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.....4
1.1 统一身份认证.....4
1.2 基本概念.....4
1.3 产品优势.....8
1.4 产品功能.....9
1.5 约束与限制.....10
2 购买指南.....12
2.1 资源节点.....12
2.2 计费说明.....12
3 快速入门.....13
3.1 示例场景.....13
3.2 步骤 1：创建用户组并授权.....14
3.3 步骤 2：创建 IAM 用户并登录.....16
4 用户指南.....18
4.1 IAM 用户.....18
4.1.1 创建 IAM 用户.....18
4.1.2 为 IAM 用户授权.....19
4.1.3 查看或编辑 IAM 用户信息.....20
4.1.4 管理 IAM 用户访问密钥.....21
4.2 用户组及授权.....22
4.2.1 创建用户组并授权.....22
4.2.2 用户组添加/移除用户.....24
4.2.3 查看/修改/删除用户组.....24
4.2.4 移除用户组权限.....25
4.2.5 依赖角色的授权方法.....25
4.3 权限管理.....26
4.3.1 权限基本概念.....26
4.3.2 角色.....27
4.3.3 策略.....29

4.3.3.1 策略内容 29
4.3.3.1 策略语法 29
4.3.3.1 策略鉴权 34
4.3.4 查看授权记录 35
4.3.5 自定义策略 36
4.3.5.1 创建自定义策略 36
4.3.5.2 修改、删除自定义策略 39
4.3.5.3 自定义策略使用样例 40
4.4 项目 43
4.5 委托 43
4.5.1 委托其他账号管理资源 43
4.5.1.1 基本流程 43
4.5.1.2 创建委托（委托方操作） 45
4.5.1.3 分配委托权限（被委托方操作） 47
4.5.1.4 切换角色（被委托方操作） 48
4.5.2 委托其他云服务管理资源 50
4.5.3 删除或修改委托 51
4.6 用户凭证 51
4.6.1 查看我的凭证和项目信息 52
4.6.2 管理访问秘钥 52
4.7 查看 IAM 操作记录 53
4.7.1 开通云审计服务 53
4.7.2 查看 IAM 的云审计日志 55
5 常见问题 56
5.1 权限管理类 56
5.1.1 无法找到特定服务的权限怎么办？ 56
5.1.2 权限没有生效怎么办？ 56
5.1.3 同时设置了 IAM 和企业项目管理授权时的检查规则 57
5.2 项目管理类 58
5.2.1 IAM 与企业项目管理的区别 58
5.2.2 IAM 项目与企业项目的区别 59
5.2.3 区域和可用区 60
5.3 委托管理类 61
5.3.1 创建委托时提示权限不足怎么办 61
5.4 秘钥凭证类 61
5.4.1 如何获取访问密钥 AK/SK 61
5.4.2 丢失访问密钥 AK/SK 怎么办 61
5.4.3 什么是临时安全凭证（临时 AK/SK 和 SecurityToken） 62

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，是提供用户权限管理的基础服务，可以帮助您安全的控制云服务和资源的访问及操作权限。

IAM 服务免费使用，您只需要为您帐号中的云服务和资源进行付费。

1.2 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、身份凭证、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、分配用户权限等。

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

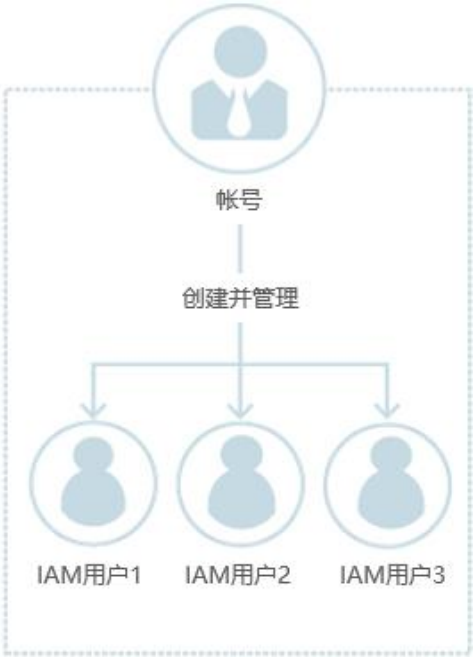
由帐号在 IAM 中创建的用户，一般为具体云服务的使用人员，具有独立的身份凭证（密码和访问密钥），根据帐号授予的权限使用资源。

如果您忘记了 IAM 用户的登录密码，可以在天翼云网门户“账号中心 > 子用户”中重置密码。

帐号与 IAM 用户的关系

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。

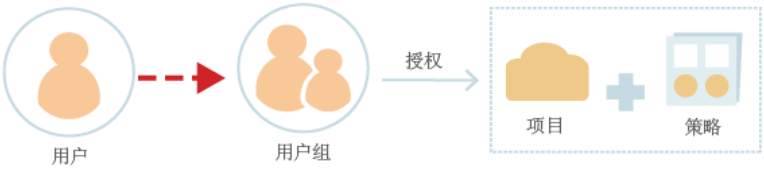
图1-1 账号与 IAM 用户



授权

授权是您将完成具体工作所需要的权限授予 IAM 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1-2 授权



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

权限

如果您仅授予 IAM 用户 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1-4 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主机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。

- 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。目前支持可视化视图、JSON 视图进行自定义策略配置。

图1-5 权限策略示例

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

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 访问云服务时，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。
- 访问秘钥：即 AK/SK（Access Key ID/Secret Access Key），调用云服务 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。

项目

每个资源池默认对应一个项目，目前这个项目由系统预置，用来隔离各资源池的资源（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。

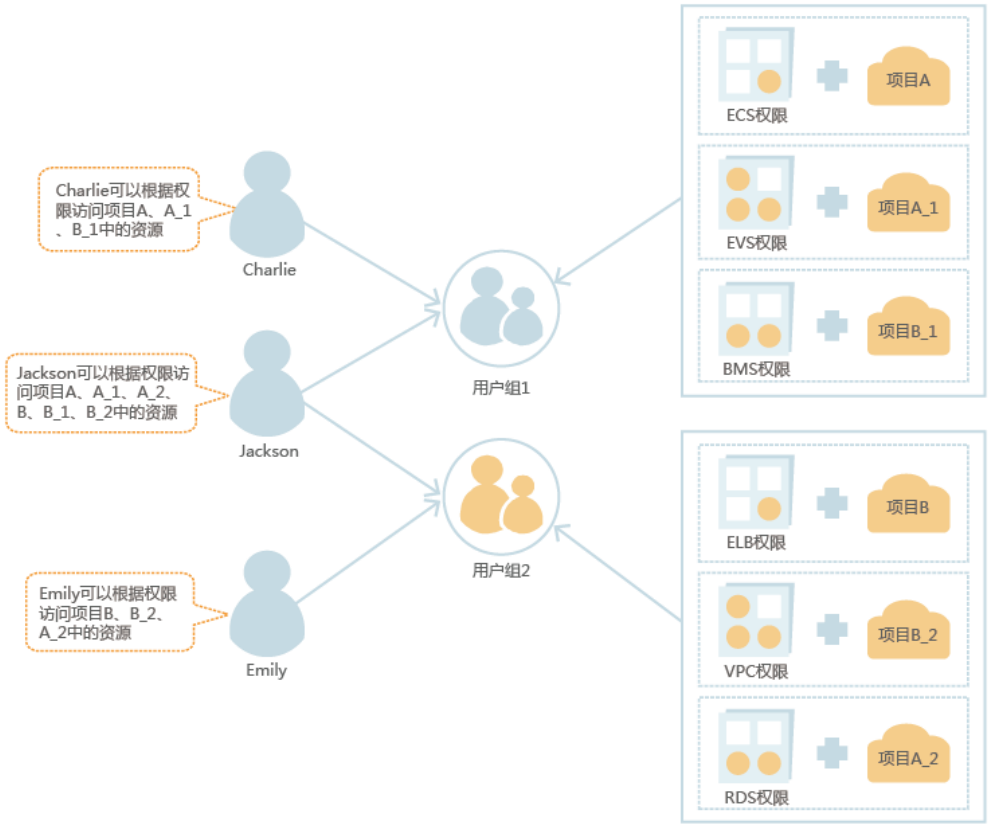
- 委托其他天翼云帐号：通过委托信任功能，您可以将自己帐号中的资源操作权限委托给其他帐号，被委托的帐号可以根据权限代替您进行资源运维工作。
- 委托其他云服务：由于云服务之间存在业务交互关系，一些云服务需要与其他云服务协同工作，需要您创建云服务委托，将操作权限委托给该服务，让该服务以您的身份使用其他云服务，代替您进行一些资源运维自动化工作。

1.3 产品优势

对资源进行精细访问控制

您注册后，系统自动创建帐号，帐号是对其所拥有的资源具有完全控制权限，可以访问系统中所有的云服务。

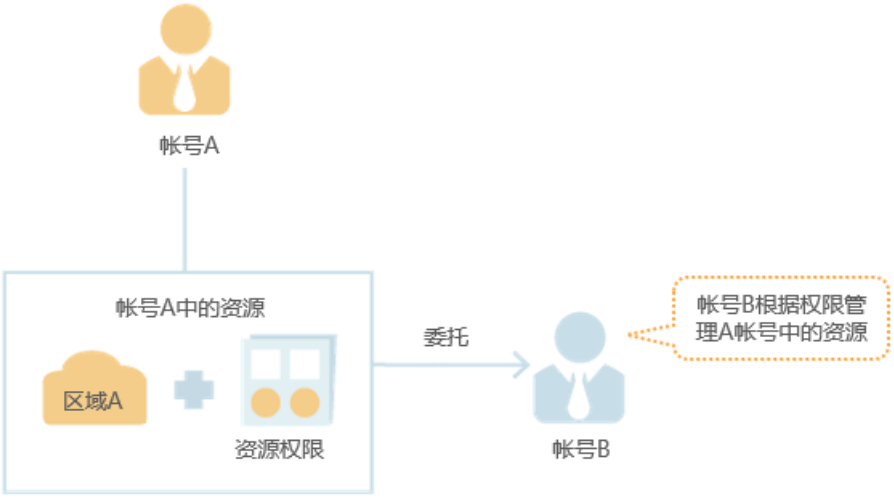
如果您创建了多种资源，例如弹性云主机、云硬盘、物理机等，您的团队或应用程序需要使用您的资源，您可以为员工或应用程序创建 IAM 用户，并授予 IAM 用户刚好能完成工作所需的权限，新创建的 IAM 用户可以使用自己单独的用户名和密码登录云服务平台。IAM 用户的作用是多用户协同操作同一帐号时，避免分享帐号的密码。



跨帐号的资源操作与授权

如果您创建了多种资源，其中一种资源希望由其它帐号管理，您可以使用 IAM 提供的委托功能。

例如您希望将资源委托给一家专业的代运维公司来运维，通过 IAM 的委托功能，代运维公司可以使用自己的帐号对您委托的资源进行运维。当委托关系发生变化时，您可以随时修改或撤消对代运维公司的授权。下图中帐号 A 即为委托方，帐号 B 为被委托方。



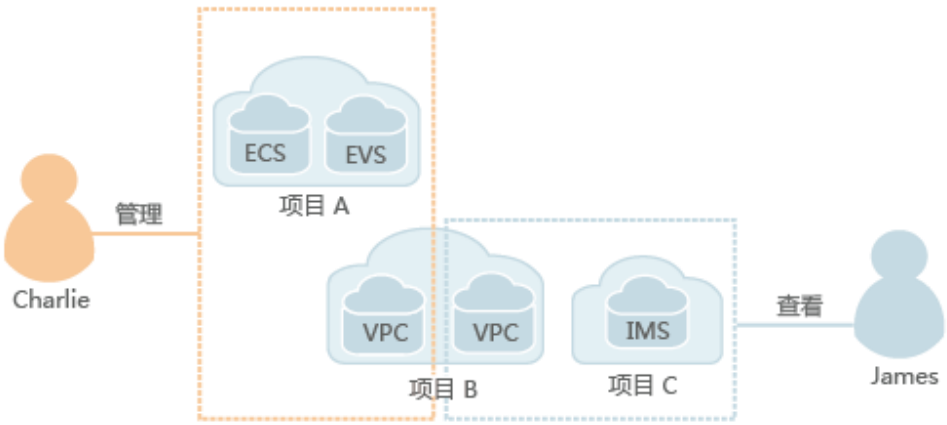
1.4 产品功能

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。例如：控制用户 Charlie 能管理项目 B 的 VPC，而让用户 James 只能查看项目 B 中 VPC 的数据。

图1-6 权限管理模型



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更专业、高效的其他帐号或者云服务，这些账号或者云服务可以根据权限代替您进行日常工作。

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。

限制分类	限制项	限制值	是否支持修改
用户	IAM 用户数	50	√
	用户名的字符数	32	x
	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
用户组	用户组数	20	√
	用户组名的字符数	64	x
	一个用户组中可添加的用户数	帐号下的 IAM 用户数	x
	一个用户组基于 IAM 项目可绑定的权限数（包括系统权限和自定义策略）	200	√
策略	策略名称的字符数	64	x
自定义策略	自定义策略个数	128	√
	字符数	6144	x
	Statement	8 个/策略	x
	Action	100 个/Statement Action 数组	x

限制分类	限制项	限制值	是否支持修改
	Resource	10 个/Statement Resource 数组	x
	Condition	10 个/statement Condition 数组	x
委托	委托数	50	√
	委托名称的字符数	64	x
	一个委托可绑定的权限数（包括系统权限和自定义策略）	200	√

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、华北。

2.2 计费说明

统一身份认证 IAM 服务目前免费。

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。

业务场景

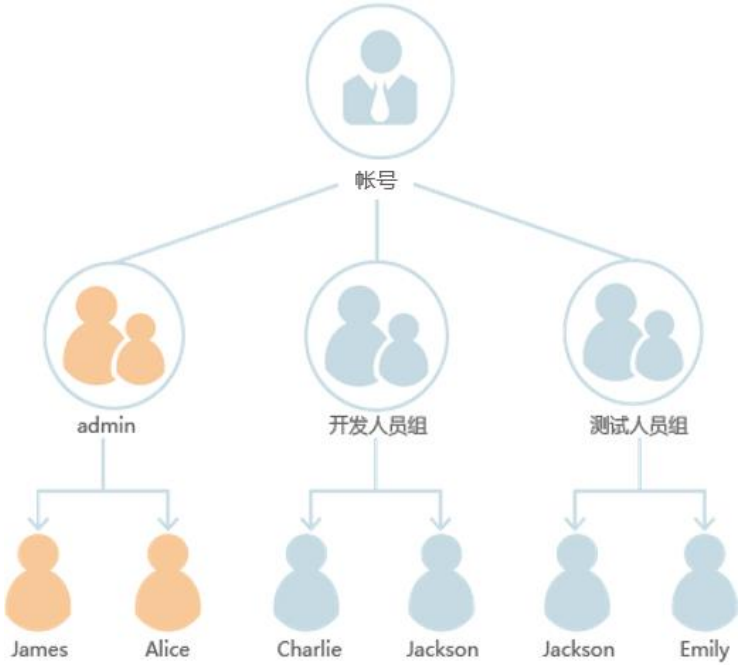
A 公司是一家负责网站开发的公司，公司中有三个职能团队。为了方便 A 公司统一创建、分配资源并管理用户，A 公司的人员不需要每人都注册帐号，而是由公司的管理员注册一个帐号，在这个帐号下创建 IAM 用户并分配权限，然后将创建的 IAM 用户分发给公司的人员使用。

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（对应下图中的“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（对应下图中的“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（对应下图中的“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，需要使用弹性云主机（ECS）、虚拟私有云（VPC）以及云硬盘（EVS）。
- 测试人员主要负责网站的监控及测试，需要使用云监控服务（CES）。

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：创建用户组并授权。
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 2：创建 IAM 用户并登录。

3.2 步骤 1：创建用户组并授权

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。

创建用户组

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

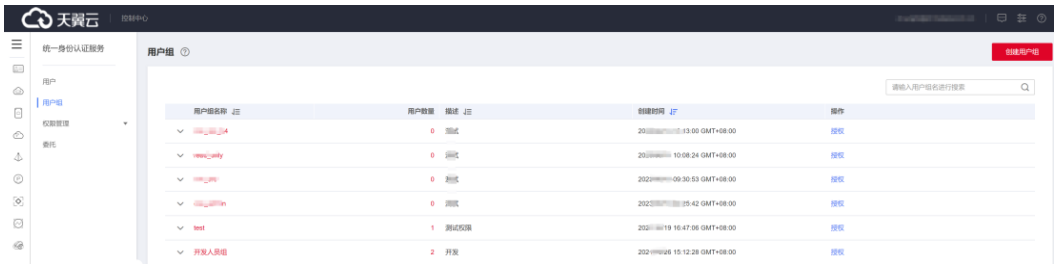
给用户组授权

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 CES，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。

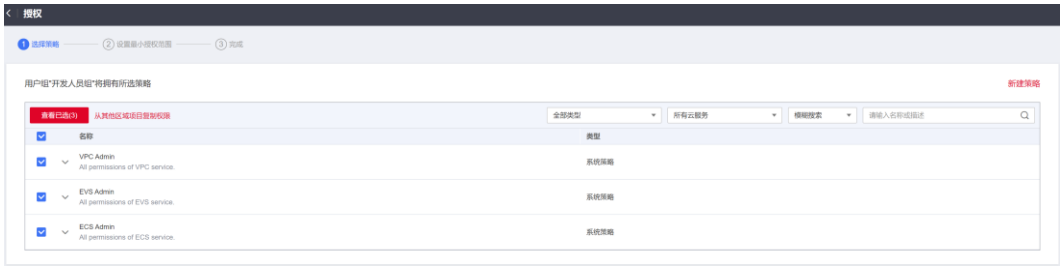
步骤 1 A 公司管理员使用已注册的天翼云帐号登录天翼云网门户。

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

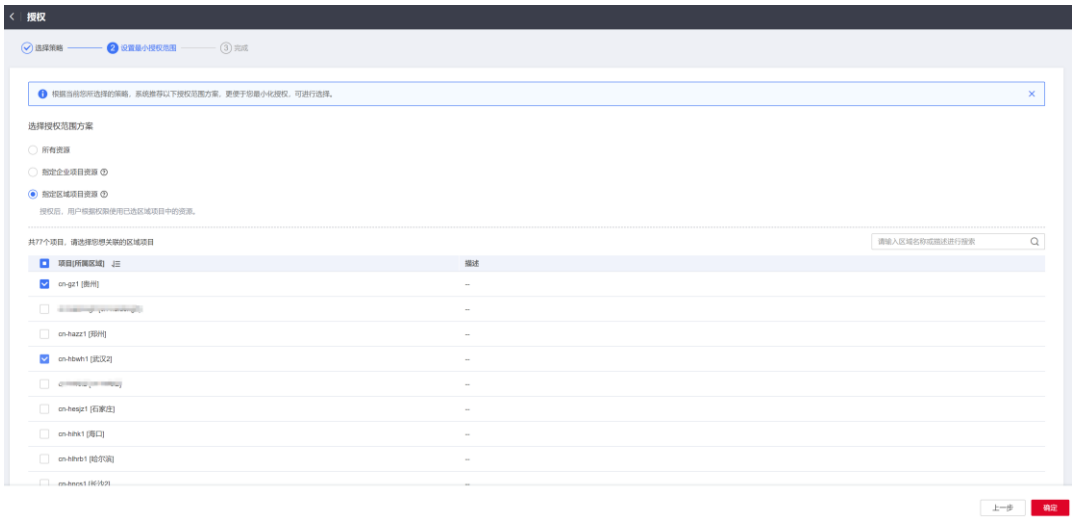
步骤 3 在统一身份认证服务控制台页面，单击左侧功能菜单“用户组”，找到已创建的“开发人员组”用户组，单击右侧 “授权”。



步骤 4 在用户组权限管理页面，勾选需要授予用户组的服务权限，如在本例中，为“开发人员组”添加 ECS Admin、VPC Admin 和 EVS Admin 三个策略授权，然后单击“下一步”。



步骤 5 选择授权范围方案为“指定区域项目资源”，并选择要授权的区域项目，即资源池，然后单击“确定”。完成设置后，开发人员组仅在授权的区域有操作权限，其它区域将提示没有权限。



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，为“测试人员组”授予“CES Administrator ”的权限。

----结束

3.3 步骤 2：创建 IAM 用户并登录

步骤 1 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。

创建 IAM 用户

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”。

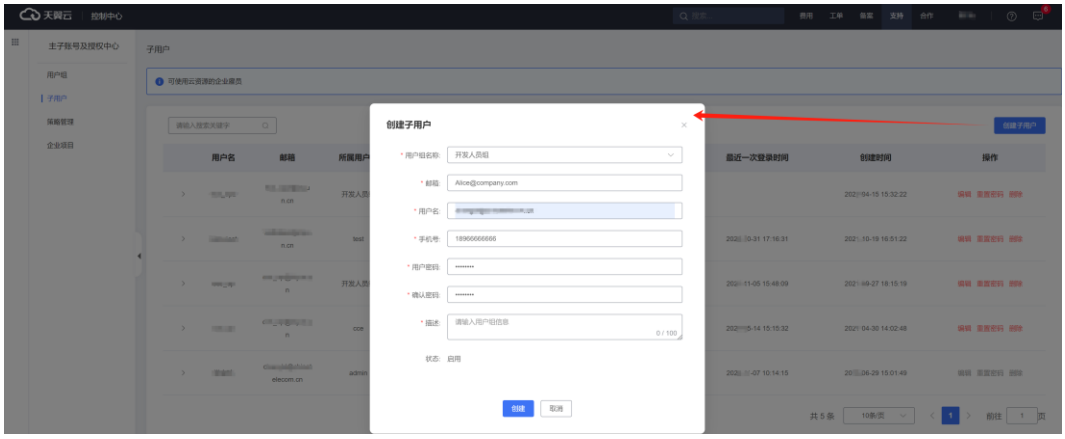
步骤 4 在主子账号及授权管理页，单击左侧导航菜单中的“子用户”。

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

IAM 用户登录

通过前述步骤，A 公司已在其天翼云帐号中创建了名为 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及各云服务平台。

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。

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 IAM 用户

4.1.1 创建 IAM 用户

如果您是管理员，在云服务平台创建了多种资源，例如弹性云主机、云硬盘、物理机等，您需要将资源分配给企业中不同的员工或者应用程序使用，为了避免分享自己的帐号密码，您可以使用天翼云网门户的用户管理功能，给员工或应用程序创建 IAM 用户。

默认情况下，**新创建的 IAM 用户没有任何权限**，管理员需要为其授予权限，或将其加入用户组，并给用户组授权，用户组中的用户将获得用户组的权限。IAM 用户拥有权限后，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。

如果删除并重新创建同名用户，则需要重新授权。

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”。

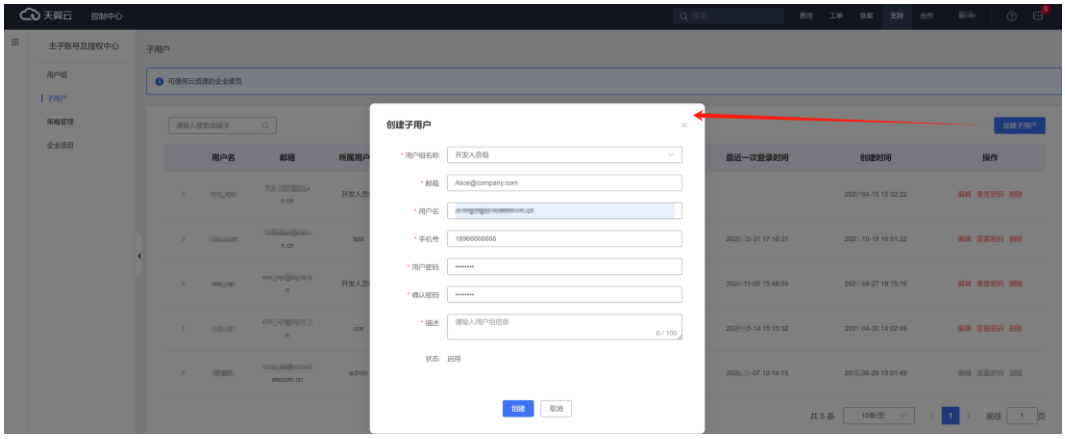
步骤 4 在主子账号及授权管理页，单击左侧导航菜单中的“子用户”。

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

4.1.2 为 IAM 用户授权

如果管理员在创建 IAM 用户时，没有将其加入任何用户组，**则新创建的 IAM 用户不具备任何权限，不能对云服务进行操作**，管理员可以在 IAM 控制台或天翼云网门户将其加入用户组，为其授予所属用户组的权限策略。授权后，用户即可根据用户组权限使用帐号中的云服务资源。

基于用户组授权

步骤 1 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 找到计划加入的用户组，单击右侧的“用户管理”。

步骤 6 选择 IAM 子用户，单击“确认”，将 IAM 用户加入用户组，加入用户组后，IAM 用户将拥有所属用户组的所有权限。

说明

- 如果将 IAM 用户加入默认用户组“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。
- **所有使用 IAM 授权的云服务的系统策略，请参见：权限集。**
- 如果您开通了企业管理，将不能创建 IAM 项目，请谨慎操作。

基于企业项目授权

步骤 1 管理员登录 IAM 控制台。

步骤 2 管理员在用户列表中，单击用户名称，进入 IAM 用户详情页面。

步骤 3 在 IAM 用户详情页面，单击“授权记录”页签，然后单击“授权”，可**直接给用户授权（适用于企业项目授权）**，直接给 IAM 用户授予云服务权限，勾选对应的云服务权限后，单击“下一步”。

说明

- 该授权方式仅在您开通企业项目后支持。

步骤 4 在“设置最小授权范围”页面，选择授权 IAM 用户使用的企业项目。

步骤 5 单击“确定”，完成 IAM 用户授权。

授权完成后，管理员可以在“权限管理>授权管理”页面查看、修改该 IAM 用户的权限。

----结束

4.1.3 查看或编辑 IAM 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 管理 IAM 用户访问密钥

访问密钥即 AK/SK（Access Key ID/Secret Access Key），是您通过开发工具（API、SDK）访问部分云服务平台时的身份凭证，不能登录控制台。系统通过 AK 识别访问用户的身份，通过 SK 进行签名验证，通过加密签名验证可以确保请求的机密性、完整性和请求者身份的正确性。

说明

目前支持通过 AK/SK 访问的云服务包括对象存储 OBS。

如果 IAM 用户不能登录控制台，在需要使用访问密钥或者访问密钥遗失的情况下，可以由管理员在 IAM 中管理 IAM 用户的访问密钥。

管理员在 IAM 用户列表中，单击用户名称进入用户详情页，然后单击右侧的“安全设置”页签，新增或者删除用户的访问密钥。

说明

- IAM 提供的“安全设置”功能，适用于管理员管理 IAM 用户的访问密钥。在我的凭证中也可以管理访问密钥，我的凭证适用于所有用户在可以登录控制台的情况下，自行管理访问密钥。
- 帐号和 IAM 用户的访问密钥是单独的身份凭证，即帐号和 IAM 用户仅能使用自己的访问密钥进行 API 调用。

- 新增访问密钥并下载
  a. 单击“新增访问密钥”。

说明

每个用户最多可以拥有 2 个访问密钥，有效期为永久。为了帐号安全性，建议管理员定期给用户更换访问密钥。

  b. 若开启操作保护，则管理员需输入验证码或密码。
  c. 单击“确定”，生成并下载访问密钥后，将访问密钥提供给用户。
- 删除访问密钥
  a. 单击“删除”。
  b. 若开启操作保护，则管理员需输入验证码或密码。
  c. 单击“确定”。
- 启用、停用访问密钥

新创建的访问密钥默认为启用状态，如需停用该访问密钥，步骤如下：

a. 在“访问密钥”页签中，在需要停用的访问密钥右侧单击“停用”。

b. 若开启操作保护，则需输入验证码或密码。然后单击“是”，停用访问密钥。

启用访问密钥方式与停用类似，请参考以上步骤。

4.2 用户组及授权

4.2.1 创建用户组并授权

管理员可以创建用户组，并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 预置了各服务的常用权限，例如管理员权限、只读权限，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操作。

创建用户组

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

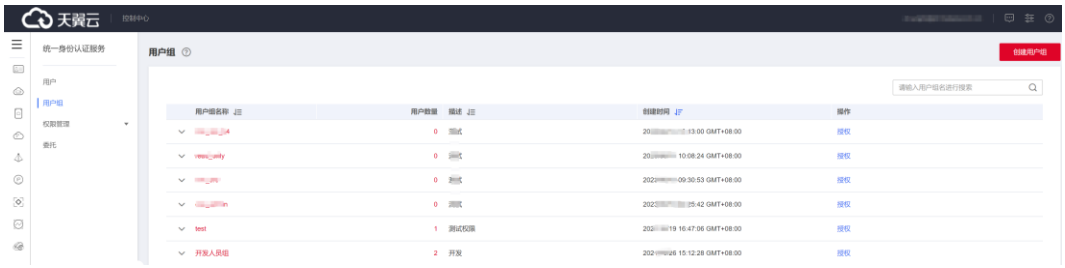
给用户组授权

以下步骤仅适用于给用户组新增权限。如需移除权限，请参见移除用户组权限。

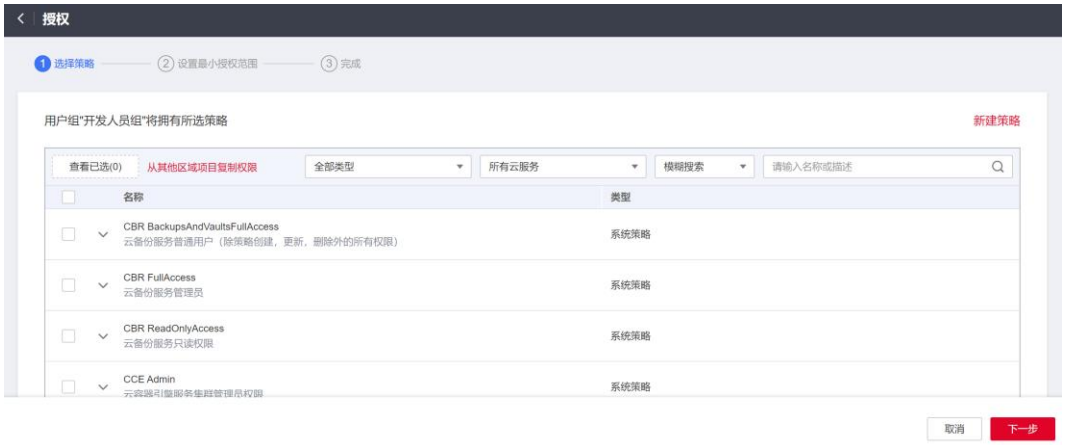
步骤 1 企业管理员使用已注册的天翼云帐号登录天翼云网门户。

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 “授权”。



步骤 4 用户组选择策略页面中，勾选需要授予用户组的权限。单击“下一步”。



如果系统策略不满足授权要求，可以单击权限列表右上角的“新建策略”创建自定义策略，并勾选新创建的策略来进行精细的权限控制，自定义策略是对系统策略的扩展和补充。详情请参考创建自定义策略。

步骤 5 选择权限的作用范围。系统会根据您所选择的策略，自动推荐授权范围方案，便于为用户选择合适的授权作用范围，下表为 IAM 提供的所有授权范围方案。

表4-1 授权范围方案

可选方案	方案说明
所有资源	IAM 用户可以根据权限使用帐号中所有的区域项目、全局服务资源。
指定企业项目资源	选择指定企业项目，IAM 用户可以根据权限使用该企业项目中的资源。**仅开通企业项目后可选。** 如果您暂未开通企业项目，将不支持基于企业项目授权。
指定区域项目资源	选择指定区域项目，IAM 用户可以根据权限使用该区域项目中的资源。 如果选择作用范围为“区域项目”，且所勾选的策略包含全局服务权限，系统自动将全局服务权限的作用范围设置为**所有资源**，勾选的区域项目权限的作用范围仍为指定区域项目。
全局服务资源	IAM 用户可以根据权限使用全局服务。全局服务部署时不区分物理区域。访问全局级服务时，不需要切换区域，如对象存储服务（OBS）等。 如果选择作用范围为“全局服务”，且所勾选的策略包含项目级服务权限，系统自动将项目权限作用范围设置为**所有资源**，勾选的全局服务权限的作用范围仍为全局服务。

步骤 6 单击“确定”，完成用户组授权。

----结束

4.2.2 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

4.2.3 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

4.2.4 移除用户组权限

操作步骤

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名称，进入用户组详情页。

步骤 4 在“授权记录”页签下，单击需要移除权限右侧的“删除”。

步骤 5 在弹窗中，单击“是”，移除用户组权限。

----结束

4.2.5 依赖角色的授权方法

由于云服务平台各服务之间存在业务交互关系，个别服务的角色依赖其他服务的角色实现功能。因此管理员在基于角色授权时，对于有依赖则需要授予依赖的角色才会生效。策略不存在依赖关系，不需要进行依赖授权。

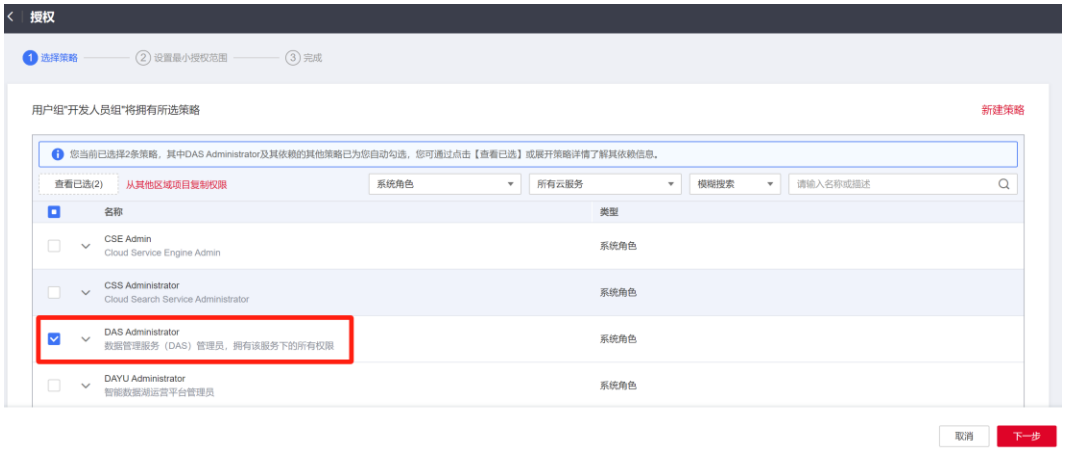
操作步骤

步骤 1 管理员登录 IAM 控制台。

步骤 2 在用户组列表中，单击新建用户组右侧的“授权”。

步骤 3 在授权页面进行授权时，管理员在权限列表的搜索框中搜索需要的角色。

步骤 4 选择角色，系统将自动勾选依赖角色。



步骤 5 单击勾选权限下方的 ，查看角色的依赖关系。

例如“DAS Administrator”，角色内容中存在“Depends”字段，表示存在依赖关系。给用户组授予“DAS Administrator”角色时，还需要在同项目同时授予“Tenant Guest”角色，“DAS Administrator”才能生效。

步骤 6 单击“确定”，完成依赖角色的授权。

----结束

4.3 权限管理

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 用户仅能对云主机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。

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。具体可参见“用户组及授权 > 依赖角色的授权方法”

角色内容

给用户组选择角色时，单击角色前面的 ，可以查看角色的详细内容，以“DAS Administrator”为例，说明角色类权限的内容。

参数说明

表4-2 参数说明

参数		含义	值
Version		角色的版本	1.0：代表基于角色的访问控制。 1.1：代表基于策略的访问控制。
Statement： 角色的授权语句	Action：授权项	操作权限	格式为：服务名:资源类型:操作 "DAS:DAS:*"：表示对 DAS 服务中 DAS 资源的所有操作。其中“DAS”为服务名；“DAS”为资源类型；“*”为通配符，表示对 DAS 资源类型可以执行所有操作。
	Effect：作用	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。 **说明** 当同一个 Action 的 Effect 既有 Allow 又有 Deny 时，遵循 Deny 优先的原则。
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	依赖的角色名称	角色名称。 **说明** 给用户组授予示例的“DAS Administraor”角色时，必须同时勾选该角色依赖的角色“Tenant Guest”，“DNS Administraor”才会生效。

4.3.3 策略

4.3.3.1 策略内容

给用户组选择策略时，单击策略前面的 ，可以查看策略的详细内容，以系统策略“IAM ReadOnlyAccess”为例。

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

4.3.3.1 策略语法

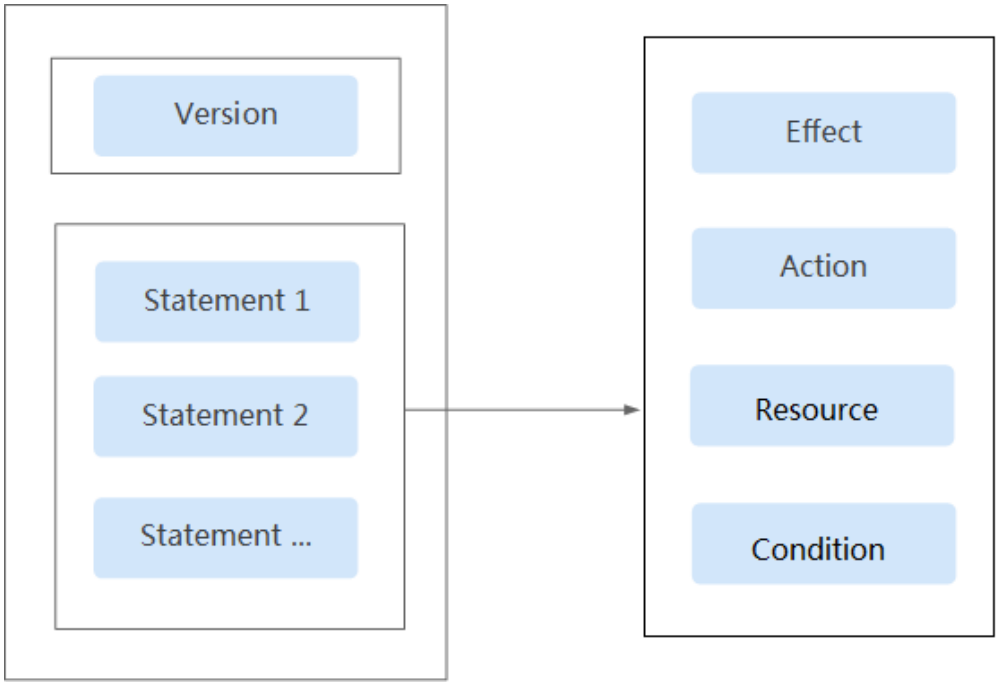
以 OBS 的自定义策略为例，说明策略的语法。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:bucket:ListAllMyBuckets",
                "obs:bucket:HeadBucket",
                "obs:bucket:ListBucket",
                "obs:bucket:GetBucketLocation"
            ],
            "Condition": {
                "StringEndWithIfExists": {
                    "g:UserName": [
                        "specialCharactor"
                    ]
                },
                "Bool": {
                    "g:MFAPresent": [
                        "true"
                    ]
                }
            },
            "Resource": [
                "obs:*:*:bucket:*"
            ]
        }
    ]
}
```

策略结构

策略结构包括 Version（策略版本号）和 Statement（策略权限语句）两部分，其中 Statement 可以有多个，表示不同的授权项。

图4-1 策略结构



策略参数

策略参数包含 Version 和 Statement 两部分，下面介绍策略参数详细说明。了解策略参数后，您可以根据场景自定义策略。

表4-3 策略参数说明

参数		含义	值
Version		策略的版本。	1.0：代表基于角色的访问控制。 1.1：代表基于策略的访问控制。
Statement： 策略的授权语句	Effect：作用	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。 说明 当同一个 Action 的 Effect 既有 Allow 又有 Deny 时，遵循 Deny 优先的原则。

参数		含义	值
	Action：授权项	操作权限。	格式为“服务名:资源类型:操作”。授权项支持通配符号*，通配符号*表示所有。 示例： "obs:bucket:ListAllMybuckets"：表示查看 OBS 桶列表权限，其中 obs 为服务名，bucket 为资源类型，ListAllMybuckets 为操作。 您可以在对应服务的 API 接口资料中查看该服务所有授权项。
	Condition：条件	使策略生效的特定条件，包括条件键和运算符。	格式为“条件运算符:{条件键：[条件值 1,条件值 2]}”。 如果您设置多个条件，同时满足所有条件时，该策略才生效。 示例: "StringEndWithIfExists":{"g:UserName":["specialCharactor"]}：表示当用户输入的用户名以"specialCharactor"结尾时该条 statement 生效。
	Resource:资源类型	策略所作用的资源。	格式为“服务名:region:domainId:资源类型:资源路径”，资源类型支持通配符号*，通配符号*表示所有。 示例： • "obs:*:*:bucket:*"：表示所有的 OBS 桶。 • "obs:*:*:object:my-bucket/my-object/*"：表示 my-bucket 桶 my-object 目录下的所有对象。

- **条件键**

  条件键表示策略语句的 Condition 元素中的键值。根据适用范围，分为全局条件键和服务条件键。

  - 全局级条件键（前缀为 g:）适用于所有操作，IAM 提供**通用全局条件键**。
    - 通用全局条件键：在鉴权过程中，云服务不需要提供用户身份信息，IAM 将自动获取并鉴权。详情请参见表-通用全局条件键。
  - 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，详情请参见对应云服务的用户指南。

表4-4 通用全局条件键

全局条件键	类型	说明
g:CurrentTime	时间	接收到鉴权请求的时间。以 ISO 8601 格式表示，例如：2012-11-11T23:59:59Z
g:DomainName	字符串	帐号名称
g:MFAPresent	布尔值	是否使用 MFA 多因素认证方式获取 Token
g:MFAAge	数值	通过 MFA 多因素认证方式获取的 Token 的生效时长。该条件需要和 g:MFAPresent 一起使用
g:ProjectName	字符串	项目名称
g:ServiceName	字符串	服务名称
g:UserId	字符串	IAM 用户 ID
g:UserName	字符串	IAM 用户名

- **运算符**

  运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，策略才能生效，详情请参见下表。运算符可以增加后缀“IfExists”，表示对应请求值为空或满足条件的请求值均使策略生效，如“StringEqualsIfExists”表示请求值为空或请求值等于条件值均使策略生效。

表4-5 运算符（字符串型运算符，如未增加说明，不区分大小写。）

运算符	类型	说明
StringEquals	字符串	请求值等于条件值（区分大小写）
StringNotEquals	字符串	请求值不等于条件值（区分大小写）
StringEqualsIgnoreCase	字符串	请求值等于条件值
StringNotEqualsIgnoreCase	字符串	请求值不等于条件值
StringLike	字符串	请求值包含条件值
StringNotLike	字符串	请求值不包含条件值
StringStartWith	字符串	请求值以条件值开头
StringEndWith	字符串	请求值以条件值结尾
StringNotStartWith	字符串	请求值不以条件值开头
StringNotEndWith	字符串	请求值不以条件值结尾

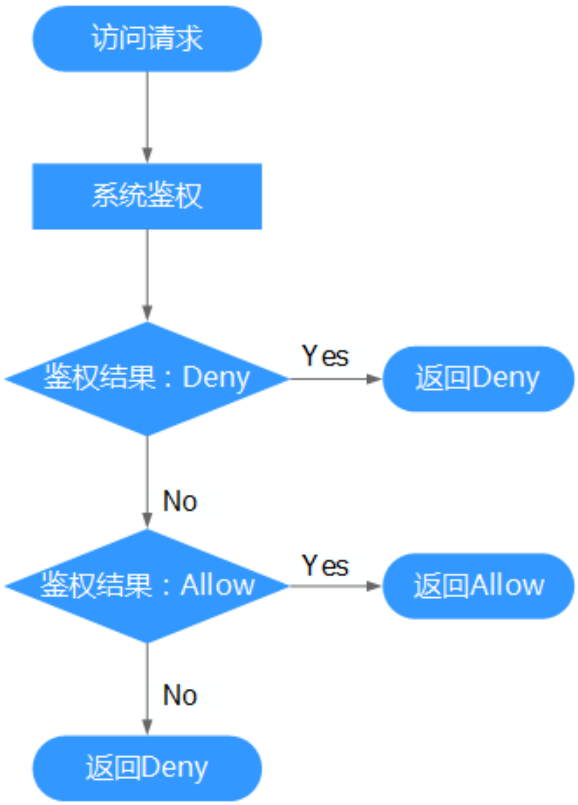
运算符	类型	说明
StringEqualsAnyOf	字符串	可配置多个条件值，请求值与任意一个条件值相同（区分大小写）
StringNotEqualsAnyOf	字符串	可配置多个条件值，请求值与所有条件值都不同（区分大小写）
StringEqualsIgnoreCaseAnyOf	字符串	可配置多个条件值，请求值与任意一个条件值相同
StringNotEqualsIgnoreCaseAnyOf	字符串	可配置多个条件值，请求值与所有条件值都不同
StringLikeAnyOf	字符串	可配置多个条件值，请求值包含任意一个条件值
StringNotLikeAnyOf	字符串	可配置多个条件值，请求值不包含所有条件值
StringStartWithAnyOf	字符串	可配置多个条件值，请求值以任意一个条件值开头
StringEndWithAnyOf	字符串	可配置多个条件值，请求值以任意一个条件值结尾
StringNotStartWithAnyOf	字符串	可配置多个条件值，请求值不以任意一个条件值开头
StringNotEndWithAnyOf	字符串	可配置多个条件值，请求值不以任意一个条件值结尾
NumberEquals	数值	请求值等于条件值
NumberNotEquals	数值	请求值不等于条件值
NumberLessThan	数值	请求值小于条件值
NumberLessThanEquals	数值	请求值小于或等于条件值
NumberGreaterThan	数值	请求值大于条件值
NumberGreaterThanEquals	数值	请求值大于或等于条件值
NumberEqualsAnyOf	数值	可配置多个条件值，请求值与任意一个条件值相同
NumberNotEqualsAnyOf	数值	可配置多个条件值，请求值与所有条件值都不同
DateLessThan	时间	请求值早于条件值
DateLessThanEquals	时间	请求值早于或等于条件值
DateGreaterThan	时间	请求值晚于条件值

运算符	类型	说明
DateGreaterThanEquals	时间	请求值晚于或等于条件值
Bool	布尔值	请求值等于条件值
IpAddress	IP 地址	请求值在条件值所设置的 IP 地址范围内
NotIpAddress	IP 地址	请求值不在条件值所设置的 IP 地址范围内
IsNullOrEmpty	空值	请求值为 null 或者空字符串
IsNull	空值	请求值为 null
IsNotNull	空值	请求值不为 null

4.3.3.1 策略鉴权

用户在发起访问请求时，系统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4-2 系统鉴权逻辑图



1. 用户发起访问请求。

2. 系统在用户被授予的策略中寻找请求对应的 action，优先寻找 Deny 指令。如果找到一个适用的 Deny 指令，系统将返回 Deny 决定。
3. 如果没有找到 Deny 指令，系统将寻找适用于请求的任何 Allow 指令。如果找到一个 Allow 指令，系统将返回 Allow 决定。
4. 如果找不到 Allow 指令，最终决定为 Deny，鉴权结束。

4.3.4 查看授权记录

如果您需要查看当前帐号下的所有授权关系，可以进入“权限管理 > 授权管理”页面。IAM 权限管理为您呈现帐号中的所有授权关系，支持使用**“策略名”、“用户名/用户组名/委托名”、“项目区域”、“企业项目（已开启企业项目）”“主体类型”**为过滤条件查看指定授权关系。

- 如果您已开通并使用企业项目，可以选择 IAM 项目视图、企业项目视图，分别查看 IAM 项目、企业项目的授权关系。
- 如果您暂未开通企业项目，将自动显示 IAM 项目视图。

IAM 项目视图

在 IAM 项目视图下，您可以选择如下过滤条件查看对应授权记录。

- **策略名**：权限的名称。单击权限名称可以查看权限详情。

  如需查看指定权限的授权记录，选择过滤条件为“策略名”，输入指定权限名称，查看该权限的授权记录。
- **用户名/用户组名/委托名**：IAM 用户、用户组、委托的名称。

  如需查看指定 IAM 用户/用户组/委托的 IAM 项目授权记录，选择过滤条件为“用户名”、“用户组名”或“委托名”，输入指定对应名称，查看其授权记录。

  说明

  基于 IAM 项目授权，最小授权单位为用户组。查看 IAM 项目视图下指定 IAM 用户授权记录时，将显示该 IAM 用户所属用户组的授权记录。
- **项目区域**：IAM 项目或区域名称，即权限的作用范围。查看 IAM 项目授权情况，请选择：
  - 全局服务：查看所有全局服务授权记录。
  - 所有项目：查看基于所有项目授权的授权记录。基于“所有项目”授权，权限对所有项目都生效，包括全局服务和所有项目（包括未来创建的项目）。
  - 指定项目：查看基于默认区域、子项目授权的授权记录。
- **主体类型**：授权对象类型，可以选择用户、用户组、委托 3 种。IAM 项目视图下，可以选择主体类型为“用户组”、“委托”，如果选择“用户”，筛选结果为空。
- **企业项目**：企业项目的名称。如果您在 IAM 用户视图下，选择“企业项目”为过滤条件，并输入企业项目名称，将自动切换至企业项目视图。

企业项目视图

在企业项目视图下，您可以选择如下过滤条件查看对应授权记录。

- **策略名**：权限的名称。单击权限名称可以查看权限详情。

  如需查看指定权限的授权记录，选择过滤条件为“策略名”，输入指定权限名称，查看该权限的授权记录。

- **用户名/用户组名/委托名**：IAM 用户、用户组、委托的名称。

  如需查看指定 IAM 用户/用户组的企业项目授权记录，选择过滤条件为“用户名”、“用户组名”，输入指定对应名称，查看其授权记录。

  说明

  - 企业项目不支持委托功能，请选择过滤条件为“用户名”、“用户组名”。
  - 基于企业项目授权，最小授权单位为用户，查看企业项目视图下指定 IAM 用户授权记录时，显示该 IAM 用户及其所属用户组的授权记录。

- **企业项目**：企业项目的名称，即权限的作用范围。查看指定企业项目的授权记录，选择区域过滤条件为“企业项目”，输入企业项目名称，查看基于该企业项目的所有授权记录。
- **主体类型**：授权对象类型，可以选择用户、用户组、委托 3 种。企业项目视图下，可以选择主体类型为“用户”、“用户组”；如果选择“委托”，筛选结果为空。
- **项目区域**：IAM 项目或区域。如果您在企业项目视图下，选择“项目区域”为过滤条件，并选择指定项目，将自动切换至 IAM 项目视图。

4.3.5 自定义策略

4.3.5.1 创建自定义策略

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 登录 IAM 控制台。

步骤 2 在统一身份认证服务，左侧导航窗格中，选择“权限管理>权限”页签，单击右上方的“创建自定义策略”。

步骤 3 输入“策略名称”。

步骤 4 “策略配置方式”选择“可视化视图”。

步骤 5 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。
- 暂不支持一个自定义策略同时包含全局级云服务和项目级云服务。如果需要同时设置全局级服务和项目级服务的自定义策略，请创建两条自定义策略，便于授权时设置最小授权范围。

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“特定资源”可以单击“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）

表4-6 资源类型

类型	说明
特定资源	授予 IAM 用户特定资源的相应权限。如授予 IAM 用户以 TestBucket 命名开头的桶相应权限，需将 bucket 设置为通过资源路径指定，添加资源路径：OBS:*:*:bucket:TestBucket*。 说明 • 指定桶资源： 【格式】OBS:*:*:bucket:*桶名称* 对于桶资源，IAM 自动生成资源路径前缀**“obs:*:*:bucket:”**。通过**桶名称**指定具体的资源路径，支持通配符*。例如：obs:*:*:bucket:*表示任意 OBS 桶。 • 指定对象资源： 【格式】OBS:*:*:object:*桶名称/对象名称* 对于对象资源，IAM 自动生成资源路径前缀**“obs:*:*:object:”**。通过**桶名称/对象名称**指定具体的资源路径，支持通配符*。例如：obs:*:*:object:my-bucket/my-object/*表示 my-bucket 桶下 my-object 目录下的任意对象。
所有资源	授予 IAM 用户所有资源的相应权限。

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4-7 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，详情请参见对应云服务的用户指南。
运算符	与条件键、条件值一起使用，构成完整的条件判断语句。

参数名称	参数说明
值	与条件键、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，构成完整的条件判断语句。

表4-8 全局级请求条件

全局条件键	条件类型	说明
g:CurrentTime	时间	接收到鉴权请求的时间。以 ISO 8601 格式表示，例如：2012-11-11T23:59:59Z。
g:DomainName	字符串	帐号名称。
g:MFAPresent	布尔值	是否使用 MFA 多因素认证方式获取 Token。
g:MFAAge	数值	通过 MFA 多因素认证方式获取的 Token 的生效时长。该条件需要和 g:MFAPresent 一起使用。
g:ProjectName	字符串	项目名称。
g:ServiceName	字符串	服务名称。
g:UserId	字符串	IAM 用户 ID。
g:UserName	字符串	IAM 用户名。

步骤 6 （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 7 （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 8 输入“策略描述”（可选）。

步骤 9 单击“确定”，自定义策略创建完成。

步骤 10 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，详情请参考“用户组及授权”

----结束

JSON 视图配置自定义策略

步骤 1 登录 IAM 控制台。

步骤 2 在统一身份认证服务，左侧导航窗格中，选择“权限管理>权限”页签，单击右上方的“创建自定义策略”。

步骤 3 输入“策略名称”。

步骤 4 “策略配置方式”选择“JSON 视图”。

步骤 5 （可选）在“策略内容”区域，单击“从已有策略复制”，例如选择“EVS FullAccess”作为模板。

说明

此处可以同时选择多个服务的策略，这些策略的作用范围必须一致，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，便于授权时设置最小授权范围。

步骤 6 单击“确定”。

步骤 7 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（如所示）中“授权项”中的内容，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 8 （可选）输入“策略描述”。

步骤 9 单击“确定”后，系统会自动校验语法，如跳转到策略列表，则自定义策略创建成功；如提示“策略内容错误”，请按照语法规范进行修改。

步骤 10 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，详情请参考“创建用户组并授权”

----结束

4.3.5.2 修改、删除自定义策略

本节为您介绍如何修改和删除已创建的自定义策略。

修改自定义策略

修改自定义策略名称、描述和内容。

1. 管理员在 IAM 控制台左侧导航窗格中，选择“权限管理>权限”页签。
2. 在指定策略的操作列中单击“编辑”，或者单击需要修改的策略名称，进入策略详情页。
3. 可根据需要修改“策略名称”和“策略描述”。
4. 按可视化视图配置自定义策略方式修改策略。
5. 单击“确定”完成修改。

删除自定义策略

说明

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。

1. 管理员在 IAM 控制台左侧导航窗格中，选择“权限管理>权限”。
2. 在指定策略的操作列中单击“删除”。
3. 单击“确定”完成删除。

4.3.5.3 自定义策略使用样例

配合较高权限系统策略使用

如果您给 IAM 用户授予较高权限的系统策略，例如“FullAccess” ，但不希望 IAM 用户拥有某个服务的权限，例如云审计服务。您可以创建一个自定义策略，并将自定义策略的 Effect 设置为 Deny，然后将较高权限的系统策略和自定义策略同时授予用户，根据 Deny 优先原则，则授权的 IAM 用户除了云审计服务，可以对其他所有服务执行所有操作。

以下策略样例表示：拒绝 IAM 用户使用云审计服务。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                    "cts:*:*"
            ]
        }
    ]
}
```

说明

- Action 为授权项，格式为：服务名:资源类型:操作。

  "cts:*:*"：表示对云审计的所有操作。其中 cts 为服务名；“*”为通配符，表示对所有的资源类型可以执行所有操作。
- Effect 为作用，Deny 表示拒绝，Allow 表示允许。

配合单个服务系统策略使用

- 如果您给 IAM 用户授予单个服务系统策略，例如“BMS FullAccess”，但不希望用户拥有 BMS FullAccess 中的创建物理机权限（bms:servers:create），可以创建一条相同 Action 的自定义策略，并将自定义策略的 Effect 设置为 Deny，然后将系统策略 BMS FullAccess 和自定义策略同时授予用户，根据 Deny 优先原则，则用户可以对 BMS 执行除了创建物理机外的所有操作。

  以下策略样例表示：拒绝 IAM 用户创建物理机。

```
{
    "Version": "1.1",
    "Statement": [
        {
```

```
            "Effect": "Deny",
            "Action": [
                  "bms:servers:create"
            ]
        }
    ]
}
```

- 如果您给 IAM 用户授予“OBS ReadOnlyAccess”权限，但不希望部分用户查看指定 OBS 资源（例如，不希望用户名以“TestUser”开头的用户查看以“TestBucket”命名开头的桶），可以再创建一条自定义策略来指定特定的资源，并将自定义策略的 Effect 设置为 Deny，然后将 OBS ReadOnlyAccess 和自定义策略同时授予用户。根据 Deny 优先原则，则用户可以对以“TestBucket”命名开头之外的桶进行查看操作。

  以下策略样例表示：拒绝以 TestUser 命名开头的用户查看以 TestBucket 命名开头的桶。

```
{
       "Version": "1.1",
       "Statement": [
              {
                     "Effect": "Deny",
                     "Action": [
                            "obs:bucket:ListAllMybuckets",
                            "obs:bucket:HeadBucket",
                            "obs:bucket:ListBucket",
                            "obs:bucket:GetBucketLocation"
                     ],
                     "Resource": [
                        "obs:*:*:bucket:TestBucket*"
                     ],
                     "Condition": {
                        "StringStartWith": {
                           "g:UserName": [
                              "TestUser"
                  ]
              }
           }
              }
       ]
}
```

说明

当前仅部分服务支持资源级授权，例如 OBS 对象存储服务；对于不支持资源级别授权的服务，若自定义策略中含有资源类型，则无法创建成功。

完全使用自定义策略

您也可以不使用系统策略，只创建自定义策略，实现 IAM 用户的指定服务授权。

- 以下策略样例表示：仅允许 IAM 用户使用 ECS、EVS、VPC、ELB、AOM

```
{
       "Version": "1.1",
       "Statement": [
              {
```

```
                "Effect": "Allow"
                "Action": [
                        "ecs:*:*",
                        "evs:*:*",
                        "vpc:*:*",
                        "elb:*:*",
                        "aom:*:*"
                ]
        }
    ]
}
```

- 以下策略样例表示：允许特定 IAM 用户（以 TestUser 命名开头）删除特定 OBS 对象（my-bucket 桶 my-object 目录下的所有对象）。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:DeleteObject"
            ],
            "Resource": [
                "obs:*:*:object:my-bucket/my-object/*"
            ],
            "Condition": {
                "StringStartWith": {
                    "g:UserName": [
                        "TestUser"
                ]
            }
        }
    ]
}
```

- 以下策略样例表示：允许 IAM 用户使用除了 ECS、EVS、VPC、ELB、AOM 外的其他所有服务。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                    "*:*:*"
            ]
        },
        {
            "Action": [
                    "ecs:*:*",
                    "evs:*:*",
                    "vpc:*:*",
                    "elb:*:*",
                    "aom:*:*",
            ],
            "Effect": "Deny"
        }
```

```
        ]
}
```

4.4 项目

每个区域默认对应一个项目，这个项目由系统预置，用来隔离物理区域间的资源（计算资源、存储资源和网络资源），以区域默认单位为项目进行授权，IAM 用户可以访问您帐号中该区域的所有资源。

基于项目给用户组授权

以项目为单位进行授权，使得 IAM 用户仅能访问特定项目中的资源。

步骤 1 在用户组列表中，单击用户组右侧的“授权”，进入授权页面。

步骤 2 在授权页面中，勾选需要授予用户组的区域级项目权限，并单击“下一步”。

步骤 3 选择作用范围。此处选择区域项目，则还需要选择待授权的项目。

步骤 4 单击“确定”，完成授权。

说明

更多有关用户组授权的内容，请参见“创建用户组并授权”。

----结束

切换项目或区域

登录后需要先切换区域或项目，才能访问并使用授权的云服务，否则系统将提示没有权限。全局区域服务无需切换。

步骤 1 登录控制台。

步骤 2 进入具体的云服务页面，若云服务为项目级服务，则单击页面顶部区域下拉框，切换区域。

----结束

4.5 委托

4.5.1 委托其他账号管理资源

4.5.1.1 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。

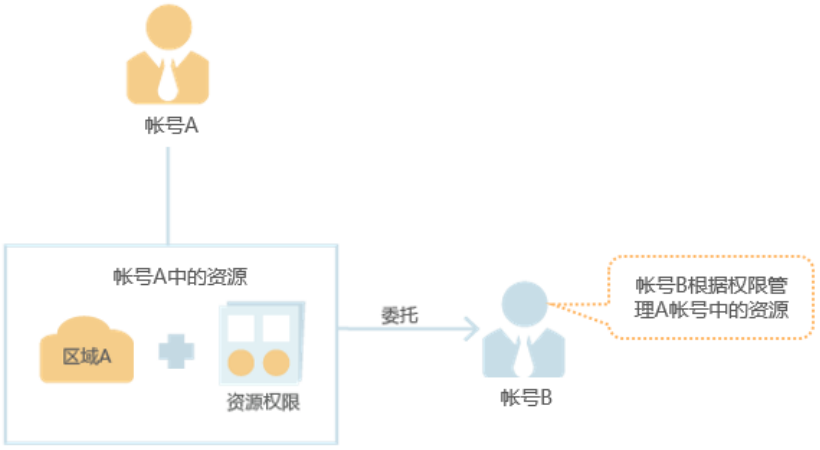
须知

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。A 帐号为委托方，B 帐号为被委托方。

步骤 1 账号 A 创建委托。

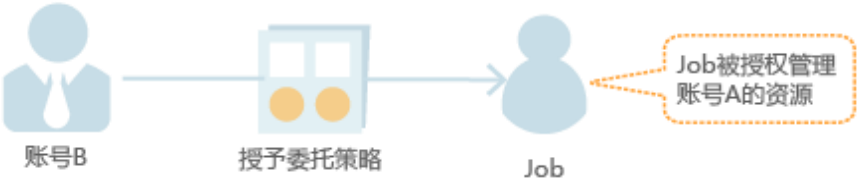
图4-3 委托方创建委托



步骤 2 （可选）账号 B 分配委托权限。

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

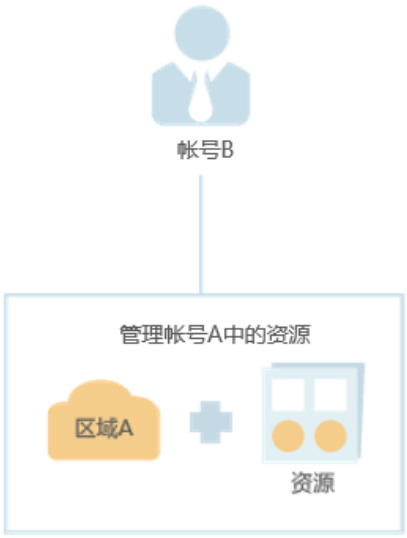
图4-4 为被委托方分配委托权限



步骤 3 账号 B 或 IAM 用户根据权限管理委托资源。

1. 被委托方登录自己的账号，并切换角色到账号 A。
2. 切换到被授权的区域，并根据权限管理账号 A 的资源。

图4-5 被委托方切换角色



----结束

4.5.1.2 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”，“委托类型”选择“普通帐号”，在“委托的帐号”中输入需要建立委托关系的其他帐号的帐号名。

说明

- 普通帐号：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帐号中的资源。委托的帐号只能是帐号，不能是 IAM 用户名。
- 云服务：授权指定云服务使用其他云服务。详情请参见“委托其他云服务管理资源”

步骤 6 设置“持续时间”及“描述”信息。

步骤 7 单击“下一步”，进入给委托授权页面。

步骤 8 勾选需要授予委托的权限，单击“下一步”，选择权限的作用范围。

说明

- 给委托授权即给其他帐号授权，给用户组授权即给帐号中的 IAM 用户授权，两者操作方法相同，仅可选择的权限个数不同，授权操作请参见“给用户组授权”。
- 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 9 单击“确定”，委托创建完成。

说明

委托方操作完成，将自己的帐号名称、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

4.5.1.3 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。

如果您有多个委托关系，可以授予 IAM 用户较大的委托权限，即管理所有的委托，也可以授予 IAM 用户精细的权限，仅管理指定的委托，即 IAM 用户进行角色切换时，仅能切换到被授权的委托中，不能切换其他委托，您可以创建细粒度的委托权限，授权 IAM 用户管理指定的委托。

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、所创建的委托名称以及委托 ID。

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“授权”。
8. 创建自定义策略。

说明

如果需要授予 IAM 用户精细的委托权限，仅管理指定的委托，请执行以下步骤创建细粒度的委托权限。如果不需要进行精细的委托授权，授予 IAM 用户管理所有的委托权限，请跳过该步骤，直接执行下一步骤。

a. 在选择策略页面，单击权限列表右上角“新建策略”。
b. 输入“策略名称”。
c. “策略配置方式”选择“JSON 视图”。
d. 在“策略内容”区域，填入以下内容：

```
{
       "Version": "1.1",
       "Statement": [
              {
                     "Action": [
                            "iam:agencies:assume"
                     ],
                     "Resource": {
```

```
                        "uri": [
                            "/iam/agencies/b36b1258b5dc41a4axxx..."
                        ]
                    },
                    "Effect": "Allow"
                }
            ]
}
```

说明

- "b36b1258b5dc41a4axxx..."需要替换为待授权委托的 ID，需要提前向委托方获取，其他内容不需修改，直接拷贝即可。
- 本文简要讲述快速完成委托细粒度授权的必要操作，更多权限内容，详情请参考“权限管理”章节。

e. 单击“下一步”，继续完成授权。

9. 选择上一步创建的自定义策略或者“Agent Operator”权限，单击“下一步”。
   - 自定义策略：用户仅能管理指定 ID 的委托，不能管理其他委托。
   - “Agent Operator”权限：用户可以管理所有委托。
10. 选择授权范围方案。
11. 单击“确定”，用户组授权完成。

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。

说明

分配委托权限操作完成，新创建的 IAM 用户可以通过切换角色至委托方帐号中，帮助您管理委托资源。

----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。

4.5.1.4 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 使用被委托方账号或已分配委托权限的 IAM 用户登录天翼云，单击页面顶部“控制台”。

说明

只有被委托的账号及该账号下被分配委托权限的 IAM 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。

4.5.2 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“下一步”，进入给委托授权页面。

步骤 9 勾选需要授予委托的权限，单击“下一步”，选择权限的作用范围，给委托授权。

步骤 10 单击“确定”，委托创建完成。

----结束

4.5.3 删除或修改委托

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。

说明

- 云服务委托支持修改云服务、持续时间、描述、权限，委托名称、类型不支持修改。
- 修改云服务委托权限后可能会影响该云服务部分功能的使用，请谨慎操作。

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。

批量删除委托

如果需要删除多个委托，可在委托列表中勾选需要删除的委托，然后单击列表上方的“删除”。

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。

4.6 用户凭证

当您通过 API 访问部分云服务（如对象存储 OBS）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，可以在“我的凭证”中查看这些安全凭证。

表4-9 用户凭证信息

基本信息	说明
IAM 用户名	IAM 用户的登录名，归属于某一个天翼云账号，用户登录系统时需要提供。
IAM 用户 ID	IAM 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），在天翼云注册时自动创建。
账号 ID	账号在系统中的标识 ID，由系统自动生成。
项目	项目一般是一个资源池，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，通过不同的项目实现资源的隔离管理。
项目列表信息	账号可访问的项目列表，在访问云服务 API 时需要指定项目 ID（projectId）等参数。

基本信息	说明
访问密钥	用户的长期身份凭证 ，最多可创建两对，在访问部分云服务 API（如对象存储 OBS）时，调用者需要使用 AK/SK 进行加密签名。

4.6.1 查看我的凭证和项目信息

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 IAM 用户 ID、账号 ID 等。

项目 ID 是 IAM 用户的云服务所在区域（资源池）ID，您在调用云服务 API 接口进行云资源管理（如创建 VPC）时，需要提供项目名称和项目 ID。

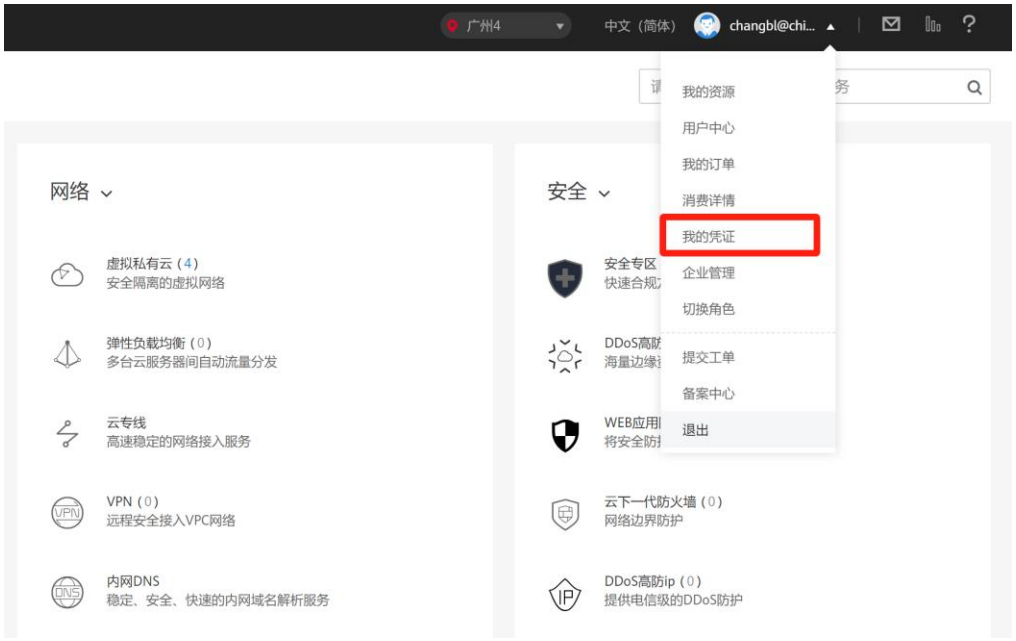
我的凭证信息和项目信息可以在我的凭证中查看。

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 IAM 用户 ID、账号 ID、项目 ID 等信息。

----结束

4.6.2 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部分云服务 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，单击右侧“访问密钥”。

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。

4.7 查看 IAM 操作记录

4.7.1 开通云审计服务

云审计服务（Cloud Trace Service，以下简称 CTS），是安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

为了方便查看 IAM 的关键操作事件，例如创建用户、删除用户等，管理员需开启云审计服务。

操作步骤

步骤 1 管理员登录控制台。

步骤 2 选择“服务列表 > 管理与监管 > 云审计服务 2.0”，如之前账号未开通过云审计服务，会进入云审计服务授权页面，单击“同意授权并开通”，进入云审计服务页面。

步骤 3 在贵州区域创建 1 个管理追踪器，用于记录 IAM 服务的管理操作事件。

在 IAM 进行操作，例如创建用户、用户组等，CTS 将会记录这些操作。CTS 支持记录的 IAM 相关的操作事件，如下表所示。

表4-10 CTS 支持的 IAM 操作列表

操作名称	资源类型	事件名称
用户登录	user	login
用户登出	user	logout
创建用户	user	createUser
修改用户信息	user	updateUser
删除用户	user	deleteUser
创建 AK/SK	user	createCredential、addCredential
删除 AK/SK	user	deleteCredential
停用、启用 AK/SK	user	changeCredentialStatus
修改 AK/SK	user	updateCredential
创建用户组	userGroup	createUserGroup
更新用户组	userGroup	updateGroup、updateUserGroup
删除用户组	userGroup	deleteUserGroup
添加用户到用户组	userGroup	addUserToGroup、updateUser/updateUserGroup
从用户组删除用户	userGroup	removeUserFromGroup、updateUser/updateUserGroup
创建委托	agency	createAgency
修改委托	agency	updateAgency
删除委托	agency	deleteAgency

操作名称	资源类型	事件名称
切换角色	agency	switchRole
	Token	createToken
创建自定义策略	role	createRole
修改自定义策略	role	updateRole
删除自定义策略	role	deleteRole

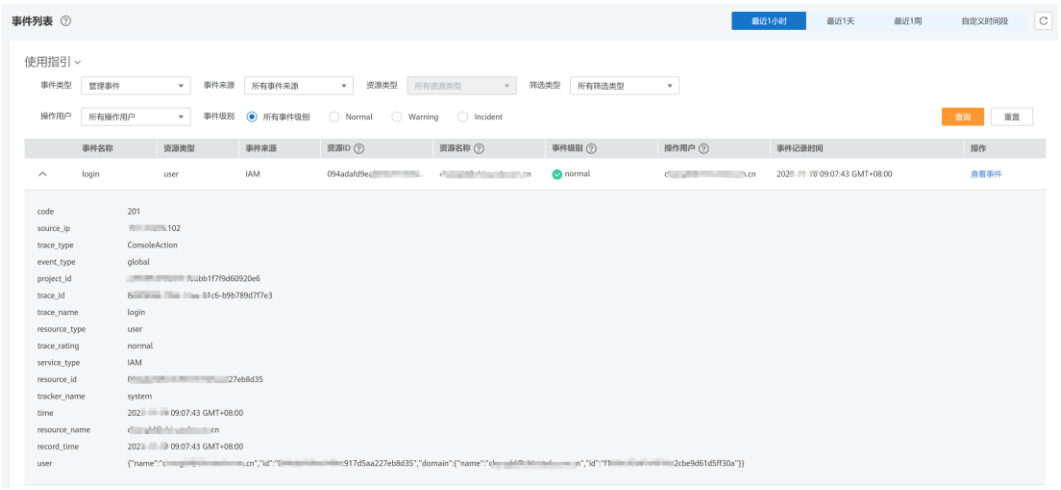
4.7.2 查看 IAM 的云审计日志

开通云审计服务后，云审计服务开始记录操作事件，包括 IAM 以及其他服务的操作事件，云审计服务保存最近 7 天的操作记录。

操作步骤

步骤 1 管理员在 IAM 控制台进行操作，例如登录控制台或创建 IAM 用户。

步骤 2 进入云审计服务控制台，查看 IAM 的操作记录。



步骤 3 单击 ，可以查看事件的基本信息。

步骤 4 单击“查看事件”，可以查看事件的结构。

----结束

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和服务名称仍无法找到服务，则该需要设置权限的服务暂不支持 IAM。

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。

1. 可能原因：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：用户指南 > 用户组及授权。

2. 可能原因：管理员授予的权限已拒绝相关操作的授权项。

   解决方法：管理员查看已授予 IAM 用户的系统权限详情，确认已授予的权限是否有拒绝操作的语句，方法请参考：用户指南 > 权限管理> 策略。如系统权限无法满足您的场景需要，管理员可以创建自定义策略，允许该操作对应的授权项，方法请参考：用户指南 > 权限管理 > 自定义策略。

3. 可能原因：管理员给用户组授予权限后，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：用户指南 > 用户组及授权 > 用户组添加/移除用户。

4. 可能原因：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。如果管理员授予用户默认区域项目的权限，用户只能访问该默认项目中的资源，不拥有该默认项目下 IAM 子项目的权限，建议您授予 IAM 用户最小区域权限，方法请参见：用户指南 > 用户组及授权 > 创建用户组并授权。

5. 可能原因：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，方法请参见：用户指南 > 项目。

6. 可能原因：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。

7. 可能原因：浏览器缓存导致权限信息未更新。

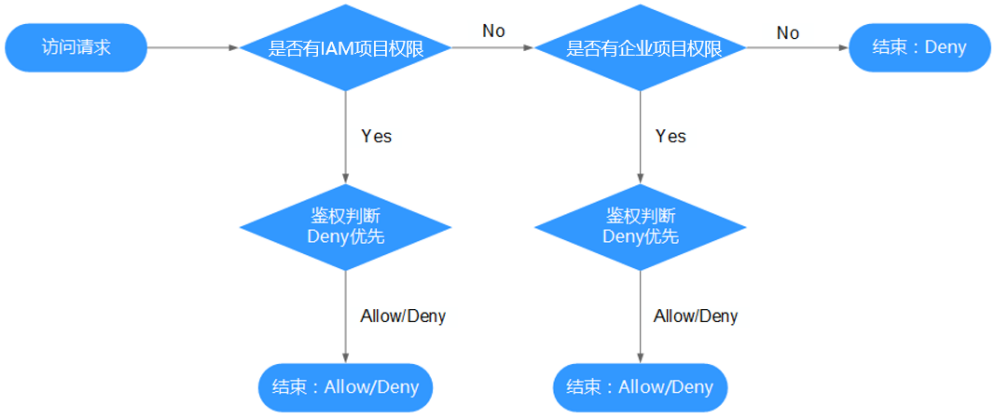
   解决方法：请清理浏览器缓存后重试。

8. 可能原因：管理员同时在 IAM 和企业管理给用户授权，基于企业项目管理权限可能不生效。IAM 鉴权优先于企业管理。

   解决方法：请管理员根据情况在 IAM 控制台修改用户权限。

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。主要包括企业项目资源管理和权限管理。

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 和企业管理的区别

- 开通方式
  - IAM 是云平台的身份管理服务，注册系统后，无需付费即可使用。
  - 企业管理是云平台的资源管理服务，注册系统后，需提交客服工单申请开通，开通后无需付费免费使用。
- 资源隔离
  - IAM 通过在每一个区域中创建项目，隔离不同区域中的资源。以项目为单位进行授权，用户可以访问指定项目中的所有资源。
  - 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。企业项目还可以实现对特定云资源的授权，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。

IAM 与企业管理的关系

- IAM 和企业管理的创建用户以及用户组功能，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 和企业管理中同时给用户组授权，用户同时拥有基于 IAM 项目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 中设置的生效，例如：用户请求创建弹性云主机，鉴权结果为 IAM 中定义的 Deny，不能创建弹性云主机。

```
IAM 项目策略中包含以下 action：
{
  "Action": [
    "ecs:cloudServers:create"
  ],
  "Effect": "Deny"
}

企业项目策略中包含以下 action：
```

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

- 如果策略中包含不同的 Action，则 IAM 和企业管理中设置的都生效。以下示例表示用户可以创建弹性云主机以及删除弹性云主机。

```
IAM 项目策略中包含以下 action:
{
  "Action": [
    "ecs:cloudServers:create"
  ],
  "Effect": "Allow"
}
企业项目策略中包含以下 action:
{
  "Action": [
    "ecs:cloudServers:delete"
  ],
  "Effect": "Allow"
}
```

5.2.2 IAM 项目与企业项目的区别

IAM 项目

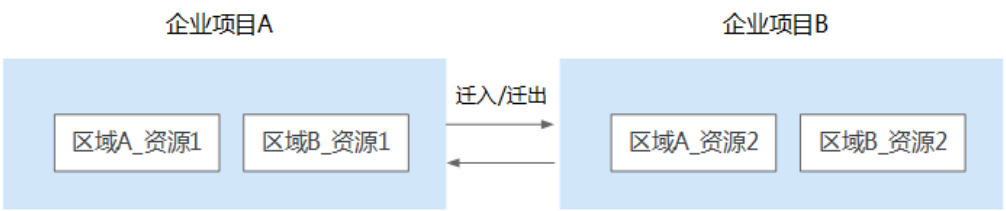
IAM 项目是以每一个天翼云资源节点为粒度进行资源及服务隔离，是物理隔离。

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。如果您开通了企业管理，将不能创建 IAM 项目。



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。

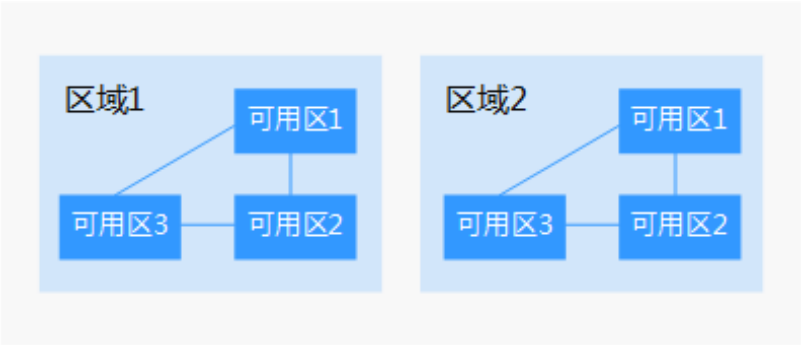
5.2.3 区域和可用区

什么是区域、可用区？

区域和可用区用来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）指物理的数据中心。每个区域完全独立，这样可以实现最大程度的容错能力和稳定性。资源创建成功后不能更换区域。
- 可用区（AZ，Availability Zone）是同一区域内，电力和网络互相隔离的物理区域，一个可用区不受其他可用区故障的影响。一个区域内可以有多个可用区，不同可用区之间物理隔离，但内网互通，既保障了可用区的独立性，又提供了低价、低时延的网络连接。

图5-1 区域和可用区



如何选择区域？

建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

如何选择可用区？

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

5.3 委托管理类

5.3.1 创建委托时提示权限不足怎么办

问题描述

IAM 用户尝试进入 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：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“FullAccess”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

- 请管理员创建委托。
- 请管理员授予使用 IAM 服务的权限。

5.4 秘钥凭证类

5.4.1 如何获取访问密钥 AK/SK

- 如果您有登录密码，可以登录控制台，在“控制台”页面，鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”，单击“访问密钥”页签，您可以在访问密钥列表中查看访问密钥 ID（AK），在下载的.csv 文件中查看秘密访问密钥（SK）。
- 如果您没有登录密码，不能登录控制台，在访问密钥异常丢失或者需要重置时，可以联系您的账号管理员在 IAM 中生成您的访问密钥，并发送给您。

5.4.2 丢失访问密钥 AK/SK 怎么办

如果您的访问密钥 AK/SK 已丢失，建议您先创建新的访问密钥 AK/SK，并使用新的访问密钥 AK/SK 替换正在使用的应用程序等的访问秘钥 AK/SK 之后，确认无其他业务影响，再将丢失的访问密钥 AK/SK 停用或删除。

说明

- 每个用户最多可创建 **2** 个访问密钥，不支持增加配额。
- 如果您无法管理您的访问密钥，请联系您企业的账号管理员。

5.4.3 什么是临时安全凭证（临时 AK/SK 和 SecurityToken）

什么是临时安全凭证

临时安全凭证是**具备临时访问权限**的身份凭证，包括临时 AK/SK 和 SecurityToken，临时安全凭证与永久安全凭证的工作方式几乎相同，仅存在小量差异。

临时安全凭证与永久安全凭证的差异

- 临时安全凭证存在有效期，可以在 15 分钟至 24 小时之间进行设置；永久安全凭证的有效期为永久，并且不能进行设置。
- 临时安全凭证没有数量限制；每个 IAM 用户最多可创建 2 个永久安全凭证。
- 临时安全凭证通过接口获取临时 AK/SK 获取；永久安全凭证通过我的凭证界面控制台获取。
- 临时安全凭证为动态生成，即时使用，不能嵌入应用程序中，或者进行存储，到期后无法重复使用，只能重新获取。

临时安全凭证的优势

在给外部联邦用户授权时，临时安全凭证的优势尤为明显，您不必给外部联邦用户授予需要定时轮换，主动撤销的永久安全凭证，而是给这些外部联邦用户授予即时使用，定时过期的临时安全凭证，提高帐号的安全性，遵循权限最小化的安全实践原则。

临时安全凭证的使用方法

临时安全凭证包括临时 AK/SK 和 SecurityToken，临时 AK/SK 和 SecurityToken 必须同时使用，临时安全凭证与永久安全凭证的使用方法几乎相同，使用临时安全凭证进行鉴权时，请求头中需要添加“x-security-token”字段。