组织

用户指南

文档版本 01

发布日期 2025-12-10

华为云计算技术有限公司

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云计算技术有限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，华为云计算技术有限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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 权限管理

1.1 创建 IAM 用户并授权管理组织

本章节介绍**管理账号**如何创建用户并给用户授予组织的管理权限。

如果您需要对您所拥有的Organizations云服务进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 将管理账号的组织管理权限进行拆分，根据用户职能给用户分配不同的访问和管理权限，以达到用户之间的权限隔离。例如管理账号有两个IAM用户，一个IAM用户可以创建和删除组织单元，一个IAM用户只能查看组织单元。
- 给管理账号中不同职能部门的员工创建IAM用户，让员工拥有唯一和独立安全凭证访问华为云，并使用Organizations云服务资源，提高账号安全性。
- 将Organizations云服务资源委托给更专业、高效的其他华为云账号或者云服务，这些华为云账号或者云服务可以根据权限进行代运维。

如果华为账号或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，您可以跳过本章节，不影响您使用Organizations云服务的其它功能。

本章节为您介绍创建IAM用户并对IAM用户授权的方法，操作流程如**图1**所示。

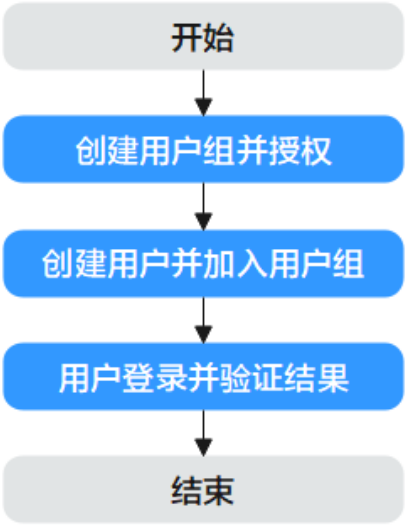
前提条件

给用户组授权之前，请您了解用户组可以添加的Organizations云服务权限，并结合实际需求进行选择，Organizations云服务支持的系统权限，请参见：**权限管理**。

若您需要对除Organizations云服务之外的其它服务授权，IAM支持服务的所有权限请参见**系统权限**。

示例流程

图 1-1 给用户授予 Organizations 权限流程



1. **创建用户组并授权**

   在IAM控制台创建用户组，授予Organizations云服务只读权限“Organizations ReadOnlyAccess”。

2. **创建用户并加入用户组**

   在IAM控制台创建用户，并将其加入**1**中创建的用户组。

3. **用户登录**并验证权限

   使用新创建的用户登录组织管理控制台，能正常进入组织服务并可查看组织的相关信息，然后尝试添加组织单元报错，报错信息提示“权限不足，请联系管理员处理”，表示“Organizations ReadOnlyAccess”已生效，您只有组织的查看权限。

1.2 自定义策略

如果系统预置的Organizations云服务权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考**权限及授权项说明**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，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。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的Organizations云服务自定义策略样例。

Organizations 自定义策略样例

- 示例1：授权IAM用户邀请账号加入组织、从组织中移除成员账号。

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:accounts:invite",
                "organizations:accounts:remove"
            ]
        }
    ]
}
```

- 示例2：拒绝IAM用户删除OU、移除成员账号。

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。如果没有主动授权某一操作，则系统默认**Deny**。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循**Deny优先原则**。

  如果您给用户授予OrganizationsFullAccess的系统策略，但不希望用户拥有OrganizationsFullAccess中定义的删除OU、移除成员账号的权限，您可以创建一条拒绝删除OU、成员账号的自定义策略，然后同时将OrganizationsFullAccess和拒绝策略授予用户，根据Deny优先原则，则用户可以对组织执行除了删除OU、移除成员账号外的所有操作。拒绝策略示例如下：

  ```
  {
      "Version": "5.0",
      "Statement": [
          {
              "Effect": "Deny",
              "Action": [
                  "organizations:ous:delete",
                  "organizations:accounts:remove"
              ]
          }
      ]
  }
  ```


2 组织管理

2.1 组织概述

什么是组织

组织是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OU、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OU和多层级OU组成的树状结构。成员账号可以关联在根OU或任一层级的OU。有关Organizations云服务的基本概念参见：**基本概念**。

本章节将为您呈现以下内容：

- **创建组织**。使用您当前的账号作为管理账号创建组织，并邀请其他账号加入组织。
- **查看组织信息**。查看根、组织、OU和账号的详细信息。
- **关闭组织**。当您不再需要组织时关闭它。

2.2 创建组织

本节将介绍使用华为云账号作为管理账号来创建组织。创建组织之后，您可以通过**邀请现有账号**或**创建账号**的方式向您的组织添加账号，可以通过**创建OU**来为您的组织添加OU实现账号的结构化管理。

前提条件

当前账号没有加入组织。已经加入组织的账号，不能创建组织，请退出已加入的组织后再进行创建组织操作，退出组织操作步骤请参见**成员账号退出组织**。

当前账号需开通企业中心并成为企业主账号，详情请参见：**开通企业中心功能**。

操作步骤

您可通过控制台和**创建组织API接口**来创建组织。此处介绍如何通过控制台创建组织：

步骤1 登录华为云，进入**组织管理控制台**。

步骤2 开通Organizations云服务。进入开通页，单击“立即开通”。

图 2-1 开通 Organizations 云服务

开通Organizations云服务后，系统会自动创建组织和根组织单元，并将开通服务的账号设置为管理账号。

说明

组织开启后，管理账号一旦生成，无法转移给任何其他华为云账号/华为账号。

----结束

现在，您可以**邀请现有账号**加入组织或在组织中**创建账号**，还可以为组织**创建OU**实现账号的结构化管理。

2.3 查看组织详细信息

管理账号可查看组织所有信息，成员账号仅能查看组织ID，管理账号名称，管理账号ID。

管理账号查看组织信息

以组织管理员或管理账号身份登录**组织管理控制台**，进入控制面板页，即可查看组织ID、组织的URN、管理账号名称及管理账号ID等信息。

图 2-2 管理账号查看组织信息

管理账号查看根信息

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 单击选中组织的根，组织结构树右侧即可展示根的详细信息，包括根的ID、创建时间、URN以及根绑定的策略、标签。

----结束

管理账号查看 OU 信息

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 单击选中要查看的组织单元，组织结构树右侧即可展示选中组织单元的详细信息，包括OU名称、ID、URN和创建时间，以及绑定的策略和标签。

----结束

管理账号查看账号信息

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 单击选中要查看的账号，组织结构树右侧即可展示选中账号的详细信息，包括账号名称、ID、URN、加入组织的时间和归属组织单元，以及账号绑定的策略、标签和委托服务。

----结束

成员账号查看组织信息

以成员账号的身份登录**组织管理控制台**，进入控制面板页，即可查看组织ID、URN、管理账号名称和管理账号ID。

2.4 删除组织

前提条件

当您不需要使用组织功能时，可删除组织。

说明

只有删除组织里所有的成员账号、组织单元和策略后，才可以删除组织。

删除组织的影响

- **对管理账号的影响**
  - 管理账号将成为独立账号。您可以继续将此账号作为独立账号使用，也可以使用它创建不同的组织，它也可以作为成员账号接受其他组织的邀请。
  - 组织的管理账号从来不受服务控制策略（SCP）的影响，所以组织删除后，管理账号及管理账号的IAM用户权限没有任何更改。
- **对成员账号的影响**
  - 成员账号将成为独立账号。您可以继续将它作为独立账号使用，也可以使用它创建不同的组织，它也可以作为成员账号接受其他组织的邀请。
  - 删除组织后，组织的成员账号将不再受到服务控制策略（SCP）的影响，成员账号及成员账号的IAM用户权限可能会发生改变。

- **对策略的影响**
  - 如果您删除组织，则无法恢复它。如果您在组织内创建了服务控制策略，则也将删除这些策略，并且将不能恢复。

操作步骤

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**，进入控制面板页面。

步骤2 在删除组织栏目下，单击“删除组织”，在弹窗中单击“确定”，完成删除组织。

图 2-3 删除组织

----结束

3 OU 管理

3.1 OU 概述

什么是 OU

组织单元OU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、子公司或者项目组等。OU可以嵌套，一个OU只能有一个父OU，一个OU下可以关联多个子OU或者成员账号。

本章节将为您介绍如下内容：

- **创建OU**
- **修改OU**
- **查看OU详细信息**
- **删除OU**

3.2 创建 OU

您可以在组织的根下创建OU。OU最深可嵌套至5层。创建OU请执行以下步骤。

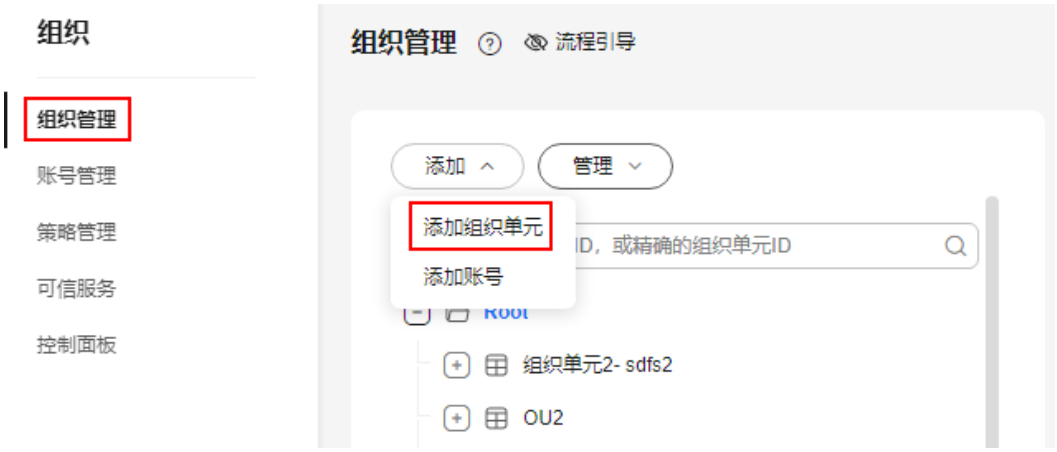
步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 在组织结构树中选中父OU的名称（而不是展开框）。如您是首次创建OU，则需选中根OU的名称（即Root）。

OU最深可嵌套5层，一个OU只能有一个父OU，一个OU下可以关联多个子OU。父OU即为上一层的OU，创建OU时请确保选中正确的父OU。

步骤3 单击组织结构树上方的“添加”，单击“添加组织单元”。

图 3-1 添加组织单元



步骤4 在弹窗中填写组织单元名称。

步骤5 （可选）为组织单元添加标签。

标签以键值对的形式表示，用于标识组织单元，便于对组织单元进行分类和搜索。一个组织单元最多添加20个标签。

标签的设置说明如表3-1所示。

表 3-1 标签说明

参数	说明	举例
键	输入标签的键，同一个组织单元标签的键不能重复。键可以自定义，也可以选择预先在标签管理服务（TMS）创建好的标签的键。 键命名规则如下： • 不能为空。 • 长度为1~128个字符。 • 由英文字母、数字、下划线、中划线、UNICODE字符（\u4E00-\u9FFF）组成。	Key_0001
值	输入标签的值，标签的值可以重复，并且可以为空。 标签值的命名规则如下： • 可以为空。 • 长度为1~225个字符。 • 由英文字母、数字、下划线、点、中划线、UNICODE字符（\u4E00-\u9FFF）组成。	Value_0001

步骤6 然后单击“确定”，完成OU创建。

----结束

3.3 修改 OU

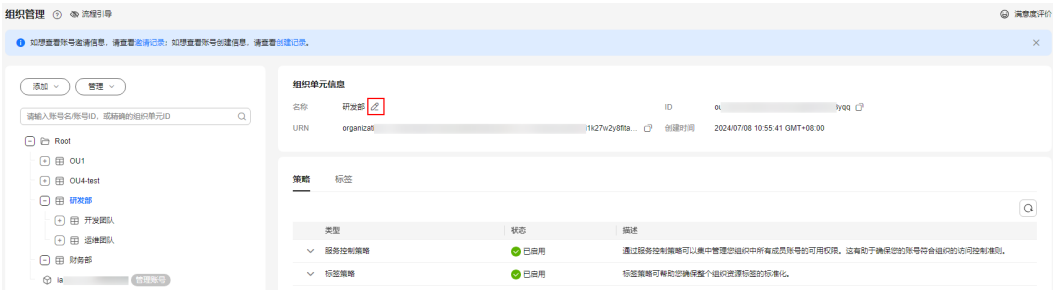
OU创建后，您可以随时修改OU的名称、标签和策略，其中修改标签和策略的详细步骤请参见：**标签管理**和**绑定和解绑SCP**。

操作步骤

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要修改的OU，在右侧的组织单元信息页，单击组织单元名称后方的 。

图 3-2 修改 OU 名称



步骤3 在编辑框中修改OU名称，然后单击 保存，完成OU重命名。

----结束

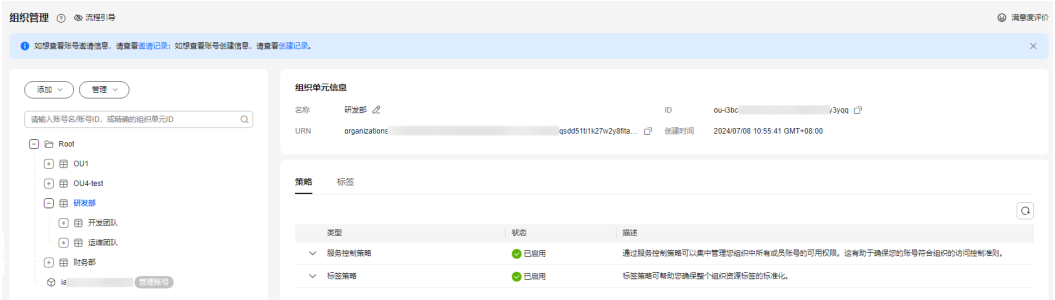
3.4 查看 OU 详细信息

OU创建后，您可以随时查看OU的详细信息，具体请参见如下步骤。

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 单击选中要查看的OU，在树状组织结构图右侧即可查看组织单元详细信息。包括组织单元的名称、ID、URN、创建时间和绑定的策略、标签。

图 3-3 查看组织单元详细信息



----结束

3.5 删除 OU

当您不再需要某个OU时，可以删除OU。

说明

只能删除资源为空的OU，被删除的OU中不能嵌套子OU，不能包含账号。

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要删除的OU，单击组织结构树上方的“管理”。

步骤3 单击“删除组织单元”，在弹窗中单击“确定”，完成OU删除。

图 3-4 删除组织单元

----结束

4 账号管理

4.1 账号概述

组织中的账号

账号中包含了您的华为云资源，账号是构成组织的最小单位。组织中的账号分为管理账号和成员账号。

表 4-1 账号分类

账号分类	功能	配额
管理账号	管理账号是创建组织的账号，使用Organizations服务创建组织，并管理组织中的组织单元（Organizational Unit，以下简称OU）、账号和整个组织的相关策略。	1（一个组织只能有一个管理账号）
成员账号	除管理账号外，组织中的剩余账号都为成员账号。一个账号一次只能是一个组织的成员，成员账号一般用于承载企业具体的某个应用或者项目的资源。	9

加入组织的影响

如果您**邀请现有账号**或**创建新账号**加入组织后，Organizations将自动对新的成员账号进行如下更改：

- Organizations会在成员账号内创建服务关联委托，该委托是云服务委托，委托权限为“OrganizationsServiceLinkedAgencyPolicy”系统权限，授权范围为所有资源。
- 新加入组织的成员账号权限将会受到服务控制策略和标签策略的影响。附加到根或包含新的成员账号的OU上的服务控制策略和标签策略，将应用到新的成员账号和成员账号名下的所有IAM用户中。

- 管理账号开启可信服务时，支持成员账号内部创建对应可信服务的服务关联委托。

本章将为您介绍如下内容，以帮助您管理组织中的账号：

- **邀请账号加入组织**，包括管理账号创建邀请、管理您已发出的邀请，以及成员账号接受或拒绝邀请。
- **创建成员账号**，管理账号可在组织中直接创建新账号。
- **关闭成员账号**，管理账号可在组织中关闭不再需要账号，只有创建的账号才可以关闭，无法关闭邀请的账号。
- **移动成员账号**，将账号从一个OU移动到另外一个OU。
- **查看账号详细信息**，包括账号名称、ID、加入时间、归属组织单元、绑定的策略、标签和委托服务。
- **移除成员账号**，管理账号从组织中移除成员账号。
- **查看账号邀请/创建记录**，组织的管理账号可在账号管理页查看账号列表、邀请记录、创建记录及其相关信息，还可以进行邀请、创建、关闭、移动、移除账号以及取消邀请等操作。

4.2 邀请账号加入组织

组织的管理账号可邀请华为账号或华为云账号加入组织，当管理账号邀请账号时，Organizations将向账号所有者发送邀请，该所有者确定接受还是拒绝邀请。您可以使用Organizations控制台启动和管理您发送到其他账号的邀请。

说明

邀请其他成员账号加入组织，要求成员账号需要完成企业或个人实名认证，详情参见：**实名认证**。

邀请加入组织的成员账号，原财务关系不会调整，保留原有企业主子账号之间的财务模式。

本章节包含如下内容：

- **向账号发送邀请**
- **管理组织的待处理邀请**
- **接受或拒绝来自组织的邀请**

向账号发送邀请

您可通过以下步骤，邀请其他账号加入组织，成为组织的成员账号。注意，邀请进入组织的成员账号会默认放置到根OU中，更换所属OU请参见**移动成员账号**。

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 单击组织结构树上方的“添加”，单击“添加账号”。

图 4-1 添加账号

步骤3 在弹窗中，选择“邀请现有账号”，输入邀请账号的账号名或账号ID。

如何获取账号名和账号ID请参见：**获取账号名和ID**。

图 4-2 邀请现有账号

步骤4 （可选）为账号添加标签。

标签以键值对的形式表示，用于标识账号，便于对账号进行分类和搜索。一个账号最多添加20个标签。

标签的设置说明如**表4-2**所示。

表 4-2 标签说明

参数	说明	举例
键	输入标签的键，同一个账号标签的键不能重复。键可以自定义，也可以选择预先在标签管理服务（TMS）创建好的标签的键。 键命名规则如下： • 不能为空。 • 长度为1~128个字符。 • 由英文字母、数字、下划线、中划线、UNICODE字符（\u4E00-\u9FFF）组成。	Key_0001
值	输入标签的值，标签的值可以重复，并且可以为空。 标签值的命名规则如下： • 可以为空。 • 长度为1~225个字符。 • 由英文字母、数字、下划线、点、中划线、UNICODE字符（\u4E00-\u9FFF）组成。	Value_0001

步骤5 单击“确定”，即可向受邀账号发出邀请。

----结束

管理组织的待处理邀请

登录到管理账号后，您可以查看和管理组织创建的邀请，具体步骤如下。

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**，进入账号管理页面。

步骤2 选择“邀请记录”页签，此页面展示组织发送的所有邀请及当前状态。

步骤3 单击邀请记录操作列的“取消邀请”，在弹框中单击“确定”可完成邀请取消。您只能取消“邀请中”的账号。

取消邀请后，邀请的状态将从“邀请中”更改为“已取消”。邀请取消后若要再次邀请当前账号，则必须重新发出邀请，才能让其加入您的组织。

图 4-3 取消邀请

----结束

接受或拒绝来自组织的邀请

您的账号可能会收到加入某个组织的邀请，您可以接受或拒绝邀请。

说明

一个账号只能加入一个组织。如果您收到多个加入组织邀请，只能接受其中一个。如果当前您已加入组织，则需要退出当前组织后，才能再次接受组织邀请。

步骤1 以受邀成员账号的身份登录**组织管理控制台**。

步骤2 此时界面会向您展示邀请列表。接受邀请则单击对应邀请操作列的“接受”，拒绝邀请则单击对应邀请操作列的“拒绝”。

图 4-4 接受或拒绝邀请

----结束

4.3 创建成员账号

组织的管理账号可在组织中直接创建新账号加入组织。在组织中直接创建的账号为资源账号，关于资源账号的详细说明请参见**资源账号与普通的财务托管子账号有哪些差异?** 。如有需要，您可以**将资源账号转为云账号**。

本章节包含如下内容：

- **创建账号**
- **通过委托登录创建的账号**
- **通过IAM身份中心登录创建的账号**

约束与限制

- 组织管理员最多可以同时创建5个账号。
- 在组织中创建的账号仅支持通过委托切换角色和IAM身份中心进行登录。
- 通过组织云服务创建的账号，财务默认托管于组织管理账号。

注意

- Organizations创建账号时会在新建账号内创建一个委托，委托对象为管理账号，该委托在新建成员账号内可删除，在删除前请启用IAM身份中心并配置相关身份与权限，保障业务责任人可正常访问该账号。

创建账号

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 单击组织结构树上方的“添加”，单击“添加账号”。

图 4-5 添加账号

步骤3 在弹窗中，选择“创建新账号”。

步骤4 输入账号名称，账号描述根据需要选择输入。注意，创建的账号名称不能与已有账号名称重复。

系统会默认提供委托名，可以保持默认，或者进行自定义修改。

图 4-6 新建账号

步骤5 （可选）为账号添加标签。

标签以键值对的形式表示，用于标识账号，便于对账号进行分类和搜索。一个账号最多添加20个标签。

标签的设置说明如表4-3所示。

表 4-3 标签说明

参数	说明	举例
键	输入标签的键，同一个账号标签的键不能重复。键可以自定义，也可以选择预先在标签管理服务（TMS）创建好的标签的键。 键命名规则如下： ● 不能为空。 ● 长度为1~128个字符。 ● 由英文字母、数字、下划线、中划线、UNICODE字符（\u4E00-\u9FFF）组成。	Key_0001
值	输入标签的值，标签的值可以重复，并且可以为空。 标签值的命名规则如下： ● 可以为空。 ● 长度为1~225个字符。 ● 由英文字母、数字、下划线、点、中划线、UNICODE字符（\u4E00-\u9FFF）组成。	Value_0001

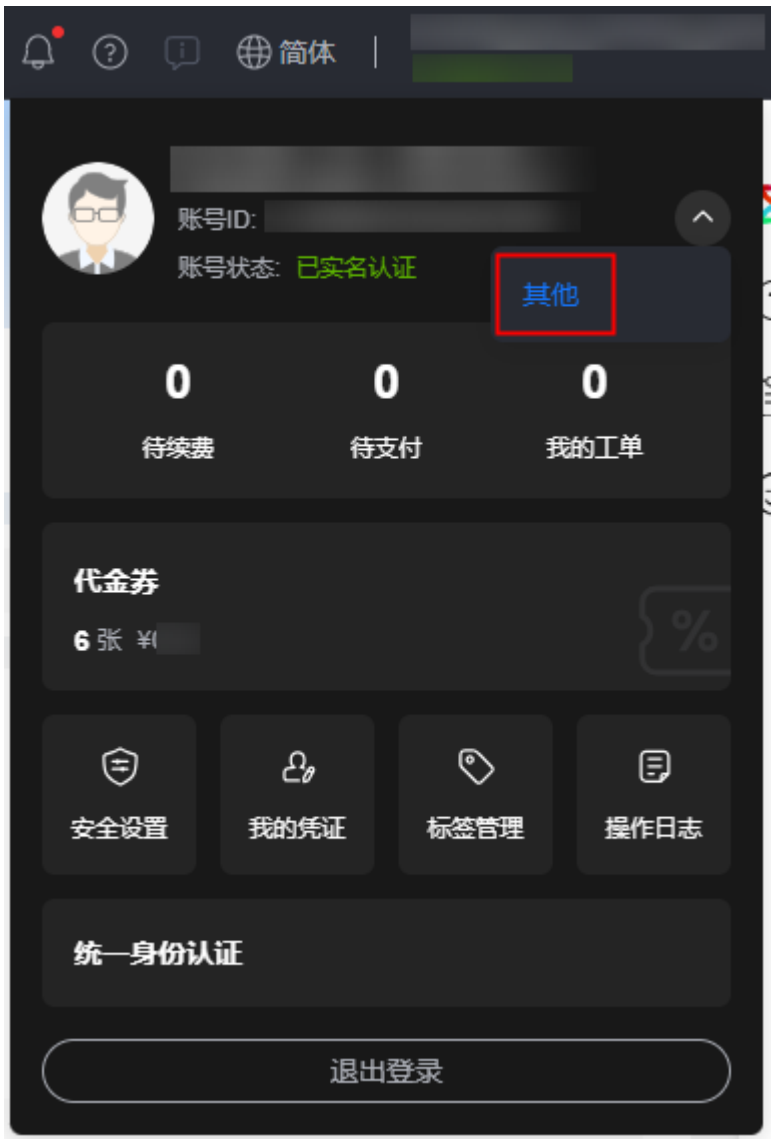
步骤6 单击“确定”，创建成功的账号将会显示在列表中。

----结束

通过委托登录创建的账号

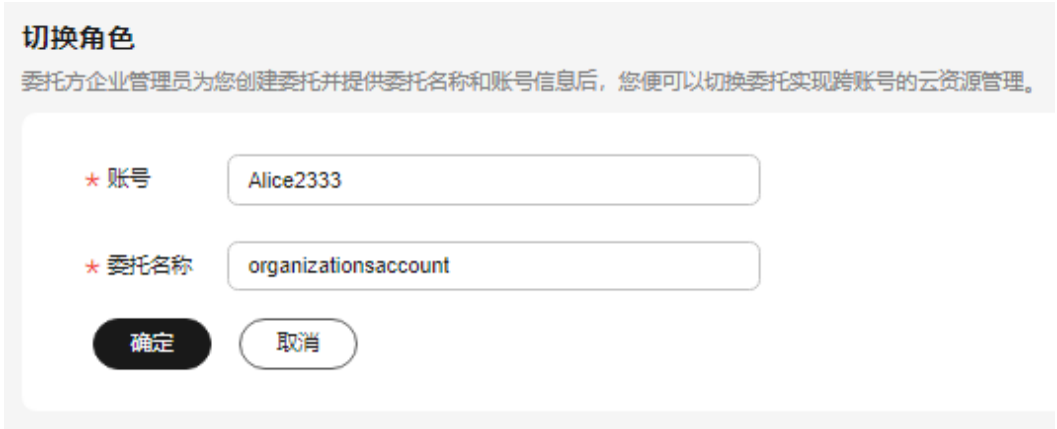
步骤1 鼠标移动至右上方的用户名，选择“其他”，进入切换角色页面。

图 4-7 切换角色



步骤2 在“切换角色”页面中，输入创建的账号名称。

图 4-8 输入创建的账号名称



说明

输入账号名称后，系统将会按照顺序自动匹配创建账号时输入的委托名称。匹配的委托名称中，也会出现以cbc_开头的委托名称，该委托主要用于企业主账号对企业费用的统一管理，对子账号进行委托授权。需要选用创建账号时输入的委托名称。

步骤3 单击“确定”，切换至创建的新账号中。

----结束

通过 IAM 身份中心登录创建的账号

账号创建完成后，可以将其与IAM身份中心的用户和权限集进行关联，关联后即可通过IAM身份中心的用户门户URL登录组织管理控制台，登录后可以访问组织下账号的资源。资源具体的访问权限由IAM身份中心权限集控制。

步骤1 **账号关联用户/组和权限集**。

步骤2 **登录创建的账号并访问资源**。

----结束

4.4 关闭成员账号

组织的管理账号可在组织中关闭不再需要的账号。以下步骤仅适用于关闭成员账号，如要关闭管理账号，您必须**关闭组织**

注意

- 账号关闭申请一旦提交则无法取消，账号内数据便会开始删除且无法恢复，请谨慎操作。
- 账号内数据删除完成后，该账号的状态变为“已关闭”，将继续在账号列表中保留90天，之后才会彻底注销。

约束与限制

- 只有创建的账号才可以关闭，无法关闭邀请的账号。
- 创建的账号如已转为云账号则无法关闭。
- 已设置为委托管理员的账号无法关闭，如需关闭请先**取消委托管理员**。
- 管理账号在30天内仅可以关闭组织中10%的成员账号，最多支持关闭200个成员账号，最多可以同时关闭3个成员账号。
- 创建新账号时，不能使用关闭中状态的账号所关联的手机号、邮箱。
- 如果账号中存在预付费资源（一般为包年/包月计费模式，先付费后使用）则无法关闭，请提前确认并退订相关包年/包月资源后，再进行关闭账号操作。如何退订资源请参见**退订使用中的资源**。
- 如果账号中存在欠费资源则无法关闭，请及时进行充值还款后，再进行关闭账号操作。如何充值还款请参见**充值和还款**。

操作步骤

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要关闭的账号。单击组织结构树上方的“管理”，选择“关闭账号”。

图 4-9 关闭账号

步骤3 在弹窗中阅读并勾选关闭账号的风险点，并输入需关闭账号的名称进行二次确认。

步骤4 单击“确定”，完成账号关闭。

----结束

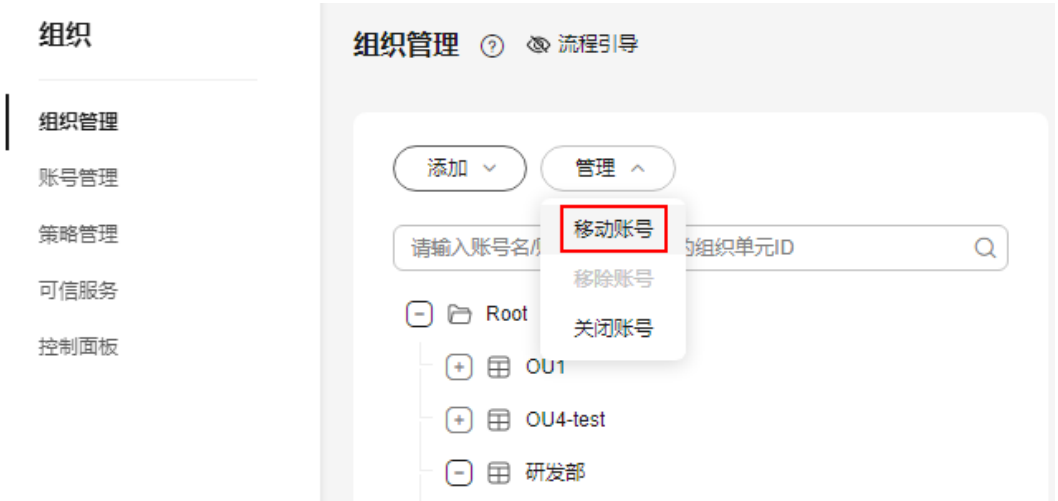
4.5 移动成员账号

登录到管理账号后，您可以移动组织内的账号，将账号从当前组织单元，移动到其他的组织单元中。

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要移动的账号。单击组织结构树上方的管理，选择“移动账号”。

图 4-10 移动账号



步骤3 在弹窗中选中要移动的目标组织单元，在下方的文本框中输入“确认”，然后单击“确定”，完成账号移动。

----结束

4.6 查看账号详细信息

您可以随时查看组织内账号的详细信息，具体请参见如下步骤。

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**，进入组织管理页。

步骤2 选中要查看的账号，在界面右侧即可查看账号详细信息。包括账号名称、ID、归属组织单元、URN、加入方式、加入时间或创建时间、账号状态、邮箱、账号描述，以及绑定的策略、标签、委托服务等信息。

图 4-11 查看账号详情

----结束

4.7 移除成员账号

移除须知

组织管理员从组织中移除成员账号或成员账号主动退出组织之前，您需要了解以下内容：

- 在组织中创建的账号被移除组织或主动退出组织时，该账号创建成功的时间需大于七个自然日。
- 在组织中创建的账号被移除组织或主动退出组织时，需先将其转换为华为云账号。如何转换请参见**将资源账号转为云账号**。
- 邀请加入组织的账号为华为云账号时才支持移除组织或主动退出组织，详情请参见**资源账号与华为云账号的差异**。
- 已设置为委托管理员的账号无法从组织中移除或主动退出组织，需先**取消委托管理员**。
- 在组织中创建账号时默认创建的IAM委托，账号离开组织后并不会自动删除，组织管理账号可继续通过此委托访问成员账号的数据，如需终止组织管理账号的此访问权限，需成员账号手动**删除委托**。

- 在组织中创建的账号离开组织后，不会改变该账号与组织管理账号的财务托管模式。邀请加入组织的账号离开组织后，不会改变该账号原有的财务关系。如需调整请参见**解除关联子账号**。
- 当某个成员账号离开组织后，组织策略施加的权限限制将不再影响该账号，这意味着该账号可能拥有比之前更多的权限。当组织已启用可信服务，成员账号离开组织后将无法再使用该服务与组织集成的相关功能。
- 当成员账号离开组织时，所有附加到该账号的标签都将被删除。

移除账号

登录组织的管理账号后，您可以从组织中移除不再需要的成员账号，步骤如下。注意，以下步骤仅适用于移除成员账号，要移除管理账号，您必须**删除组织**。

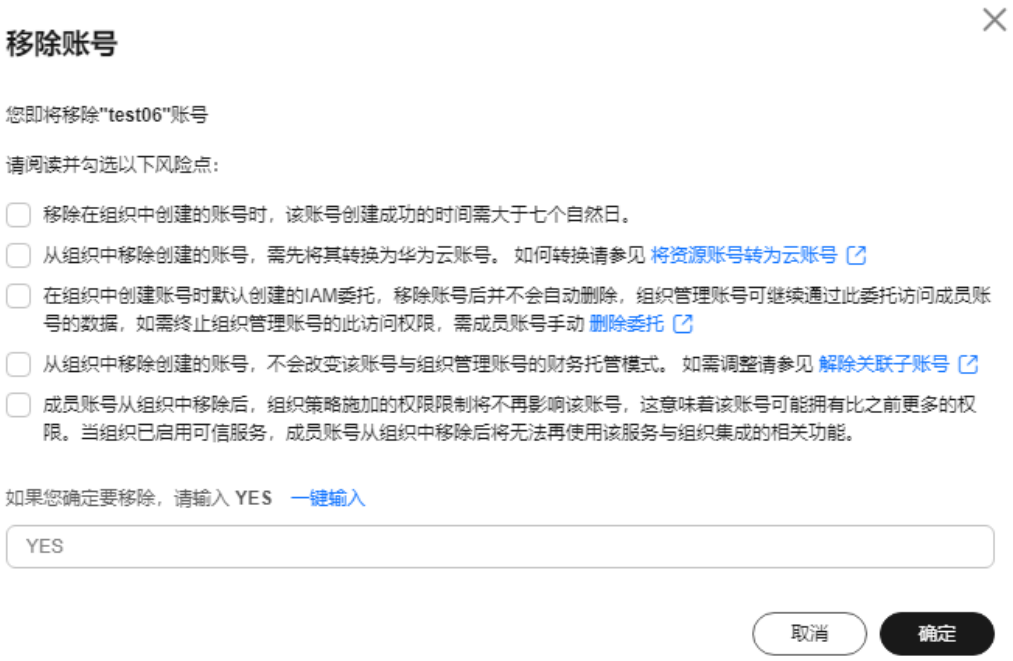
步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要移除的账号。单击组织结构树上方的管理，选择“移除账号”。

图 4-12 移除账号

步骤3 在弹窗中阅读并勾选移除账号的风险点，并输入“YES”，单击“确定”，完成成员账号移除。

图 4-13 确认移除账号



----结束

成员账号退出组织

登录成员账号后，您可以选择从组织中退出。管理账号不能使用“退出组织”的方法离开组织，要移除管理账号，您必须**删除组织**。

已设置为委托管理员的账号无法退出组织，如需退出请先**取消委托管理员**。

步骤1 以成员账号的身份登录**组织管理控制台**。

步骤2 在控制面板页面中的退出组织栏目下，单击“退出组织”，在弹窗中阅读退出组织的注意事项后，输入“YES”，单击“确认”，完成退出组织操作。

图 4-14 确认退出组织

----结束

4.8 查看账号邀请/创建记录

组织的管理账号可在账号管理页查看账号列表、邀请记录、创建记录及其相关信息，还可以进行邀请、创建、关闭、移动、移除账号以及取消邀请等操作。

本章节包含如下内容：

- **查看账号列表**
- **查看邀请记录**
- **查看创建记录**

查看账号列表

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入账号管理页，选择“账号列表”页签。

在列表中可查看组织中的全部账号及其相关信息。

步骤3 在列表中单击账号名，可查看账号的详细信息。

步骤4 在列表中的操作列，可对账号进行移动、移除、关闭操作。

邀请加入组织的账号不支持关闭操作。

步骤5 在列表左上方单击“添加”，可进行邀请现有账号和创建新账号加入组织的操作。

图 4-15 账号列表

----结束

查看邀请记录

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入账号管理页，选择“邀请记录”页签。

在列表中可查看全部的账号邀请记录及其相关信息。

步骤3 在列表中的操作列，可对状态为“邀请中”的邀请记录进行取消邀请操作。

步骤4 在列表左上方单击“邀请”，可进行邀请现有账号加入组织的操作。

图 4-16 邀请记录

----结束

查看创建记录

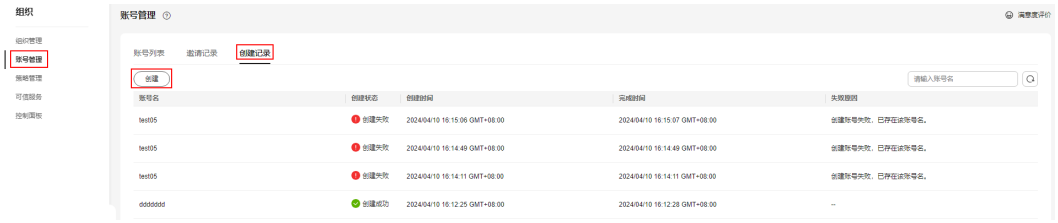
步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入账号管理页，选择“创建记录”页签。

在列表中可查看全部创建账号的记录及其相关信息。

步骤3 在列表左上方单击“创建”，可进行创建新账号加入组织的操作。

图 4-17 创建记录



----结束

5 服务控制策略管理

5.1 服务控制策略（SCP）介绍

5.1.1 服务控制策略概述

什么是服务控制策略

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。SCP可以关联到组织、OU和成员账号。当SCP关联到组织或OU时，该组织或OU下所有账号均受该策略影响。

本节将从以下几方面为您介绍SCP：

- **SCP原理介绍**：介绍SCP的分类，作用原理，继承规则，与IAM策略的关系。
- **SCP语法介绍**：介绍SCP的组成结构与策略参数。

测试 SCP 的影响

针对SCP对账号的影响，强烈建议您在生产环境应用SCP前，使用测试账号、测试环境、测试用例开展充分且彻底的系统设计和系统测试，避免对生产环境中服务资源的使用产生不必要的影响。在测试环境充分验证之后，且需要在生产环境应用时，您可以先创建一个OU，并每次移入一个账号或少量账号，以确保不会意外中断服务资源的使用。

⚠ 注意

对于系统预置的SCP系统策略“FullAccess”，解绑操作需谨慎处理，除非您将其替换为具有允许操作的自定义策略，否则不应解绑该策略。**当您确定需要解绑“FullAccess”并且配置具有允许操作的自定义策略时，除配置业务需要的授权项外，必须额外配置iamToken::*和signin::*。**

- 如果解绑Root的“FullAccess”策略，则整个组织内所有账号的可操作性权限都将失效。此操作风险极高，需谨慎操作。
- 如果解绑OU的“FullAccess”策略，则该OU（包含下级OU）内账号的可操作权限都将失效。
- 如果解绑成员账号的“FullAccess”策略，则该账号的可操作权限将失效。

不受 SCP 限制的任务

您无法使用SCP来限制以下任务：

- 组织管理账号及其IAM用户执行的任何操作。
- 使用服务关联委托执行的任何操作。
- 由不支持SCP的云服务对支持SCP的云服务发起的API调用请求，将不受SCP限制。当前支持SCP的云服务请参见：**支持SCP的云服务**。
- 通过**API方式获取Token**后，使用该Token访问支持SCP的云服务的API，在大多数场景下将不受SCP限制。

相关链接

统一身份认证服务与组织权限访问控制的区别，请参见**IAM与Organizations权限访问控制的区别**。

5.1.2 SCP 原理介绍

SCP 分类

SCP按照策略创建者可分为两类，分别是系统策略和自定义策略。

- **系统策略**

华为云服务在组织预置了常用SCP，称为系统策略。组织管理员给组织单元或账号绑定SCP时，可以直接使用这些策略。系统策略只能使用，不能修改。现有的SCP系统策略请参见：**SCP系统策略列表**。

- **自定义策略**

如果系统策略无法满足授权要求，管理账号可以根据各服务支持的授权项，自行创建和修改自定义策略。自定义策略是对系统策略的扩展和补充。目前Organizations云服务支持策略编辑器和JSON视图两种自定义策略配置方式。

权限控制原理

- **划定权限边界**

  SCP不直接进行授权，只划定权限边界。将SCP绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单

元包含的成员账号的授权范围。IAM策略授予权限的有效性受SCP限制，只有在SCP允许范围内的权限才能生效。SCP禁止的权限操作，即便授予IAM用户权限，用户也不能执行相关操作。

比如成员账号A绑定了某一条SCP，SCP允许操作A的权限，拒绝操作B的权限。那么成员账号A可以给自己名下的IAM用户授予操作A的权限，不能授予操作B的权限，即便授予了操作B的权限，也无法生效。

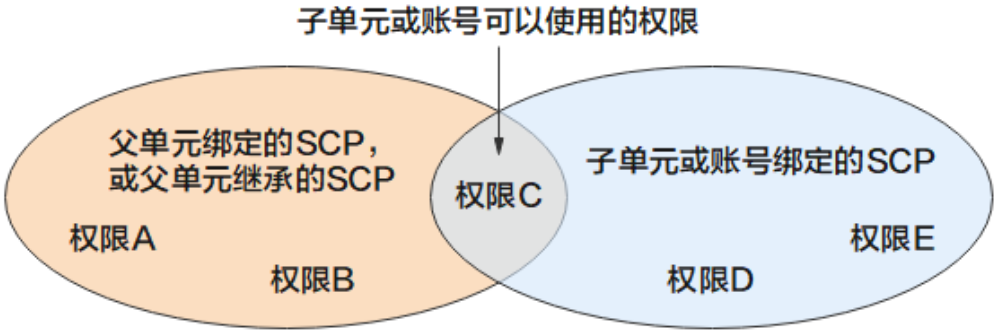
- **交集有效**

  权限边界的叠加遵从交集有效准则，父OU的SCP与子OU（或账号）的SCP共同允许的权限，作为子OU的最终权限边界。

  如下图所示，左侧的椭圆表示附加到父OU的SCP，它允许权限A、B和C。右侧椭圆表示子OU（或账号）绑定SCP允许的权限，子OU（或账号）允许权限C、D和E。由于附加到父OU的SCP不允许D或E，因此父OU下的所有子OU和账号都不能使用它们，即使子OU的SCP明确允许D和E，它们最终仍然会被父OU的SCP阻止。子OU（或账号）的SCP不允许A或B，因此， 子OU（或账号）将阻止这些权限。最终，子OU的权限是父OU权限和子OU（或账号）绑定SCP的权限交集，即下图中的权限C。

  如果椭圆右侧是一个成员账号，则交集是授予该账号中的用户和用户组的最大权限集合。如果椭圆右侧是OU，则交集是该子OU可继承的最大权限集合。

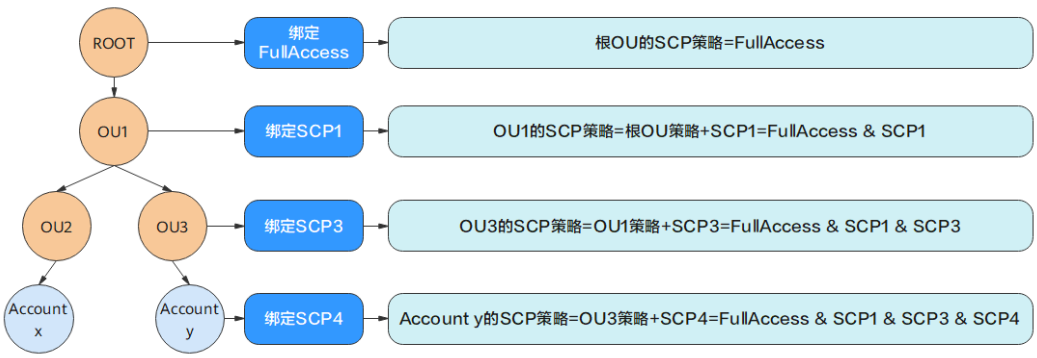
图 5-1 SCP 原理图



- **筛选继承**

  组织单元或账号绑定的SCP包括两部分，直接绑定的策略和继承的策略。某组织单元绑定的SCP，会继承给该组织单元下的所有子级OU和账号。账号和组织单元的权限边界，由所有上级OU的SCP和自身直接绑定的SCP共同决定。如下图所示，Account y隶属于OU3，Account y的权限边界是由继承自Root，OU1和OU3的SCP与Account y绑定的SCP共同决定。

图 5-2 SCP 继承规则



如果要在成员账号级别允许使用某个云服务的操作，则必须在账号和根组织单元之间的每个层级上允许该操作。这意味着，必须在根组织单元和账号之间的每个层级，附加允许该操作的SCP。您可以使用下列任一策略执行此操作：

添加拒绝策略。拒绝策略会使用默认附加到每个OU和账号上的FullAccess SCP。此SCP将覆盖默认的隐式Deny，并明确允许所有权限从根组织单元传递到每个账号，除非创建并附加到相应OU或账号的其他SCP明确了拒绝权限。具有拒绝策略的OU层级以下的任何账号都不能使用被拒绝的操作，也无法在组织结构中较低的层级中添加该权限。

- **默认允许**

  组织启用SCP时，默认会为所有OU和账号附加全部权限（FullAccess策略），默认允许所有操作。除非您为OU或账号附加其他的明确拒绝策略。

显式拒绝和隐式拒绝的区别

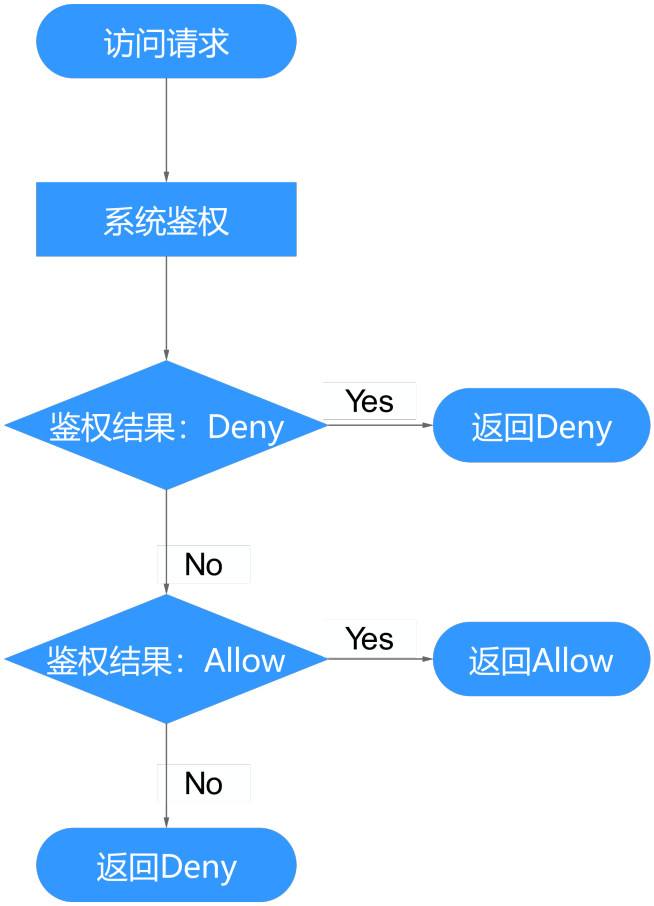
Effect（效果）：Deny（拒绝），表示拒绝执行某操作的权限。

当没有策略设置权限为Deny时，默认情况即为Deny权限，称为隐式拒绝。

如果策略设置权限为Deny，则为显式拒绝。

用户在发起访问请求时，鉴权规则如下：

图 5-3 系统鉴权逻辑图



1. 用户发起访问请求。

2. 系统优先寻找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。

5.1.3 SCP 语法介绍

下面以RAM的自定义策略为例，说明策略的语法。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:create"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
       "ForAnyValue:StringNotEquals": {
          "g:RequestTag/owner": [
            "Alice",
            "Jack"
          ]
        }
      }
    }
  ]
}
```

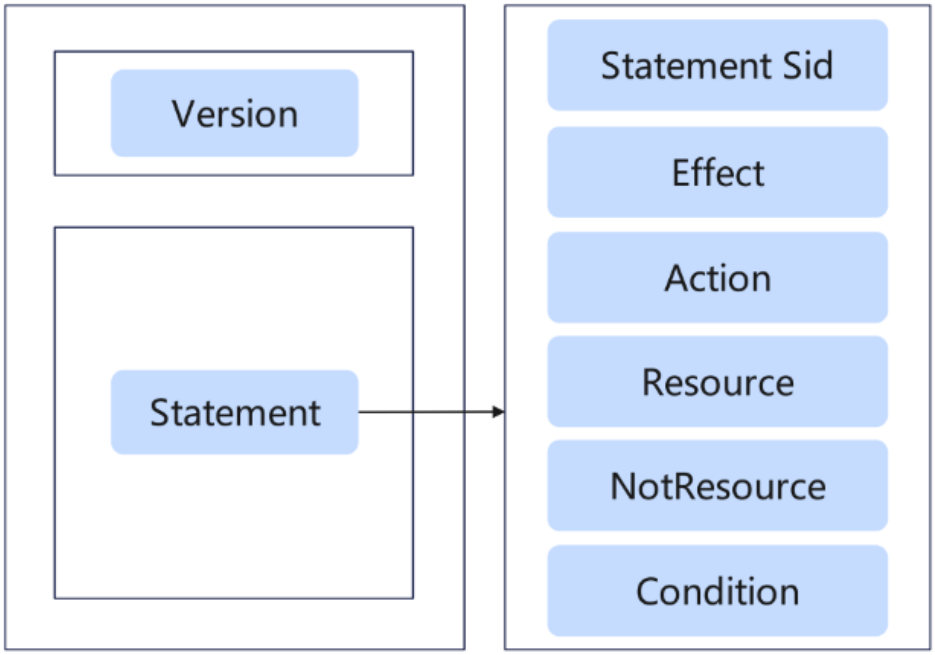
说明

SCP的语法与IAM身份策略的语法一致。

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元素的值可以是多个对象组成的数组，表示不同的权限约束。

图 5-4 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。

表 5-1 策略参数说明

参数		是否必选	含义	值
Version		必选	策略的版本。	5.0（不可自定义）
Statement： 策略的授权语句	Statement Sid	可选	策略语句标识符。您可为语句数组中的每个策略语句指定Sid值。	用户自定义字符串。
	Effect：作用	必选	定义Action中的操作权限是否允许执行。	Deny：不允许执行。
	Action：授权项	Deny时可选	操作权限。	格式为“服务名:资源类型:操作”。例如“vpc:subnets:list”：表示查看VPC子网列表权限，其中vpc为服务名，subnets为资源类型，list为操作。

参数		是否必选	含义	值
	Condition：条件	Deny时可选	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":["specialCharacter"]}：表示当用户输入的用户名以"specialCharacter"结尾时该条statement生效。
	Resource：资源类型	可选 未指定时，Resource默认为“*”，策略应用到所有资源。	策略所作用的资源。	Deny时，可选择“*”或具体资源，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："ecs:*:*:instance:*"：表示所有的ECS实例。
	NotResource: 排除在策略外的资源类型	可选 未指定时，参考Resource。	策略不作用的资源。	

说明

SCP中不支持以下元素：

- Principal
- NotPrincipal
- NotAction

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。详情请参见**全局条件键**中各服务支持的条件键。

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。运算符可以增加后缀“IfExists”，表示对应请求值不存在或请求值存

在且满足条件时均使策略生效，如“StringEqualsIfExists”表示表示请求值不存在或请求值等于条件值均使策略生效。详情请参见**运算符**。

5.2 启用和禁用 SCP 功能

启用 SCP

在创建SCP并将其附加到组织单元和账号之前，必须先启用SCP，且只能使用组织的管理账号启用SCP。启用SCP后，组织将自动给所有OU和账号绑定FullAccess策略，默认允许所有操作。

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入策略管理页，单击“服务控制策略”操作列的“启用”。

步骤3 在弹窗中勾选确认框，然后单击“确定”，完成SCP功能启用。

图 5-5 启用 SCP

----结束

禁用 SCP

如果您不想再使用SCP管理组织权限，可以禁用SCP，且只能使用组织的管理账号禁用SCP。

注意

- 禁用SCP后，所有SCP会自动从组织中的所有实体解绑，包括所有OU和账号，但是策略本身不会被删除。
- 若禁用SCP后再重新启用SCP，则组织中的所有实体将恢复到只绑定FullAccess的状态。实体与其他SCP的绑定关系将丢失，如需恢复则需要用户重新绑定。

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入策略管理页，单击“服务控制策略”操作列的“禁用”。

图 5-6 禁用 SCP

步骤3 在弹窗中单击“确定”，完成SCP功能禁用。

----结束

5.3 创建 SCP

本章为您介绍如何创建自定义SCP，SCP常用示例请参见：**SCP配置示例**。

约束与限制

- 自定义SCP策略中的Effect仅支持使用Deny，不支持使用Allow。
- 自定义SCP策略中的关键字仅支持使用Action，不支持使用NotAction。
- Action前缀仅支持使用已对接IAM5.0的云服务名称，例如Action="ram:*:*"，不支持使用通配符，比如Action="*" 或 Action="*:*:*"。
- 自定义SCP策略中的授权项必须包含3个字段并包含以下结构:

  "service-name:type-name:action-name"

操作步骤

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入策略管理页，单击“服务控制策略”，进入SCP管理页。

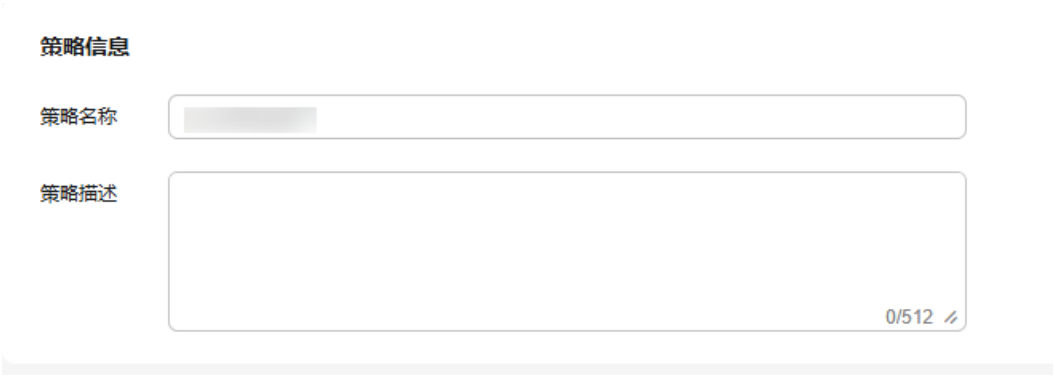
图 5-7 进入 SCP 管理页

步骤3 单击“创建”，进入SCP创建页面。

图 5-8 创建 SCP

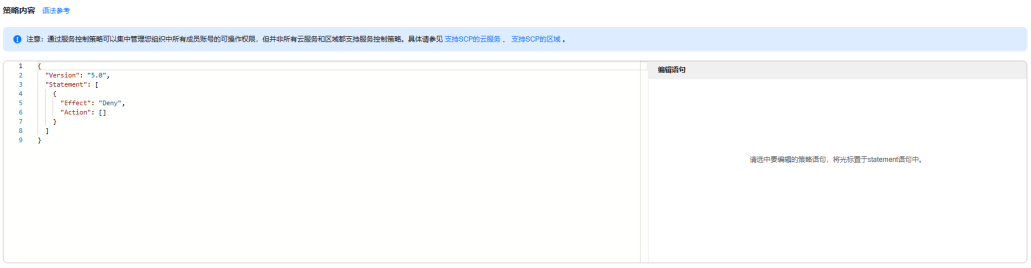
步骤4 输入策略名称。新创建的策略名称不能与已有策略名称重复。

（可选）输入策略描述。



步骤5 在策略内容左侧可以直接编写JSON格式的策略内容。

关于如何编写JSON格式的策略语句可参考**SCP语法介绍**和**SCP配置示例**。



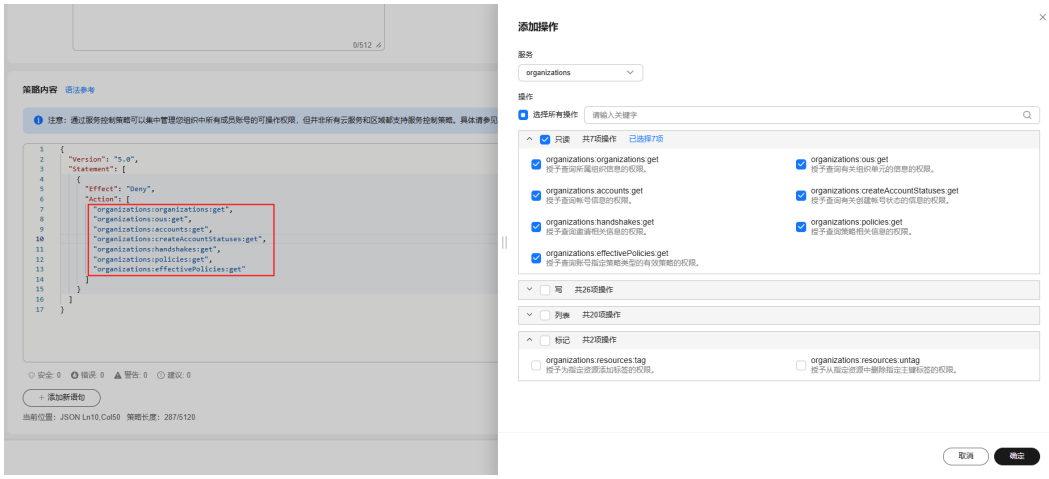
说明

自定义策略版本号（Version）固定为5.0，不可修改。

步骤6 将光标置于策略内容左侧的statement语句中，即可在策略内容右侧使用策略编辑器进行编辑自定义策略的操作、资源和条件。

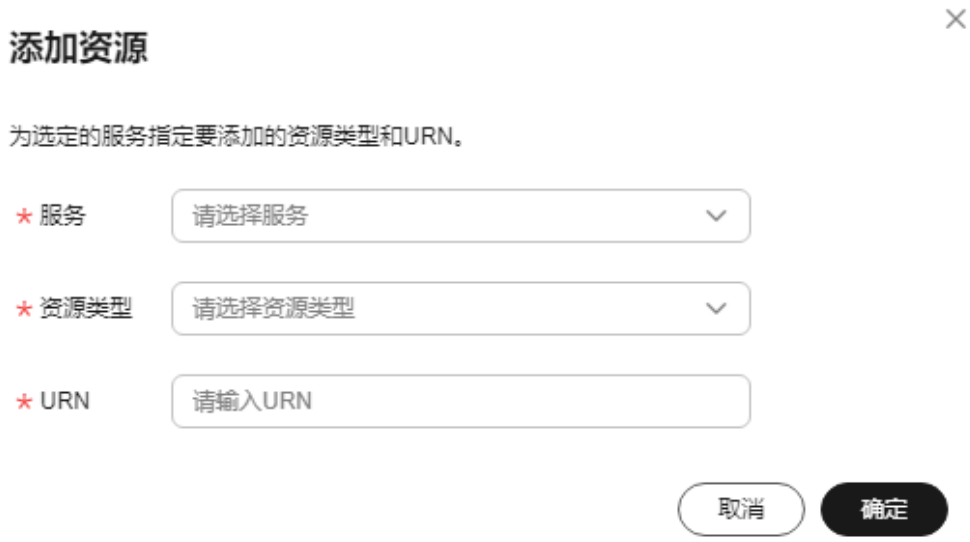
- 添加操作：单击 ⊕ 号，选择或搜索要添加的服务及相应操作项，添加成功的操作项会自动显示在策略内容左侧的Action元素下。如**图5-9**所示。

图 5-9 添加操作



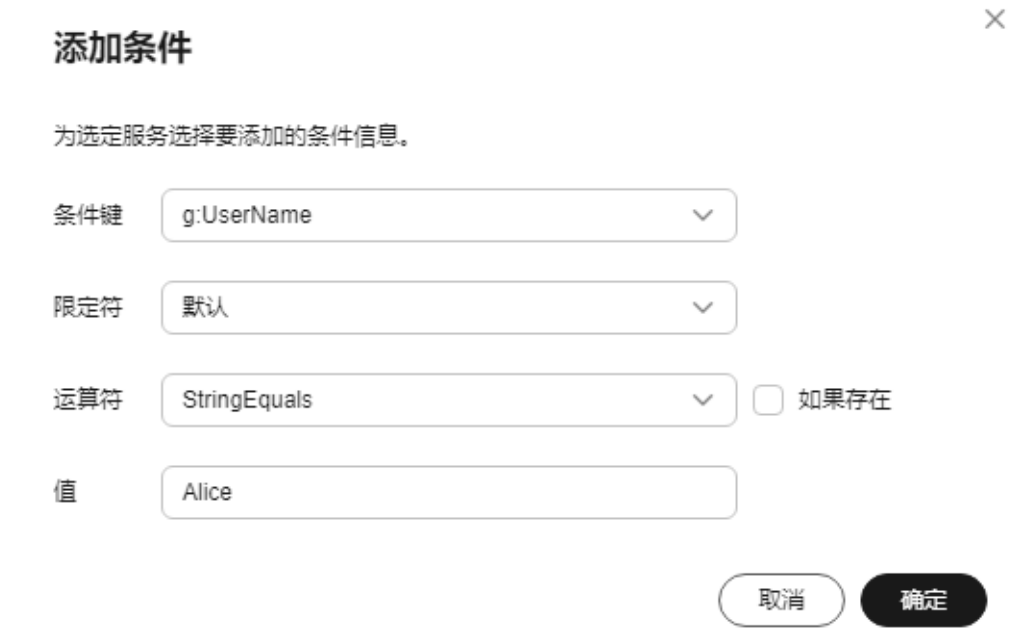
- 添加资源：仅支持资源级授权的服务可添加。单击 ⊕ 号，选择操作对应的服务，在选择资源类型，根据实际情况填写URN。如图5-10所示。

图 5-10 添加资源



- 添加条件（可选）：单击 ⊕ 号，添加条件键和运算符，规定策略生效的条件。如图5-11所示。

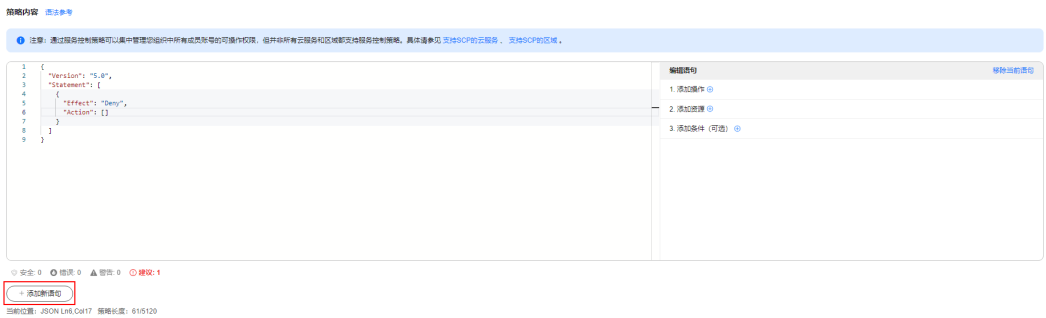
图 5-11 添加条件



步骤7 （可选）单击“添加新语句”，可添加Statement元素的对象。

Statement元素的值可以是多个对象组成的数组，表示不同的权限约束。

图 5-12 添加新语句



步骤8 （可选）为策略添加标签。在标签栏目下，输入标签键和标签值，单击“添加”。

图 5-13 为 SCP 添加标签

步骤9 单击右下角“保存”后，系统会自动校验语法，如跳转到策略列表，则SCP创建成功；如系统提示策略内容有误，则请按照语法规范进行修改。

----结束

5.4 修改和删除 SCP

本章为您介绍如何修改和删除已创建的自定义SCP。

修改 SCP

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

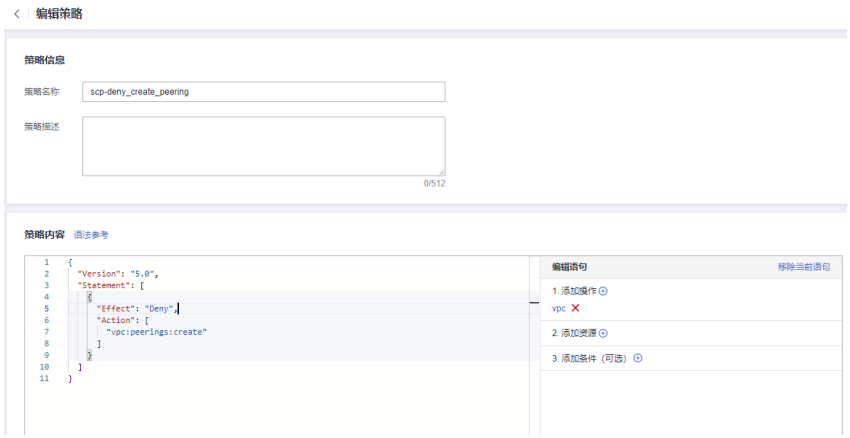
步骤2 进入策略管理页，单击“服务控制策略”，进入SCP管理页。

步骤3 单击自定义SCP操作列的“编辑”，在弹窗中输入“确认”，单击“确定”。

图 5-14 修改 SCP

步骤4 进入编辑策略页面，按需修改“策略名称”和“策略描述”，如**图5-15**所示。

图 5-15 修改 SCP



步骤5 按需修改策略内容。可使用语句编辑器进行修改，策略语法请参考**SCP语法介绍**。

步骤6 单击右下角“保存”后，系统会自动校验语法，如跳转到策略列表，则SCP编辑成功；如系统提示策略内容有误，则请按照语法规范进行修改。

----结束

删除 SCP

如果当前SCP已与组织单元或账号绑定，则无法删除。组织单元或账号解绑该SCP后，才可顺利删除。

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入策略管理页，单击“服务控制策略”，进入SCP管理页。

步骤3 单击自定义SCP操作列的“删除”。

步骤4 在弹窗中单击“确定”，完成SCP删除。

图 5-16 删除 SCP

----结束

5.5 绑定和解绑 SCP

管理账号可以为根、OU和账号绑定和解绑SCP。

约束与限制

- SCP不会影响组织管理账号及其IAM用户和委托，仅会影响组织内的成员账号。
- 策略完成绑定后将在30分钟内生效。
- 无法为组织管理员绑定SCP。

绑定 SCP

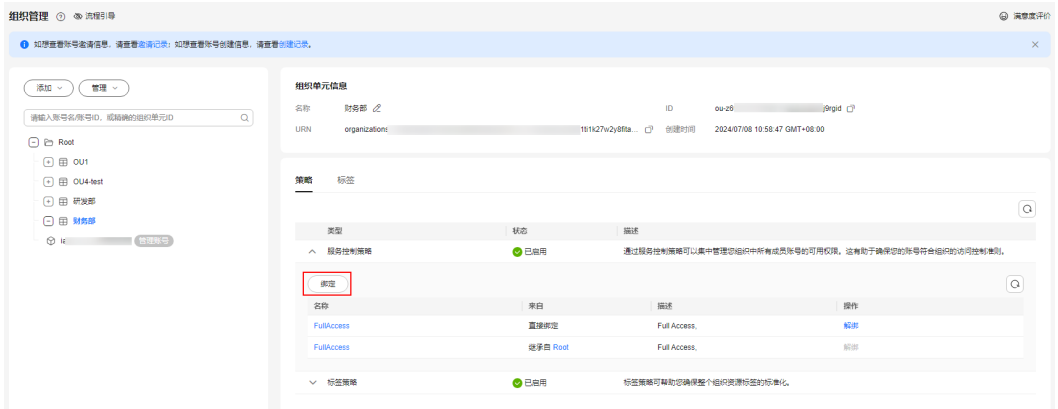
方式一：

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要绑定SCP的OU或者账号。

步骤3 在右侧详情页，选择策略页签，展开“服务控制策略”列表，单击列表上方的“绑定”。

图 5-17 绑定 SCP



步骤4 在弹窗中选择要添加的策略后，在文本框中输入“确认”，然后单击“确认”按钮，完成策略绑定。

----结束

方式二：

步骤1 在组织管理控制台，进入策略管理页。

步骤2 单击“服务控制策略策略”，进入SCP策略列表页。

步骤3 单击SCP策略操作列的“绑定”，选中要绑定SCP策略的OU或者账号。

步骤4 在弹窗中输入“确认”，单击“确定”，完成策略绑定。

图 5-18 绑定 SCP

----结束

解绑 SCP

方法一：

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要解绑SCP的OU或者账号。

步骤3 在右侧详情页，选策略页签，展开“服务控制策略”列表，在列表单击要解绑的SCP操作列的“解绑”。

步骤4 在弹窗中输入“确认”，单击“确定”，完成策略解绑。

图 5-19 解绑 SCP

说明

OU和账号至少直接绑定一个SCP，最后一个直接绑定策略，不可解绑。

----结束

方式二：

步骤1 在**组织管理控制台**，进入策略管理页。

步骤2 单击“服务控制策略策略”，进入SCP策略列表页。

步骤3 单击SCP策略的名称，选择“目标”页签。

步骤4 单击需要解绑的OU或账号操作列的“解绑”，在弹窗中输入“确认”，单击“确定”，完成策略解绑。

图 5-20 解绑 SCP

----结束

5.6 SCP 配置示例

本章节为您介绍SCP的常用示例，包含如下内容：

- **阻止成员账号退出组织**
- **阻止根用户的服务访问**
- **禁止创建带有指定标签的资源**
- **禁止访问指定区域的资源**

- **禁止共享到组织外**
- **禁止共享指定类型的资源**
- **禁止组织内账号给组织外的账号进行聚合授权**
- **阻止IAM用户和委托进行某些修改**
- **阻止IAM用户和委托进行某些修改，但指定的账号除外**
- **阻止IAM用户和委托进行某些修改，但指定的委托除外**
- **使用NotResource，除指定的ecs实例外，阻止对其他ecs实例的启动**

阻止成员账号退出组织

使用以下SCP阻止成员账号主动退出组织。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "organizations:organizations:leave"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

阻止根用户的服务访问

使用以下SCP禁止成员账号使用根用户执行指定的操作。您可以根据需要修改SCP语句中的操作（Action）和资源类型（Resource）。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ecs:*:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "BoolIfExists": {
          "g:PrincipalIsRootUser": "true"
        }
      }
    }
  ]
}
```

禁止创建带有指定标签的资源

如下SCP表示禁止用户创建带有 {"team": "engineering"} 标签的资源共享实例。您可以根据需要修改SCP语句中的操作（Action）、资源类型（Resource）和条件（Condition）。

```
{
    "Version":"5.0",
    "Statement":[
```



```
    {
        "Effect":"Deny",
        "Action":["ram:resourceShares:create"],
        "Resource":["*"],
        "Condition":{
            "StringEquals":{
                "g:RequestTag/team":"engineering"
            }
        }
    }
  ]
}
```

禁止访问指定区域的资源

如下SCP表示禁止用户访问“regionid1”区域的ECS服务的全部资源。您可以根据需要修改SCP语句中的操作（Action）、资源类型（Resource）和条件（Condition）。

此SCP仅适用于区域级服务，SCP中的“regionid1”仅为区域示例，使用时请填入具体区域ID。

```
{
  "Version":"5.0",
  "Statement":[
    {
        "Effect":"Deny",
        "Action":["ecs:*:*"],
        "Resource":["*"],
        "Condition":{
            "StringEquals":{
                "g:RequestedRegion":"ap-southeast-1"
            }
        }
    }
  ]
}
```

禁止共享到组织外

使用以下SCP禁止本组织内的账号给组织外账号共享资源。此SCP建议绑定至组织的根OU，使其对整个组织生效。

```
{
 "Version": "5.0",
 "Statement": [
  {
   "Effect": "Deny",
   "Action": [
    "ram:resourceShares:create",
    "ram:resourceShares:associate"

   ],
   "Resource": [
    "*"
   ],
   "Condition": {
    "ForAnyValue:StringNotLike": {
     "ram:TargetOrgPaths": [
      "organization_id/root_id/ou_id"【备注：此处需填写组织的路径ID】
     ]
    }
   }
  }
 ]
}
```


禁止共享指定类型的资源

使用以下SCP禁止用户共享VPC子网资源。您可以根据需要修改SCP语句条件键（Condition）元素中的资源类型。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:create"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "ram:RequestedResourceType": [
            "vpc:subnet"【备注：可根据需要修改此处的资源类型】
          ]
        }
      }
    }
  ]
}
```

禁止组织内账号给组织外的账号进行聚合授权

使用以下SCP禁止本组织内账号给组织外的账号进行聚合授权。此SCP建议绑定至组织的根OU，使组织外账号无法获取组织内账号下的资源清单信息。您也可以将此SCP绑定给接受授权的账号（源账号），禁止该账号接受来自聚合器账号的授权请求。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "rms:aggregationAuthorizations:create"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotMatch": {
          "rms:AuthorizedAccountOrgPath": [
            "organization_id/root_id/ou_id"【备注：此处需填写组织的路径ID】
          ]
        }
      }
    }
  ]
}
```

阻止 IAM 用户和委托进行某些修改

使用此SCP阻止IAM用户和委托对组织内所有账号创建的资源共享进行修改。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:update",
```



```
      "ram:resourceShares:delete",
      "ram:resourceShares:associate",
      "ram:resourceShares:disassociate",
      "ram:resourceShares:associatePermission",
      "ram:resourceShares:disassociatePermission"
    ],
    "Resource": [
      "ram::*:resourceShare:resource-id"
    ]
  }
 ]
}
```

阻止 IAM 用户和委托进行某些修改，但指定的账号除外

使用此SCP阻止IAM用户和委托对组织内所有账号创建的资源共享进行修改，但指定的账号除外。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:update",
        "ram:resourceShares:delete",
        "ram:resourceShares:associate",
        "ram:resourceShares:disassociate",
        "ram:resourceShares:associatePermission",
        "ram:resourceShares:disassociatePermission"
      ],
      "Resource": [
        "ram::*:resourceShare:resource-id"
      ],
      "Condition": {
        "StringNotEquals": {
          "g:DomainId": [
            "account-id"【备注：此处需填写排除账号的ID】
          ]
        }
      }
    }
  ]
}
```

阻止 IAM 用户和委托进行某些修改，但指定的委托除外

使用此SCP阻止IAM用户和委托对组织内所有账号创建的资源共享进行修改，但指定的委托除外。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:create"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotMatch": {
          "g:PrincipalUrn": "sts::*:assumed-agency:AgencyName/*"
        }
      }
    }
```



```
  ]
}
```

使用 NotResource，除指定的 ecs 实例外，阻止对其他 ecs 实例的启动

如下SCP表示禁止启动除ecs:*:8c1eef3a241xxxxxxxxx3a6b0252e783:instance:test-ecs外的其他ecs实例，通过NotResource将ecs:*:8c1eef3a241xxxxxxxxx3a6b0252e783:instance:test-ecs排除在外。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ecs:cloudServers:start"
      ],
      "NotResource": [
        "ecs:*:8c1eef3a241xxxxxxxxx3a6b0252e783:instance:test-ecs"
      ]
    }
  ]
}
```

5.7 SCP 系统策略列表

现有华为云预置的SCP系统策略如下表所示：

表 5-2 华为云 SCP 系统策略

策略名	描述
FullAccess	允许所有资源的所有权限。

说明

每个根、OU和账号必须始终绑定至少一个SCP。

5.8 支持 SCP 的云服务

当前支持使用SCP的云服务如下表所示：

说明

支持SCP的云服务同时也支持IAM的身份策略。

计算

序号	服务名称	相关文档
1	弹性云服务器（ECS）	**弹性云服务器 ECS**
2	裸金属服务（BMS）	**裸金属服务器 BMS**

序号	服务名称	相关文档
3	镜像服务（IMS）	镜像服务 IMS
4	弹性伸缩（AS）	弹性伸缩 AS
5	函数工作流（FunctionGraph）	函数工作流 FunctionGraph

存储

序号	服务名称	相关文档
1	云备份（CBR）	云备份 CBR
2	云硬盘（EVS）	云硬盘 EVS
3	高性能弹性文件服务 SFS Turbo	高性能弹性文件服务 SFS Turbo
4	对象存储服务 OBS	对象存储服务 OBS

网络

序号	服务名称	相关文档
1	虚拟私有云（VPC）	虚拟私有云 VPC
2	弹性公网IP（EIP）	弹性公网IP EIP
3	NAT网关（NAT）	NAT网关 NAT
4	弹性负载均衡（ELB）	弹性负载均衡 ELB
5	VPC终端节点（VPCEP）	VPC终端节点 VPCEP
6	云专线（DC）	云专线 DC
7	企业路由器（ER）	企业路由器 ER
8	全球加速服务（GA）	全球加速服务 GA
9	云连接（CC）	云连接 CC
10	云解析服务（DNS）	云解析服务 DNS

容器

序号	服务名称	相关文档
1	云容器引擎（CCE）	云容器引擎 CCE
2	容器镜像服务（SWR）	容器镜像服务（基础版） SWR

CDN 与智能边缘

序号	服务名称	相关文档
1	内容分发网络（CDN）	内容分发网络 CDN

数据库

序号	服务名称	相关文档
1	云数据库（RDS）	云数据库 RDS
2	文档数据库服务（DDS）	文档数据库服务 DDS
3	云数据库 GaussDB	云数据库 GaussDB
4	数据管理服务 （DAS）	数据管理服务 DAS

安全与合规

序号	服务名称	相关文档
1	原生基础防护（Anti-DDoS）	原生基础防护 Anti-DDoS
2	DDoS原生高级防护（CNAD）	原生高级防护 CNAD
3	DDoS高防（AAD）	DDoS高防 AAD
4	密码安全中心（DEW），包含如下微服务： • 密钥管理服务（KMS） • 云凭据管理服务（CSMS） • 密钥对管理服务（KPS） • 专属加密（DHSM）	密码安全中心 DEW
5	主机安全服务（HSS）	主机安全服务 HSS
6	安全云脑（SecMaster）	安全云脑 SecMaster
7	云防火墙（CFW）	云防火墙 CFW
8	数据安全中心（DSC）	数据安全中心 DSC
9	云堡垒机（CBH）	云堡垒机 CBH
10	数据库安全服务（DBSS）	数据库安全服务 DBSS
11	Web应用防火墙（WAF）	Web应用防火墙 WAF

人工智能

序号	服务名称	相关文档
1	AI开发平台 ModelArts	AI开发平台 ModelArts

大数据

序号	服务名称	相关文档
1	数据湖探索（DLI）	数据湖探索 DLI
2	数据治理中心（DataArts Studio）	数据治理中心 DataArts Studio
3	云搜索服务（CSS）	云搜索服务 CSS

应用中间件

序号	服务名称	相关文档
1	分布式缓存服务（DCS）	分布式缓存服务 DCS
2	分布式消息服务Kafka版	分布式消息服务Kafka版
3	分布式消息服务RabbitMQ版	分布式消息服务RabbitMQ版
4	分布式消息服务RocketMQ版	分布式消息服务RocketMQ版
5	微服务引擎（CSE）	微服务引擎 CSE
6	API网关（APIG）	API网关 APIG

开发与运维

序号	服务名称	相关文档
1	软件开发生产线（CodeArts）	软件开发生产线 CodeArts
2	流水线（CodeArts Pipeline）	流水线 Codearts Pipeline
3	云应用引擎 CAE	云应用引擎 CAE

视频

序号	服务名称	相关文档
1	视频直播服务 Live	视频直播服务 Live

管理与监管

序号	服务名称	相关文档
1	消息通知服务（SMN）	消息通知服务 SMN
2	云日志服务（LTS）	云日志服务 LTS
3	统一身份认证（IAM）	统一身份认证 IAM
4	IAM身份中心（IdentityCenter）	IAM身份中心
5	组织（Organizations）	组织 Organizations
6	资源访问管理（RAM）	资源访问管理 RAM
7	企业项目管理服务 （EPS）	企业项目管理 EPS
8	标签管理服务（TMS）	标签管理服务 TMS
9	配置审计（Config）（原 资源管理服务 RMS）	配置审计 Config
10	访问分析（AccessAnalyzer）	访问分析 IAM Access Analyzer
11	云审计服务（CTS）	云审计服务 CTS
12	应用运维管理（AOM）	应用运维管理 AOM
13	应用性能管理 APM	应用性能管理 APM
14	优化顾问 OA	优化顾问 OA

迁移

序号	服务名称	相关文档
1	对象存储迁移服务（OMS）	对象存储迁移服务 OMS
2	主机迁移服务（SMS）	主机迁移服务 SMS

用户服务

序号	服务名称	相关文档
1	费用中心	费用中心
2	成本中心	成本中心
3	账号中心	账号中心
4	企业中心	企业中心

5.9 支持 SCP 的区域

当前支持使用SCP的区域如下表所示：

说明

支持SCP的区域与支持IAM身份策略的区域相同。

表 5-3 支持 SCP 的区域

区域名称	区域代码
亚太-新加坡	ap-southeast-3
亚太-曼谷	ap-southeast-2
亚太-雅加达	ap-southeast-4
亚太-马尼拉	ap-southeast-5
华东-上海一	cn-east-3
华东-上海二	cn-east-2
中国-香港	ap-southeast-1
华北-北京一	cn-north-1
华北-北京四	cn-north-4
华南-广州	cn-south-1
华北-乌兰察布一	cn-north-9
西南-贵阳一	cn-southwest-2
华东-青岛	cn-east-5
土耳其-伊斯坦布尔	tr-west-1
非洲-约翰内斯堡	af-south-1
拉美-墨西哥城一	na-mexico-1
拉美-墨西哥城二	la-north-2
拉美-圣保罗一	sa-brazil-1
拉美-圣地亚哥	la-south-2
中东-利雅得	me-east-1
非洲-开罗	af-north-1
华东二	cn-east-4
华北三	cn-north-12

6 标签策略管理

6.1 标签策略概述

标签策略简介

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。在标签策略中，您可以限定为资源添加的标签必须符合规范。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。

例如：标签策略规定为某资源添加的标签A，需要遵循标签策略中定义的大小写规则和标签值。若标签A使用的大小写、标签值不符合标签策略，则资源将会被标记为不合规。

标签策略当前的应用方式为事前拦截：标签策略开启强制执行后，则会阻止在指定的资源类型上完成不合规的标记操作。

标签策略可以绑定到组织的根、OU和账号。当绑定到根和OU时，所有子OU和子账号都继承该标签策略。账号继承的所有标签策略和直接绑定到账户上的所有标签策略，根据继承运算符最终聚合为有效标签策略。

功能介绍

标签策略管理

可以对标签策略进行创建、修改、删除、绑定、解绑等操作。系统会从一个或多个父节点（如父组织单元）继承标签策略，最后聚合为一个有效的标签策略，对子账号、子OU的资源生效。

6.2 标签策略语法

标签策略基本语法

以下标签策略显示了基本标签策略语法：

```
{
   "tags": {
      "costcenter": {                <!-- 策略键 -->
```



```
        "tag_key": {
            "@@assign": "CostCenter"                <!-- 标签键 -->
        },
        "tag_value": {
            "@@assign": [
                "100",              <!-- 策略值 -->
                "200"
            ]
        },
        "enforced_for": {               <!-- 强制执行 -->
            "@@assign": [
                "apig:instance"             <!-- 服务和资源类型 -->
            ]
        }
    }
  }
}
```

- 策略键：唯一标识策略语句的策略键。它必须与标签键的值相匹配，除了大小写处理。
- 标签键：值必须跟策略键一致，但可以有多种大小写形式。如果不指定标签键，则默认为全部小写，即便策略键有大写也会使用全部小写指定。例如策略键指定为costcenter，标签键指定为CostCenter，则后续检验规则以CostCenter为准；策略键指定为CostCenter，标签键不指定，则后续校验规则以costcenter为准。
- 策略值：一个或多个可接受标签值的列表。如果标签策略没有为标签键指定标签值，则任何值（包括没有值）都将视为合规。
- 强制执行：表示阻止对指定服务和资源执行任何不合规标记操作。如未指定任何服务和资源类型，则此标签策略不会对任何资源生效。
- 通配符：可以在标签值和强制执行字段中使用通配符 "*"，不过必须遵循以下约束：
  - 每个标签值仅使用一个通配符。例如，允许使用 *@example.com，但不允许使用 *@*.com。
  - 对于强制执行，可以用“<service>:*”对该服务的所有资源启用强制执行。但是不能使用通配符指定所有服务或指定所有服务的某个资源。

继承运算符

在标签策略样例中，标签键，标签值和强制执行中使用了"@@assign"标识，该标识即为继承运算符。

继承运算符指定标签策略如何与组织树中的其他标签策略合并，以创建账号的有效标签策略。运算符包括值设置运算符和子控制运算符。

- **值设置运算符**

  您可以使用以下值设置运算符来控制策略与其父策略交互的方式：

表 6-1 值设置运算符

运算符	说明
@@assign	用指定设置覆盖任何继承的策略设置。如果未继承指定的设置，则此运算符会将该设置添加到有效策略中。此运算符可以应用于任何类型的任何策略设置。 对于单值设置，此运算符将继承的值替换为指定值。 对于多值设置（JSON数组），此运算符将删除所有继承的值，并将其替换为此策略指定的值。
@@append	向继承的设置添加指定的设置（而不删除任何设置）。如果未继承指定的设置，则此运算符会将该设置添加到有效策略中。只能将此运算符用于多值设置。 此运算符将指定的值添加到继承数组中的任何值。
@@remove	从有效策略中删除指定的继承设置（如果存在）。只能将此运算符用于多值设置。 此运算符仅从继承自父策略的值数组中删除指定值。其他值可以继续存在于数组中，并且可由子策略继承。

- **子控制运算符**

  默认情况下，允许所有运算符 (@@all)。

  - "@@operators_allowed_for_child_policies":["@@all"]表示：子OU和账号可以在策略中使用任何运算符。默认情况下，子策略中允许使用所有运算符。
  - "@@operators_allowed_for_child_policies":["@@assign", "@@append", "@@remove"]表示：子OU和账号只能在子策略中使用指定的运算符。您可以在此子控制运算符中指定一个或多个值设置运算符。
  - "@@operators_allowed_for_child_policies":["@@none"]表示：子OU和账号不能在策略中使用运算符。可以使用此运算符有效锁定在父策略中定义的值，以使子策略无法添加、追加或删除这些值。

6.3 启用和禁用标签策略

只有组织管理账号才可以启用或禁用标签策略，委托管理员无法执行此操作。

启用标签策略

在创建标签策略并将其附加到组织单元和账号之前，必须先启用标签策略，且只能使用组织的管理账号启用标签策略。

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入策略管理页，单击标签策略操作列的“启用”。

图 6-1 启用标签策略

步骤3 在弹窗中勾选确认框，然后单击“确定”，完成标签策略功能启用。

----结束

禁用标签策略

如果您不想再使用标签策略管理组织的标签规则，可以禁用标签策略，但只有组织的管理账号才可以禁用标签策略。

⚠ 注意

- 禁用标签策略后，所有标签策略会自动从组织中的所有实体解绑，包括所有OU和账号，但是策略本身不会被删除。
- 若禁用标签策略后再重新启用标签策略，实体与其他标签策略的绑定关系将丢失，如需恢复则需要管理账号重新绑定。

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入策略管理页，单击标签策略操作列的“禁用”。

图 6-2 禁用标签策略

步骤3 在弹窗中单击“确定”，完成标签策略禁用。

----结束

6.4 创建标签策略

当您需要对组织中的标签进行标准化管理时，可以通过创建标签策略来制定标签创建的规则。

只有组织管理员才可以创建标签策略，委托管理员无法执行此操作。

操作步骤

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入策略管理页，单击“标签策略”，进入标签策略页面。

图 6-3 进入标签策略管理页

步骤3 单击“创建”，进入创建标签策略页面。

步骤4 编辑策略名称。系统会自动生成策略名称，您可根据需要自行修改。但请注意，新创建策略的名称不能与已有策略名称重复。

（可选）输入策略描述。

步骤5 编辑策略内容，目前支持通过“可视化编辑器”和“JSON”两种方式进行编辑。

- 可视化编辑器：通过可视化编辑器编辑策略内容，无需了解JSON语法，编辑完成后可自动生成策略。具体步骤如下：

  a. 输入标签策略定义的标签的键。

  b. 指定标签键的大小写形式。

  勾选此项则表示使用标签键的大小写形式进行校验，如不勾选则表示使用标签键的全小写形式，即便标签键有大写也会使用全部小写进行校验。例如标签键为CostCenter，勾选此项后，后续检验规则以CostCenter为准；不勾选此项，则后续校验规则以costcenter为准。

  c. 指定标签键的允许值。

  勾选此项后单击“添加值”，为标签键指定的一个或多个允许值，表示此标签键仅允许使用此处指定的值，否则为不合规。如不勾选此项或勾选后未添加标签值，则此标签键使用任何值（包括没有值）都将视为合规。

  图 6-4 添加标签键的允许值

  d. 指定执行标签策略检查的资源类型。

  勾选此项后单击“添加资源类型”，在弹窗中阅读并勾选确认标签策略存在的风险说明，然后选择资源类型，单击“确定”。

  说明

  如未指定任何服务和资源类型，则此标签策略不会对任何资源生效。

图 6-5 指定策略生效的资源类型

e. 单击“添加标签键”，可在策略内容中添加多个标签键用于标签策略检查。

- JSON：通过JSON语法编辑策略内容，根据**标签策略语法**，在JSON编辑框内编写JSON格式的策略内容。编辑时系统会自动校验语法。如不正确，请根据提示进行修正。

图 6-6 使用 JSON 编辑策略

步骤6 （可选）为策略添加标签。在标签栏目下，输入标签键和标签值，单击“添加”。

图 6-7 添加标签

步骤7 单击右下角的“保存”后，如跳转到标签策略列表，则标签策略创建成功。

----结束

6.5 查看有效的标签策略

标签策略可以绑定到组织的根、OU和账号。当绑定到根和OU时，所有子OU和子账号都继承该标签策略。账号继承的所有标签策略和直接绑定到账户上的所有标签策略，根据继承运算符最终聚合为有效标签策略。

有效标签策略生效的逻辑规则如下：

- 为同层级绑定标签策略时：
  - 单值运算符：如果绑定多个标签策略，策略中@@assign运算符最早设置的策略将会生效。
  - 多值运算符：如果绑定多个标签策略，策略中@@assign运算符最早设置的策略将会生效，同时其他策略的@@append和@@remove运算符依然生效。
- 为上下层级绑定标签策略时：

  当上下层标签策略中的标签键相同时，策略将从上层依次向下层进行计算，计算时根据子控制运算符的不同类型来判断生效，最终形成一个有效的标签策略；当上下层标签策略中的标签键不同时，上下层策略将直接合并为一个有效的标签策略。

本章为您介绍如何在控制台上查看绑定在组织的根、OU和账号上的有效标签策略。

操作步骤

步骤1 进入**组织管理控制台**，进入组织管理页面。

步骤2 单击选中组织的根、OU或账号，组织结构树右侧即可展示详细信息。

步骤3 在右侧详细信息下，选择“策略”页签。

步骤4 展开“标签策略”列表，单击列表上方的“查看有效标签策略”，在JSON视图查看有效标签策略内容。

图 6-8 查看有效标签策略

----结束

6.6 修改和删除标签策略

本章为您介绍如何修改和删除已创建的标签策略。

只有组织管理员才可以修改或删除标签策略，委托管理员无法执行此操作。

修改标签策略

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入策略管理页，单击“标签策略”，进入标签策略列表。

步骤3 单击标签策略操作列的“编辑”，进入编辑标签策略页面。

图 6-9 编辑标签策略

步骤4 可根据需要修改“策略名称”和“策略描述”。

步骤5 按需修改策略内容。可通过“可视化编辑器”和“JSON”两种方式进行修改。

步骤6 单击右下角“保存”后，如跳转到标签策略列表，则标签策略修改成功。

----结束

删除标签策略

如果当前标签策略已与组织单元或账号绑定，则无法删除。组织单元或账号解绑该标签策略后，才可顺利删除。

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入策略管理页，单击“标签策略”，进入标签策略列表。

步骤3 单击标签策略操作列的“删除”。

步骤4 在弹窗中单击“确定”，完成标签策略删除。

图 6-10 删除标签策略

----结束

6.7 绑定和解绑标签策略

管理账号可以为根、OU和账号绑定和解绑标签策略。

约束与限制

- 一个账号最多可以绑定10个标签策略。
- 只有组织管理员才可以绑定或解绑标签策略，委托管理员无法执行此操作。
- 标签策略完成绑定后将在30分钟内生效。

绑定标签策略

方式一：

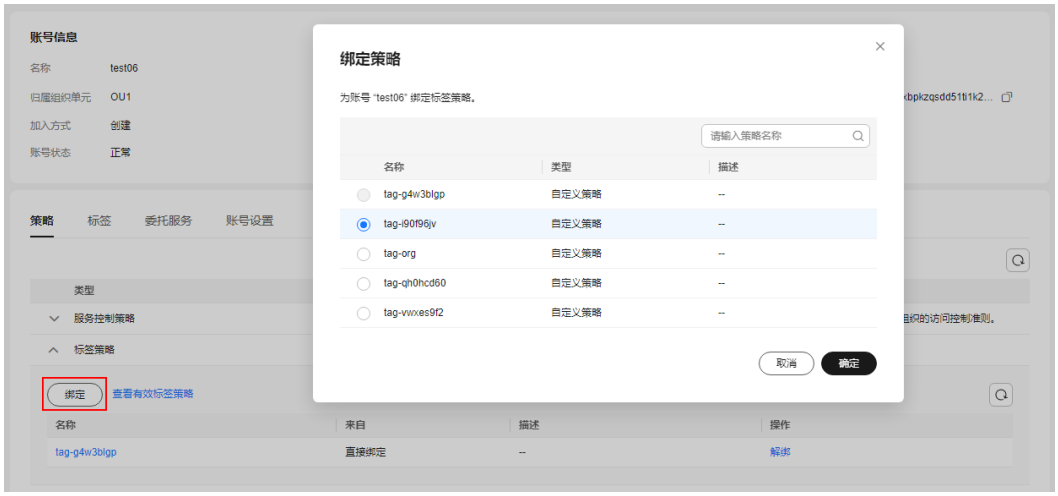
步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要绑定标签策略的OU或者账号。

步骤3 在右侧详情页，选择策略页签。展开“标签策略”列表，单击列表上方的“绑定”。

步骤4 在弹窗中选择要添加的策略后，单击“确定”，完成策略绑定。

图 6-11 绑定标签策略



----结束

方式二：

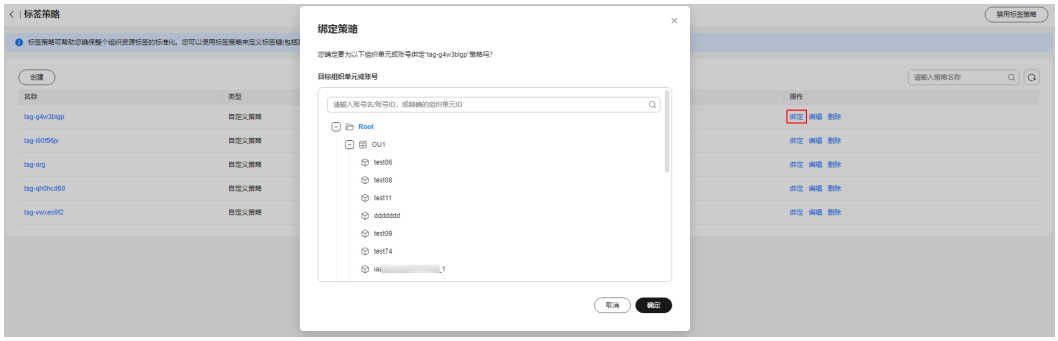
步骤1 在**组织管理控制台**，进入策略管理页。

步骤2 单击“标签策略”，进入标签策略列表。

步骤3 单击标签策略操作列的“绑定”，选中要绑定标签策略的OU或者账号。

步骤4 单击“确定”，完成策略绑定。

图 6-12 绑定标签策略



----结束

解绑标签策略

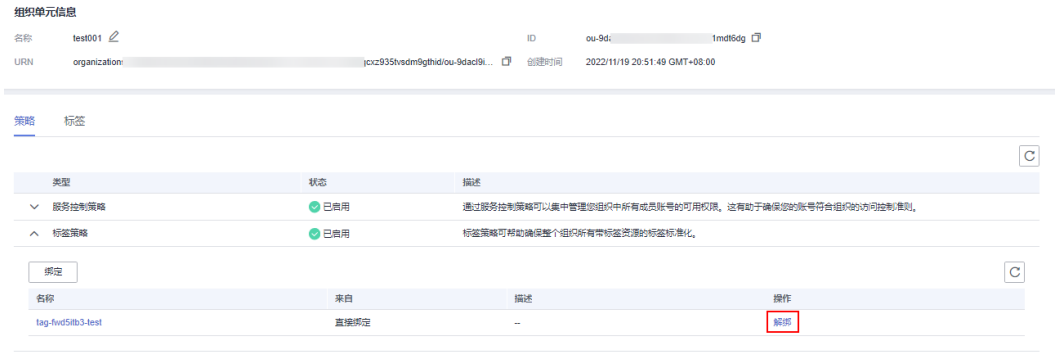
方式一：

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要解绑标签策略的OU或者账号。

步骤3 在右侧详情页，选策略页签，展开“标签策略”列表，在列表中单击要解绑的标签策略操作列的“解绑”。

图 6-13 解绑标签策略



步骤4 在弹窗中单击“解绑”，完成策略解绑。

----结束

方式二：

步骤1 在组织管理控制台，进入策略管理页。

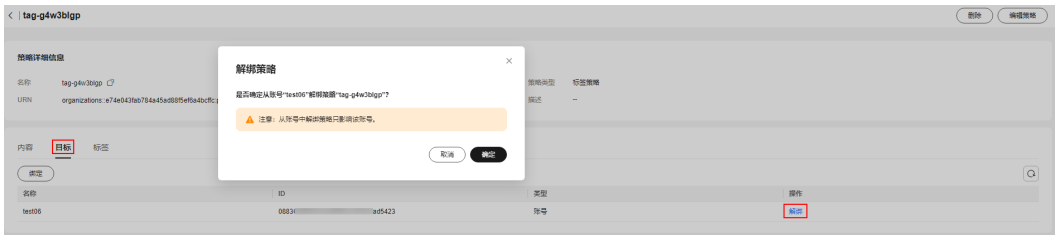
步骤2 单击“标签策略”，进入标签策略列表。

步骤3 单击标签策略的名称，选择“目标”页签。

步骤4 单击需要解绑的OU或账号操作列的“解绑”。

步骤5 单击“确定”，完成策略解绑。

图 6-14 解绑标签策略



----结束

6.8 支持标签策略的云服务

当前支持使用标签策略的云服务和资源类型如下表所示：

表 6-2 支持标签策略的云服务和资源类型

服务名称	资源类型
DDoS原生基础防护服务（Anti-DDoS）	公网IP（ip）
DDoS防护服务（AAD）	实例（instance）
应用运维管理（AOM）	告警规则（alarmRule）
API网关（APIG）	实例（instance）
弹性伸缩（AS）	弹性伸缩组（scalingGroup）
裸金属服务器（BMS）	实例（instance）
云堡垒机（CBH）	实例（instance）
云备份（CBR）	存储库（vault）
云连接（CC）	• 带宽包（bandwidthPackage） • 中心网络（centralNetwork） • 云连接（cloudConnection）
云容器引擎（CCE）	集群（cluster）
云容器实例 CCI	命名空间（namespace）
内容分发网络（CDN）	域名（domain）

服务名称	资源类型
云监控服务（CES）	告警规则（alarm）
云防火墙（CFW）	实例（instance）
DDoS原生高级防护（CNAD）	防护包（package）
微服务引擎（CSE）	引擎（engine）
云凭据管理服务（CSMS）	凭据（secret）
云搜索服务（CSS）	• 集群（cluster） • 日志流（logstream） • 存储库（repository）
云审计服务（CTS）	追踪器（tracker）
数据治理中心（DataArts Studio）	• 实例（instance） • 工作空间（workspace）
数据库安全服务（DBSS）	审计实例（auditInstance）
云专线（DC）	• 物理连接（directconnect） • 全域接入网关（gdgw） • 链路聚合组（lag） • 虚拟网关（vgw） • 虚拟接口（vif）
分布式缓存服务（DCS）	实例（instance）
文档数据库服务（DDS）	实例名称（instanceName）
专属加密（DHSM）	硬件安全模块（hsm）
数据湖探索（DLI）	• 数据库（database） • 增强型跨源连接（edsconnection） • 弹性资源池（elasticresourcepool） • 作业（jobs） • 队列（queue） • 资源（resource）
分布式消息服务（DMS）	• Kafka实例（kafka） • RabbitMQ实例（rabbitmq） • RocketMQ实例（rocketmq）
云解析服务（DNS）	• 反向解析记录（ptr） • 域名（zone）
数据复制服务（DRS）	任务（job）
数据仓库服务（DWS）	集群（cluster）

服务名称	资源类型
弹性云服务器（ECS）	实例（instance）
弹性负载均衡（ELB）	• 监听器（listener） • 负载均衡器（loadbalancer）
企业路由器（ER）	• 连接（attachments） • 实例（instances） • 路由表（routeTables）
云硬盘（EVS）	磁盘（volume）
函数工作流（FunctionGraph）	函数（function）
全球加速（GA）	• 加速器实例（accelerator） • 监听器（listener）
云数据库 GaussDB	实例（instance）
云数据库 GaussDB(for MySQL)	实例（instance）
云数据库 GeminiDB（原 云数据库 GaussDB for NoSQL）	实例（instance）
统一身份认证服务（IAM）	• 委托（agency） • 用户（user）
镜像服务（IMS）	镜像（image）
设备接入 IoTDA	实例（instance）
密钥管理服务（KMS）	用户主密钥（cmk）
云日志服务（LTS）	• 日志接入（accessConfig） • 主机组（hostGroup） • 日志组（logGroup） • 日志流（logStream）
AI开发平台 ModelArts	• Notebook实例（notebook） • 资源池（pool） • 服务（service） • 训练作业（trainJob）
MapReduce服务（MRS）	集群（cluster）
NAT网关	• 公网NAT网关（gateway） • 私网NAT网关（privateGateway） • 中转IP（privateTransitIp） • 中转子网（transitSubnet）
对象存储服务（OBS）	桶（bucket）

服务名称	资源类型
组织（Organizations）	• 账号（account） • 组织单元（ou） • 策略（policy） • 根（root）
私有证书管理服务（PCA）	私有CA（ca）
资源访问管理（RAM）	资源共享实例（resourceShare）
云数据库（RDS）	实例 (instances)
配置审计（Config）（原 资源管理服务 RMS）	合规规则（policyAssignments）
SSL证书管理服务（SCM）	证书（cert）
安全云脑（SecMaster）	工作空间（workspace）
应用管理与运维平台（ServiceStage）	• 应用（app） • 环境（environment）
高性能弹性文件服务（SFS Turbo）	SFS Turbo（shares）
消息通知服务（SMN）	主题（topic）
虚拟私有云（VPC）	• 弹性公网IP（publicip） • 子网（subnet） • 虚拟私有云（vpc） • 网络ACL（firewall） • 安全组（securityGroup）
VPC终端节点（VPCEP）	• 终端节点服务（endpointServices） • 终端节点（endpoints）
虚拟专用网络（VPN）	• 对端网关（customerGateways） • VPN连接（vpnConnections） • VPN网关（vpnGateways）
Web应用防火墙（WAF）	高级实例（premiumlnstance）

6.9 支持标签策略的区域

当前支持使用标签策略的区域如下表所示：

表 6-3 支持标签策略的区域

区域名称	区域代码
亚太-新加坡	ap-southeast-3
亚太-曼谷	ap-southeast-2
亚太-雅加达	ap-southeast-4
华东-上海一	cn-east-3
华东-上海二	cn-east-2
中国-香港	ap-southeast-1
华北-北京一	cn-north-1
华北-北京四	cn-north-4
华南-广州	cn-south-1
华北-乌兰察布一	cn-north-9
西南-贵阳一	cn-southwest-2
华东-青岛	cn-east-5
土耳其-伊斯坦布尔	tr-west-1
非洲-约翰内斯堡	af-south-1
拉美-墨西哥城一	na-mexico-1
拉美-墨西哥城二	la-north-2
拉美-圣保罗一	sa-brazil-1
拉美-圣地亚哥	la-south-2
中东-利雅得	me-east-1

7 可信服务管理

7.1 可信服务概述

什么是可信服务

可信服务是指可与Organizations服务集成，提供组织级相关能力的华为云服务。管理账号可以在组织中开启某个云服务为可信服务。成为可信服务后，云服务可以获取组织中的组织单元及成员账号信息，并基于此信息提供组织级的管理能力。例如，开启CTS云审计为可信服务后，CTS可以获取组织单元及成员账号信息，统一为整个组织提供云审计服务，记录组织中所有账号的操作。能与组织搭配使用的云服务列表参见：**已对接组织的云服务列表**。

什么是委托管理员

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，该成员账号下的用户可以使用对应可信服务的组织级管理能力。例如，某一个成员账号成为CTS云服务的委托管理员后，可以查看所有成员账号的云审计日志。

服务关联委托

Organizations使用IAM服务的委托信任功能，使可信服务能够在您组织的成员账号中代表您执行任务。当您启用某个服务为可信服务时，该服务可以请求Organizations在其成员账号中创建服务关联委托，可信服务按需异步执行此操作。此服务关联委托具有预定义的IAM权限，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。当前支持的可信服务及其功能简介请参见：**已对接组织的可信服务**。

当您在组织中创建账号或邀请现有账号加入组织时，Organizations会在成员账号内创建服务关联委托，该委托是云服务委托，委托权限为“OrganizationsServiceLinkedAgencyPolicy”系统权限，授权范围为所有资源。仅Organizations服务本身可以承担此委托，该委托具有允许Organizations为其他云服务创建服务关联委托的权限。

说明

Organizations的SCP不会影响服务关联委托，使用服务关联委托执行的任何操作将免受SCP限制。

7.2 启用和禁用可信服务

- 组织管理员禁用某个云服务的可信访问后，此云服务便不能给成员账号创建此服务的服务关联委托。
- 组织管理员关闭组织或成员账号离开组织后，Organizations服务会清理掉本服务的服务关联委托。
- 禁用AOM可信服务前，请先在AOM界面删除多账号实例，然后再在Organizations控制台界面禁用AOM可信服务。否则多账号实例将会继续获取成员账号的指标数据。
- 禁用LTS可信服务前，请先在LTS界面删除多账号日志汇聚配置，然后再在Organizations控制台界面禁用LTS可信服务。否则多账号日志汇聚将会继续获取成员账号的日志数据。

启用可信服务

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入可信服务页，在列表中单击云服务操作列的“启用”。

步骤3 在弹窗中单击“确定”，完成可信服务启用。

图 7-1 启用可信服务

----结束

禁用可信服务

登录到组织的管理账号时，您可以禁用可信服务，步骤如下。

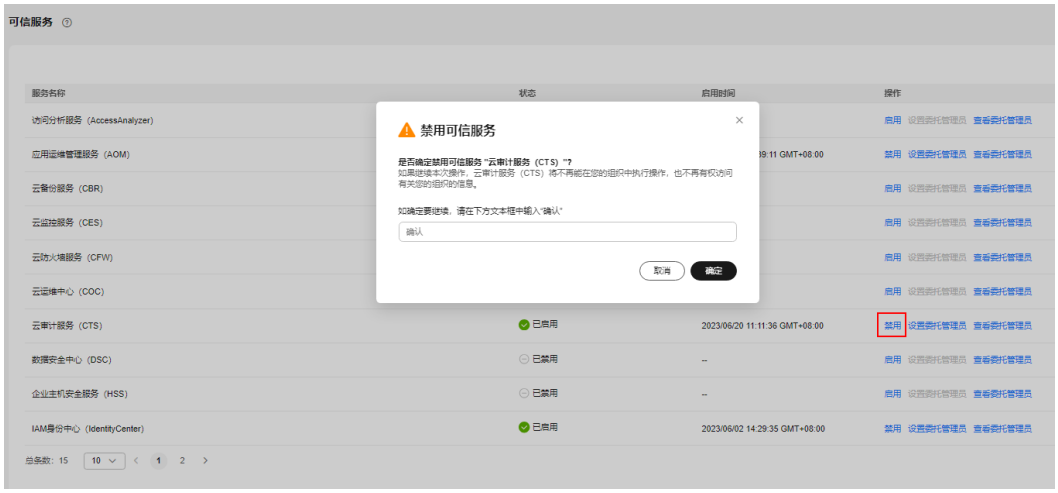
步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入可信服务页，在列表中单击云服务操作列的“禁用”。

图 7-2 禁用可信服务

步骤3 在弹窗中输入“确认”，然后单击“确定”，完成可信服务禁用。

图 7-3 禁用可信服务



----结束

7.3 已对接组织的可信服务

以组织管理员或管理账号的身份登录**组织管理控制台**，进入可信服务页，即可查看可信服务列表。

下表列出了可与华为云Organizations一起使用的云服务。

表 7-1 已对接组织的可信服务列表

服务名称	功能简介	是否支持委托管理员	最大委托管理员支持数量	相关文档
配置审计服务跨账号资源合规配置（Config）	配置审计服务支持基于组织创建合规规则、合规规则包、资源聚合器等功能，组织管理员或Config服务的委托管理员可以统一进行配置并直接作用于组织内账号状态为“正常”的成员账号中。	是	无限制	• 组织合规规则 • 组织合规规则包 • 资源聚合器
资源访问管理（RAM）	资源访问管理服务支持基于组织共享资源能力，当您的账号由组织管理时，您可以与组织内的所有账号共享资源，组织内账号无需接受邀请即可使用共享资源。	是	无限制	启用与组织共享资源
云审计服务（CTS）	云审计服务支持基于组织配置组织追踪器功能，组织管理员或CTS服务的委托管理员可以配置组织追踪器作用于整个组织，实现多账号安全审计等云审计能力。	是	无限制	组织追踪器

服务名称	功能简介	是否支持委托管理员	最大委托管理员支持数量	相关文档
应用运维管理服务（AOM）	应用运维管理服务提供多账号聚合类型Prometheus实例的创建功能。 当同组织下多个成员账号均已接入云服务指标时，组织管理员或AOM服务的委托管理员可以通过该功能统一监控同一组织下多个成员账号的云服务指标。	是	无限制	**Prometheus实例 for 多账号聚合实例**
云备份服务（CBR）	云备份服务支持基于组织的统一策略管理能力，组织管理员或CBR服务的委托管理员可以通过创建组织备份策略和组织复制策略，为组织内成员账号统一设置备份策略和复制策略。	是	无限制	**组织策略管理**
云监控服务（CES）	云监控服务支持基于组织跨账号查看我的看板功能，组织管理员或CES服务的委托管理员可以查看其组织下所有账号的看板。	是	无限制	**跨账号查看我的看板**

服务名称	功能简介	是否支持委托管理员	最大委托管理员支持数量	相关文档
云防火墙服务（CFW）	云防火墙服务具备安全可靠的跨账号数据汇聚和资源访问能力，组织管理员或CFW服务的委托管理员可以对组织内所有成员账号的EIP进行统一的资产防护。	是	无限制	多账号管理
数据安全中心（DSC）	数据安全中心服务具备安全可靠的跨账号数据汇聚和资源访问能力，组织管理员或DSC服务的委托管理员可以对组织内所有成员账号进行统一的数据安全防护，而无需登录每个成员账号。	是	无限制	多账号管理
企业主机安全服务（HSS）	主机安全服务具备安全可靠的跨账号数据汇聚和资源访问能力，组织管理员或HSS服务的委托管理员可以对组织内所有成员账号进行统一的工作负载安全防护。	是	无限制	账号管理

服务名称	功能简介	是否支持委托管理员	最大委托管理员支持数量	相关文档
IAM身份中心（IdentityCenter）	IAM身份中心为用户提供基于组织的多账号统一身份管理与访问控制。可以统一管理企业中使用华为云的用户，一次性配置企业的身份管理系统与华为云的单点登录，以及所有用户对组织下账号状态为“正常”的账号的访问权限。	是	无限制	什么是IAM身份中心
云日志服务（LTS）	云日志服务联合组织服务推出多账号日志汇聚中心，组织管理员或LTS服务的委托管理员可以在LTS将组织下指定账号的日志流复制到自己的账号中，实现多账号日志的集中存储和分析，满足安全合规、集中分析等不同场景下的诉求。	是	无限制	多账号日志汇聚中心
安全云脑（SecMaster）	安全云脑支持基于组织的多账号空间托管能力，组织管理员或安全云脑服务的委托管理员创建空间托管时，可以选择组织下的一个或多个账号进行托管。	是	无限制	创建托管

服务名称	功能简介	是否支持委托管理员	最大委托管理员支持数量	相关文档
访问分析服务（AccessAnalyzer）	访问分析提供组织级的访问分析功能，组织管理员或委托管理员可以在组织内创建和管理访问分析器，用于识别组织内与外部共享的资源等。	是	1	暂无
云运维中心（COC）	云运维中心基于组织的跨账号能力，支持组织管理员或服务委托管理员在云运维中心查看其组织内成员的运维态势和资源情况，并支持对资源进行跨账号的作业任务执行。	是	1	暂无
资源编排资源栈集服务（RF）	资源编排资源栈集服务支持基于组织的多账号管理功能，组织管理员或资源编排资源栈集服务的委托管理员可以通过指定组织单元，实现对组织中多账号跨区域的资源编排，且无需手动创建部署所需委托	是	无限制	暂无

7.4 添加、查看和取消委托管理员

须知

- 取消AOM可信服务的委托管理员前，请先在AOM界面删除多账号实例，然后再在Organizations控制台界面取消AOM可信服务的委托管理员。否则多账号实例将会继续获取成员账号的指标数据。
- 取消LTS可信服务的委托管理员前，请先在LTS界面删除多账号日志汇聚配置，然后再在Organizations控制台界面取消LTS可信服务的委托管理员。否则多账号日志汇聚将会继续汇聚成员账号的日志数据。

添加委托管理员

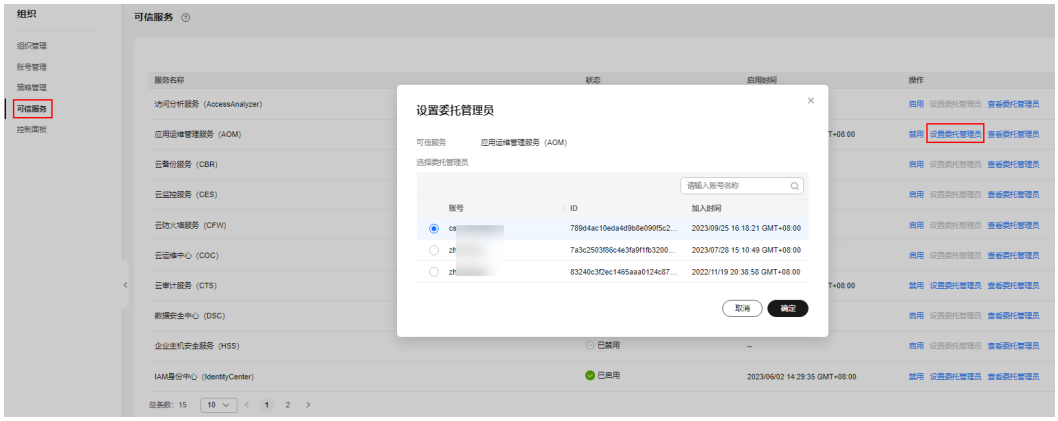
关闭中状态的账号无法设置为委托管理员。

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入可信服务页，在列表中单击云服务操作列的“设置委托管理员”。

步骤3 在弹窗中选择要设置为委托管理员的账号，单击“确定”，完成委托管理员设置。

图 7-4 设置委托管理员



----结束

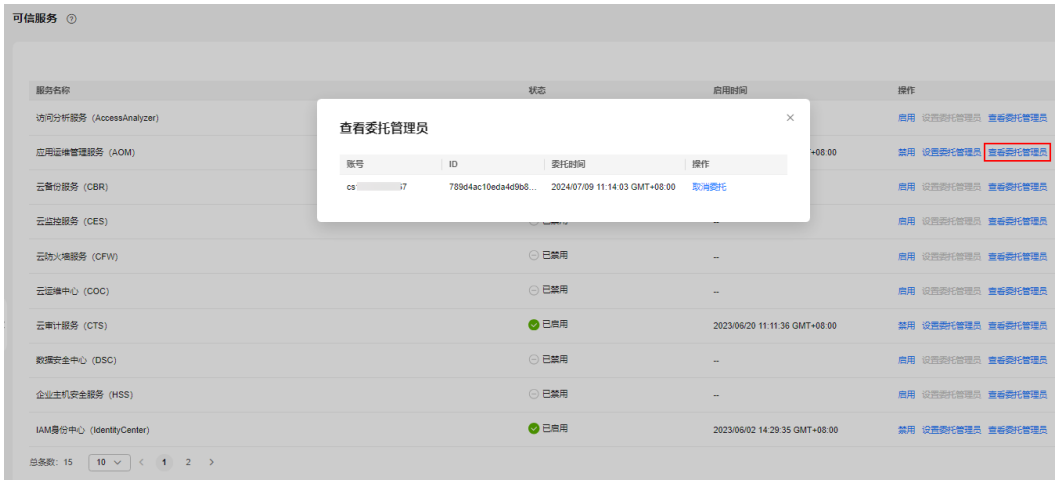
查看委托管理员

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入可信服务页，在列表中单击云服务操作列的“查看委托管理员”。

步骤3 系统将弹窗展示该云服务的委托管理员信息。

图 7-5 查看委托管理员



----结束

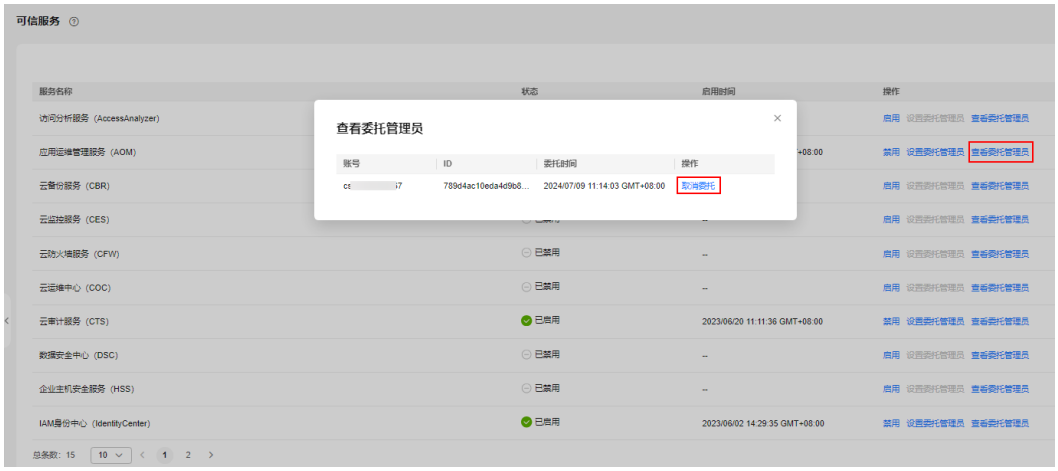
取消委托管理员

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入可信服务页，在列表中单击云服务操作列的“查看委托管理员”。

步骤3 在弹窗中单击委托管理员操作列的“取消委托”。

图 7-6 取消委托管理员



步骤4 在弹窗中单击“确定”，完成取消委托管理员操作。

----结束

8 标签管理

8.1 标签概述

标签简介

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。您可以向以下组织资源添加标签：

- 组织的根
- 组织单元（Organizational Unit，以下简称OU）
- 账号
- 服务控制策略（Service Control Policy，以下简称SCP）
- 标签策略

您可以在以下时间添加标签：

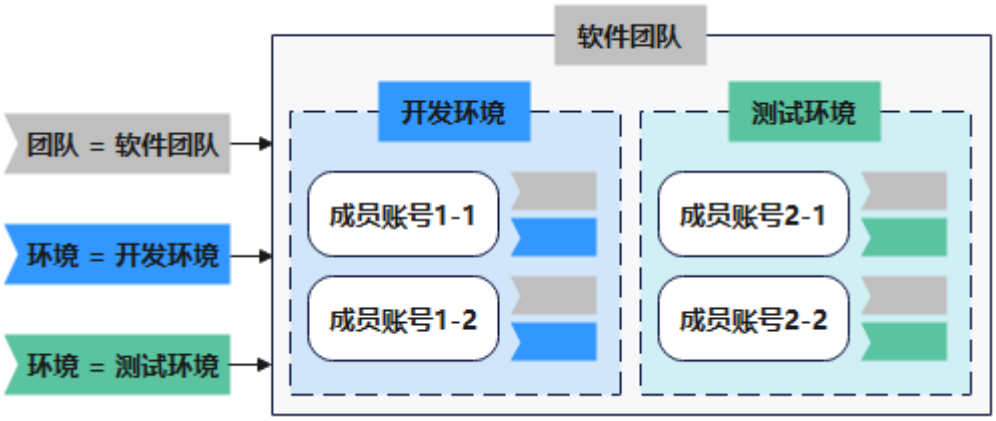
- 在创建OU、账号、SCP和标签策略时，可以添加标签。
- 根、OU、账号、SCP和标签策略创建完成后，可以在各自的详情页面添加、修改、查看、删除标签。

标签的基本知识

标签用于标识资源，当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类。

标签的工作方式如图8-1所示。在此示例中，您为每个组织成员账号分配了两个标签，每个标签都包含您定义的一个“键”和一个“值”，一个标签使用键为“团队”，另一个使用键为“环境”，每个标签都拥有相关的值。

图 8-1 标签示例



您可以根据为云资源添加的标签快速搜索和筛选特定的云资源。例如，您可以为账号中的资源定义一组标签，以跟踪每个云资源的所有者和用途，使资源管理变得更加轻松高效。

标签的使用约束

- 每个标签由“标签键”和“标签值”组成，“标签键”和“标签值”的命名规则如下：

  “标签键”：
  - 不能为空。
  - 长度为1~128个字符。
  - 由英文字母、数字、下划线、中划线、UNICODE字符（\u4E00-\u9FFF）组成。

  “标签值”：
  - 可以为空。
  - 长度为1~225个字符。
  - 由英文字母、数字、下划线、点、中划线、UNICODE字符（\u4E00-\u9FFF）组成。
- 每个云资源最多可以添加20个标签。
- 对于每个云资源，每个“标签键”都必须是唯一的，每个“标签键”只能有一个“标签值”。

本章将为您介绍如下内容：

- **添加标签**，为已有的OU、账号、SCP和标签策略添加标签。
- **修改标签**，修改OU、账号、SCP和标签策略的标签键值。
- **查看标签**，查看OU、账号、SCP和标签策略的标签。
- **删除标签**，删除OU、账号、SCP和标签策略的标签。

8.2 添加标签

添加根、OU 和账号标签

操作场景

本章节指导用户为已有的根、OU和账号添加标签。

操作步骤

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要添加标签的OU，在右侧的组织单元信息页，选择“标签”页签，单击“添加”。

步骤3 在弹窗中，输入标签键和标签值，单击“添加”，然后单击“确定”，完成标签添加。

在标签键和标签值的输入框的下拉列表中，可直接选择在TMS创建的预定义标签，具体请参见**创建预定义标签**。

图 8-2 添加标签

----结束

添加策略标签

操作场景

本章节指导用户为SCP自定义策略和标签策略添加标签。

操作步骤

为SCP自定义策略和标签策略添加标签的方法类似，以SCP为例，说明添加标签的方法。

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入策略管理页，单击“服务控制策略”，进入SCP管理页。

步骤3 在列表中单击自定义策略的名称，进入策略详情页。

步骤4 选择“标签”页签，单击“添加”。

步骤5 在弹窗中输入标签键和标签值， 单击“添加”，然后单击“确定”，完成标签添加。

在标签键和标签值的输入框的下拉列表中，可直接选择在TMS创建的预定义标签，具体请参见**创建预定义标签**。

图 8-3 添加标签

----结束

8.3 修改标签

修改根、OU 和账号标签

操作场景

本章节指导用户修改根、OU和账号的标签。

操作步骤

修改根、OU和账号标签的方法类似，以OU为例，说明修改标签的方法。

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要修改标签的OU，在右侧的组织单元信息页，选择“标签”页签，进入标签列表页面。

步骤3 在弹窗中输入新的标签值，单击“确定”，完成标签修改。

图 8-4 修改标签

----结束

修改策略标签

操作场景

本章节指导用户修改SCP自定义策略和标签策略的标签。

操作步骤

修改SCP自定义策略和标签策略标签的方法类似，以SCP为例，说明修改标签的方法。

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

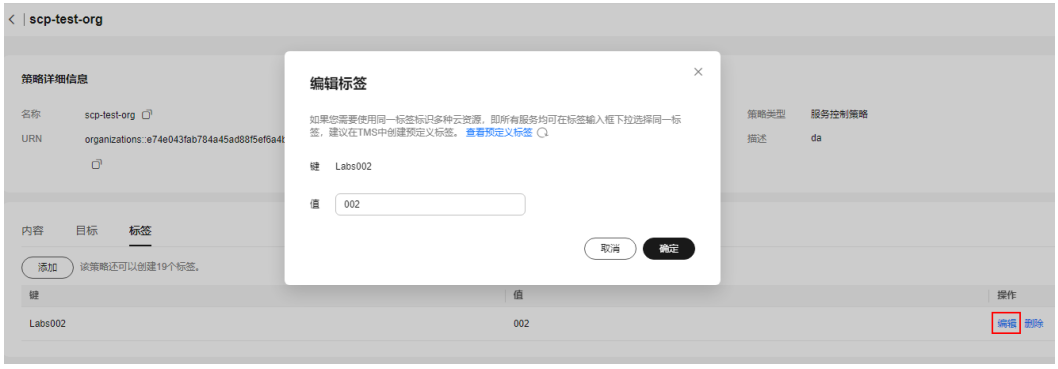
步骤2 进入策略管理页，单击服务控制策略，进入SCP管理页。

步骤3 在列表中单击自定义策略的名称，进入策略详情页。

步骤4 选择标签页签，单击要修改标签操作列的“编辑”。

步骤5 在弹窗中输入修改后标签值， 单击“确定”，完成标签修改。

图 8-5 修改标签



----结束

8.4 查看标签

查看根、OU 和账号标签

操作场景

本章节指导用户查看根、OU和账号的标签。

操作步骤

查看根、OU和账号标签的方法类似，以OU为例，说明查看标签的方法。

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要查看标签的OU，在右侧的组织单元信息页，选择“标签”页签，进入标签列表页面。

步骤3 在标签列表中，可查看此组织单元已添加的全部标签信息。

----结束

查看策略标签

操作场景

本章节指导用户查看SCP自定义策略和标签策略的标签。

操作步骤

查看SCP自定义策略和标签策略标签的方法类似，以SCP为例，说明查看标签的方法。

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入策略管理页，单击服务控制策略，进入SCP管理页。

步骤3 在列表中单击自定义策略的名称，进入策略详情页。

步骤4 选择“标签”页签，可查看此SCP已添加的全部标签信息。

----结束

8.5 删除标签

删除根、OU 和账号标签

操作场景

本章节指导用户删除根、OU和账号的标签。

操作步骤

删除根、OU和账号标签的方法类似，以OU为例，说明删除标签的方法。

步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要删除标签的OU，在右侧的组织单元信息页，选择“标签”页签。

步骤3 单击要删除标签操作列的“删除”，在弹窗中选择“确定”，完成标签删除。

图 8-6 删除标签

----结束

删除策略标签

操作场景

本章节指导用户删除SCP自定义策略和标签策略的标签。

操作步骤

删除SCP自定义策略和标签策略标签的方法类似，以SCP为例，说明删除标签的方法。

步骤1 以组织管理员或管理账号的身份登录**组织管理控制台**。

步骤2 进入策略管理页，单击服务控制策略，进入SCP管理页。

步骤3 在列表中单击自定义策略的名称，进入策略详情页。

步骤4 选择“标签”页签，单击要修改标签操作列的“删除”。

步骤5 在弹窗中单击“确定”，完成标签删除。

图 8-7 删除标签

----结束

9 使用 CTS 审计组织操作事件

9.1 支持审计的关键操作

通过云审计服务，您可以记录与组织云服务相关的操作事件，便于日后的查询、审计和回溯。

表 9-1 云审计支持的 Organizations 操作列表

操作名称	资源类型	事件名称
创建组织	organization	createOrganization
查询所属组织信息	organization	showOrganization
关闭组织	organization	deleteOrganization
退出组织	organization	leaveOrganization
列出组织的根	root	listRoots
创建组织单元	organizationUnit	createOrganizationalUnit
列出组织单元	organizationUnit	listOrganizationalUnits
查询有关组织单元的信息	organizationUnit	showOrganizationalUnit
修改组织单元	organizationUnit	updateOrganizationalUnit
删除组织单元	organizationUnit	deleteOrganizationalUnit
邀请账号	account	inviteAccount
创建账号	account	createAccount
创建账号	account	createAccountV2
关闭账号	account	closeAccount
更新账号	account	updateAccount

操作名称	资源类型	事件名称
移动账号	account	moveAccount
移除账号	account	removeAccount
列出组织中的账号	account	listAccounts
查询账号信息	account	showAccount
列出创建账号的状态	accountStatus	listCreateAccountStatuses
查询有关创建账号状态的信息	accountStatus	showCreateAccountStatus
列出关闭账号的状态	accountStatus	listCloseAccountStatuses
接受邀请	handshake	acceptHandshake
拒绝邀请	handshake	declineHandshake
取消邀请	handshake	cancelHandshake
查询邀请相关信息	handshake	showHandshake
列出收到的邀请	handshake	listReceivedHandshakes
列出发送的邀请	handshake	listHandshakes
启用可信服务	trustedService	enableTrustedService
禁用可信服务	trustedService	disableTrustedService
列出组织的可信服务列表	trustedService	listTrustedServices
设置委托管理员	delegatedAdministrator	registerDelegatedAdministrator
取消委托管理员	delegatedAdministrator	deregisterDelegatedAdministrator
列出指定账号是其委托管理员的服务	delegatedAdministrator	listDelegatedServices
列出此组织中指定为委托管理员的账号	delegatedAdministrator	listDelegatedAdministrators
创建策略	policy	createPolicy
修改策略	policy	updatePolicy
删除策略	policy	deletePolicy
列出策略	policy	listPolicies
查询策略相关信息	policy	showPolicy
启用策略类型	policy	enablePolicyType

操作名称	资源类型	事件名称
禁用策略类型	policy	disablePolicyType
查询组织策略的dry run的配置	policy	showDryRunConfig
更新组织策略的dry run的配置	policy	updateDryRunConfig
创建dry run策略	policy	createDryRunPolicy
列出dry run策略	policy	listDryRunPolicies
查询dry run策略相关信息	policy	showDryRunPolicy
更新dry run策略相关信息	policy	updateDryRunPolicy
删除dry run策略相关信息	policy	deleteDryRunPolicy
绑定策略	policy	attachPolicy
解绑策略	policy	detachPolicy
将dry run策略跟实体绑定	policy	attachDryRunPolicy
将dry run策略跟实体解绑	policy	detachDryRunPolicy
列出跟指定策略绑定的所有实体	policy	listEntitiesForPolicy
列出跟指定dry run策略绑定的所有实体	policy	listEntitiesForDryRunPolicy
查询有效的策略	policy	showEffectivePolicies
添加标签	• account • organizationUnit • policy • root • tag	tagResource
删除标签	• account • organizationUnit • policy • root • tag	untagResource
列出绑定到指定资源的标签	• account • organizationUnit • policy • root • tag	listTagsForResource

操作名称	资源类型	事件名称
列出组织中的根、组织单元和账号	entity	listEntities
列出所有可以与组织服务集成的云服务	service	listServices
列出被添加到标签策略强制执行的资源类型	policy	listTagPolicyServices
列出绑定到指定资源的标签	• account • organizationUnit • policy • root • tag	listTagResources
为指定资源添加标签	• account • organizationUnit • policy • root • tag	createTagResource
从指定资源中删除指定主键标签	• account • organizationUnit • policy • root • tag	deleteTagResource
根据资源类型及标签信息查询实例列表	resourceInstance	listResourceInstances
根据资源类型及标签信息查询实例数量	resourceCount	showResourceInstancesCount
查询项目标签	tag	listResourceTags
列出租户的组织配额	quota	listQuotas

9.2 在 CTS 事件列表查看云审计事件

场景描述

云审计服务能够为您提供云服务资源的操作记录，记录的信息包括发起操作的用户身份、IP地址、具体的操作内容的信息，以及操作返回的响应信息。根据这些操作记录，您可以很方便地实现安全审计、问题跟踪、资源定位，帮助您更好地规划和利用已有资源、甄别违规或高危操作。

什么是事件

事件即云审计服务追踪并保存的云服务资源的操作日志，操作包括用户对云服务资源新增、修改、删除等操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。

什么是管理类追踪器和数据类追踪器

管理追踪器会自动识别并关联当前用户所使用的所有云服务，并将当前用户的所有操作记录在该追踪器中。管理追踪器记录的是管理类事件，即用户对云服务资源新建、修改、删除等操作事件。

数据追踪器会记录用户对OBS桶中的数据操作的详细信息。数据类追踪器记录的是数据类事件，即OBS服务上报的用户对OBS桶中数据的操作事件，例如上传数据、下载数据等。

约束与限制

- 管理类追踪器未开启组织功能之前，单账号跟踪的事件可以通过云审计控制台查询。管理类追踪器开启组织功能之后，多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。组织追踪器的详细介绍请参见**组织追踪器概述**。
- 用户通过云审计控制台只能查询最近7天的操作记录，过期自动删除，不支持人工删除。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务（OBS）或云日志服务（LTS），才可在OBS桶或LTS日志流里面查看历史事件信息。否则，您将无法追溯7天以前的操作记录。
- 用户对云服务资源做出创建、修改、删除等操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。

前提条件

1. **注册华为云并实名认证。**

   如果您已有一个华为账户，请跳到下一个任务。如果您还没有华为账户，请参考以下步骤创建。

   a. 打开**华为云官网**，单击“注册”。

   b. 根据提示信息完成注册，详细操作请参见**注册华为账号并开通华为云**。

   注册成功后，系统会自动跳转至您的个人信息界面。

   c. 参考**实名认证**完成个人或企业账号实名认证。

2. **为用户添加操作权限。**

   如果您是以主账号登录华为云，请跳到下一个任务。

   如果您是以IAM用户登录华为云，需要联系CTS管理员（主账号或admin用户组中的用户）对IAM用户授予CTS FullAccess权限。授权方法请参见**给IAM用户授权**。

查看审计事件

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 CTS 新版事件列表查看审计事件

步骤1 登录CTS控制台。

步骤2 单击左侧导航栏的“事件列表”，进入事件列表信息页面。

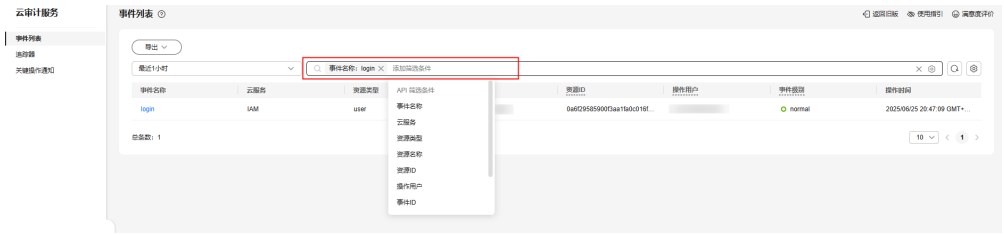
步骤3 在列表上方，可以通过筛选时间范围，查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

步骤4 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件。

表 9-2 事件筛选参数说明

参数名称	说明
是否只读	下拉选项包含“是”、“否”，只可选择其中一项。 • 是：筛选只读操作事件，例如查询资源操作。当用户在“配置中心”页面开启了只读事件上报后，并触发了只读事件，才支持选择该选项。 • 否：筛选非只读操作事件，例如创建资源操作、修改资源操作、删除资源操作。
事件名称	操作事件的名称。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 各个云服务支持审计的操作事件的名称请参见支持审计的服务及详细操作列表。 示例：updateAlarm
云服务	云服务的名称缩写。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 示例：IAM
资源名称	操作事件涉及的云资源名称。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。 示例：ecs-name
资源ID	操作事件涉及的云资源ID。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 当该资源类型无资源ID或资源创建失败时，该字段为空。 示例：*{虚拟机ID}*
事件ID	操作事件日志上报到CTS后，查看事件中的trace_id参数值。 输入的值需全字符匹配，不支持模糊匹配模式。 示例：01d18a1b-56ee-11f0-ac81-******1e229

参数名称	说明
资源类型	操作事件涉及的资源类型。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 各个云服务的资源类型请参见**支持审计的服务及详细操作列表**。 示例：user
操作用户	触发事件的操作用户。 下拉选项中选择一个或多个操作用户。 查看事件中的trace_type的值为“SystemAction”时，表示本次操作由服务内部触发，该条事件对应的操作用户可能为空。 IAM身份与操作用户对应关系，以及操作用户名称的格式说明，请参见**IAM身份与操作用户对应关系**。
事件级别	下拉选项包含“normal”、“warning”、“incident”，只可选择其中一项。 ● normal代表操作成功。 ● warning代表操作失败。 ● incident代表比操作失败更严重的情况，如引起其他故障等。
企业项目ID	资源所在的企业项目ID。 查看企业项目ID的方式：在EPS服务控制台的“项目管理”页面，可以查看企业项目ID。 示例：b305ea24-c930-4922-b4b9-******1eb2
访问密钥ID	访问密钥ID，包含临时访问凭证和永久访问密钥。 查看访问密钥ID的方式：在控制台右上方，用户名下拉选项中，选择“我的凭证 > 访问密钥”，可以查看访问密钥ID。 示例：HSTAB47V9V*******TLN9



步骤5 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。

- 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
- 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx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。
- 单击按钮，可以自定义事件列表的展示信息。启用表格内容折行开关，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。

步骤6 （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

----结束

在 CTS 旧版事件列表查看审计事件

步骤1 登录**CTS控制台**。

步骤2 单击左侧导航栏的“事件列表”，进入事件列表信息页面。

步骤3 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。

步骤4 在页面右上方，可以通过筛选时间范围，查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

步骤5 事件列表支持通过筛选来查询对应的操作事件。

表 9-3 事件筛选参数说明

参数名称	说明
事件类型	事件类型分为“管理事件”和“数据事件”。 • 管理类事件，即用户对云服务资源新建、修改、删除等操作事件。 • 数据类事件，即OBS服务上报的OBS桶中的数据的操作事件，例如上传数据、下载数据等。
云服务	在下拉选项中，选择触发操作事件的云服务名称。
资源类型	在下拉选项中，选择操作事件涉及的资源类型。 各个云服务的资源类型请参见**支持审计的服务及详细操作列表**。
操作用户	触发事件的操作用户。 下拉选项中选择一个或多个操作用户。 查看事件中的trace_type的值为“SystemAction”时，表示本次操作由服务内部触发，该条事件对应的操作用户可能为空。 IAM身份与操作用户对应关系，以及操作用户名称的格式说明，请参见**IAM身份与操作用户对应关系**。
事件级别	可选项包含“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。 • Normal代表操作成功。 • Warning代表操作失败。 • Incident代表比操作失败更严重的情况，如引起其他故障等。

步骤6 选择完查询条件后，单击“查询”。

步骤7 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。

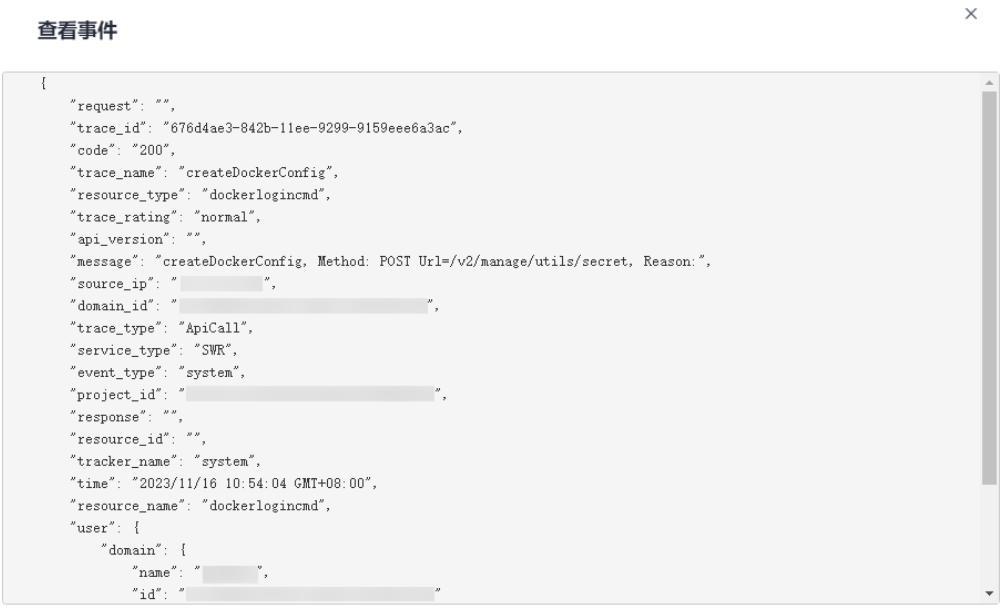
- 单击按钮，可以获取到事件操作记录的最新信息。

步骤8 在事件的“是否篡改”列中，您可以查看该事件是否被篡改：

- 上报的审计日志没有被篡改，显示“否”；
- 上报的审计日志被篡改，显示“是”。

步骤9 在需要查看的事件左侧，单击 展开该记录的详细信息。

步骤10 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。



步骤11 （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

----结束

相关文档

- 关于事件结构的关键字段详解，请参见**事件结构**和**事件样例**。
- 您可以通过以下示例，来学习如何查询具体的事件：
  - 使用云审计服务，审计最近两周内云硬盘服务的创建和删除操作。具体操作，请参见**安全审计**。
  - 使用云审计服务，定位现网某个弹性云服务器在某日上午发生的故障，以及定位现网创建弹性云服务器操作失败的问题。具体操作，请参见**问题定位**。

- 使用云审计服务，查看某个弹性云服务器的所有的操作记录。具体操作，请参见**资源跟踪**。

10 调整配额

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组织单元、邀请多少成员账号等。

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。

怎样查看我的配额?

1. 登录华为云控制台。
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。

   图 10-1 我的配额

3. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
   如果当前配额不能满足业务要求，请参考后续操作，申请扩大配额。

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。

图 10-2 我的配额

3. 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”。