云运维中心

快速入门

文档版本 2.0

发布日期 2024-06-06

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 账号与授权.....1
2 开通云运维中心.....4
3 应用资源建模.....9
4 运维基础配置.....12
5 跨账号管理.....16
5.1 跨账号管理概述.....16
5.2 开启跨账号管理.....16
6 入门实践.....19
7 修订记录.....20

1 账号与授权

使用云运维中心（Cloud Operations Center，以下简称COC）之前，您需要拥有一个华为账号或一个可用于访问COC的IAM用户，本节将介绍如何注册华为账号开通华为云并实名认证，创建IAM用户并完成授权。

注册华为账号开通华为云并实名认证

请参考以下步骤注册华为账号开通华为云并完成实名认证。如果您已经有一个华为账号，无需重新注册。

步骤1 访问**华为云**，单击“**注册**”。

步骤2 根据提示信息完成注册开通，详细操作请参见**注册华为账号并开通华为云**。

步骤3 完成个人或企业账号实名认证。

- 个人账号：**实名认证**
- 企业账号：**实名认证**

----结束

创建 IAM 用户

IAM用户由账号创建并管理，可以确保账号及资源的安全性，有关IAM的详细介绍请参见**IAM用户**。此处介绍如何创建一个具有COC使用权限的IAM用户。若您不需要使用IAM用户，可以略过此部分内容。

步骤1 访问**华为云**，使用账号和密码登录管理控制台。

步骤2 在“控制台”页面，鼠标悬浮至右上方登录的用户名，在下拉列表中选择“**统一身份认证**”。

图 1-1 统一身份认证

步骤3 **创建用户组并授权**。

在左侧导航栏中选择“**用户组**”，在“用户组”页面，单击“**创建用户组**”，在弹出的“创建用户组”页面填写用户组名称和描述信息，完成用户组创建。

图 1-2 创建用户组

步骤4 用户组创建成功后，单击用户组“操作”列的“**授权**”，进入用户组选择策略页面，在右上角搜索框中按关键字“COC”搜索策略，勾选需要授予用户组的权限。COC权限说明参见**权限管理**。

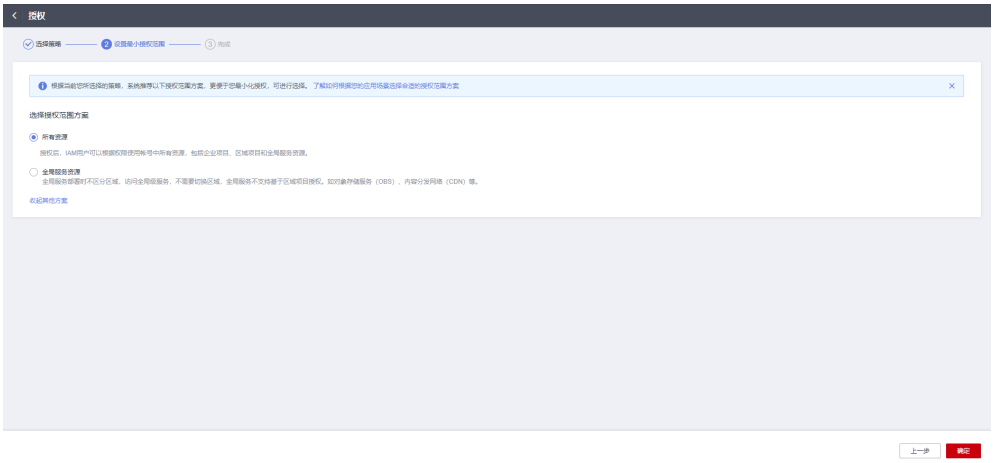
图 1-3 选择策略

说明

- COC FullAccess策略中包含的权限较大，请慎重添加。
- 如只需给用户授权部分COC功能，可**创建自定义策略**使用细粒度授权。

步骤5 策略配置完成后，在设置最小授权范围页面中，选择授权范围方案，单击右下角的“**确定**”完成授权。

图 1-4 设置最小授权范围



步骤6 **创建用户并加入用户组**

创建用户时选择**步骤3**创建的具有COC权限的用户组。

----结束

获取访问密钥（AK/SK）

账号和IAM用户的访问密钥是单独的身份凭证，即账号和IAM用户仅能使用自己的访问密钥进行API调用/鉴权。获取访问密钥的方法请参见**新增访问密钥**。

2 开通云运维中心

新用户首次登陆云运维中心 COC，由于COC提供了对云服务资源的自动化运维、故障管理等能力，需要获得访问其他云服务的委托权限。COC需要创建名为ServiceLinkedAgencyForCOC和ServiceAgencyForCOC的委托。委托包含的权限可见**表1**以及**表2**。

图 2-1 开通 COC

表 2-1 ServiceAgencyForCOC 包含的权限

权限	权限描述	项目[所属区域]	使用场景
IAM ReadOnlyAccess	统一身份认证服务的只读权限	全局服务 [全局]	人员管理中读取IAM账户下的人员信息

权限	权限描述	项目[所属区域]	使用场景
ECS FullAccess	弹性云服务器所有权限	所有资源 [包含未来新增项目]	资源运维中对ECS实例进行批量操作以及自动化运维操作
RMS ReadOnlyAccess	资源管理服务只读权限	全局服务 [全局]	资源管理中同步纳管云服务资源
KMS CMKFullAccess	密钥管理服务加密密钥所有权限	所有资源 [包含未来新增项目]	参数中心以及账号管理中，通过加密密钥对用户资源进行加密
CCE Administrator	云容器引擎（CCE）管理员，拥有该服务下的所有权限	所有资源 [包含未来新增项目]	混沌演练中对CCE资源执行故障注入
RDS FullAccess	关系型数据库服务所有权限	所有资源 [包含未来新增项目]	资源运维中对RDS实例进行批量操作以及自动化运维操作
SMN FullAccess	拥有消息通知服务的所有权限	所有资源 [包含未来新增项目]	人员管理添加通知方式，需要在SMN服务中添加订阅
CES FullAccess	云监控服务所有权限	所有资源 [包含未来新增项目]	故障管理中获取CES告警信息
AOM FullAccess	应用运维管理服务所有权限	所有资源 [包含未来新增项目]	故障管理中获取AOM告警信息，自动化运维中通过AOM Uniagent执行命令下发
DCS UserAccess	分布式缓存服务普通用户权限(无实例创建、修改、删除、扩缩容)	所有资源 [包含未来新增项目]	混沌演练中对DCS资源执行故障注入

表 2-2 ServiceLinkedAgencyForCOC 包含的权限

权限	授权项	使用场景
下发agent作业	aom:uniagentJob:create	自动化运维中执行脚本、作业、定时任务
查询agent作业日志	aom:uniagentJob:get	自动化运维中查看脚本、作业、定时任务的日志
查询用户列表	IdentityCenter:user:list	人员管理中同步人员信息
创建主题	smn:topic:create	人员管理中添加通知订阅

权限	授权项	使用场景
查询主题列表	smn:topic:listTopic	故障管理、自动化运维等场景发送通知
更新主题	smn:topic:updateTopic	人员管理中修改通知订阅
查询主题详情	smn:topic:get	故障管理、自动化运维等场景发送通知
删除主题	smn:topic:delete	人员管理中删除通知订阅
查询主题策略	smn:topic:listAttributes	故障管理、自动化运维等场景发送通知
删除主题策略	smn:topic:deleteAttribute	人员管理中删除通知订阅
更新主题策略	smn:topic:updateAttribute	人员管理中修改通知订阅
主题下创建订阅	smn:topic:subscribe	人员管理中添加通知订阅
查询指定主题的订阅列表	smn:topic:listSubscriptionsByTopic	故障管理、自动化运维等场景发送通知
查询所有主题的订阅列表	smn:topic:listSubscriptions	故障管理、自动化运维等场景发送通知
删除指定主题下的订阅	smn:topic:deleteSubscription	人员管理中删除通知订阅
发送消息	smn:topic:publish	故障管理、自动化运维等场景发送通知
列举IAM用户	iam:users:listUsersV5	人员管理中同步人员信息
获取IAM用户信息	iam:users:getUserV5	人员管理中同步人员信息
删除服务关联委托	iam:agencies:deleteServiceLinkedAgencyV5	删除IAM中的服务关联委托
查看用户所有的资源列表	rms:resources:list	资源管理同步纳管账号下资源列表
查询参数详情	coc:parameter:*	自动化运维引用参数中心的参数
获取服务器密码对	ecs:serverKeypairs:get	重装、切换操作系统，设置密码对
获取服务器密码对列表	ecs:serverKeypairs:list	重装、切换操作系统，查询密码对列表
批量关闭云服务器	ecs:cloudServers:stop	资源运维中批量关闭云服务器

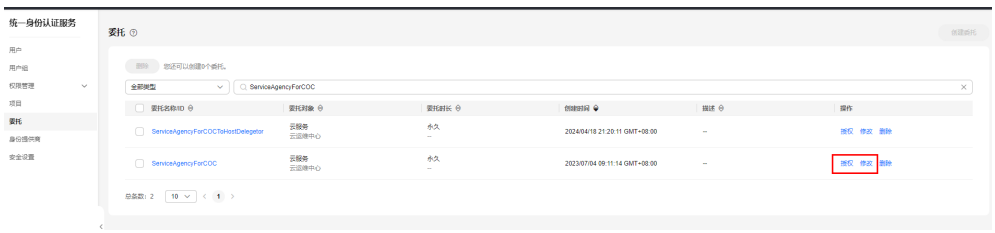
权限	授权项	使用场景
批量重启云服务器	ecs:cloudServers:reboot	资源运维中批量重启云服务器
批量启动云服务器	ecs:cloudServers:start	资源运维中批量启动云服务器
切换弹性云服务器操作系统	ecs:cloudServers:changeOS	资源运维中批量切换云服务器的操作系统
重装弹性云服务器操作系统	ecs:cloudServers:rebuild	资源运维中批量重装云服务器的操作系统
获取云服务器信息	ecs:servers:get	资源运维中执行批量操作时获取云服务信息
列出组织中的账号	organizations:accounts:list	跨账号场景下，查询当前组织下的账号
列出此组织中指定为委托管理员的帐号	organizations:delegatedAdministrators:list	跨账号场景下，查询当前组织下的委托管理员账号
查询所属组织信息	organizations:organizations:get	跨账号场景下，查询当前组织信息
列举组织单元	organizations:ous:list	跨账号场景下，查询当前组织单元
列出组织的可信服务列表	organizations:trustedServices:list	跨账号场景下，查询当前组织已开通的可信服务列表
列出组织的根	organizations:roots:list	跨账号场景下，查询当前组织的root

修改或删除委托权限

若开通COC后，识别到存在委托权限过大或权限不足的情况，可以前往**统一身份认证服务**中修改委托策略。

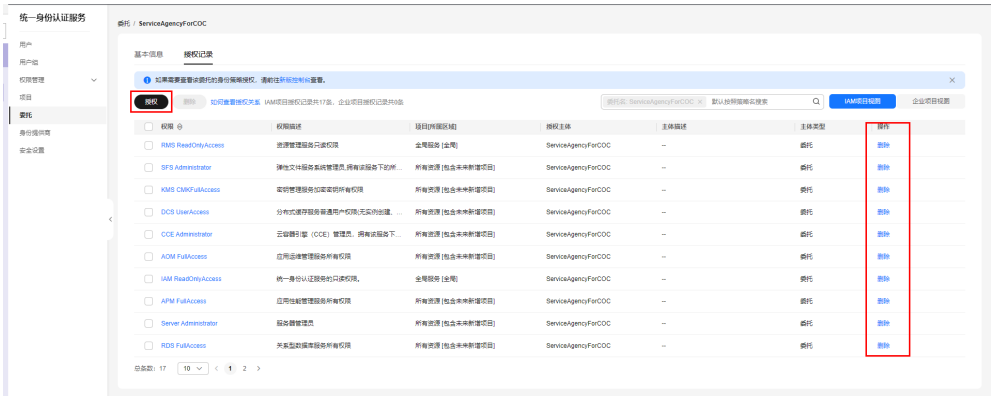
如果需要修改委托的权限、持续时间、描述等，可以在委托列表中，单击委托右侧的“修改”，修改委托。

图 2-2 委托列表



可在授权记录页面中，对该委托进行授权或删除已授权的权限。

图 2-3 授权记录



说明

- 云服务委托支持修改云服务、持续时间、描述、权限，委托名称、类型不支持修改。
- 修改云服务委托权限后可能会影响该云服务部分功能的使用，请谨慎操作。
- 需要了解更多委托相关信息，请访问**统一身份认证服务**进行了解。

3 应用资源建模

本章节介绍在“应用资源管理”页面，如何通过COC快速管理您的资源和应用，包括同步资源、创建应用并建模、执行UniAgent操作等。主要操作如下：

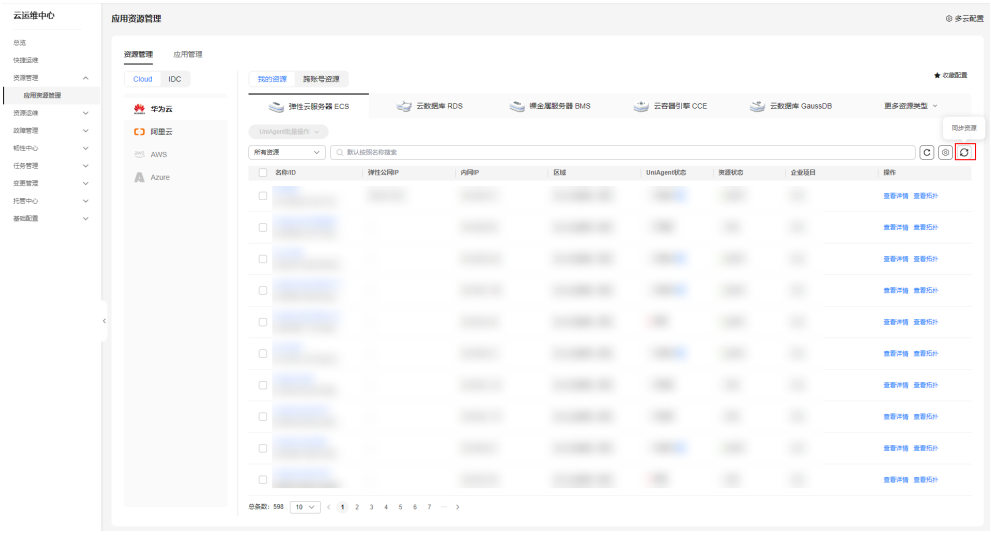
1. **同步资源**：获取当前用户所属的所有Region下资源数据并同步至COC。
2. **创建应用并建模**：通过应用资源建模，按业务逻辑单元便捷地进行资源管理。
3. **执行Agent操作**：给对应机器资源执行UniAgent的安装、升级和卸载操作。

同步资源

步骤1 登录COC。

步骤2 在左侧导航栏选择“**资源管理 > 应用资源管理**”，进入“应用资源管理”页面，选择“**资源管理**”标签，单击 按钮同步资源。

图 3-1 同步资源

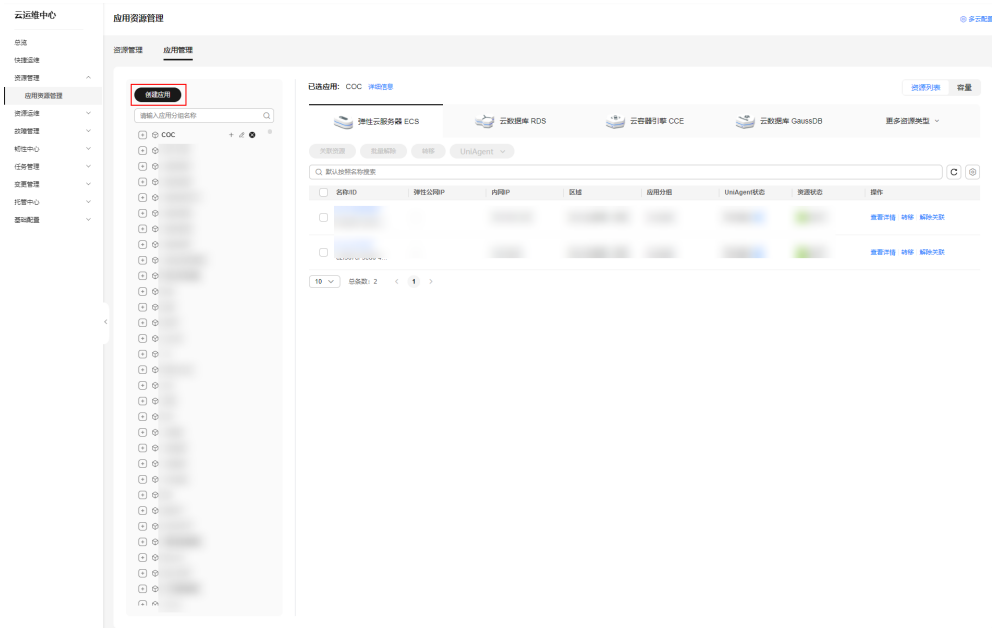


----结束

创建应用并建模

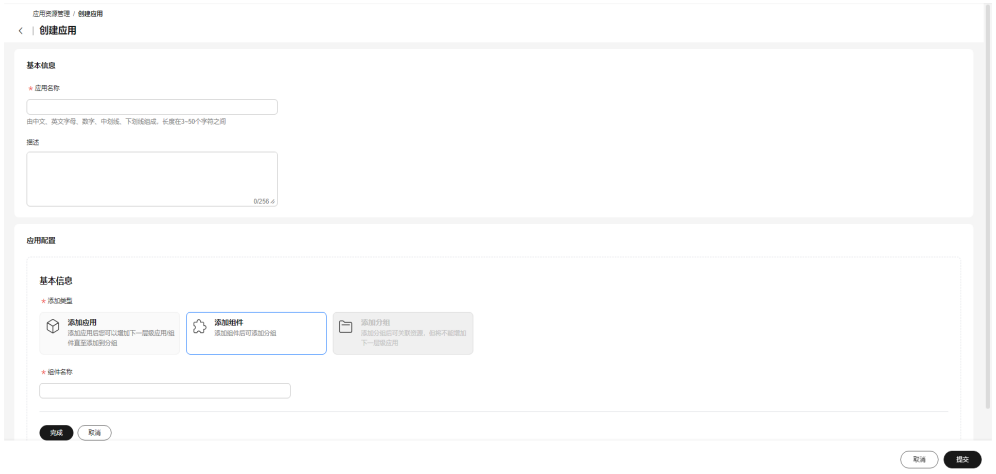
步骤1 在左侧导航栏选择“**资源管理 > 应用资源管理**”，进入“应用资源管理”页面，选择“**应用管理**”页签，单击“**创建应用**”。

图 3-2 创建应用



步骤2 进入“创建应用”页面，填写完整信息后，单击“**提交**”。

图 3-3 填写信息，创建应用

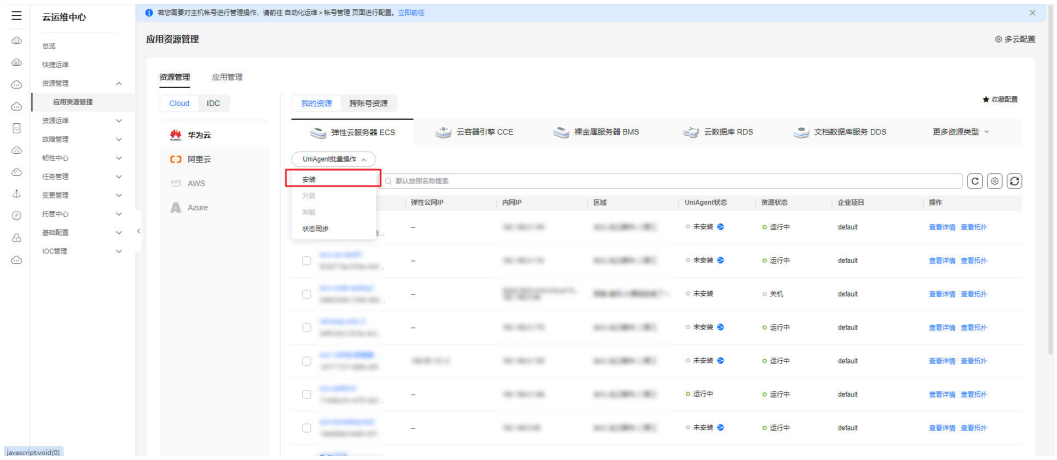


----结束

执行 UniAgent 操作

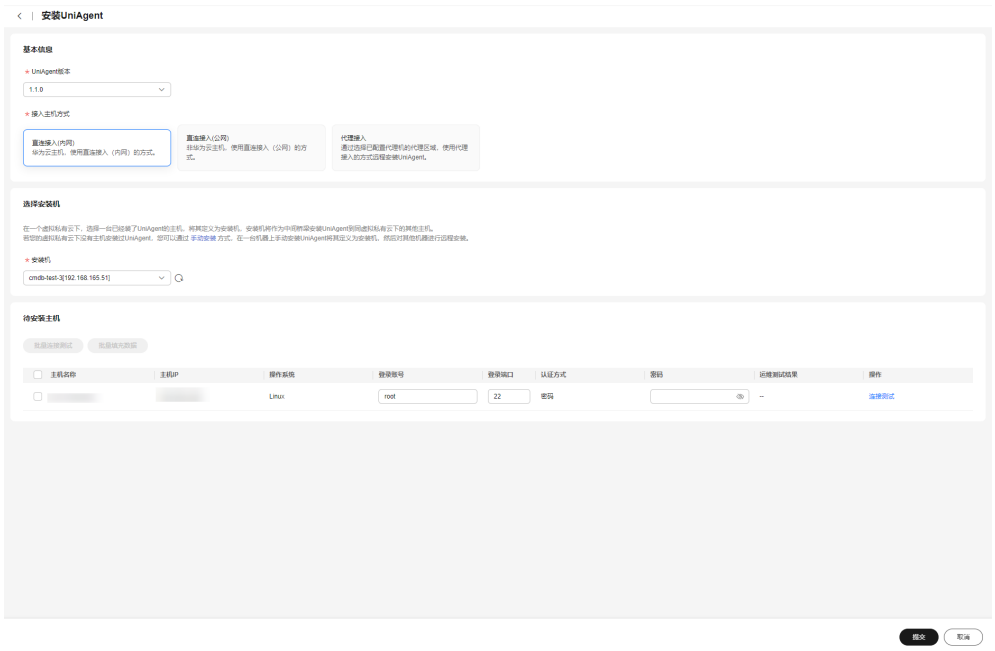
步骤1 在左侧导航栏选择“**资源管理 > 应用资源管理**”，进入“应用资源管理”页面，选择“**资源管理**”页签，勾选对应机器，单击“**UniAgent批量操作 > 安装**”。

图 3-4 安装 UniAgent



步骤2 在跳转的安装UniAgent页面下，填写信息，单击“**提交**”，即触发自动流程，等待操作完成即可。

图 3-5 填写信息



说明

同一个VPC下安装UniAgent时，首台主机需要手动安装UniAgent，并把安装成功后的主机设置成安装机，操作指导详见：**首次安装UniAgent**。

----结束

4 运维基础配置

本章节介绍在COC进行人员管理/排班管理/通知规则配置；上述基础配置将应用至事件单流程、运维事务责任人、各审批场景、消息通知等。

- **人员管理**：人员管理页面的数据作为云运维中心的用户基础数据，供创建待办、定时运维、通知管理、事件中心等多个基础功能模块使用。
- **排班管理**：为云运维中心提供了统一的、多维度、多形式、可自定义的人员管理模式。
- **通知管理**：为用户创建通知实例，通知实例包含通知场景及匹配规则条件等，当满足规则触发条件时向指定人员发送消息，实现了自动通知的功能。

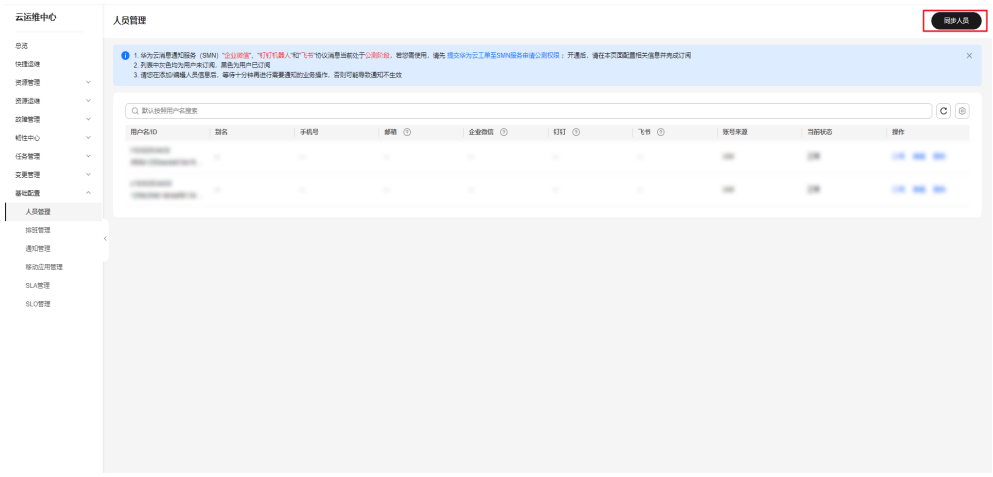
人员管理

人员管理为云运维中心提供了统一的人员数据管理。您可以在人员管理页面管理当前租户下的用户，人员管理中的用户从 IAM 同步，人员管理页面的数据作为云运维中心的用户基础数据，供创建待办、定时运维、通知管理、事件中心等多个基础功能模块使用。更多人员管理功能描述及操作步骤详情请见：**COC人员管理**。

步骤1 登录**COC**。

步骤2 在左侧导航栏选择“**基础配置** > **人员管理**”，进入“人员管理”页面，单击页面右上角“**同步人员**”。

图 4-1 人员管理



----结束

排班管理

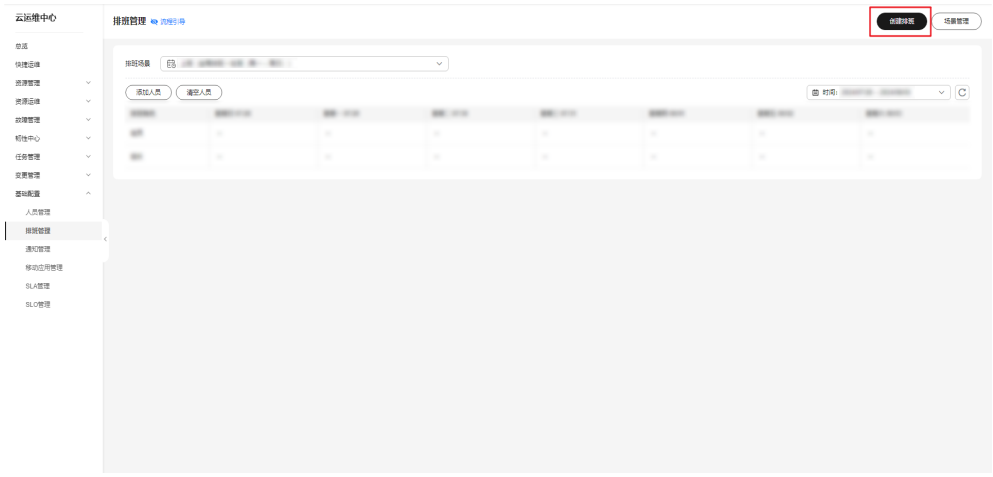
排班管理为云运维中心提供了统一的、多维度、多形式、可自定义的人员管理模式。您可以在排班管理页面创建排班场景、排班角色，并将“人员管理”中的人员添加到排班场景、排班角色中完成排班的设置。

步骤1 登录COC。

步骤2 在左侧导航栏选择“**基础配置 > 排班管理**”，进入“排班管理”页面。

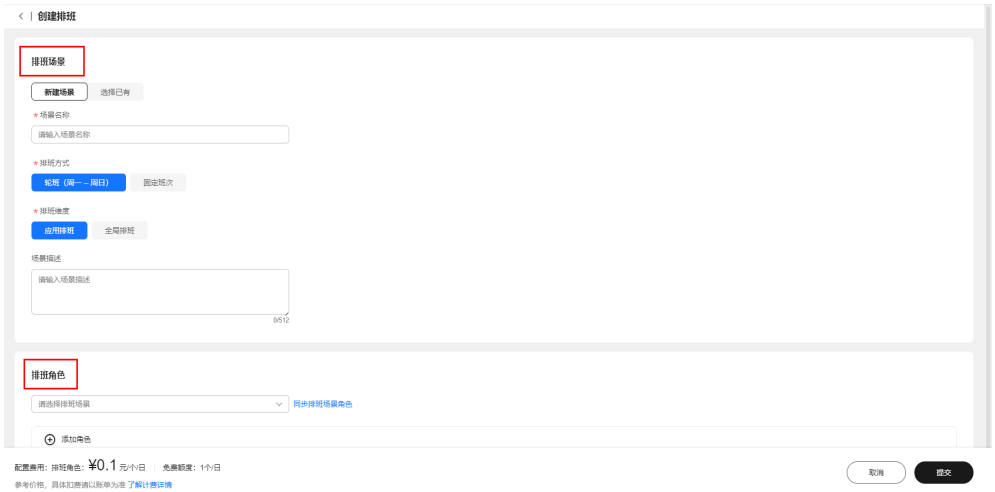
步骤3 在排班管理页面，单击“**创建排班**”。

图 4-2 创建排班



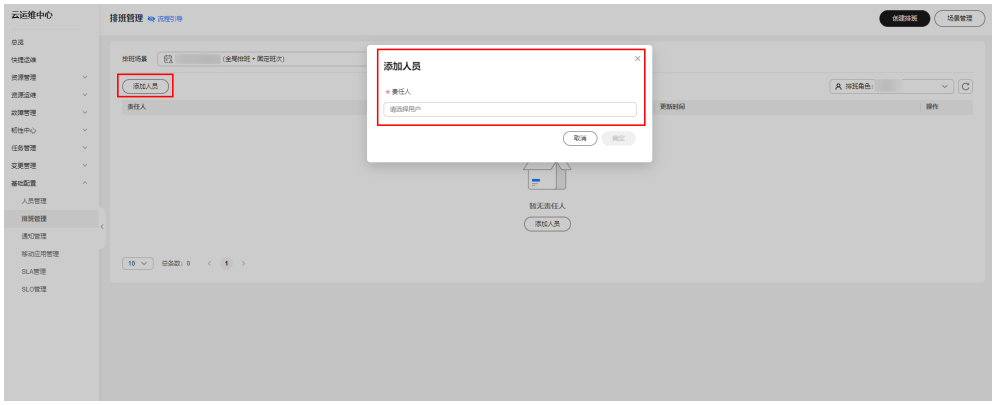
步骤4 新增或选择已有的排班场景和排班角色。

图 4-3 排班场景和排班角色



步骤5 返回排班管理首页，选择上一步创建的排班，单击“**添加人员**”配置排班人员。

图 4-4 添加人员



----结束

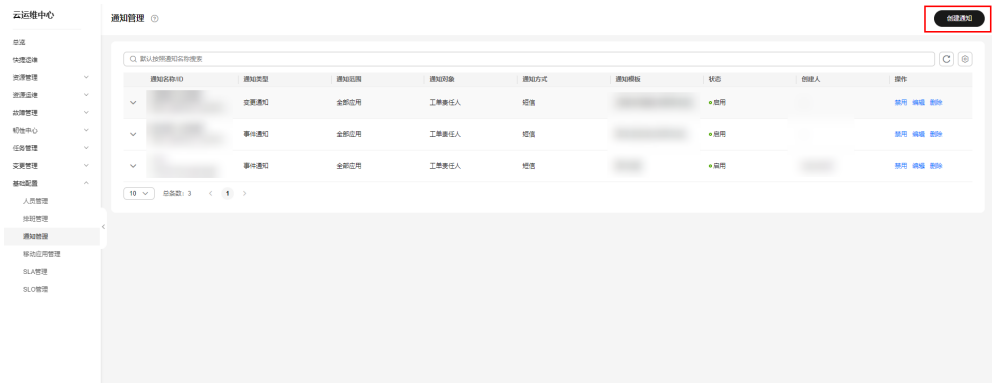
通知管理

通知管理为用户创建通知实例，通知实例包含通知场景及匹配规则条件等，当出现一个运维类工单时，通知模块会启动场景匹配和规则匹配，解析出需要通知的人员、内容和发送通知的渠道，进行发送通知信息，实现了自动通知的功能。

步骤1 登录COC。

步骤2 在左侧导航栏选择“**基础配置** > **通知管理**”，进入“通知管理”页面，单击页面右上角的“**创建通知**”，进入“创建通知”页面。

图 4-5 创建通知



步骤3 填写创建通知的配置信息，填写完成后单击“**确定**”，创建通知的名词解释、通知规则的其他场景操作请见：**COC通知管理**。

----结束

5 跨账号管理

5.1 跨账号管理概述

云运维中心服务具备安全可靠的跨账号数据汇聚和资源运维能力，如果您的账号由组织管理，您可以在云运维中心对组织内所有成员账号进行统一的资源管理、自动化运维以及运维态势感知，而无需逐个登录到成员账号。

通过COC对组织成员账号进行跨账号管理需要执行以下操作（以A账号管理B账号为例）：

1. 如果A账号是组织管理员，则跳过此步骤。如果A账号不是组织管理员，则由组织管理员将A账号添加为委托管理员，相关操作请参见**添加委托管理员**。

   说明

   管理员可以添加或者取消成员的委托管理员权限，组织成员架构变动时需要1-2分钟后刷新页面才能生效。

2. 由组织管理员或委托管理员邀请B账号加入组织，相关操作请参见**邀请账号加入组织**。
3. B账号加入组织后，登录A账号在COC服务“运维态势感知”、”资源管理”、”作业管理”页面可对B账号进行跨账号运维管理。

有关组织的详细说明请参见**《组织用户指南》**。

说明

为了请求B账号下的数据资产信息，COC会自动在B账号中创建服务关联委托：

- 该委托是云服务委托，“委托权限”为“COCAssumeServiceLinkedAgencyPolicy”，“委托名称”为“ServiceLinkedAgencyForCOC”。
- 删除B账号时，COC会自动删除B账号内的服务关联委托。

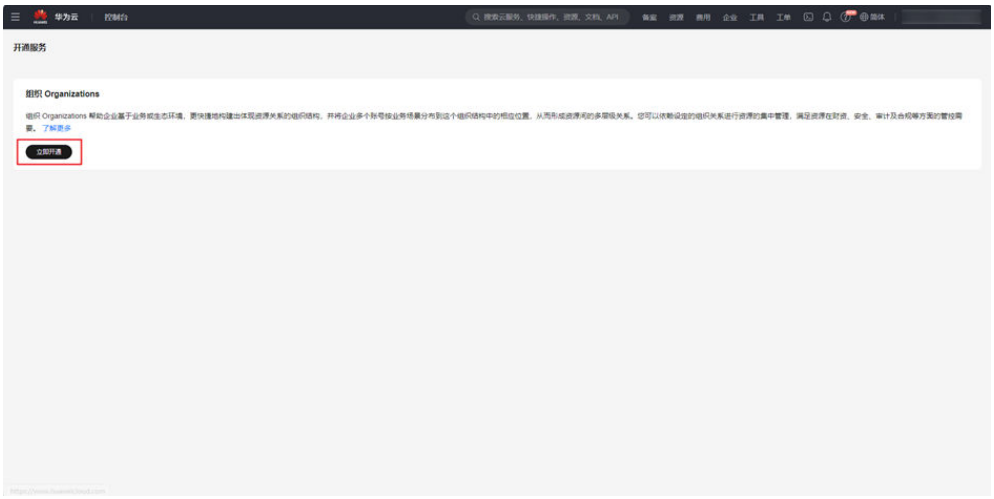
5.2 开启跨账号管理

开启跨账号管理功能后，组织/委托管理员在云运维中心对组织内所有成员账号进行统一的资源管理、自动化运维以及运维态势感知，而无需逐个登录到成员账号，本章介绍如何开启跨账号管理功能。

前提条件

- 开通组织服务，请参见**开通组织服务**。

图 5-1 开通组织服务

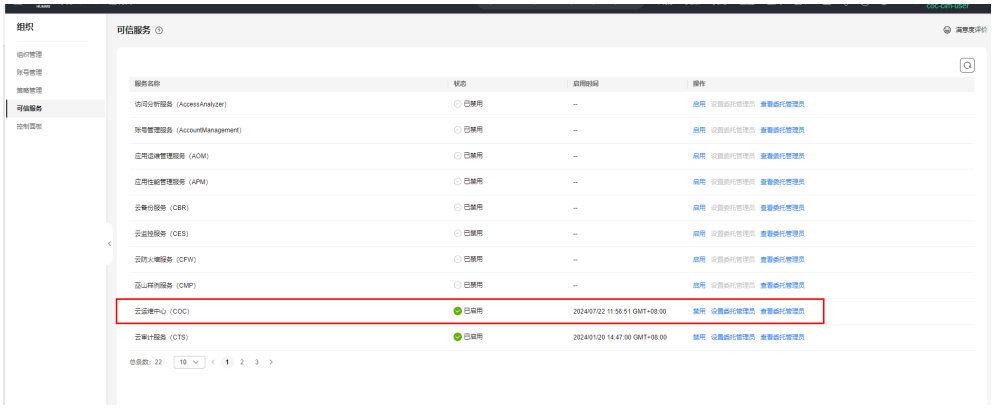


说明

- 只有企业中心的企业主账号的权限才能创建组织，非企业账号不支持使用Organizations。
- 企业中心创建组织后，需要在Organizations重新授权，即可访问组织所有功能。
- 组织开通之后，跳转到组织管理页面，按照以下步骤创建组织：
  1. 组织管理员需要创建一个组织，一个账号只能有一个组织；
  2. 成员账号看不到除了控制面板外的东西；
  3. 成员账号也必须是企业级账号；

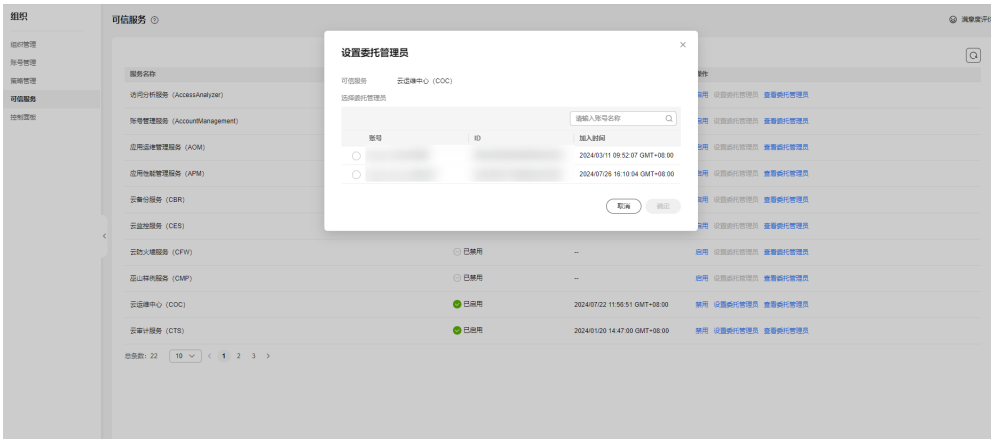
- 授权COC为可信服务，请参见**授权为可信服务**。

图 5-2 授权为可信服务



- 该账号为管理员或者委托管理员，如果不是请参照**添加委托管理员**章节的内容。

图 5-3 添加委托管理员



使用约束

邀请成员账号加入组织之后，管理员或服务委托管理员可以在云运维中心查看和管理该组织下成员账号的数据与资源，支持的跨账号管理的功能有运维态势感知、资源管理和作业管理。

6 入门实践

当您完成了账号与授权、应用资源建模、运维基础配置等基本操作后，可以根据自身的业务需求使用云运维中心提供的一系列常用实践。

表 6-1 常用最佳实践

实践	描述
标准化故障管理	建立标准化的事件流程，实现规范性处理
全旅程混沌工程方案	对系统进行混沌演练，通过演练结果检验和提升系统的可用性
一站式资源运维	检查主机操作系统（OS）补丁的合规性情况，避免主机因为OS补丁缺失产生漏洞，导致业务受损

7 修订记录

日期	修订记录
2023-11-30	第一次发布
2024-06-06	随服务版本刷新资料内容