

企业管理服务

# 用户指南

文档版本 02  
发布日期 2022-11-30



版权所有 © 华为技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 安全声明

## 漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

---

# 目录

<b>1 什么是企业项目</b>	<b>1</b>
<b>2 应用场景</b>	<b>2</b>
<b>3 支持的云服务</b>	<b>5</b>
<b>4 权限说明</b>	<b>6</b>
4.1 企业项目权限说明	6
4.2 云服务权限说明	7
<b>5 如何进入项目管理页面</b>	<b>8</b>
<b>6 多项目管理实践案例</b>	<b>9</b>
6.1 实践场景	9
6.2 实践步骤	10
<b>7 企业项目管理</b>	<b>14</b>
7.1 创建企业项目	14
7.2 修改/启用/停用企业项目	15
7.3 为新创建的云资源选择企业项目	16
<b>8 企业项目资源管理</b>	<b>18</b>
8.1 资源管理简介	18
8.2 查看企业项目下的资源	18
8.3 为企业项目迁入资源	19
8.4 迁出企业项目资源	19
<b>9 企业项目人员管理</b>	<b>21</b>
9.1 查看企业项目用户组	21
9.2 为企业项目添加用户组并授权	21
9.3 移除企业项目用户组	22
<b>10 审计</b>	<b>24</b>
10.1 支持审计的关键操作列表	24
10.2 查询审计事件	25
<b>11 关于配额</b>	<b>27</b>
<b>12 常见问题</b>	<b>28</b>
12.1 IAM 和企业管理的区别	28

---

12.2 IAM 项目和企业项目的区别.....	30
12.3 在什么场景下可以看到所有的企业项目.....	30
12.4 如何获取企业项目 ID.....	31
12.5 最多可以创建多少个企业项目? .....	31
12.6 资源迁入/迁出企业项目会影响资源所在的 VPC 和网段吗? .....	31
<b>13 修订记录.....</b>	<b>32</b>

# 1 什么是企业项目

## 简介

企业管理（Enterprise Management，简称“EM”），又称“企业项目管理服务（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平台。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、业务的管理，提供企业项目管理、资源管理、人员管理能力。

### 说明

企业项目管理为免费服务，无需付费即可使用。

# 2 应用场景

用户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。

下面介绍企业项目的典型应用场景。

## 按业务项目划分场景

企业中有多个项目，多个项目的资源需要分开结算，且分属不同人员进行管理。同时项目可以单独启动或停止，对其他项目没有影响。那么可以针对企业中的每个项目，分别建立企业项目，管理各自的资源，并且针对不同的企业项目，设置不同的人员进行管理。

例如：某游戏公司上线多款游戏产品（例如A、B、C三款游戏），每款游戏独立核算成本。有些游戏受大众欢迎，持续运营。有些游戏大众反应不好，运营一段时间后下线。那么该游戏公司可以申请账号，将游戏公司下面的每款游戏作为单独的企业项目进行管理（企业项目A、B、C），同时为每个企业项目设置不同的用户组进行管理。此场景中，企业架构示意图如[图2-1](#)所示，对应的解决方案示意图如[图2-2](#)所示。

图 2-1 企业架构示意图

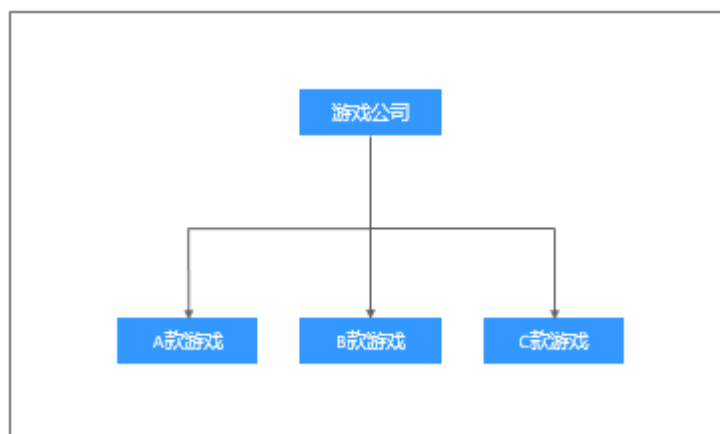
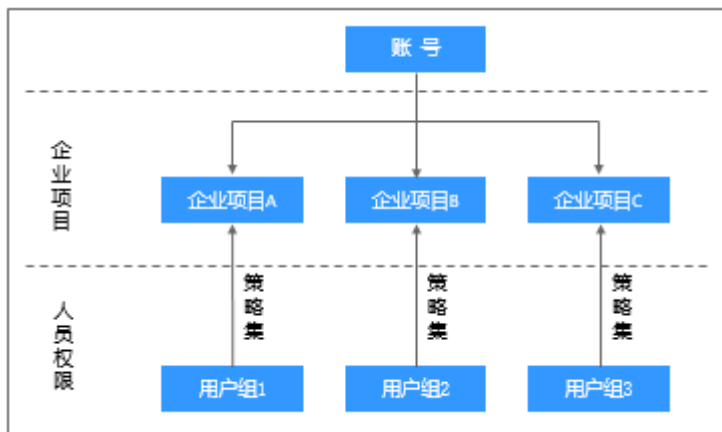


图 2-2 解决方案示意图



### 按组织架构+业务项目划分场景

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

例如：某互联网企业在软件开发过程中需要部署开发环境和生产环境，开发环境用来做Alpha、Beta、Gamma测试，生产环境用来按项目核算成本（例如APP项目、商城项目、协同办公项目）。且要求开发环境和生产环境隔离，避免开发测试影响到生产环境的成本核算。那么该互联网企业可以申请两个账号，将开发环境和生产环境作为账号1和账号2，然后将开发环境下的Alpha、Beta、Gamma环境分别作为企业项目A、企业项目B、企业项目C，将生产环境下的APP项目、商城项目、协同办公项目分别作为企业项目D、企业项目E、企业项目F。同时为每个企业项目设置不同的用户组进行管理。此场景中，企业架构示意图如图2-3所示，对应的解决方案示意图如图2-4所示。

图 2-3 企业架构示意图

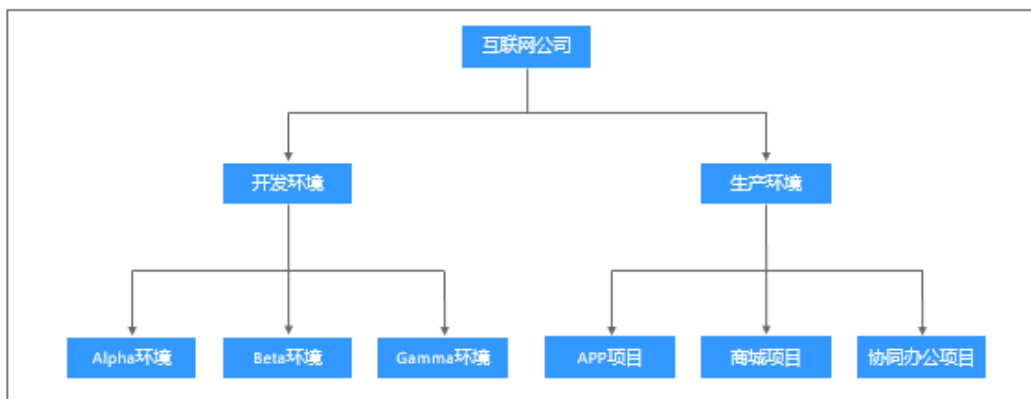
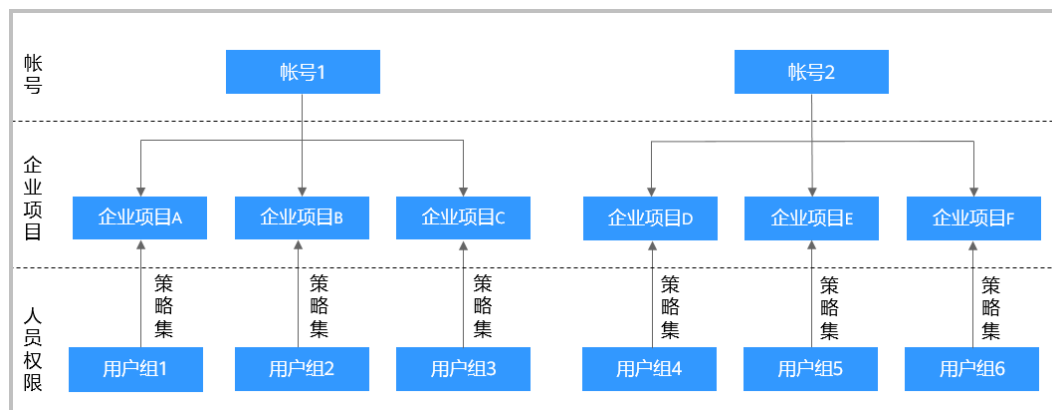




图 2-4 解决方案示意图



# 3 支持的云服务

---

企业项目管理支持的云服务及对应资源类型请以控制台界面显示为准。

进入“企业项目管理”页面，在企业项目列表中单击任一企业项目操作列的“查看资源”，系统进入企业项目详情页面，在“资源”页签下可查看企业项目支持的服务及其对应资源类型等信息。

# 4 权限说明

## 4.1 企业项目权限说明

**管理员用户权限：**可以对企业项目管理页面的所有菜单项执行任意操作。

**IAM用户权限：**IAM用户的操作由管理员用户授权，登录企业项目管理页面后，仅显示管理员用户分配给IAM用户有权管理的企业项目信息，只能操作管理员用户分配的资源。若管理员用户为IAM用户设置了具体的权限策略，则IAM用户可以拥有策略内容中对应的权限。

管理员用户可以通过系统策略或自定义策略为IAM用户设置具体权限，目前与企业项目相关的策略主要包括EPS FullAccess、EPS ReadOnlyAccess。您可以通过统一身份认证服务给IAM用户配置企业项目相关权限，详见《统一身份认证服务用户指南》。

在IAM侧设置和在企业管理侧设置时，权限内容不同。建议管理员结合企业需求选择IAM或是企业管理进行资源权限管理。

表 4-1 企业管理系统权限

服务名称	权限名称	权限说明	适用的典型人员
企业管理	EPS FullAccess	<ul style="list-style-type: none"> <li>企业管理的管理员权限，包括企业项目以及人员管理的所有权限，可以创建企业、迁移资源、添加移除用户组，为用户组设置策略等。由管理员在IAM侧的全局服务中设置。</li> <li>单个企业项目的管理员权限，仅拥有指定企业项目的权限，包括修改、启用、停用、查看企业项目。可以由管理员以及具备IAM侧EPS FullAccess的用户在企业管理中设置。</li> </ul>	企业资产管理

服务名称	权限名称	权限说明	适用的典型人员
	EPS ReadOnlyAccess	<p>企业项目的只读权限，拥有该权限的用户可以执行查询操作。</p> <ul style="list-style-type: none"> <li>• 企业管理的只读权限，可以查看所有企业项目以及用户信息。由管理员在IAM侧的全局服务中设置。</li> <li>• 单个企业项目的只读权限，可以由管理员以及具备IAM侧EPS FullAccess的用户在企业管理中设置。</li> </ul>	企业资产查询人员

表 4-2 常用操作与系统权限的关系

操作	EPS FullAccess	
查看企业项目下资源	√	√
创建企业项目	√	×
修改企业项目	√	×
启用企业项目	√	×
停用企业项目	√	×
企业项目资源迁入	√	×
企业项目资源迁出	√	×

## 4.2 云服务权限说明

企业管理支持通过给企业相关的用户组添加相应的云服务权限实现对云服务的管理。

- 在企业管理中为用户组添加策略，具体操作请参见[为企业项目添加用户组并授权](#)。
- 在IAM中为用户组添加策略，具体请参见。
- 在IAM中自定义策略，具体操作请参见。

# 5 如何进入项目管理页面

---

## 前提条件

您必须已经获得使用企业项目管理服务的授权。

## 操作步骤

**步骤1** 登录管理控制台。

**步骤2** 在控制台页面，鼠标移动至右上方的账号名，在下拉列表中选择“企业管理”。  
系统进入“企业项目管理”页面。

----结束

# 6 多项目管理实践案例

## 6.1 实践场景

A公司是企业用户，企业中有多个项目团队，需要为项目团队申请资源、配置人员、进行项目管理。本文针对A公司提出的企业需求，给出多项目管理最佳实践。

### 企业需求

- **需求1:** A公司需要同时在“region\_01”、“region\_02”创建多种资源，并将其按需分配给两个项目团队，两个项目中的资源相互隔离。
- **需求2:** 每个项目团队的成员只能访问其所在项目团队的资源，且仅拥有能够完成工作的资源使用最小权限。

### 解决方案

- **针对需求1:** 当前提供的企业管理服务（EM）和统一身份认证服务（IAM），均可实现项目之间的资源隔离，但两种服务的实现逻辑及功能不同。
  - 企业管理服务：在企业管理服务中创建企业项目，企业项目之间的资源是逻辑隔离，针对企业不同项目间的资源进行分组和管理，**一个企业项目中可以包含多个区域的资源**。企业项目之间的资源可以动态的迁入和迁出。
  - 统一身份认证服务：在统一身份认证服务中创建IAM项目可以实现资源之间的物理隔离，针对同一个区域内的资源进行分组和隔离，**一个IAM项目中只能包含一个区域中的资源**。IAM项目之间的资源无法动态地迁入和迁出。

综上，企业管理服务能够实现项目间跨区域的资源隔离，隔离逻辑更加灵活，因此，推荐A公司使用企业管理服务进行项目资源管理，以下需求将基于企业管理服务提出解决方案。如需了解更多统一身份认证和企业管理的区别，请参见：[IAM和企业管理的区别](#)。

- **针对需求2:** A公司需要配合使用企业管理服务和统一身份认证服务，在统一身份认证服务中创建用户组、为每个员工创建IAM用户并加入用户组，再将用户组添加至**需求1**创建的企业项目，并按照**表1**为各企业项目中的用户组授予相应的资源使用权限。

图 6-1 A 公司人员配置模型

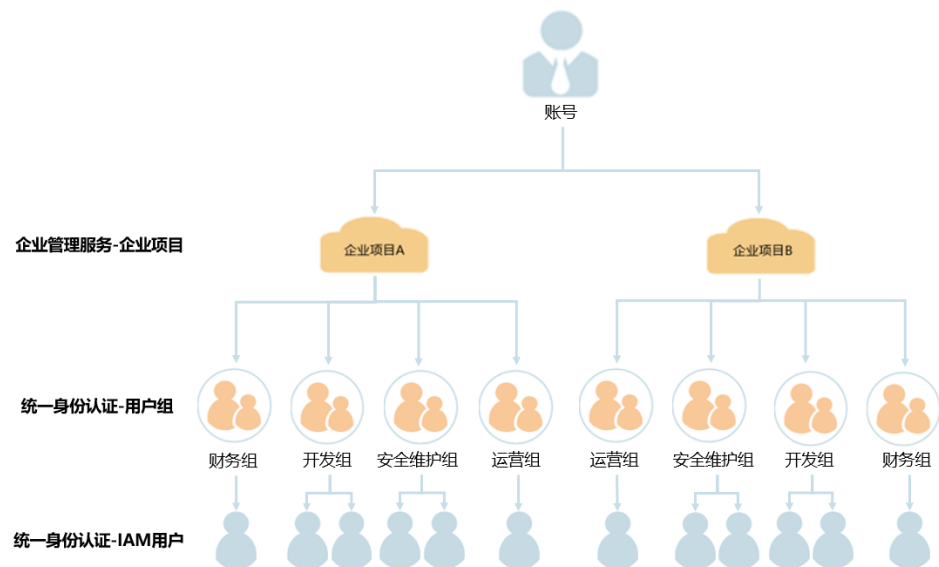


表 6-1 A 公司各用户组权限配置模型

用户组	职责	所需权限	描述
开发组	负责使用资源进行项目开发。		弹性负载均衡（ELB）的所有执行权限。
		OBS Administrator	对象存储服务（OBS）的所有执行权限。
		EPS FullAccess	企业管理服务（EM）的所有执行权限。
安全维护组	负责项目的安全运维。	ECS CommonOperations	弹性云服务器（ECS）的普通操作权限。
运营组	负责所有项目的总体运营。	EPS FullAccess	企业管理服务的所有执行权限，包括修改、启用、停用、查看企业项目。

**说明**

如需了解所有云服务的系统权限，请参见：[系统权限](#)。

## 6.2 实践步骤

针对A公司的企业需求及其解决方案，按照如下流程构建项目团队、创建资源，实现企业项目管理。

图 6-2 企业项目管理流程图



**步骤1：创建企业项目：**在企业管理服务控制台创建企业项目。

**步骤2：创建IAM用户及用户组：**在统一身份认证服务控制台为各职能团队创建用户组、为员工创建IAM用户，并将IAM用户加入用户组，实现人员分组。

**步骤3：企业项目与IAM用户组关联授权：**在企业管理服务控制台为各用户组授予应有的权限，并将其加入相应的企业项目，实现人员授权。

**步骤4：创建资源并关联企业项目：**在云服务控制台创建资源，并选择所属企业项目，实现资源隔离。

**后续操作：企业项目管理：**在企业管理服务控制台进行人员、资源管理。

## 创建企业项目

通过本节在企业管理控制台创建名为“企业项目A”、“企业项目B”的企业项目。

**步骤1** 在企业项目管理页面，单击“创建企业项目”。

**步骤2** 在创建企业项目页面，输入“名称”为“企业项目A”，单击“确定”，完成“企业项目A”创建。

**步骤3** 重复步骤3~4，创建“企业项目B”。

创建企业项目后，项目管理列表中显示新创建的“企业项目A”和“企业项目B”。

----结束



## 创建 IAM 用户及用户组

本节以创建名为“企业项目A\_开发”的用户组、名为“Murphy”的用户，并将“Murphy”加入“企业项目A\_开发”为例，介绍创建用户组、IAM用户的方法。

### 步骤1 创建用户组。

1. 在管理控制台，单击“管理与部署”，选择“统一身份认证服务”。
2. 在统一身份认证服务的左侧导航栏中，选择“用户组”页签，单击右上方的“创建用户组”。
3. 在创建用户组页面，输入“用户组名称”为“企业项目A\_开发”，单击“确定”，用户组“企业项目A\_开发”创建完成。
4. 重复2~3为两个企业项目分别创建财务组、安全维护组、运营组。

创建用户组后，用户组列表中显示新创建的用户组。

### 步骤2 创建IAM用户并加入用户组。详见《统一身份认证服务用户指南》。

1. 在统一身份认证服务的左侧导航中，选择“用户”，单击右上方的“创建用户”。
2. 在创建用户页面，填写“用户信息”并选择“访问方式”、“凭证类型”和“登录保护”，单击“下一步”。
3. 勾选要加入的用户组，将用户加入到用户组。加入用户组后，用户将具备用户组的权限。单击“下一步”，IAM用户“Murphy”创建完成。
4. 重复1~3为所有员工创建IAM用户，并将其加入相应的用户组。

创建IAM用户后，用户列表中显示新创建的用户。在用户组的“用户组管理”页面可以查看各个用户组中的IAM用户。

----结束

## 企业项目与 IAM 用户组关联授权

本节介绍添加用户组“企业项目A\_开发”至企业项目“企业项目A”，并为“企业项目A\_开发”授予EPS FullAccess权限，使“企业项目A\_开发”拥有管理企业项目“企业项目A”的权限。通过本节，您将了解企业项目与IAM用户组关联授权的详细步骤。

**步骤1** 在企业管理页面，单击“企业项目A”右侧的“查看用户组”。

**步骤2** 在企业项目A详情页，选择“权限管理 > 用户组 > 添加授权”。

**步骤3** 在添加授权页面，选择“项目团队A\_开发”，单击“下一步”。


**步骤4** 搜索并选择“EPS FullAccess”，单击“确定”，即可授予用户组“企业项目A\_开发”对企业项目A的管理权限。

企业项目与IAM用户组关联授权后，可单击企业项目右侧的“查看用户组”，在“权限管理”页签中查看用户组，单击用户组右侧的“设置策略”即可查看或修改用户组权限。

----结束

## 创建资源并关联企业项目

本节以创建弹性负载均衡并将其关联至企业项目“企业项目A”为例，介绍如何为企业项目关联资源。

- 步骤1** 登录管理控制台，单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
- 步骤2** 单击页面右上角的“创建弹性负载均衡”，系统进入创建页。
- 步骤3** 配置弹性负载均衡各项信息，在“企业项目”下拉列表中选择“企业项目A”。
- 步骤4** 单击页面右下角的“立即申请”。
- 步骤5** 确认配置信息，并单击“提交”。
- 步骤6** 按照**步骤1~步骤5**的方法，为两个企业项目分别创建所需资源。

创建成功后，可以在企业管理页面中单击“企业项目A”、“企业项目B”右侧的“查看资源”查看企业项目中的资源。

#### 说明

- 目前企业项目支持管理部分云服务资源，详情请参见：[支持的云服务](#)。
- 如果您已创建资源，仅需要关联资源与企业项目，可以使用企业管理服务提供的迁入功能，详情请参见：[为企业项目迁入资源](#)。

----结束

## 后续操作：企业项目管理

经过以上步骤，用户可以在“企业项目管理”页面，管理自己的企业项目。

- **资源管理**：单击企业项目右侧的“查看资源”，即可查看企业项目的已有资源，并[为企业项目迁入资源](#)。
- **人员管理**：单击企业项目右侧的“查看用户组”，即可查看企业项目所包含的用户、用户组，并修改用户组及其权限。

# 7 企业项目管理

## 7.1 创建企业项目

### 操作场景

您可以根据部门或者业务，创建对应的企业项目，本小节指导您创建企业项目。

### 前提条件

创建企业项目的用户必须是管理员，或在IAM侧已关联EPS FullAccess策略的用户。

### 约束与限制

每个账号默认可以创建100个企业项目。

### 操作步骤

**步骤1** 在控制台页面，鼠标移动至右上方的账号名，单击账号名，在下拉列表中选择“企业管理”。

系统进入“企业项目管理”页面。

**步骤2** 在企业项目管理页面，单击页面右上方的“创建企业项目”。

系统显示“创建企业项目”页面。

**步骤3** 输入名称和描述，单击“确定”。

表 7-1 配置规则信息

参数	说明
名称	名称不超过255个字符，只能由中文、英文字母、数字、下划线、中划线组成，且不能使用任何大小写形式的“default”。 例如：project_A

参数	说明
描述	描述不超过512个字符。 例如：The Enterprise project is used to manage the resources of Project A.

#### 说明

为了避免个人数据泄露，建议用户勿将个人及敏感信息包含在企业项目描述或资源标签中。

----结束

## 7.2 修改/启用/停用企业项目

### 操作场景

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。

#### 说明

- 已停用企业项目无法使用修改功能。
- 停用后的企业项目仍会占用企业项目配额，如果您的企业项目配额不足，建议您联系运维人员为您提供企业项目删除功能。
- 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。
- 默认企业项目无法编辑和停用。

### 修改企业项目

当企业项目的名称有变化或需要修改企业项目的描述时，您可以根据以下操作步骤对企业项目进行修改。

**步骤1** 在控制台页面，鼠标移动至右上方的账号名，在下拉列表中选择“企业管理”。

系统进入“企业项目管理”页面。

**步骤2** 选择待修改的企业项目，单击操作列的“更多”，选择“修改”。

系统弹出“修改企业项目”页面。

**步骤3** 修改“名称”或“描述”。

表 7-2 配置规则信息

参数	说明
名称	名称不超过255个字符，只能由中文、英文字母、数字、下划线、中划线组成，且不能使用任何大小写形式的“default”。 例如：project_A
描述	描述不超过512个字符。 例如：The Enterprise project is used to manage the resources of Project A.

**步骤4** 单击“确定”，完成修改。

----结束

## 启用企业项目

对于已经停用的企业项目，如需再次使用时，可进行启用操作。

**步骤1** 在控制台页面，鼠标移动至右上方的账号名，在下拉列表中选择“企业管理”。

系统进入“企业项目管理”页面。

**步骤2** 选择状态为已停用的企业项目，单击右侧操作列的“更多”，选择“启用”。

系统弹出启用企业项目确认页面。

**步骤3** 单击“是”，企业项目启用成功。

----结束

## 停用企业项目

当企业结构进行调整或者业务缩减时，不再使用某些企业项目时，可停用该企业项目。

**步骤1** 在控制台页面，鼠标移动至右上方的账号名，在下拉列表中选择“企业管理”。

系统进入“企业项目管理”页面。

**步骤2** 选择状态为已启用的企业项目，单击右侧操作列的“更多”，选择“停用”。

系统弹出停用企业项目确认页面。

**步骤3** 单击“是”，企业项目停用成功。

----结束

## 7.3 为新创建的云资源选择企业项目

### 操作场景

在创建云资源页面，您可以选择已启用的企业项目，新创建的云资源将可按此企业项目进行管理。

有以下方式可以为新建云资源选择企业项目：

- 通过企业项目管理控制台的创建资源入口。
- 通过支持按企业项目管理的云服务控制台选择企业项目。

## 约束与限制

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。

### 通过企业项目管理控制台选择企业项目

**步骤1** 在控制台页面，鼠标移动至右上方的账号名，在下拉列表中选择“企业管理”。

系统进入“企业项目管理”页面。

**步骤2** 在企业项目列表中单击某个企业项目的名称，进入某个企业项目详情页。

**步骤3** 通过页面右上方的“创建资源”或“网络规划”入口，为企业项目添加需要的云资源。

----结束

### 通过支持按企业项目管理的云服务控制台选择企业项目

在创建云资源页面，配置“企业项目”时，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。

以弹性云服务器为例，操作步骤如下：

**步骤1** 登录管理控制台。

**步骤2** 单击管理控制台左上角的 ，选择区域和项目。

**步骤3** 选择“计算 > 弹性云服务器”。

**步骤4** 单击页面右上角的“创建弹性云服务器”。

系统进入创建页。

**步骤5** 配置弹性云服务器各项信息，在“企业项目”下拉列表中选择目标企业项目。

**步骤6** 单击“立即申请”。

**步骤7** 弹性云服务器创建成功后，您可以在弹性云服务器信息页面看到您新创建的弹性云服务器已归属所选企业项目。

----结束

# 8 企业项目资源管理

## 8.1 资源管理简介

企业项目管理提供了一种按企业项目管理云资源的方式，帮助您实现以企业项目为基本单元的资源及人员的统一管理。

### 说明

IAM项目和企业项目的区别请参见[IAM项目和企业项目的区别](#)。

## 8.2 查看企业项目下的资源

### 操作场景

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** 在控制台页面，鼠标移动至右上方的账号名，在下拉列表中选择“企业管理”。

系统进入“企业项目管理”页面。

**步骤2** 选择待查看的企业项目，单击操作列“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3** 设置资源搜索条件。

1. 选择搜索区域。
2. 选择服务类型。
3. 选择资源类型。

页面下方列表展示筛选后的所有资源。

----结束

## 8.3 为企业项目迁入资源

### 操作场景

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入到同一企业项目授权管理。

### 操作步骤

**步骤1** 在控制台页面，鼠标移动至右上方的账号名，在下拉列表中选择“企业管理”。  
系统进入“企业项目管理”页面。


**步骤2** 选择待迁入资源的企业项目，单击操作列的“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3** 单击“迁入”。  
系统显示“迁入资源”页面。

**步骤4** 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，例如该ECS绑定的EIPs和EVS disks。
- 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EVS disks、EIPs同时迁入。

**步骤5** 在资源列表上方的筛选框中对“服务”、“区域”和“企业项目”进行筛选，或者在搜索框中直接输入资源名称进行精确搜索。

**步骤6** 单击列表中资源类型列的，对“资源类型”进行筛选。  
下方展示符合条件的资源。  
迁入方式为“ECS关联迁入”时，不支持对“服务”和“资源类型”进行筛选。

**步骤7** 勾选待迁入资源，单击“确定”。  
资源迁入完成，在当前企业项目的资源列表中即可查看迁入的资源。

----结束

## 8.4 迁出企业项目资源

### 操作场景

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** 在控制台页面，鼠标移动至右上方的账号名，在下拉列表中选择“企业管理”。  
系统进入“企业项目管理”页面。

**步骤2** 选择待迁入资源的企业项目，单击操作列的“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3** 勾选待迁出资源，单击“迁出”。  
系统显示“迁出资源”页面。

**步骤4** 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，例如该ECS绑定的EIPs和EVS disks。
- 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EVS disks、EIPs同时迁出。

**步骤5** 选择目标企业项目，单击“确定”。  
若该资源需按照其他企业项目管理时，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，在迁入企业项目的资源列表中即可查看已迁出的资源。

---结束

# 9 企业项目人员管理

## 9.1 查看企业项目用户组

**步骤1** 在控制台页面，鼠标移动至右上方的账号名，在下拉列表中选择“企业管理”。  
系统进入“企业项目管理”页面。

**步骤2** 选择待查看的企业项目，单击操作列的“查看用户组”。

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

---结束

## 9.2 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。本小节指导您如何为企业项目添加用户组。

### 添加用户组

**步骤1** 在控制台页面，鼠标移动至右上方的账号名，在下拉列表中选择“企业管理”。  
系统进入“企业项目管理”页面。

**步骤2** 选择待查看的企业项目，单击操作列的“查看用户组”。

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

**步骤3** 单击“添加授权”。

系统显示“添加授权”页面。

**步骤4** （可选）查询可选用户组。

在“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。

**步骤5** 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”展示框。

也可单击左下方“创建用户组”立即创建用户组。创建用户组的具体操作请参见《统一身份认证服务用户指南》。

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

1. 选择策略。您可以在可选策略的下拉复合框中按照“所有策略”、“自定义策略”、“系统策略”对已有策略进行筛选，也可以创建自定义策略。

设置策略时，一个用户组最多可以选择25个策略。

- 创建自定义策略的具体操作请参见《统一身份认证服务用户指南》。

2. 勾选待添加的策略，将选择的策略同步至“已选策略”展示框。

**步骤7** 单击“确定”，用户组添加完成。

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。

#### 说明

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

## 其他操作

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**步骤6**。

管理员创建用户组并授权后，将用户加入用户组中，使用户具备用户组的权限，实现用户的授权。给已授权的用户组中添加或者移除用户，快速实现用户的权限变更。

## 9.3 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。

可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企业项目，如需再次使用，需要重新给企业项目添加该用户组。

### 单个移除

**步骤1** 在控制台页面，鼠标移动至右上方的账号名，在下拉列表中选择“企业管理”。

系统进入“企业项目管理”页面。

**步骤2** 选择待移除用户组的企业项目，单击操作列的“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3** 选择待移除的用户组，单击右侧操作列的“移除”。

系统显示“确定要移除以下用户组吗？”页面。

- 步骤4** 单击“是”。
- 用户组移除完成。
- 结束

## 批量移除

- 步骤1** 在控制台页面，鼠标移动至右上方的账号名，在下拉列表中选择“企业管理”。
- 系统进入“企业项目管理”页面。
- 步骤2** 选择待移除用户组的企业项目，单击操作列的“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3** 勾选待移除的用户组，单击用户组列表上方的“批量移除”。
- 系统显示“确定要移除以下用户组吗？”页面。
- 步骤4** 单击“是”。
- 用户组批量移除完成。
- 结束

# 10 审计

## 10.1 支持审计的关键操作列表

云审计服务支持的企业项目管理操作列表如表10-1所示。

表 10-1 云审计服务支持的 EPS 操作列表

操作名称	资源类型	事件名称
创建企业项目	enterpriseProject	createEnterpriseProject
修改企业项目	enterpriseProject	modifyEnterpriseProject
停用企业项目	enterpriseProject	disableEnterpriseProject
启用企业项目	enterpriseProject	enableEnterpriseProject
资源迁移	enterpriseProjectResource	migrate
资源关联迁出	enterpriseProjectResource	associatedMigrateOut
资源关联迁入	enterpriseProjectResource	associatedMigrateIn
资源迁入	enterpriseProjectResource	migrateIn
资源迁出	enterpriseProjectResource	migrateOut

## 10.2 查询审计事件

### 操作场景

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

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录：

- [在事件列表查看审计事件](#)

### 在事件列表查看审计事件


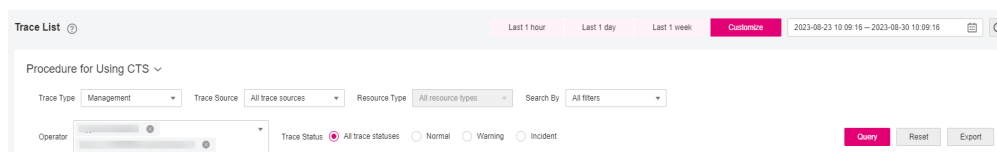


1. 登录管理控制台。
2. 单击左上角 ，选择“管理与部署 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过筛选来查询对应的操作事件，如图10-1所示。当前事件列表支持四个维度的组合查询，详细信息如下：

图 10-1 筛选框



- 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
    - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
    - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。
    - 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。
  - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
  - 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
  - 时间范围：可选择查询最近7天内任意时间段的操作事件。
  - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
5. 选择完查询条件后，单击“查询”。
  6. 在事件列表页面，您还可以导出操作记录文件和刷新列表。
    - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。

- 单击  按钮，可以获取到事件操作记录的最新信息。
7. 在需要查看的事件左侧，单击  展开该记录的详细信息。

Trace Name	Resour...	Trac...	Resource ID	Resource Name...	Trace Stat...	Operator	Operation Time	Operat...
login	user	IAM	3c...	7...	normal	14399999999999999999	Nov 25, 2022 15...	View Trace

trace_id	01
code	302
trace_name	login
resource_type	user
trace_rating	normal
message	["User_type":"domain owner","login_protect":{"status":"off"}]
source_ip	
trace_type	ConsoleAction
service_type	IAM
event_type	global
project_id	
resource_id	3
tracker_name	system
time	Nov 25, 2022 15:35:44 GMT+08:00
resource_name	
user	["Domain":{"name":"...", "id":"...", "name":"...", "id":"..."}]
record_time	Nov 25, 2022 15:35:44 GMT+08:00

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

✕

**查看事件**

```

{
  "request": "",
  "trace_id": "676d4ae3-842b-11ee-9299-9159eee6a3ac",
  "code": "200",
  "trace_name": "createDockerConfig",
  "resource_type": "dockerlogincmd",
  "trace_rating": "normal",
  "api_version": "",
  "message": "createDockerConfig, Method: POST Url=/v2/manage/utlils/secret, Reason:",
  "source_ip": "",
  "domain_id": "",
  "trace_type": "ApiCall",
  "service_type": "SWR",
  "event_type": "system",
  "project_id": "",
  "response": "",
  "resource_id": "",
  "tracker_name": "system",
  "time": "2023/11/16 10:54:04 GMT+08:00",
  "resource_name": "dockerlogincmd",
  "user": {
    "domain": {
      "name": "",
      "id": ""
    }
  }
}

```

9. 关于事件结构的关键字段详解，请参见“云审计服务事件参考 > 事件结构”章节和“云审计服务事件参考 > 事件样例”章节。

# 11 关于配额

## 什么是配额？

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少个企业项目。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

一个账号允许创建的企业项目数量默认为100个，如需调整企业项目最大配额，您可以申请扩大配额。

企业项目数量的配额最大支持调整为256个。

## 如何申请扩大配额？

1. 登录管理控制台。
2. 在页面右上角，选择“资源 > 我的配额”。  
系统进入“服务配额”页面。
3. 在页面右上角，单击“申请扩大配额”。
4. 在“新建工单”页面，根据您的需求，填写相关参数。  
其中，“问题描述”项请填写需要调整的内容和申请原因。
5. 填写完毕后，勾选协议并单击“提交”。



# 12 常见问题

## 12.1 IAM 和企业管理的区别

企业管理是提供给企业客户的与多层次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、人员管理、资源管理。

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

与IAM相同的是，企业管理可以进行人员管理及权限分配，不同的是，企业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管理服务。

更多有关IAM功能的介绍请参见《统一身份认证服务用户指南》。

### IAM 和企业管理的区别

- 开通方式
  - IAM是身份管理服务，注册系统账号后，无需付费即可使用。
  - 企业管理是资源管理服务，注册系统账号后，无需付费即可使用。
- 资源隔离
  - 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。
- 使用企业管理的用户组授权功能时，该功能依赖IAM的细粒度授权。如果企业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：用户请求创建云服务器，鉴权结果为IAM中定义的Deny，不能创建云服务器。

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云服务器以及删除云服务器。

IAM项目策略中包含以下action：

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

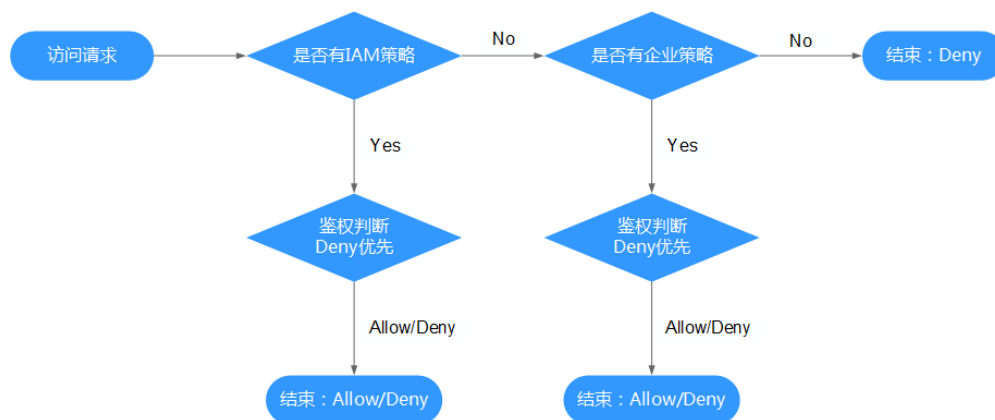
企业项目策略中包含以下action：

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

## 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：

图 12-1 请求鉴权逻辑图



1. 用户发起访问请求。

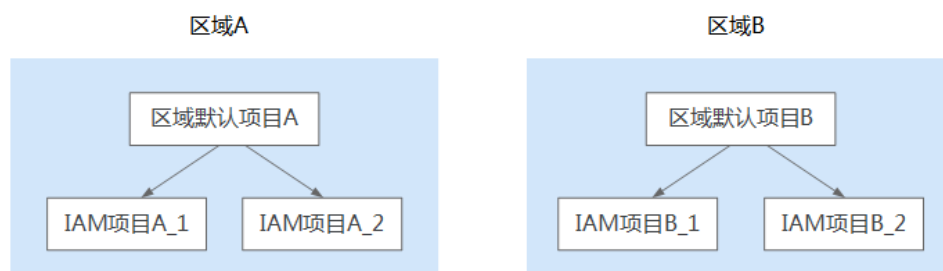
2. 系统在用户被授予的访问策略中，优先寻找基于IAM项目授权的策略，在策略中寻找请求对应的action。
3. 如果找到匹配的Allow或者Deny的action，系统将返回对请求的鉴权决定，Allow或者Deny，鉴权结束。
4. 如果在基于IAM项目的策略中没有找到请求对应的action，系统将寻找基于企业项目授权的策略，在策略中寻找请求对应的action。
5. 如果找到匹配的Allow或者Deny的action，系统将返回对请求的鉴权决定，Allow或者Deny，鉴权结束。
6. 如果用户不具备任何策略，系统将返回鉴权决定Deny，鉴权结束。

## 12.2 IAM 项目和企业项目的区别

### IAM 项目

IAM项目是针对同一个区域内的资源进行分组和隔离，是**物理隔离**。

在IAM项目中的资源不能转移，只能删除后重建。

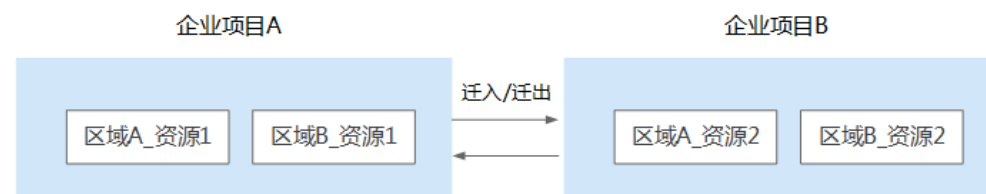


### 企业项目

企业项目针对企业在全部区域内的资源进行分组与管理，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。

如果您开通了企业管理，将不能创建IAM项目。



## 12.3 在什么场景下可以看到所有的企业项目

- 管理员用户登录时，可以查看所有的企业项目信息。
- IAM用户登录时，如果管理员用户有对该IAM用户的全局授权策略，那么IAM用户将能看到所有的企业项目信息。

## 12.4 如何获取企业项目 ID

- 通过调用接口获取。  
各云服务可通过IAM授权，调用企业项目管理的查询企业项目列表接口获取。具体接口信息请参考《企业项目管理服务API参考》。
- 通过在企业项目详情页查询获取。  
操作步骤如下：
  - a. 在控制台页面，鼠标移动至右上方的账号名，单击账号名，在下拉列表中选择“企业管理”。  
系统进入“企业项目管理”页面。
  - b. 单击待查询企业项目的名称，进入该企业项目详情页即可查看企业项目ID。

## 12.5 最多可以创建多少个企业项目？

企业项目数量默认配额是100个。

如果默认配额无法满足您的需求，您可以[申请扩大配额](#)。

## 12.6 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。

资源从一个企业项目迁移到另一个企业项目，不会影响资源本身。例如：资源实例不会重启、网络配置不会变更、资源所有者不会变更等。

但是，如果您有基于企业项目范围的授权策略，则资源所属企业项目发生变更，可能会导致用户对资源访问权限的变更。例如：您给项目A的成员授予企业项目A范围的操作权限，此时成员可以访问企业项目A内的资源。当资源从企业项目A迁移到企业项目B时，由于成员只有企业项目A的权限，则此时成员将不再具有此资源的操作权限。

# 13 修订记录

版本日期	变更说明
2022-11-30	第二次正式发布。 本次变更如下： 新增： <ul style="list-style-type: none"><li>• <a href="#">多项目管理实践案例</a></li><li>• <a href="#">最多可以创建多少个企业项目？</a></li><li>• <a href="#">资源迁入/迁出企业项目会影响资源所在的VPC和网段吗？</a></li></ul>
2022-08-11	第一次正式发布。