天翼云

企业项目管理

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 企业项目管理.....4
1.2 应用场景.....4
1.2.1 场景一：按业务项目划分.....4
1.2.2 场景二：按组织架构+业务项目划分.....6
1.3 产品功能.....7
1.4 基本概念.....7
1.5 约束与限制.....11
2 购买指南.....12
2.1 资源节点.....12
2.2 计费说明.....12
2.3 申请开通.....12
3 快速入门.....14
3.1 示例场景.....14
3.2 步骤 1：创建用户组.....15
3.3 步骤 2：创建 IAM 用户并添加用户组.....16
3.4 步骤 3：创建企业项目.....17
3.5 步骤 4：为企业项目添加用户组并授权.....18
3.6 步骤 5：为企业项目迁入资源.....20
3.7 验证结果.....21
4 用户指南.....22
4.1 管理企业项目.....22
4.1.1 创建企业用户.....22
4.1.2 修改/启用/停用企业项目.....23
4.1.3 为新购云资源选择企业项目.....24
4.2 管理企业项目资源.....25
4.2.1 查看全部资源.....25
4.2.2 查看企业项目资源.....26
4.2.3 为企业项目迁入资源.....26

4.2.4 迁出企业项目资源 28
4.3 管理企业项目人员授权 29
4.3.1 查看企业项目用户组 29
4.3.2 为企业项目添加用户组并授权 30
4.3.3 移除企业项目用户组 32
5 常见问题 34
5.1 权限管理类 34
5.1.1 同时设置了 IAM 和企业项目管理授权时的检查规则 34
5.1.2 无法找到特定服务的权限怎么办？ 35
5.1.3 资源迁入/迁出企业项目会影响资源所在的 VPC 和网段吗？ 35
5.2 项目管理类 35
5.2.1 IAM 与企业项目管理的区别 35
5.2.2 IAM 项目与企业项目的区别 36
5.2.3 如何获取企业项目 ID 37
5.3 委托管理类 37
5.3.1 创建委托时提示权限不足怎么办 37

1 产品简介

1.1 企业项目管理

企业项目管理（Enterprise Project Management Service，简称“EPS”），为客户提供与企业组织架构和业务管理模型匹配的云治理能力。以面向企业资源管理为出发点，帮助企业以公司、部门、项目等组织架构分级管理和项目业务结构来实现企业在云上的人、物、权管理，提供企业人员管理、项目管理、资源管理等能力。

企业项目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 应用场景

企业可以根据组织架构规划企业项目，将企业分布在不同区域的资源按照企业项目进行统一管理，同时可以为每个企业项目设置拥有不同权限的用户组和用户。下面介绍企业项目的典型应用场景。

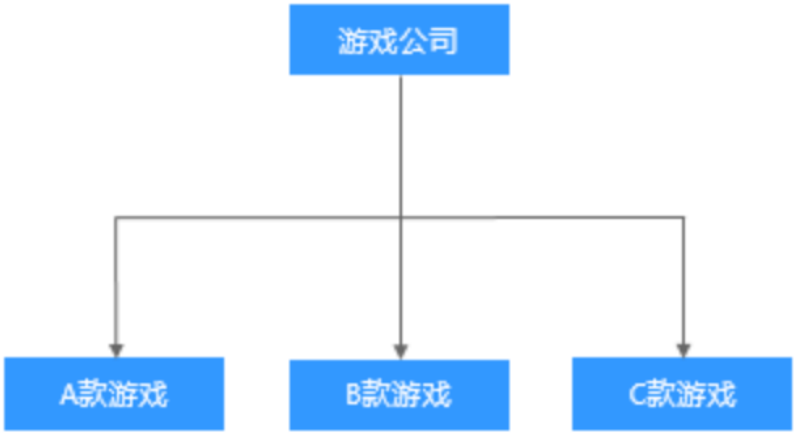
1.2.1 场景一：按业务项目划分

企业中有多个项目，多个项目之间相互独立，资源分开管理，且分属不同的人员进行管理。

客户场景

某游戏公司上线 A、B、C 三款游戏，每款游戏的开发人员、开发资源和财务独立管理。

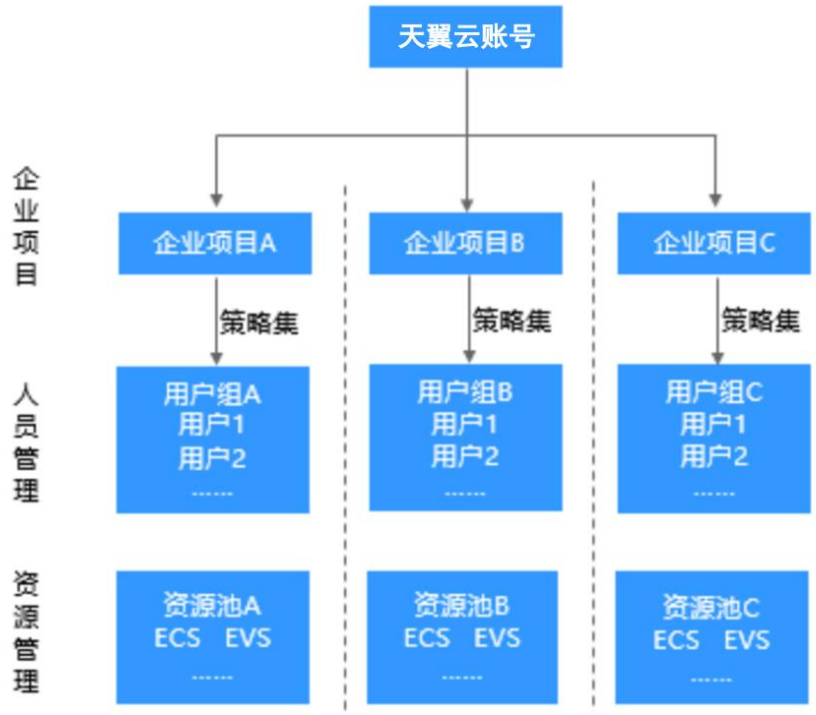
图1-1 企业架构示意图



解决方案

1. 该游戏公司先注册天翼云帐号，并开通 IAM 及企业项目管理功能；
2. 将这 3 款游戏作为单独的企业项目进行管理：企业项目 A、企业项目 B、企业项目 C；
3. 为这 3 个企业项目设置管理访问权限（用户组和用户）；
4. 按企业项目管理所拥有的资源：迁入/迁出资源；

图1-2 解决方案示意图



此场景中，企业架构示意图如图 1 所示，天翼云对应的解决方案示意图如图 2 所示。

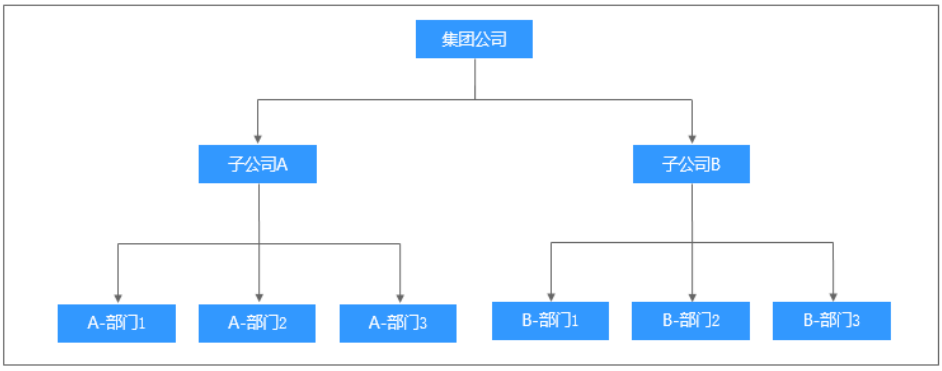
1.2.2 场景二：按组织架构+业务项目划分

企业可以根据组织架构，按组织划分企业项目，且子帐号之间资源隔离，网络互不相通。

客户场景

某集团公司下面有两个子公司（子公司 A 和子公司 B），每个子公司分别有 3 个部门，要求按部门实现人员、资源和财务的独立管理。

图1-3 企业架构示意图



解决方案

该该游戏公司先注册天翼云帐号，开通统一身份认证 IAM、企业项目管理 EPS 和企业主帐号相关服务；

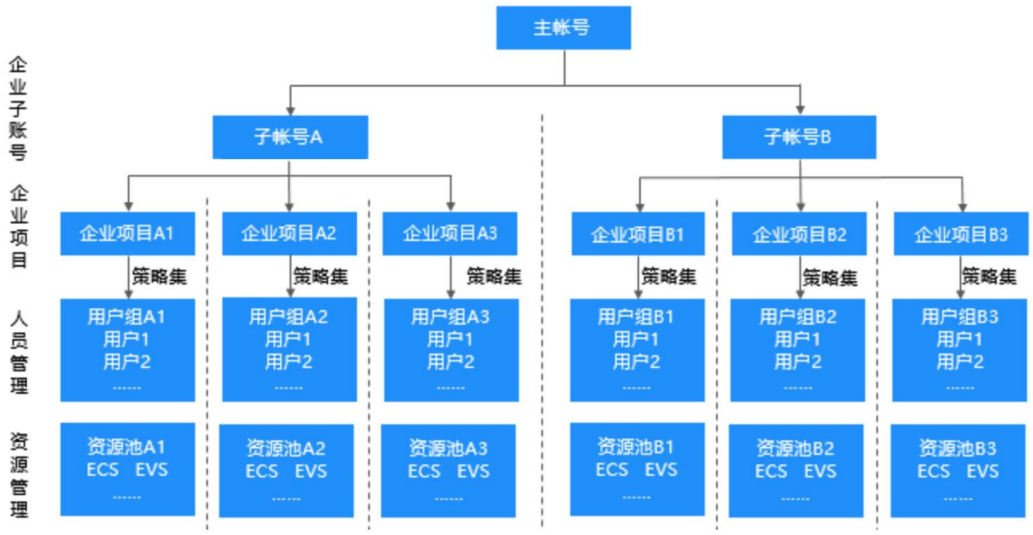
将子公司 A 和子公司 B 分别作为子帐号 A 和子帐号 B，并与企业主帐号关联；

将子公司下的部门作为单独的企业项目进行管理：企业项目 A1、企业项目 A2、企业项目 A3，企业项目 B1、企业项目 B2、企业项目 B3；

分别为每个企业项目设置资源管理和访问权限（基于用户组/用户）；

按企业项目管理所拥有的资源：迁入/迁出资源；

每个企业项目之间财务管理相互独立。



此场景中，企业架构示意如图 3 所示，天翼云对应的解决方案如图 4 所示。

1.3 产品功能

企业项目管理为您提供的主要功能包括：企业项目管理、企业项目资源管理等。

企业项目管理

- 创建企业项目
- 修改/启用/停用企业项目
- 为新购的云资源配置所属企业项目

企业项目资源管理

- 查看企业项目下的资源
- 为企业项目迁入资源
- 迁出企业项目资源

企业项目人员权限管理

- 配置企业项目关联的用户组
- 配置企业项目关联用户组的资源操作权限

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。

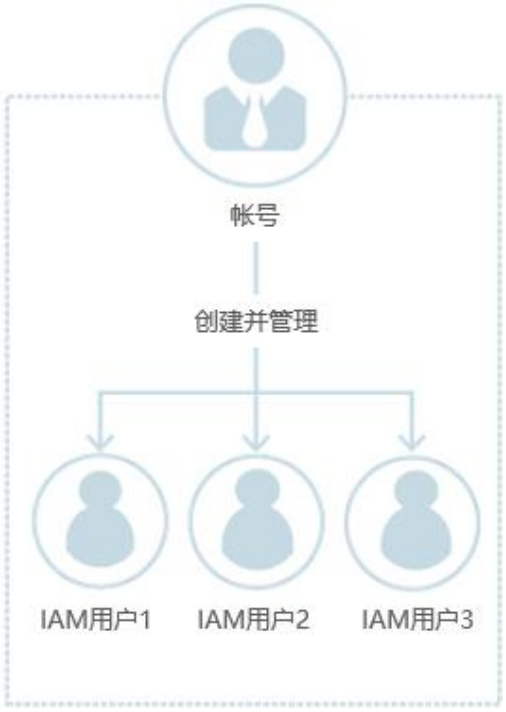
帐号不能在 IAM 中修改和删除，您可以在天翼云网门户“个人中心”修改帐号信息，如果您需要删除帐号，可以在“个人中心”进行注销。

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1-4 天翼云账号与 IAM 用户



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。

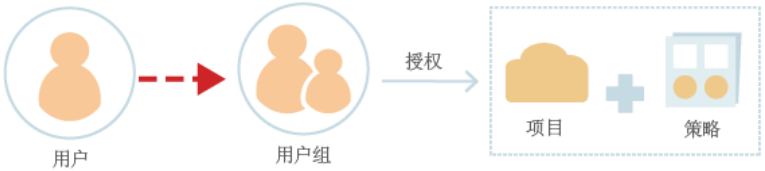
“admin”为系统缺省提供的用户组，具有所有云服务资源的操作权限。将 IAM 用户加入该用户组后，IAM 用户可以操作并使用所有云资源，包括但不仅限于创建用户组及用户、修改用户组权限、管理资源等。

图1-5 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1-6 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1-7 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1-8 权限策略示例

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

IAM 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。

1.5 约束与限制

企业管理中组织数、组织策略数、企业项目数等有一定的限制，各限制项默认的最大值如表 1 所示。

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

企业项目管理（Enterprise Project Management Service，简称“EPS”）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

企业项目管理 EPS 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企业项目管理。

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。
- 请确保您的企业账号已开通统一身份认证服务 IAM。

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“申请开通企业项目管理”，如账号的 IAM 主子账号管理尚未开通，可在一张工单中同时申请开通统一认证服务 IAM 和企业项目管理 EPS。

步骤 6 填写联系方式等信息，单击“确认提交”完成企业项目管理开通申请。

3 快速入门

3.1 示例场景

企业项目管理可支持通过不同的 IAM 用户对云资源进行细粒度管理。

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 IAM 和企业项目管理服务 EPS，如服务未开通，请首先在天翼云网门户提交申请开通工单。
- 创建企业项目的用户必须是管理员，或在 IAM 侧已被授予 EPS Full Access 权限的 IAM 用户。

业务场景

用户已购买了多种天翼云资源，为了方便云资源的管理和使用的安全性，可以通过创建不同的 IAM 用户并授予不同云服务的管理权限，从而实现 IAM 用户对云资源的分类管理。

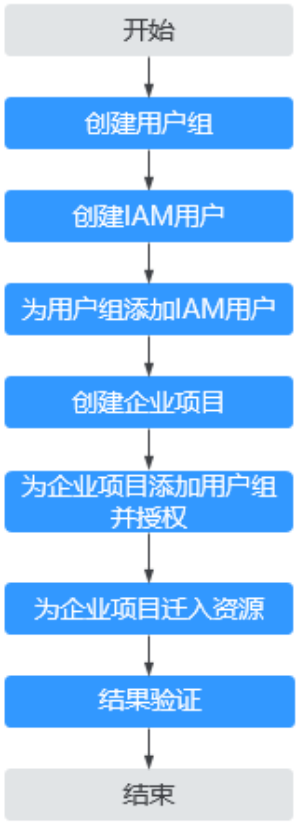
本节以一个案例让您了解如何通过企业项目管理实现 IAM 用户拥有独立、隔离的云资源管理权限。

操作规划

操作项目	描述
创建用户组	在 IAM 控制台分别创建用户组 Test_ECS_A 和 Test_ECS_B。
创建 IAM 用户并添加至用户组	在 IAM 控制台分别创建用户 Test_User_A 和 Test_User_B。 - 将用户 Test_User_A 添加至用户组 Test_ECS_A； - 将用户 Test_User_B 添加至用户组 Test_ECS_B。
创建企业项目并将用户组	在企业项目管理页面分别创建企业项目 project_A 和

操作项目	描述
添加至项目	project_B。 ❿ 将用户组 Test_ECS_A 添加至企业项目 project_A； ❿ 将用户组 Test_ECS_B 添加至企业项目 project_B。
企业项目迁入资源	在企业项目管理页面分别给企业项目 project_A 和 project_B 迁入对应的云资源。

操作流程



3.2 步骤 1：创建用户组

管理员可以参考以下操作分别创建用户组 Test_ECS_A 和 Test_ECS_B

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 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“Test_ECS_A”和“Test_ECS_B”

----结束

3.3 步骤 2：创建 IAM 用户并添加用户组

管理员可以参考以下操作分别创建 IAM 用户 Test_User_A 和 Test_User_B，并添加至相应用户组。

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 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”。

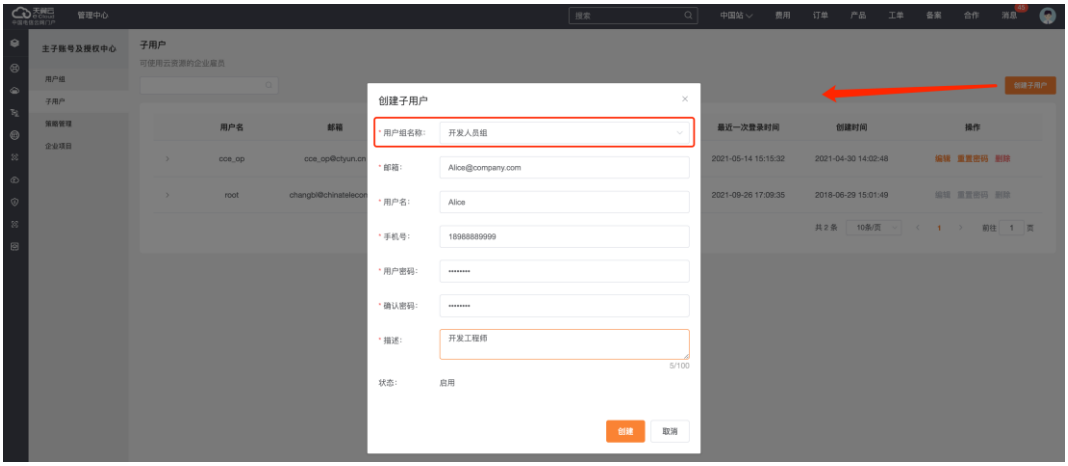
步骤 4 在主子账号及授权管理页，单击左侧导航菜单中的“子用户”。

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 Test_ECS_A/ Test_ECS_B，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 Test_User_A、Test_User_A，并加入对应的用户组。

----结束

3.4 步骤 3：创建企业项目

管理员可以参考以下操作分别创建企业项目 project_A 和 project_B。

操作步骤

步骤 1 企业管理员使用天翼云帐号登录天翼云网门户。

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，单击您的用户名后弹出下拉菜单，单击“企业管理”。

步骤 4 单击企业管理控制台左侧导航菜单“项目管理”，然后再单击右上角“＋创建企业项目”。

步骤 5 在创建企业项目对话框中，输入项目名称和描述，单击“确定”完成项目创建。

参考步骤 4 至步骤 5 的方法，依次创建企业项目 project_A、project_B。

----结束

3.5 步骤 4：为企业项目添加用户组并授权

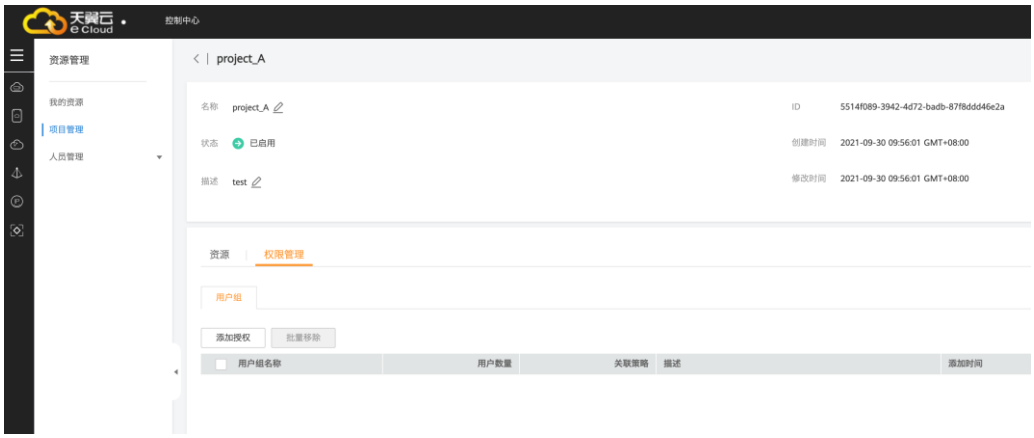
企业管理员可以参考以下操作分别给企业项目 project_A 添加用户组 Test_ECS_A 和企业项目 project_B 添加用户组 Test_ECS_B，并给用户组授予策略或角色，使得用户组中的 IAM 用户获得相应的权限。

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，单击天翼云首页顶部右侧“控制台”。

步骤 2 在控制台首页顶部右侧，单击您的用户名后弹出下拉菜单，单击“企业管理”，在企业管理控制台左侧导航菜单中，单击“项目管理”。

步骤 3 在企业项目管理页中的项目列表，单击企业项目名称“project_A”，在企业项目详情页中，单击“权限管理”页签。



步骤 4 单击“权限管理”页签中的“添加授权”。

步骤 5 在“可选用户组”栏中，勾选待添加用户组即可将待添加的用户组同步至“已选用户组”栏中。

步骤 6 单击“下一步”，对新添加的用户组设置策略，使该用户组在所属企业项目中拥有策略定义的权限。

在可选策略栏中勾选需添加的策略即可同步至“已选策略”栏。

如本例中为用户组添加“ECS Admin”策略。

步骤 7 单击“确定”，完成企业项目用户组的添加及权限授权。

参考步骤 3 至步骤 7 的方法，分别为“project_A”和“project_B”关联用户组并添加相应权限。

----结束

3.6 步骤 5：为企业项目迁入资源

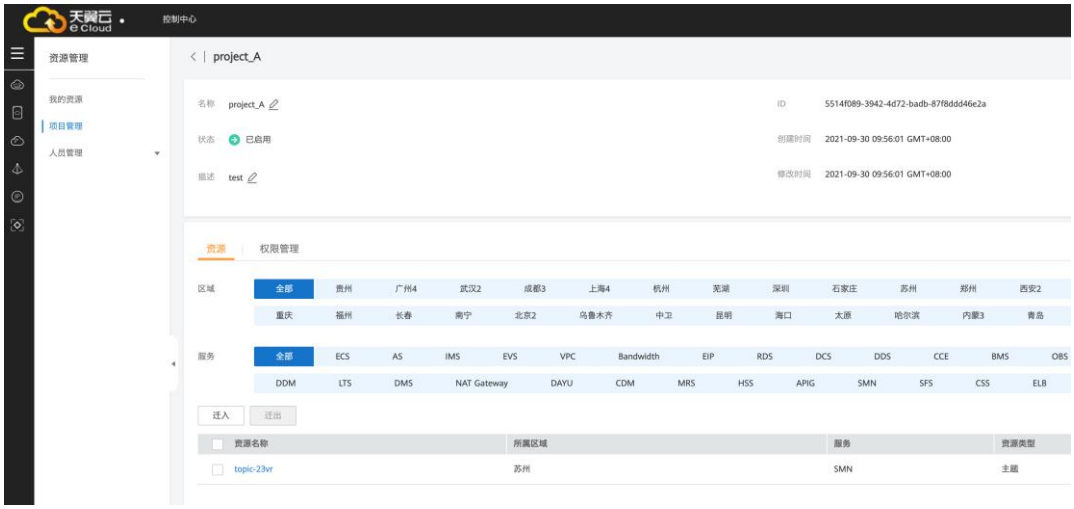
管理员可以参考以下操作分别给企业项目 project_A 和 project_B 迁入对应的云资源

操作步骤

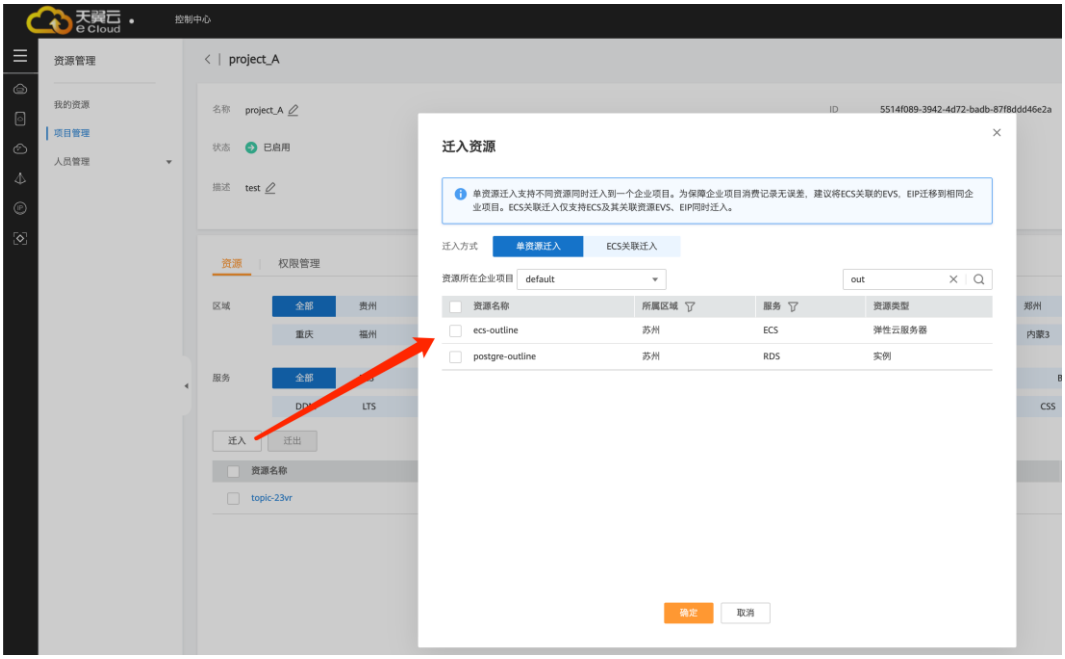
步骤 1 企业管理员使用已注册的天翼云帐号登录天翼云网门户，单击天翼云首页顶部右侧“控制台”。

步骤 2 在控制台首页顶部右侧，单击您的用户名后弹出下拉菜单，单击“企业管理”，在企业管理控制台左侧导航菜单中，单击“项目管理”。

步骤 3 在企业项目管理页中的项目列表，单击企业项目名称“project_A”，在企业项目详情页中，单击“资源”页签。



步骤 4 在“资源”页签，单击“迁入”，弹出迁入资源对话框。



步骤 5 勾选待迁入的资源，单击“确定”。

资源迁入完成后，在当前企业项目的资源列表中即可查看已迁入的资源。

----结束

3.7 验证结果

通过前述步骤，已创建了企业项目、用户组及 IAM 子用户，接下来这些用户即可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 用户可以联系企业管理员重置密码。

操作步骤

步骤 1 IAM 子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。

步骤 3 单击顶部“控制台”，并进入各云服务的管理控制台，检查是否可看到云资源及相应操作权限。

----结束

4 用户指南

4.1 管理企业项目

4.1.1 创建企业用户

您可以根据部门或者业务对资源隔离的要求，创建对应的企业项目，本节指导您创建企业项目。

操作步骤

❿ 创建企业项目的用户必须是企业管理员账号，或在 IAM 侧已被授权 EPS FullAccess 策略的 IAM 子用户。

操作步骤

步骤 1 企业管理员或已被授权 EPS FullAcces 的 IAM 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，单击您的用户名后弹出下拉菜单，单击“企业管理”。

步骤 4 单击企业管理控制台左侧导航菜单“项目管理”，然后再单击右上角“＋创建企业项目”。

步骤 5 在创建企业项目对话框中，输入项目名称和描述，单击“确定”完成项目创建。

----结束

4.1.2 修改/启用/停用企业项目

当您的业务发生变化时，可以对已存在的企业项目进行修改、启用、停用操作。

为了保证您的资源安全，目前暂不支持删除企业项目。如果您不再使用企业项目，您可以停用企业项目。

须知

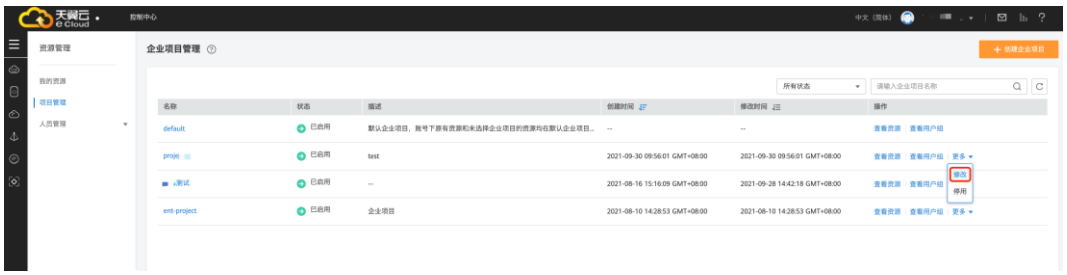
- 已停用企业项目无法使用修改功能。
- 企业项目停用后在云服务创建页的“企业项目”中将不可见，无法迁入资源和添加用户组，如需再次使用，请重新启用该企业项目。
- 当未完成的订单包含该企业项目时，需完成订单后才可停用该企业项目。未完成的订单状态包括：待支付、处理中、待审核、待审批。
- 默认企业项目（default）无法编辑和停用。

修改企业项目

步骤 1 企业管理员登录天翼云网门户，单击天翼云首页顶部右侧“控制台”。

步骤 2 在控制台首页顶部右侧，单击您的用户名后弹出下拉菜单，单击“企业管理”。

步骤 3 在企业项目管理页面，单击左侧功能菜单“项目管理”，进入企业项目列表页面，单击待修改企业项目右侧的“更多”，单击更多下拉菜单中的“修改”。



步骤 4 在修改企业项目信息弹出框中，输入新的“名称”和“描述”。

步骤 5 单击“确定”完成企业项目修改。

----结束

启用/停用企业项目

步骤 1 企业管理员登录天翼云网门户，单击天翼云首页顶部右侧“控制台”。

步骤 2 在控制台首页顶部右侧，单击您的用户名后弹出下拉菜单，单击“企业管理”。

步骤 3 在企业项目管理页面，单击左侧功能菜单“项目管理”，进入企业项目列表页面，单击待启用/停用企业项目右侧的“更多”，单击更多下拉菜单中的“启用”/“停用”。

步骤 4 在企业项目启用/停用确认框中，单击“是”完成企业项目启用/停用。

----结束

4.1.3 为新购云资源选择企业项目

天翼云支持以下两种方式为新建云资源选择企业项目：

- 通过企业项目管理控制台将资源迁入；
- 通过支持按企业项目管理的云服务控制台在开通资源时选择企业项目。

  在购买云资源页面，您可以选择已启用的企业项目，新购云资源将在开通后直接迁入企业项目进行管理。

须知

- **已停用的企业项目无法添加新的云资源，需启用该企业项目后，才可添加新建的云资源。**
- **目前仅有部分云服务支持在购买时直接选择所属企业项目。**

新购资源选择企业项目

在创建云资源页面，您可以选择已启用的企业项目，新创建云资源将可按此企业项目进行管理。以弹性云主机为例，操作步骤如下：

步骤 1 登录天翼云网门户，进入弹性云主机创建页面。

步骤 2 配置弹性云主机的各项信息，在“确认配置”步骤页面中的“企业项目”下拉列表中选择目标企业项目。

步骤 3 单击页面右下方的“立即购买”，完成云资源开通。

步骤 4 弹性云追击购买成功后，您可以在弹性云主机控制台看到您新购买的云资源已归属到所选企业项目。

----结束

4.2 管理企业项目资源

企业项目管理帮助您将相关的资源（例如，具有相同使用用途的资源）集中在一起，按企业中真实项目的方式来管理云资源。

4.2.1 查看全部资源

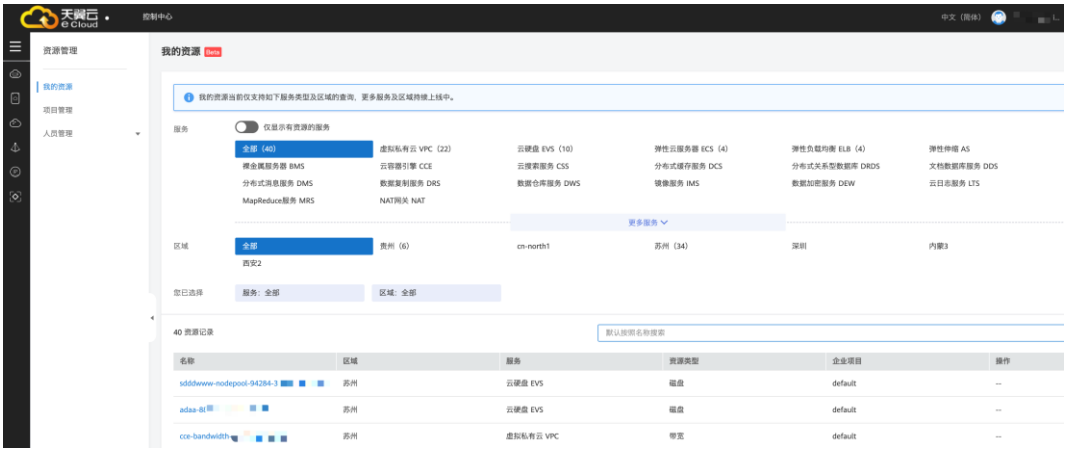
如果您需要查看当前帐号下所有有权限的资源，可以通过“我的资源”页面查看。

操作步骤

步骤 1 企业管理员登录天翼云网门户，单击天翼云首页顶部右侧“控制台”。

步骤 2 在控制台首页顶部右侧，单击您的用户名后弹出下拉菜单，单击“企业管理”。

步骤 3 在企业项目管理页面，单击左侧功能菜单“我的资源”。



步骤 4 “我的资源”页面默认展示部分云服务。您可以单击“更多服务”，查看资源管理支持的所有服务。

您也可以通过打开“仅显示有资源的服务”开关，只查看您拥有资源的服务。

----结束

4.2.2 查看企业项目资源

您可以选择查看某个企业项目下的全部资源，方便您快速了解该企业项目所拥有的资源情况。

操作步骤

步骤 1 企业管理员登录天翼云网门户，单击天翼云首页顶部右侧“控制台”。

步骤 2 在控制台首页顶部右侧，单击您的用户名后弹出下拉菜单，单击“企业管理”。

步骤 3 在企业项目管理页面，单击左侧功能菜单“项目管理”，进入企业项目列表页面，单击待查看企业项目右侧的“查看资源”。

进入企业项目详情页面，在“资源”页签下可查看该企业项目下的资源信息。默认展示全部资源节点及全部产品类型的资源信息，可输入资源名称关键字进行资源筛选。

----结束

4.2.3 为企业项目迁入资源

当资源需要按照企业业务进行分组管理或当资源分组发生变化时，可以对资源进行迁入或迁出操作，实现资源管理权限的重新分配。

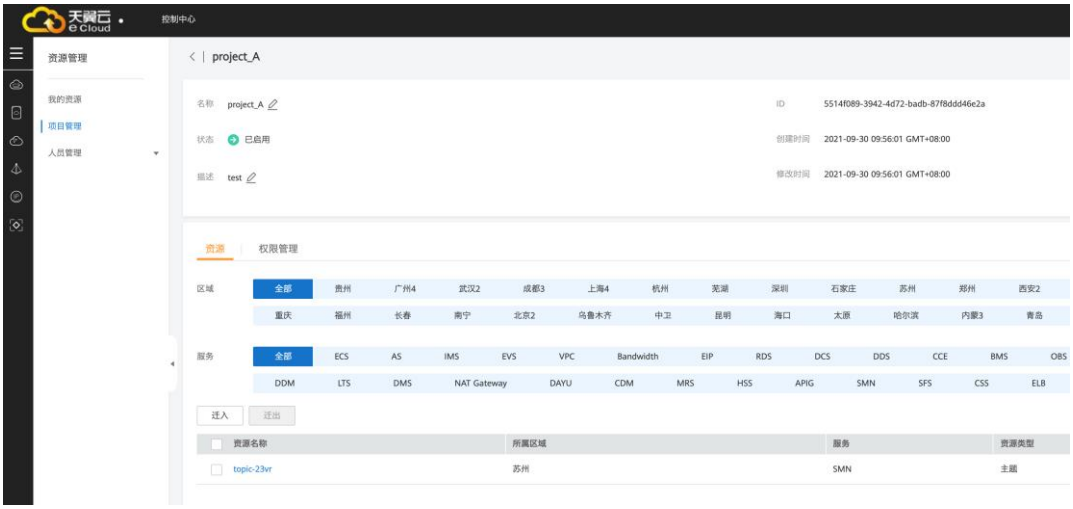
企业项目管理支持跨资源节点将资源迁入到同一企业项目授权管理。

操作步骤

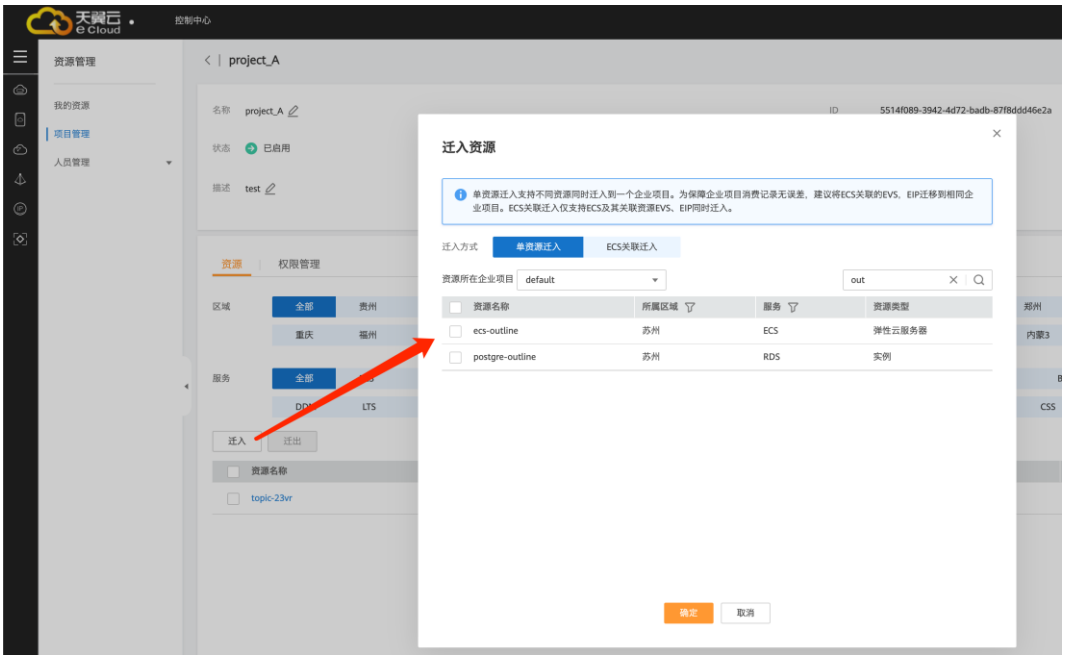
步骤 1 企业管理员使用已注册的天翼云帐号登录天翼云网门户，单击天翼云首页顶部右侧“控制台”。

步骤 2 在控制台首页顶部右侧，单击您的用户名后弹出下拉菜单，单击“企业管理”，在企业管理控制台左侧导航菜单中，单击“项目管理”。

步骤 3 在企业项目管理页中的项目列表，单击企业项目名称，在企业项目详情页中，单击“资源”页签。



步骤 4 在“资源”页签，单击“迁入”，弹出迁入资源对话框。



步骤 5 选择迁入方式。

- 单资源迁入：将每个资源作为独立资源迁入，并且可以同时迁入多个资源。

  如果是除 ECS 外的其他资源时，那么必须选择此项。

  如果资源是 ECS，可以选择此项，表示只迁入 ECS，不迁入 ECS 的关联资源，例如 ECS 绑定的弹性 IP 和云硬盘。

- ECS 关联迁入：只需选择 ECS 资源，其关联的资源将自动同时迁入。

仅当资源是 ECS，才可以选择此项，目前仅支持 ECS 及其关联资源弹性 IP、云硬盘同时迁入。

步骤 6 选择待迁入资源所在的企业项目（“资源所在企业项目”），下方列表展示该企业项目下的所有资源。

步骤 7 勾选待迁入的资源，单击“确定”。

可输入资源名称关键字进行资源筛选。

资源迁入完成后，在当前企业项目的资源列表中即可查看已迁入的资源。

----结束

4.2.4 迁出企业项目资源

当资源需要按照企业业务进行分组管理或当资源分组发生变化时，可以对资源进行迁入或迁出操作，实现资源的重新分配。

企业项目管理支持跨区域将资源迁出到同一企业项目授权管理。

迁出企业项目资源包括以下两种场景：

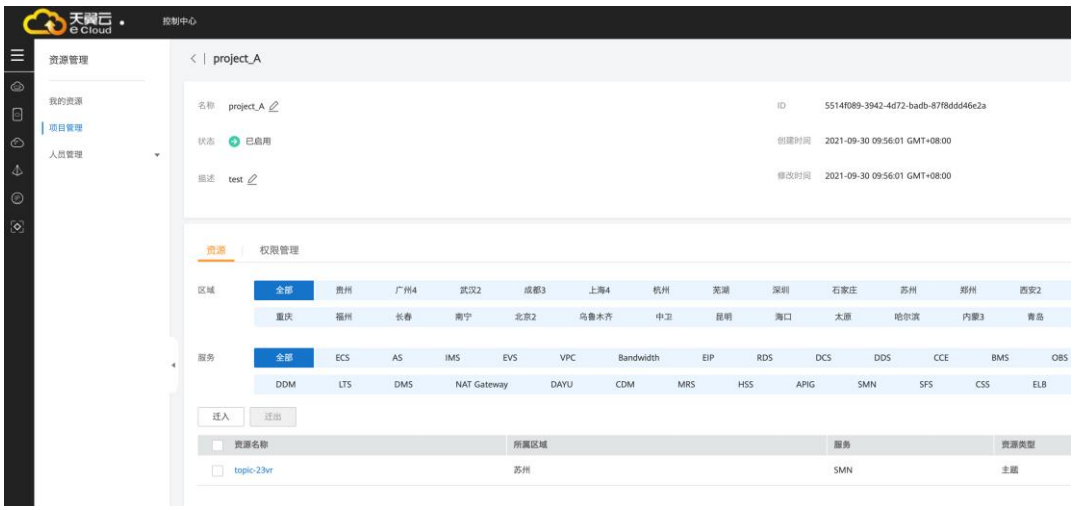
- 将资源从该企业项目迁出到目标企业项目；
- 将资源迁出该企业项目，不再按照已规划的企业项目进行管理（将迁入到系统默认的企业项目“default”中）。

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，单击天翼云首页顶部右侧“控制台”。

步骤 2 在控制台首页顶部右侧，单击您的用户名后弹出下拉菜单，单击“企业管理”，在企业管理控制台左侧导航菜单中，单击“项目管理”。

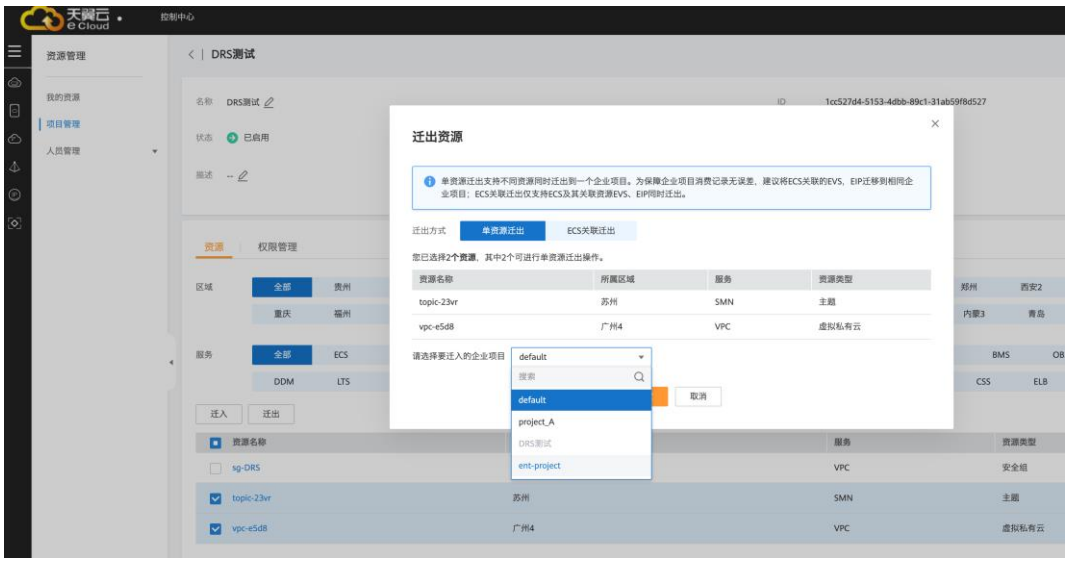
步骤 3 在企业项目管理页中的项目列表，单击待迁出资源企业项目右侧的“查看资源”。



系统进入企业项目详情页面，在“资源”页签下可查看该企业项目内资源信息。

步骤 4 勾选待迁出资源，单击“迁出”。

系统显示“迁出资源”页面。



步骤 5 选择迁出方式。

- 单资源迁出：将每个资源作为独立资源迁出，并且可以同时迁出多个资源。

  如果是除 ECS 外的其他资源时，那么必须选择此项。

  如果资源是 ECS，可以选择此项，表示只迁出 ECS，不迁出 ECS 的关联资源，例如 ECS 绑定的弹性 IP 和云硬盘。

- ECS 关联迁出：只需选择 ECS 资源，其关联的资源将自动同时迁出。

  仅当资源是 ECS，才可以选择此项，目前仅支持 ECS 及其关联资源弹性 IP、云硬盘同时迁出。

步骤 6 选择要迁入的企业项目，单击“确定”。

- 若该资源需按照其他企业项目管理时，在下拉框中选择要迁入的企业项目即可。
- 若该资源不需按照已规划的企业项目管理时，选择系统默认的企业项目“default”即可。

资源迁出完成，在迁入的企业项目资源列表中即可查看已迁出的资源。

----结束

4.3 管理企业项目人员授权

4.3.1 查看企业项目用户组

您可以选择查看某个企业项目下的全部用户组，方便您快速了解该企业项目所拥有的用户组情况。

操作步骤

步骤 1 企业管理员登录天翼云网门户，单击天翼云首页顶部右侧“控制台”。

步骤 2 在控制台首页顶部右侧，单击您的用户名后弹出下拉菜单，单击“企业管理”。

步骤 3 在企业项目管理页面，单击左侧功能菜单“项目管理”。

步骤 4 在企业项目管理列表页面，单击待查看企业项目右侧的“查看用户组”。

系统进入企业项目详情页面，在“用户组”页签下可查看该企业项目所属用户组信息。

----结束

4.3.2 为企业项目添加用户组并授权

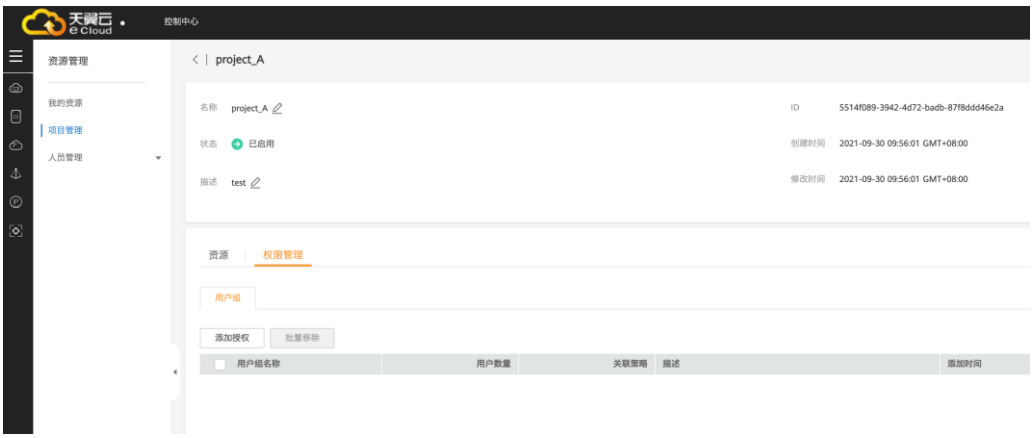
将用户组添加至企业项目中，并为其设置一定的权限策略，该用户组中的用户即可拥有策略定义的对该企业项目中资源的使用权限。

操作步骤

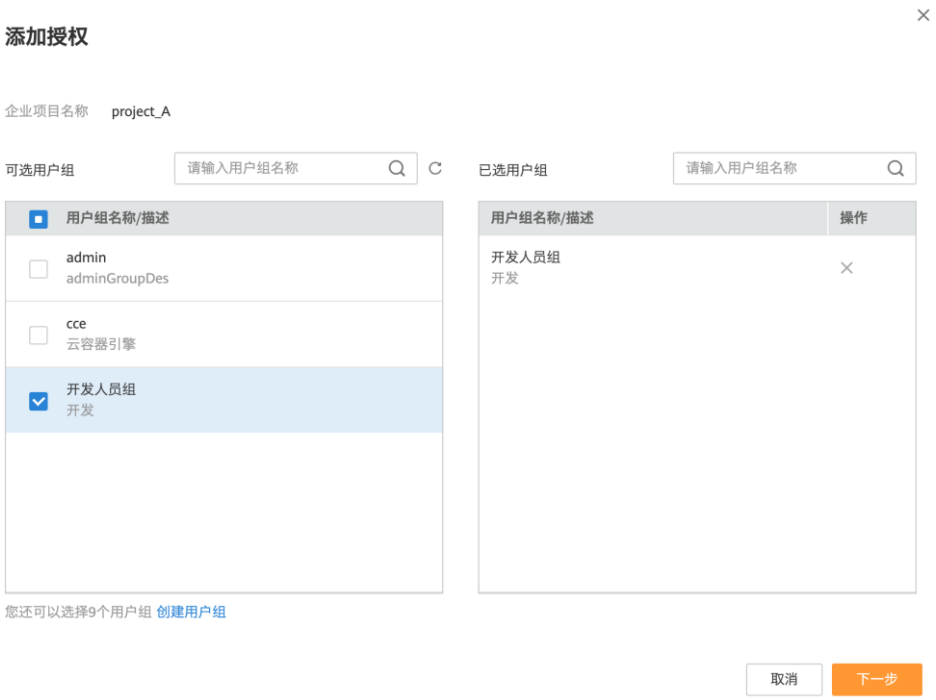
步骤 1 企业管理员使用已注册的天翼云帐号登录天翼云网门户，单击天翼云首页顶部右侧“控制台”。

步骤 2 在控制台首页顶部右侧，单击您的用户名后弹出下拉菜单，单击“企业管理”，在企业管理控制台左侧导航菜单中，单击“项目管理”。

步骤 3 在企业项目管理页中的项目列表，单击待配置企业项目右侧的“查看用户组”。系统进入企业项目详情页面，在“用户组”页签下可查看该企业项目所属用户组信息。



步骤 4 单击“权限管理”页签中的“添加授权”。



步骤 5 （可选）查询可选用户组。

如“可选用户组”展示框中展示用户组过多时，可在输入框中输入待添加用户组，进行查询。

也可单击添加授权窗口下方的“创建用户组”，创建新的用户组。

步骤 6 在“可选用户组”栏中，勾选待添加用户组即可将待添加的用户组同步至“已选用户组”栏中。

您也可点击“添加授权”栏下方的“创建用户组”，新创建用户组后再选择。

步骤 7 单击“下一步”，对新添加的用户组设置策略，使该用户组在所属企业项目中拥有策略定义的权限。

在可选策略栏中勾选需添加的策略即可同步至“已选策略”栏。

步骤 8 单击“确定”，完成企业项目用户组的添加及权限授权。

在当前企业项目的用户组列表中即可查看添加的用户组信息。

须知

策略生效时间大约需要 30s，您可以选择重新登录进行查看。

----结束

其它操作

若需要为该企业项目下已有的用户组设置策略时，可单击该用户组右侧操作列的“设置策略”，具体设置方式请参见本节步骤 7。

4.3.3 移除企业项目用户组

当企业业务发生变化，原用户组不再拥有企业项目的使用权限时，可将这些用户组从该企业项目中移除。

支持进行单个移除和批量移除。

当用户组被移除后，该用户组用户将无法管理该项目，如需再次使用，需要重新给项目添加该用户组。

操作步骤

步骤 1 企业管理员登录天翼云网门户，单击天翼云首页顶部右侧“控制台”。

步骤 2 在控制台首页顶部右侧，单击您的用户名后弹出下拉菜单，单击“企业管理”。

步骤 3 在企业项目管理页面，单击左侧功能菜单“项目管理”。

步骤 4 在企业项目管理列表页面，单击待查看企业项目右侧的“查看用户组”。

系统进入企业项目详情页面，在“用户组”页签下可查看该企业项目所属用户组信息。

步骤 5 选择待移除的用户组，单击右侧操作列的“移除”。

如需批量移除，勾选待移除的用户组，单击上方“批量移除”。

步骤 6 在移除用户组确认框中，单击“是”完成用户组移除。

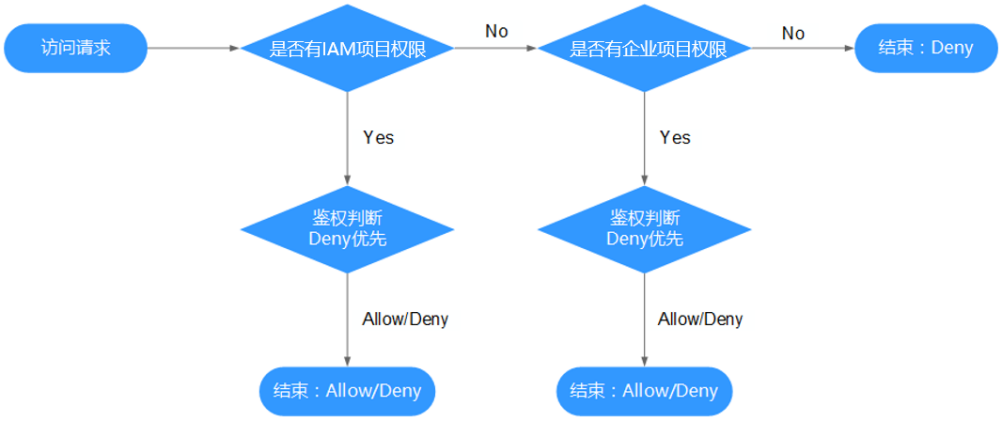
----结束

5 常见问题

5.1 权限管理类

5.1.1 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。

5.1.2 无法找到特定服务的权限怎么办？

如已正确筛选云服务仍无法找到，则该需要设置权限的服务暂不支持企业项目管理EPS，可由企业管理员给对应云服务提交工单，申请该服务接入企业项目管理。

5.1.3 资源迁入/迁出企业项目会影响资源所在的 VPC 和网段吗？

不会。

企业项目发生变化可能会影响其关联的用户的权限，但其下的资源所关联的 VPC 和网段不会变化。

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

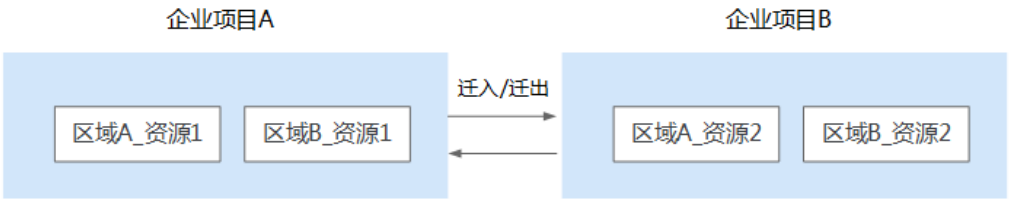
IAM 项目

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。

5.2.3 如何获取企业项目 ID

登录天翼云网门户，进入“控制台”页面，单击右上角用户名，在下拉菜单中选择“业务管理”，单击待查询企业项目名称，进入该企业项目详情页即可查看企业项目 ID。

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。