天翼云•统一身份认证

用户使用指南

天翼云科技有限公司

目 录

1 产品简介

1.1 统一身份认证

统一身份认证（Identity and Access Management，简称 IAM）服务，是提供用户身份认证、权限分配、访问控制等功能的身份管理服务。

IAM 服务申请开通后免费使用，您只需要为您帐号中的资源进行付费。

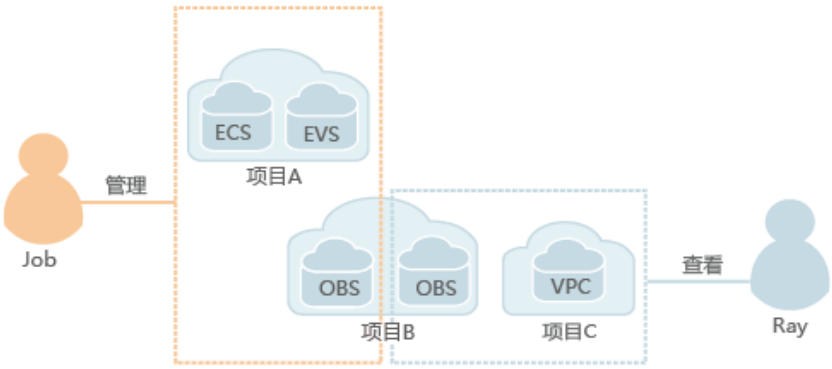
1.2 产品优势

IAM 可为您提供身份认证、权限管理和用户授权等统一身份认证服务：

- 精细的权限管理

  您可以通过 IAM 控制不同用户具备不同的权限。例如：控制某些用户可以配置弹性云主机参数，而让另外一些用户只能读取弹性云主机参数。

  图1-1 权限管理模型



- 便捷的用户授权

  使用 IAM 完成用户授权仅需要两步：

  a. 按照用户职责规划用户组，并将对应职责的权限授予用户组。

b. 将用户加入用户组。

- 为其他服务提供认证和鉴权功能

  使用 IAM 认证后的用户可以根据权限使用天翼中的其他服务，如：关系型数据库、云主机、对象存储等。

- 委托第三方账号或者云服务管理资源

  通过委托信任机制，天翼云用户可以将自己的操作权限委托给其它天翼云账号或者云服务，该账号或者云服务可以代维管理用户的资源。

1.3 产品功能

IAM 为您提供的主要功能包括：精细的权限管理、安全访问、通过用户组批量管理用户权限、委托其他帐号或者云服务管理资源等。

精细的权限管理

使用 IAM，您可以将帐号内不同的资源按需分配给创建的 IAM 用户，实现精细的权限管理。

安全访问

您可以使用 IAM 为用户或者应用程序生成身份凭证，不必与其他人员共享您的帐号密码，系统会通过身份凭证中携带的权限信息允许用户安全地访问您帐号中的资源。

通过用户组批量管理用户权限

您不需要为每个用户进行单独的授权，只需规划用户组，并将对应权限授予用户组，然后将用户添加至用户组中，用户就继承了用户组的权限。如果用户权限变更，只需在用户组中删除用户或将用户添加进其他用户组，实现快捷的用户授权。

委托其他帐号或者云服务管理资源

通过委托信任功能，您可以将自己的操作权限委托给其他天翼云帐号或者云服务，这些帐号或者云服务可以根据权限代替您进行日常工作。

1.4 基本概念

使用 IAM 服务时常用的基本概念包括：帐号、IAM 用户、帐号与 IAM 用户的关系、用户组、授权、权限、项目、委托、身份凭证。

账号

当您首次使用天翼云时注册的帐号，该帐号是您的天翼云资源归属、资源使用计费的主体，对其所拥有的资源及云服务具有完全的访问权限，可以重置用户密码、分配子用户权限。

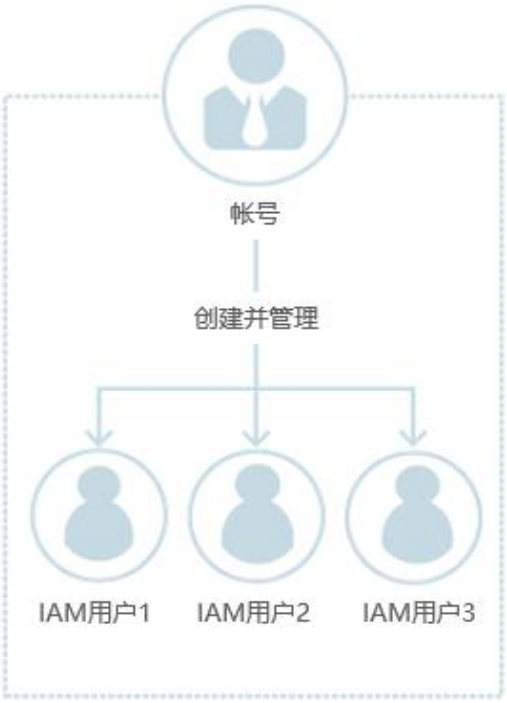
帐号不能在 IAM 中修改和删除，您可以在天翼云网门户“个人中心”修改帐号信息，如果您需要删除帐号，可以在“个人中心”进行注销。

IAM 用户

由帐号在 IAM 中创建的用户，一般为具体云服务的使用人员，具有独立的身份凭证（密码和访问密钥），根据帐号授予的权限使用资源。

帐号与 IAM 用户可以类比为父子关系，帐号是资源归属以及计费主体，对其拥有的资源具有所有权限。IAM 用户由帐号创建，只能拥有帐号授予的资源使用权限，帐号可以随时修改或者撤销 IAM 用户的使用权限。IAM 用户进行资源操作时产生的费用统一计入帐号中，IAM 用户不需要为资源付费。

图1-2 天翼云账号与 IAM 用户



身份凭证

身份凭证是识别用户身份的依据，您通过控制台或者 API 访问天翼云时，需要使用身份凭证来进行系统的认证鉴权。身份凭证包括密码和访问密钥，您可以在 IAM 中管理自己以及帐号中 IAM 用户的身份凭证。

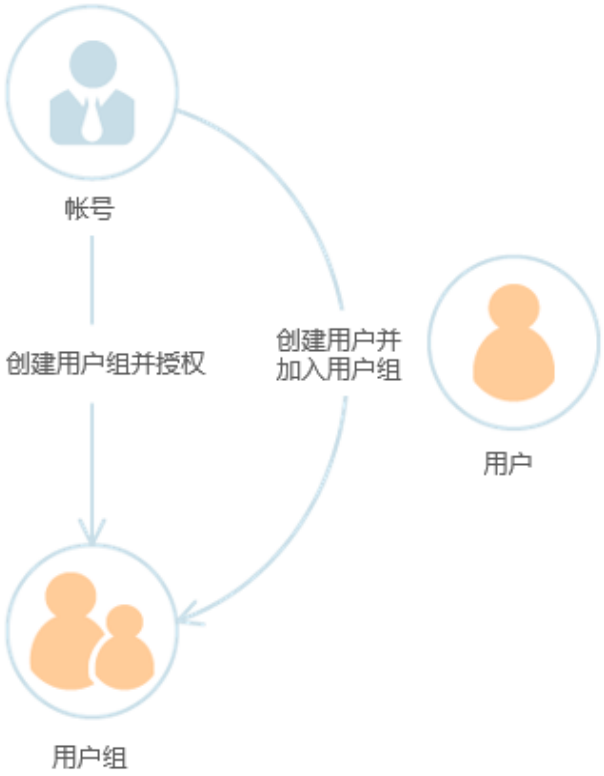
- 密码：常见的身份凭证，密码可以用来登录控制台。
- 访问密钥：即 AK/SK（Access Key ID/Secret Access Key），调用天翼云 API 接口的身份凭证，不能登录控制台。访问密钥中具有验证身份的签名，通过加密签名验证可以确保机密性、完整性和请求双方身份的正确性。

用户组

用户组是用户的集合，IAM 通过用户组功能实现用户的授权。您创建的 IAM 用户，需要加入特定用户组后，才具备对应的权限，否则 IAM 用户无法访问您帐号中的任何资源或者云服务。当某个用户加入多个用户组时，此用户同时拥多个用户组的权限，即多个用户组权限的全集。

“admin”为系统缺省提供的用户组，具有所有云服务资源的操作权限。将 IAM 用户加入该用户组后，IAM 用户可以操作并使用所有云资源，包括但不仅限于创建用户组及用户、修改用户组权限、管理资源等。

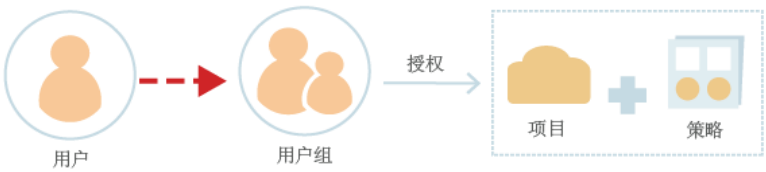
图1-3 用户组与用户



授权

授权是您将用户完成具体工作需要的权限授予用户，授权通过定义权限策略生效，通过给用户组授予策略（包括系统策略和自定义策略），用户组中的用户就能获得策略中定义的权限，这一过程称为授权。用户获得具体云服务的权限后，可以对云服务进行操作，例如，管理您帐号中的 ECS 资源。

图1-4 授权



权限

如果您授予 IAM 用户弹性云服务器 ECS 的权限，则该 IAM 用户除了 ECS，不能访问其他任何服务，如果尝试访问其他服务，系统将会提示没有权限。

图1-5 系统提示没有权限

权限根据授权的精细程度，分为策略和角色。

角色：角色是 IAM 早期提供的一种粗粒度的授权能力，当前有部分云服务不支持基于角色的授权。角色不能全部满足用户对精细化授权的要求。

策略：策略是 IAM 提供的最新细粒度授权能力，可以精确到具体操作、条件等。使用基于策略的授权是一种更加灵活地授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对 ECS 服务，管理员能够控制 IAM 用户仅能对某一类云服务器的资源进行指定的管理操作。

策略包含系统策略和自定义策略。

云服务在 IAM 预置了常用授权项，称为系统策略。管理员给用户组授权时，可以直接使用这些系统策略，系统策略只能使用，不能修改。如果管理员在 IAM 控制台给用户组或者委托授权时，无法找到特定服务的系统策略，原因是该服务暂时不支持 IAM，管理员可通过天翼云网门户给对应云服务提交工单，申请该服务在 IAM 预置权限。

如果系统策略无法满足授权要求，管理员可以根据各服务支持的授权项，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，自定义策略是对系统策略的扩展和补充。目前支持可视化 JSON 视图自定义策略配置。

图1-6 权限策略示例

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "vpc:*:*",
                "ecs:*:get*",
                "ecs:*:list*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

项目

每个天翼云资源节点对应一个 IAM 默认项目，目前这个项目由系统预置，用来隔离各资源节点的资源（计算资源、存储资源和网络资源等），以该默认项目为范围进行授权，用户可以访问您帐号中该资源节点（即该默认项目）的所有资源。

委托

委托根据委托对象的不同，分为委托其他天翼云帐号和委托其他云服务。

委托其他天翼云帐号：通过委托信任功能，您可以将自己帐号中的资源操作权限委托给其他天翼云帐号，被委托的帐号可以根据权限代替您进行资源运维工作。

委托其他云服务：由于天翼云各服务之间存在业务交互关系，一些云服务需要与其他云服务协同工作，需要您创建云服务委托，将操作权限委托给该服务，让该服务以您的身份使用其他云服务，代替您进行一些资源运维自动化工作。

1.5 约束与限制

IAM 中的用户数、用户组数等有限定的配额， 其中“是否支持修改”列标示“√”的，表示该限制项可以修改。如果当前资源配额无法满足业务需要，您可在天翼云网门户提交工单，申请扩大配额。

限制项	限制值	是否支持修改
IAM 用户数	50	√
用户组数	20	√
一个用户组中可添加的用户数	帐号下的 IAM 用户数	x
委托数	50	√
用户可加入的用户组数	10	x
用户可创建的访问密钥（AK/SK）数	2	x
用户名的字符数	32	x
用户组名的字符数	64	x
策略名称的字符数	64	x

2 购买指南

2.1 资源节点

统一身份认证（Identity and Access Management，简称 IAM）服务目前支持的天翼云资源节点：

上海 4、杭州、苏州、芜湖、南昌、福州、深圳、广州 4、南宁、西宁、长沙 2、海口、武汉 2、郑州、西安 2、中卫、乌鲁木齐、兰州、贵州、重庆、成都 3、昆明、青岛、北京 2、太原、石家庄、天津、长春、哈尔滨、沈阳 3、内蒙 3。

2.2 计费说明

统一身份认证 IAM 服务目前免费。

2.3 申请开通

已实名认证的天翼云企业类型帐号可申请开通统一身份认证服务。

前提条件

- 请确保您已拥有天翼云企业帐号，若您还没有帐号，请先进行注册。
- 请确保您的企业账号已完成实名认证。

开通步骤

步骤 1 企业管理员使用已注册的天翼云企业帐号登录天翼云网门户。

步骤 2 单击顶部右侧“管理中心”，在管理中心页面单击页面顶部右侧“工单”。

步骤 3 在工单中心业务，单击左侧导航菜单“新建工单”。

步骤 4 在新建工单页面，所属产品选择“会员账号”，单击卡片右侧的“提问”按钮。

步骤 5 问题分类点选“其它问题”，在创建工单业务，填写工单标题/工单内容为“申请开通账号 IAM 主子账号管理服务”

步骤 6 填写联系方式等信息，单击“确认提交”完成 IAM 开通申请。

3 快速入门

3.1 示例场景

您可以根据用户职责规划用户组。使用安全管理员访问 IAM 并创建用户组，再根据职责赋予用户组对应的权限。

前提条件

- 请确保您已拥有天翼云帐号，若您还没有帐号，请先进行注册。
- 请确保您已开通统一身份认证服务，如 IAM 服务未开通，请首先在天翼云网门户提交申请开通工单。

业务场景

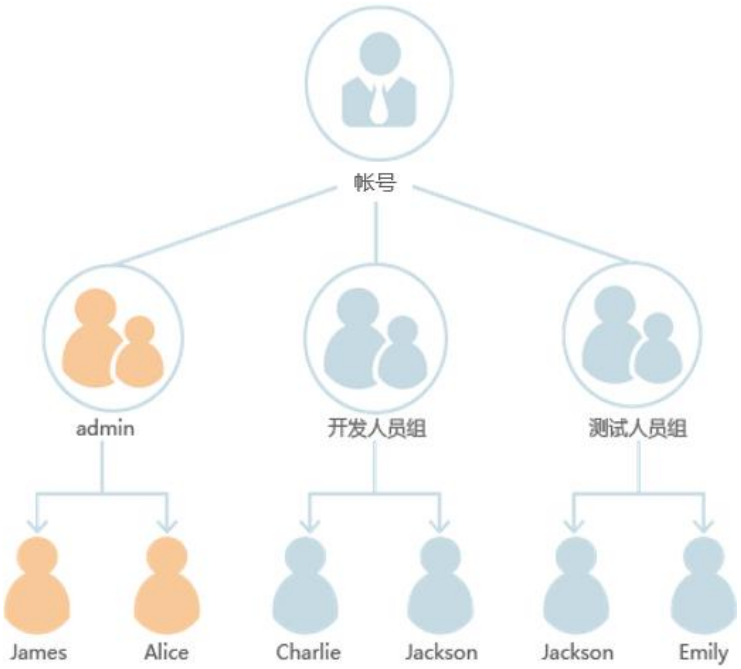
A 公司是一家负责网站开发的公司，公司地址位于中国上海，公司中有三个职能团队。为了方便 A 公司统一购买、分配资源并管理用户，A 公司的人员不需要每人都注册帐号，而是由公司的管理员注册一个帐号，在这个帐号下创建 IAM 用户并分配权限，然后将创建的 IAM 用户分发给公司的人员使用。

本节以 A 公司使用 IAM 创建用户及用户组为例，帮助您快速了解，企业如何使用 IAM 完成天翼云服务权限的配置。

A 公司人员组成

- 负责管理公司的人员以及资源的管理团队（对应图 1 中的“admin”），进行权限分配，资源调配等。团队成员包括 James 和 Alice。
- 负责开发公司网站的开发团队（对应图 1 中的“开发人员组”）。团队成员包括 Charlie 和 Jackson。
- 对开发团队开发出的网站进行测试的测试团队（对应图 1 中的“测试人员组”）。团队成员包括 Jackson 和 Emily。其中 Jackson 同时负责开发及测试，因此他需要同时加入“开发人员组”及“测试人员组”，以分别获得两个用户组的权限。

图3-1 用户管理模型



A 公司业务组成

- admin 组主要负责公司人员权限分配，需要使用 IAM 服务。
- 开发人员组在网站开发过程中，需要使用弹性云服务器（ECS）、虚拟私有云（VPC）以及云硬盘（EVS）。
- 测试人员主要负责网站的功能及性能测试，需要使用应用运维管理（AOM）。

用户管理流程

1. A 公司的管理员使用注册的帐号登录天翼云，创建“开发人员组”及“测试人员组”，并给用户组授权。操作步骤请参见：步骤 1：创建用户组、步骤 2：为用户组授权。
2. A 公司的管理员给三个职能团队中的成员创建 IAM 用户，并让他们使用新创建的 IAM 用户登录天翼云。操作步骤请参见：步骤 3：创建 IAM 用户、步骤 4：登录并使用 IAM 用户。

3.2 步骤 1：创建用户组

A 公司的团队分为管理组（admin）、开发人员组和测试人员组。由于系统默认内置了 admin 组，用于拥有帐号所有资源的使用及管理权限，因此 A 公司的团队只需要在 IAM 中再创建开发人员组及测试人员组即可。

操作步骤

步骤 1 A 公司管理员使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 鼠标移动至天翼云首页右上角用户头像，在下拉列表中单击“个人中心”。

步骤 3 个人中心左侧菜单中，单击“主子账号及授权管理”。

步骤 4 在主子账号及授权管理页，单击左侧导航菜单中的“用户组”。

步骤 5 在“用户组”管理界面中，单击“创建用户组”。

步骤 6 输入“用户组名称”和“描述”，单击“确定”。

返回用户组列表页，用户组列表中将显示新创建的用户组。

依照以上流程，分别创建“开发人员组”和“测试人员组”

----结束

3.3 步骤 2：为用户组授权

A 公司的开发人员需要使用的云服务为 ECS、VPC 及云硬盘，需要为“开发人员组”授予这些服务的管理员权限。测试人员需要使用云服务 AOM，需要为“测试人员组”授予此服务的权限。完成用户组的授权后，用户组中的用户才可以使用这些云服务。

操作步骤

步骤 1 A 公司管理员使用已注册的天翼云帐号登录天翼云网门户。

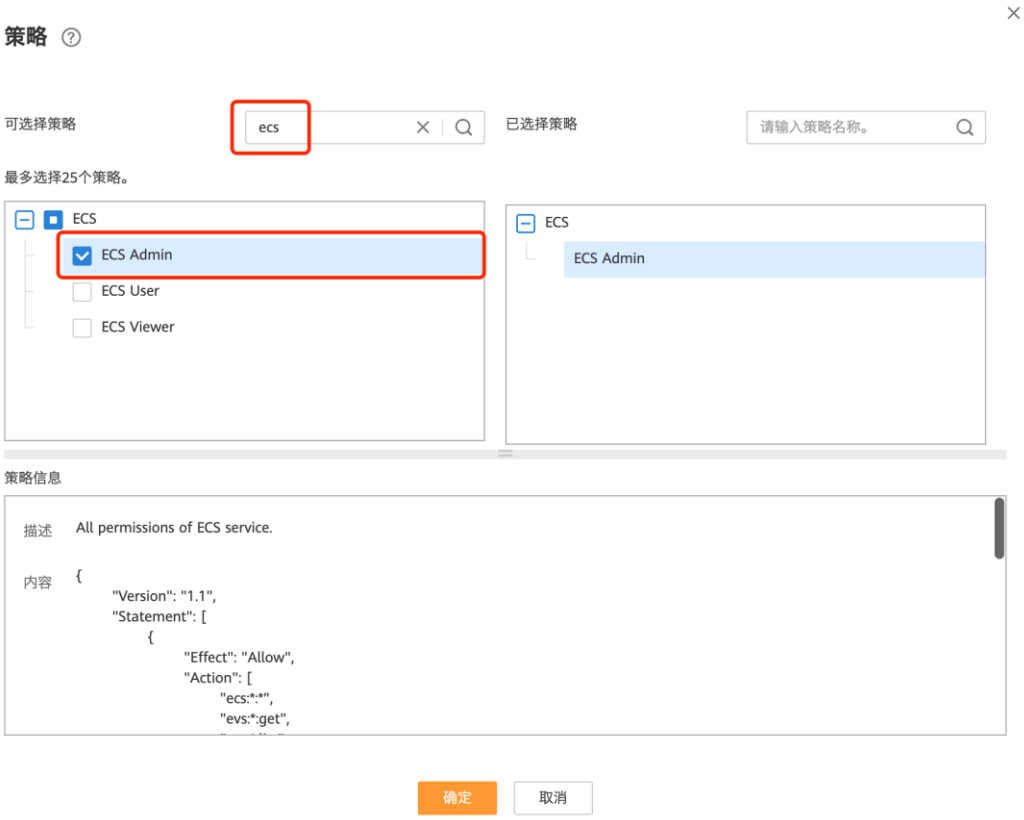
步骤 2 单击首页顶部控制台，在控制中心页面“管理与部署”类中，单击“统一身份认证服务”。

步骤 3 在统一身份认证服务管理页面，单击左侧功能菜单“用户组”，找到在步骤 1 中已创建的用户组“开发人员组”，单击右侧 “修改”。

步骤 4 在用户组权限管理页面，找到在本例中需要设置的项目（上海资源池），单击右侧的“修改”。

步骤 5 在弹出的用户组授权对话框中，找出并勾选（可多选）需要设置的权限策略，在本例中，为开发人员组添加 ECS Admin、VPC Admin 和 EVS Admin 三个策略授权。

可在选择策略搜索框中输入服务名称英文缩写并单击右侧搜索按钮，快速定位需授权的服务权限。



步骤 6 单击“确定”，完成用户组的权限授权。

参考步骤 3 至步骤 5 的方法，给“测试人员组”授予“上海”项目“AOM Admin”的权限。

----结束

3.4 步骤 3：创建 IAM 用户

步骤 1 和步骤 2 已完成用户组的创建并完成了授权，本节将描述 A 公司使用已注册的天翼云帐号，给公司成员创建 IAM 用户并加入用户组的操作，使得他们拥有独立的用户和密码，可以独立登录天翼云并管理权限范围内的资源。

操作步骤

步骤 1 A 公司管理员使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 鼠标移动至天翼云首页右上角用户头像，在下拉列表中单击“个人中心”。

步骤 3 个人中心左侧菜单中，单击“主子账号及授权管理”。

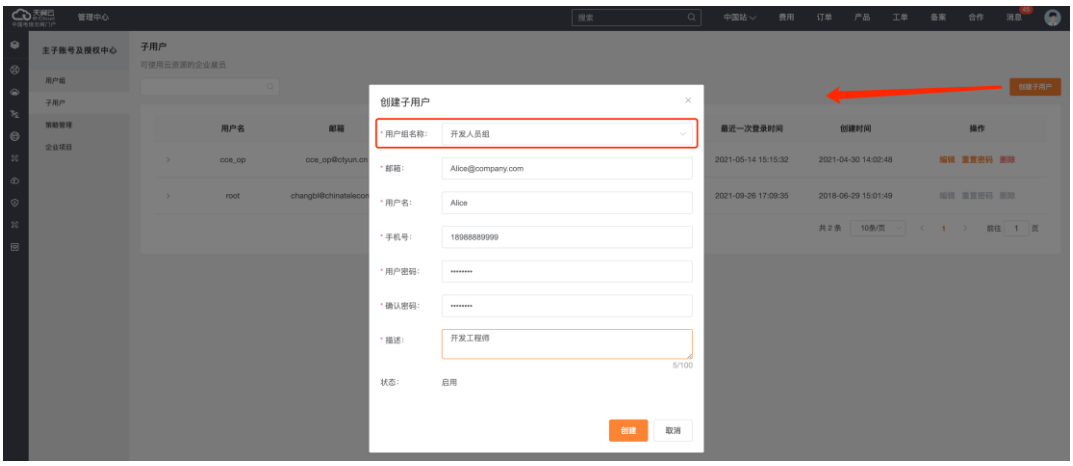
步骤 4 在主子账号及授权管理页，单击左侧导航菜单中的“子用户”。

步骤 5 在“子用户”管理界面中，单击“创建子用户”。

步骤 6 在弹出的创建用户对话框中，输入以下子用户信息：

用户组：在下拉菜单中选择步骤 1 中已创建好的用户组“开发人员组”，新用户将具备此用户组的全部权限，这一过程即给用户授权。

用户基本信息：依次输入新用户的“邮箱”、“用户名”等基本信息，并为用户设置初始登录密码。



步骤 7 单击“确定”，完成 IAM 用户创建，用户列表中将显示新创建的 IAM 用户。

参考步骤 5 至步骤 7 的方法，创建用户 Charlie、Jackson 和 Emily，并加入对应的用户组。

----结束

3.5 步骤 4：登录并使用 IAM 用户

通过前述步骤，A 公司已在主帐号中创建了名为 James、Alice、Charlie、Jackson 和 Emily 的 IAM 用户。完成 IAM 用户创建后，A 公司管理员需要将帐号名、IAM 用户名及初始密码告知对应的员工，这些员工就可以使用自己的用户名及密码访问天翼云。

如果 IAM 用户登录失败或忘记密码，IAM 用户可以联系 A 公司管理员重置密码。

操作步骤

步骤 1 A 公司 IAM 用户打开天翼云网门户首页。

步骤 2 单击顶部右上角“登录”，在登录页面输入用户名 IAM 用户名（一般为邮箱地址）、密码，单击“登录”按钮，登录天翼云。

----结束

4 用户指南

4.1 管理 IAM 用户

4.1.1 创建 IAM 用户

当您需要与新用户共享您账号中的资源时，您可以使用安全管理员通过 IAM 创建用户。创建用户时可以设置安全凭证和权限。这些用户可以通过管理控制台或 API、CLI、SDK 等开发工具访问系统。

默认情况下，新创建的 IAM 用户没有任何权限，管理员需要将其加入用户组，并给用户组授权，用户组中的用户将获得用户组的权限。授权后，IAM 用户就可以基于权限对云服务进行操作。

须知

“admin”为缺省用户组，具有所有云服务资源的操作权限。将用户加入该用户组后，用户可以操作并使用所有云服务资源，包括但不仅限于创建用户组及用户、修改用户组权限、管理资源等。

操作步骤

步骤 1 企业的天翼云管理员使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 鼠标移动至天翼云首页右上角用户头像，在下拉列表中单击“个人中心”。

步骤 3 个人中心左侧菜单中，单击“主子账号及授权管理”。

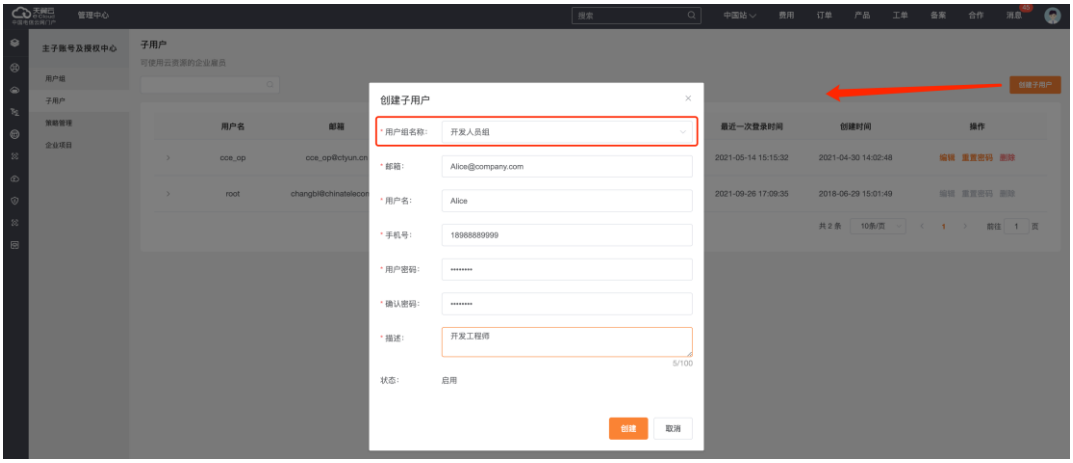
步骤 4 在主子账号及授权管理页，单击左侧导航菜单中的“子用户”。

步骤 5 在“子用户”管理界面中，单击“创建子用户”。

步骤 6 在弹出的创建用户对话框中，输入以下子用户信息：

用户组：在下拉菜单中选择已创建好的用户组，新用户将具备此用户组的全部权限，这一过程即给用户授权。

用户基本信息：依次输入新用户的“邮箱”、“用户名”等基本信息，并为用户设置初始登录密码。



步骤 7 单击“确定”，完成 IAM 用户创建，返回子用户列表，将显示新创建的 IAM 用户。

----结束

相关任务

- 查看用户信息和修改用户信息（包括用户状态、绑定的邮箱、手机号码、所属用户组、描述等）。
- 删除用户：在用户列表中，单击“删除”。

4.1.2 为 IAM 用户授权

您授权的最小单位是用户组，IAM 用户的授权通过将其加入用户组来实现。管理员给用户组授予策略，然后将用户加入用户组，使得用户组中的用户获得策略定义的权限，这一过程称为授权。

- 如果创建 IAM 用户时，IAM 用户没有加入任何用户组，则 IAM 用户不具备任何权限，不能对云服务进行操作，请参考创建用户组并授权和用户组添加/移除用户给 IAM 用户授权。
- 如果创建 IAM 用户时，IAM 用户加入了默认用户组“admin”，则 IAM 用户为管理员，可以对所有云服务执行任意操作。
- 当某个用户加入多个用户组时，此用户同时拥多个用户组的权限，即取多个用户组权限的全集。

4.1.3 查看或编辑用户信息

管理员可以查看用户的基本信息、所属用户组以及用户日志。当人员职责发生变动时，管理员可以通过修改用户所属的用户组来修改用户所拥有的权限。

查看用户信息

步骤 1 企业的天翼云管理员使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 鼠标移动至天翼云首页右上角用户头像，在下拉列表中单击“个人中心”。

步骤 3 个人中心左侧菜单中，单击“主子账号及授权管理”。

步骤 4 在主子账号及授权管理页，单击左侧导航菜单中的“子用户”。

步骤 5 在用户列表中，单击对应用户左侧的 > 展开详情卡片，查看用户的详细信息。

----结束

修改用户信息及状态

步骤 1 企业的天翼云管理员使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 鼠标移动至天翼云首页右上角用户头像，在下拉列表中单击“个人中心”。

步骤 3 个人中心左侧菜单中，单击“主子账号及授权管理”。

步骤 4 在主子账号及授权管理页，单击左侧导航菜单中的“子用户”。

步骤 5 在用户列表中，单击对应用户右侧的“编辑”，弹出用户详情编辑框。

步骤 6 编辑用户的绑定邮箱、电话、用户名、描述等信息，如需暂停使用此 IAM 用户，在用户状态栏选择“禁用”选项。

步骤 7 单击“确定”，完成用户信息修改。

----结束

4.1.4 重置 IAM 用户密码

当用户忘记或遗失密码时，管理员可以重置 IAM 用户的登录密码。

须知

- IAM 提供的密码重置功能，适用于通过管理员重置 IAM 用户的密码。
- IAM 子用户可以在天翼云用户中心页面自行修改密码。

操作步骤

步骤 1 企业的天翼云管理员使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 鼠标移动至天翼云首页右上角用户头像，在下拉列表中单击“个人中心”。

步骤 3 个人中心左侧菜单中，单击“主子账号及授权管理”。

步骤 4 在主子账号及授权管理页，单击左侧导航菜单中的“子用户”。

步骤 5 在用户列表中，单击对应用户右侧的“重置密码”，弹出重置密码对话框。

步骤 6 输入天翼云主账号绑定的手机号码并单击“发送验证码”，填写收到的短信验证码、新密码，单击“确定”，完成 IAM 用户密码重置。

----结束

4.1.5 删除 IAM 用户

管理员如仅想将停止授权指定的 IAM 用户，可先将其从用户组移除。

⚠ 注意

删除后该 IAM 用户的所有数据将被删除且不可恢复，请谨慎操作！

操作步骤

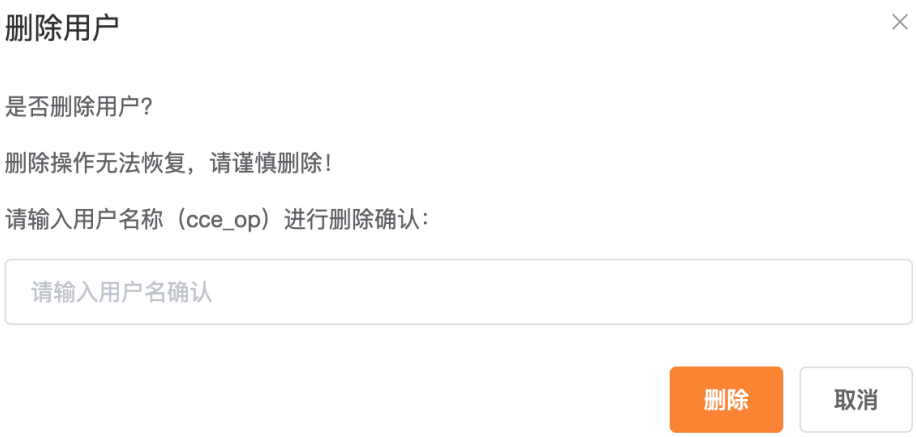
步骤 1 企业的天翼云管理员使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 鼠标移动至天翼云首页右上角用户头像，在下拉列表中单击“个人中心”。

步骤 3 个人中心左侧菜单中，单击“主子账号及授权管理”。

步骤 4 在主子账号及授权管理页，单击左侧导航菜单中的“子用户”。

步骤 5 在用户列表中，单击对应用户右侧的“删除”，弹出删除用户确认框。



步骤 6 输入待删除的用户名称，单击“删除”，完成 IAM 用户删除。

----结束

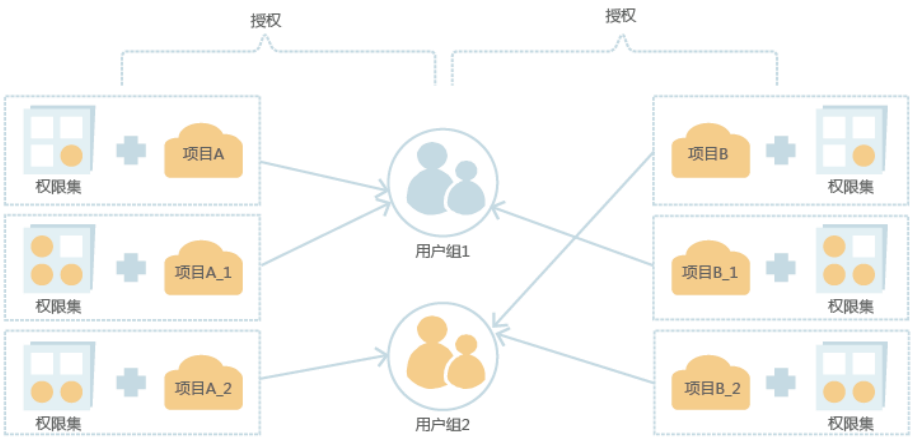
4.2 管理用户组

4.2.1 用户及其权限管理

您可以通过为用户组授权并将用户加入到用户组的方式，使用户具有用户组中的权限，用户可以根据权限访问系统。

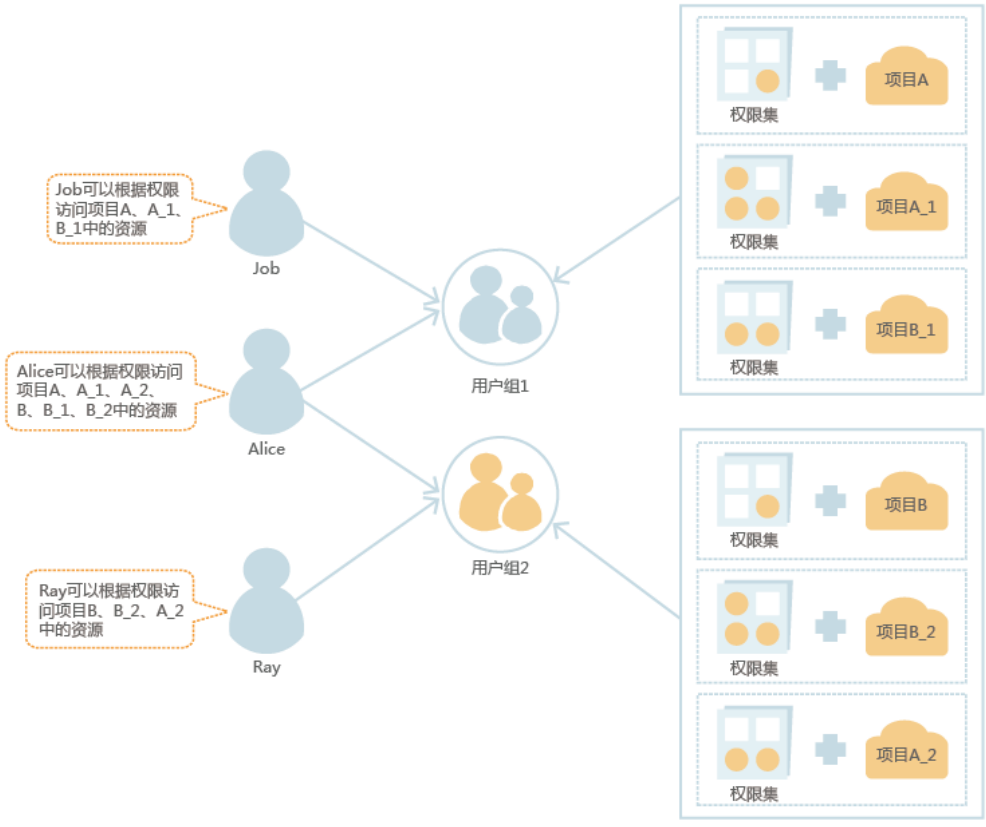
步骤 1 管理员按照用户职责规划用户组并为用户组授权。

图4-1 用户组授权模型



步骤 2 管理员创建用户并根据用户职责将用户加入到对应的用户组中。

图4-2 用户授权模型



步骤 3 用户根据权限访问系统。

----结束

4.2.2 创建用户组

您可以根据用户职责规划用户组，并赋予用户组对应职责的权限，使得用户组中的用户拥有对应职责的权限。通过用户组来管理用户权限可以使权限管理更有条理。

操作步骤

步骤 1 使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 鼠标移动至天翼云首页右上角用户头像，在下拉列表中单击“个人中心”。

步骤 3 个人中心左侧菜单中，单击“主子账号及授权管理”。

步骤 4 在主子账号及授权管理页，单击左侧导航菜单中的“用户组”。

步骤 5 在“用户组”管理界面中，单击“创建用户组”。

步骤 6 输入“用户组名称”和“描述”，单击“确定”。

返回用户组列表页，用户组列表中将显示新创建的用户组。

----结束

4.2.3 用户组添加/移除授权

管理员创建用户组后给用户组授予策略或角色，然后将用户加入用户组，使得用户组中的用户获得相应的权限。

IAM 预置了云服务的常用权限，例如服务的管理员权限、只读权限，企业管理员可以直接使用这些系统权限给用户组授权，授权后，用户就可以基于权限对云服务进行相应操作。

为用户组授权

步骤 1 企业管理员使用已注册的天翼云帐号登录天翼云网门户。

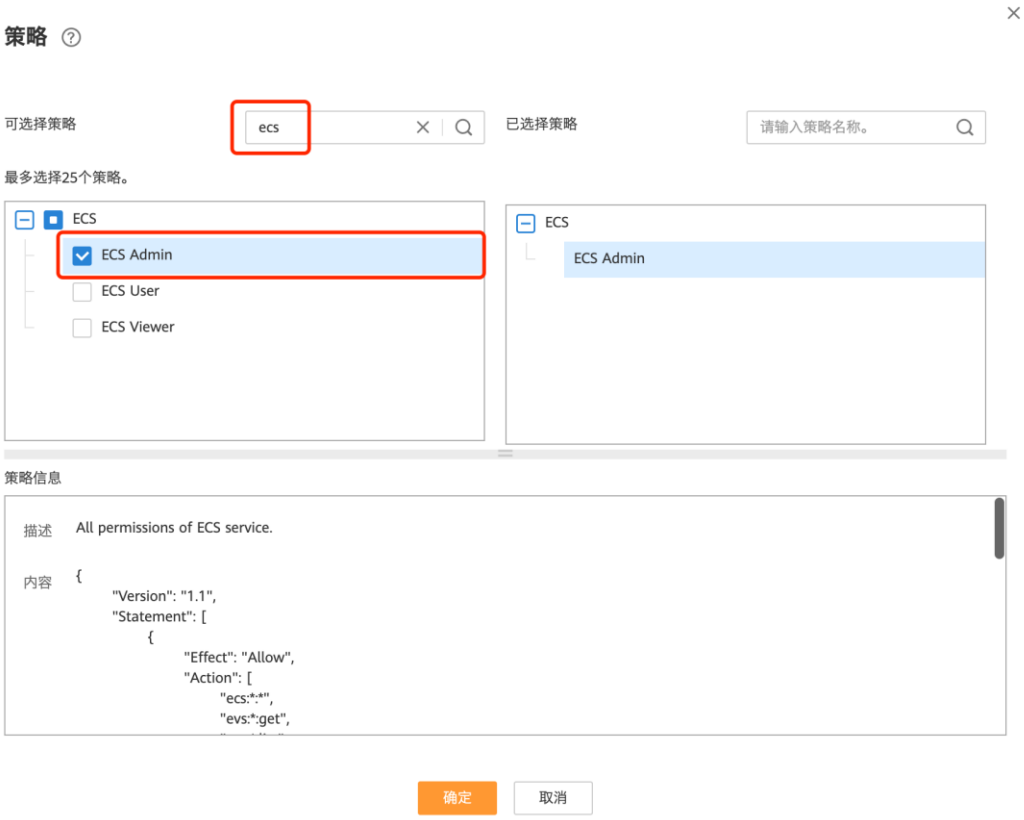
步骤 2 单击首页顶部控制台，在控制中心页面“管理与部署”类中，单击“统一身份认证服务”。

步骤 3 在统一身份认证服务管理页面，单击左侧功能菜单“用户组”，单击待添加授权用户组右侧的 “修改”。

步骤 4 在用户组权限管理页面，选定待授权的项目（如上海 4 资源池），单击右侧的“修改”。

步骤 5 在弹出的用户组授权对话框中，选定并勾选（可多选）需要设置的权限策略。

可在选择策略搜索框中输入服务名称英文缩写并单击右侧搜索按钮，快速定位需授权的服务权限。



步骤 6 单击“确定”，完成用户组的权限授权。

----结束

为用户组移除授权

步骤 1 企业管理员使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 单击首页顶部控制台，在控制中心页面“管理与部署”类中，单击“统一身份认证服务”。

步骤 3 在统一身份认证服务管理页面，单击左侧功能菜单“用户组”，单击待移除授权用户组右侧的 “修改”。

步骤 4 在用户组权限管理页面，选定待移除授权的项目，单击右侧的“修改”。

步骤 5 在弹出的用户组授权对话框中，取消勾选需要移除的权限策略。

可在选择策略搜索框中输入服务名称英文缩写并单击右侧搜索按钮，快速定位需移除授权的服务权限。

步骤 6 单击“确定”，完成移除用户组权限授权。

----结束

4.2.4 用户组添加/移除用户

企业管理员创建用户组、授权并将用户加入用户组，使 IAM 用户具备用户组的权限，实现用户的授权。在已授权的用户组中添加或者移除 IAM 用户，快速实现用户的权限变更。

操作步骤

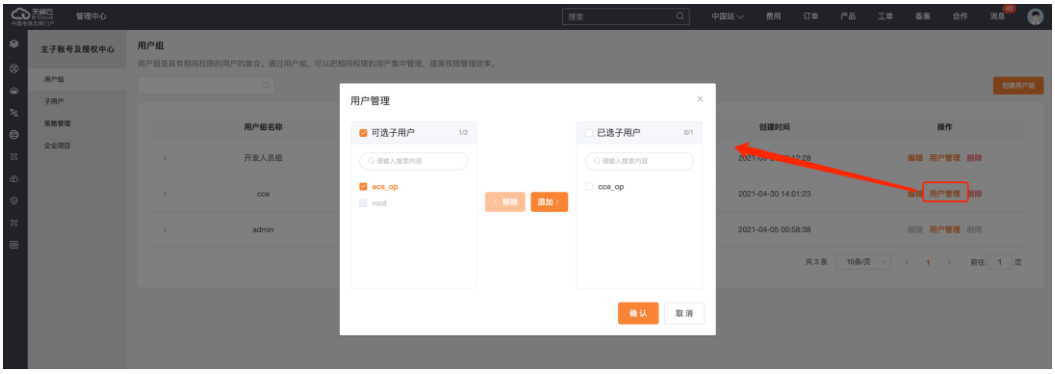
步骤 1 使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 鼠标移动至天翼云首页右上角用户头像，在下拉列表中单击“个人中心”。

步骤 3 个人中心左侧菜单中，单击“主子账号及授权管理”。

步骤 4 在主子账号及授权管理页，单击左侧导航菜单中的“用户组”。

步骤 5 在“用户组”列表页面，单击待调整用户组右侧的“用户管理”。



步骤 6 在“用户管理”弹出框，勾选待添加或移除的 IAM 用户，并单击“添加”或“移除”，确认调整完毕后单击“确认”，完成用户组中用户的添加/移除。

----结束

4.2.5 查看/修改/删除用户组

企业管理员可以查看用户组详情及包含的 IAM 子用户、修改用户组的基本信息、删除不再需要的用户组。

操作步骤

步骤 1 使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 鼠标移动至天翼云首页右上角用户头像，在下拉列表中单击“个人中心”。

步骤 3 个人中心左侧菜单中，单击“主子账号及授权管理”。

步骤 4 在主子账号及授权管理页，单击左侧导航菜单中的“用户组”。

步骤 5 在“用户组”列表页面：

单击用户组左边的 `>`，可查看用户组详情信息。

单击用户组右边的“编辑”，弹出“编辑用户组”对话框，完成修改用户组名称及描述。

单击用户组右边的“删除”， 弹出“删除用户组”确认框，再次输入待删除的用户组名称并单击“确认”，完成用户组删除。

----结束

4.3 管理权限

4.3.1 权限基本概念

权限

默认情况下，管理员创建的 IAM 子用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

权限的分类

权限根据授权精细程度分为角色和策略。

- **角色**：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。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于天翼云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色不能完全满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。

- **策略**：IAM 最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对 ECS 服务，管理员能够控制 IAM 用户仅能对云服务器资源进行某一类指定的管理操作。

策略根据创建的对象，分为系统策略和自定义策略。

策略-系统策略

云服务在 IAM 预置了常用授权项，称为系统策略。管理员给用户组授权时，可以直接使用这些系统策略，系统策略只能使用，不能修改。

如果管理员在 IAM 控制台给用户组或者委托授权时，无法找到特定服务的系统策略，原因是该服务暂时不支持 IAM，管理员可以通过给对应云服务提交工单，申请该服务在 IAM 预置权限。

策略-自定义策略

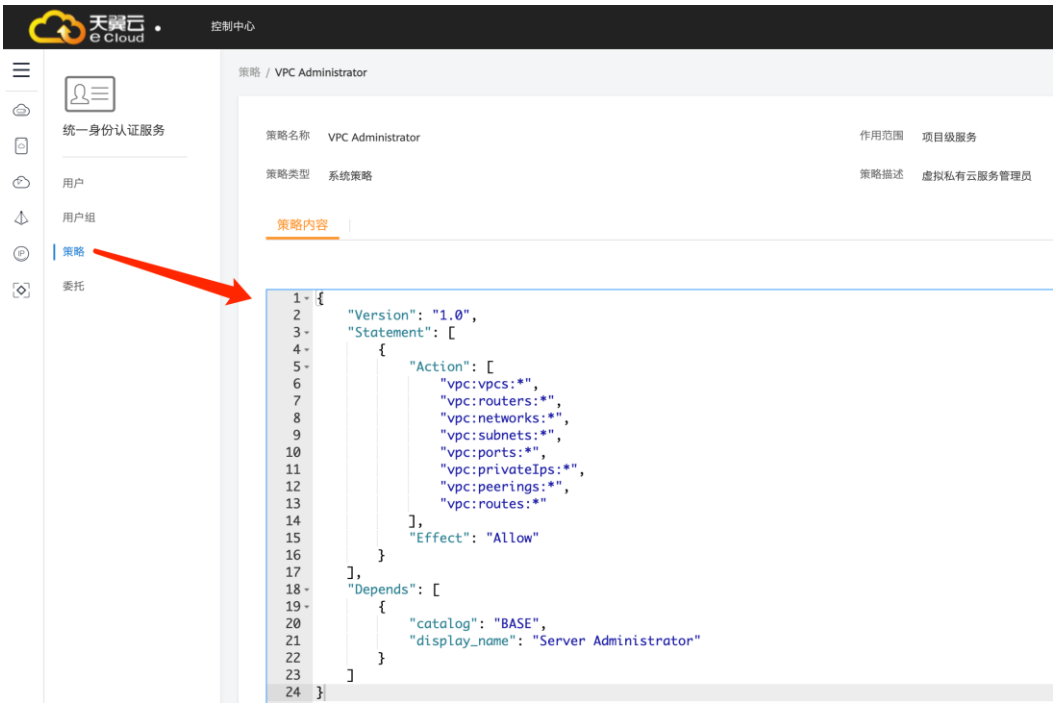
如果系统策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制，自定义策略是对系统策略的扩展和补充。目前 IAM 支持可视化视图、JSON 视图两种自定义策略配置方式。

4.3.2 角色

角色是 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。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于天翼云各服务之间存在业务依赖关系，因此给用户组授予角色时，需要将依赖的其他角色一并授予该用户组，保证用户权限生效。

角色内容

在 IAM 控制台中，单击左侧导航菜单“策略”，可以查看角色类权限的详细内容，以“VPC Administrator”为例，说明角色类权限的内容。



角色内容的参数说明：

参数段 1	参数段 2	说明
Version 权限版本		1.0：角色类权限 1.1：策略类权限
Statement 角色的授权语句	Action 授权项	服务的操作权限
	Effect 定义 Action 中的操作权限是否允许执行	Allow：允许执行 Deny：不允许执行
Depends 角色的依赖关系	Catalog 依赖的角色所属服务	服务名称，例如： BASE、VPC
	display_name	如 VPC Administator 依赖

参数段 1	参数段 2	说明
	依赖的角色名称	Server Administrator 角色

4.3.3 策略

策略是描述一组权限集的语言，它可以精确地描述对授权云服务可以执行的操作。通过策略，用户可以自由搭配需要授予的权限集。通过给用户组授予策略，用户组中的用户就能获得策略中定义的权限。IAM 通过策略定义的权限内容实现精细的权限管理。

IAM 支持以下两种形式的策略：

- 系统策略：系统预置的常用权限集，主要针对不同云服务的只读权限或管理员权限，比如对 ECS 的只读权限、对 ECS 的管理员权限等；系统策略只能用于授权，不能编辑和修改。
- 自定义策略：由用户自己创建和管理的权限集，是对系统策略的扩展和补充。

策略内容

细粒度授权策略内容包括策略版本号（Version）及策略授权语句（Statement）列表。

- 策略版本号：Version，标识策略的版本号，主要用于区分 Role-Based Access Control 策略和细粒度策略。
  - 1.0：Role-Based Access Control（RBAC）)策略。即“角色”，RBAC 策略是将服务作为一个整体进行授权，授权后，用户可以拥有这个服务的所有权限，RBAC 策略只能由系统预置。
  - 1.1：细粒度策略。相比角色类策略，细粒度策略基于服务的 API 接口进行权限拆分，授权更加精细。授权后，用户可以对这个服务执行特定的操作。细粒度策略包括系统预置和用户自定义两种：
    - 系统预置策略：系统预置服务常用的权限集，包括服务的只读权限或管理员权限。
    - 用户自定义策略：由用户自己创建和管理的权限集，是对系统策略的扩展和补充。例如：针对 ECS 服务，控制用户仅能变更云服务器规格。
- 策略授权语句：Statement，描述的是策略的详细信息，包含作用（Effect）和授权项（Action）。
  - 作用（Effect）

    作用包含两种：允许（Allow）和拒绝（Deny），一个自定义策略中可以同时包含允许和拒绝的授权语句，当策略中既有允许又有拒绝的授权语句时，遵循 Deny 优先的原则。
  - 授权项（Action）

    对资源的具体操作权限，支持单个或多个操作权限。

    格式为：服务名:资源类型:操作，例如：vpc:ports:create。

说明

- 服务名：产品名称，例如 ecs、evs 和 vpc 等，服务名仅支持小写。

- 资源类型和操作没有大小写要求，支持通配符号*，用户不需要罗列全部授权项，通过配置通配符号*可以方便快捷地实现授权。

策略样例

- 支持单个操作权限，例如：查询弹性云服务器详情权限

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:servers:list",
                "ecs:servers:get",
                "ecs:serverVolumes:use",
                "ecs:diskConfigs:use",
                "ecs:securityGroups:use",
                "ecs:serverKeypairs:get",
                "vpc:securityGroups:list",
                "vpc:securityGroups:get",
                "vpc:securityGroupRules:get",
                "vpc:networks:get",
                "vpc:subnets:get",
                "vpc:ports:get",
                "vpc:routers:get"
            ]
        }
    ]
}
```

- 支持多个操作权限，例如：锁定云服务器和创建云硬盘权限。

```
{
   "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:servers:lock",
                "evs:volumes:create"
            ]
        }
    ]
}
```

- 通配符号*用法示例：对 IMS 服务资源的所有权限。

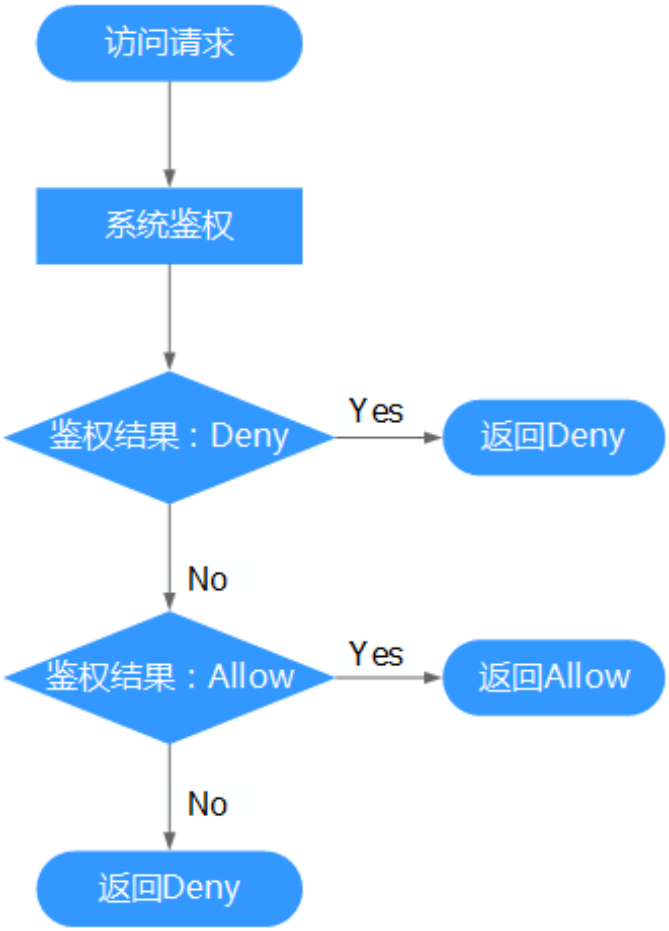
```
{
      "Version": "1.1",
      "Statement": [
            {
                "Action": [
                      "ims:*:*",
                      "ecs:*:list",
                      "ecs:*:get",
                      "evs:*:get"
                ],
```

```
                "Effect": "Allow"
            }
        ]
}
```

策略鉴权规则

用户在发起操作请求时，系统首先根据用户被授予的访问策略中的 action 进行鉴权判断。鉴权规则如下：

图4-3 系统鉴权逻辑图



说明

每条策略做评估时， Action 之间是或(or)的关系。

1. 用户访问云服务，发起操作请求。
2. 系统评估用户被授予的访问策略，鉴权开始。
3. 在用户被授予的访问策略中，系统将优先寻找显式拒绝指令。如找到一个适用的显式拒绝，系统将返回 Deny 决定。
4. 如果没有找到显式拒绝指令，系统将寻找适用于请求的任何 Allow 指令。如果找到一个显式允许指令，系统将返回 Allow 决定。

5. 如果找不到显式允许，最终决定为 Deny，鉴权结束。

4.3.4 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，自定义策略是对系统策略的扩展和补充。

目前 IAM 支持以下两种方式创建自定义策略：

- **可视化视图：**通过可视化视图创建自定义策略，无需了解 JSON 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：**通过 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。

可视化视图配置自定义策略

步骤 1 企业管理员使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 单击首页顶部控制台，在控制中心页面“管理与部署”分类中，单击“统一身份认证服务”。

步骤 3 在统一身份认证服务管理页面，单击左侧功能菜单“策略”后，单击右上角“＋创建自定义策略”按钮。

步骤 4 进入创建自定义策略页面，输入“策略名称”。

步骤 5 选择“作用范围”，即自定义策略的生效范围，根据服务的部署区域选择。

- 全局级服务：权限策略中该服务的“所属区域”为“全局区域”，表示该服务为全局级服务。创建全局级服务的自定义策略时，作用范围选择“全局级服务”。给用户组授予该自定义策略时，需要在全局区域中进行。
- 项目级服务：权限策略中该服务的“所属区域”为“除全局区域外其他区域”，表示该服务为项目级服务。创建项目级服务的自定义策略时，作用范围选择“项目级服务”。给用户组授予该自定义策略时，需要在除全局区域外其他区域中进行。

例如：创建 EVS 的自定义策略（"evs:volumes:create"），由于 EVS 服务属于项目级服务，作用范围必须选择项目级服务。

说明

如果一个自定义策略中包含多个服务的授权语句，这些服务必须是同一属性，即都是全局级服务或者项目级服务。如果需要同时设置全局服务和项目级服务的自定义策略，请创建两条自定义策略，“作用范围”分别为“全局级服务”以及“项目级服务”。

步骤 6 “策略配置方式”选择“可视化视图”。

步骤 7 在“策略内容”下配置策略。

1. 选择“允许”或“拒绝”。
2. 选择“云服务”。

说明

此处只能选择一个云服务，如需配置多个云服务的自定义策略，请在完成此条配置后，单击“添加权限”，创建多个服务的授权语句；或使用 JSON 视图配置自定义策略。

3. 选择“操作”，根据需求勾选产品权限。
4. （可选）选择资源类型，如选择“特定类型”可以点击“通过资源路径指定”来指定需要授权的资源。

说明

支持为特定资源授权的云服务目前仅包括对象存储服务（OBS）、分布式消息服务（DMS）

5. （可选）添加条件，单击“添加条件”，选择“条件键”，选择“运算符”，根据运算符类型填写相应的值。

表4-1 条件参数

参数名称	参数说明
条件键	条件键表示策略语句的 Condition 元素中的键值。分为全局条件键和服务级条件键。全局级条件键（前缀为 g:）适用于所有操作，服务级条件键（前缀为服务缩写，如 obs:）仅适用于对应服务的操作。
运算符	与条件键一起使用，构成完整的条件判断语句。
值	与条件键和运算符一起使用，当运算符需要某个关键字时，需要输入关键字的值，构成完成的条件判断语句。

步骤 8 （可选）在“策略配置方式”选择 JSON 视图，将可视化视图配置的策略内容转换为 JSON 语句，您可以在 JSON 视图中对策略内容进行修改。

说明

如果您修改后的 JSON 语句有语法错误，将无法创建策略，可以自行检查修改内容或单击界面弹窗中的“重置”，将 JSON 文件恢复到未修改状态。

步骤 9 （可选）如需创建多条自定义策略，请单击“添加权限”；也可在已创建的策略最右端单击“+”，复制此权限。

步骤 10 输入“策略描述”（可选）。

步骤 11 单击“确定”，自定义策略创建完成。

步骤 12 将新创建的自定义策略授予用户组，使得用户组中的用户具备自定义策略中的权限。

说明

给用户组授予自定义策略与系统策略操作一致。

----结束

JSON 视图配置自定义策略

步骤 1 企业管理员使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 单击首页顶部控制台，在控制中心页面“管理与部署”分类中，单击“统一身份认证服务”。

步骤 3 在统一身份认证服务管理页面，单击左侧功能菜单“策略”后，单击右上角“＋创建自定义策略”按钮。

步骤 4 进入创建自定义策略页面，输入“策略名称”。

步骤 5 选择“作用范围”，即自定义策略的生效范围，根据服务的部署区域选择。

- 全局级服务：权限策略中该服务的“所属区域”为“全局区域”，表示该服务为全局级服务。创建全局级服务的自定义策略时，作用范围选择“全局级服务”。给用户组授予该自定义策略时，需要在全局区域中进行。
- 项目级服务：权限策略中该服务的“所属区域”为“除全局区域外其他区域”，表示该服务为项目级服务。创建项目级服务的自定义策略时，作用范围选择“项目级服务”。给用户组授予该自定义策略时，需要在除全局区域外其他区域中进行。

例如：创建 EVS 的自定义策略（"evs:volumes:create"），由于 EVS 服务属于项目级服务，作用范围必须选择项目级服务。

说明

如果一个自定义策略中包含多个服务的授权语句，这些服务必须是同一属性，即都是全局级服务或者项目级服务。如果需要同时设置全局服务和项目级服务的自定义策略，请创建两条自定义策略，“作用范围”分别为“全局级服务”以及“项目级服务”。

步骤 6 “策略配置方式”选择“JSON 视图”。

步骤 7 （可选）在“策略内容”区域，单击“从已有策略复制”，例如选择“VPC Admin”作为模板。

步骤 8 单击“确定”。

步骤 9 修改模板中策略授权语句。

- 作用（Effect）：允许（Allow）和拒绝（Deny）。
- 权限集（Action）：写入各服务 API 授权项列表中“授权项”的内容，例如："evs:volumes:create"，来实现细粒度授权。

说明

- 自定义策略版本号（Version）固定为 1.1，不可修改。

步骤 10 单击“校验语法”，如果系统提示语法错误，请按照语法规范进行修改。

步骤 11 （可选）输入“策略描述”。

步骤 12 单击“确定”，自定义策略创建完成，策略列表中显示新创建的策略。

步骤 13 将新创建的自定义策略授予用户组，使得用户组中的用户具备自定义策略中的权限。

说明

给用户组授予自定义策略与系统策略操作一致。

----结束

修改自定义策略

步骤 1 企业管理员使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 单击首页顶部控制台，在控制中心页面“管理与部署”分类中，单击“统一身份认证服务”。

步骤 3 在统一身份认证服务管理页面，单击左侧功能菜单“策略”后，选定待修改的自定义策略，单击右侧的“编辑”。

步骤 4 按照本章“可视化/Json 视图配置自定义策略”方式，修改策略内容。

步骤 5 单击“确定”完成策略修改。

----结束

删除自定义策略

须知

如果当前自定义策略已被授权给用户组或委托，则无法删除。移除该用户组或委托中的自定义策略后，才可删除自定义策略。

步骤 1 企业管理员使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 单击首页顶部控制台，在控制中心页面“管理与部署”分类中，单击“统一身份认证服务”。

步骤 3 在统一身份认证服务管理页面，单击左侧功能菜单“策略”后，选定待删除的自定义策略，单击右侧的“删除”。

步骤 4 在弹出的删除确认框中，单击“是”完成策略删除。

----结束

4.4 管理委托

4.4.1 委托其他账号管理资源

4.4.1.1 基本流程

通过委托信任功能，您可以将自己的操作权限委托给更专业、高效的其他账号或者云服务，账号或者云服务可以根据权限代替您进行日常资源管理工作。

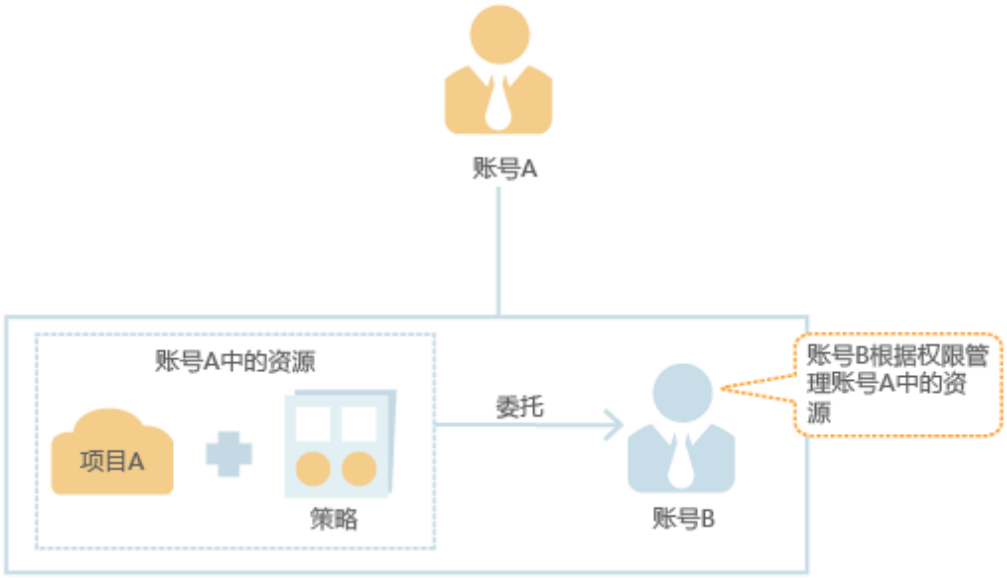
须知

只能对天翼云主帐号进行委托，不能对 IAM 子用户进行委托。

以账号 A 委托账号 B 管理账号 A 中的某些资源为例，说明委托的原理及方法。

步骤 1 账号 A 创建委托。

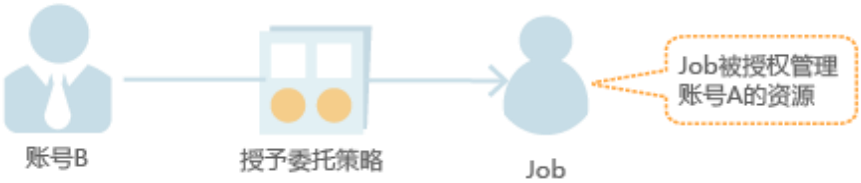
图4-4 创建委托模型



步骤 2 （可选）账号 B 分配委托权限，授予用户 Job 管理账号 A 的权限。

1. 创建用户组（如：Agency）并授予用户组管理委托的权限策略。
2. 将用户 Job 加入到用户组（Agency）中。

图4-5 委托授权模型



步骤 3 （可选）账号 B 或用户 Job 根据权限管理账号 A 的资源。

1. Job 登录系统，并切换角色到账号 A。
2. 切换到项目 A，并根据权限管理账号 A 的资源。

图4-6 管理委托模型

----结束

4.4.1.2 创建委托（委托方操作）

通过创建委托，可以将资源共享给其他帐号，或委托更专业的人或团队来代为管理资源。被委托方使用自己的帐号登录后，切换到委托方帐号，即可管理委托方委托的资源，避免委托方共享自己的安全凭证（密码/密钥）给他人，确保帐号安全。

操作步骤

步骤 1 委托方使用已注册的天翼云帐号登录天翼云网门户。

步骤 2 单击首页顶部控制台，在控制中心页面“管理与部署”分类中，单击“统一身份认证服务”。

步骤 3 在统一身份认证服务管理页面，单击左侧功能菜单“委托”。

步骤 4 在“委托”页面，单击“＋创建委托”。

步骤 5 在“创建委托”页面，输入“委托名称”、配置“委托类型”。

表4-2 委托类型

委托类型	描述
普通账号	系统的其他普通账号，用于将资源共享给其他天翼云账号或委托更专业的人或团队来代为管理账号中的资源。 须知 委托的帐号只能是天翼云主帐号，不能是 IAM 子用户。
云服务	系统的服务，用于授权云服务访问或者维护用户数据。例如，通过与 ECS 建立委托关系，ECS 可以获取用户的访问密钥调用 API 接口，帮助用户运维或者监控数据。 须知 委托类型为云服务的委托创建成功后，不支持修改。

- 如果选择“委托类型”为“普通账号”，在“委托的账号”中输入需要建立委托关系的其他天翼云账号的账号名。
- 如果选择“委托类型”为“云服务”，单击“选择”，选择需要委托管理的云服务。

步骤 6 设置“持续时间”及“描述”信息。

步骤 7 在“权限选择”区域中，单击需要设置的区域对应项目的“修改”，为委托企业配置权限策略。

须知

- 给委托授权即为给其他帐号授权，给用户组授权即为给帐号中的 IAM 用户授权，两者操作方法相同。
- 为了保障您的帐号安全，委托将不能添加 Security Administrator 权限，建议您按照业务场景为委托授予最小权限。

步骤 8 单击“确定”，委托创建完成

委托方操作完成，将自己的天翼云帐号名称、创建的委托名称、委托 ID 以及委托的资源权限告知被委托方后，被委托方可以通过切换角色至委托方帐号中管理委托资源。

----结束

后续操作

修改委托

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。

删除委托

如果不再需要使用委托，可以在委托列表中，单击委托右侧的“删除”，删除委托。

说明

删除委托后，将撤销被委托方帐号的权限，被委托方将无法管理您的委托资源，对您的其他业务合作伙伴没有影响。

4.4.1.3 分配委托权限（被委托方操作）

当其他帐号与您创建了委托关系，即您是被委托方，默认情况下只有较大权限的用户（帐号本身以及 admin 用户组中的成员）可以管理委托资源，如果您需要普通 IAM 用户帮助您管理委托，可以将管理委托的权限分配给 IAM 子用户。

前提条件

- 已有天翼云账号与您创建了委托关系。
- 您已经获取到委托方的账号名称、所创建的委托名称。

操作步骤

步骤 1 创建用户组并授权。

1. 被委托方使用天翼云帐号登录天翼云网门户。

2. 单击首页顶部控制台，在控制中心页面“管理与部署”分类中，单击“统一身份认证服务”。
3. 在统一身份认证服务左侧导航窗格中，单击“用户组”。
4. 在“用户组”界面中，单击“创建用户组”，在跳转页面中再次单击“创建用户组”。
5. 在弹出框中输入“用户组名称”、“描述”。
6. 单击“确定”。

   返回统一身份认证服务的用户组列表页面，用户组列表中显示新创建的用户组。
7. 单击新建用户组右侧的“修改”。
8. 在“用户组权限”区域中，单击需要授权项目右侧的“修改”。
9. 选择“Agent Operator”权限。

   说明

   具有“Agent Operator”权限的用户可以切换角色并访问委托方账号中的资源。
10. 单击“确定”完成用户组授权

步骤 2 创建 IAM 用户并加入用户组。

1. 在统一身份认证服务左侧导航菜单中，单击“用户”
2. 在“用户”界面，单击“创建用户”。在跳转页面中再次单击“创建子用户”。
3. 在弹出的“创建子用户”对话框，输入“邮箱”、“用户名”、“手机号”等用户基本信息。
4. 在“所属用户组”的下拉框中，选择步骤 1 中创建的用户组。
5. 单击“创建”，完成 IAM 子用户创建

----结束

后续操作

被委托方帐号或分配了委托权限的 IAM 用户登录天翼云后，均可以“切换角色”至委托方帐号中，查看并根据权限使用委托资源。

4.4.1.4 切换角色（被委托方操作）

当其他帐号与您创建了委托关系，即您是被委托方，您以及分配了委托权限的用户，可以切换角色至委托方帐号中，根据权限管理委托方的资源。

前提条件

- 已有账号与您创建了委托关系。
- 您已经获取到委托方的账号名称及所创建的委托名称。

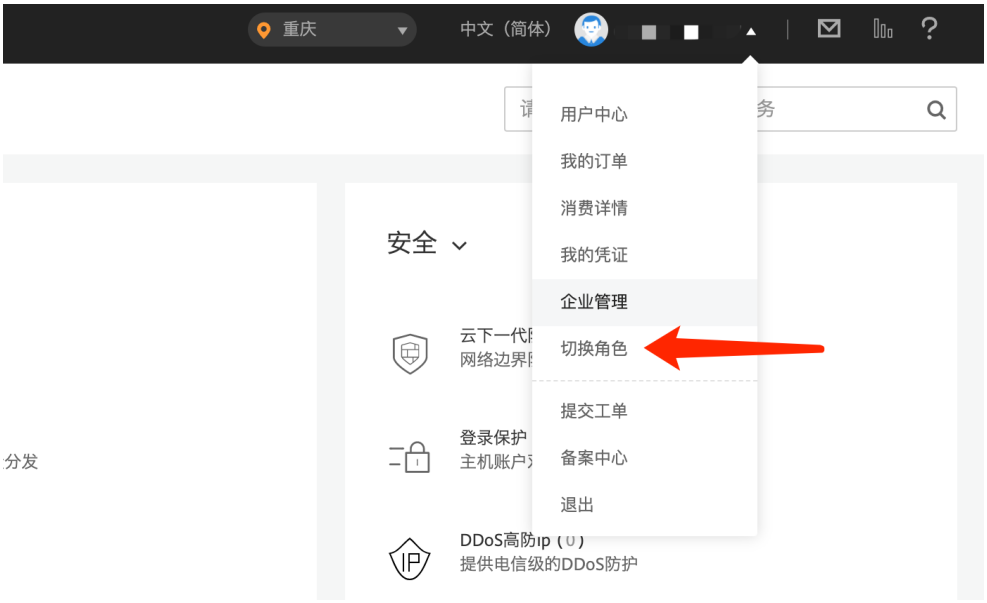
操作步骤

步骤 1 使用步骤 2 中新建的用户登录天翼云，单击页面顶部“控制台”。

说明

步骤 2 中新建的用户具有管理委托的权限，可以切换角色。

步骤 2 单击右上方已登录的账号，在下拉菜单中选择“切换角色”。



步骤 3 在“切换角色”页面中，输入委托方的账号、委托名称。

说明

输入账号名称后，系统将会按照顺序自动匹配委托名称，如果自动匹配的是没有授权的委托，系统将提示您没有权限访问，您可以删除委托名称，在下拉框中选择已授权的委托名称。

步骤 4 单击“确定”，切换至委托方账号中。

----结束

后续操作

单击右上角切换的委托账号，选择“切换角色”，可以返回到被委托方的账号。

4.4.2 委托其他云服务管理资源

由于云服务平台各服务之间存在业务交互关系，一些云服务需要与其他云服务协同工作，需要您创建云服务委托，将操作权限委托给该服务，让该服务以您的身份使用其他云服务，代替您进行一些资源运维工作。

当前 IAM 提供两种创建委托方式：

1. 在 IAM 控制台创建云服务委托

   以对象存储服务 OBS 为例：将操作权限委托给 OBS，允许 OBS 以您的身份使用其他服务，例如访问 AOM 读取监控数据。
2. 在云服务控制台使用某项资源时，系统提示您自动创建委托，以完成云服务间的协同工作。

以创建弹性文件服务 SFS 委托为例：

a. 在 SFS 控制台创建文件系统。

b. 在创建文件系统页面，开启“静态数据加密”。

c. 弹窗提示需要创建 SFS 委托，单击“确定”，系统自动为您在当前项目创建 SFS 委托，并授予 KMS CMKFullAccess 权限，授权成功后，SFS 可以获取 KMS 密钥用来加解密文件系统。

d. 您可以在 IAM 控制台的委托列表中查看已创建的委托。

在 IAM 控制台创建云服务委托

步骤 1 登录统一身份认证服务控制台。

步骤 2 在统一身份认证服务的左侧导航菜单中，单击“委托”。

步骤 3 在委托列表页面，单击右上角“＋创建委托”。

步骤 4 在创建委托页面，设置“委托名称”。

步骤 5 “委托类型”选择“云服务”，在“云服务”中选择需要授权的云服务。

步骤 6 选择“持续时间”。

步骤 7 （可选）填写“委托描述”。建议填写描述信息。

步骤 8 单击需要授权区域右侧的“修改”，并在“修改策略”弹窗中选择所需策略，单击“确定”，为委托授权。

步骤 9 单击“确定”，委托创建完成。

----结束

相关操作

- 修改委托

  如果需要修改云服务委托的权限，可以在委托列表中，单击委托右侧的“修改”，修改委托授权内容。

  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。
  - 修改权限后可能会影响该云服务部分功能的使用，请谨慎操作。

- 删除委托

  如果不再需要使用委托，可以在委托列表中，单击委托右侧的“删除”，删除委托。

4.5 管理用户凭证

当您通过天翼云界面控制台或者原生 API 访问云服务时，需要使用您的安全凭证，例如用户名、用户 ID 和访问秘钥等，您可以在“我的凭证”中查看这些安全凭证。

表4-3 用户凭证信息

基本信息	说明
用户名	用户的登录名，登录系统时需要提供。
用户 ID	用户在系统中的标识 ID，由系统自动生成。
账号名	账号的名称，账号是承担费用的主体（例如一个企业），在注册时自动创建，云服务资源按账号完全隔离。
账号 ID	账号在系统中的标识 ID，由系统自动生成。
已验证邮箱	用户绑定的邮箱地址，可以通过已验证邮箱登录系统或者重置密码，也可以接收验证码和系统推送信息。单击右侧的“修改”，可以修改绑定的邮箱。
已验证手机	用户绑定的手机号码，可以通过已验证手机登录系统或者重置密码，也可以接收验证码和系统推送信息。单击右侧的“修改”，可以修改绑定的手机。
项目	项目用于将云资源（计算资源、存储资源和网络资源等）进行分组和隔离。用户拥有的资源必须挂载在项目下，项目一般是一个资源池。通过不同的项目实现资源的隔离管理。
项目列表	账号可访问的项目列表，在访问云服务原生 API 时需要指定 project 参数。
访问密钥	用户的长期身份凭证 ，最多可创建两对，在访问云服务原生 API 时，调用者需要使用 AK/SK 进行加密签名。

4.5.1 查看我的凭证

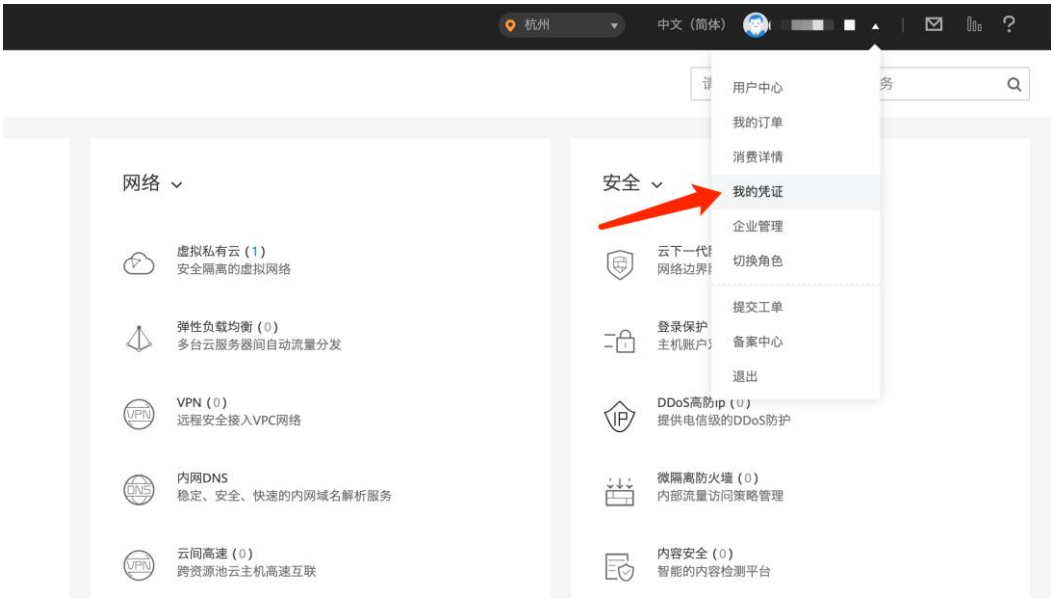
我的凭证是将用户的安全凭证信息进行集中展示与管理的服务，安全凭证包括已验证手机、已验证邮箱、用户 ID 和账号 ID 等。

操作步骤

步骤 1 用户使用天翼云帐号或 IAM 子用户登录天翼云网门户。

步骤 2 单击天翼云首页顶部右侧“控制台”。

步骤 3 在控制台首页顶部右侧，单击您的用户名，弹出下拉菜单。



步骤 4 单击“我的凭证”，进入凭证详情页，查看用户 ID、账号 ID 等凭证信息。

----结束

4.5.2 查看项目名称和项目 ID

项目 ID 是云服务所在资源池的 ID，如果您在调用原生 API 接口进行云资源管理（如创建 VPC）时，需要提供项目名称和 ID，可以在我的凭证中查看。

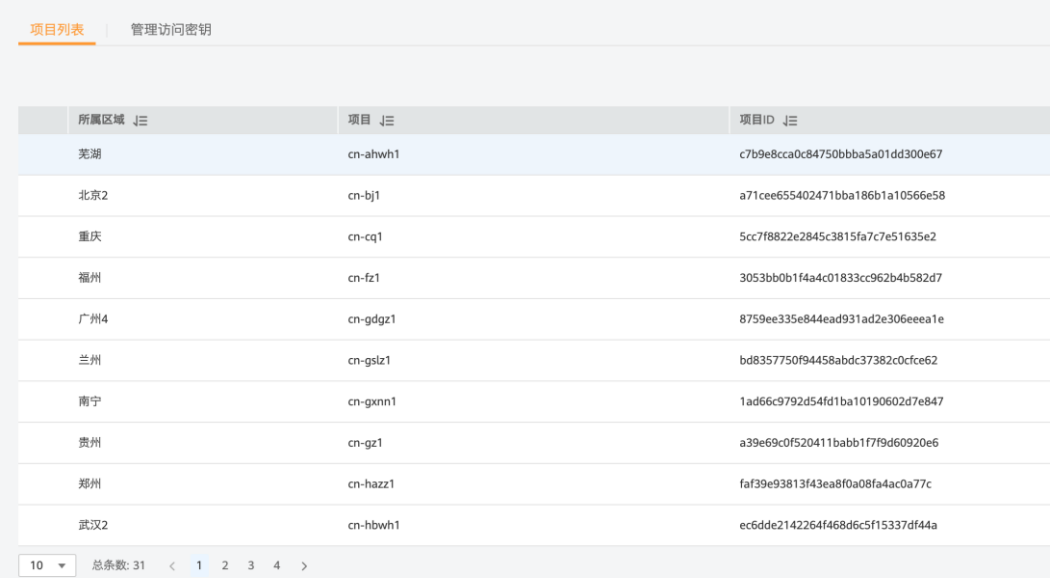
操作步骤

步骤 1 使用天翼云帐号或 IAM 子用户登录天翼云网门户。

步骤 2 单击天翼云首页顶部右侧“控制台”。

步骤 3 在控制台首页顶部右侧，单击您的用户名，弹出下拉菜单。

步骤 4 单击“我的凭证”进入凭证详情页，在“项目列表”页签中查看项目名称、项目 ID。



----结束

4.5.3 管理访问秘钥

访问密钥（AK/SK，Access Key ID/Secret Access Key）包含访问密钥 ID（AK）和秘密访问密钥（SK）两部分，是您在系统的长期身份凭证，您可以通过访问密钥对云服务原生 API 的请求进行签名。系统通过 AK 识别访问用户的身份，通过 SK 对请求数据进行签名验证，用于确保请求的机密性、完整性和请求者身份的正确性。

新增访问密钥

1. 登录天翼云并进入“控制台”页面，单击右上方的用户名，在下拉列表中选择“我的凭证”。
2. 在“我的凭证”页面，单击“管理访问密钥”页签。
3. 单击“新增访问密钥”，输入验证码。

说明

如果您绑定了邮箱或者手机，需要输入验证码，如果没有绑定邮箱或者手机，仅需要输入登录密码即可新增访问密钥。

4. 单击“确定”，生成并下载访问密钥。

说明

最多可创建 2 个访问密钥，有效期为永久。为了账号安全性，建议您妥善保管并定期修改访问密钥，修改访问密钥的方法为删除旧访问密钥，然后重新生成。

删除访问密钥

1. 在“管理访问密钥”页签中，单击待删除密钥右侧的“删除”。
2. 输入验证码，单击“确定”，删除访问密钥。

说明

- 如果您绑定了邮箱或者手机，需要输入验证码，如果没有绑定邮箱或者手机，仅需要输入登录密码即可删除访问密钥。
- 当您发现访问密钥被异常使用（包括丢失、泄露等情况），可以在我的凭证中自行删除访问密钥。

5 常见问题

5.1 权限管理类

5.1.1 无法找到特定服务的权限怎么办？

天翼云服务分为项目级服务和全局级服务两种，需正确选择权限作用范围才能找到特定权限。如对象存储 OBS 属于全局级服务，弹性云主机属于项目级服务。

如已正确选择服务级别仍无法找到服务，则该需要设置权限的服务暂不支持 IAM，可由企业管理员给对应云服务提交工单，申请该服务在 IAM 预置权限。

5.1.2 权限没有生效怎么办？

企业管理员在 IAM 控制台给 IAM 用户设置权限后，IAM 子用户登录天翼云后发现权限没有生效，无法使用服务。

可能原因 1：管理员授予 IAM 用户所在用户组的权限不正确。

解决方法：管理员确认并修改授予 IAM 用户所在用户组的权限，方法请参考：修改用户组权限。

可能原因 2：管理员授予的权限有依赖角色，没有同步设置依赖角色，导致权限没有生效。

解决方法：管理员为用户组增加有依赖的角色或服务授权。

可能原因 3：管理员给用户组授权后，忘记将 IAM 用户添加至用户组中。

解决方法：管理员将 IAM 用户添加至用户组中，方法请参见：用户组添加用户。

可能原因 4：对于区域级服务，管理员没有在在对应的区域进行授权。

解决方法：管理员在对 IAM 所在用户组授权时，选择对应的区域，方法请参见：用户组添加授权。

可能原因 5：对于区域级服务，IAM 用户登录控制台后，没有切换到授权区域。

解决方法：IAM 用户访问区域级服务时，请切换至授权区域资源池。

可能原因 6：管理员授予的 OBS 权限由于系统设计的原因，授权后需等待 15-30 分钟才可生效。

解决方法：请 IAM 用户和管理员等待 15-30 分钟后重试。

可能原因 7：浏览器缓存导致权限信息未更新。

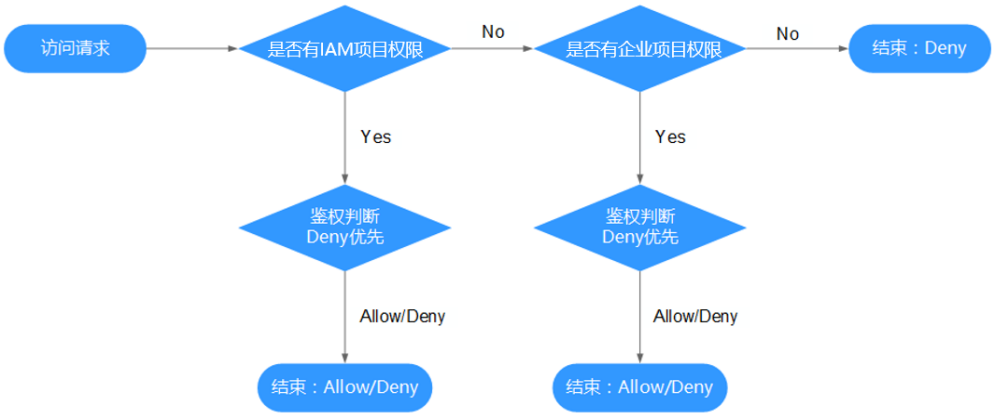
解决方法：请清理浏览器缓存后重试。

可能原因 8：该服务可能提供了独立于 IAM 的服务级权限控制机制。

解决方法：请查看对应服务的帮助文档，并授予用户对应的服务级权限。

5.1.3 同时设置了 IAM 和企业项目管理授权时的检查规则

用户在发起访问请求时，系统根据用户被授权的访问策略中的 action 进行鉴权判断。检查规则如下：



1. 用户发起访问请求。
2. 系统在用户被授予的访问权限中，优先寻找基于 IAM 项目授权的权限，在权限中寻找请求对应的 action。
3. 如果找到匹配的 Allow 或者 Deny 的 action，系统将返回对请求的鉴权决定，Allow 或者 Deny，鉴权结束。
4. 如果在基于 IAM 项目的权限中没有找到请求对应的 action，系统将继续寻找基于企业项目授权的权限，在权限中寻找请求对应的 action。
5. 如果找到匹配的 Allow 或者 Deny 的 action，系统将返回对请求的鉴权决定，Allow 或者 Deny，鉴权结束。

6. 如果用户不具备任何权限，系统将返回鉴权决定 Deny，鉴权结束。

5.2 项目管理类

5.2.1 IAM 与企业项目管理的区别

统一身份认证（Identity and Access Management，简称 IAM）服务是提供用户身份认证、权限分配、访问控制等功能的身份管理服务。

企业项目管理是提供给企业客户的与多层级组织和项目结构相匹配的云资源管理服务。主要包括企业项目管理。

与 IAM 相同的是，企业项目管理可以进行人员管理及权限分配；企业项目管理对资源的授权粒度比 IAM 的更为精细，建议中大型企业使用企业项目管理服务。

IAM 与企业项目管理的区别

- 资源隔离颗粒度：IAM 通过在区域中创建子项目，隔离同一个区域中的资源。以子项目为单位进行授权，用户可以访问指定子项目中的所有资源；企业项目管理通过创建企业项目，隔离企业不同项目之间的资源，企业项目中可以包含多个区域的资源。
- 支持的服务：各云服务与 IAM 和企业项目管理需分别对接实现权限控制，因此两者支持的云服务范围不同。

IAM 与企业项目管理的关系

IAM 和企业项目管理的用户授权功能，两边是相互同步关系。

申请开通企业项目管理服务后，使用企业项目管理中的用户组授权功能时，该功能依赖 IAM 的策略授权。如果企业项目管理中系统预置的策略不能满足您的使用要求，需要在 IAM 中创建自定义策略，自定义策略会同步到企业管理中，可以在 IAM 或者企业项目管理中给用户组授权自定义策略。

如果在 IAM 和企业项目管理中同时给用户组授权，用户同时拥有基于 IAM 的策略和基于企业项目的策略，在发起访问请求时，系统根据用户被授权的全部访问策略中的 Action 进行鉴权判断。

如果策略中包含相同的 Action，以在 IAM 中设置的为准。

例如，在 IAM 项目策略中包含以下 action：

```
{
  "Action": [
    "ecs:cloudServers:create"
  ],
  "Effect": "Deny"
}
```

在企业项目策略中包含以下 action：

```
{
  "Action": [
```

```
    "ecs:cloudServers:create"
  ],
  "Effect": "Allow"
}
```

用户请求创建云服务器，鉴权结果为 IAM 中定义的 Deny，用户不能创建云服务器。

如果策略中包含不同的 Action，则 IAM 和企业项目管理中设置的都生效。

例如，在 IAM 项目策略中包含以下 action：

```
{
  "Action": [
    "ecs:cloudServers:create"
  ],
  "Effect": "Allow"
}
```

在企业项目策略中包含以下 action：

```
{
  "Action": [
    "ecs:cloudServers:delete"
  ],
  "Effect": "Allow"
}
```

以上示例表示用户可以创建云服务器以及删除云服务器。

5.2.2 IAM 项目与企业项目的区别

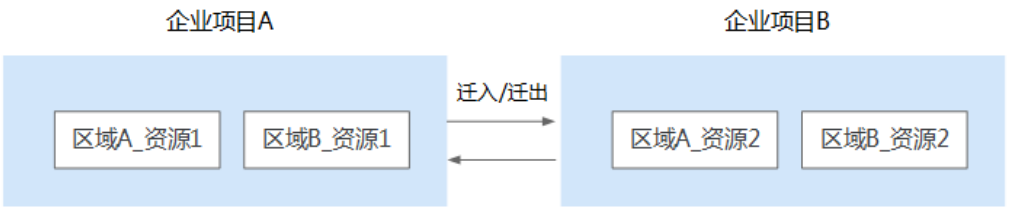
IAM 项目

IAM 项目是以每一个天翼云资源节点为粒度进行资源及服务隔离，是物理隔离。

IAM 项目与资源节点一一对应，IAM 项目中的资源不能转移，只能删除后重建。

企业项目

企业项目可理解为 IAM 项目的升级版，针对企业不同项目间资源的分组和管理，是逻辑隔离。



企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。企业项目可以实现对特定云资源的细粒度授权，例如：将一台特定的 ECS 添加至企业项目，对企业项目进行授权后，可以控制用户仅能管理这台特定的 ECS。

未来 IAM 项目将逐渐被企业项目所替代，推荐使用更为灵活的企业项目。

5.3 委托管理类

5.3.1 创建委托时提示权限不足怎么办

IAM 用户进入 IAM 控制台创建委托时，系统提示权限不足。

可能原因

- 该 IAM 用户不具备使用 IAM 的权限。

拥有 IAM 使用权限的对象为：

- 帐号：天翼云主帐号可以使用所有服务，包括 IAM。
- admin 用户组中的用户：IAM 默认用户组 admin 中的用户，可以使用所有服务，包括 IAM。
- 授予了“Security Administrator”或“Full Access”权限的用户：具备该权限的用户为 IAM 管理员，可以使用 IAM。

解决方法

- 由具备权限的管理员代为创建委托。
- 管理员为 IAM 用户授予使用 IAM 服务的权限。