IAM 身份中心

用户指南

文档版本 01

发布日期 2024-02-20

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 用户管理

1.1 创建用户

开通IAM身份中心服务后，您需要创建用户。将用户与组织下的多个账号关联并配置权限，然后使用用户登录即可访问多个账号下的资源，无需重复登录。

如您首次使用IAM身份中心，界面将显示服务开通页，单击“立即开通”，即可开通IAM身份中心服务并使用相关功能。

操作步骤

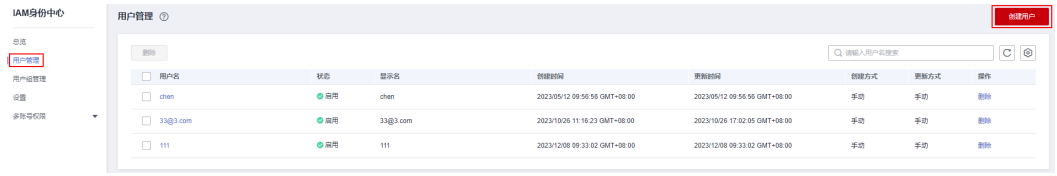
步骤1 登录华为云控制台。

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“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

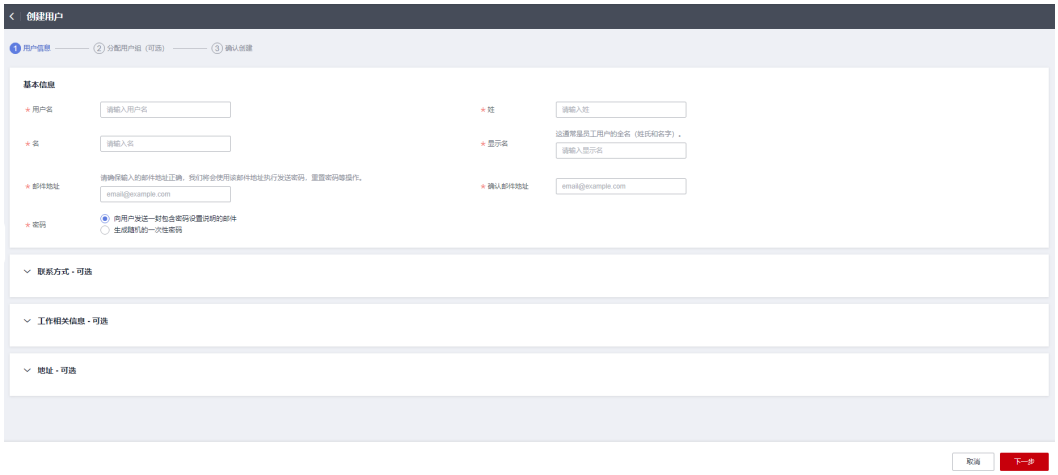
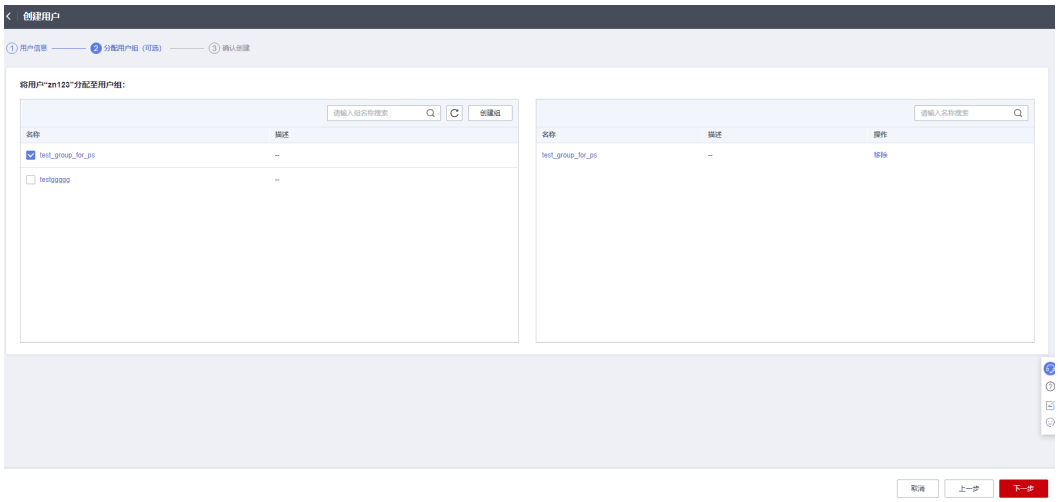


表 1-1 基本信息

参数	描述
用户名	IAM身份中心用户名称。 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”。

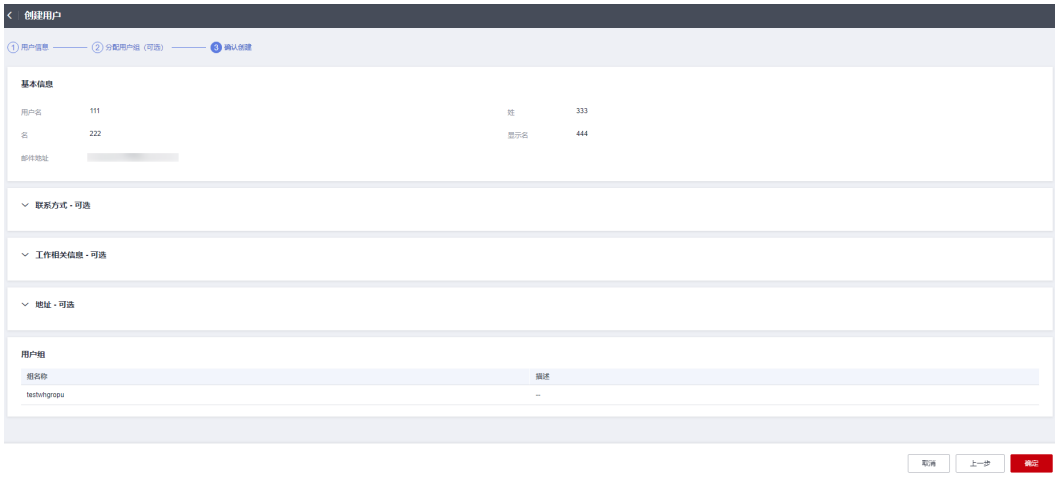
图 1-3 分配用户组（可选）



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 1-4 确认创建



----结束

1.2 用户登录并访问资源

用户创建完成后，用户即可使用用户名和密码通过用户门户URL登录控制台，如需访问资源，则还需关联权限集和组织下的一个或多个成员账号，这样登录后才能访问组织下账号的资源，而资源具体的访问权限由权限集控制。具体请参见**创建权限集**和**账号关联用户/组和权限集**。

管理员开通IAM身份中心后，系统会自动生成唯一的用户门户URL，此管理员创建的所有用户均可使用此URL登录控制台。管理员可对用户门户URL进行一次自定义修改，具体请参见：**自定义用户门户URL**。

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 1-5 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”。

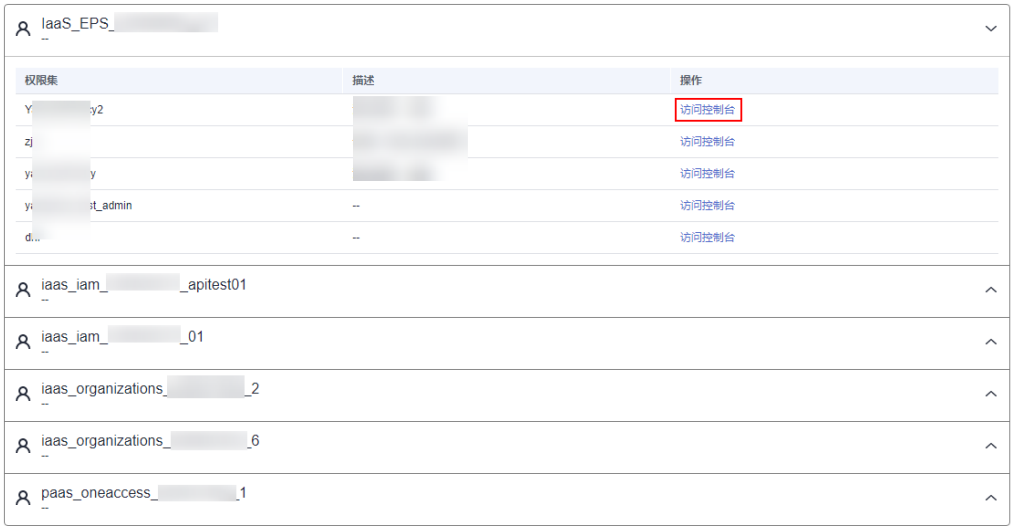
用于登录的用户名和密码在**创建用户**时获取。如果忘记密码或需要修改密码，管理员可以使用**重置密码**功能，重新向用户发送密码设置邮件或生成一次性密码。

图 1-6 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 1-7 访问资源



----结束

1.3 管理用户

用户创建完成后，在用户详情页您可以查看用户信息，还可以进行修改用户信息、重置密码、禁用/启用/删除用户和加入/退出用户组等操作。

本章节包含如下内容：

- **修改用户信息**
- **禁用/启用/删除用户**
- **重置密码**
- **加入/退出用户组**

修改用户信息

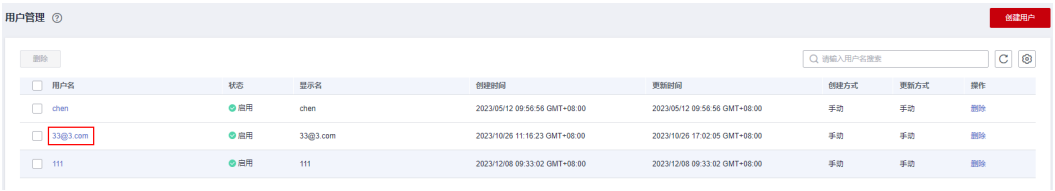
步骤1 登录**华为云控制台**。

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 在用户列表中，单击用户名，进入用户信息详情页。

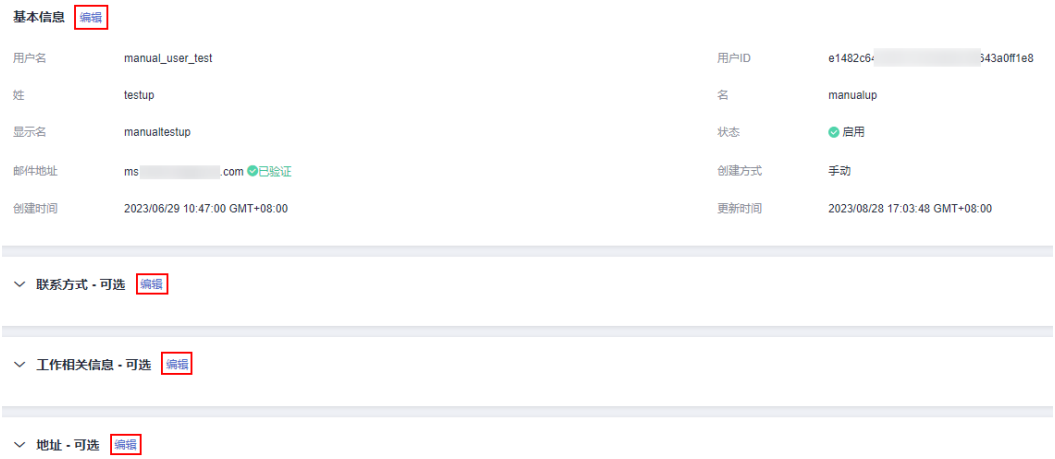
图 1-8 选择用户



步骤5 单击基本信息后方的“编辑”，修改用户基本信息。

步骤6 （可选）单击联系方式、工作相关信息和地址后方的“编辑”，修改相关信息。

图 1-9 编辑用户信息



步骤7 编辑完成后，单击“保存”，用户信息修改完成。

----结束

禁用/启用/删除用户

当您暂时不需要使用某个用户时，可以禁用此用户的访问权限。如需重新使用，您可以将其再次启用。

您也可以删除用户，删除操作无法恢复，请谨慎使用。

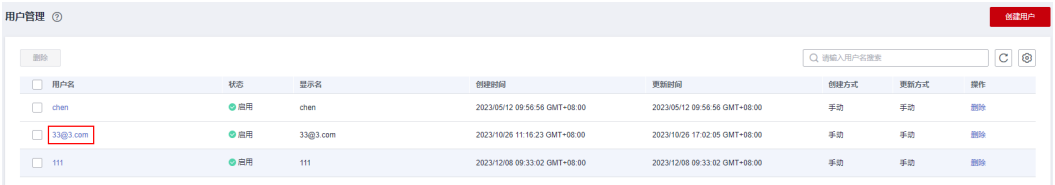
步骤1 登录华为云控制台。

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 在用户列表中，单击用户名，进入用户信息详情页。

图 1-10 选择用户



步骤5 单击页面右上角的“禁用”。

图 1-11 禁用用户

步骤6 在弹出的确认框中单击“确定”，此用户的状态变为停用。

步骤7 如需启用用户，则在用户列表中，单击已禁用的用户名称，进入用户详细信息页，单击右上角的“启用”。

步骤8 在弹出的确认框中单击“确定”，此用户的状态变为启用。

步骤9 如需删除用户，则在用户详细信息页，单击右上角的“删除用户”。

图 1-12 删除用户

步骤10 在弹出的确认框中单击“确定”，可将此用户删除。

----结束

重置密码

当您需要修改某个用户的密码时，可以使用重置密码功能。

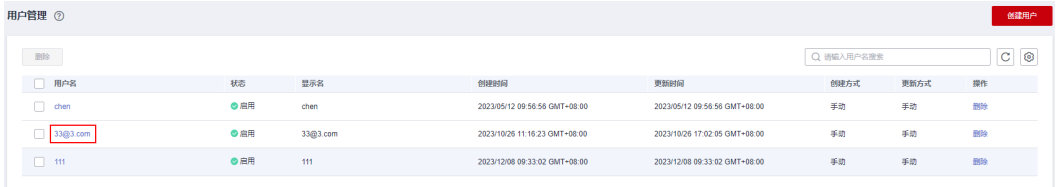
步骤1 登录华为云控制台。

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 在用户列表中，单击用户名，进入用户信息详情页。

图 1-13 选择用户



步骤5 单击页面右上角的“重置密码”。

图 1-14 重置密码

步骤6 在弹出的确认框中选择密码的重置方式，单击“确定”，用户的密码重置完成。

图 1-15 选择重置密码的方式

选择重置密码的方式：

- 向用户发送一封包含密码重置说明的电子邮件：系统通过邮件发送密码重置说明给用户，用户根据邮件说明重置密码。
- 生成一次性密码并与用户共享该密码：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。

----结束

加入/退出用户组

用户创建完成后，您可以将其添加到用户组，或者将其从用户组中移除。

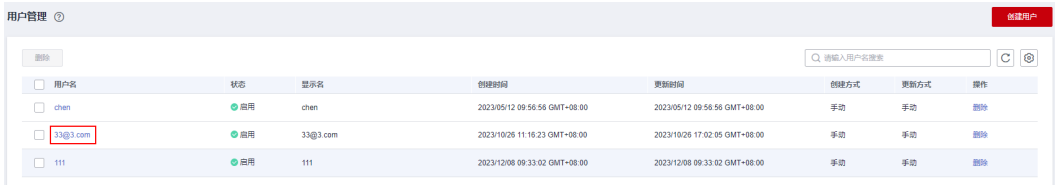
步骤1 登录华为云控制台。

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 在用户列表中，单击用户名，进入用户信息详情页。

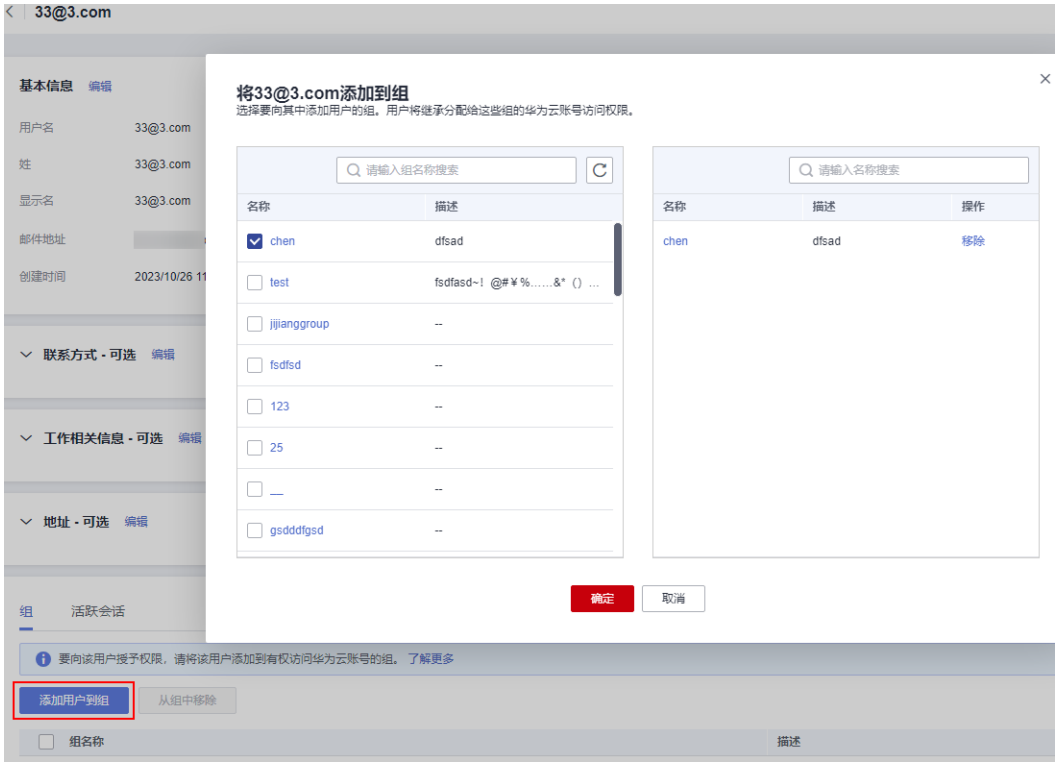
图 1-16 选择用户



步骤5 在用户详情页下方的“组”页签中单击“添加用户到组”。

步骤6 在弹窗的用户组列表中勾选需要加入的用户组，单击“确定”，用户添加到用户组完成。

图 1-17 用户加入用户组



步骤7 在用户组列表中，勾选需要退出的用户组，单击“从组中移除”。

也可以在用户组列表中单击操作列的“移除”，进行单个用户组移除操作。

步骤8 在弹出的确认框中单击“确定”，用户从用户组中移除完成。

图 1-18 退出用户组

----结束

1.4 删除用户

当您不再需要使用某个用户时，可以删除此用户。删除用户将移除有关此用户的所有信息，并移除其访问权限。

删除操作无法恢复，请谨慎使用。

删除单个用户

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 在用户列表中，单击操作列的“删除”。

图 1-19 删除用户

步骤5 在弹出的确认框中单击“确定”，用户删除完成。

----结束

批量删除用户

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 在用户列表中，勾选多个需要删除的用户，单击列表上方的“删除”。

图 1-20 批量删除用户

步骤5 在弹出的确认框中单击“确定”，所选用户删除完成。

----结束

1.5 配置用户门户会话的持续时间

默认情况下，用户门户会话的持续时间为8小时，即用户无需重新进行身份验证即可登录用户门户的最长时间，超出会话最长持续时间后用户将从用户门户页面登出，需重新进行身份验证。您可以参考如下步骤设置不同的持续时间。

> **说明**
>
> 如果您使用外部身份提供商（IdP）作为IAM身份中心的身份源，则用户门户会话的持续时间是您在IdP或IAM身份中心设置的持续时间中较短的一个。例如，您的IdP会话持续时间为24小时，并且您在IAM身份中心将会话持续时间设置为18小时，则您的用户必须在18小时后在用户门户中重新进行身份验证。

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“设置”，进入设置页面。

步骤4 选择“会话设置”页签，配置用户的访问用户门户会话的最长持续时间。

会话最长持续时间默认为8小时，您可以指定不同的持续时间，从最少的15分钟到最多的90天。

会话最长持续时间的下拉框中提供常用的时长供您直接选择，您也可以选择“自定义持续时间”，并在后方输入具体的持续分钟数（15~129600之间）。

图 1-21 会话设置

步骤5 单击“应用”，配置完成。

----结束

2 用户组管理

2.1 创建用户组

管理员可以创建用户组，并给用户组关联权限集和账号，然后将用户加入用户组，使用户组下的全部用户获得相应的权限，方便统一权限管理。

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“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 2-1 创建用户组

步骤5 在“创建用户组”界面，输入“名称”和“描述”。

用户组名称不可与其他IAM身份中心用户组名称重复。

步骤6 （可选）选择需要添加至用户组中的用户。

步骤7 单击“确定”，用户组创建完成，用户组列表中显示新创建的用户组。

----结束

2.2 用户组添加/移除用户

将用户添加或移除至特定用户组后，用户将具备或失去对应用户组的权限，快速实现用户的权限变更。

当某个用户加入多个用户组时，此用户同时拥有多个用户组的权限，即多个用户组权限的全集。

用户组添加用户

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“用户组管理”，进入“用户组管理”页面。

步骤4 在用户组列表中，单击用户组名称，进入用户组详细信息页面。

图 2-2 选择用户组

步骤5 在“用户”页签下，单击“添加用户”，系统弹出添加用户页面。

步骤6 在用户列表中选择需要添加至用户组中的用户，单击“确定”，用户添加完成。

图 2-3 用户组添加用户

----结束

用户组移除用户

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“用户组管理”，进入“用户组管理”页面。

步骤4 在用户组列表中，单击用户组名称，进入用户组详细信息页面。

图 2-4 选择用户组

步骤5 在用户列表中的操作列，单击“移除”。

步骤6 在弹出的确认框中单击“确定”，单个用户移除完成。

图 2-5 单个移除用户

步骤7 在用户列表中勾选多个需要移除的用户，单击“移除用户”。

步骤8 在弹出的确认框中单击“确定”，所选用户批量移除完成。

图 2-6 批量移除用户

----结束

2.3 删除用户组

当您不再需要某个用户组时，可以将其删除。删除用户组后，用户组中的所有用户将失去相关权限。

删除操作无法恢复，请谨慎使用。

删除单个用户组

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“用户组管理”，进入“用户组管理”页面。

步骤4 在用户组列表中，单击需要删除用户组操作列的“删除”。

步骤5 在弹出的确认框中单击“确定”，用户组删除完成。

图 2-7 单个删除用户组

----结束

批量删除用户组

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“用户组管理”，进入“用户组管理”页面。

步骤4 在用户组列表中，勾选多个需要删除的用户组，单击列表上方的“删除”。

图 2-8 批量删除用户组

步骤5 在弹出的确认框中单击“确定”，所选用户组删除完成。

----结束

3 多账号权限管理

3.1 设置委托管理员

IAM身份中心默认由组织管理员账号使用和管理，组织中的成员账号如需使用IAM身份中心，需组织管理员将其设置为委托管理员。

此操作会将IAM身份中心的管理访问权限委托给此成员账号中的用户。对此委托管理员账号拥有足够权限的所有用户可以从该账号执行所有IAM身份中心管理任务，但以下任务除外：删除IAM身份中心、设置其他成员账号为委托管理员、管理向管理账号分配的任务，或管理在管理账号中预置的权限集。

操作步骤

步骤1 登录华为云控制台。

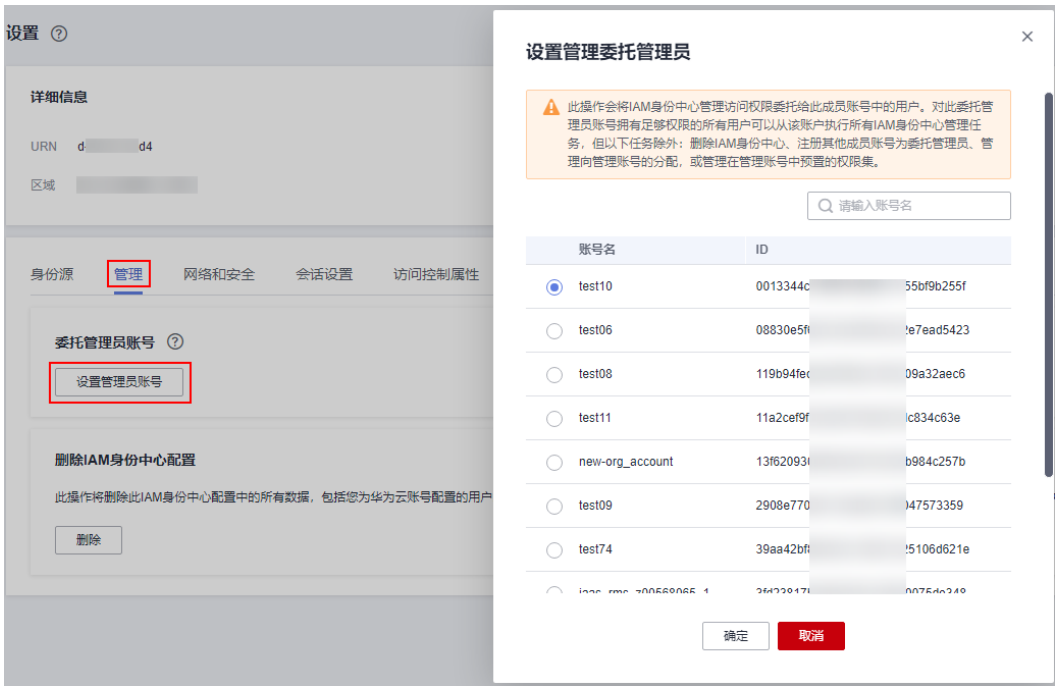
步骤2 单击页面左上角的 ☰ ，选择“管理与监管 > IAM身份中心”，进入“IAM身份中心”页面。

步骤3 单击左侧导航栏的“设置”，进入设置页面。

步骤4 在“管理”页签中单击“设置管理员账号”。

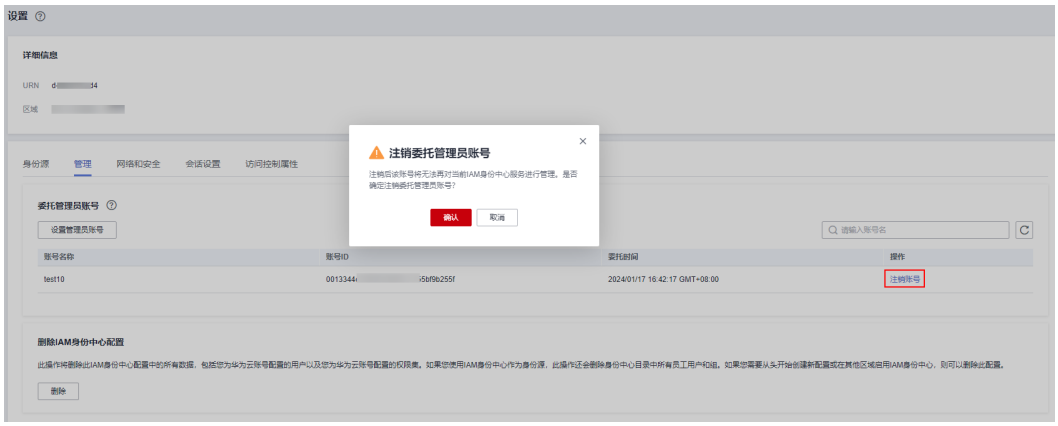
步骤5 在“设置管理委托管理员”页面中，选择成员账号，单击“确定”，委托管理员设置成功。

图 3-1 设置委托管理员



步骤6 在委托管理员账号列表中单击操作列的“注销账号”，可注销此委托管理员账号，注销后该账号将无法再对当前IAM身份中心服务进行管理。

图 3-2 注销委托管理员账号



----结束

3.2 权限集管理

3.2.1 创建权限集

权限集是管理员创建和维护的权限模板，它定义了一个或多个IAM策略的集合。权限集简化了IAM身份中心的用户和用户组对账号访问权限的分配。可以实现批量的账号权限配置，无需再进行单独的权限配置。

创建权限集为必需操作，使用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。

云服务在IAM预置了常用授权项，称为系统策略。创建权限集时，可以直接使用这些系统策略，系统策略只能使用，不能修改。如果系统策略无法满足您的授权要求，您可以创建自定义身份策略或自定义策略，对系统策略进行扩展和补充。如需查看所有云服务的系统策略，请参见：**系统权限**。

说明

单个权限集最多可以包含18个系统策略+1个自定义身份策略+1个自定义策略。

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 > 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 3-3 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 3-4 配置基本信息

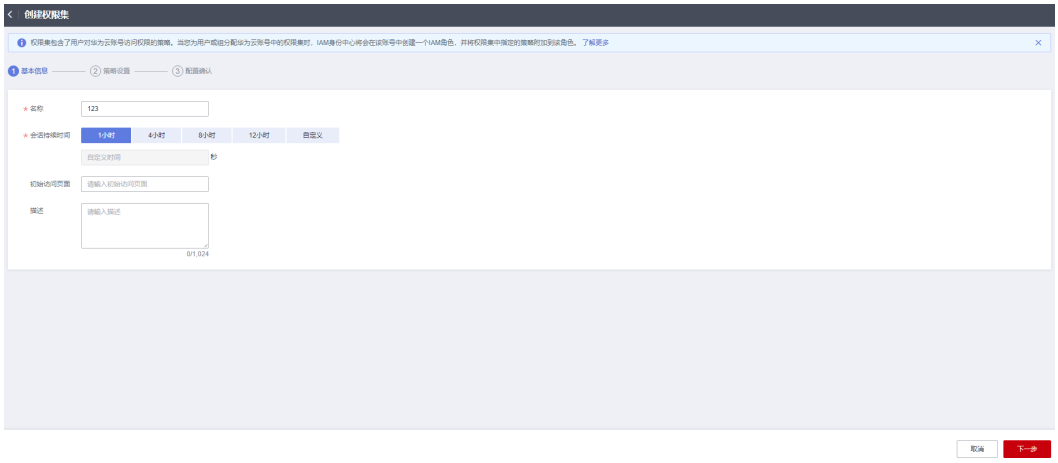


表 3-1 权限集基本信息

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。

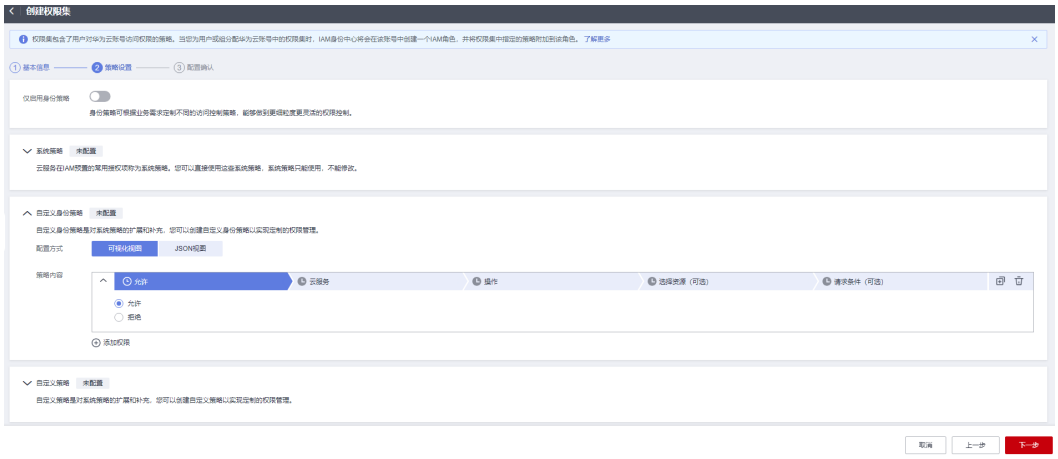
参数	描述
会话持续时间	使用此权限集授权的IAM身份中心用户登录控制台后的会话持续时间。 登录时间超出设置的会话持续时间后，会话将过期，用户将自动登出，如需继续访问，需重新登录。
初始访问页面	IAM身份中心用户通过门户URL登录控制台后访问的初始页面。 例如您可以输入IAM控制台的URL，登录后将直接显示IAM控制台页面。
描述	权限集的描述信息。

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。

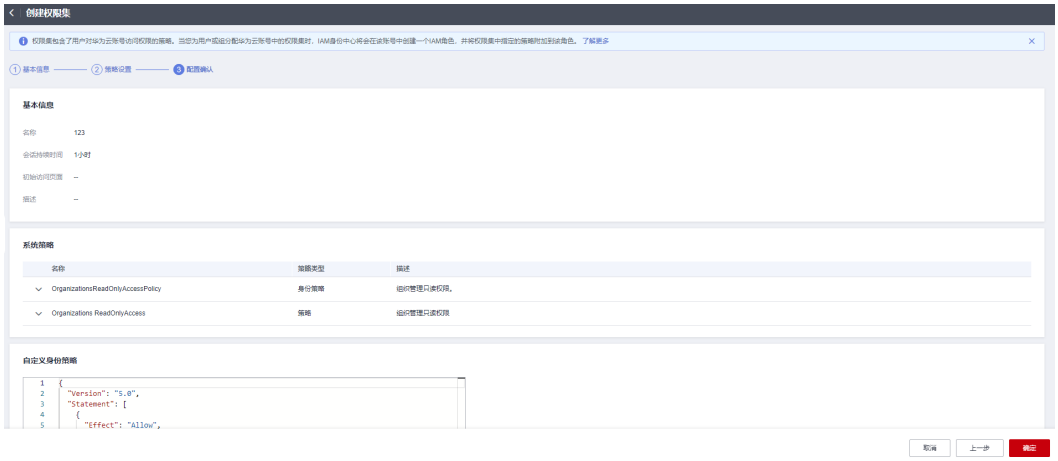
- 系统策略：在列表中直接选择云服务在IAM预置的系统策略，系统策略分为策略和身份策略两种类型。
- 自定义身份策略：如果系统身份策略无法满足您的授权要求，您可以创建自定义身份策略，对系统身份策略进行扩展和补充。当前支持通过可视化视图和JSON视图两种方式创建自定义身份策略。
- 自定义策略：如果系统策略无法满足您的授权要求，您可以创建自定义策略，对系统策略进行扩展和补充。当前仅支持通过JSON视图创建自定义策略。

图 3-5 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 3-6 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

3.2.2 查看或修改权限集

完成权限集的创建后，支持对权限集的基本信息和策略设置进行查看和修改，以及对关联的账号进行更新权限集操作。

查看权限集

步骤1 登录华为云控制台。

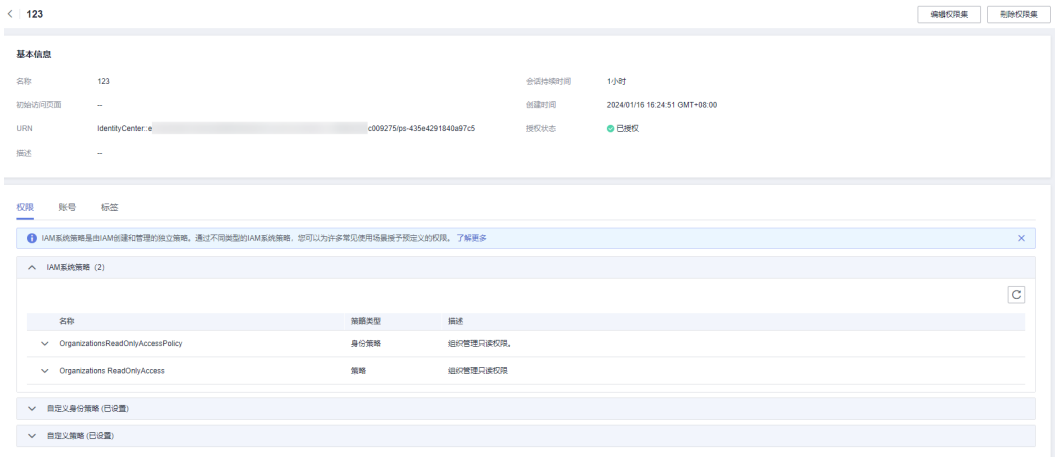
步骤2 单击页面左上角的 ☰，选择“管理与监管 > IAM身份中心”，进入“IAM身份中心”页面。

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 在列表中可查看当前已创建的权限集及其相关信息。

步骤5 在权限集列表中，单击权限集名称，进入权限集详情页，可查看权限集的基本信息、权限配置和关联账号详情。

图 3-7 权限集详情页



----结束

修改权限集

步骤1 登录华为云控制台。

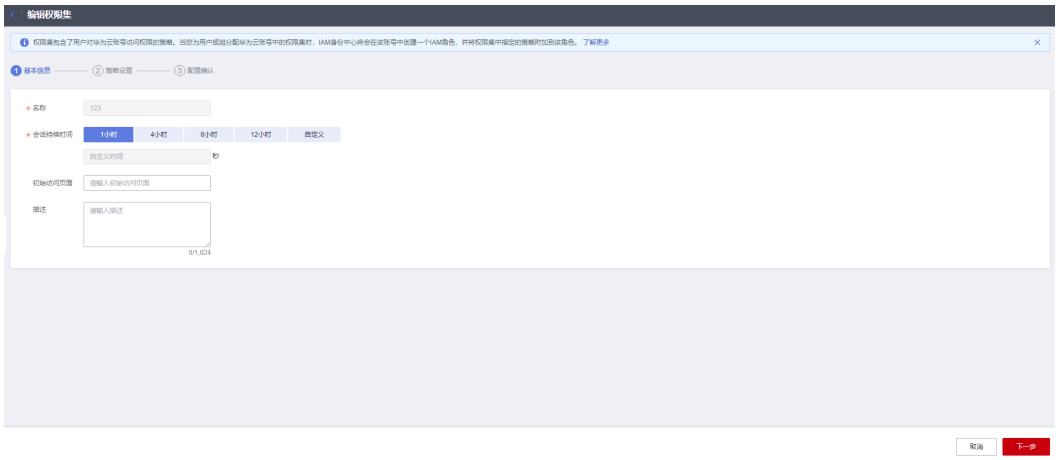
步骤2 单击页面左上角的 ☰ ，选择“管理与监管 > IAM身份中心”，进入“IAM身份中心”页面。

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 在权限集列表中单击操作列的“编辑”，进入编辑权限集页面。

步骤5 在“基本信息”页面，您可以修改会话持续时间、初始访问页面和描述，修改完成后单击“下一步”。

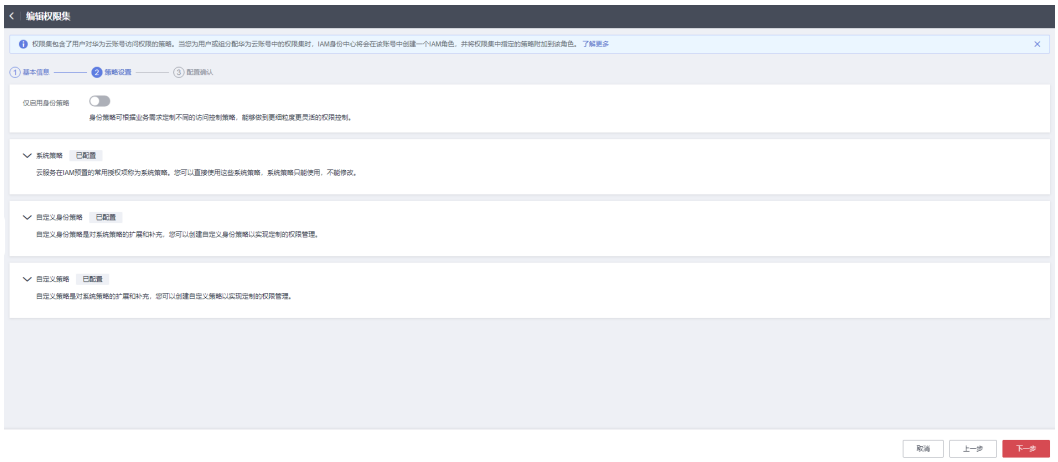
图 3-8 修改基本信息



步骤6 在“策略设置”页面，您可以修改系统策略、自定义身份策略和自定义策略，并且还可修改“仅启用身份策略”开关，修改完成后单击“下一步”。

如权限集中已配置策略和自定义策略，此时开启“仅启用身份策略”开关将删除已配置的策略和自定义策略。

图 3-9 修改策略设置



步骤7 进入“配置确认”页面，确认修改无误后单击“确定”，权限集修改完成。

----结束

更新权限集

当遇到权限集同步失败的异常情况时，账号列表中的权限集状态会变为“未同步”，此时需要更新关联账号的权限集信息。

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 在权限集列表中，单击权限集名称，进入权限集详情页。

步骤5 在页面下方的“账号”页签中，勾选权限集状态为“未同步”的账号，单击上方的“更新”，或在账号列表中单击操作列的“更新”。

图 3-10 更新权限集

步骤6 进入更新权限集页面，单击页面右下方的“更新”，权限集更新成功。账号列表中的权限集状态变为“已同步”。

----结束

3.2.3 删除权限集

当您不再需要某个权限集时，可以将其删除。需将权限集关联的账号全部解绑后，权限集才能删除。如何解绑账号请参见**删除关联的用户/组和权限集**。

删除操作无法恢复，请谨慎使用。

操作步骤

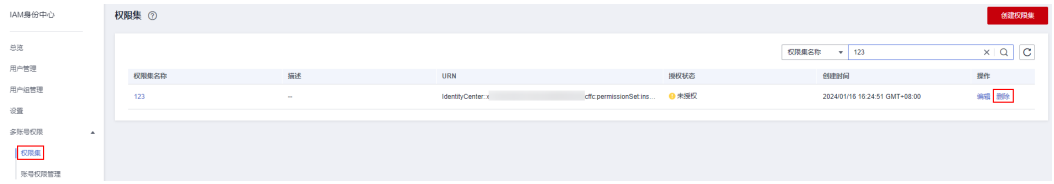
步骤1 登录华为云控制台。

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 > 权限集”，进入“权限集”页面。

步骤4 在权限集列表中单击操作列的“删除”，在弹出的确认框中单击“确定”，权限集删除完成。

图 3-11 删除权限集



----结束

3.2.4 管理权限集标签

标签简介

标签用于标识云资源，当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类。

IAM身份中心支持为权限集添加标签，您可以根据标签快速搜索和筛选特定的权限集，使您可以更轻松高效的识别和管理已创建的权限集。

您可以在权限集创建完成后，在权限集的详情页添加、修改、查看、删除标签，您最多可以给每个权限集添加20个标签。

标签的使用约束

- 每个标签由“标签键”和“标签值”组成，“标签键”和“标签值”的命名规则如下：

  “标签键”：

  - 不能为空。
  - 长度不超过128个字符。
  - 由英文字母、数字、下划线、中划线、UNICODE字符（\u4E00-\u9FFF）组成。

  “标签值”：

  - 可以为空。
  - 长度不超过225个字符。
  - 由英文字母、数字、下划线、点、中划线、UNICODE字符（\u4E00-\u9FFF）组成。
- 每个云资源最多可以添加20个标签。

- 对于每个云资源，每个“标签键”都必须是唯一的，每个“标签键”只能有一个“标签值”。

操作步骤

您可以在IAM身份中心控制台对权限集进行添加、编辑和删除标签的操作。

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 在权限集列表中，单击权限集名称，进入权限集详情页。

步骤5 在“标签”页签中，单击“添加”。

步骤6 在弹窗中输入标签键和标签值（可选），单击“添加”，然后单击“确定”，完成权限集标签的添加。

您还可以在标签键的下拉框中选择已在TMS创建的预定义标签，关于预定义标签的更多信息请参见**预定义标签**。

图 3-12 添加标签

步骤7 在标签列表中单击标签操作列的“编辑”，在弹窗中可修改已添加标签的“值”，然后单击“确定”。

图 3-13 编辑标签

步骤8 在标签列表中单击标签操作列的“删除”，在弹出的确认框中单击“确定”，可删除已添加的标签。

图 3-14 删除标签

----结束

3.3 账号权限管理

3.3.1 账号关联用户/组和权限集

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用户/组和权限集，这样使用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。

当前仅支持为组织下的一个或多个成员账号关联用户/组和权限集，不支持直接选择整个组织或组织单元。

IAM身份中心的账号数据来自您的企业/组织在华为云已配置的组织结构，如需管理账号数据请前往**组织服务控制台**操作。

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。

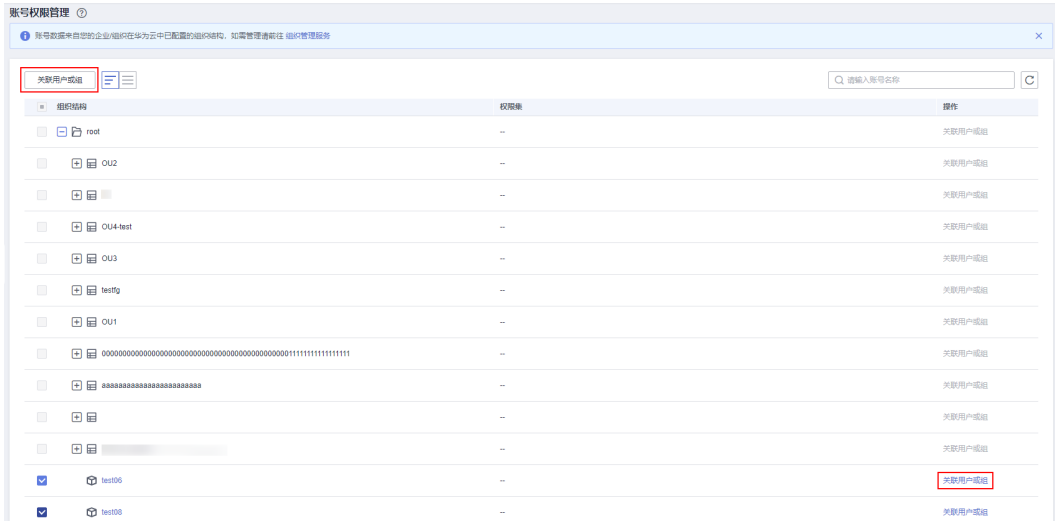
账号权限管理列表默认以组织结构树的形式显示，在列表左上方单击 ，列表将只显示组织下的所有成员账号，而不显示组织结构树。

图 3-15 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”。

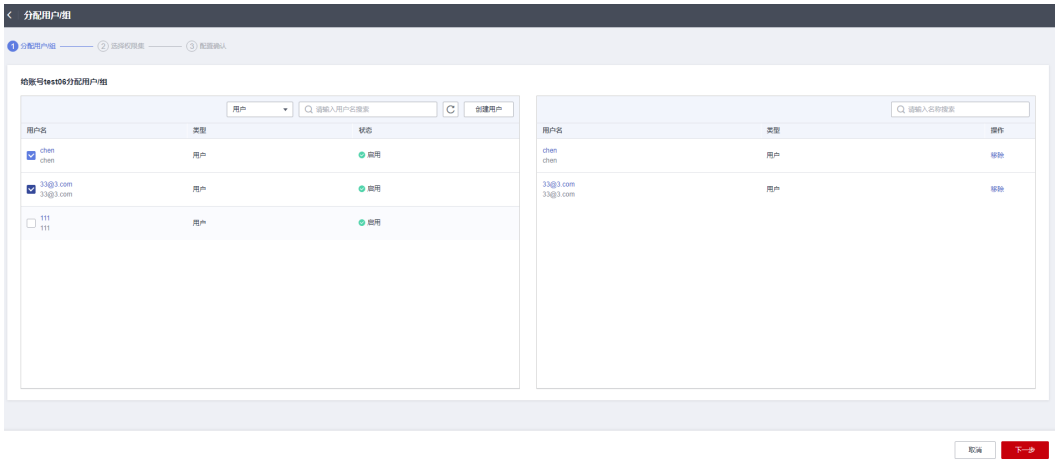
您也可以在账号列表中单击某一账号操作列的“关联用户或组”。

图 3-16 选择账号



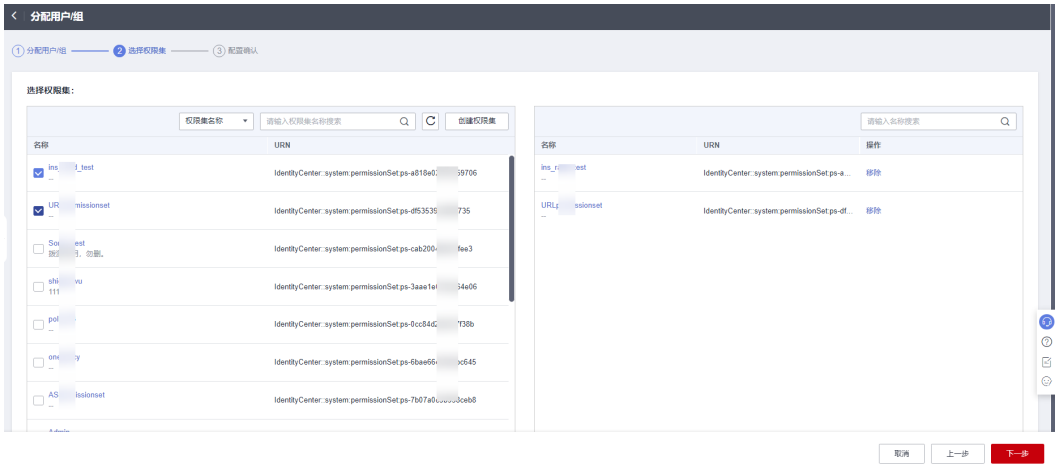
步骤5 进入“分配用户/组”页面，在列表中勾选需要关联的用户/组，单击“下一步”。

图 3-17 分配用户/组



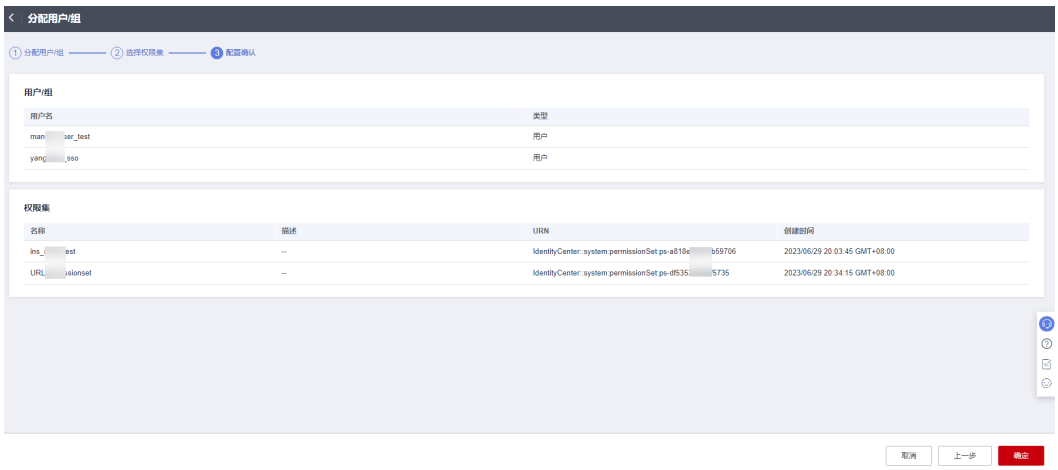
步骤6 进入“选择权限集”页面，在权限集列表中勾选需要关联的权限集，单击“下一步”。

图 3-18 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 3-19 配置确认



----结束

3.3.2 修改关联的用户/组和权限集

当您需要修改某一账号关联的用户/组和权限集时，请参考如下步骤进行操作。

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 3-20 账号列表显示方式切换

步骤4 在账号列表中单击需要修改的账号名称，进入账号详情页。

步骤5 在“用户/组”页签中单击“分配用户/组”，即可修改此账号关联的用户/组和权限集，具体请参见**账号关联用户/组和权限集**。

图 3-21 分配用户/组

步骤6 在用户/组列表中勾选一个或多个用户/用户组，单击“更改权限集”，或单击单个用户/用户组操作列的“更改权限集”。

步骤7 进入更改权限集页面，在权限集列表中勾选或去勾选权限集，单击页面右下角的“确认更改”，用户或用户组的权限集新增/删除完成。

图 3-22 更改权限集

步骤8 如果账号关联权限集的基本信息或包含策略有修改，您可以在“权限集”页签中勾选需要更新的权限集，单击“更新”，或单击单个权限集操作列的“更新”。

图 3-23 更新权限集

步骤9 进入更新权限集页面，单击右下角的“更新”，权限集更新成功。

----结束

3.3.3 删除关联的用户/组和权限集

当您需要删除某一账号关联的用户/组和权限集时，请参考如下步骤进行操作。

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 3-24 账号列表显示方式切换

步骤4 在账号列表中单击需要修改的账号名称，进入账号详情页。

步骤5 在“用户/组”页签中勾选一个或多个的用户/用户组，单击“移除访问权限”，或单击单个用户/用户组操作列的“移除访问权限”。

步骤6 在弹出的确认框中单击“确定”，用户/用户组以及关联的权限集均移除完毕。

图 3-25 移除访问权限

步骤7 如果仅需移除关联的权限集，您可以在“权限集”页签中勾选一个或多个权限集，单击“移除”，或单击单个权限集操作列的“移除”，

步骤8 在弹出的确认框中单击“确定”，权限集移除完成。

图 3-26 移除权限集

----结束

3.4 基于属性的访问控制（ABAC）

3.4.1 ABAC 概述和配置流程

ABAC 概述

基于属性的访问控制（ABAC）是一种授权策略，该策略基于用户属性来定义权限。您可以使用IAM身份中心或外部身份提供商等不同身份源的用户属性，在IAM身份中心管理用户对华为云资源的访问权限。用户属性也可以称之为标签，使用用户属性作为标签可以帮助您简化在华为云中创建细粒度权限的过程，并确保用户只能获得具有匹配标签的华为云资源相关权限，实现更精细的权限管理。

例如，您可以将两个不同用户User_A和User_B关联相同的权限集，然后基于用户的显示名属性来进行访问控制。当User_A和User_B登录用户门户访问此权限集定义的资源时，IAM身份中心会将他们的显示名与资源的标签值进行匹配，只有当他们的显示名与资源上的添加的标签值匹配时，User_A和User_B才能访问该资源。如果User_A后续不再需要访问此权限集下的某些资源，您只需修改这些资源的标签即可使User_A失去访问权限，而无需更新任何权限集配置。

基于属性的访问控制还有助于减少您需要在IAM身份中心中创建和管理的权限集数量，因为与相同权限集关联的用户现在可以根据其用户属性拥有唯一权限。您可以在权限集中使用这些用户属性，以实现对华为云资源基于用户属性的访问控制，并在规模上简化权限管理。

使用 ABAC 的优势

- ABAC需要的权限集更少：由于您不必为不同的用户创建不同的权限集，因此可以减少权限集数量，这将降低权限管理的复杂性。
- 使用ABAC，团队可以快速变化和成长：在创建资源时为其添加适当的标签，系统会根据用户属性自动授予新建资源的权限。
- 通过ABAC使用企业目录中的员工属性：您可以使用IAM身份中心配置的任何身份源的现有员工属性在华为云中做出访问控制决策。

ABAC 配置流程

如下表格包括准备华为云资源和配置IAM身份中心以进行ABAC访问控制所需的操作，使用ABAC需完成此表格中的各项操作。

表 3-2 ABAC 配置流程

步骤	说明	参考文档
为资源添加标签	要在IAM身份中心中实施ABAC，您首先要为需要实施ABAC的资源添加标签。资源标签的值要与用户属性设置一致，这样才能在权限策略中匹配成功，从而使访问控制策略生效。 例如您需要使用用户的用户名属性进行访问控制，用户的用户名为“User1”，那么您给资源添加的标签值也需为“User1”。	为云资源添加标签
配置身份源	IAM身份中心当前支持两种身份源：IAM身份中心和外部身份提供商。两种身份源的用户属性均支持实施ABAC，您可以在IAM身份中心切换两种身份源。	更改身份源
在IAM身份中心启用并配置ABAC	• IAM身份中心身份源：在IAM身份中心控制台启用ABAC，并添加用于ABAC的用户属性。 • 外部身份提供商身份源：首先在IAM身份中心控制台启用ABAC，然后您可以在IAM身份中心配置ABAC，还可以在外部身份提供商处配置。	启用和配置访问控制属性

步骤	说明	参考文档
为ABAC创建权限策略	在权限集中创建自定义身份策略，并使用访问控制属性创建ABAC相关规则，用于控制用户只能访问带有匹配标签的资源。您在上一步中添加的用户属性用作访问控制决策的标签，您可以使用“PrincipalTag/key”条件键引用权限策略中的访问控制属性。	**为ABAC创建权限策略**
账号关联用户/组和权限集	将相关账号和IAM身份中心用户与上一步创建的权限集关联，这样用户登录用户门户访问关联账号下的资源时，只能访问基于用户属性匹配标签的资源。	**账号关联用户/组和权限集**
用户登录并访问资源	完成以上步骤后，关联相关账号和权限集的IAM身份中心用户登录用户门户，将根据匹配的用户属性获得相应资源的访问权限。	**用户登录并访问资源**

3.4.2 启用和配置访问控制属性

操作场景

在任一身份源中实施ABAC，首先都需在IAM身份中心启用访问控制属性功能，并在其中添加需要在权限集策略中使用的用户属性来控制用户对资源的访问权限。可添加的用户属性如用户的基本信息、联系方式、工作相关信息和地址信息等。当前支持实施ABAC的用户属性请参见**支持配置的用户属性**。

例如您要根据用户的用户名分配其对组织资源的访问权限，您可以在“访问控制属性”页面上添加用户名属性用于ABAC。然后在IAM身份中心的权限集中添加一个自定义身份策略，该策略仅在用户的用户名与您分配给组织资源的标签值匹配时才授予用户访问权限。关于ABAC相关自定义策略的详细信息请参见：**为ABAC创建权限策略**。

对于不同的身份源实施ABAC的差异如下：

- 当使用IAM身份中心作为身份源时， 您需要在IAM身份中心的“访问控制属性”页面添加实施ABAC的属性。
- 当使用外部身份提供商作为身份源时，有如下两种方法可以添加实施ABAC的属性。
  - 在外部身份提供商处添加ABAC属性。您可以将外部身份提供商配置为通过SAML断言发送属性，在这种情况下，IAM身份中心将获取来自外部身份提供商传递的属性键和属性值用于策略评估。具体配置请参考外部身份提供商文档的相关内容。

    说明

    通过SAML断言传递的属性在IAM身份中心的“访问控制属性”页面不可见，您必须提前了解这些属性，并在创建权限策略时将其添加到访问控制规则中。

- 在IAM身份中心的“访问控制属性”页面配置ABAC属性。如果在IAM身份中心和外部身份提供商处设置的ABAC属性相同，则优先以IAM身份中心设置的属性进行访问控制决策。

本章节仅体现IAM身份中心的相关操作，外部身份提供商处的操作请参考外部身份提供商的相关文档。

启用访问控制属性

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“设置”，进入设置页面。

步骤4 在“访问控制属性”页签中单击“启用”。

图 3-27 启用访问控制属性

----结束

配置访问控制属性

启用访问控制属性功能后，您需要添加属性键和属性值用于访问控制，最多可以添加20个属性。

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“设置”，进入设置页面。

步骤4 在“访问控制属性”页签中单击“添加”。

步骤5 在弹出的配置框中添加用于访问控制的用户属性键和属性值。

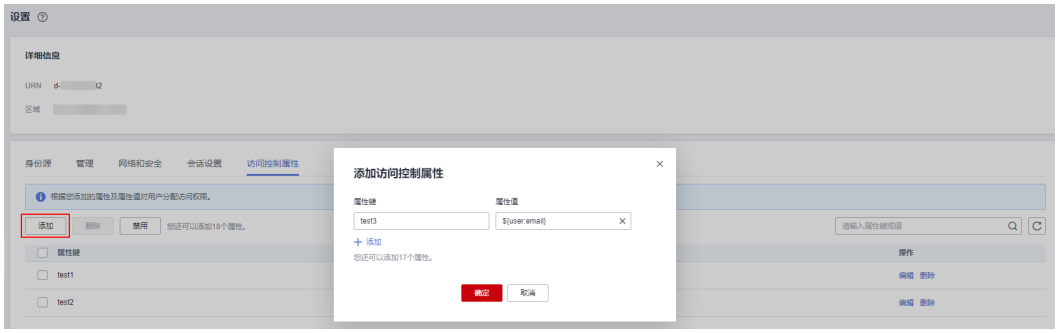
- 属性键：表示您为用户属性指定的名称，以便在权限策略中使用，仅支持输入单值。

  您可以输入任意名称，后续在权限集中编写自定义身份策略时需使用该名称。例如您将属性键设置为“User_A”， 则自定义身份策略中的**PrincipalTag**条件键也需设置为“User_A”，即"g:ResourceTag/*tag-key*": "${g:PrincipalTag/User_A}"。

- 属性值：表示用户属性的类型，您可以在下拉框中选择需进行访问控制的用户属性类型。

  例如您选择${user:name}，就表示使用用户的用户名进行访问控制，也就是在授权时会将用户名与资源标签的值进行匹配校验。当前支持的用户属性请参见**支持配置的用户属性**。

图 3-28 添加访问控制属性



步骤6 配置完成后单击“确定”。

现在您已经启用并配置访问控制属性，接下来需在权限集中添加ABAC的自定义身份策略，具体请参见：**为ABAC创建权限策略**。

----结束

编辑/删除访问控制属性

访问控制属性添加完成后，您可以根据需要随时修改和删除它们。

步骤1 登录**华为云控制台**。

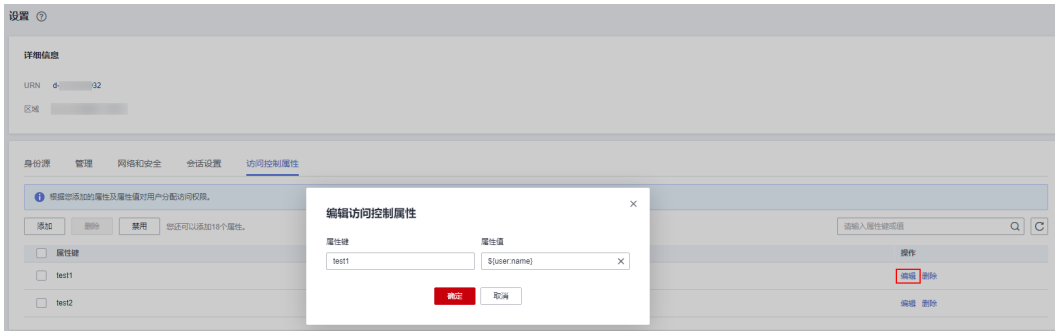
步骤2 单击页面左上角的 ☰，选择“管理与监管 > IAM身份中心”，进入“IAM身份中心”页面。

步骤3 单击左侧导航栏的“设置”，进入设置页面。

步骤4 选择“访问控制属性”页签，在列表中的操作列单击“编辑”。

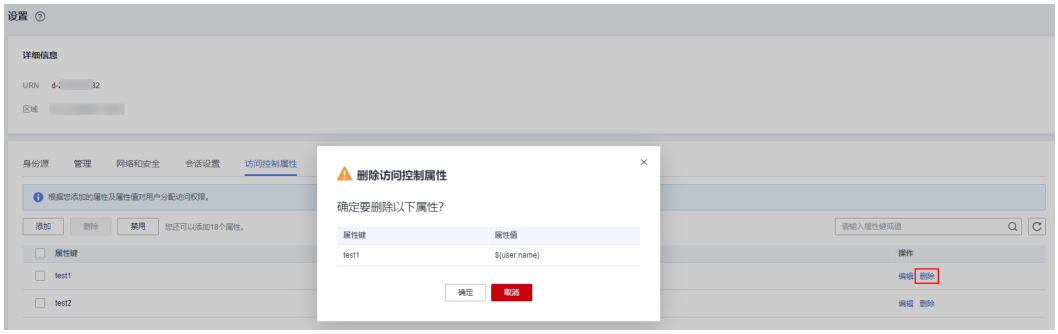
步骤5 在弹出的配置框中修改属性键或属性值，修改完成后单击“确定”。

图 3-29 编辑控制访问属性



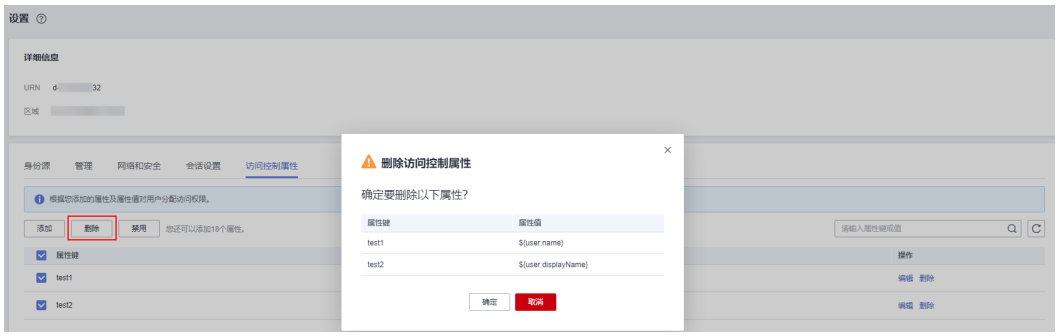
步骤6 在列表中的操作列单击“删除”，在弹出的确认框中单击“确定”，单个访问控制属性删除完成。

图 3-30 单个删除访问控制属性



步骤7 在列表中勾选需要删除的多个属性，单击列表上方的“删除”，在弹出的确认框中单击“确定”，多个访问控制属性批量删除完成。

图 3-31 批量删除访问控制属性



----结束

禁用访问控制属性

如您不再需要使用ABAC功能，您可以随时禁用此功能，禁用访问控制属性将删除所有已配置的属性，且不可恢复，请谨慎操作。

步骤1 登录华为云控制台。

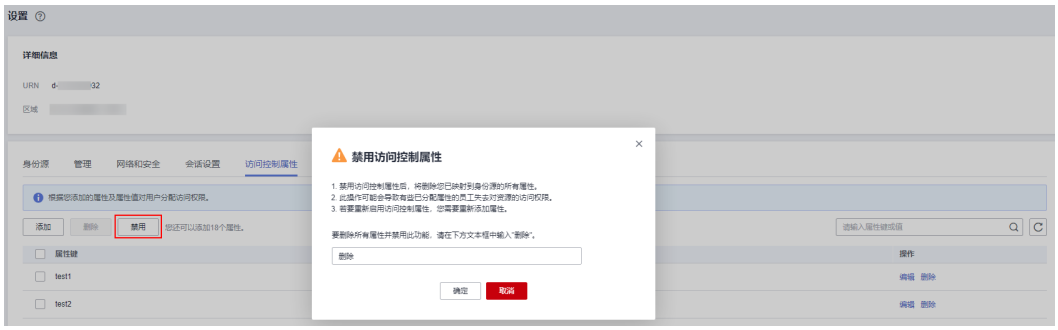
步骤2 单击页面左上角的 ☰ ，选择“管理与监管 > IAM身份中心”，进入“IAM身份中心”页面。

步骤3 单击左侧导航栏的“设置”，进入设置页面。

步骤4 在“访问控制属性”页签中单击“禁用”。

步骤5 在“禁用访问控制属性”确认框中，仔细阅读页面中禁用此功能的影响说明，确认清楚后在下方输入“删除”，然后单击“确定”。

图 3-32 禁用访问控制属性



----结束

3.4.3 为 ABAC 创建权限策略

概述

在您已为资源添加标签，并在IAM身份中心启用并配置访问控制属性后，您还需要在权限集的自定义身份策略中添加基于属性的访问控制规则。您可以通过**PrincipalTag**条件键在权限集中使用访问控制属性来创建访问控制规则，即在策略语句的Condition元素中写入"**g:ResourceTag/*tag-key***": "**${g:PrincipalTag/*tag-key*}**"。

- **g:ResourceTag/*tag-key***：全局级条件键，用于指定资源的标签键。您为资源添加标签后，需在此条件键中输入资源的标签键，也就是将***tag-key***替换为具体的资源标签键。
- **g:PrincipalTag/*tag-key***：全局级条件键，用于指定访问控制属性的属性键。您启用并添加访问控制属性后，需在此条件键中输入访问控制属性的属性键，也就是将***tag-key***替换为具体的属性键。

上述访问控制规则配置完成后，权限策略会根据您指定的资源标签键和属性键，对资源标签的值和属性值进行匹配校验，只有资源标签的值和属性值匹配成功的用户才会获得此权限集定义的资源访问权限。

策略示例

创建权限集的具体操作请参见：**创建权限集**。此处仅举例说明如何在权限集的自定义身份策略中添加基于属性的访问控制规则，以及策略示例。

例如您创建权限集时选择“OrganizationsFullAccessPolicy”系统策略，表示与此权限集关联的用户拥有组织服务的所有权限，但是您不希望某些用户拥有删除指定组织OU的权限，您可以在权限集的自定义身份策略中写入如下策略内容，表示拒绝用户进行删除指定组织OU的操作。

此自定义身份策略对哪些用户和资源生效由条件键控制，示例中的条件键表示资源的标签键为“orgtag1”，访问控制属性的属性键为“User_A”，最终策略评估时会将标签“orgtag1”的值与属性“User_A”的属性值进行匹配，例如您将“orgtag1”标签的值设置为“test1”，访问控制属性“User_A”的属性值选择“${user:name}”，那么只有用户名为“test1”的用户才会获得此策略定义的权限。

对于较为复杂的授权场景，如多用户与多资源授权，可参考如下说明：

- 如果您需要通过此策略授予某一用户多个资源的权限，那么您只需要为多个资源绑定相同的标签即可。

- 如果您需要通过此策略控制多个用户对某一资源的访问权限，那么您可以为此资源绑定多个标签，并在权限集的自定义身份策略中写入多个条件键，分别对应多个用户的属性即可。
- 如果您需要通过此策略控制多个用户多个资源的访问权限，您可以给多个资源添加标签键相同但标签值不同的标签，以此对应多个用户的属性。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "organizations:ous:delete"
      ],
      "Condition": {
        "StringEquals": {
          "g:ResourceTag/orgtag1": "${g:PrincipalTag/User_A}"
        }
      }
    }
  ]
}
```

3.4.4 支持配置的用户属性

IAM身份中心当前支持两种身份源：IAM身份中心和外部身份提供商。两种身份源当前支持实施ABAC的用户属性如下表所示。这些用户属性是可以在配置访问控制属性时选择的属性值，对应用户的基本信息、联系方式、工作相关信息和地址信息等，选择这些用户属性并给其赋予属性键，用于实施ABAC时进行访问控制决策。

如果使用外部身份提供商身份源，您在IAM身份中心和外部身份提供商处均可以设置实施ABAC的用户属性，如果在两处设置的ABAC属性的属性键相同，则优先以IAM身份中心设置的属性进行访问控制决策。

表 3-3 支持配置的用户属性

身份源	用户属性
IAM身份中心	${user:email}
	${user:familyName}
	${user:givenName}
	${user:middleName}
	${user:name}
	${user:displayName}
外部身份提供商	${path:userName}
	${path:name.familyName}
	${path:name.givenName}
	${path:displayName}
	${path:nickName}
	${path:emails[primary eq true].value}

身份源	用户属性
	${path:addresses[type eq "work"].streetAddress}
	${path:addresses[type eq "work"].locality}
	${path:addresses[type eq "work"].region}
	${path:addresses[type eq "work"].postalCode}
	${path:addresses[type eq "work"].country}
	${path:addresses[type eq "work"].formatted}
	${path:phoneNumbers[type eq "work"].value}
	${path:userType}
	${path:title}
	${path:locale}
	${path:timezone}
	${path:enterprise.employeeNumber}
	${path:enterprise.costCenter}
	${path:enterprise.organization}
	${path:enterprise.division}
	${path:enterprise.department}
	${path:enterprise.manager.value}

4 管理身份源

4.1 更改身份源

IAM身份中心支持基于SAML协议的单点登录，如果您已经有自己的企业管理系统，同时您的用户需要使用您账号内的云服务资源，您可以使用IAM的身份提供商功能，实现用户使用企业管理系统账号单点登录华为云，这一过程称之为联邦身份认证。关于IAM身份提供商的具体信息请参见：**身份提供商**。

IAM身份中心支持连接到基于SAML 2.0协议的外部身份提供商系统，例如微软AD和Okta，具体实现如下：

- 允许管理员将IAM身份中心使用的SAML 2.0协议连接到外部身份提供商系统。
- 支持通过SCIM协议自动化用户预置过程。管理员可以在外部身份提供商处管理用户，用户信息会自动同步到IAM身份中心，无需人工干预。
- 外部身份提供商用户可使用现有账号密码登录其门户，然后自动跳转至华为云来访问华为云账号下的资源，无需IAM身份中心管理员重新分配密码。

华为云当前支持两种身份源：IAM身份中心和外部身份提供商。在IAM身份中心可以切换两种身份源。

更改为外部身份提供商

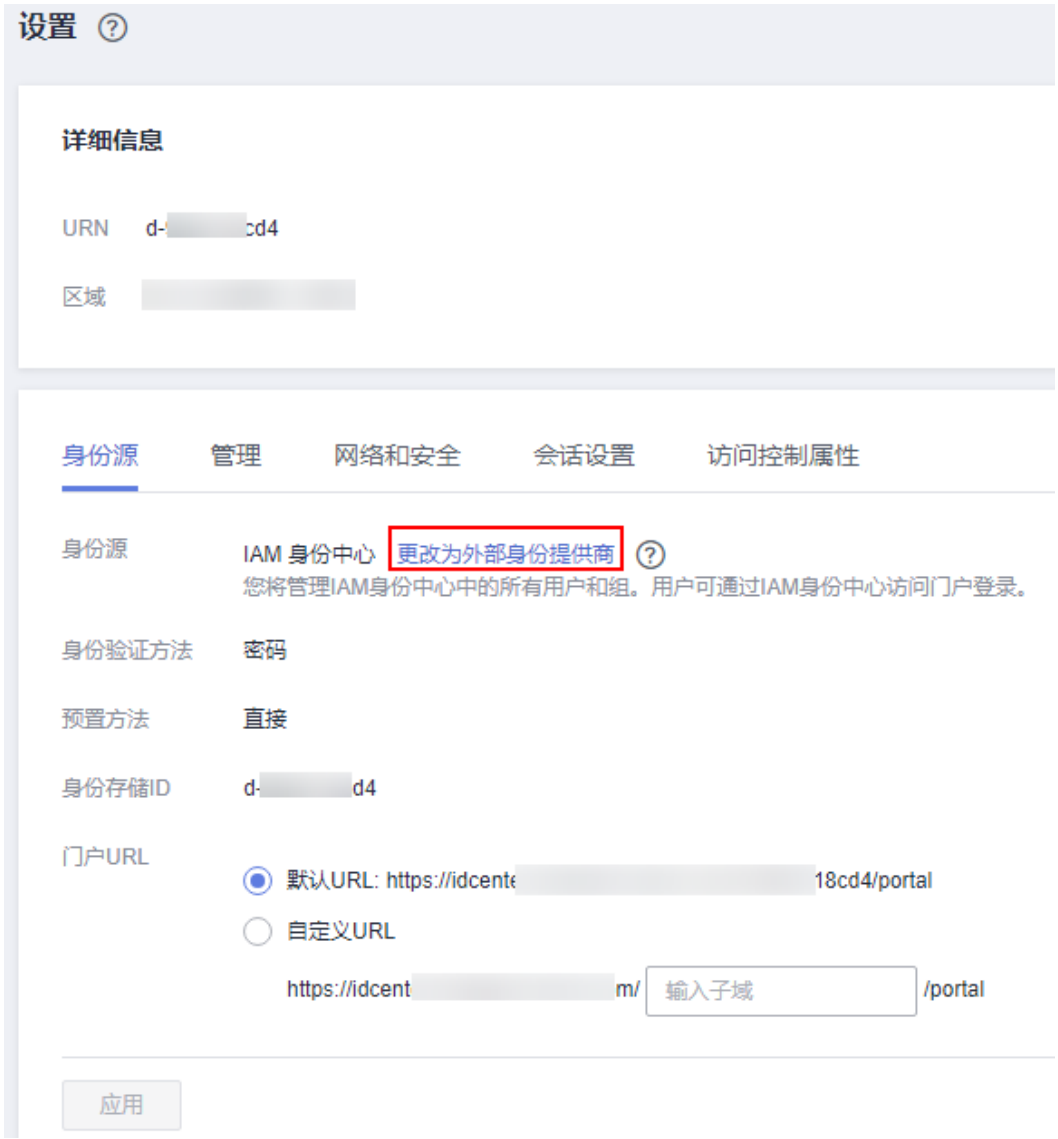
步骤1 登录**华为云控制台**。

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“设置”，进入设置页面。

步骤4 在“身份源”页签中单击“更改为外部身份提供商”，进入“更改身份源”页面。

图 4-1 更改为外部身份提供商



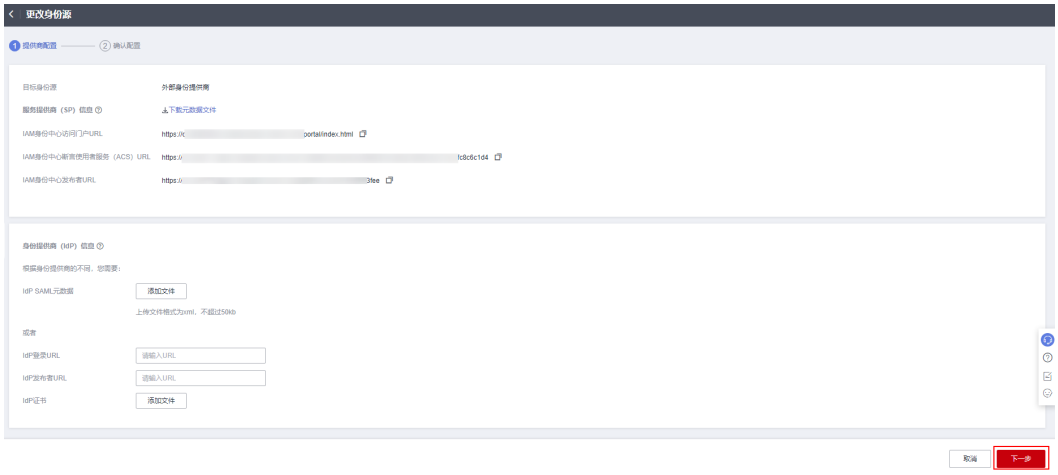
步骤5 在“提供商配置”页签中配置相关信息，配置完成，单击“下一步”。

- 服务提供商（SP）信息：

  单击“下载元数据文件”，下载元数据文件并将其保存在您的系统上。您的外部身份提供商需要上传IAM身份中心SAML元数据文件。

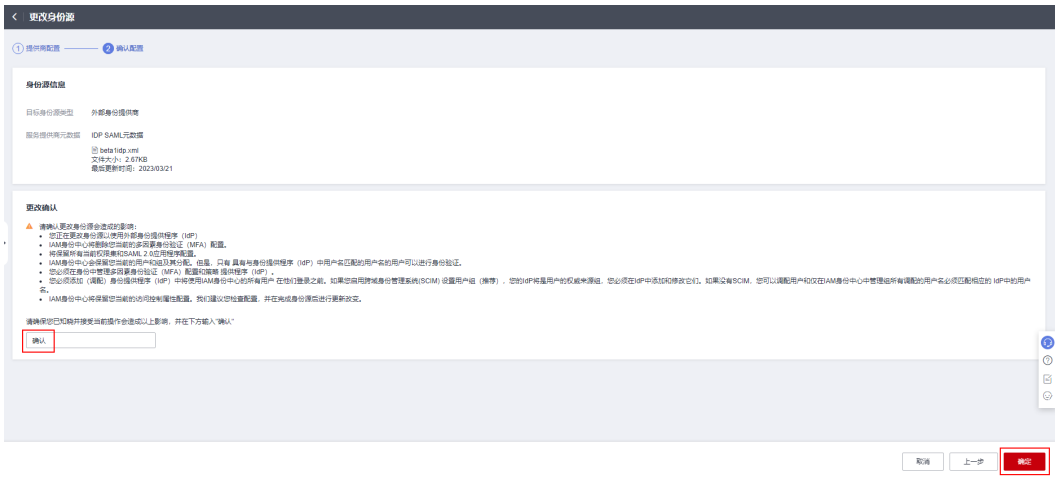
- 身份提供商（IdP）信息：
  - 在“IdP SAML元数据”后单击“添加文件”，上传您从外部身份提供商下载的SAML元数据文件。此元数据文件包含用于信任从IdP发送消息的证书。
  - 如您没有IdP SAML元数据文件，也可以输入IdP登录URL、IdP发布者URL和上传IdP证书。

图 4-2 提供商配置



步骤6 进入“配置确认”页签，请仔细阅读更改身份源会造成的影响，如您已知晓并接受当前操作会造成的影响，请在“更改确认”区域下方的确认框中输入“确认”，然后单击页面右下角的“确定”，身份源更改为外部身份提供商。

图 4-3 确认更改身份源



说明

身份源切换为外部身份提供商后，系统将支持SAML 2.0的身份验证方式，以及SCIM自动和手动的预置方法切换，具体请参见**外部身份提供商配置**。

----结束

更改为 IAM 身份中心

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。

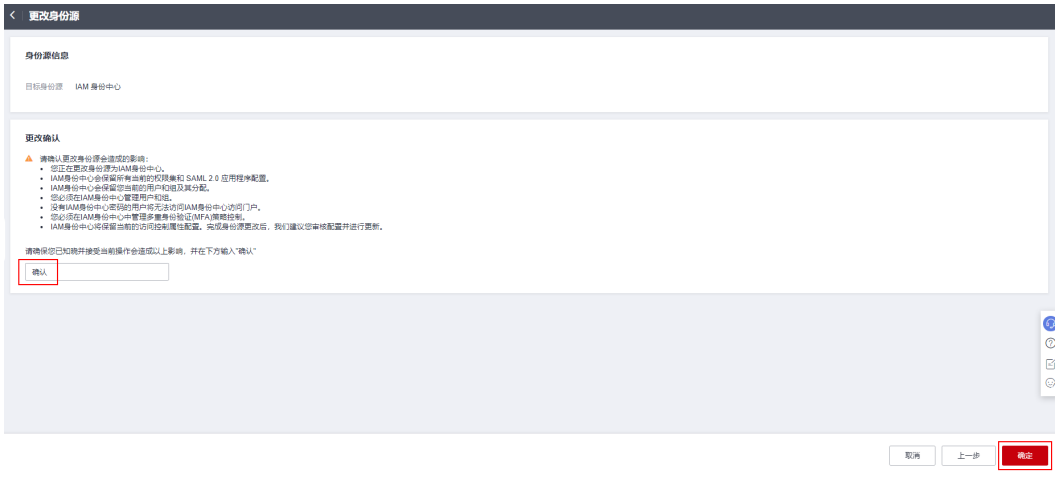
步骤3 单击左侧导航栏的“设置”，进入设置页面。

步骤4 在“身份源”页签中单击“更改为IAM身份中心”，进入“更改身份源”页面。

图 4-4 更改为 IAM 身份中心

步骤5 请仔细阅读更改身份源会造成的影响，如您已知晓并接受当前操作会造成的影响，请在“更改确认”区域下方的确认框中输入“确认”，然后单击页面右下角的“确定”，身份源更改为IAM身份中心。

图 4-5 确认更改身份源



----结束

4.2 自定义用户门户 URL

管理员开通IAM身份中心后，系统会自动生成唯一的用户门户URL，管理员可对此URL进行自定义修改，但仅支持修改一次，修改URL完成后，后续无法对其进行再次编辑。

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“设置”，进入设置页面。

步骤4 在“身份源”页签中选择“自定义URL”。

步骤5 输入自定义子域，单击“应用”，用户门户URL修改完成。

自定义子域的长度必须在1~62个字符之间，只能包含字母、数字和连字符，且必须以字母或数字开头和结尾。不能以“d-”开头。

图 4-6 自定义用户门户 URL

----结束

4.3 外部身份提供商配置

4.3.1 概述

SAML 2.0

安全断言标记语言（Secturity Assertion Markup Language 2.0，缩写为SAML 2.0）是一个由一组协议组成，用来传输安全声明的XML框架。SAML2.0是由标准化组织OASIS提出的用于安全操作的标准，是很多身份提供商（IdP）使用的一种开放标准，关于SAML2.0的详细描述请参见：**SAML 2.0技术概述**。IAM支持使用SAML2.0协议进行联邦身份认证，因此与华为云建立联邦身份认证的企业IdP必须支持SAML2.0协议。

IAM身份中心将SAML IdP功能添加到您的IAM身份中心存储或外部身份提供商应用程序，然后用户可以单点登录到支持SAML的服务，包括华为云管理控制台和第三方应用程序。但是SAML协议没有提供查询IdP来了解用户和用户组的方法，因此您必须将这些用户和用户组配置到IAM身份中心来获取这些用户和用户组。

SCIM

IAM身份中心为跨域身份管理系统（SCIM）v2.0标准提供支持。SCIM可以使IAM身份中心身份与来自身份提供商（IdP）的身份保持同步，包括在外部身份提供商中进行创建、更新、删除用户等。关于如何实现SCIM的更多信息，请参见**SCIM自动配置**。

4.3.2 修改 SAML2.0 配置

身份源切换为外部身份提供商后，您可以随时修改SAML2.0的配置。

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“设置”，进入“设置”页面。

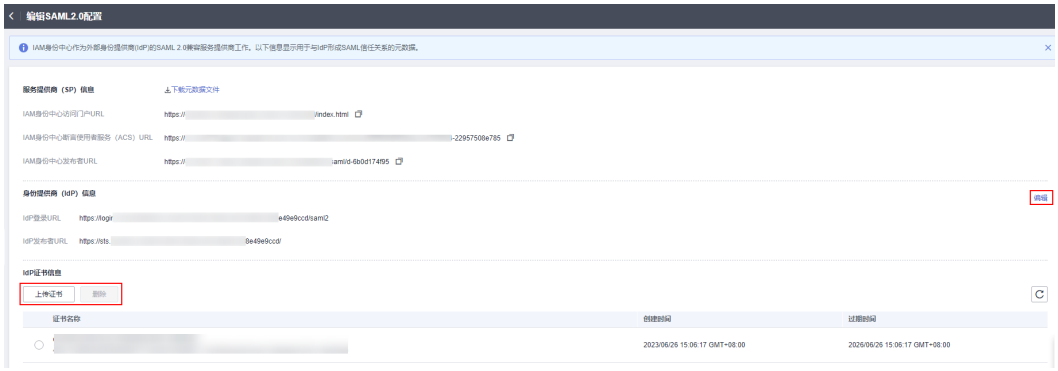
步骤4 在“身份源”页签中的“身份验证方法”列，单击“修改SAML2.0配置”。

步骤5 进入“编辑SAML2.0配置”页面，在“身份提供商（IdP）信息”区域右侧单击“编辑”。

步骤6 修改IdP登录URL和IdP发布者URL，单击“保存”。

步骤7 在“IdP证书信息”区域可查看证书信息，以及上传或删除证书，具体请参见**管理证书**。

图 4-7 编辑 SAML2.0 配置



----结束

4.3.3 SCIM 自动配置

IAM身份中心支持使用跨域身份管理系统（SCIM）v2.0协议将用户/用户组信息从身份提供商（IdP）自动配置（同步）到IAM身份中心。配置SCIM同步时，您可以创建身份提供商（IdP）用户属性到IAM身份中心命名属性的映射，这会让IAM身份中心和身份提供商（IdP）之间的预期属性相匹配。您可以使用在IAM身份中心生成SCIM端点和访问令牌在身份提供商（IdP）中配置此连接。

本章节包含如下内容：

- 启用自动配置
- 禁用自动配置
- 生成/删除访问令牌

启用自动配置

仅当身份源更改为外部身份提供商后，才支持配置此功能。

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“设置”，进入“设置”页面。

步骤4 在“身份源”页签中选择预置方法为“SCIM自动”，单击“应用”。

图 4-8 启用 SCIM 自动配置

步骤5 在弹出的入站自动配置对话框中，复制“SCIM端点”和“访问令牌”两个信息。在配置身份提供商（IdP）并创建信任关系时需要用到此信息。

访问令牌的信息仅在此弹窗中显示一次，后续无法再次查看，但是您可以随时生成新的令牌，具体请参见**生成/删除访问令牌**。

图 4-9 入站自动配置信息

步骤6 单击“关闭”。

----结束

禁用自动配置

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“设置”，进入“设置”页面。

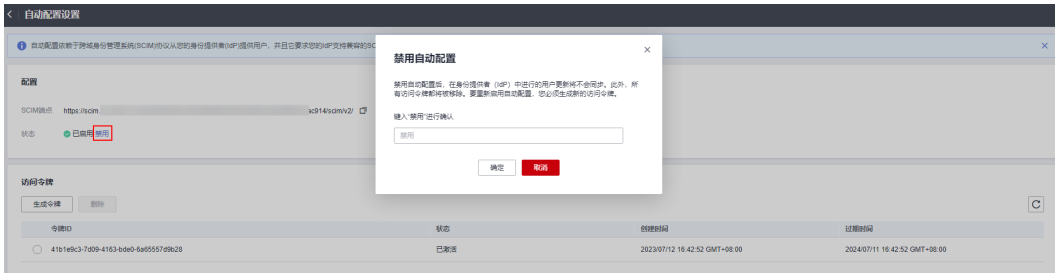
步骤4 在“身份源”页签中，单击预置方法列的“自动配置设置”进入“自动配置设置”页面。

图 4-10 自动配置设置

步骤5 单击状态列的“禁用”，在弹出的确认框中输入“禁用”，单击“确定”。

禁用自动配置后，在身份提供者（IdP）中进行的用户更新将不会同步。此外，所有访问令牌都将被移除。要重新启用自动配置，您必须生成新的访问令牌。

图 4-11 禁用自动配置



----结束

生成/删除访问令牌

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。

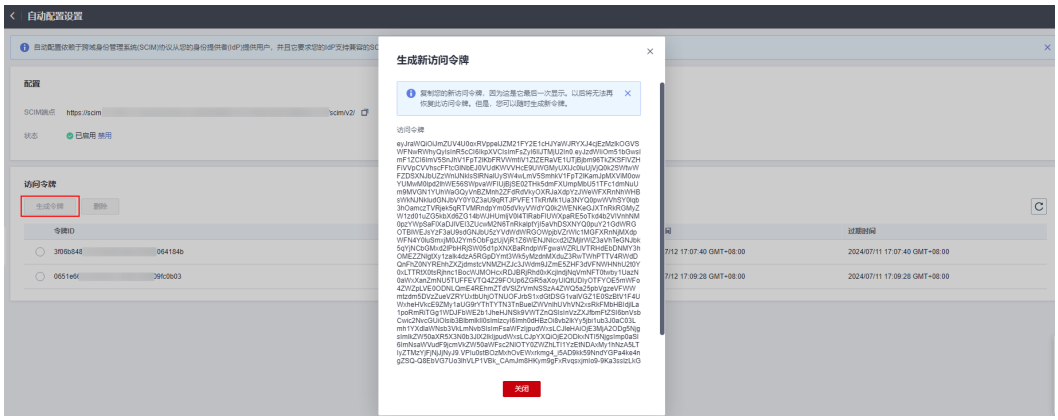
步骤3 单击左侧导航栏的“设置”，进入“设置”页面。

步骤4 在“身份源”页签中，单击预置方法列的“自动配置设置”进入“自动配置设置”页面。

图 4-12 自动配置设置

步骤5 单击“生成令牌”，系统弹出新的访问令牌信息。

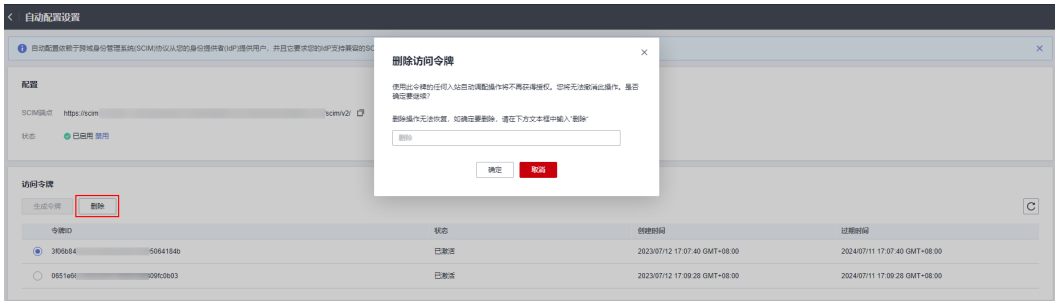
图 4-13 生成新访问令牌



步骤6 在访问令牌列表中选择需要删除的令牌，单击“删除”。

步骤7 在弹出的确认框中输入“删除”，单击“确定”。

图 4-14 删除访问令牌



说明

IAM身份中心最多支持同时存在两个访问令牌，如需生成额外的访问令牌，需删除其他过期或未使用的访问令牌。

----结束

4.3.4 手动配置

当某些外部身份提供商不支持跨域身份管理系统（SCIM），或具有不兼容的SCIM实现时，您需要通过IAM身份中心手动配置用户和用户组。创建用户时，请确保将用户名和邮件地址设置为与外部身份提供商中的一致；创建用户组则不需要与外部身份提供商中存在的群组一致。

操作步骤

当身份源更改为外部身份提供商后，预置方法默认为手动配置，如您需要从SCIM自动配置切换为手动配置，请参考以下步骤。

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“设置”，进入“设置”页面。

步骤4 在“身份源”页签中选择预置方法为“手动”，单击“应用”。

启用手动配置后，您就可以在IAM身份中心创建和管理用户/用户组，具体方法请参见用户管理和用户组管理。

图 4-15 启用手动配置

----结束

4.3.5 管理证书

IAM身份中心使用证书在IAM身份中心和外部身份提供商之间建立SAML信任关系。在切换身份源为外部身份提供商时，必须从外部身份提供商获得至少一个SAML 2.0证书。该证书通常包含在SAML元数据文件中，在切换身份源上传IdP SAML元数据时自动安装。

您可能需要定期导入证书，以便轮换身份提供商颁发的无效或过期证书，这有助于防止身份验证中断或停机。用新证书替换旧证书的过程称为证书轮换。所有导入的证书

都将自动激活，当前最多支持同时存在两个证书。只有在确保相关身份提供商不再使用证书后，才可以删除证书。

你还应该考虑到某些身份提供商可能不支持多个证书。在这种情况下，使用证书轮换可能意味着您的用户会暂时中断服务，证书轮换成功重新建立与该身份提供商的信任关系后，服务将恢复。因此建议在非高峰时段执行此操作。

说明

如果发现现有SAML证书出现泄露或处理不当的迹象时，应立即删除并轮换该证书。

证书轮换

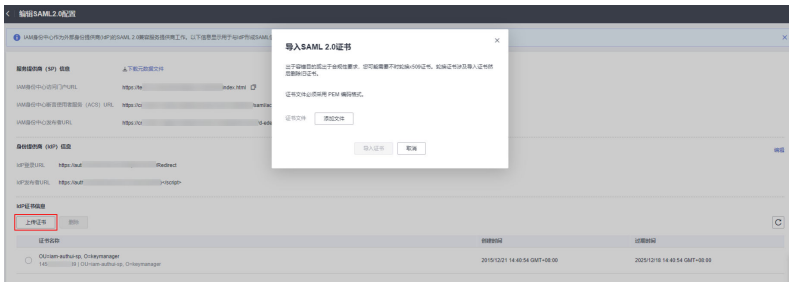
步骤1 从外部身份提供商处获取新证书。

前往外部身份提供商网站下载SAML 2.0证书，确保是以PEM编码格式下载证书文件。大多数身份提供商都允许创建多个SAML 2.0证书，它们很可能会被标记为已禁用或未激活状态。

步骤2 将新证书导入IAM身份中心。

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. 单击左侧导航栏的“设置”，进入“设置”页面。
4. 在“身份源”页签中的“身份验证方法”列，单击“修改SAML2.0配置”。
5. 进入“编辑SAML2.0配置”页面，单击“上传证书”。
6. 在“导入SAML 2.0证书”对话框中，单击“添加文件”，选择从步骤1中获取的新证书，然后单击“导入证书”。

图 4-16 导入证书



此时，IAM身份中心将信任通过您导入的两个证书签名的所有传入的SAML消息。

步骤3 在外部身份提供商中激活新证书。

返回外部身份提供商网站并将您之前创建的新证书标记为主证书或已激活证书。此时，所有由外部身份提供商签名的SAML消息都应使用新证书。

步骤4 删除旧证书。

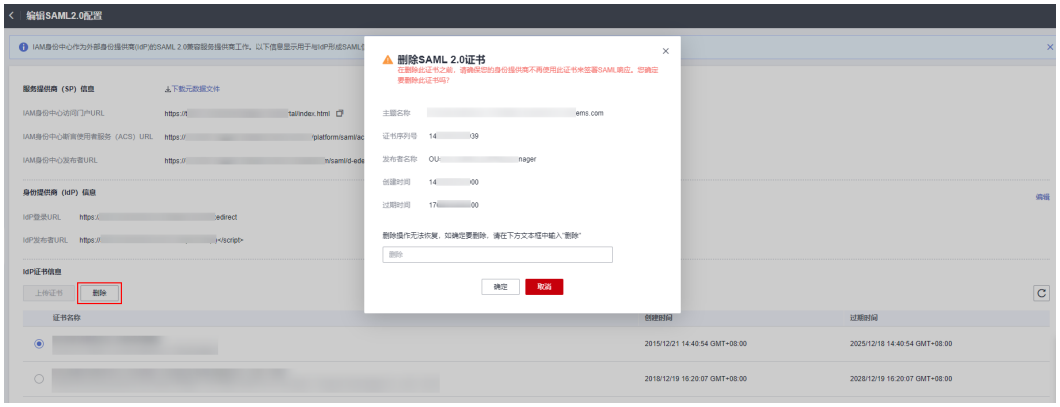
说明

在删除证书之前，请确保外部身份提供商不再使用此证书来签署SAML响应。

证书列表中必须始终存在至少一个有效证书，并且不能将其删除。

1. 进入“编辑SAML2.0配置”页面，在证书列表中选择需要删除的证书，单击“删除”。
2. 在“删除SAML 2.0 证书”对话框中，输入“删除”，然后单击 “确定”。

图 4-17 删除证书



3. 返回外部身份提供商网站，执行相关操作删除较旧的证书。

----结束

4.4 常用的身份提供商

4.4.1 微软 AD

IAM身份中心支持使用跨域身份管理系统（SCIM）v2.0协议将用户/用户组信息从微软AD自动配置（同步）到IAM身份中心。您可以使用IAM身份中心生成的SCIM端点和访问令牌在微软AD中配置此连接。配置SCIM同步时，您可以在微软AD中创建用户属性与IAM身份中心中的命名属性的映射，这会使IAM身份中心和微软AD之间的预期属性相匹配。

4.4.2 Okta

IAM身份中心支持使用跨域身份管理系统（SCIM）v2.0协议将用户和用户组信息从Okta自动配置（同步）到IAM身份中心。您可以使用IAM身份中心生成的SCIM端点和访问令牌在Okta中配置此连接。配置SCIM同步时，您可以在Okta中创建用户属性与IAM身份中心中的命名属性的映射，这会使IAM身份中心和Okta之间的预期属性相匹配。

5 重置 IAM 身份中心

如果您不再需要使用IAM身份中心，或需要从头开始创建新配置，或需要在其他区域启用IAM身份中心，您可以删除IAM身份中心配置的所有数据。

由于IAM身份中心为项目级服务，您在当前区域启用IAM身份中心后，如需在其他区域使用，则需要删除当前区域的IAM身份中心数据，然后才可以在其他区域重新开通并使用IAM身份中心。

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“设置”，进入设置页面。

步骤4 在“管理”页签中单击“删除”。

步骤5 在弹出的确认框中勾选全部确认项，并根据提示输入此IAM身份中心的实例ID，单击“确定”，IAM身份中心配置删除成功。

图 5-1 删除 IAM 身份中心配置

说明

此操作将删除此IAM身份中心配置中的所有数据，且不可恢复，请谨慎使用。

----结束

6 多因素认证（MFA）

6.1 多因素认证概述

什么是多因素认证

多因素认证Multi-Factor Authentication（MFA）是一种非常简单的安全实践方法，它能够在用户名称和密码之外再额外增加一层保护。启用多因素认证后，用户进行操作时，除了需要提供用户名和密码外（第一次身份验证），还需要提供验证码（第二次身份验证），多因素身份认证结合起来将为您的账号和资源提供更高的安全保护。

IAM身份中心的多因素认证主要应用在登录验证中，开启了登录验证功能后，用户登录控制台时，除了需要输入用户名和密码外，还需要在登录验证页面输入多因素认证设备中的验证码，再次确认登录者身份，进一步提高账号安全性。

多因素认证支持的设备

IAM身份中心当前支持如下多因素认证设备：

- 身份验证器应用程序：

  即虚拟MFA设备。虚拟Multi-Factor Authentication (MFA) 是能产生6位数字认证码的设备，遵循基于时间的一次性密码 （TOTP）标准。MFA设备可以基于硬件也可以基于软件，目前仅支持基于软件的虚拟MFA，即虚拟MFA应用程序，可以在移动硬件设备（包括智能手机）上运行，非常方便。

- 安全密钥：

  安全密钥是兼容FIDO2的外部硬件身份验证器，您可以购买并通过USB、BLE或NFC连接到设备。当您被提示输入MFA时，您只需通过触摸YubiKey等硬件安全密钥来验证身份即可。安全密钥包括YubiKey等密钥，最常见的安全密钥包括YubiKey等会创建一个设备绑定的FIDO凭证。

  FIDO2是基于公钥密码学的标准，它包含了CTAP2和WebAuthn标准。FIDO凭证具有防网络钓鱼功能，因为它对于网站来说具有唯一性。

6.2 多因素认证（MFA）

6.2.1 启用 MFA

您可以参考以下步骤在IAM身份中心控制台启用多因素认证（MFA）。

说明

如果将身份源切换为外部身份提供商，此功能需在外部身份提供商处管理和配置，在IAM身份中心将不会看到 “网络和安全” 页签。

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“设置”，进入设置页面。

步骤4 选择 “网络和安全” 页签。

步骤5 在“提示用户进行MFA”部分，根据业务所需的安全级别选择以下身份验证模式之一：

- 仅当登录环境发生变化时（环境感知）

  选择此模式后，IAM身份中心为用户提供在登录期间信任其设备的选项。用户登录期间勾选“是否信任此设备”选项后，IAM身份中心会提示用户输入MFA验证码一次，并分析用户后续登录的登录上下文（如设备、浏览器和IP地址）。后续登录时，如果用户的登录上下文未更改，将不触发MFA认证；如果用户的登录上下文更改，将提示用户进行MFA认证。

  此模式为经常从工作场所登录的用户提供了易用性，因此用户不需要在每次登录时完成MFA认证。只有在登录上下文更改时，才会提示用户进行MFA认证。

  说明

  设备的信任记录有效时长为7天，选择信任设备7天后，需重新进行MFA认证。

- 每次登录时（始终开启）

  选择此模式后，IAM身份中心要求具有注册MFA设备的用户每次登录时都会得到提示。如果您的组织或合规性策略要求用户每次登录用户门户时完成MFA认证，则应使用此模式。

- 从不（禁用）

  选择此项将禁用MFA。所有用户仅使用标准用户名和密码登录。

图 6-1 启用 MFA

步骤6 单击“应用”。

----结束

6.2.2 选择 MFA 验证类型

您可以参考以下步骤配置用户在访问用户门户时可以进行多因素认证（MFA）的设备类型。

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“设置”，进入设置页面。

步骤4 选择 “网络和安全” 页签。

步骤5 在“MFA验证类型”部分，根据业务需求选择以下MFA类型，支持同时选择两种MFA类型。更多信息请参见多因素认证支持的设备。

- 身份验证器应用程序
- 安全密钥

图 6-2 选择 MFA 验证类型

步骤6 单击“应用”。

----结束

6.2.3 配置 MFA 强制执行

您可以参考以下步骤配置用户在访问用户门户时是否必须拥有已注册的多因素认证（MFA）设备。

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“设置”，进入设置页面。

步骤4 选择 “网络和安全” 页签。

步骤5 在“如果用户没有已注册的MFA设备”部分，根据业务需要选择用户登录时是否必须拥有已注册的MFA设备。

- 要求在登录时注册MFA设备

  如果您希望要求尚未注册MFA设备的用户在成功进行密码身份验证后，在登录期间自行注册设备，请使用此选项。如何注册MAF设备请参见注册MFA设备。

- 阻止登录

  强制每个用户在登录时使用MFA设备验证，否则将阻止其登录。

- 允许登录

选择此项表示用户不需要MFA设备验证即可登录用户门户。

图 6-3 配置 MFA 强制执行

步骤6 单击“应用”。

----结束

6.2.4 允许用户自行注册 MFA 设备

您可以参考以下步骤允许用户可以自行添加和管理自己的多因素认证（MFA）设备。

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“设置”，进入设置页面。

步骤4 选择 “网络和安全” 页签。

步骤5 在“是否允许用户自己管理”部分，选择是否允许用户管理自己的MFA设备，启用此功能后，用户可以自行添加和管理自己的MFA设备。

图 6-4 允许用户自行注册 MFA 设备

步骤6 单击“应用”。

----结束

6.3 管理多因素认证（MFA）

6.3.1 注册 MFA 设备

您必须具有对用户MFA设备的物理访问权限才能注册该设备。例如，您需要为在智能手机上运行MFA设备的用户配置MFA，在这种情况下，您必须有用户的智能手机才能完成该向导。因此建议允许用户可以自行添加和管理自己的MFA设备，具体请参见**允许用户自行注册MFA设备**。

注册 MFA 设备

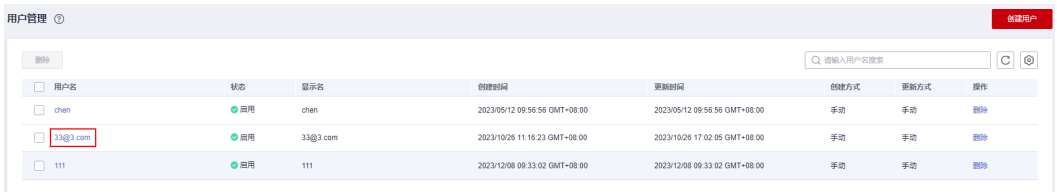
步骤1 登录**华为云控制台**。

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 在用户列表中，单击用户名，进入用户信息详情页。

图 6-5 选择用户



步骤5 选择用户详情页下方的“MFA设备”页签，单击“注册MFA设备”。

图 6-6 注册 MFA 设备

步骤6 系统跳转至注册MFA页面，选择以下MFA设备类型之一，然后根据说明进行操作。

- 身份验证器应用程序

  在“绑定虚拟MFA”页面上将显示新MFA设备的配置信息，包括二维码图形等。根据界面提示完成如下操作：

  a. 在手机上安装支持虚拟MFA的应用，如华为云App。

  b. 您可以通过扫描二维码、手动输入两种方式绑定MFA设备，下面以“华为云”手机应用程序为例绑定虚拟MFA：

     - 扫描二维码

       打开手机上已安装好的“华为云”手机应用程序，选择“控制台-MFA-添加-扫码添加”，扫描“绑定虚拟MFA”弹窗中的二维码。扫描成功后，“华为云”手机应用程序会自动添加用户，虚拟MFA列表中出现账号/IAM用户名及对应的MFA动态码。

     - 手动输入

       打开手机上已安装好的“华为云”手机应用程序，选择“控制台-MFA-添加-手动输入”。账号绑定虚拟MFA，输入账号和密钥；IAM用户绑定虚拟MFA，输入IAM用户名和密钥。单击“添加”手动添加用户。

       说明

       手动输入添加用户方式只支持基于时间模式，建议在移动设备中开启自动设置时间功能。

  c. 添加用户完成，在“华为云”手机应用程序“虚拟MFA页面”，查看虚拟MFA的动态口令页面。动态口令每30秒自动更新一次。

  d. 在“绑定虚拟MFA”页面输入动态码。

  e. 单击“确定”，完成绑定虚拟MFA设备的操作。

- 安全密钥

  在 “注册安全密钥” 页面上，根据浏览器或平台显示的说明进行操作。

说明

- 此处的体验因不同的操作系统和浏览器而异，因此请按照浏览器或平台显示的说明进行操作。
- 当您同时注册“身份验证器应用程序”和“安全密钥”两种类型的MFA设备，用户在登录用户门户需要进行MFA验证时以验证安全密钥设备优先，身份验证器应用程序其次。

----结束

6.3.2 管理用户的 MFA 设备

当您需要重命名或删除用户的MFA设备时，请参见以下步骤。

重命名 MFA 设备

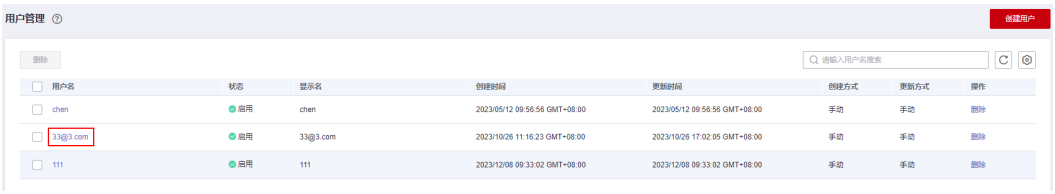
步骤1 登录华为云控制台。

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 在用户列表中，单击用户名，进入用户信息详情页。

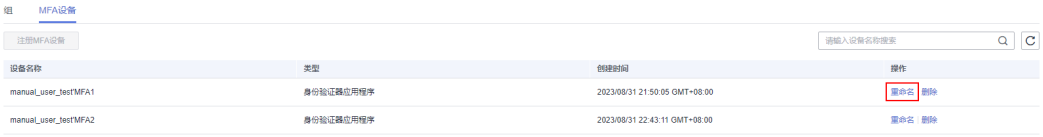
图 6-7 选择用户



步骤5 在“MFA设备”页签中，单击MFA设备操作列的“重命名”。

步骤6 输入新的MFA设备名称，单击“确定”。

图 6-8 重命名 MFA 设备



----结束

删除 MFA 设备

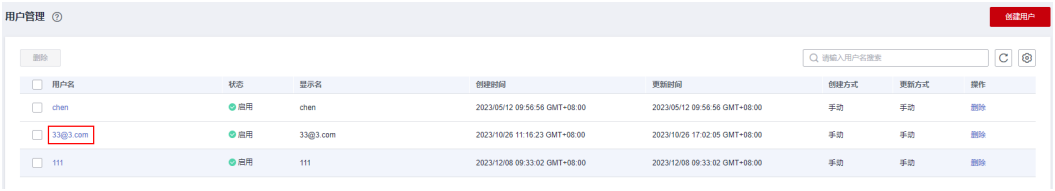
步骤1 登录华为云控制台。

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 在用户列表中，单击用户名，进入用户信息详情页。

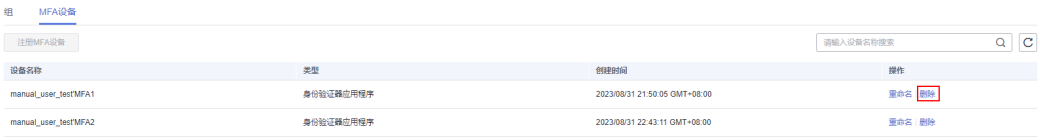
图 6-9 选择用户



步骤5 在“MFA设备”页签中，单击MFA设备操作列的“删除”。

步骤6 在弹出的确认框中单击“确定”，MFA设备删除完成。

图 6-10 删除 MFA 设备



----结束

7 权限管理

7.1 创建 IAM 用户并授权使用 IAM 身份中心

如果您需要对您所拥有的IAM身份中心服务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），通过IAM，您可以：

- 根据企业的业务组织，在您的账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用IAM身份中心资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将IAM身份中心资源委托给更专业、高效的其他账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果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IAM身份中心服务的其它功能。

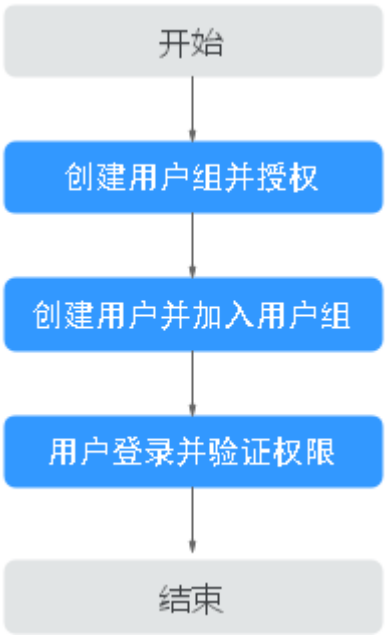
本章节为您介绍对用户授权的方法，操作流程如**图1**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的IAM身份中心权限，并结合实际需求进行选择，IAM身份中心支持的系统权限，请参见：**权限管理**。若您需要对除IAM身份中心之外的其它服务授权，IAM支持服务的所有权限请参见**系统权限**。

示例流程

图 7-1 给用户授予 IAM 身份中心权限流程



1. **创建用户组并授权**
   在IAM控制台创建用户组，并授予IAM身份中心只读权限“**IdentityCenter ReadOnlyAccess**”。
2. **创建用户并加入用户组**
   在IAM控制台创建用户，并将其加入**1**中创建的用户组。
3. **用户登录**并验证权限
   新创建的用户登录控制台，验证IAM身份中心的“**IdentityCenter ReadOnlyAccess**”权限。

7.2 创建 IAM 身份中心自定义策略

如果系统预置的IAM身份中心权限，不满足您的授权要求，可以创建自定义策略。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的IAM身份中心自定义策略样例。

IAM 身份中心自定义策略样例

- 示例1：授权用户创建权限集

```
{
    "Version": "1.1",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "IdentityCenter:permissionSet:create"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:delegatedAdministrators:list"
      ]
    }
  ]
}
```

- 示例2：拒绝用户删除权限集

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循**Deny优先原则**。

  如果您给用户授予IdentityCenter FullAccess的系统策略，但不希望用户拥有IdentityCenter FullAccess中定义的删除权限集权限，您可以创建一条拒绝删除权限集的自定义策略，然后同时将IdentityCenter FullAccess和拒绝策略授予用户，根据Deny优先原则，则用户可以对IAM身份中心执行除了删除权限集外的所有操作。拒绝策略示例如下：

  ```
  {
    "Version": "1.1",
    "Statement": [
      {
        "Effect": "Deny",
        "Action": [
          "IdentityCenter:permissionSet:delete"
        ]
      }
    ]
  }
  ```

- 示例3：多个授权项策略

  一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下：

  ```
  {
    "Version": "1.1",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "IdentityCenter:permissionSet:delete",
          "IdentityCenter:user:create",
          "IdentityCenter:permissionSet:create"
        ]
      },
      {
        "Effect": "Allow",
        "Action": [
          "organizations:delegatedAdministrators:list"
        ]
      }
    ]
  }
  ```


8 审计

8.1 支持审计的关键操作

通过云审计服务，您可以记录与IAM身份中心相关的操作事件，便于日后的查询、审计和回溯。

表 8-1 云审计支持的 IAM 身份中心操作列表

操作名称	资源类型	事件名称
开通IAM身份中心服务	Instance	StartIdentityCenter
关闭IAM身份中心服务	Instance	DeleteIdentityCenter
注册Region	Instance	RegisterRegion
更新单点登录配置	Instance	UpdateSsoConfiguration
更新身份存储的MFA设备管理配置	Instance	UpdateMfaDeviceManagementForIdentityStore
添加自定义域名	Instance	CreateAlias
启用指定实例的访问控制功能	Instance	CreateInstanceAccessControlAttributeConfiguration
解除指定实例的访问控制属性配置	Instance	DeleteInstanceAccessControlAttributeConfiguration
更新指定实例的访问控制属性配置	Instance	UpdateInstanceAccessControlAttributeConfiguration
使用指定的权限集为指定账号分配对主体（用户/用户组）的访问权限	AccountAssignment	CreateAccountAssignment

操作名称	资源类型	事件名称
使用指定的权限集从指定账号删除主体的访问权限	AccountAssignment	DeleteAccountAssignment
解除用户或用户组绑定的所有权限集	AccountAssignment	DisassociateProfile
在指定的IAM身份中心实例中创建权限集	PermissionSet	CreatePermissionSet
删除指定的权限集	PermissionSet	DeletePermissionSet
更新指定的权限集	PermissionSet	UpdatePermissionSet
将系统管理策略附加到权限集	PermissionSet	AttachManagedPolicyToPermissionSet
将附加的系统策略从指定的权限集中移除	PermissionSet	DetachManagedPolicyFromPermissionSet
将系统管理角色附加到权限集	PermissionSet	AttachManagedRoleToPermissionSet
将附加的系统角色从指定的权限集中分离	PermissionSet	DetachManagedRoleFromPermissionSet
将指定权限集预分配给指定账号	PermissionSet	ProvisionPermissionSet
删除指定权限集中的自定义策略	PermissionSet	DeleteCustomPolicy
将自定义策略附加到权限集	PermissionSet	PutCustomPolicy
用户登录后为用户生成凭证	User	Authenticate
激活设备授权码	User	ActiveDevice
取消设备授权码	User	CancelDevice
创建用户	User	CreateUser
删除用户	User	DeleteUser
更新用户	User	UpdateUser
停用用户	User	DisableUser
启用用户	User	EnableUser
创建MFA设备	User	CreateMfaDeviceForUser
删除绑定的MFA设备	User	DeleteMfaDeviceForUser
更新MFA信息	User	UpdateMfaDeviceForUser

操作名称	资源类型	事件名称
通过电子邮件发送密码重置链接或生成用户的一次性密码	User	UpdatePwdMode
重置用户密码	User	ResetPassword
通过电子邮件发送验证邮箱的链接	User	VerifyEmail
更新邮箱验证状态	User	UpdateEmailStatus
创建用户组	Group	CreateGroup
删除用户组	Group	DeleteGroup
更新用户组	Group	UpdateGroup
创建用户组关联关系	GroupMembership	CreateGroupMembership
删除用户组关联关系	GroupMembership	DeleteGroupMembership
批量绑定用户和组	GroupMembership	BatchCreateMembership
批量删除用户和组的绑定关系	GroupMembership	BatchDeleteMembership
批量替换用户和组的绑定关系	GroupMembership	BatchReplaceMembership
创建外部身份提供商目录配置	IdP	CreateExternalIdPConfigurationForDirectory
启用外部身份提供商	IdP	EnableExternalIdPConfigurationForDirectory
删除外部身份提供商目录配置	IdP	DeleteExternalIdPConfigurationForDirectory
停用外部身份提供商	IdP	DisableExternalIdPConfigurationForDirectory
更新外部身份提供商目录配置	IdP	UpdateExternalIdPConfigurationForDirectory
删除证书	IdP	DeleteExternalIdPCertificate
导入证书	IdP	ImportExternalIdPCertificate
创建承载令牌	IdP	CreateBearerToken
创建身份源对应的租户信息	IdP	CreateProvisioningTenant
删除承载令牌	IdP	DeleteBearerToken

操作名称	资源类型	事件名称
删除身份源对应的租户信息	IdP	DeleteProvisioningTenant

8.2 查询审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录：

- **在新版事件列表查看审计事件**
- **在旧版事件列表查看审计事件**

使用限制

- 单账号跟踪的事件可以通过云审计控制台查询。多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。
- 用户通过云审计控制台只能查询最近7天的操作记录。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务(OBS)，才可在OBS桶里面查看历史文件。否则，您将无法追溯7天以前的操作记录。
- 云上操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。

在新版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ☰ ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
   - 事件名称：输入事件的名称。
   - 事件ID：输入事件ID。
   - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
   - 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
   - 云服务：在下拉框中选择对应的云服务名称。
   - 资源类型：在下拉框中选择对应的资源类型。
   - 操作用户：在下拉框中选择一个或多个具体的操作用户。

- 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
  - normal：表示操作成功。
  - warning：表示操作失败。
  - incident：表示比操作失败更严重的情况，例如引起其他故障等。
- 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近1周内任意时间段的操作事件。

5. 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
   - 在搜索框中输入任意关键字，单击 按钮，可以在事件列表搜索符合条件的数据。
   - 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击 按钮，可以获取到事件操作记录的最新信息。
   - 单击 按钮，可以自定义事件列表的展示信息。启用表格内容折行开关 ，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。
6. 关于事件结构的关键字段详解，请参见**事件结构**和**事件样例**。
7. （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

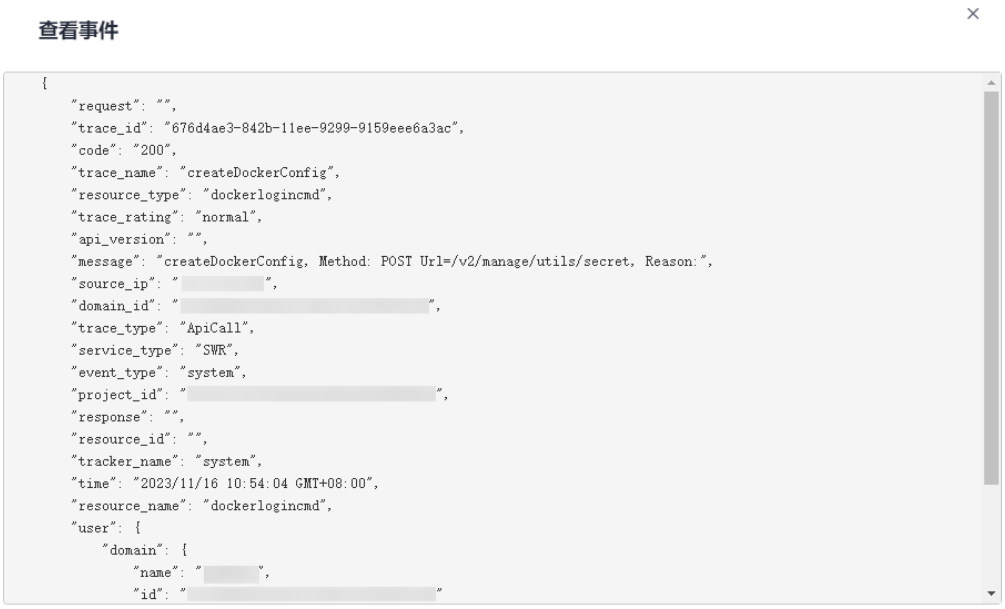
在旧版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
   - 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
     - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
     - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。
     - 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。
   - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
   - 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。

- 时间范围：可选择查询最近7天内任意时间段的操作事件。
- 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。

6. 选择完查询条件后，单击“查询”。
7. 在事件列表页面，您还可以导出操作记录文件和刷新列表。
   - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击按钮，可以获取到事件操作记录的最新信息。
8. 在需要查看的事件左侧，单击 展开该记录的详细信息。

9. 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。



10. 关于事件结构的关键字段详解，请参见**事件结构**和**事件样例**。
11. （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

9 调整配额

什么是配额?

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少个IAM身份中心用户、用户组等。IAM身份中心的配额请参见**约束与限制**。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

如何申请扩大配额?

1. 登录管理控制台。
2. 在页面右上角，选择“资源 > 我的配额”。
   系统进入“服务配额”页面。

   图 9-1 我的配额

3. 单击“申请扩大配额”。
4. 在“新建工单”页面，根据您的需求，填写相关参数。
   其中，“问题描述”项请填写需要调整的内容和申请原因。
5. 填写完毕后，勾选协议并单击“提交”。

10 修订记录

发布日期	修订记录
2024-02-20	第三次正式发布。 本次变更如下： • 新增**管理权限集标签**。 • 更新**创建权限集**、**查看或修改权限集**。 • 新增**基于属性的访问控制（ABAC）**。
2023-11-24	第二次正式发布。 本次变更如下： • **创建用户**时新增可选填的用户信息项。 • 新增**配置用户门户会话的持续时间**。 • **多因素认证（MFA）**设备新增“安全密钥”设备类型。
2023-06-30	第一次正式发布。