



企业项目管理

用户指南

发布日期 2025-03-28

目 录

1 什么是企业项目..... 1

2 应用场景.....2

3 支持的云服务..... 5

4 约束与限制..... 6

5 权限说明..... 7

5.1 企业项目权限说明..... 7

5.2 云服务权限说明.....8

6 如何进入项目管理页面.....9

7 企业项目管理..... 10

7.1 创建企业项目.....10

7.2 修改/启用/停用企业项目..... 11

7.3 为新购云资源选择企业项目..... 12

8 企业项目资源管理..... 14

8.1 资源管理简介.....14

8.2 查看企业项目下的资源..... 14

8.3 为企业项目迁入资源..... 15

8.4 迁出企业项目资源.....16

8.5 查看迁入迁出事件..... 17

9 企业项目人员管理..... 18

9.1 查看企业项目授权记录..... 18

9.2 如何管理企业项目用户组.....18

9.2.1 为企业项目关联用户组并授权.....18

9.2.2 移除企业项目关联的用户组..... 19

10 关于配额..... 20

11 常见问题..... 21

11.1 IAM 和企业管理的区别..... 21

11.2 IAM 项目和企业项目的区别.....23

11.3 在什么场景下可以看到所有的企业项目..... 23

11.4 如何获取企业项目 ID..... 24

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。

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。

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，并开通企业项目功能，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

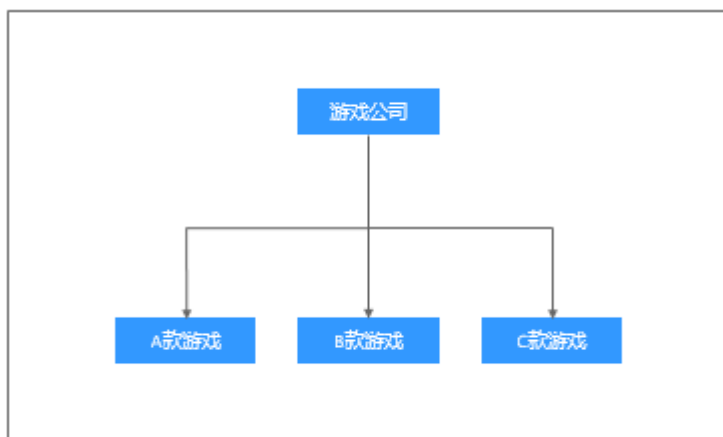
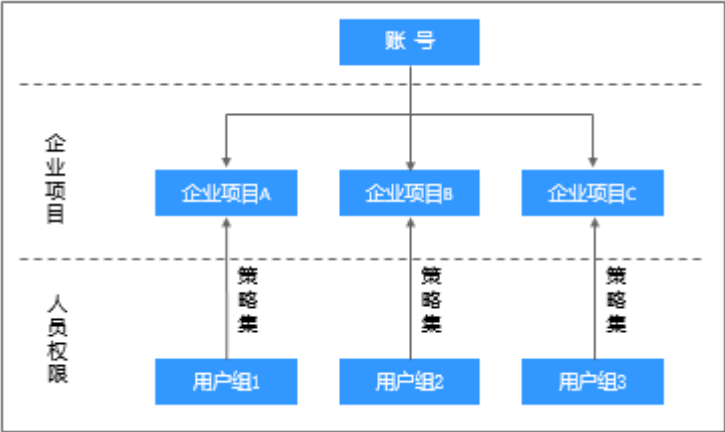


图 2-2 解决方案示意图



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，且子账号之间资源隔离，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账号，开通企业项目功能和企业主账号功能，并将开发环境和生产环境作为子账号1和子账号2，与企业主账号关联，并同时开通企业项目功能，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

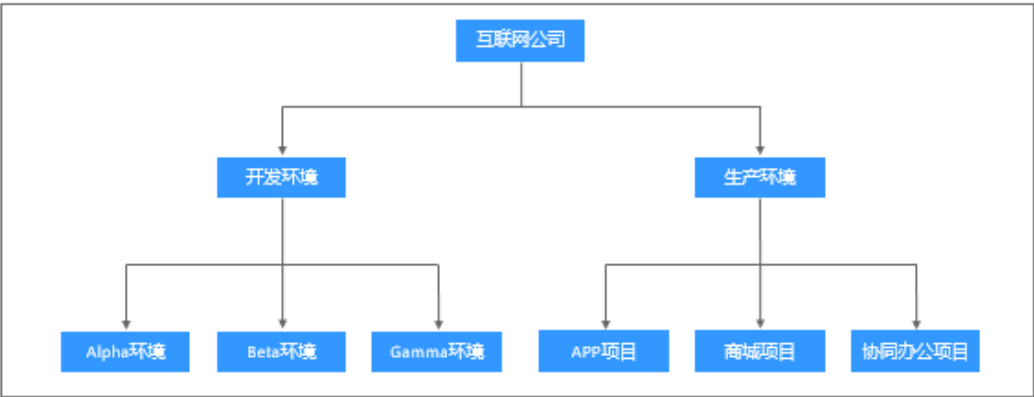
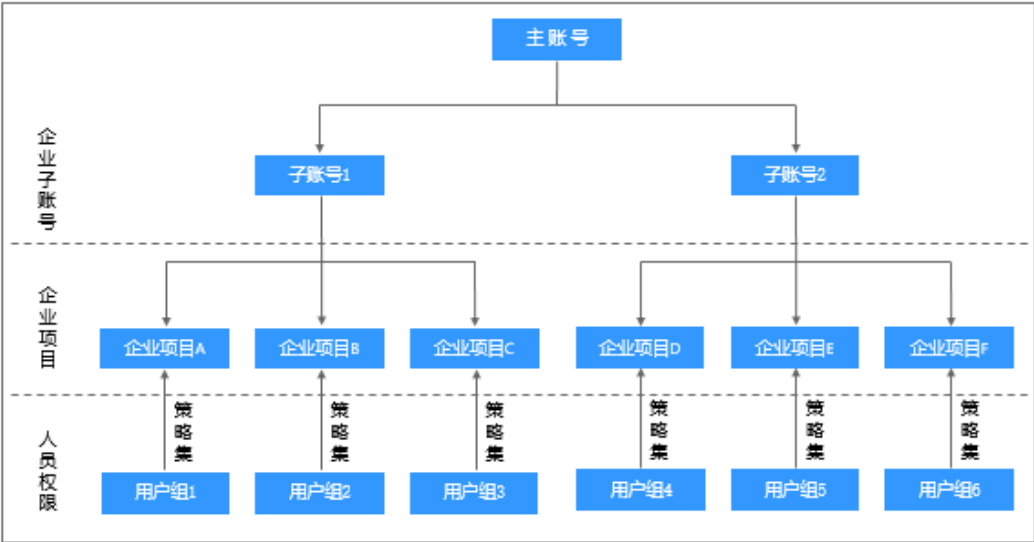


图 2-4 解决方案示意图



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 约束与限制

本文介绍企业项目管理（EPS）在使用过程中的约束和限制。

- 仅企业账号才可申请开通企业项目。
- 每个账号默认可以创建100个企业项目，如需调整企业项目最大配额，您可以提交工单申请扩大配额。企业项目数量的配额最大支持调整为256个。
- 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。
- 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。
- 测试类企业项目不支持停用操作。
- 目前不支持商用生产项目转测试类项目。
- 目前仅支持从商用生产项目到商用生产项目或测试类项目到测试类项目之间的资源迁移。
- 系统默认的企业项目“default”为商用生产项目，因此不支持在测试类项目与默认企业项目“default”之间进行资源迁移。
- 仅企业主账号或拥有Administor权限的IAM用户才可查看企业项目的资源迁入迁出事件。
- 企业项目的名称和描述的字符数限制，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”；描述不超过512个字符。
- 在企业项目管理中进行资源标签管理时，每个资源最多可以添加10个标签。

5 权限说明

5.1 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 5-1 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	- 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。 - 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。	企业资产管理员

服务名称	权限名称	权限说明	适用的典型人员
	EPS ReadOnlyAccess	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。 • 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。 • 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。	企业资产查询人员

表 5-2 常用操作与系统权限的关系

操作	EPS FullAccess	EPS ReadOnlyAccess
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	√	×

5.2 云服务权限说明

在统一身份认证服务为用户或用户组基于企业项目授予相应的云服务权限，实现基于企业项目对云服务权限的管理。

当这些云服务与暂时不支持企业项目管理的云服务存在关联业务时，这部分关联业务需要依赖其他权限才能成功操作。云服务依赖策略的配置方法主要分为以下两种：

- 在统一身份认证服务中为用户组添加云服务系统策略。
- 如果系统策略不满足授权要求，您还可以在统一身份认证服务中创建自定义策略，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。

6 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，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。

----结束

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

登录管理控制台，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。

约束与限制

- 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（default）无法编辑和停用。
- 测试类企业项目不支持停用操作。
- 目前不支持商用生产项目转测试类项目。

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

登录管理控制台，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** 登录管理控制台，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** 在企业项目管理页面，选择状态为已停用的企业项目，单击操作列的“更多”，选择“启用”。
系统弹出启用企业项目的确认页面。
- 步骤3** 单击“确定”，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，不再使用某些企业项目时，可停用该企业项目。

- 步骤1** 登录管理控制台，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** 在企业项目管理页面，选择状态为已启用的企业项目，单击操作列的“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“确定”，企业项目停用成功。
- 结束

7.3 为新购云资源选择企业项目

操作场景

在购买云资源页面，您可以选择已启用的企业项目，新购云资源将按此企业项目进行管理。

有以下两种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 登录管理控制台，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

说明

- “创建资源”仅支持常用的三种云资源入口：弹性云服务器 ECS、云硬盘 EVS、弹性公网IP EIP。
- 企业项目支持的所有云资源信息请参见[支持的云服务](#)。

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 单击管理控制台左上角的，选择区域和项目。

步骤2 选择“计算 > 弹性云服务器”。

步骤3 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4 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5 单击右侧配置栏的“立即申请”。

步骤6 在规格确认页面，您可以查看资源详情并提交订单。

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

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

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。

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 登录管理控制台，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。

单击“搜索”，页面下方列表展示筛选后的所有资源。

说明

当服务选择为“EIP”时，支持查看已绑定实例。已绑定实例目前仅支持查看资源为：云服务器、负载均衡器（目前仅支持增强型）、裸金属服务器、虚拟IP地址。

---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。

约束与限制

- 目前仅支持从商用生产项目到商用生产项目或测试类项目到测试类项目之间的资源迁移。
- 系统默认的企业项目“default”为商用生产项目，因此测试类项目在迁入资源时无法选择默认企业项目“default”下的资源。
- 已停用的企业项目无法迁入资源和添加用户组。

操作步骤

步骤1 登录管理控制台，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 在企业项目管理页面，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。

此处企业项目下拉框中未显示的企业项目为已停用状态或与当前企业项目类型不同。

步骤6 对于包含多种资源类型的服务，可在列表中单击资源类型列的，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）。

约束与限制

- 目前仅支持从商用生产项目到商用生产项目或测试类项目到测试类项目之间的资源迁移。
- 系统默认的企业项目“default”为商用生产项目，因此测试类项目不支持将资源迁出至默认企业项目“default”中。

操作步骤

步骤1 登录管理控制台，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 在企业项目管理页面，选择待迁出资源的企业项目，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，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。

待迁入企业项目下拉框中未显示的企业项目为已停用状态或与当前企业项目类型不同。

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

说明

目前仅支持从商用生产项目到商用生产项目或测试类项目到测试类项目之间的资源迁移。

8.5 查看迁入迁出事件

操作场景

您可以通过查看迁入迁出事件回溯资源迁移记录信息，包括迁移时间、操作用户、操作方式、资源ID、源企业项目与目标企业项目等。

约束与限制

最多显示近7天的事件。

仅企业主账号或拥有Administrator权限的IAM用户才可查看迁入迁出事件。

操作步骤

步骤1 登录管理控制台，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 在项目管理页面，单击企业项目列表上方的“查看迁入迁出事件”。

系统进入“查看迁入迁出事件”页面，列表中显示近7天的资源迁入迁出事件。

----结束

9 企业项目人员管理

9.1 查看企业项目授权记录

操作场景

您可以通过IAM的授权管理页面查看基于企业项目的全部授权记录，方便您统一查看和管理企业项目的授权关系。

操作步骤

- 步骤1** 登录管理控制台，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** 在企业项目管理页面，选择待查看的企业项目，单击操作列的“权限管理”。
 - 步骤3** 系统将跳转至IAM的授权管理页面，单击页面右上方的“企业项目视图”，列表中显示基于企业项目的全部授权记录。
 - 步骤4** “授权主体”列为与企业项目关联的用户或用户组名称，单击授权主体即可跳转至相应用户或用户组详情页。
- 结束

9.2 如何管理企业项目用户组

9.2.1 为企业项目关联用户组并授权

操作场景

将用户组与企业项目关联，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关联用户组并授权。

操作步骤

步骤1 登录管理控制台，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 在企业项目管理页面，单击待查看的企业项目的名称。

步骤3 系统进入企业项目详情页面，在“权限管理”页签中单击“用户组授权”。

系统将跳转至IAM的用户组页面，在“用户组”页签中为企业项目关联用户组并授权。

具体请参见《统一身份认证用户指南》中的“创建用户组并授权”章节。

----结束

9.2.2 移除企业项目关联的用户组

操作场景

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，可将这些用户组与该企业项目的关联关系删除。

可进行单个删除和批量删除。

当用户组与企业项目的关联关系被删除后，该用户组用户将无法管理该企业项目，如需再次使用，需要重新给该用户组关联企业项目。

操作步骤

步骤1 登录管理控制台，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 在企业项目管理页面，单击待查看的企业项目的名称。

步骤3 系统进入企业项目详情页面，在“权限管理”页签中单击“用户组授权”。

步骤4 系统将跳转至IAM的用户组页面，在“用户组”列表单击用户组名称进入用户组详情页面。

步骤5 在“授权记录”页签中单击“企业项目视图”，选择待删除关联关系的企业项目，单击右侧操作列的“删除”。

如需批量删除用户组关联的企业项目，可在列表中勾选多个企业项目，单击列表上方的“删除”按钮。

步骤6 在弹出的确认框中单击“确定”。

用户组关联的企业项目删除完成。

----结束

10 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。

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。

11 常见问题

11.1 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、人员管理、财务管理和应用管理。

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，企业管理还可以管理财务及应用，同时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，注册系统后，无需付费即可使用。
 - 企业管理是资源管理服务，注册系统后，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。
- 申请开通企业管理服务后，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"
}
```

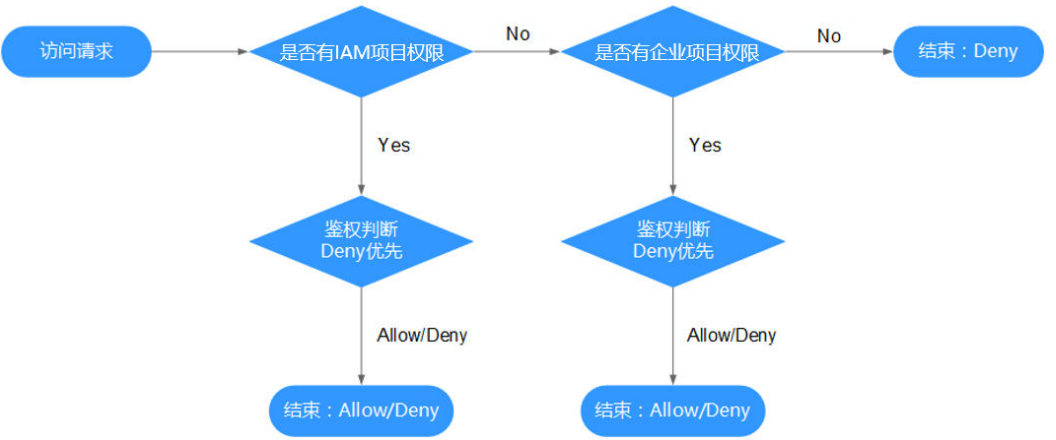
企业项目策略中包含以下action：

```
{
  "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 11-1 请求鉴权逻辑图



1. 用户发起访问请求。

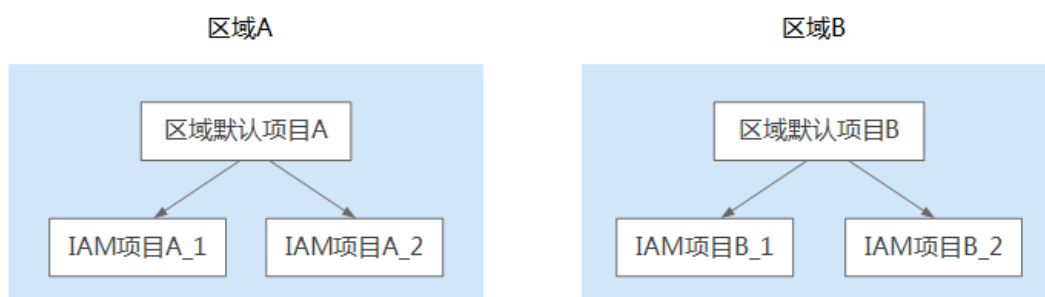
2. 系统在用户被授予的访问策略中，优先寻找基于IAM项目授权的策略，在策略中寻找请求对应的action。
3. 如果找到匹配的Allow或者Deny的action，系统将返回对请求的鉴权决定，Allow或者Deny，鉴权结束。
4. 如果在基于IAM项目的策略中没有找到请求对应的action，系统将继续寻找基于企业项目授权的策略，在策略中寻找请求对应的action。
5. 如果找到匹配的Allow或者Deny的action，系统将返回对请求的鉴权决定，Allow或者Deny，鉴权结束。
6. 如果用户不具备任何策略，系统将返回鉴权决定Deny，鉴权结束。

11.2 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。

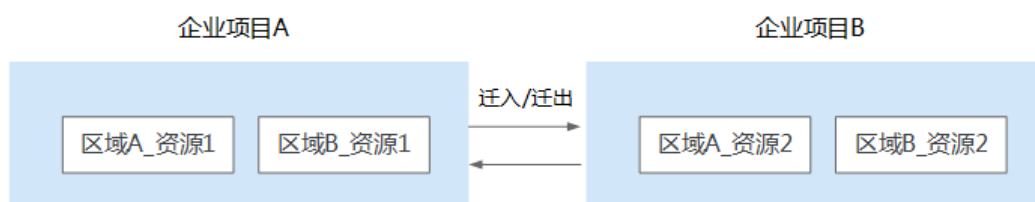


企业项目

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。



11.3 在什么场景下可以看到所有的企业项目

一般情况下，用户仅可以查看到其拥有权限的企业项目，其中如下场景的用户可以查看所有企业项目：

- 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，如果该IAM用户具有管理员用户授予的全局授权策略，那么该IAM用户将能看到所有的企业项目信息。

11.4 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. 登录管理控制台，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。
 - b. 在企业项目管理页面，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。