组织

产品介绍

文档版本 01

发布日期 2024-03-14

华为技术有限公司

商标声明


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

1 什么是组织云服务

简介

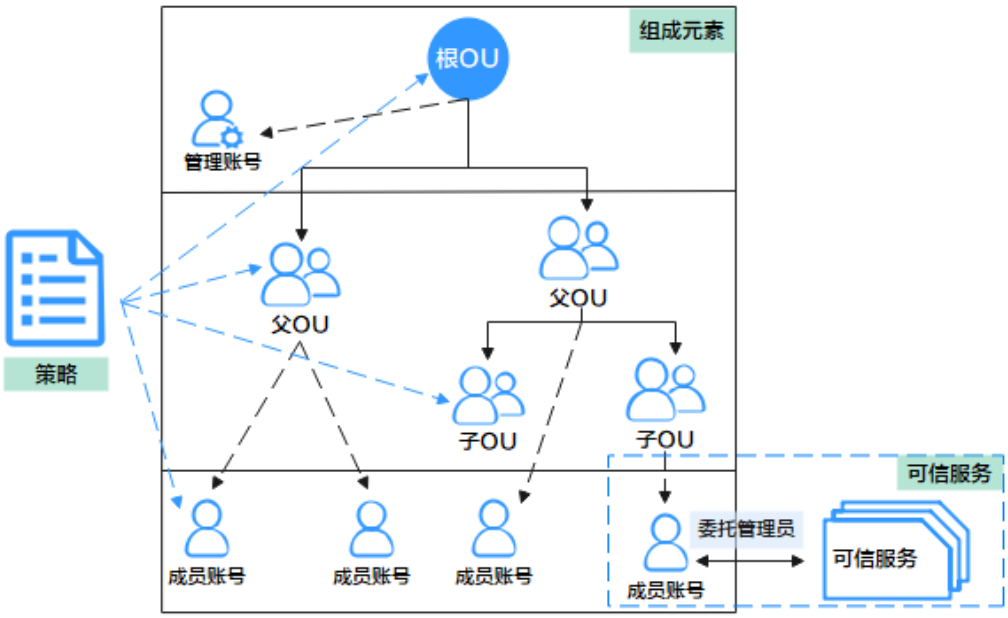
组织（以下简称Organizations）云服务为企业用户提供多账号关系的管理能力。Organizations支持用户将多个华为云账号整合到创建的组织中，并可以集中管理组织下的所有账号。用户可以在组织中统一治理策略，帮助用户更好地满足业务的安全性和合规性需求。

Organizations服务为**免费服务**，不收取任何费用。用户只需要对各账号中使用的其他云服务或者资源实例付费。

产品架构

Organizations服务的产品架构可以分为：组织的组成元素、组织策略、可信服务。

图 1-1 Organizations 服务的产品架构



组织的组成元素

- **组织**

  为管理多账号关系而创建的实体。一个组织由**管理账号**、**成员账号**、**根组织单元**、**组织单元**（Organizational Unit，以下简称OU）四个部分组成。一个组织有且仅有一个管理账号，若干个成员账号，以及由一个根组织单元和多层级组织单元组成的树状结构。成员账号可以关联在根组织单元或任一层级的组织单元。

- **根组织单元**

  当您开通Organizations云服务并创建组织后，系统会为您自动生成根组织单元。根组织单元位于整个组织树的顶端，组织由根组织单元向下关联组织单元和账号。

- **组织单元**

  组织单元是可以理解为成员账号的容器或分组单元，通常可以映射为企业的部门、子公司或者项目族等。组织单元可以嵌套，一个组织单元只能有一个父组织单元，一个组织单元下可以关联多个子组织单元或者成员账号。

- **管理账号**

  管理账号是标准的华为云账号。企业管理员在管理账号中，使用Organizations服务创建组织，并管理组织中其他账号。在管理账号中还可以管理整个组织的相关策略和可信服务。

- **成员账号**

  当启用Organizations服务后，通过Organizations服务邀请加入或直接创建的账号称为成员账号。成员账号是标准的华为账号或华为云账号，可以关联在根组织单元或者任一个组织单元下。

- **邀请**

  邀请其他账号加入组织的过程。邀请只能由管理账号发出，被邀请账号只有接受邀请后，才会加入组织。通过邀请加入组织的账号，不会改变该账号的费用结算关系。

组织策略

- **服务控制策略**

  服务控制策略 (Service Control Policy，以下简称SCP) 是一种基于组织的访问控制策略。组织管理账号可以使用SCP指定组织中成员账号的权限边界，限制账号内用户的操作。服务控制策略可以关联到组织、组织单元和成员账号。当服务控制策略关联到组织或组织单元时，该组织或组织单元下所有账号受到该策略影响。详情可参考**服务控制策略介绍**。

- **标签策略**

  标签策略是策略的一种类型，可帮助您在组织账号中对资源添加的标签进行标准化管理。标签策略可以关联到组织、组织单元和成员账号。标签策略对未添加标签的资源或未在标签策略中定义的标签不会生效。

可信服务

- **可信服务**

  可信服务是指可与Organizations服务集成，提供组织级管理能力的华为云服务。启用华为云服务为可信服务后，可信服务会在成员账号中创建一个服务关联委托，该委托允许可信服务在成员账号中拥有执行可信服务文档中所述任务的权限，相当于云服务能力在多账号组织场景下的拓展。目前支持的可信服务请参见：**已对接组织的可信服务列表**。

- **委托管理员账号**

  委托管理员账号是一个组织中有特殊权限的成员账号。管理账号可指定某个成员账号成为某个可信服务的委托管理员账号。成为委托管理员账号后，该账号下的用户可以使用对应可信服务的组织级管理能力。

如何访问 Organizations 云服务

通过管理控制台、基于HTTPS请求的API（Application Programming Interface）两种方式访问Organizations云服务。

- 管理控制台方式

  管理控制台是网页形式的，您可以使用直观的界面进行相应的操作。登录**管理控制台**，从主页选择“管理与监管 > 组织 Organizations”。

- API方式

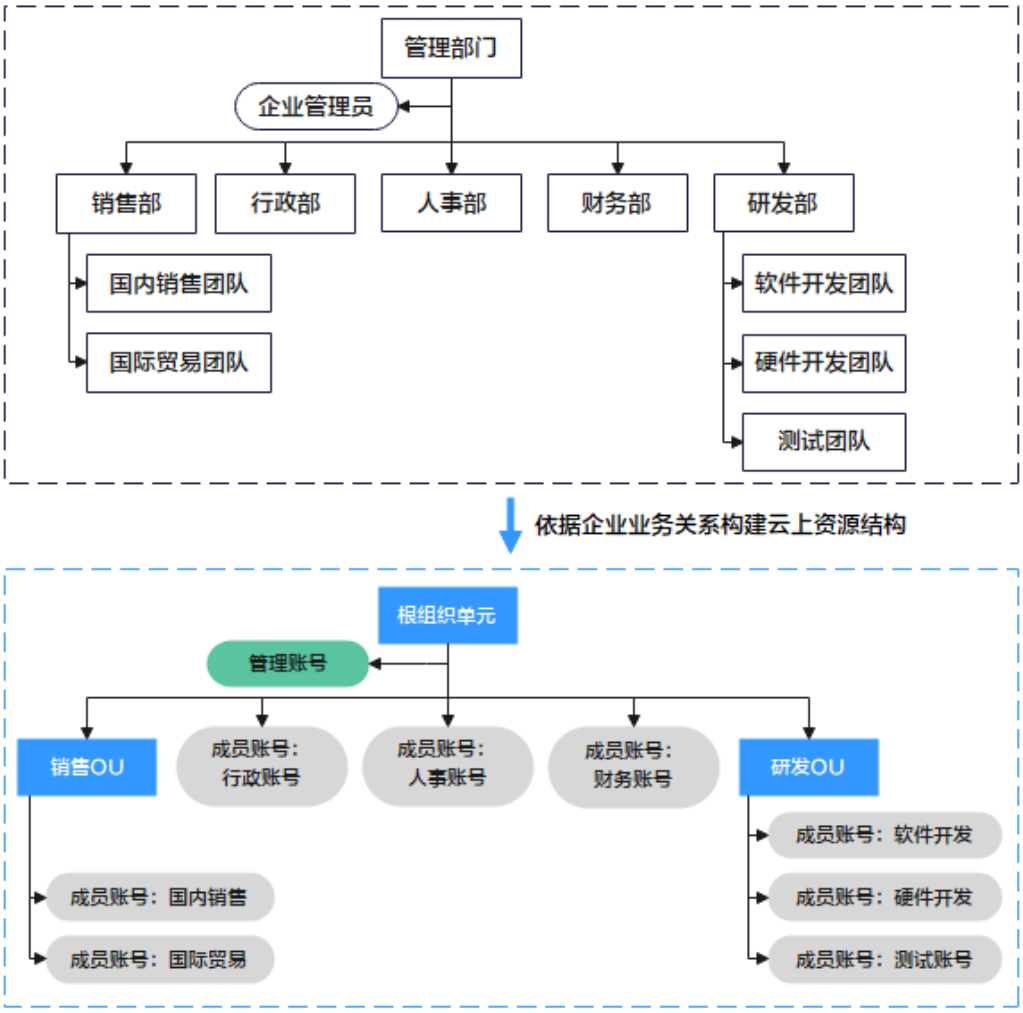
  如果用户需要将云服务平台上的组织服务集成到第三方系统，用于二次开发，请使用API方式访问Organizations云服务。具体操作请参见**Organizations云服务API参考**。

2 应用场景

依据企业业务关系构建云上资源结构

企业拥有多个分公司、部门或者不同的业务应用，通过Organizations服务，企业可以在云上构建符合自身管理和工作方式的多层级资源结构。

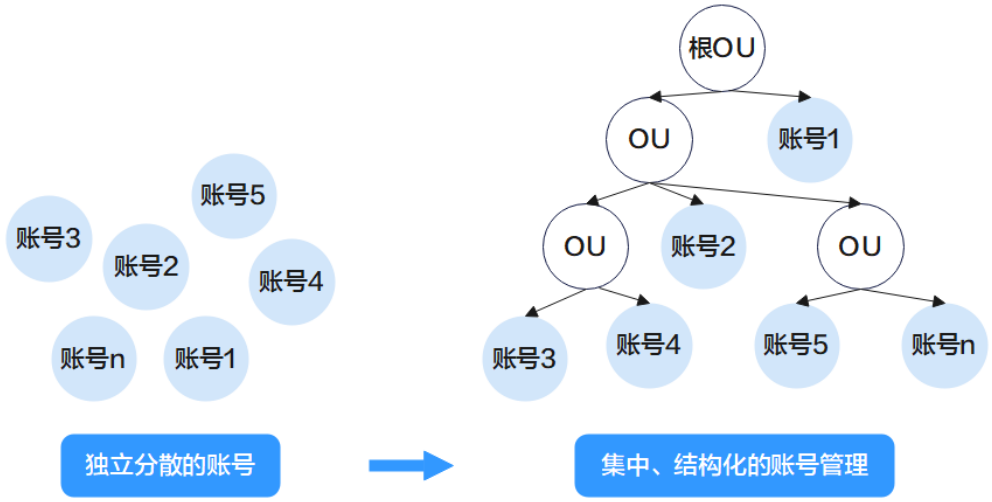
图 2-1 依据企业业务关系构建云上资源结构



集中管理企业多个云账号

企业拥有多个华为云账号，企业希望能够集中管理多个账号及账号中的资源。Organizations服务能够将多个分散的华为云账号，纳入到Organizations构建的组织中，实现对账号和资源的集中管理。

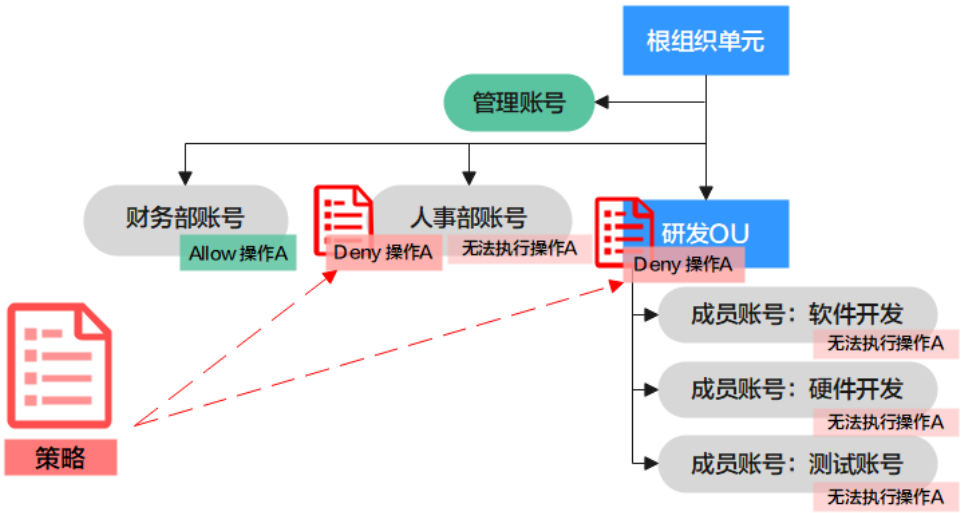
图 2-2 集中管理企业多个云账号



预防各业务的违规行为

企业可以根据内外部要求，为不同的部门、业务环境（生产、测试或开发）等设置云上的行为边界，Organizations服务可以主动拦截不符合要求的行为，预防违规行为发生。

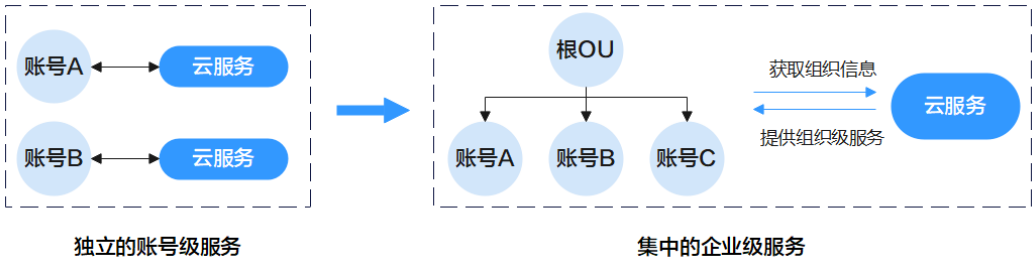
图 2-3 使用策略管控各账号行为



提供多种企业级的治理能力

配置审计Config等多个云服务与Organizations服务集成，为客户提供在同一资源架构下集中式的资源审计、操作审计、多业务共享资源等企业级能力。

图 2-4 提供企业级治理能力



3 功能概览

Organizations服务的主要功能：

- 集中管理企业多账号：企业可以将多个账号邀请加入组织，或者直接创建账号，并根据企业的管理或工作方式将账号进行分层分组。
- 集中控制每个账号可执行的操作：管理员通过使用服务控制策略，为组织或者组织单元设置权限边界，阻止组织内的成员账号对相应服务的控制台或API的访问。
- 与其他华为云服务集成：Organizations服务通过和其他华为云服务的集成（可信服务），使用户可以在其他服务上执行组织级别的相关能力。可信服务及其相关能力的具体详情，请参考**已对接组织的可信服务**。

表 3-1 Organizations 云服务功能概览

功能	功能描述	参考链接
组织管理	您可以创建组织，并邀请其他账号加入组织。查看组织、根、组织单元 (OU) 和账号的详细信息。当您不再需要组织时可关闭组织。	**组织管理**
组织单元管理	管理账号可以创建OU、修改OU、查看OU详细信息、删除OU。	**组织单元管理**
账号管理	管理账号可邀请账号加入组织、创建账号、关闭账号、更改成员账号所属组织单元、查看成员账号详细信息、移除成员账号。	**账号管理**
服务控制策略	管理账号可创建SCP、修改和删除SCP，为OU和账号绑定和解绑SCP。	**服务控制策略**
标签策略	管理账号可创建标签策略、修改和删除标签策略，为OU和账号绑定和解绑标签策略。	**标签策略**
可信服务	管理账号可以在组织中，启用或禁用某个云服务为可信服务，并设置成员账号为可信服务委托管理员。	**可信服务**

功能	功能描述	参考链接
标签管理	标签用于标识云资源，可通过标签实现对云资源的分类和搜索。支持添加标签的组织资源包括：组织的根、组织单元（OU）、账号、服务控制策略（SCP）	**标签管理**

4 权限管理

如果您要为管理账号中不同的用户，根据职能设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并授权控制他们对华为云资源的访问范围。例如您的员工中有负责管理账号的人员，您希望他们拥有邀请账号加入组织的权限，但是不希望他们拥有策略管理权限，那么您可以使用IAM为账号管理员创建用户，通过授予仅使能邀请账号，但是不允许进行策略的创建和修改，控制他们对组织的管理范围。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用Organizations服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您华为云账号中的资源进行付费。

关于IAM的详细介绍，请参见**IAM产品介绍**。

Organizations 服务权限

默认情况下，管理员创建的IAM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。

Organizations服务为全局服务。授权时，“授权范围”需要选择“全局服务资源”。

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。由于华为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。角色并不能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。多数细粒度策略以API接口为粒度进行权限拆分，权限的最小粒度为API授权项（action），Organizations服务支持的API授权项请参见**权限及授权项说明**。

如**表1**所示，包括了Organizations服务的所有系统权限。

表 4-1 Organizations 服务系统权限

系统角色/策略名称	描述	类别	依赖关系
Organizations FullAccess	拥有该权限的用户可以执行Organizations服务支持的所有功能，包括创建、更改、删除、查询等操作。	系统策略	无
Organizations ReadOnlyAccess	拥有该权限的用户可以对组织信息执行只读访问。它不允许用户进行任何更改。	系统策略	无

表2列出了Organizations常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 4-2 组织常用操作与系统权限的关系

操作	Organizations FullAccess	Organizations ReadOnlyAccess
创建组织	√	x
查看组织	√	√
关闭组织	√	x
创建OU	√	x
修改OU	√	x
查看OU详细信息	√	√
删除OU	√	x
邀请账号加入组织	√	x
创建账号	√	x
关闭账号	√	x
更新账号所属OU	√	x
查看账号详细信息	√	√
移除成员账号	√	x
启用服务控制策略	√	x
禁用服务控制策略	√	x
创建SCP	√	x
修改SCP	√	x
查看SCP	√	√

操作	Organizations FullAccess	Organizations ReadOnlyAccess
删除SCP	√	x
绑定SCP	√	x
解绑SCP	√	x
启用可信服务	√	x
禁用可信服务	√	x
设置委托管理员	√	x
添加标签	√	x
修改标签	√	x
查看标签	√	√
删除标签	√	x

相关链接

- IAM产品介绍
- 创建用户并授权使用Organizations服务
- 权限及授权项说明

Organizations FullAccess 策略内容

```
{
   "Version": "1.0",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": "organizations:*",
         "Resource": "*"
      },
      {
         "Effect": "Allow",
         "Action": "iam:agencies:createServiceLinkedAgency",
         "Resource": ["*"],
         "Condition": {
            "StringEquals": {
               "iam:ServicePrincipal": "service.organizations"
            }
         }
      }
   ]
}
```

Organizations ReadOnlyAccess 策略内容

```
{
   "Version": "1.0",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
```

```
            "organizations:organizations:get",
            "organizations:roots:list",
            "organizations:ous:list",
            "organizations:ous:get",
            "organizations:accounts:list",
            "organizations:accounts:get",
            "organizations:accounts:listAncestors",
            "organizations:receivedHandshakes:list",
            "organizations:handshakes:list",
            "organizations:trustedServices:list",
            "organizations:delegatedServices:list",
            "organizations:delegatedAdministrators:list",
            "organizations:policies:list",
            "organizations:policies:get",
            "organizations:attachedEntities:list",
            "organizations:tags:list",
            "organizations:entities:list"
        ],
        "Resource": "*"
    }
  ]
}
```


5 约束与限制

使用约束

- 使用Organizations云服务之前，需要先**开启企业中心**服务。
- 只能使用企业中心的主账号创建组织。
- 中国站的组织无法邀请国际站账号，国际站的组织也无法邀请中国站账号。

功能规格

表 5-1 Organizations 服务的约束与限制

规格项	默认配额	申请更多配额
一个账号允许创建的组织数量	1个 **说明** 成员账号无法创建组织	无
根组织单元数量	1个	无
组织中组织单元的数量	1000个 **说明** 不包含根组织单元	无
组织单元可嵌套层数	5个 **说明** 不包含根组织单元和成员账号	无
组织中成员账号数量	10个	工单申请
组织管理员最多可以同时创建成员账号的数量	5个	无
组织管理员在30天内最多支持关闭的成员账号数量	10%、最多200个	无
组织管理员最多可以同时关闭成员账号的数量	3个	无

规格项	默认配额	申请更多配额
24小时内可以执行的最大邀请尝试次数	20次	无
邀请有效期	14天	无
邀请记录在列表中保留的时间	1年	无
组织内可创建服务控制策略的数量	1000个	无
服务控制策略的长度	5120字符	无
组织内可创建标签策略的数量	1000个	无
标签策略的长度	10000字符	无
根、组织单元、账号、服务控制策略、标签策略上可附加的标签数量	20个	无
绑定在根、组织单元、账号上的服务控制策略的最大数量	5个	无
绑定在根、组织单元、账号上的标签策略的最大数量	10个	无

6 基本概念

本章为您介绍使用组织Organization服务时常用的基本概念：组织、根组织单元、组织单元、服务控制策略、URN、Principal。

组织

为管理多账号关系而创建的实体。一个组织由**管理账号**、**成员账号**、**根组织单元**、**组织单元**（Organizational Unit，以下简称OU）四个部分组成。一个组织有且仅有一个管理账号，若干个成员账号，以及由一个根组织单元和多层级组织单元组成的树状结构。成员账号可以关联在根组织单元或任一层级的组织单元。

根组织单元

当您开通Organizations云服务并创建组织后，系统会为您自动生成根组织单元。根组织单元位于整个组织树的顶端，组织由根组织单元向下关联组织单元和账号。

组织单元

组织单元是可以理解为成员账号的容器或分组单元，通常可以映射为企业的部门、子公司或者项目族等。组织单元可以嵌套，一个组织单元只能有一个父组织单元，一个组织单元下可以关联多个子组织单元或者成员账号。

服务控制策略

服务控制策略 (Service Control Policy，SCP) 是一种基于组织的访问控制策略。组织管理账号可以使用SCP指定组织中成员账号的权限边界，限制账号内用户的操作。服务策略可以关联到组织、组织单元和成员账号。当服务策略关联到组织或组织单元时，该组织或组织单元下所有账号受到该策略影响。详情可参考**服务控制策略介绍**。

标签策略

标签策略是策略的一种类型，可帮助您在组织账号中对资源添加的标签进行标准化管理。标签策略对未添加标签的资源或未在标签策略中定义的标签不会生效。详情可参考**标签策略**。

URN

统一资源标识（Uniform Resource Name，URN），用于唯一标识云服务资源。

格式为：<service-name>:<region>:<account-id>:<type-name>:<resource-path>

- service-name：云服务简称，小写，例如ecs。填入的云服务简称必须存在，无法使用通配。
- region：资源所在的区域，例如cn-north-1。如果是全局服务的资源，填空或者用*填充。
- account-id：账号ID。“system”表示系统公共资源，例如系统策略。
- type-name：资源类型，需要使用小驼峰命名。
- resource-path：资源路径，格式由云服务自定义。

7 修订记录

时间	修订记录
2024-03-14	第三次正式发布。 本次变更说明如下： ● 组织（Organizations）云服务正式商用。 ● 更新“约束与限制”章节。
2023-03-30	第二次正式发布。 本次变更说明如下： 上线标签策略特性相关内容。
2022-09-30	第一次正式发布。