IAM 身份中心

最佳实践

文档版本 01

发布日期 2025-07-08

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 通过 IAM 身份中心对企业多账号的身份和权限进行管理

方案概述

本文主要介绍管理账号A在IAM身份中心中创建一个用户Alice，并将其与组织下的一个成员账号（a__abc）进行关联，且该账号已关联权限集PolicySet（已配置ECS管理权限），实现多账号的身份和权限的管理。

前提条件

IAM身份中心依赖组织云服务定义的组织来获取成员账号信息。在使用IAM身份中心之前，必须先**开通组织云服务并创建组织**，以组织管理账号登录并使用IAM身份中心。

步骤一：创建用户

步骤1 以组织管理账号登录**华为云控制台**。

步骤2 单击页面左上角的 ☰，选择“管理与监管 > IAM身份中心”，进入“IAM身份中心”页面。

步骤3 单击左侧导航栏的“用户管理”，进入“用户管理”页面。

步骤4 单击页面右上方的“创建用户”，进入创建用户页面。

图 1-1 创建用户

步骤5 配置用户信息，配置完成后，单击页面右下角的“下一步”。

其中基本信息为必填项，联系方式、工作相关信息和地址信息为非必填项，可根据需要填写。

图 1-2 用户信息

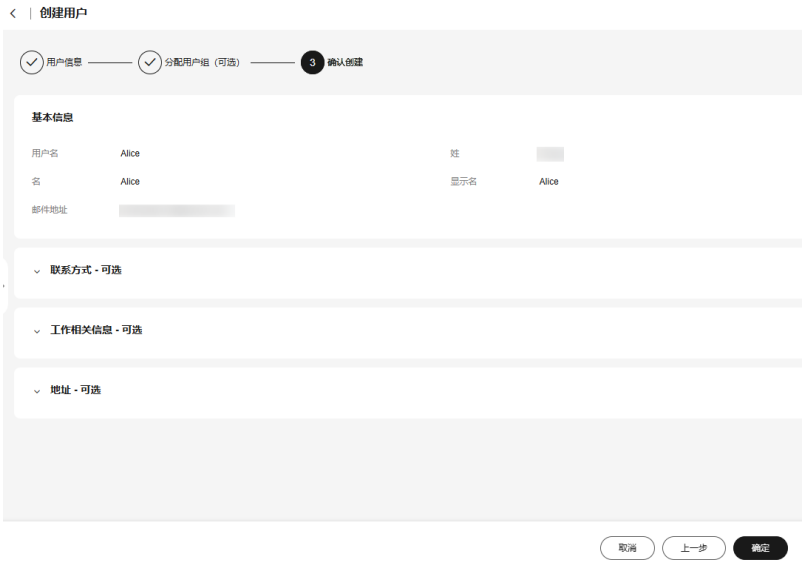
表 1-1 基本信息

参数	描述
用户名	IAM身份中心用户名称。此处以Alice为例。 自定义，不可与其他IAM身份中心用户名重复。
密码	选择密码的生成方式。 ● 向用户发送一封包含密码设置说明的邮件：系统通过邮件发送密码设置说明给用户，用户根据邮件说明设置密码。 ● 生成随机的一次性密码：管理员创建用户成功后，系统会在创建成功的界面，显示自动生成的一次性密码信息。管理员将这些信息复制并发送给用户，用户使用一次性密码通过门户URL登录时系统会提示用户重新设置密码，密码设置成功后才能登录控制台，后续均使用自行设置的密码登录。 **注意** 系统生成的一次性密码信息页面关闭后将无法再次显示，需**重置密码**才能再次获取。
邮件地址	用户的邮件地址。 自定义，不可与其他用户重复。可用于用户的身份验证、重置密码等。
确认邮件地址	再次输入邮件地址进行确认，两次输入的邮件地址必须一致。
姓	用户的姓氏。
名	用户的名字。
显示名	IAM身份中心用户的显示名称。 自定义，可与其他IAM身份中心用户显示名重复，一般为用户的真实姓名。

步骤6 进入“确认创建”页面，确认配置无误后，单击页面右下角的“确定”，用户创建完成，用户列表中显示新创建的用户。

- 如果“5 > 密码”选择了“向用户发送一封包含密码设置说明的邮件”，界面会跳转至用户列表，用户列表中显示新创建的用户。
- 如果“5 > 密码”选择了“生成随机的一次性密码”，系统会弹出一次性密码的详细信息页面，您可以将这些信息复制并发送给用户，用户使用用户名和一次性密码通过门户URL进行登录。

图 1-3 确认创建



----结束

步骤二：创建用户组

步骤1 以组织管理账号登录华为云控制台。

步骤2 单击页面左上角的 ☰，选择“管理与监管 > IAM身份中心”，进入“IAM身份中心”页面。

步骤3 单击左侧导航栏的“用户组管理”，进入“用户组管理”页面。

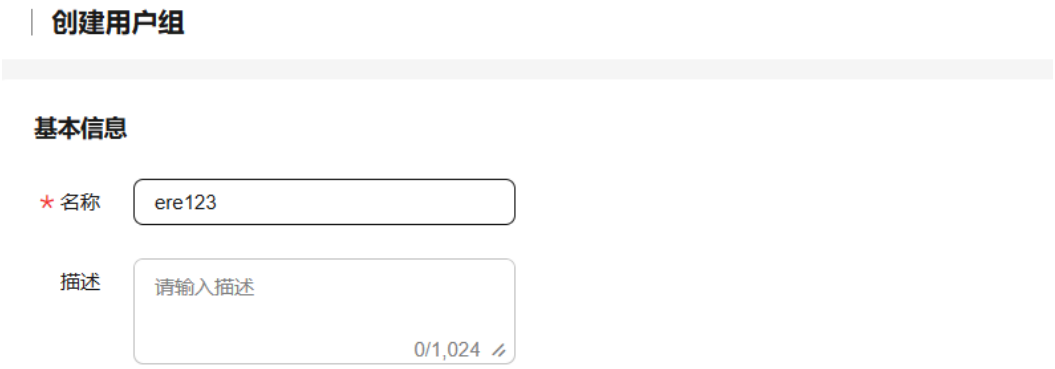
步骤4 单击页面右上方的“创建组”，进入创建用户组页面。

图 1-4 创建用户组

步骤5 在“创建用户组”界面，输入“名称”和“描述”，名称以“ere123”为例。

用户组名称不可与其他IAM身份中心用户组名称重复。

图 1-5 创建用户组



步骤6 （可选）选择需要添加至用户组中的用户。

图 1-6 添加用户

步骤7 单击“确定”，用户组创建完成，创建成功的用户组“ere123”将会展示在用户组列表中。

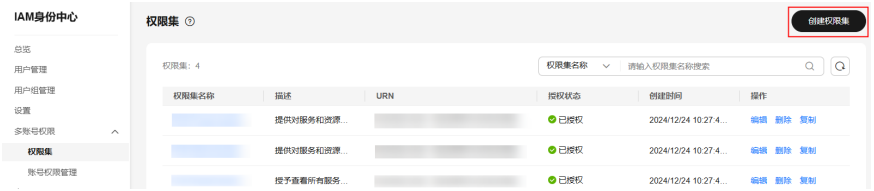
----结束

步骤三：创建权限集

步骤1 组织管理账号在左侧导航栏中，选择“多账号权限 > 权限集”，进入“权限集”页面。

步骤2 单击页面右上方的“创建权限集”，进入创建权限集页面。

图 1-7 创建权限集



步骤3 在“基本信息”页签中配置权限集的基本信息，配置完成后，单击“下一步”。

图 1-8 配置基本信息

表 1-2 权限集基本信息

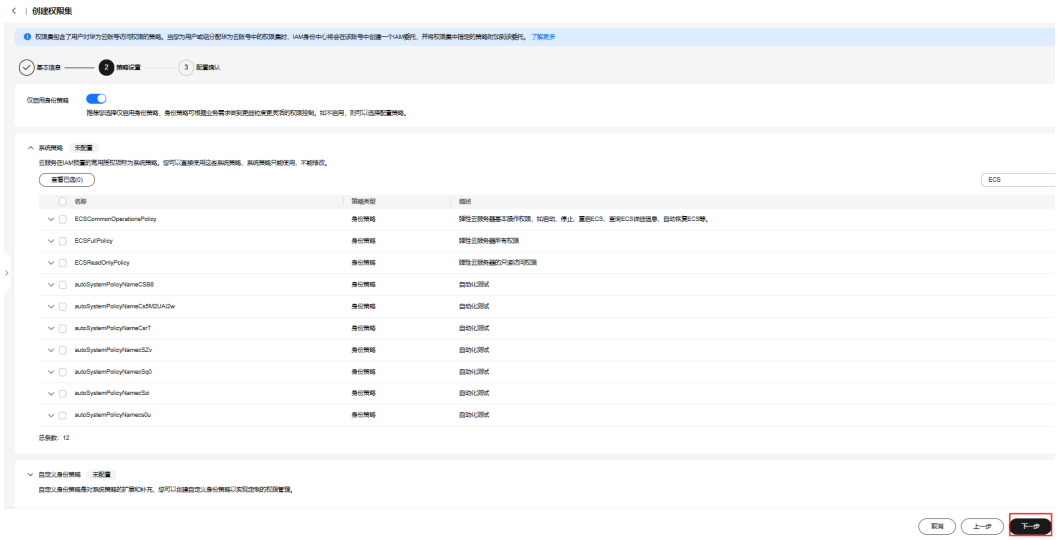
参数	描述
名称	权限集的名称。此处以PolicySet为例。 自定义，不可与其他权限集名称重复。
会话持续时间	使用此权限集授权的IAM身份中心用户登录控制台后的会话持续时间。 登录时间超出设置的会话持续时间后，会话将过期，用户将自动登出，如需继续访问，需重新登录。
初始访问页面	IAM身份中心用户通过门户URL登录控制台后访问的初始页面。 例如您可以输入IAM控制台的URL，登录后单击“访问控制台”，显示初始页面。
描述	权限集的描述信息。

步骤4 进入“策略设置”页签，配置权限集的系统策略、自定义身份策略和自定义策略，单击“下一步”。

您可以选择仅启用身份策略，启用后系统策略列表中将仅显示身份策略，自定义策略配置框也将隐藏。若云服务没有身份策略，您可以选择关闭仅启用身份策略，关闭后，对于云服务的某些功能，可以选择身份策略加策略的方式来生效。

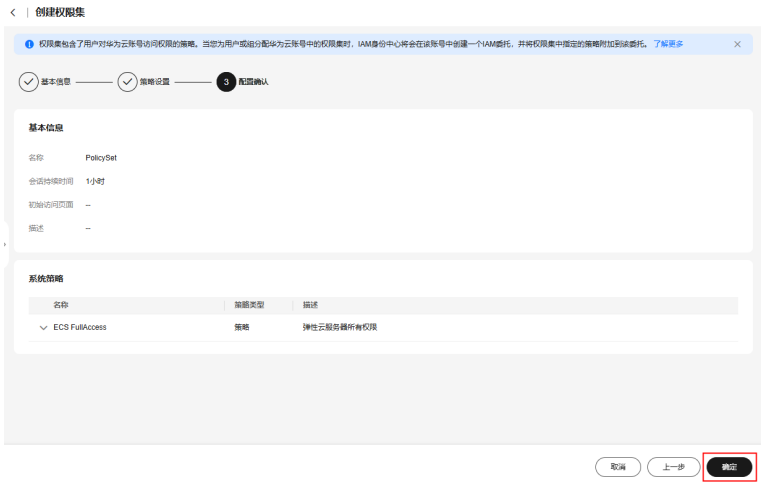
- 系统策略：在列表中直接选择云服务在IAM预置的系统策略，系统策略分为策略和身份策略两种类型。
- 自定义身份策略：如果系统身份策略无法满足您的授权要求，您可以创建自定义身份策略，对系统身份策略进行扩展和补充。当前支持通过可视化视图和JSON视图两种方式创建自定义身份策略。
- 自定义策略：如果系统策略无法满足您的授权要求，您可以创建自定义策略，对系统策略进行扩展和补充。当前仅支持通过JSON视图创建自定义策略。

图 1-9 策略设置



步骤5 进入“配置确认”页面，确认配置无误后，单击页面右下角的“确定”，权限集创建完成。

图 1-10 配置确认



说明

新创建权限集的授权状态为“未授权”，权限集关联账号后授权状态将变为“已授权”。

----结束

步骤四：账号关联用户和权限集

步骤1 组织管理账号在左侧导航栏中，选择“多账号权限 > 账号权限管理”，进入“账号权限管理”页面。

账号权限管理列表默认以组织结构树的形式显示，在列表左上方单击  ，列表将只显示组织下的所有成员账号，而不显示组织结构树。

图 1-11 账号列表显示方式切换

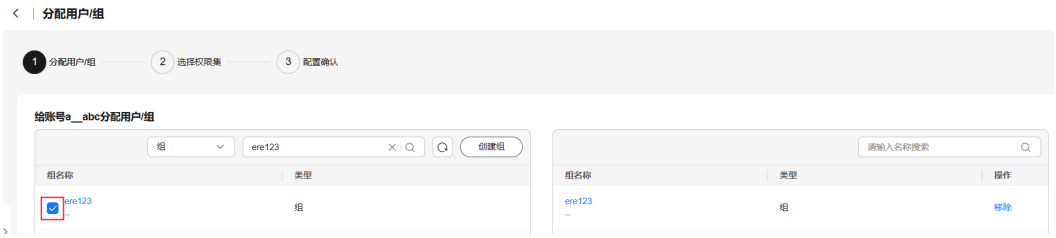
步骤2 在账号列表中勾选账号a_abc，单击左上方的“关联用户或组”。

您也可以在账号列表中单击操作列的“关联用户或组”。

图 1-12 选择账号

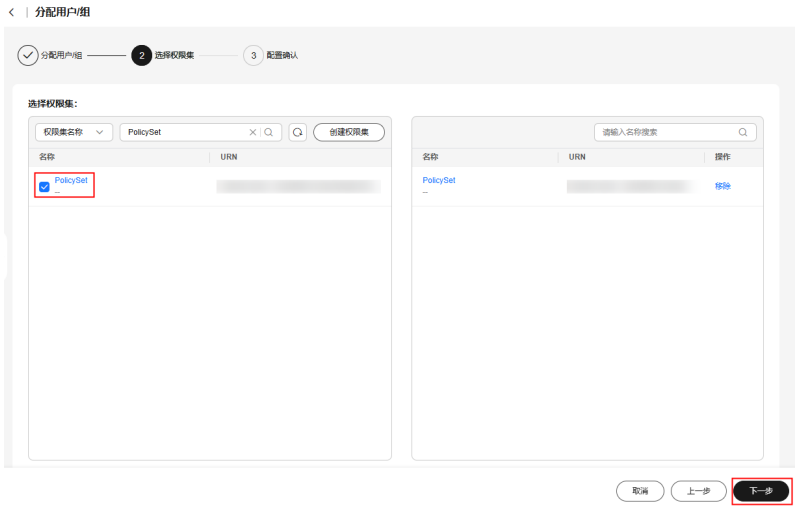
步骤3 进入“分配用户/组”页面，在列表中勾选需要关联的用户/组，以关联组为例，单击“下一步”。

图 1-13 分配用户/组



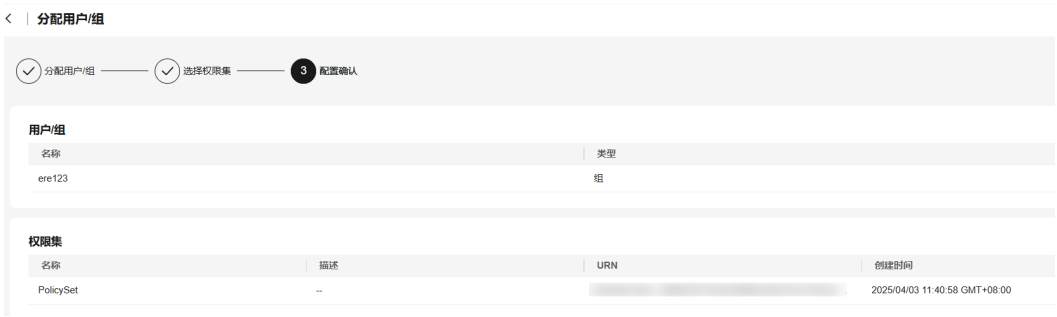
步骤4 进入“选择权限集”页面，在权限集列表中勾选权限集PolicySet，单击“下一步”。

图 1-14 分配权限集



步骤5 进入“配置确认”页面，确认配置无误后，单击页面右下角的“确定”，为账号关联组和权限集完成。

图 1-15 配置确认



----结束

步骤五：用户登录并访问资源

步骤1 组织管理账号单击左侧导航栏的“总览”，在总览页面可获取用户门户URL，并将该URL传递给用户Alice。

管理员在创建用户时，在向用户发送的密码设置邮件中或者生成的一次性密码页面中也可以获取用户门户URL。

图 1-16 获取用户门户 URL

步骤2 用户Alice使用浏览器打开用户门户URL，输入用户名Alice并单击“下一步”。

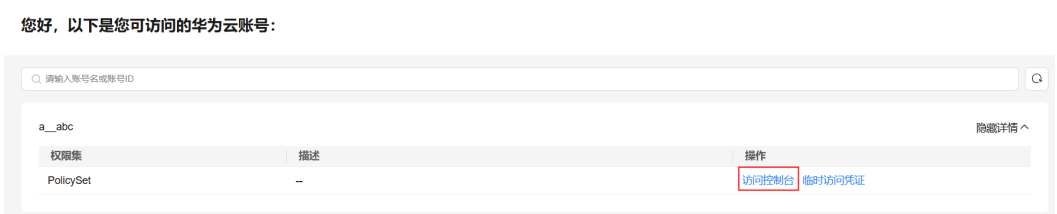
用于登录的密码在**创建用户**时获取。如果忘记密码或需要修改密码，管理员可以使用**重置密码**功能，重新向用户发送密码设置邮件或生成一次性密码。

图 1-17 用户登录

步骤3 输入登录密码，单击“登录”。

步骤4 单击操作列的“访问控制台”，即可访问此账号下对应权限集PolicySet控制的ECS资源。

图 1-18 访问资源



----结束

相关链接

IAM身份中心与其他外部身份源对接指南请参考：

- **IAM身份中心如何对接微软Entra ID**
- **IAM身份中心如何对接阿里云IDaaS**
- **IAM身份中心如何对接Okta**
- **IAM身份中心如何对接Google Workspace**
- **IAM身份中心如何与华为云OneAccess对接**
- **IAM身份中心与ADFS对接操作指导**
- **华为云IAM身份中心如何与CyberArk对接**