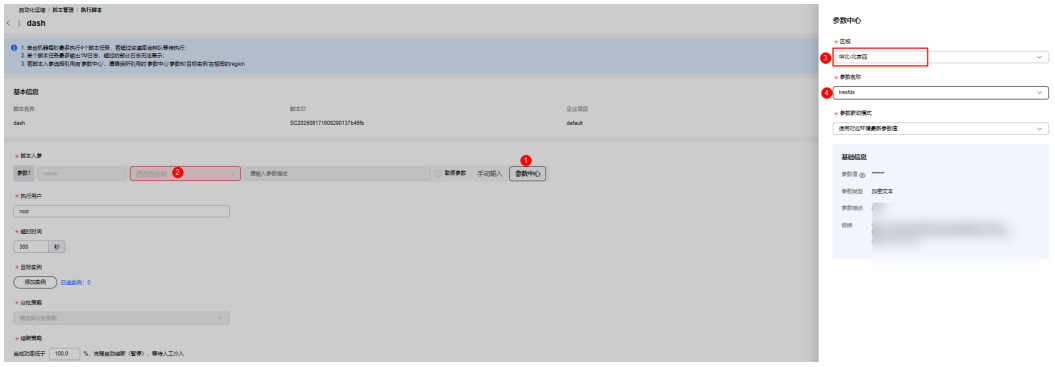
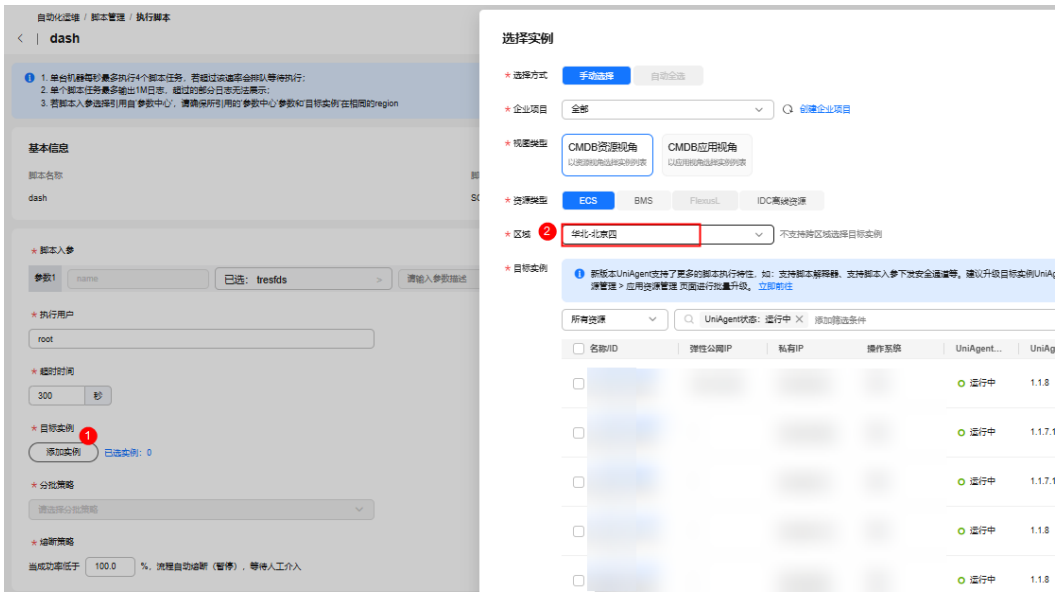


图 6-2 选择实例



7 资源运维常见问题

7.1 资源运维权限和授权项说明

如果您需要对您所拥有的COC的资源运维操作进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称IAM），如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用ECS服务的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于策略对云服务进行操作。

根据授权的精细程度，分为**角色**和**策略**。角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略以API接口为粒度进行权限拆分，授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

COC系统策略说明请参考**COC权限管理**。

说明

如果您需要允许或者禁止某个接口的操作权限，请使用策略。

使用账号下的IAM用户发起API请求时，该IAM用户必须具备调用该接口所需的权限，否则，API请求将调用失败。每个接口所需要的权限，与各个接口所对应的授权项相对应，只有发起请求的用户被授予授权项所对应的策略，该用户才能成功调用该接口。例如，用户要调用接口来查询云服务器列表，那么这个IAM用户被授予的策略中必须包含允许“ecs:servers:list”的授权项，该接口才能调用成功。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。策略支持的操作与API相对应，授权项列表说明如下：

- 权限：允许或拒绝对指定资源在特定条件下进行某项操作。
- 对应API接口：自定义策略实际调用的API接口。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

- 依赖的授权项：部分Action存在对其他Action的依赖，需要将依赖的Action同时写入授权项，才能实现对应的权限功能。
- IAM项目(Project)/企业项目(Enterprise Project)：自定义策略的授权范围，包括IAM项目与企业项目。授权范围如果同时支持IAM项目和企业项目，表示此授权项对应的自定义策略，可以在IAM和企业管理两个服务中给用户组授权并生效。如果仅支持IAM项目，不支持企业项目，表示仅能在IAM中给用户组授权并生效，如果在企业管理中授权，则该自定义策略不生效。

  关于IAM项目与企业项目的区别，详情请参见：**IAM与企业管理的区别**。
- 实例授权/标签授权：自定义策略的生效范围。如果同时支持实例授权和标签授权，表示此授权项对应的自定义策略，可以对某些指定实例或某些绑定指定标签的实例生效。如果仅支持标签授权，不支持实例授权，表示该授权项只能对某些绑定指定标签的实例生效。

  该功能目前在“华北-乌兰察布一”暂不开放。

  说明

  “√”表示支持，“x”表示暂不支持。

COC资源运维支持的自定义策略授权项如下所示：

表 7-1 资源运维支持的自定义策略授权项

功能场景	授权项	描述	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）	实例授权	标签授权
资源同步	coc:instance:listResources	授予查询资源列表的权限。	-	√	x	x	x
	coc:application:listResources	授予查询应用资源列表的权限。	-	√	x	x	x
	coc:instance:syncResources	授予同步资源列表的权限。	-	√	x	x	x
定时运维	coc:schedule:list	查询定时任务列表的权限。	-	√	x	x	x
	coc:schedule:enable	启用定时任务的权限。	-	√	x	x	x
	coc:schedule:update	更新定时任务的权限。	-	√	√	x	x
	coc:schedule:disable	禁用定时任务列表的权限。	-	√	x	x	x

功能场景	授权项	描述	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）	实例授权	标签授权
	coc:schedule:approve	审批定时任务列表的权限。	-	√	x	x	x
	coc:schedule:create	创建定时任务列表的权限。	-	√	√	x	x
	coc:schedule:delete	删除定时任务的权限。	-	√	x	x	x
	coc:schedule:count	查询定时任务数量的权限。	-	√	x	x	x
	coc:schedule:get	查询定时任务记录的权限。	-	√	x	x	x
	coc:schedule:getHistories	查询定时任务执行历史的权限。	-	√	x	x	x
深度诊断	coc:application:GetDiagnosisTaskDetails	查询应用资源诊断任务的权限。	aom:uniagentAgent:install; aom:uniagentAgent:uninstall;	√	x	x	x
	coc:application:CreateDiagnosisTask	创建应用诊断任务的权限。		√	x	x	x
	coc:job:action	授予操作工单的权限。		√	x	x	x
脚本管理/作业管理	coc:document:create	创建文档	aom:uniagentAgent:install; aom:uniagentAgent:list; aom:uniagentInstallHost:list; aom:uniagentProxyRegion:get; iam:agencies:list;	√	x	x	x
	coc:document:listRunbookAtomics	查看作业原子能力列表		√	x	x	x
	coc:document:getRunbookAtomicDetails	查询作业原子能力详情		√	x	x	x
	coc:document:list	查询文档列表		√	x	x	x

功能场景	授权项	描述	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）	实例授权	标签授权
	coc:document:delete	删除文档		√	x	x	x
	coc:document:update	修改文档		√	x	x	x
	coc:document:get	查看文档		√	x	x	x
	coc:document:analyzeRisk	分析文档风险		√	x	x	x
	coc:instance:executeDocument	在弹性云服务器上执行文档		√	x	x	x
资源批量操作	coc:instance:autoBatchInstances	实例自动化分批	ecs:serverKeypairs:list; ecs:servers:get; ecs:cloudServers:list; ecs:cloudServers:rebuild; ecs:cloudServers:changeOS; ecs:cloudServers:showServer; ecs:cloudServers:stop; ecs:cloudServers:reboot; ecs:cloudServers:start; ims:images:get; ims:images:list; bss:order:view; billing:contract:viewDiscount;	√	x	x	x
	coc:instance:executeDocument	在弹性云服务器上执行文档		√	x	x	x
	coc:instance:startRDSInstance	启用RDS实例的权限。		√	√	x	x
	coc:instance:stopRDSInstance	停止RDS实例的权限。		√	√	x	x
	coc:instance:restartRDSInstance	重启RDS实例的权限。		√	√	x	x
	coc:instance:start	启动云服务器的权限。		√	√	x	x
	coc:instance:reboot	重启云服务器的权限。		√	√	x	x
	coc:instance:stop	关闭云服务器的权限。		√	√	x	x

功能场景	授权项	描述	依赖的授权项	IAM项目（Project）	企业项目（Enterprise Project）	实例授权	标签授权
	coc:instance:reinstallOS	重装弹性云服务器操作系统的权限。		√	√	x	x
	coc:instance:changeOS	切换弹性云服务器操作系统的权限。		√	√	x	x

8 故障管理常见问题

8.1 生成事件的流程是什么?

生成事件有三种方式：手动创建事件、告警转事件和通过流转规则自动生成事件，具体介绍如下。

手动创建事件

在**故障管理>事件管理**创建事件单，具体操作详见**创建事件单**。

告警转事件

在**故障管理>事件管理**创建事件单，具体操作详见告警转事件。

流转规则自动生成事件

流转规则自动生成事件，需要做以下步骤：

步骤1 登录**云运维中心**。

步骤2 同步人员，具体参考**人员管理**。

步骤3 设置排班，并给排班中添加排班人员，具体参考**排班管理**。

步骤4 集成监控系统，自动上报告警信息，具体参考**集成管理**。

步骤5 配置流转规则，根据流转规则生成事件，具体参考**配置流转规则**。

步骤6 若事件生成后，想要接收到事件的通知信息，可配置自动通知能力，具体参考**通知管理**。

----结束

8.2 怎么能收到事件单通知?

步骤1 登录**云运维中心**。

步骤2 在人员管理中完成消息通知订阅，具体参考**人员管理**。

步骤3 在通知管理中配置通知规则，具体参考**通知管理**。

----结束

8.3 Warroom 是什么?

WarRoom定义：在发生群体性故障或重大故障时，为快速恢复业务正常运行，支撑运维、研发、运营联合作战，保障业务快速恢复而组建的会议。可通过WarRoom添加故障恢复成员、通过发送故障进展及时知会关注故障的人员、通过应用诊断、响应预案等辅助应用快速恢复。

若需拉起WarRoom群组，需在**移动应用管理**接入钉钉、企业微信或飞书。

已受理的事件可以启动Warroom，具体参考**启动WarRoom**。

Warroom使用指导，请参考**WarRoom管理**。

8.4 故障诊断异常如何处理?

问题描述

用户在“故障诊断”页面选择“ECS诊断”，发起ECS诊断后，执行过程中出现异常。

解决方案

不同的执行阶段产生问题根因并不一致，在此提供了对应的解决方案，建议参照以下步骤排查并处理。

安装插件步骤异常

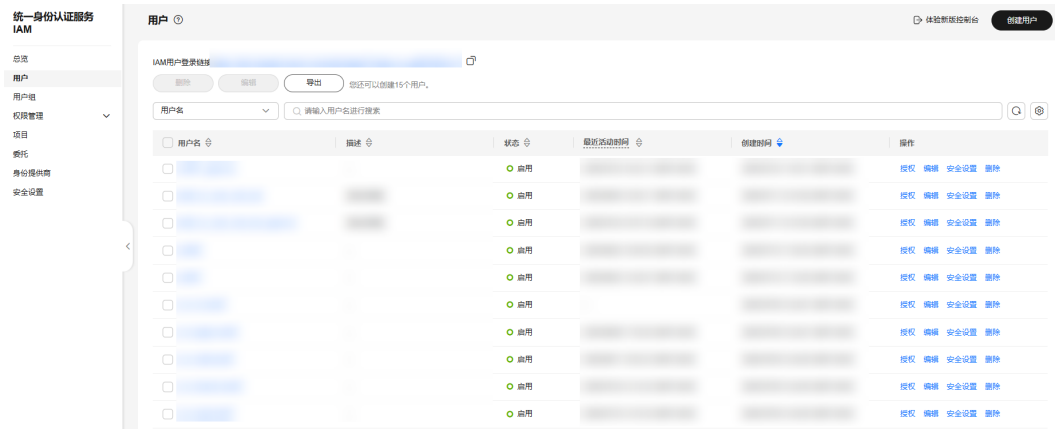
通常情况下，“安装插件”步骤报错是因为用户没有使用Uniagent进行安装插件的IAM权限。具体可参考**批量管理ICAgent插件**。

步骤1 登录**IAM控制台**。

若无IAM访问权限，请联系管理员处理。

步骤2 在左侧导航栏选择“用户”，进入用户列表页面。

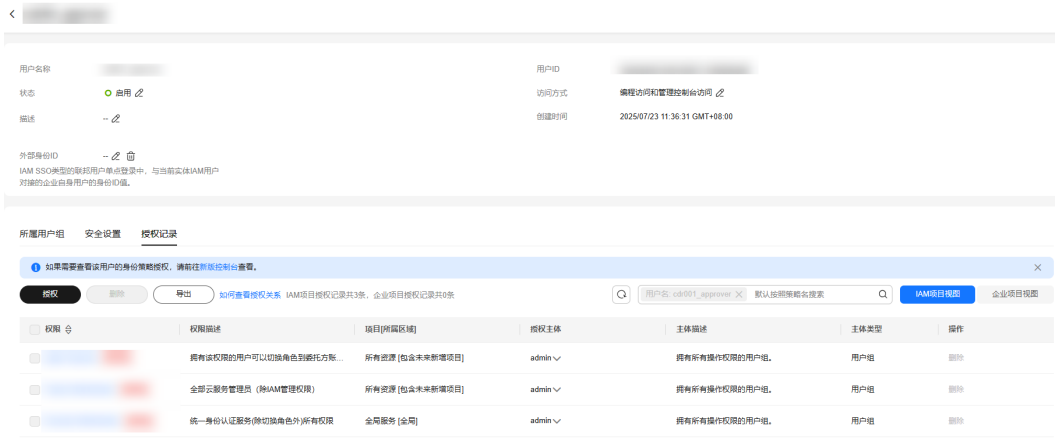
图 8-1 查看用户列表



步骤3 在用户列表中单击待查看的用户名称，进入用户详情页面。

步骤4 选择授权记录页签，查看当前用户所有授权。

图 8-2 查看用户授权记录



步骤5 单击权限名称查看详情，在策略内容中确认Action列表中是否包含aom:uniagentAgent:install权限。

图 8-3 查看权限

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "coc:*:*",
                "*:*:list*",
                "*:*:get*",
                "aom:uniagentAgent:install",
                "aom:uniagentAgent:uninstall",
                "aom:uniagentAgent:list",
                "aom:uniagentAgent:get",
                "aom:uniagentInstallHost:list",
                "aom:uniagentProxyRegion:get",
                "aom:view:get",
                "iam:agencies:createAgency",
                "iam:permissions:grantRoleToAgencyOnDomain",
                "iam:roles:listRoles",
                "iam:agencies:list*",
                "iam:agencies:createServiceLinkedAgency",
                "iam:agencies:deleteServiceLinkedAgency",
                "ecs:*:*",
                "evs:*:get",
                "evs:*:list",
                "evs:volumes:create",
```

步骤6 如果当前账号缺少所需权限，请联系账号管理员，在IAM中为登录用户申请aom:uniagentAgent:install权限。

具体操作可参见**创建用户组并授权**。

----结束

采集数据步骤异常

通常情况下，“采集数据”步骤报错是因为用户执行采集脚本报错，脚本执行报错的根因通常情况下体现在：

- OS镜像版本不符合约束；
- Uniagent版本不符合约束。

具体约束请参见**ECS诊断**页面。

步骤1 登录**云运维中心**。

步骤2 在左侧导航栏选择“任务管理 > 执行记录”。

步骤3 单击上方“脚本工单”。

步骤4 按照工单名称搜索“HWC.COC.PLATFORM-execute-linux-holmes-agent.sh”。

步骤5 单击符合“采集数据”步骤执行时间区间的工单记录，查看详细信息。

- 若出现“/usr/local/uniagentd/tmp/”字样报错，请查看UniAgent版本是否符合约束；
- 若返回正常的以JSON字符串形式展示的采集信息，但执行仍然报错，请查看OS镜像版本是否符合约束。

----结束

故障诊断步骤异常

通常情况下，可能由于网络拥塞导致小概率报错

步骤1 登录**云运维中心**。

步骤2 在左侧导航栏选择“任务管理 > 执行记录”。

步骤3 单击上方“诊断工单”，进入诊断工单页签。

步骤4 单击异常工单名称，进入诊断详情页面。

步骤5 单击“重试”按钮，自行重试即可。

----结束

卸载/清理数据步骤异常

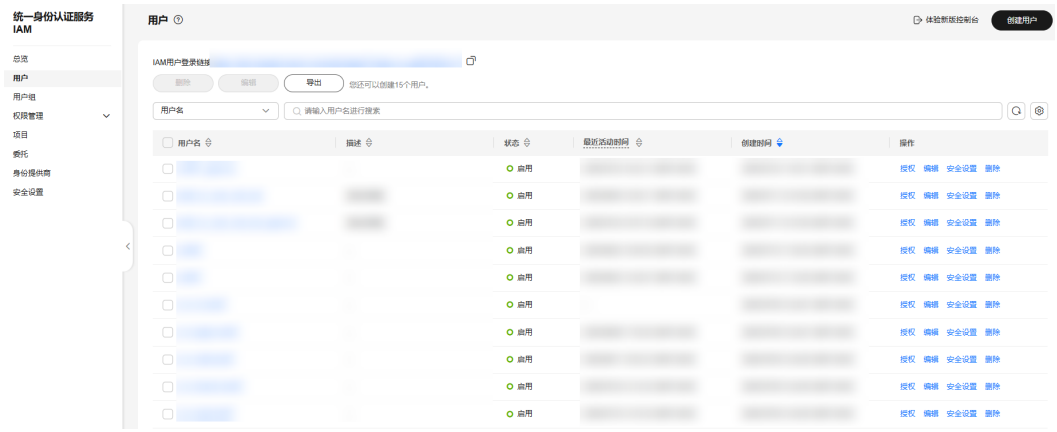
通常情况下，“卸载/清理数据”步骤报错是因为用户没有使用Uniagent进行卸载插件的IAM权限，可参考**批量管理ICAgent插件**。

步骤1 登录**IAM控制台**。

若无IAM访问权限，请联系管理员处理。

步骤2 在左侧导航栏选择“用户”，进入用户列表页面。

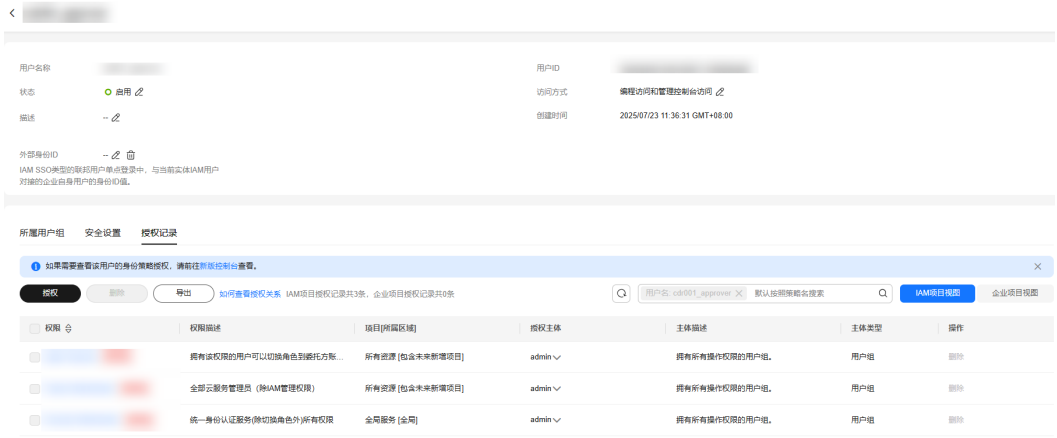
图 8-4 查看用户列表



步骤3 在用户列表中单击待查看的用户名称，进入用户详情页面。

步骤4 选择授权记录页签，查看当前用户所有授权。

图 8-5 查看用户授权记录



步骤5 单击权限名称查看详情，在策略内容中确认Action列表中是否包含aom:uniagentAgent:uninstall权限。

图 8-6 查看权限

步骤6 如果当前账号缺少所需权限，请联系账号管理员，在IAM中为登录用户申请aom:uniagentAgent:uninstall权限。

具体操作可参见**创建用户组并授权**。

----结束

9 变更管理常见问题

9.1 常规变更&紧急变更的区别?

概念上的区别

常规变更（指非紧急、能通过正常程序化的申请、评估、批准、排序、计划、测试、实施和回顾的变更）。

紧急变更（为了处理生产环境不可用或机器不可用、紧急满足业务需求而提出的计划外变更，无法满足计划性要求，或者来不及走正常流程进行评估审批的变更）。

审批环节上的区别

支持针对常规变更、紧急变更两个场景配置审批环节。

9.2 变更级别的定义?

变更级别（以A级风险最高，依次递减至D级）是变更管理体系中常见的风险量化分级逻辑，核心是通过明确的级别划分，让不同风险程度的变更得到匹配的管控资源与审批流程，避免 “高风险变更管控不足” 或 “低风险变更过度冗余” 的问题。

变更级别的本质是将 “抽象风险” 转化为 “可执行的管控标准”，A级到D级的划分并非仅靠 “主观判断”，而是需结合“风险影响范围、发生概率、后果严重度” 三个核心维度量化评估，具体对应关系可参考下表：

表 9-1 变更级别说明

变更级别	风险核心特征（量化维度）	典型风险后果
A级（最高风险）	● 影响范围：跨部门/全业务线； ● 发生概率：中高； ● 后果严重度：直接导致业务中断、合规违规、重大经济损失。	业务停服、客户大规模投诉、监管处罚、百万级以上损失。
B级（较高风险）	● 影响范围：单部门核心业务； ● 发生概率：中； ● 后果严重度：部门级效率下降、局部合规风险。	部门工作延误、小范围合规隐患、十万级损失。
C级（中等风险）	● 影响范围：单团队/单一业务环节； ● 发生概率：低； ● 后果严重度：局部操作不便、无直接经济损失。	团队内效率轻微下降、无需额外成本修复。
D级（最低风险）	● 影响范围：个人操作/非核心环节； ● 发生概率：极低； ● 后果严重度：无实质影响。	无负面后果，甚至优化体验。

10 韧性中心常见问题

10.1 混沌演练是什么?

随着传统IT基础设施运维向云服务运维方式的转变，传统的运维手段面临服务间调用复杂、应用迭代速度快、海量运维对象、复杂系统非线性等挑战。业务的停机都会给公司带来巨大的经济损失和声誉影响。

在运维过程中引入混沌工程，通过定期进行演练的方式，可以在现网问题发生前识别系统的薄弱点（软件Bug、方案设计不足之处、故障恢复流程卡点等），及早发现系统可用性的问题进行解决，持续提升应用韧性，建立运维信心。对于无法避免的场景（硬件故障、服务器异常下电、网络设备单板故障等）通过提前制定快速恢复应急预案进行应对。

COC混沌演练为用户提供一站式的自动化演练能力，覆盖从风险识别、应急预案管理、故障注入到复盘改进的端到端演练流程。承载华为云SRE在混沌演练上多年的最佳实践，使客户能对云上应用主动地进行风险识别、消减和风险验证，持续提升云应用的韧性。

10.2 支持哪些攻击场景?

混沌演练现在支持多种攻击场景供用户演练使用，包括体验类、主机资源、主机进程、主机网络、自定义故障和资源运维。通过集成武器模块和功能，用户可以更准确地模拟真实环境故障，及早发现系统可用性等问题，持续提升应用韧性。现已全面支持ECS、BMS和IDC离线设备的IPv6故障演练，通过主机网络类武器的演练，可以帮助用户快速掌握IPv6环境下的故障定位与应急响应能力，确保网络的高可用性与安全性。

攻击场景说明

表 10-1 攻击场景说明

攻击目标来源	攻击场景		说明
弹性云服务器(ECS)	体验类	小试牛刀	不产生任何故障，帮助您了解混沌演练的执行流程。
	主机资源	CPU使用率加压	模拟CPU使用率飙升，支持故障紧急终止。
		内存使用率加压	模拟内存使用率飙升，支持故障紧急终止。
		磁盘使用率加压	模拟磁盘使用率飙升，支持故障紧急终止。
		磁盘IO加压	通过不间断读写文件，对磁盘IO加压，支持故障紧急终止。
	主机进程	进程号耗尽	耗尽系统进程号（PID），不支持故障紧急终止。
		杀进程	故障持续期间重复杀进程，支持故障紧急终止；紧急终止或演练结束后演练系统不负责拉起进程，服务需自行保证进程恢复正常。
	主机网络	网络延迟	模拟网络故障导致链路延迟增大，支持故障紧急终止。
		网络丢包	模拟网络故障导致链路产生丢包，支持故障紧急终止（丢包率100%时不支持）。
		网络错包	模拟网络故障导致链路产生错包，支持故障紧急终止（错包率100%时不支持）。
		网络包重复	模拟网络故障导致链路产生重复包，支持故障紧急终止。
		网络包乱序	模拟网络故障导致链路产生包乱序，支持故障紧急终止。
		网络中断	模拟节点间网络不通，支持故障紧急终止；请勿填写演练系统和UniAgent服务器的IP地址，否则可能导致演练失败；如需要中断已建立的长连接，中断方向请选择全方向。
		网卡down	模拟网卡down的情况，因各主机网络配置不同，网卡down后有可能启动网卡失败，请做好恢复网络的应急预案，不支持故障紧急终止。

攻击目标来源	攻击场景		说明
		篡改DNS域名解析	篡改域名地址映射，支持故障紧急终止。
		端口占用	模拟系统网络端口被占用（最多100个），支持故障紧急终止。
		整机断网	模拟整机断网的情况，拒绝所有基于TCP，UDP，ICMP协议的数据包，只开放22，8002，39604，33552，33554，33557，32552，32554，32557端口，支持故障紧急终止。
		网卡带宽限速	限制网卡带宽速度，支持多网卡，支持故障紧急终止。
		网络连接耗尽	创建大量到指定IP:Port（服务端）的Socket连接进行消耗，使节点正常请求无法连接到服务端（对服务端处理其他节点的请求可能也有影响），支持故障紧急终止。
	自定义故障	自定义脚本	用户通过自动化运维的脚本创建脚本，通过执行脚本模拟故障发生的情况，支持故障紧急终止。
	资源运维	开机	提供ECS/BMS/Flexus批量开机能力，可能存在状态同步不及时问题，支持故障紧急终止。
		关机	提供ECS/BMS/Flexus批量关机能力，可能存在状态同步不及时问题，支持故障紧急终止。
		重启	提供ECS/BMS/Flexus批量重启能力，可能存在状态同步不及时问题，支持故障紧急终止。
裸金属服务器(BMS)	体验类	小试牛刀	不产生任何故障，帮助您了解混沌演练的执行流程。
	主机资源	CPU使用率加压	模拟CPU使用率飙升，支持故障紧急终止。
		内存使用率加压	模拟内存使用率飙升，支持故障紧急终止。
		磁盘使用率加压	模拟磁盘使用率飙升，支持故障紧急终止。
		磁盘IO加压	通过不间断读写文件，对磁盘IO加压，支持故障紧急终止。
	主机进程	进程号耗尽	耗尽系统进程号（PID），不支持故障紧急终止。

攻击目标来源	攻击场景		说明
		杀进程	故障持续期间重复杀进程，支持故障紧急终止；紧急终止或演练结束后演练系统不负责拉起进程，服务需自行保证进程恢复正常。
	主机网络	网络延迟	模拟网络故障导致链路延迟增大，支持故障紧急终止。
		网络丢包	模拟网络故障导致链路产生丢包，支持故障紧急终止（丢包率100%时不支持）。
		网络错包	模拟网络故障导致链路产生错包，支持故障紧急终止（错包率100%时不支持）。
		网络包重复	模拟网络故障导致链路产生重复包，支持故障紧急终止。
		网络包乱序	模拟网络故障导致链路产生包乱序，支持故障紧急终止。
		网络中断	模拟节点间网络不通，支持故障紧急终止；请勿填写演练系统和UniAgent服务器的IP地址，否则可能导致演练失败；如需要中断已建立的长连接，中断方向请选择全方向。
		网卡down	模拟网卡down的情况，因各主机网络配置不同，网卡down后有可能启动网卡失败，请做好恢复网络的应急预案，不支持故障紧急终止。
		篡改DNS域名解析	篡改域名地址映射，支持故障紧急终止。
		端口占用	模拟系统网络端口被占用（最多100个），支持故障紧急终止。
		整机断网	模拟整机断网的情况，拒绝所有基于TCP，UDP，ICMP协议的数据包，只开放22，8002，39604，33552，33554，33557，32552，32554，32557端口，支持故障紧急终止。
	资源运维	开机	提供ECS/BMS/Flexus批量开机能力，可能存在状态同步不及时问题，支持故障紧急终止。
		关机	提供ECS/BMS/Flexus批量关机能力，可能存在状态同步不及时问题，支持故障紧急终止。
		重启	提供ECS/BMS/Flexus批量重启能力，可能存在状态同步不及时问题，支持故障紧急终止。
Flexus应用服务器L实例(HCSS)	体验类	小试牛刀	不产生任何故障，帮助您了解混沌演练的执行流程。

攻击目标来源	攻击场景		说明
	主机资源	CPU使用率加压	模拟CPU使用率飙升，支持故障紧急终止。
		内存使用率加压	模拟内存使用率飙升，支持故障紧急终止。
		磁盘使用率加压	模拟磁盘使用率飙升，支持故障紧急终止。
		磁盘IO加压	通过不间断读写文件，对磁盘IO加压，支持故障紧急终止。
	主机进程	进程号耗尽	耗尽系统进程号（PID），不支持故障紧急终止。
		杀进程	HCSS故障持续期间重复杀进程，支持故障紧急终止；紧急终止或演练结束后演练系统不负责拉起进程，服务需自行保证进程恢复正常。
	主机网络	网络延迟	模拟网络故障导致链路延迟增大，支持故障紧急终止。
		网络丢包	模拟网络故障导致链路产生丢包，支持故障紧急终止（丢包率100%时不支持）。
		网络错包	模拟网络故障导致链路产生错包，支持故障紧急终止（错包率100%时不支持）。
		网络包重复	模拟网络故障导致链路产生重复包，支持故障紧急终止。
		网络包乱序	模拟网络故障导致链路产生包乱序，支持故障紧急终止。
		网络中断	模拟节点间网络不通，支持故障紧急终止；请勿填写演练系统和UniAgent服务器的IP地址，否则可能导致演练失败；如需要中断已建立的长连接，中断方向请选择全方向。
		网卡down	模拟网卡down的情况，因各主机网络配置不同，网卡down后有可能启动网卡失败，请做好恢复网络的应急预案，不支持故障紧急终止。
		篡改DNS域名解析	篡改域名地址映射，支持故障紧急终止。
		端口占用	模拟系统网络端口被占用（最多100个），支持故障紧急终止。

攻击目标来源	攻击场景		说明
		整机断网	模拟整机断网的情况，拒绝所有基于TCP，UDP，ICMP协议的数据包，只开放22，8002，39604，33552，33554，33557，32552，32554，32557端口，支持故障紧急终止。
	资源运维	开机	提供ECS/BMS/Flexus批量开机能力，可能存在状态同步不及时问题，支持故障紧急终止。
		关机	提供ECS/BMS/Flexus批量关机能力，可能存在状态同步不及时问题，支持故障紧急终止。
		重启	提供ECS/BMS/Flexus批量重启能力，可能存在状态同步不及时问题，支持故障紧急终止。
云容器引擎 (CCE) Node类型	体验类	小试牛刀	不产生任何故障，帮助您了解混沌演练的执行流程。
	主机资源	CPU使用率加压	模拟CPU使用率飙升，支持故障紧急终止。
		内存使用率加压	模拟内存使用率飙升，支持故障紧急终止。
		磁盘使用率加压	模拟磁盘使用率飙升，支持故障紧急终止。
		磁盘IO加压	通过不间断读写文件，对磁盘IO加压，支持故障紧急终止。
	主机进程	进程号耗尽	耗尽系统进程号（PID），不支持故障紧急终止。
		杀进程	故障持续期间重复杀进程，支持故障紧急终止；紧急终止或演练结束后演练系统不负责拉起进程，服务需自行保证进程恢复正常。
	主机网络	网络延迟	模拟网络故障导致链路延迟增大，支持故障紧急终止。
		网络丢包	模拟网络故障导致链路产生丢包，支持故障紧急终止（丢包率100%时不支持）。
		网络错包	模拟网络故障导致链路产生错包，支持故障紧急终止（错包率100%时不支持）。
		网络包重复	模拟网络故障导致链路产生重复包，支持故障紧急终止。
		网络包乱序	模拟网络故障导致链路产生包乱序，支持故障紧急终止。

攻击目标来源	攻击场景		说明
		网络中断	模拟节点间网络不通，支持故障紧急终止；请勿填写演练系统和UniAgent服务器的IP地址，否则可能导致演练失败；如需要中断已建立的长连接，中断方向请选择全方向。
		网卡down	模拟网卡down的情况，因各主机网络配置不同，网卡down后有可能启动网卡失败，请做好恢复网络的应急预案，不支持故障紧急终止。
		篡改DNS域名解析	篡改域名地址映射，支持故障紧急终止。
		端口占用	模拟系统网络端口被占用（最多100个），支持故障紧急终止。
		整机断网	模拟整机断网的情况，拒绝所有基于TCP，UDP，ICMP协议的数据包，只开放22，8002，39604，33552，33554，33557，32552，32554，32557端口，支持故障紧急终止。
		网卡带宽限速	限制网卡带宽速度，支持多网卡，支持故障紧急终止。
		网络连接耗尽	创建大量到指定IP:Port（服务端）的Socket连接进行消耗，使节点正常请求无法连接到服务端（对服务端处理其他节点的请求可能也有影响），支持故障紧急终止。
云容器引擎 (CCE) Pod类型	Pod资源	Pod CPU加压	模拟Pod CPU使用率飙升，请确认攻击目标可写，否则将导致演练失败，支持故障紧急终止。
		Pod内存加压	模拟Pod内存使用率飙升，请确认攻击目标可写，否则将导致演练失败，支持故障紧急终止。
		Pod磁盘IO加压	模拟不断读写IO，支持故障紧急终止。
		Pod磁盘使用率加压	模拟K8s容器文件系统加压，在指定目录写入超大文件，支持故障紧急终止。
	Pod进程	强制停止Pod实例	强制停止Pod，不支持故障紧急终止。
		强制杀掉Pod内的容器	强制杀掉Pod内的容器，不支持故障紧急终止。
	Pod网络	Pod网络延迟	模拟Pod网络故障导致网络延迟增高，支持故障紧急终止（延迟30000毫秒及以上时不支持）。

攻击目标来源	攻击场景		说明
		Pod网络丢包	模拟Pod网络故障导致网络丢包，支持故障紧急终止。
		Pod网络中断	模拟Pod到其他IP网络不通，支持故障紧急终止，如需要中断已建立的长连接，中断方向请选择全方向。
		Pod网络包乱序	模拟Pod网络故障导致链路产生包乱序，支持故障紧急终止。
		Pod网络包重复	模拟Pod网络故障导致链路产生重复包，支持故障紧急终止。
		Pod篡改DNS域名解析	在Pod内篡改域名的地址映射，请确认攻击目标的运行用户为root，否则会权限不足导致演练失败，支持故障紧急终止。
		Pod端口屏蔽	模拟Pod端口不通，支持故障紧急终止。
		Pod网络隔离	模拟Pod访问其他IP网络时被直接拒绝，支持故障紧急终止，如需要拒绝已建立的长连接，方向请选择全方向。
云数据库(RDS)	实例类	RDS主备倒换	仅支持HA模式的MySQL和PostgreSQL引擎，实例在创建、重启、数据库升级、变更规格、恢复、修改端口、删除用户、创建用户时不能进行此操作，主备倒换不会改变实例的内网地址，不支持故障紧急终止。
		RDS实例停止	同时停止主实例和只读实例，故障持续时长结束后开启实例，支持故障紧急终止。
分布式缓存服务(DCS)	实例类	DCS主备倒换	切换实例主备节点，只有主备实例支持该操作。不支持故障紧急终止。
		DCS实例重启	重启运行中的DCS缓存实例。清空Redis4.0/Redis5.0/Redis6.0的实例数据，数据清空后，无法撤销，且无法恢复，请谨慎操作。不支持故障紧急终止。
		DCS AZ下电	实现该AZ下的所有节点统一下电。不支持故障紧急终止，部分区域不支持该武器。
云搜索服务 (CSS)	实例类	CSS集群重启	重启状态可用的CSS集群。重启期间，kibana和cerebro可能会访问失败。不支持故障紧急终止。
文档数据库服务(DDS)	实例类	备节点强制升主	支持副本集、shard和config备节点强制升主。但在主备时延较大的情况下存在失败风险，不支持故障紧急终止。
IDC离线资源-虚拟机类型	体验类	小试牛刀	不产生任何故障，帮助您了解混沌演练的执行流程。

攻击目标来源	攻击场景		说明
	主机资源	CPU使用率加压	模拟CPU使用率飙升，支持故障紧急终止。
		内存使用率加压	模拟内存使用率飙升，支持故障紧急终止。
		磁盘使用率加压	模拟磁盘使用率飙升，支持故障紧急终止。
		磁盘IO加压	通过不间断读写文件，对磁盘IO加压，支持故障紧急终止。
	主机进程	进程号耗尽	耗尽系统进程号（PID），不支持故障紧急终止。
		杀进程	故障持续期间重复杀进程，支持故障紧急终止；紧急终止或演练结束后演练系统不负责拉起进程，服务需自行保证进程恢复正常。
	主机网络	网络延迟	模拟网络故障导致链路延迟增大，支持故障紧急终止。
		网络丢包	模拟网络故障导致链路产生丢包，支持故障紧急终止（丢包率100%时不支持）。
		网络错包	模拟网络故障导致链路产生错包，支持故障紧急终止（错包率100%时不支持）。
		网络包重复	模拟网络故障导致链路产生重复包，支持故障紧急终止。
		网络包乱序	模拟网络故障导致链路产生包乱序，支持故障紧急终止。
		网络中断	模拟节点间网络不通，支持故障紧急终止；请勿填写演练系统和UniAgent服务器的IP地址，否则可能导致演练失败；如需要中断已建立的长连接，中断方向请选择全方向。
		网卡down	模拟网卡down的情况，因各主机网络配置不同，网卡down后有可能启动网卡失败，请做好恢复网络的应急预案，不支持故障紧急终止。
		篡改DNS域名解析	篡改域名地址映射，支持故障紧急终止。
		端口占用	模拟系统网络端口被占用（最多100个），支持故障紧急终止。

攻击目标来源	攻击场景		说明
		整机断网	模拟整机断网的情况，拒绝所有基于TCP，UDP，ICMP协议的数据包，只开放22，8002，39604，33552，33554，33557，32552，32554，32557端口，支持故障紧急终止。
		网卡带宽限速	限制网卡带宽速度，支持多网卡，支持故障紧急终止。
		网络连接耗尽	创建大量到指定IP:Port（服务端）的Socket连接进行消耗，使节点正常请求无法连接到服务端（对服务端处理其他节点的请求可能也有影响），支持故障紧急终止。
阿里云-云服务器	体验类	小试牛刀	不产生任何故障，帮助您了解混沌演练的执行流程。
	主机资源	CPU使用率加压	模拟CPU使用率飙升，支持故障紧急终止。
		内存使用率加压	模拟内存使用率飙升，支持故障紧急终止。
		磁盘使用率加压	模拟磁盘使用率飙升，支持故障紧急终止。
		磁盘IO加压	通过不间断读写文件，对磁盘IO加压，支持故障紧急终止。
	主机进程	进程号耗尽	耗尽系统进程号（PID），不支持故障紧急终止。
		杀进程	故障持续期间重复杀进程，支持故障紧急终止；紧急终止或演练结束后演练系统不负责拉起进程，服务需自行保证进程恢复正常。
	主机网络	网络延迟	模拟网络故障导致链路延迟增大，支持故障紧急终止。
		网络丢包	模拟网络故障导致链路产生丢包，支持故障紧急终止（丢包率100%时不支持）。
		网络错包	模拟网络故障导致链路产生错包，支持故障紧急终止（错包率100%时不支持）。
		网络包重复	模拟网络故障导致链路产生重复包，支持故障紧急终止。
		网络包乱序	模拟网络故障导致链路产生包乱序，支持故障紧急终止。

攻击目标来源	攻击场景		说明
		网络中断	模拟节点间网络不通，支持故障紧急终止；请勿填写演练系统和UniAgent服务器的IP地址，否则可能导致演练失败；如需要中断已建立的长连接，中断方向请选择全方向。
		网卡down	模拟网卡down的情况，因各主机网络配置不同，网卡down后有可能启动网卡失败，请做好恢复网络的应急预案，不支持故障紧急终止。
		篡改DNS域名解析	篡改域名地址映射，支持故障紧急终止。
		端口占用	模拟系统网络端口被占用（最多100个），支持故障紧急终止。
		整机断网	模拟整机断网的情况，拒绝所有基于TCP，UDP，ICMP协议的数据包，只开放22，8002，39604，33552，33554，33557，32552，32554，32557端口，支持故障紧急终止。
		网卡带宽限速	限制网卡带宽速度，支持多网卡，支持故障紧急终止。
		网络连接耗尽	创建大量到指定IP:Port（服务端）的Socket连接进行消耗，使节点正常请求无法连接到服务端（对服务端处理其他节点的请求可能也有影响），支持故障紧急终止。

10.3 故障模式是什么？

故障模式是对云应用面临的潜在风险进行分析和评估的结果，混沌演练平台预置华为云多年积累的故障模式数据，使用FT-FMEA故障分析法帮助您分析云应用存在的潜在风险。

故障模式聚焦于云应用的风险研判，通过系统性评估应用架构、依赖关系及潜在薄弱点，精准识别可能引发服务异常的风险场景（如节点宕机、网络延迟、资源耗尽等），是混沌演练开展的核心前提与依据。

10.4 演练规划主要做什么？

演练规划是故障演练管理的核心保障，不仅能帮助演练管理人员对各类故障模式进行系统化演练排期，更可实时跟踪、管理演练全流程进展，确保故障模式通过实战演练得到有效检验。

在具体操作中，创建演练规划时需明确指定执行人与计划演练时间，形成标准化任务分配依据；执行人通过 “接单” 确认任务后，系统自动生成对应的演练任务，且该任务需精准关联预设故障模式与具体应用区域，实现演练场景与实际业务场景的高度契合，为演练效果评估与后续流程优化提供坚实支撑。

演练规划是故障演练管理的核心保障，其价值贯穿演练全生命周期：

- 在规划启动阶段，可帮助演练管理人员结合业务优先级、历史故障数据及风险评估结果，对高影响、高频发的故障模式进行分层级、分周期的系统化演练排期，避免演练资源浪费与重点场景遗漏；
- 在执行管控阶段，通过实时跟踪演练任务的启动状态、执行进度、关键节点完成情况（如故障注入、应急响应、问题修复等），并支持对延迟任务的预警提醒与执行人的协同调度，有效管理演练全流程进展，确保每一项演练动作都按计划落地；
- 最终通过标准化的规划设计，确保故障模式能通过 “场景模拟 - 实际操作 - 问题复盘” 的完整演练闭环得到有效检验，验证应急预案的可行性与团队应急处置能力。

10.5 故障模式和演练任务的关系?

故障模式与演练任务是混沌演练体系中紧密衔接、层层递进的核心环节，二者构成 “风险前置识别” 与 “实现化验证” 的闭环关系：

故障模式聚焦于云应用的风险研判，通过系统性评估应用架构、依赖关系及潜在薄弱点，精准识别可能引发服务异常的风险场景（如节点宕机、网络延迟、资源耗尽等），是混沌演练开展的核心前提与依据。

而演练任务则是故障模式的 “实现化落地载体”：它基于已识别的故障模式，将单一或关联的故障场景进行合理组合与场景化设计，再通过故障注入工具（如模拟服务器下线、注入流量拥塞等）复现对应风险，最终验证应用的容错能力、故障自愈效率及应急预案有效性，实现从 “风险识别” 到 “能力验证” 的转化。

10.6 演练报告有哪些内容?

演练任务完成后，若有演练报告的制作需求，可以直接创建报告内容。报告创建完成后，还可以一键将报告导出为PDF文件，发送给相关人员。整个过程灵活高效，轻松满足从制作到格式固化的全流程需求。

演练报告支持修改实际恢复时长、创建改进单及查看故障记录，助力用户全面地记录和管理演练活动及结果。

演练报告包含以下模块：

- **恢复能力评分模块**：支持修改实际恢复时长，系统将自动生成恢复能力评分。
- **基本信息模块**：展示演练任务的基本信息，包含演练任务名称、演练报告ID、开始时间、结束时间、演练执行人、演练耗时及期望恢复时长（单位：分钟）。
- **演练过程模块**：展示各项演练任务的卡片式信息。
- **攻击任务组模块**：展示攻击任务详情，涵盖攻击目标、稳态指标和监控指标。

  攻击目标展示已选实例列表，稳态指标和监控指标展示折线图，没有数据则展示“暂无数据”。
- **改进事项模块**：支持创建改进单，其列表会默认展开详情内容，包含处理信息和验证信息。

11 基础配置常见问题

11.1 非普通 IAM 用户登录如何使用 COC

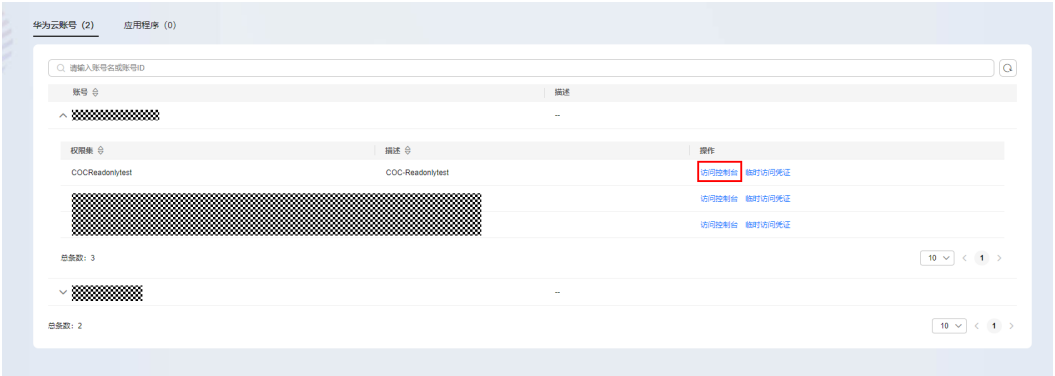
云运维中心COC当前支持以下登录方式：普通IAM用户、IAM联邦用户（包括IAM用户SSO、虚拟用户SSO）和IAM身份中心用户。若您并非通过普通IAM用户登录COC，请参考以下介绍及步骤指引，确保正常使用COC。

IAM 身份中心登录

IAM身份中心服务为用户提供基于组织的多账号统一身份管理与访问控制。在该服务创建用户后，使用特定用户名和密码即可登录统一的门户网站，访问为其分配的多个账号的资源，无需多次登录。

步骤1 通过IAM身份中心门户登录华为云。若您首次使用IAM身份中心，请参考IAM身份中心入门指引。

图 11-1 IAM 身份中心门户登录入口



步骤2 通过控制台访问云运维中心COC。

步骤3 在左侧导航栏选择“基础配置 > 人员管理”。

步骤4 单击列表上方的“同步人员”，完成IAM身份中心人员信息的同步。

图 11-2 同步人员

----结束

IAM 联邦用户登录

若您已有自己的企业管理系统，同时您的用户需要使用华为云账号的云服务资源，您可以通过IAM的身份提供商功能，实现企业管理系统账号单点登录华为云，该过程称为**联邦身份认证**。通过联邦身份认证登录的用户，简称为**联邦用户**。联邦用户目前支持两种身份提供商类型：虚拟用户SSO和IAM用户SSO。两者的区别和使用场景详见**虚拟用户SSO与IAM用户SSO的适用场景**。

若您通过IAM用户SSO登录COC，参考普通IAM用户使用COC的流程即可。

若您通过虚拟用户SSO登录COC，需要先进行以下操作。

步骤1 登录**云运维中心**。

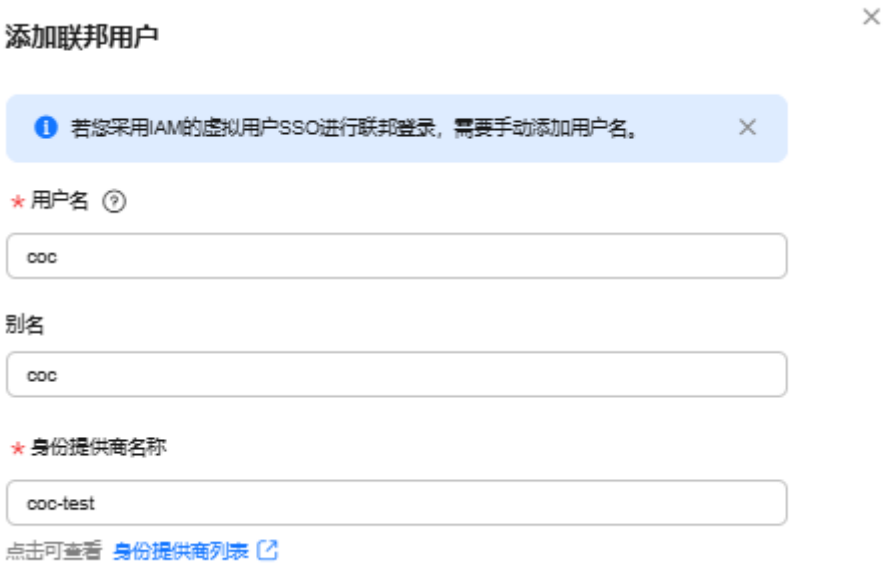
步骤2 在左侧导航栏选择“基础配置 > 人员管理”。

步骤3 单击左上方“添加联邦用户”。

步骤4 设置“添加联邦用户”。

- 用户名：用户在IAM身份转换规则中配置的在华为云中显示的用户名。
- 别名：为当前用户添加一个名称。
- 身份提供商名称：用户在IAM设置的身份提供商名称。

图 11-3 添加联邦用户



步骤5 单击“确定”，完成联邦用户的添加。

----结束

