IAM 身份中心

快速入门

文档版本 01

发布日期 2023-06-30

华为技术有限公司

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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

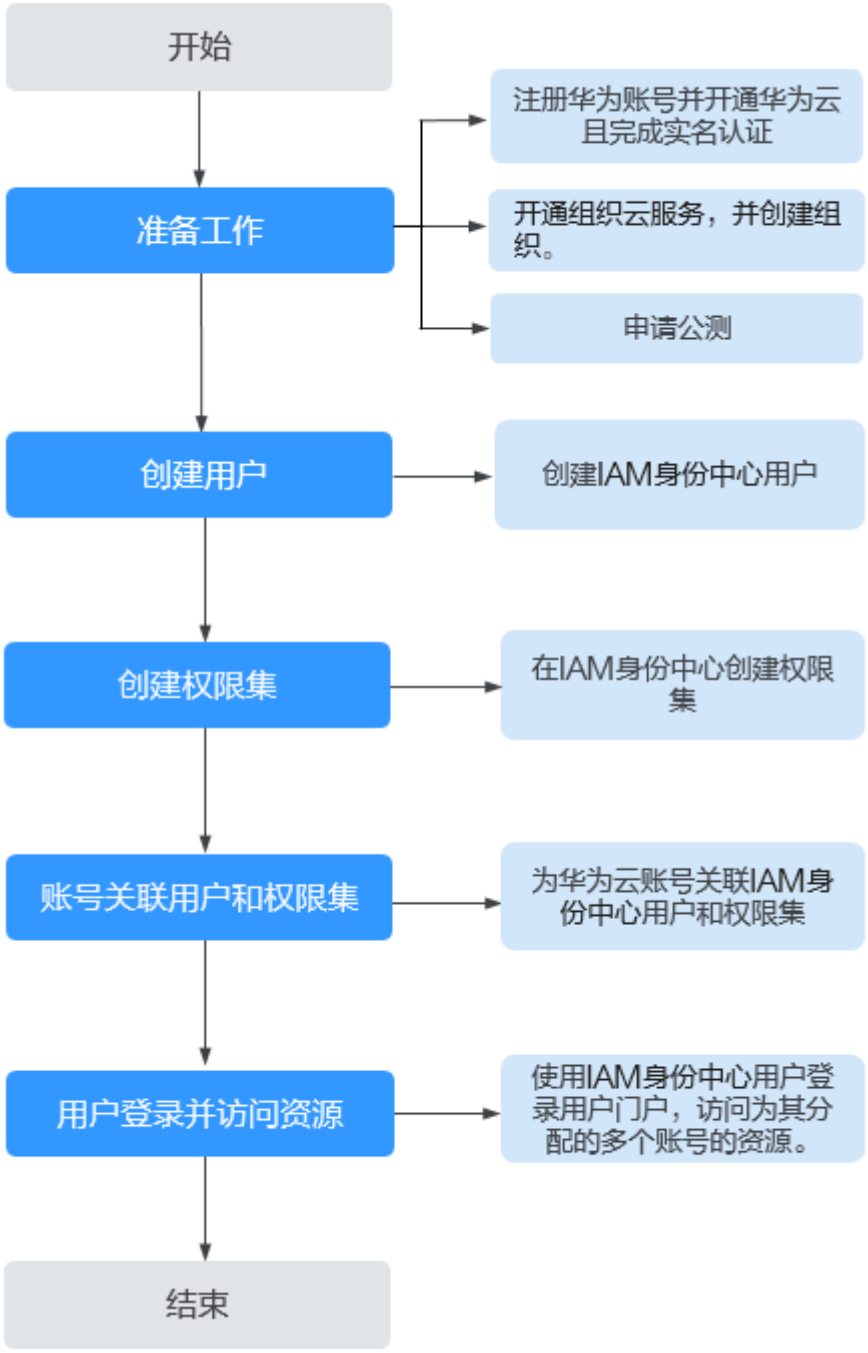
目 录

1 入门指引

如果您首次使用IAM身份中心服务，建议参考本章节。它可以帮助您快速使用IAM身份中心的主要功能。

IAM身份中心入门流程图如下：

图 1-1 IAM 身份中心快速入门流程图



2 准备工作

在使用IAM身份中心之前，您需要完成本文中的准备工作：

- **注册华为账号并开通华为云且完成实名认证**
- **开通组织云服务并创建组织**
- **申请公测并开通IAM身份中心**

注册华为账号并开通华为云且完成实名认证

如果您已有一个华为云账号，请跳到下一个任务。如果您还没有华为云账号，请参考以下步骤创建。

1. 打开**华为云官网**，单击页面右上角的“注册”。
2. 根据提示信息完成华为账号注册。
3. 勾选服务条款， 单击“开通”。系统提示开通成功。
   具体请参见：**注册华为账号并开通华为云**。
4. 参考**实名认证**完成企业账号实名认证。

说明

因为IAM身份中心为免费服务，因此无需为账号充值。

开通组织云服务并创建组织

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，所以使用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。

使用组织云服务之前，需要先**开通企业中心功能**，且只能使用企业中心的主账号创建组织，请参考以下步骤执行。

步骤1 进入**企业中心**控制台。

步骤2 单击“免费开通”，进入申请开通企业中心页面。

步骤3 勾选“我已阅读并同意《华为云企业管理服务使用声明》”，并单击“免费开通”。开通后您将自动成为企业主账号，具体请参见：**开通企业中心功能**。

步骤4 进入组织云服务控制台。

步骤5 开通组织云服务。进入开通页，单击“立即开通”。

步骤6 开通组织云服务后，系统会自动创建组织和根组织单元，并将开通服务的账号设置为管理账号。具体请参见：**创建组织**。

步骤7 邀请账号加入组织，具体请参见：**邀请账号加入组织**。

----结束

申请公测并开通 IAM 身份中心

IAM身份中心目前正在公测中，公测期间，您需要申请公测权限，审核通过后方可使用服务。支持企业用户申请免费试用。

1. 登录**华为云控制台**。
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。
3. 单击“立即申请”，进入申请公测页面。
4. 在公测申请页面，根据实际情况设置企业规模、研发人员比例、应用场景、业务当前阶段、业务描述等申请信息。
5. 勾选“同意《公测试用服务协议》”，单击“申请公测”。

   公测申请提交后，5个工作日内审核结果将发送到您的邮箱和手机。
6. 在“资源 > 我的公测”页面中，可以查看所有公测申请以及审批状态。
7. 公测申请审批通过后，在“IAM身份中心”页面单击“立即开通”，开通IAM身份中心服务。

   开通IAM身份中心服务后，系统会自动创建服务实例和身份源，并自动生成用户门户URL。

3 创建用户和权限集

创建用户

当您完成准备工作并开通IAM身份中心服务后，您需要创建IAM身份中心用户。

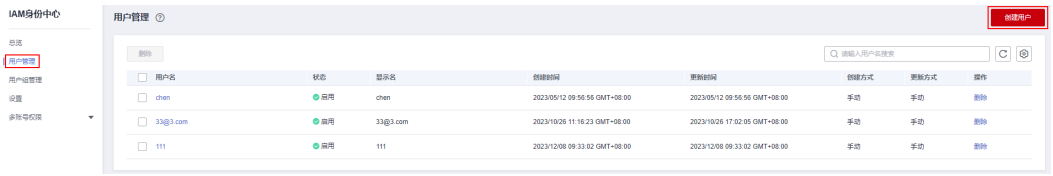
步骤1 登录华为云控制台。

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 3-1 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 3-2 用户信息

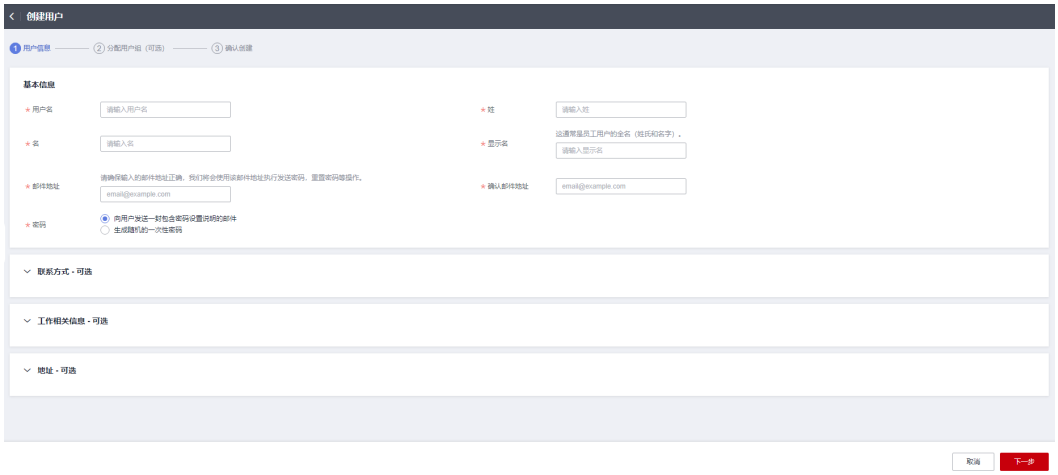
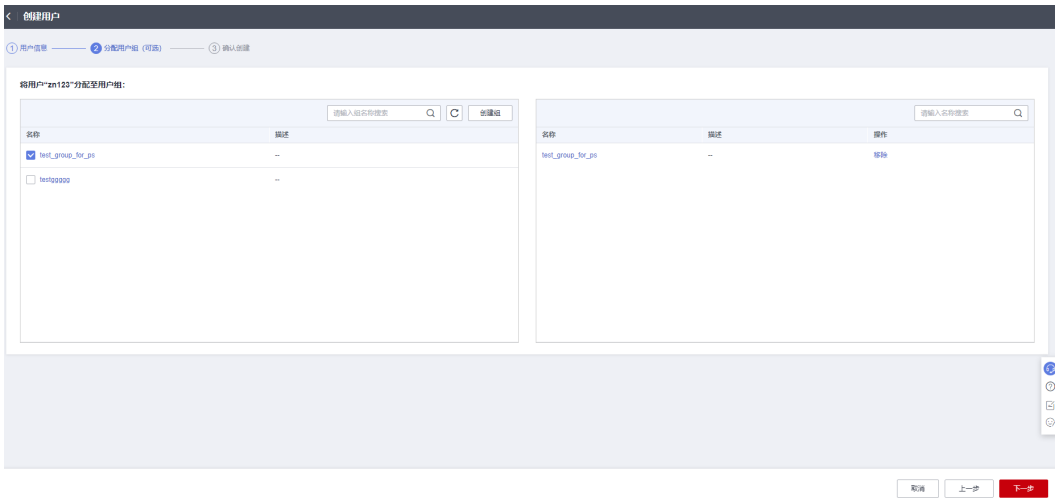


表 3-1 基本信息

参数	描述
用户名	IAM身份中心用户名称。 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 （可选）进入“分配用户组（可选）”页面，勾选要加入的用户组，将用户加入到用户组。加入用户组后，用户将具备用户组的权限。配置完成后，单击页面右下角的“下一步”。

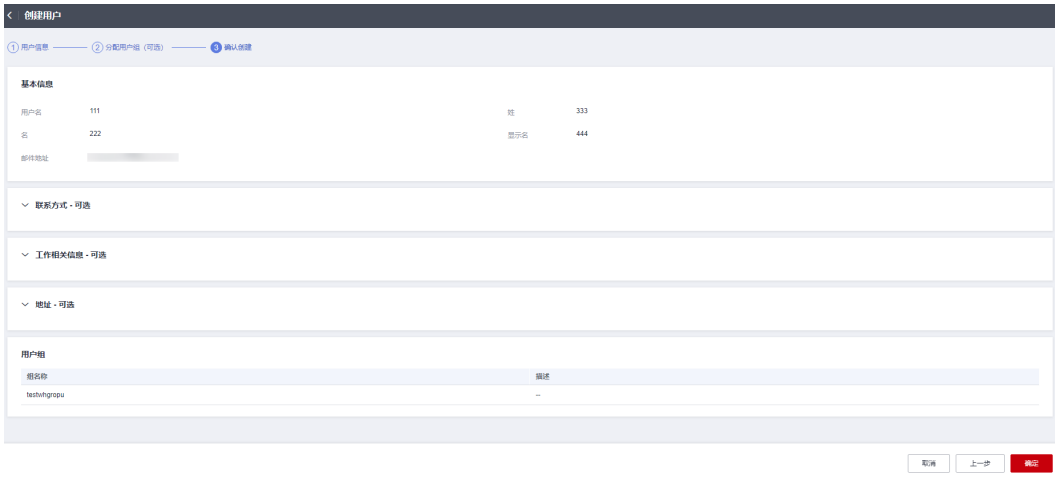
图 3-3 分配用户组（可选）



步骤7 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 3-4 确认创建



----结束

创建权限集

权限集定义了一个或多个IAM策略的集合，IAM身份中心用户可访问资源的具体权限由权限集控制。创建权限集为必须操作，使用IAM身份中心用户登录控制台访问多个账号下的资源时，必须为其关联权限集，否则登录后将无权访问任何资源。

步骤1 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 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4 单击页面右上方的“创建权限集”，进入创建权限集页面。

图 3-5 创建权限集

步骤5 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 3-6 配置基本信息

表 3-2 权限集基本信息

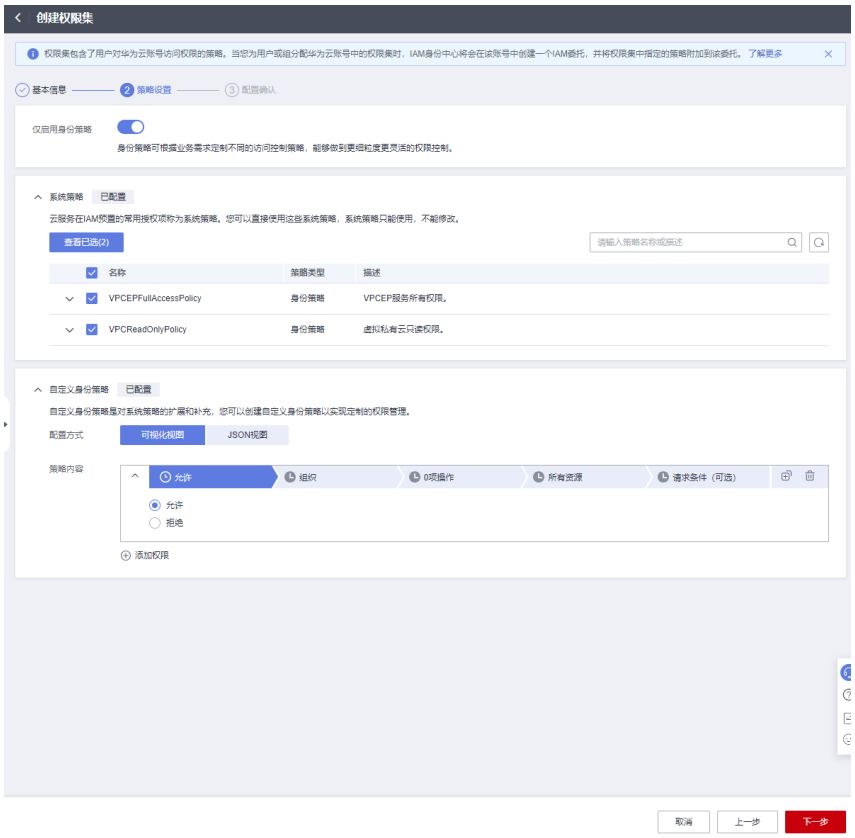
参数	描述
名称	权限集的名称。 自定义，不可与其他权限集名称重复。
会话持续时间	使用此权限集授权的IAM身份中心用户登录控制台后的会话持续时间。 登录时间超出设置的会话持续时间后，会话将过期，用户将自动登出，如需继续访问，需重新登录。
初始访问页面	IAM身份中心用户通过门户URL登录控制台后访问的初始页面。 例如您可以输入IAM控制台的URL，登录后将直接显示IAM控制台页面。
描述	权限集的描述信息。

步骤6 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。

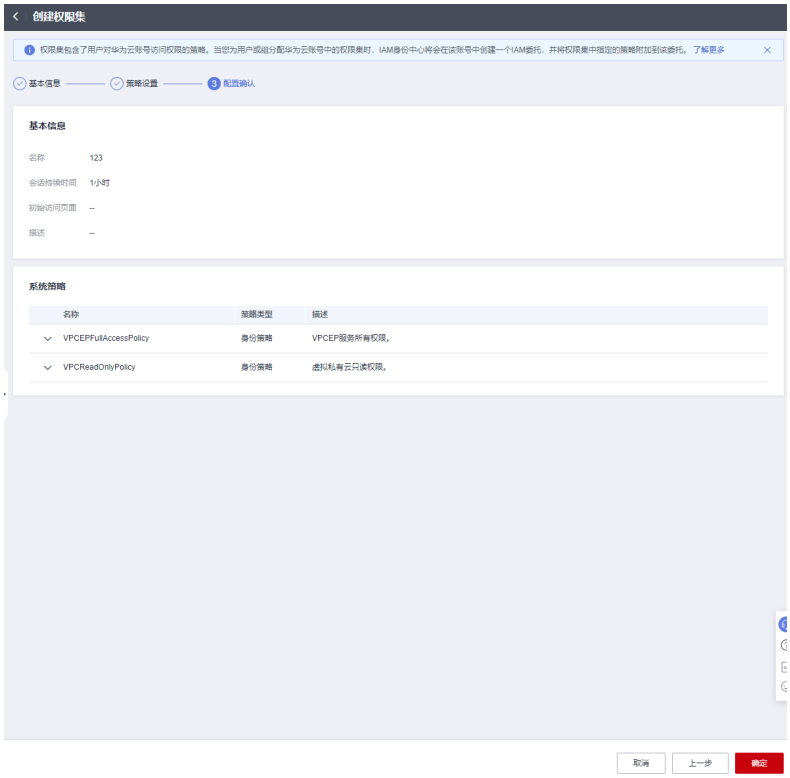
- 系统策略：在列表中直接选择云服务在IAM预置的系统策略，系统策略分为策略和身份策略两种类型。
- 自定义身份策略：如果系统身份策略无法满足您的授权要求，您可以创建自定义身份策略，对系统身份策略进行扩展和补充。当前支持通过可视化视图和JSON视图两种方式创建自定义身份策略。
- 自定义策略：如果系统策略无法满足您的授权要求，您可以创建自定义策略，对系统策略进行扩展和补充。当前仅支持通过JSON视图创建自定义策略。

图 3-7 策略设置



步骤7 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 3-8 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

4 账号关联用户和权限集

当您创建用户/组和权限集完成后，您需要将组织下的一个或多个成员账号关联IAM身份中心用户/组和权限集，这样使用IAM身份中心用户登录后才能访问关联账号下的资源，这些资源通过关联的权限集授予具体访问权限。

操作步骤

步骤1 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 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。

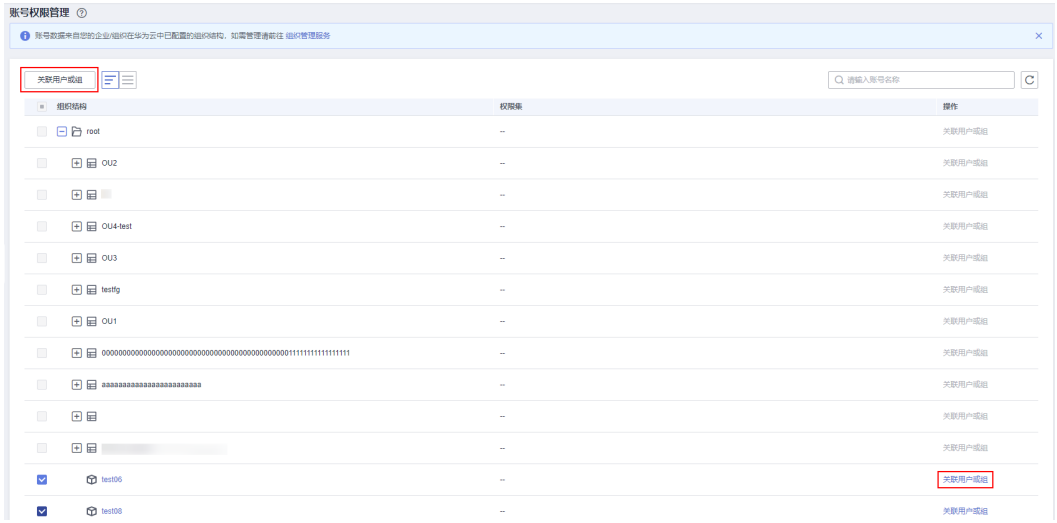
账号权限管理列表默认以组织结构树的形式显示，在列表左上方单击 ☰ ，列表将只显示组织下的所有成员账号，而不显示组织结构树。

图 4-1 账号列表显示方式切换

步骤4 在账号列表中勾选一个或多个账号，单击左上方的“关联用户或组”。

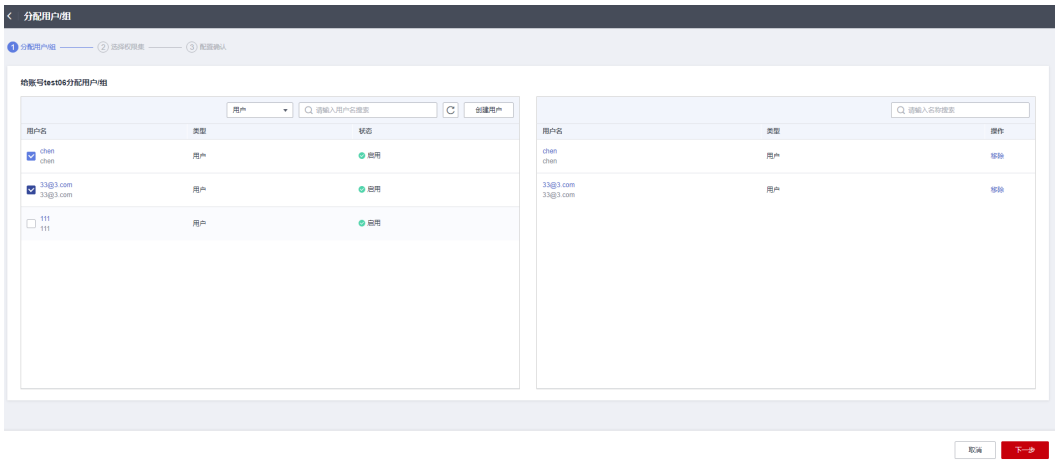
您也可以在账号列表中单击某一账号操作列的“关联用户或组”。

图 4-2 选择账号



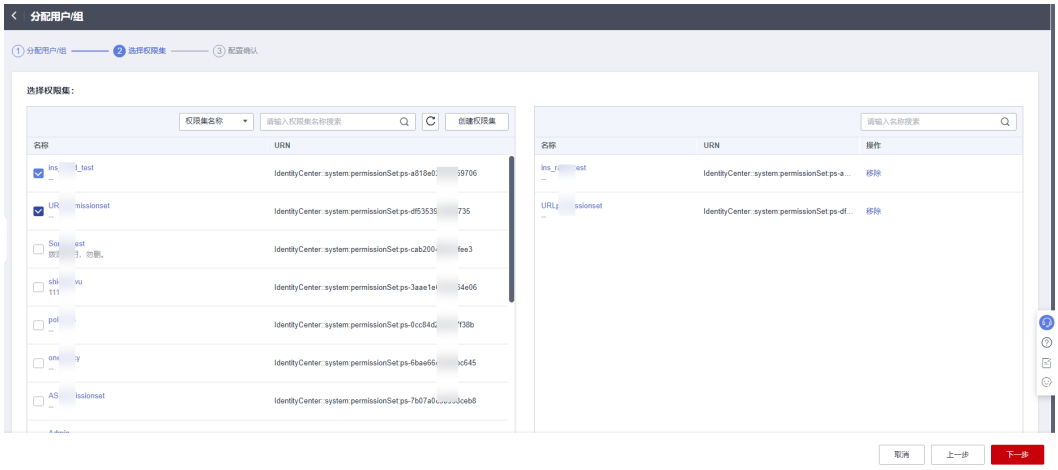
步骤5 进入“分配用户/组”页面，在列表中勾选需要关联的用户/组，单击“下一步”。

图 4-3 分配用户/组



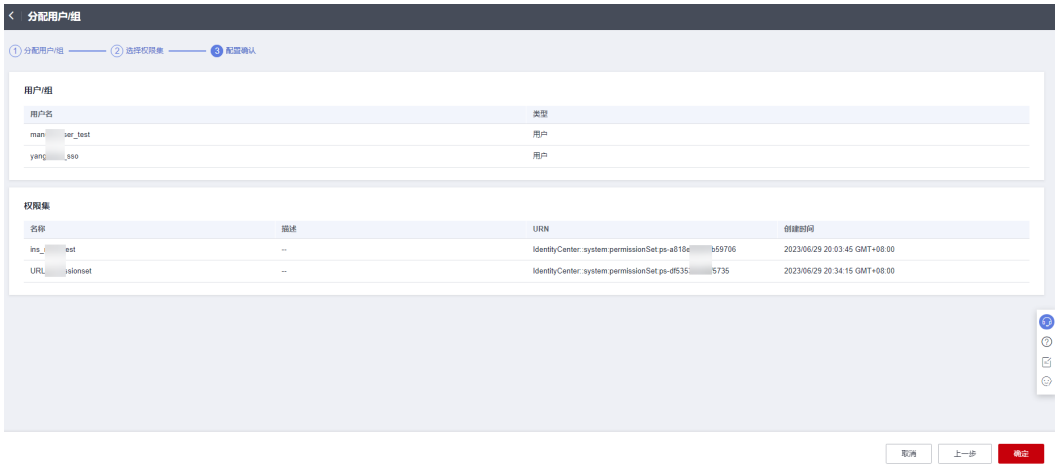
步骤6 进入“选择权限集”页面，在权限集列表中勾选需要关联的权限集，单击“下一步”。

图 4-4 分配权限集



步骤7 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”，为账号关联用户/组和权限集完成。

图 4-5 配置确认



----结束

5 用户登录并访问资源

将组织下的一个或多个成员账号与用户和权限集关联后，用户即可使用用户名和密码通过用户门户URL登录控制台并访问资源，资源具体的访问权限由权限集控制。

操作步骤

步骤1 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“总览”，在总览页面可获取用户门户URL。

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 5-1 获取用户门户 URL

步骤4 使用浏览器打开用户门户URL，输入用户名并单击“下一步”。

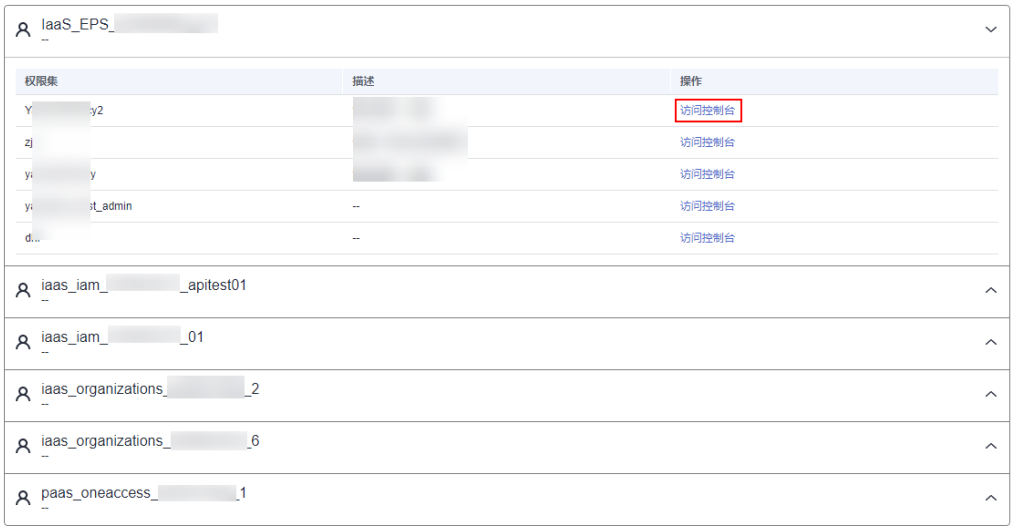
用于登录的用户名和密码在创建用户时获取。如果忘记密码或需要修改密码，管理员可以使用重置密码功能，重新向用户发送密码设置邮件或生成一次性密码。

图 5-2 用户登录

步骤5 输入登录密码，单击“登录”。

步骤6 每个账号下的资源根据关联的多个权限集分别显示登录入口，单击操作列的“访问控制台”，即可访问此账号下对应权限集控制的资源。

图 5-3 访问资源



----结束