组织

用户指南

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 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2个IAM用户，1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。

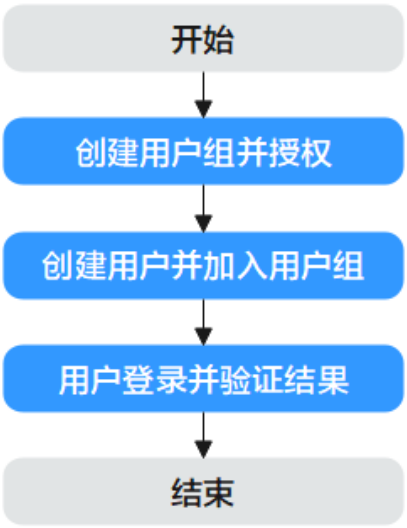
前提条件

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 给用户授予组织管理权限流程



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：

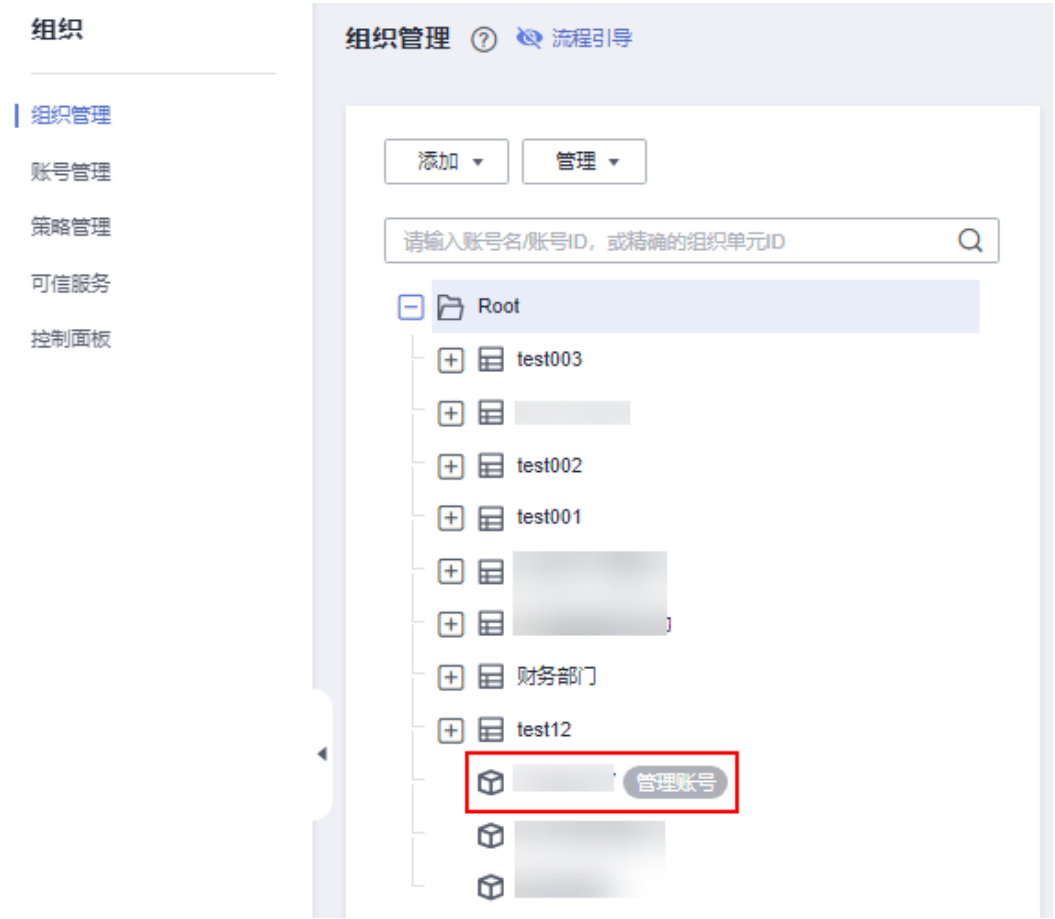
步骤1 登录华为云，进入华为云Organizations控制台。

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。

图 2-2 创建组织并成为管理账号



----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华为云，进入华为云Organizations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 2-3 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华为云，进入华为云Organizations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

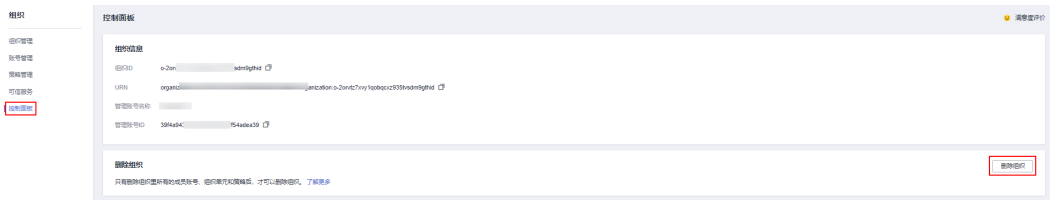
- **对管理账号的影响**
  - 管理账号将成为独立账号。您可以继续将此账号作为独立账号使用，也可以使用它创建不同的组织，它也可以作为成员账号接受其他组织的邀请。
  - 组织的管理账号从来不受服务控制策略（SCP）的影响，所以组织删除后，管理账号及管理账号的IAM用户权限没有任何更改。
- **对成员账号的影响**
  - 成员账号将成为独立账号。您可以继续将它作为独立账号使用，也可以使用它创建不同的组织，它也可以作为成员账号接受其他组织的邀请。
  - 删除组织后，组织的成员账号将不再受到服务控制策略（SCP）的影响，成员账号及成员账号的IAM用户权限可能会发生改变。
- **对策略的影响**
  - 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华为云，进入华为云Organizations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 2-4 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、子公司或者项目族等。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，然后单击“确定”，完成OU创建。

----结束

3.3 修改 OU

您可以在Organizations控制台，实现对OU的重命名、修改附加标签和附加策略。

本章节包含如下内容：

- **重命名OU**
- **修改OU标签**
- **修改OU策略**

重命名 OU

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

修改 OU 标签

- **添加OU标签**

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，选择“标签”页签，单击“添加”。

图 3-3 添加组织单元标签

步骤3 在弹窗中，填写标签键和标签值，单击“添加”。可重复本步骤添加多个标签，已添加的标签总数不能超过20个。

步骤4 单击“确定”，完成标签添加。

----结束

- **删除OU标签**

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，选择“标签”页签。

步骤3 单击标签操作列的“删除”，在弹窗中单击“确定”，完成标签删除。

图 3-4 删除标签

----结束

- **修改OU标签键值**

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，选择“标签”页签。

步骤3 单击标签操作列的“编辑”，在弹窗中填写新的标签值，单击“确定”完成标签的修改。

图 3-5 修改标签

----结束

修改 OU 策略

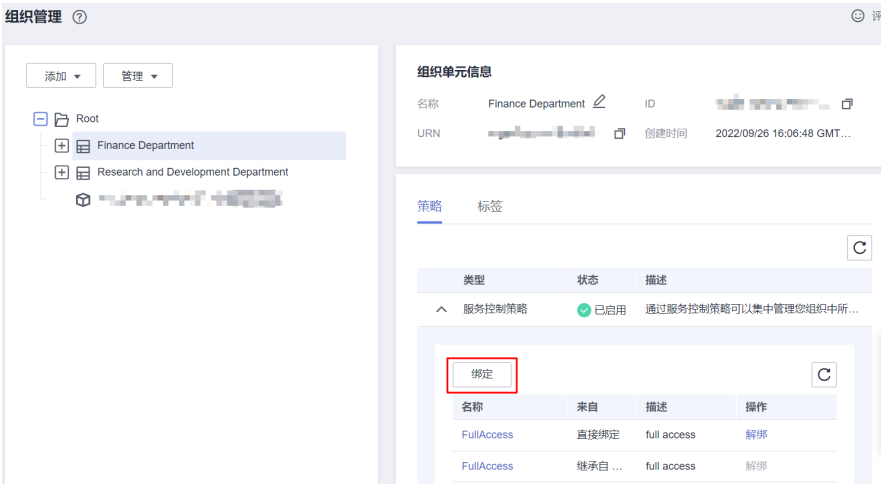
- **绑定策略**

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，选择“策略”页签。

步骤3 选择要修改的策略类型，此处以“服务控制策略”为例，单击服务控制策略前方的 ，展开策略列表，单击“绑定”。

图 3-6 绑定策略



步骤4 在弹窗中选择要添加的策略，单击“绑定”，完成策略绑定。

图 3-7 完成绑定

----结束

- **解绑策略**

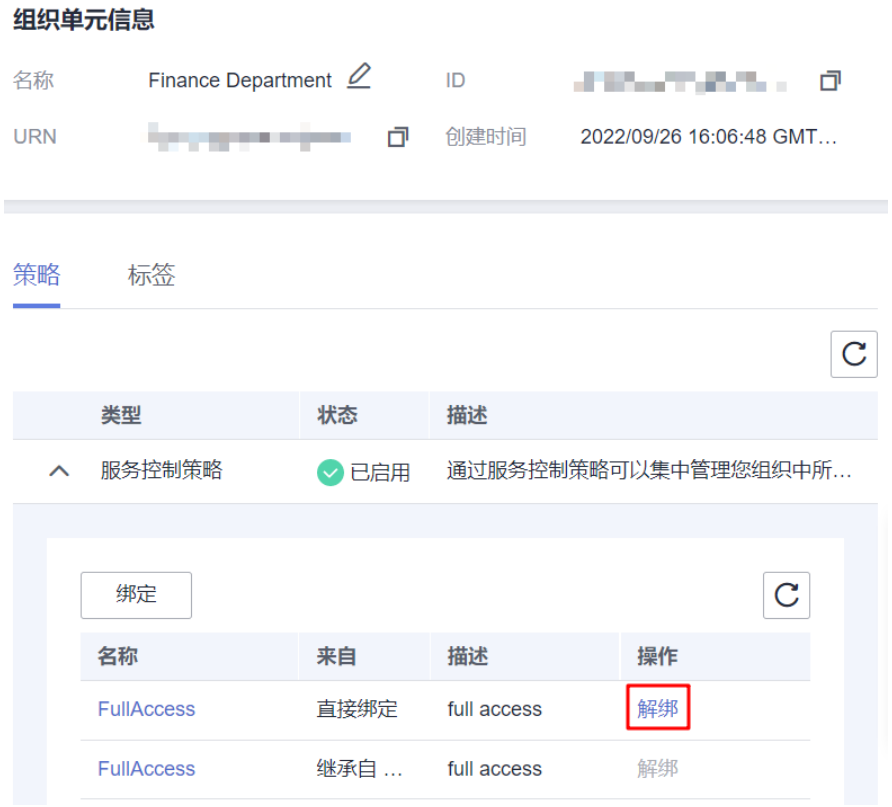
步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要修改的OU，在右侧的组织单元信息页，选择“策略”页签。

步骤3 选择要修改的策略类型，此处以“服务控制策略”为例，单击服务控制策略前方的 ，展开策略列表。

步骤4 单击要解绑策略操作列的“解绑”，在弹窗中单击“确定”，完成策略解绑。

图 3-8 解绑策略



----结束

3.4 查看 OU 详细信息

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。

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 3-9 查看组织单元详细信息

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 3-10 删除 OU

----结束

4 账号管理

4.1 账号概述

组织中的账号

组织中的账号是标准的华为账号或华为云账号，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。
- **创建账号**，管理账号可在组织中直接创建新账号。
- **关闭账号**，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。

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，如需调整请参考企业中心文档。

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“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ID。

如何获取账号ID参见：获取账号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华为云，进入华为云Organizations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华为云，进入华为云Organizations控制台。

步骤2 此时界面会向你展示邀请列表。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 查看邀请

----结束

4.3 创建账号

组织的管理账号可在组织中直接创建新账号加入组织。

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。
- 创建账号时绑定的邮箱不可以与其他账号重复。
- 新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。
- 当前创建成功的账号不支持移除，请谨慎操作。
- 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，如需调整请参考企业中心文档。

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 输入账号名称和电子邮箱。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

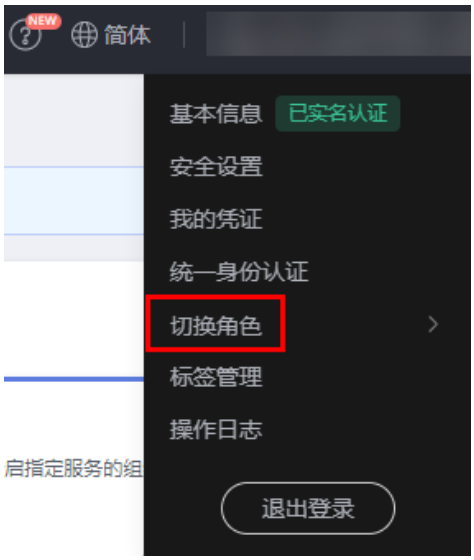
步骤6 单击“确定”，创建成功的账号将会显示在列表中。

----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“切换角色”。

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。
- 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。可以同时关闭最多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。

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，并输入账号名称。

步骤4 单击“确定”，完成账号关闭。

----结束

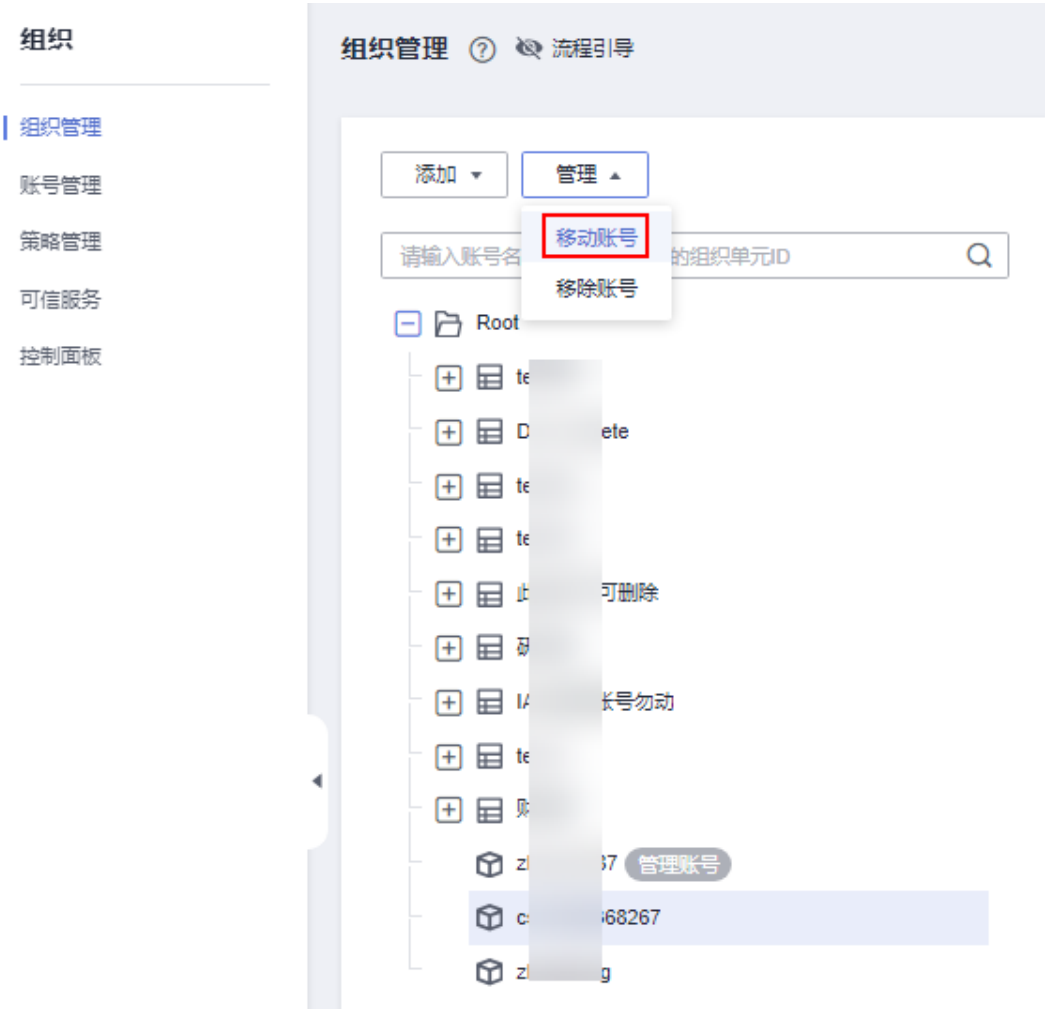
4.5 移动成员账号

登录到管理账号后，您可以移动成员账号，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 移动成员账号



步骤3 在弹窗中选中要移动的目标组织单元，单击“确定”，完成账号移动。

----结束

4.6 查看账号详细信息

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。

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，和绑定的策略、标签、委托服务。

图 4-11 查看账号详情

4.7 移除成员账号

移除须知

移除账号之前，您需要了解以下内容：

- 要移除的账号不能是组织任何可信服务的委托管理员账号。如果该账号是委托管理员，则必须先将账号从委托管理员账号更改为普通账号后，才能移除该账号。有关如何禁用或更改委托管理员账号的更多信息，请参见**添加、查看和取消委托管理员**。
- 当某个成员账号离开组织后，该账号不再有权访问其属于该组织时的数据。但是，组织的管理账号仍可以访问这些数据。如果该成员账号重新加入组织，则其将可以再次访问这些数据。
- 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。
- 被移除的成员账号不再受组织内的任何策略影响。这意味着，服务控制策略施加的权限限制将不再影响该账号，该账号中的IAM用户可能比之前拥有更多权限。
- 仅通过邀请方式加入组织的成员账号可以被移除和主动退出组织，通过组织云服务创建的账号无法被移除，也无法主动退出组织。

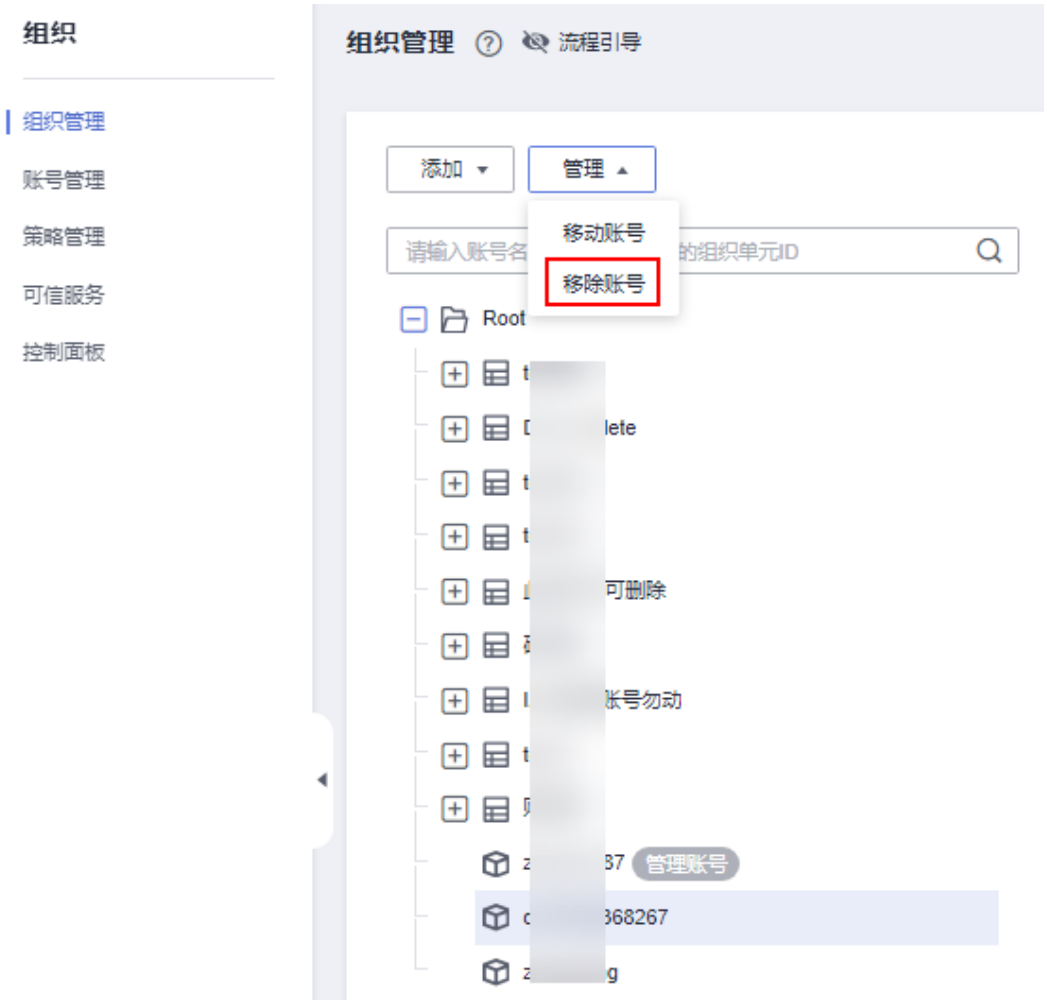
移除账号

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 在弹窗中单击“确定”，完成账号移除。

----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**。

要退出组织的成员账号不能是任何可信服务的委托管理员账号。如果该账号是委托管理员，则需先取消其委托管理员身份，具体请参见**添加、查看和取消委托管理员**。

步骤1 以成员账号的身份登录华为云，进入华为云Organizations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”，在弹窗中选择“退出”，完成退出组织操作。

图 4-13 退出组织

----结束

4.8 查看账号记录

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华为云，进入华为云Organizations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。

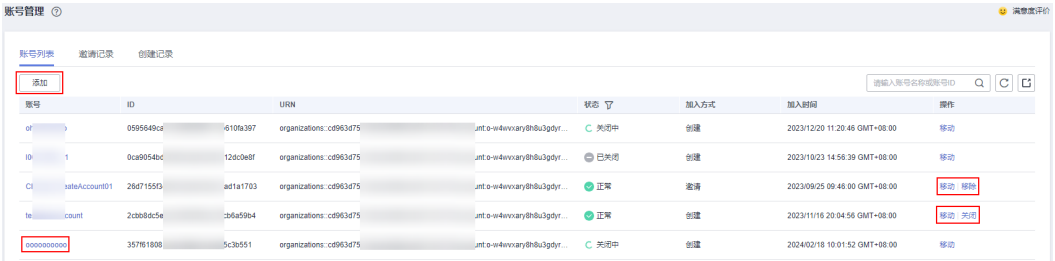
步骤3 在列表中单击账号名，可查看账号的详细信息。

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可执行移动和移除操作，在组织中创建的账号可执行移动和关闭操作。

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 4-14 账号相关操作



----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华为云，进入华为云Organizations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 4-15 取消邀请和邀请账号

----结束

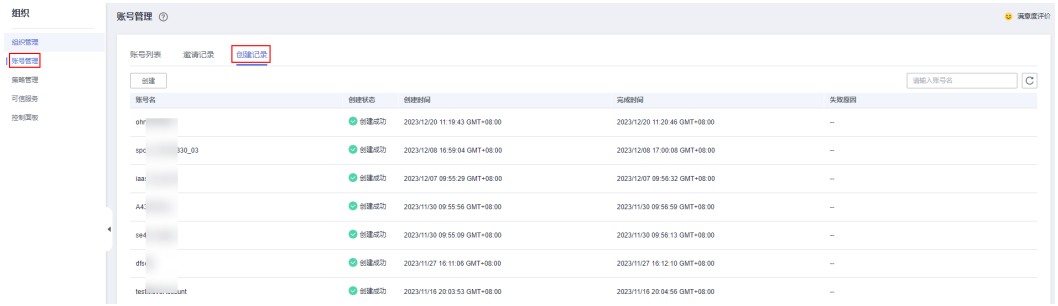
查看创建记录

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

图 4-16 查看账号创建记录



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 创建账号

----结束

5 服务控制策略管理

5.1 服务控制策略介绍

5.1.1 服务控制策略概述

概述

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、OU和成员账号。当服务策略关联到组织或OU时，该组织或OU下所有账号受到该策略影响。

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“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的云服务和区域请参见：**支持SCP的云服务**和**支持SCP的区域**。
- 通过API方式获取Token后，使用该Token访问支持SCP的云服务的API，将不受SCP限制。

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。如需查看所有云服务的华为云系统策略，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。

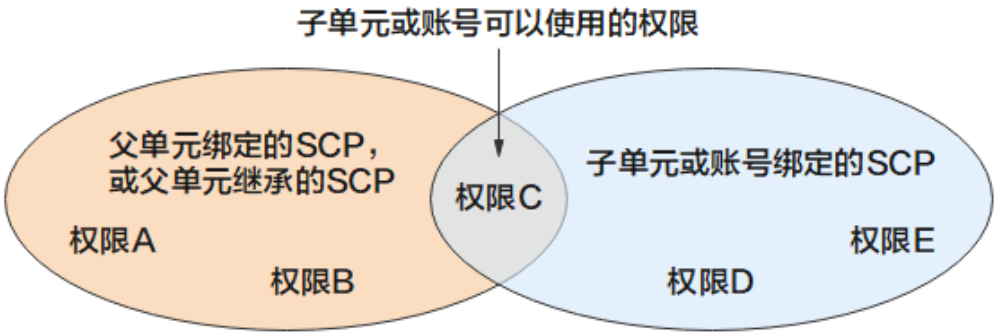
- **交集有效**

  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。

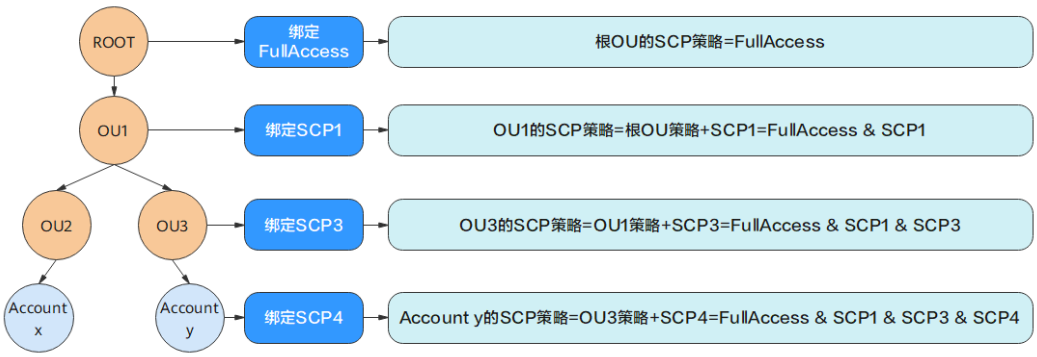
图 5-1 SCP 原理图



- **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。策略中的显式Deny始终优先于Allow。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。
- 添加允许策略。添加允许策略并删除默认附加到每个OU和账号的FullAccess SCP后，除非策略中明确允许，否则任何OU和账号都不允许任何操作权限。要允许使用某个云服务的操作，必须创建SCP并将它们附加到账号及其层级之上的每个OU，直至附加到根组织单元为止（包括根组织单元）。层次结构中的每个SCP（从根组织单元开始）必须明确允许在OU及其下面的账号中使用该操作。SCP中的显式Allow会覆盖隐式Deny。

- **拒绝优先**

  当组织单元和账号绑定多条SCP时，账号权限优先遵从拒绝语句。比如成员账号A同时绑定了两条SCP，分别是允许全部操作和禁止查看账单操作。此时执行查看账单操作，鉴权规则会优先遵从拒绝操作，即成员账号A不能查看账单。详细说明请参考**显式拒绝和隐式拒绝的区别**。

- **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

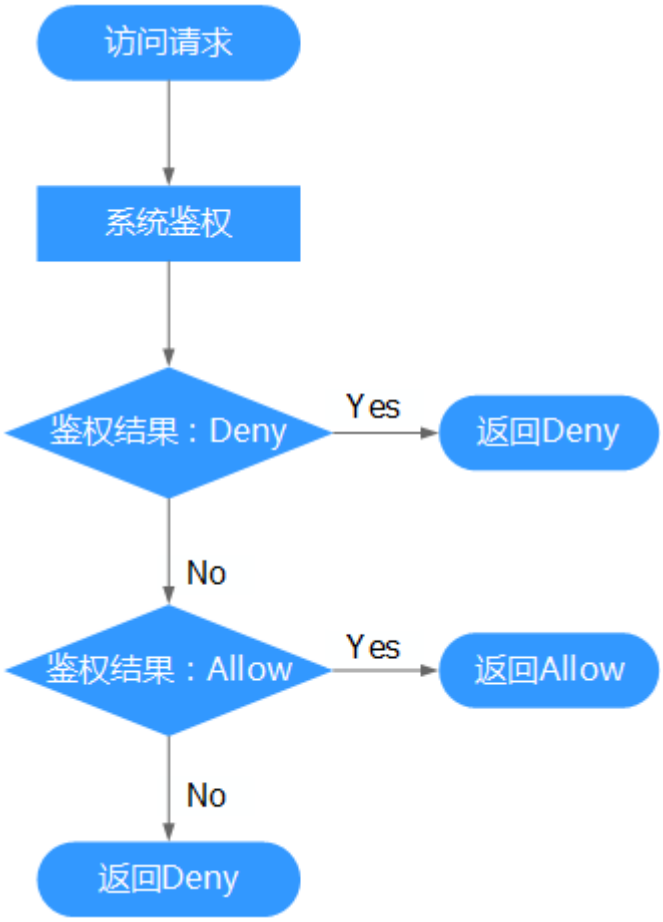
Effect（效果）包含两种：Allow（允许）和Deny（拒绝），分别表示允许或拒绝执行某操作的权限。

当没有策略设置权限为Allow和Deny时，默认情况即为Deny权限，称为隐式拒绝。当有策略授权Allow权限，且没有其他策略Deny该权限时，Allow的权限才能生效。

如果策略设置权限为Deny，则为显式拒绝。显式的Deny始终优先于Allow。例如，父OU的SCP，它允许权限A、B和C，但是子OU的SCP允许权限A、B，拒绝权限C，则该子OU的账号以及以下层级的账号，均无法使用权限C。

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",
```

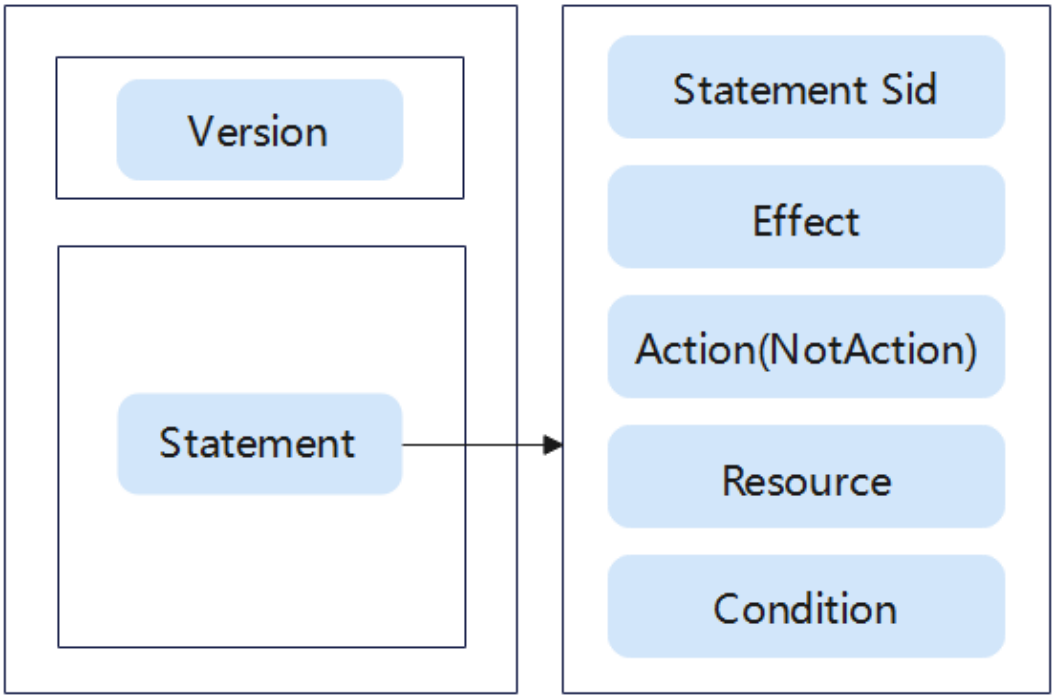


```
        "Jack"
      ]
    }
  }
 }
]
}
```

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。

参数		是否必选	含义	值
	Effect：作用	必选	定义Action中的操作权限是否允许执行。	• Allow：允许执行。 • Deny：不允许执行。 **说明** • 当同一个Action的Effect既有Allow又有Deny时，遵循Deny优先的原则。 • 当Effect为Allow时，不能有Condition元素。
	Action：授权项	Allow时必选。 Deny时与NotAction二选一。	操作权限。	格式为“服务名:资源类型:操作”。授权项支持通配符号*，通配符号*表示所有。 参数中的通配符*和?只能单独使用或放在字符串结尾处。它不能出现在字符串的开头或中间部分。 例如"obs:bucket:ListAllMybuckets"：表示查看OBS桶列表权限，其中obs为服务名，bucket为资源类型，ListAllMybuckets为操作。
	NotAction	Allow时不可选。 Deny时与Action二选一。	Deny时，NotAction列出的操作或服务不受当前策略影响，即除了NotAction列表中的操作之外，其他操作deny。	格式同Action。
	Condition：条件	Allow时不可选。	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":["specialCharactor"]}：表示当用户输入的用户名以"specialCharactor"结尾时该条statement生效。

参数		是否必选	含义	值
	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。	Allow时，只能为“*”。 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： • "obs:*:*:bucket:*": 表示所有的OBS桶。 • "obs:*:*:object:my-bucket/my-object/*": 表示my-bucket桶my-object目录下的所有对象。

说明

SCP中不支持以下元素：

- Principal
- NotPrincipal
- NotResource

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。

- 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，组织将自动获取并鉴权。详情请参见：**通用全局条件键**。
- 服务级条件键（前缀为服务缩写，如rms:）仅适用于对应服务的操作。详情请参见**SCP授权参考**中各服务支持的服务级条件键。

表 5-2 通用全局条件键

全局条件键	类型	说明
g:CalledVia	字符串	用于控制跨服务访问。示例参见1。
g:CalledViaFirst	字符串	与g:CalledVia相同，特指g:CalledVia属性中的第一个元素。
g:CalledViaLast	字符串	g:CalledVia相同，该属性特指g:CalledVia属性中的最后一个元素。
g:CurrentTime	时间	接收到鉴权请求的时间。以ISO 8601格式表示，例如：2023-11-11T23:59:59Z。示例参见2。

全局条件键	类型	说明
g:DomainName	字符串	请求者的账号名称。
g:DomainId	字符串	请求者的账号ID。
g:MFAPresent	布尔值	是否使用MFA多因素认证方式获取Token。
g:MFAAge	数值	通过MFA多因素认证方式获取的Token的生效时长。该条件需要和g:MFAPresent一起使用。
g:PrincipalAccount	字符串	与g:DomainId属性完全一致。
g:PrincipalUrn	字符串	请求者身份的URN。不同身份类型的URN格式如下： IAM用户：iam::<domain-id>:user:<user-name> IAM委托：sts::<domain-id>:assumed-agency:<agency-name>/<session-name>
g:PrincipalIsRootUser	布尔值	指请求者身份是否是IAM根用户。所有请求中都会携带该属性。
g:PrincipalIsService	布尔值	指请求者身份是否是云服务，可以通过该属性控制只有云服务身份才能访问指定API。
g:PrincipalOrgId	字符串	指请求者身份所属的组织ID，用户可以通过该属性控制只有特定组织内的身份才能访问指定API。示例参见3。
g:PrincipalOrgManagementAccountId	字符串	请求者身份所属组织的管理账号ID。示例参见4。
g:PrincipalOrgPath	字符串	请求者账号所属组织中的路径，可以通过该属性控制只有组织中特定层级的账号才能访问指定API。示例参见5。一个账号的组织路径的格式如下： <organization-id>/<root-id>/(<ou-id>/)*<account-id>
g:PrincipalServiceName	字符串	请求者的云服务Service Principal名称。示例参见6。
g:PrincipalTag/tag-key	字符串	请求者身份携带的标签，目前仅有STSToken支持的session tag可以作为该属性。
g:PrincipalType	字符串	请求者的身份类型，共有两种类型：User、AssumedAgency。当以长期IAM凭据访问时，该属性取值为User；当以IAM临时凭据访问时，取值为AssumedAgency。
g:Referer	字符串	请求携带的HTTP referer header，注意由于该属性是由客户端指定的，故不推荐使用它作为访问控制的安全依赖。

全局条件键	类型	说明
g:RequestedRegion	字符串	请求的目标区域。如请求的目标云服务是全局服务时，需要设置为NULL；如请求的目标云服务是区域级服务时，则设置为对应的区域ID即可，例如cn-north-4。示例参见7。
g:RequestTag/tag-key	字符串	请求中携带的标签。示例参见8。
g:ResourceAccount	字符串	请求所访问的资源的所属主账号ID。
g:ResourceOrgId	字符串	请求所访问的资源的所属主账号所在的组织ID。示例参见9。
g:ResourceOrgPath	字符串	请求所访问的资源的所属主账号在组织中的路径。示例参见10。
g:ResourceTag/tag-key	字符串	请求所访问的资源身上携带的标签。用户可以通过该属性控制只能访问带有特定标签的资源。示例参见11。
g:SecureTransport	布尔值	请求是否使用了SSL协议。
g:SourceAccount	字符串	指跨服务访问场景下，云服务是为哪一个资源所发起的请求，g:SourceAccount表示的是该资源的所属主账号。
g:SourceUrn	字符串	指跨服务访问场景下，云服务是为哪一个资源所发起的请求，g:SourceUrn表示的是该资源URN。
g:SourceIdentity	字符串	特指IAM临时凭据STSToken中的source_identity字段。source_identity字段在用户第一次通过STS服务的AssumeAgency API获取IAM临时凭据时指定，且在后续的委托切换中不可再更改。
g:SourceIp	IP	发起请求的源IP地址，专指来自公网的请求源IP。注意：如果请求是从VPC内的ECS发起并经过VPC Endpoint时，则会使用g:VpcSourceIp来取代g:SourceIp。示例参见12。
g:SourceVpc	字符串	请求来源的VPC ID。
g:SourceVpce	字符串	发起请求使用的VPC Endpoint ID。
g:TagKeys	字符串	指请求中携带的所有标签的key组成的列表。
g:TokenIssueTime	时间	指访问凭据中的STSToken的签发时间。
g:UserAgent	字符串	指请求携带的HTTP User-Agent header，注意该属性是由客户端指定的，故不推荐使用它作为访问控制的安全依赖。
g:PrincipalId	字符串	指请求者的身份ID，不同身份类型的ID格式如下： IAM 用户：<user-id> IAM 委托：<agency-id>:<session-name>

全局条件键	类型	说明
g:UserName	字符串	IAM用户名。
g:UserId	字符串	IAM用户ID。
g:ViaService	布尔值	指该请求是否是由云服务通过Impersonate协议代表用户身份发起的，当且仅当g:CalledVia属性非空时，该属性值为true。
g:VpcSourceIp	IP	指从VPC内发起的请求的源IP地址。
g:EnterpriseProjectId	字符串	指该请求对应的企业项目ID或者请求操作的资源所属的企业项目ID。

1. **g:CalledVia**

   示例：表示不允许通过Console服务发起的请求调用RAM服务的查询资源共享接口。

   ```
   {
       "Version": "5.0",
       "Statement": [
           {
               "Effect": "Deny",
               "Action": ["ram:resourceShares:search"],
               "Resource": ["*"],
               "Condition": {
                   "ForAnyValue:StringEquals": {
                       "g:CalledVia": "service.Console"
                   }
               }
           }
       ]
   }
   ```

2. **g:CurrentTime**

   示例：表示用户通过该属性控制云服务API在2023年3月1日到2023年3月30日的时间段内禁止被访问。

   ```
   {
       "Version": "5.0",
       "Statement": [
           {
               "Effect": "Deny",
               "Action": ["ram:resourceShares:search"],
               "Resource": ["*"],
               "Condition": {
                   "DateGreaterThan": {"g:CurrentTime": "2023-03-01T00:00:00Z"},
                   "DateLessThan": {"g:CurrentTime": "2023-03-30T23:59:59Z"}
               }
           }
       ]
   }
   ```

3. **g:PrincipalOrgId**

   示例：表示用户通过该属性限制在组织o-xxxxxxxxxxx中的账号不允许访问RAM服务的查询资源共享接口。

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



```
            "Action": ["ram:resourceShares:search"],
            "Resource": ["*"],
            "Condition": {
               "StringEquals": {
               "g:PrincipalOrgID": "o-xxxxxxxxxxx"

               }
            }
         }
      ]
}
```

4. **g:PrincipalOrgManagementAccountId**

   示例：表示条件键Condition在请求者所在组织的管理账号ID为ce20ec0406c844a08026399be5f13b08时返回true。

```
{
   "Condition": {
      "StringEquals": {
         "g:PrincipalOrgManagementAccountId": "ce20ec0406c844a08026399be5f13b08"
      }
   }
}
```

5. **g:PrincipalOrgPath**

   示例：表示条件键Condition在请求者账号属于组织单元ou-ab12-22222222时返回true。

```
{
   "Condition": {
      "StringMatch": {
         "g:PrincipalOrgPath": "o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/ou-ab12-22222222/*"
      }
   }
}
```

6. **g:PrincipalServiceName**

   示例：表示条件键Condition在请求者是RAM服务时返回true。

```
{
   "Condition": {
      "StringEquals": {
         "g:PrincipalServiceName": "service.RAM"
      }
   }
}
```

7. **g:RequestedRegion**

   示例：表示策略禁止用户访问华北-北京四cn-north-4区域的ECS服务API。仅当目标云服务是Region服务时，请求中才会携带该属性。

```
{
   "Version": "5.0",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": ["ecs:*:*"],
         "Resource": ["*"],
         "Condition": {
            "StringEquals": {
               "g:RequestedRegion": "cn-north-4"
            }
         }
      }
   ]
}
```

8. **g:RequestTag/tag-key**

   示例：表示策略不允许用户创建带有{"team": "engineering"}标签的资源共享实例。


```
{
   "Version": "5.0",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": ["ram:resourceShares:create"],
         "Resource": ["*"],
         "Condition": {
            "StringEquals": {
               "g:RequestTag/team": "engineering"
            }
         }
      }
   ]
}
```

9. **g:ResourceOrgId**

   示例：表示策略拒绝用户修改属于组织o-xxxxxxxx下的账号的RAM资源共享实例。仅当访问的资源所有者加入到某个组织时，才会携带该属性。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:delete",
        "ram:resourceShares:update"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "g:ResourceOrgId": "o-xxxxxxxx"
        }
      }
    }
  ]
}
```

10. **g:ResourceOrgPath**

    示例：表示策略拒绝用户修改属于组织路径o-a1b2c3d4e5/r-ab12/ou-ab12-11111111下的账号的RAM资源共享实例。仅当访问的资源所有者加入到某个组织时，才会携带该属性。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:delete",
        "ram:resourceShares:update"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringMatch": {
          "g:ResourceOrgPath": "o-a1b2c3d4e5/r-ab12/ou-ab12-11111111/*"
        }
      }
    }
  ]
}
```

11. **g:ResourceTag/tag-key**

示例：表示策略禁止用户修改带有{"team": "engineering"}标签的资源共享实例。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:delete",
        "ram:resourceShares:update"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "g:ResourceTag/team": "engineering"
        }
      }
    }
  ]
}
```

12. **g:SourceIp**

    示例：表示策略禁止源IP地址在10.27.128.0/24范围内时访问RAM服务。

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": ["ram:*:*"],
            "Resource": ["*"],
            "Condition": {
                "IpAddress": {
                    "g:SourceIp": "10.27.128.0/24"
                }
            }
        }
    ]
}
```

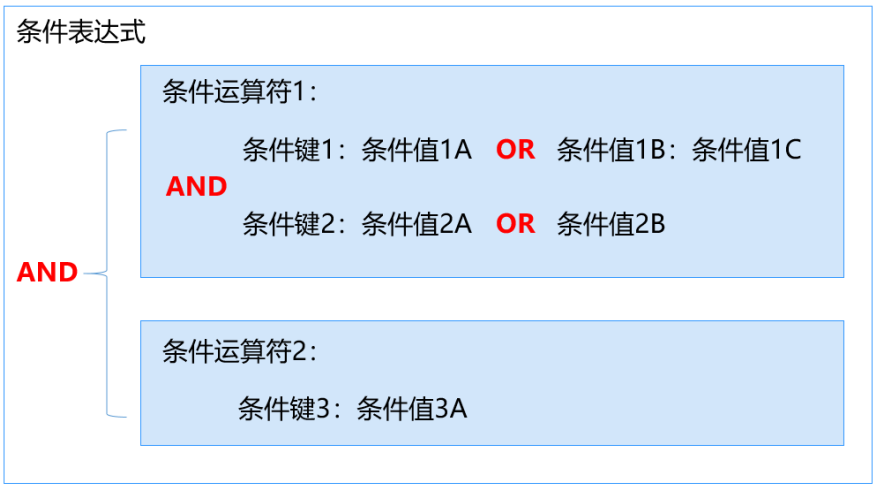
- 多值条件键

  a. （请求中的所有值）ForAllValues：测试请求集的每个成员的值是否为条件键集的子集。如果请求中的每个键值均与策略中的至少一个值匹配，则条件返回true。

  b. （请求中的任何值）ForAnyValue：测试请求值集的至少一个成员是否与条件键值集的至少一个成员匹配。如果请求中的任何一个键值与策略中的任何一个条件值匹配，则条件返回true。对于没有匹配的键或空数据集，条件返回false。

  条件键运算逻辑

图 5-5 条件键运算逻辑示意图



i. 对于同一条件键的多个条件值，采用OR运算逻辑，即请求值按照条件运算符匹配到任意一个条件值则返回true。

须知

当运算符表示否定含义的时候（例如：StringNotEquals），则请求值按照条件运算符不能匹配到所有的条件值。

ii. 同一运算符下的不同条件键之间，采用AND运算逻辑。不同运算符之间，采用AND运算逻辑。

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”，表示对应请求值为空或满足条件的请求值均使策略生效，如“StringEqualsIfExists”表示请求值为空或请求值等于条件值均使策略生效。运算符为字符串型运算符，表格中如未增加说明，不区分大小写。

- String类型

表 5-3 String 类型运算符

类型	运算符	说明
String	StringEquals	请求值与任意一个条件值相同（区分大小写）。
	StringNotEquals	请求值与所有条件值都不同（区分大小写）。
	StringEqualsIgnoreCase	请求值与任意一个条件值相同。
	StringNotEqualsIgnoreCase	请求值与所有条件值都不同。

类型	运算符	说明
	StringMatch	请求值符合任意一个条件值的正则表达式（区分大小写，正则表达式仅支持*和?）。
	StringNotMatch	请求值不符合所有条件值的正则表达式（区分大小写，正则表达式仅支持*和?）。

示例：禁止用户名为ZhangSan的请求者修改资源共享实例。

```
{
   "Version": "5.0",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": [
            "ram:resourceShares:delete",
            "ram:resourceShares:update"
         ],
         "Condition": {
            "StringEquals": {
               "g:DomainName": [
                  "ZhangSan"
               ]
            }
         }
      }
   ]
}
```

- Number类型

表 5-4 Number 类型运算符

类型	运算符	说明
Number	NumberEquals	请求值等于任意一个条件值。
	NumberNotEquals	请求值不等于所有条件值。
	NumberLessThan	请求值小于任意一个条件值。
	NumberLessThanEquals	请求值小于或等于任意一个条件值。
	NumberGreaterThan	请求值大于任意一个条件值。
	NumberGreaterThanEquals	请求值大于或等于任意一个条件值。

- Date类型

表 5-5 Date 类型运算符

类型	运算符	说明
Date	DateLessThan	请求值早于任意一个条件值。
	DateLessThanEquals	请求值早于或等于任意一个条件值。
	DateGreaterThan	请求值晚于任意一个条件值。
	DateGreaterThanEquals	请求值晚于或等于任意一个条件值。

示例：请求者禁止在2022年8月1日前访问RAM服务。

```
{
   "Version": "5.0",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": [
            "ram:*:*"
         ],
         "Condition": {
            "DateLessThan": {
               "g:CurrentTime": [
                  "2022-08-01T00:00:00Z"
               ]
            }
         }
      }
   ]
}
```

- Bool类型

表 5-6 Bool 类型运算符

类型	运算符	说明
Bool	Bool	条件值可选值：true、false。请求值等于条件值。

- Null类型

表 5-7 Null 类型运算符

类型	运算符	说明
Null	Null	条件值可选值：true、false。条件值为true，要求请求值不存在或者值为null；条件值为false，要求请求值必须存在且值不为null。

- IP类型

  表 5-8 IP 类型运算符

类型	运算符	说明
IP	IpAddress	指定IP地址或者IP范围。
	NotIpAddress	指定IP地址或者IP范围之外的所有IP地址。

  示例：拒绝IP地址在10.27.128.0到10.27.128.255范围内的请求修改指定的永久访问密钥。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "iam:credentials:updateCredentialV5"
      ],
      "Condition": {
        "IpAddress": {
          "g:SourceIp": [
            "10.27.128.0/24"
          ]
        }
      }
    }
  ]
}
```

- “IfExists”运算符后缀

  除Null运算符以外，您可以在任何条件运算符名称的末尾添加IfExists，例如：StringEqualsIfExists。如果请求的内容中存在条件键，则依照策略所述来进行匹配。如果该键不存在，则该条件元素的匹配结果将为true。

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华为云，进入华为云Organizations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”。

图 5-6 启用 SCP

步骤3 在弹窗中勾选确认框，然后单击“启用”，完成SCP功能启用。

----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华为云，进入华为云Organizations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 5-7 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

Organizations云服务支持控制台和API创建SCP，本章主要介绍控制台创建自定义策略，API创建SCP请参见：创建SCP。SCP常用示例请参见：**SCP示例**。

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。

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 5-8 进入 SCP 管理页

步骤3 单击“创建”，进入SCP创建页面。

图 5-9 创建策略

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示例**。

说明

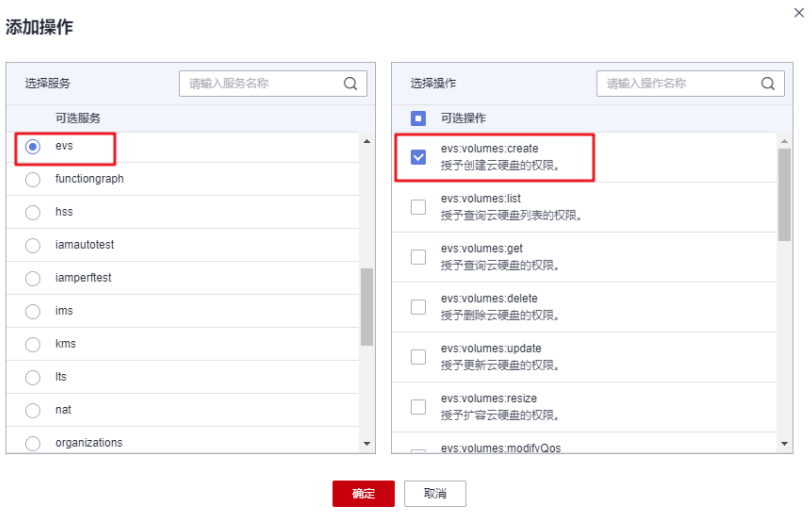
自定义策略版本号（Version）固定为5.0，不可修改。

当作用（Effect）为Allow时，不能有Condition元素，即无法添加条件键。

步骤6 在策略内容右侧可以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，可以选择服务的操作项进行添加，添加成功的操作项会自动显示在Action元素下。如**图5-10**所示。

图 5-10 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5-11**所示。

图 5-11 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5-12所示。

图 5-12 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 5-13 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 5-14 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

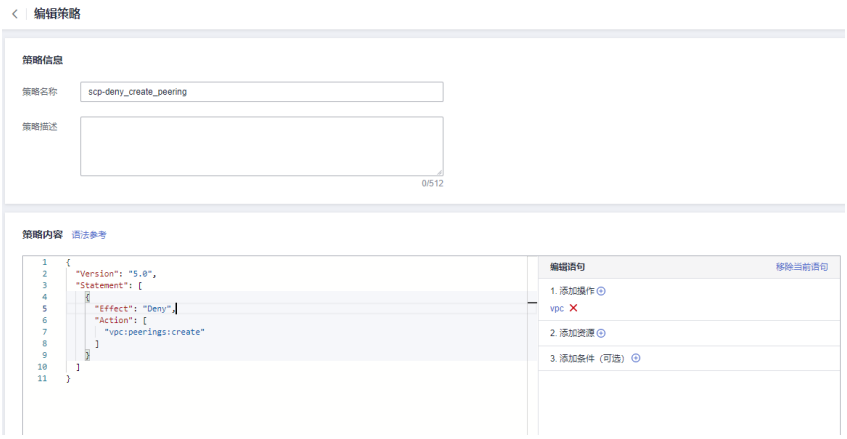
步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台。

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”。

步骤4 可根据需要修改“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华为云，进入华为云Organizations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。

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，单击“绑定”，完成策略绑定。

----结束

方式二：

步骤1 在Organizations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 单击“确定”，完成策略绑定。

----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 在弹窗中单击“确定”，完成策略解绑。

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Organizations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”。

步骤5 单击“确定”，完成策略解绑。

----结束

5.6 SCP 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**
- **禁止根用户使用除IAM之外的云服务**
- **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仅适用于项目级服务，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":"regionid1"
                }
            }
        }
    ]
}
```

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】
          ]
        }
      }
    }
  ]
}
```

禁止根用户使用除 IAM 之外的云服务

使用以下SCP禁止根用户使用除IAM之外的云服务。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "NotAction": [
        "iam:*:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "Bool": {
          "g:PrincipalIsRootUser": [
            "true"
          ]
        }
```



```
    }
   }
  ]
}
```

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 】
         ]
       }
     }
   }
  ]
}
```

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 5-9 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的各云服务相关文档中列出的授权项仅支持在SCP中使用。

表 5-10 支持 SCP 的云服务

服务名称	相关文档
标签管理服务（TMS）	**标签管理服务 TMS**
资源访问管理（RAM）	**资源访问管理 RAM**
安全令牌服务（STS）	**安全令牌服务 STS**
配置审计（Config）（原 资源管理服务 RMS）	**配置审计 Config**
组织（Organizations）	**组织 Organizations**
文档数据库服务（DDS）	**文档数据库服务 DDS**
云数据库（RDS）	**云数据库 RDS**
企业主机安全服务（HSS）	**主机安全服务 HSS**
容器镜像服务（SWR）	**容器镜像服务 SWR**
弹性公网IP（EIP）	**弹性公网IP EIP**
镜像服务（IMS）	**镜像服务 IMS**
裸金属服务（BMS）	**裸金属服务器 BMS**
消息通知服务（SMN）	**消息通知服务 SMN**
虚拟私有云（VPC）	**虚拟私有云 VPC**
弹性云服务器（ECS）	**弹性云服务器 ECS**
安全云脑（SecMaster）	**安全云脑 SecMaster**
弹性负载均衡（ELB）	**弹性负载均衡 ELB**

服务名称	相关文档
分布式缓存服务（DCS）	分布式缓存服务 DCS
NAT网关（NAT）	NAT网关 NAT
内容分发网络（CDN）	内容分发网络 CDN
云容器引擎（CCE）	云容器引擎 CCE
VPC终端节点（VPCEP）	VPC终端节点 VPCEP
云日志服务（LTS）	云日志服务 LTS
IAM身份中心（IdentityCenter）	IAM身份中心
原生基础防护（Anti-DDoS）	原生基础防护 Anti-DDoS
DDoS高防（AAD）	DDoS高防 AAD
企业项目管理服务 （EPS）	企业项目管理 EPS
SSL证书管理服务（SCM）	SSL证书管理服务 SCM
私有证书管理服务（PCA）	私有证书管理服务 PCA
统一身份认证（IAM）	统一身份认证 IAM
设备接入（IoTDA）	设备接入 IoTDA
应用管理与运维平台（Servicestage）	应用管理与运维平台 ServiceStage
资源编排服务（RFS）	资源编排服务 RFS
访问分析（AccessAnalyzer）	访问分析 IAM Access Analyzer
云审计服务（CTS）	云审计服务 CTS
云防火墙（CFW）	云防火墙 CFW
云专线（DC）	云专线 DC
流水线（CodeArts Pipeline）	流水线 Codearts Pipeline
软件开发生产线（CodeArts）	软件开发生产线 CodeArts
微服务引擎（CSE）	微服务引擎 CSE
数据湖探索（DLI）	数据湖探索 DLI

5.9 支持 SCP 的区域

当前支持使用SCP的区域如下表所示：

表 5-11 支持 SCP 的区域

区域名称	区域
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

5.10 SCP 授权参考

5.10.1 计算

5.10.1.1 弹性云服务器 ECS

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于ECS定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于ECS定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下ECS的相关操作。

表 5-12 ECS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
ecs:cloudServers:createServers	授予创建ECS云服务器的权限。	write	-	• g:RequestTag/<tag-key> • g:EnterpriseProjectId • g:TagKeys • ecs:imageID • evs:Encrypted • cbr:VaultId
ecs:cloudServers:deleteServers	授予删除ECS云服务器的权限。	write	instance *	-
ecs:cloudServers:resize	授予变更云服务器规格的权限。	write	instance *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
ecs:cloudServers:attachSharedVolume	授予批量挂载指定共享盘的权限。	write	instance *	evs:Encrypted
ecs:cloudServers:showServer	授予查询云服务器详情的权限。	read	instance *	-
ecs:cloudServers:attach	授予云服务器挂载磁盘的权限。	write	instance *	evs:Encrypted
ecs:cloudServers:showServerBlockDevice	授予查询弹性云服务器单个磁盘信息的权限。	read	instance *	-
ecs:cloudServers:updateServerBlockDevice	授予修改云服务器挂载的单个磁盘信息的权限。	write	instance *	-
ecs:cloudServers:changeOS	授予切换弹性云服务器操作系统的权限。	write	instance *	• ecs:imageID • evs:Encrypted
ecs:cloudServers:detachVolume	授予弹性云服务器卸载磁盘的权限。	write	instance *	-
ecs:cloudServers:updateMetadata	授予更新云服务器元数据的权限。	write	instance *	-
ecs:cloudServers:deleteMetadata	授予删除云服务器指定元数据的权限。	write	instance *	-
ecs:cloudServers:migrate	授予冷迁移云服务器的权限。	write	instance *	-
ecs:cloudServers:listServerInterfaces	授予查询云服务器网卡信息的权限。	list	instance *	-
ecs:cloudServers:showResetPasswordFlag	授予查询是否支持一键重置密码的权限。	read	instance *	-
ecs:cloudServers:showServerPassword	授予云服务器获取密码的权限。	read	instance *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
ecs:cloudServers:deletePassword	授予云服务器清除密码的权限。	write	instance *	-
ecs:cloudServers:listServerVolumeAttachments	授予查询弹性云服务器挂载磁盘信息的权限。	list	instance *	-
ecs:cloudServers:rebuild	授予重装弹性云服务器操作系统的权限。	write	instance *	evs:Encrypted
ecs:cloudServers:vnc	授予获取VNC远程登录地址的权限。	read	instance *	-
ecs:cloudServers:updateServer	授予修改弹性云服务器的权限。	write	instance *	-
ecs:cloudServers:addNics	授予批量添加云服务器网卡的权限。	write	instance *	-
ecs:cloudServerNics:delete	授予批量删除云服务器网卡的权限。	write	instance *	-
ecs:cloudServers:showServerTags	授予查询云服务器标签的权限。	list	instance *	-
ecs:cloudServers:batchCreateServerTags	授予批量添加云服务器标签的权限。	write	instance *	• g:RequestTag/<tag-key> • g:TagKeys
ecs:cloudServers:batchDeleteServerTags	授予批量删除云服务器标签的权限。	write	instance *	• g:RequestTag/<tag-key> • g:TagKeys
ecs:cloudServers:start	授予批量启动云服务器的权限。	write	instance *	-
ecs:cloudServers:stop	授予批量关闭云服务器的权限。	write	instance *	-
ecs:cloudServers:reboot	授予批量重启云服务器的权限。	write	instance *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
ecs:cloudServers:batchUpdateServersName	授予批量修改弹性云服务器信息的权限。	write	instance *	-
ecs:cloudServers:listServersDetails	授予查询云服务器详情列表的权限。	list	-	g:EnterpriseProjectId
ecs:cloudServerFlavors:get	授予查询云服务器规格详情和扩展信息列表的权限。	read	-	-
ecs:cloudServerQuotas:get	授予查询租户配额的权限。	read	-	-
ecs:cloudServers:resetServerPwd	授予一键重置弹性云服务器密码的权限。	write	instance *	-
ecs:cloudServers:listServerGroups	授予查询云服务器组列表的权限。	list	-	-
ecs:cloudServers:createServerGroup	授予创建云服务器组的权限。	write	-	-
ecs:cloudServers:showServerGroup	授予查询云服务器组详情的权限。	read	-	-
ecs:cloudServers:deleteServerGroup	授予删除云服务器组的权限。	write	-	-
ecs:cloudServers:addServerGroupMember	授予添加云服务器组成员的权限。	write	-	-
ecs:cloudServers:deleteServerGroupMember	授予删除云服务器组成员的权限。	write	-	-
ecs:cloudServers:listResizeFlavors	授予查询云服务器规格变更支持列表的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
ecs:cloudServers:listServerTags	授予查询项目标签的权限。	list	-	-

ECS的API通常对应着一个或多个授权项。表5-13展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-13 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1.1/{project_id}/cloudservers	ecs:cloudServers:createServers	• eip:publicIps:create • eip:publicIps:update • iam:agencies:pass
POST /v1/{project_id}/cloudservers	ecs:cloudServers:createServers	• eip:publicIps:create • eip:publicIps:update • iam:agencies:pass
POST /v1/{project_id}/cloudservers/delete	ecs:cloudServers:deleteServers	-
POST /v1.1/{project_id}/cloudservers/{server_id}/resize	ecs:cloudServers:resize	-
POST /v1/{project_id}/batchaction/attachvolumes/{volume_id}	ecs:cloudServers:attachSharedVolume	evs:volumes:use
GET /v1/{project_id}/cloudservers/{server_id}	ecs:cloudServers:showServer	-
POST /v1/{project_id}/cloudservers/{server_id}/attachvolume	ecs:cloudServers:attach	evs:volumes:use
GET /v1/{project_id}/cloudservers/{server_id}/block_device	ecs:cloudServers:listServerBlockDevices	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/cloudservers/{server_id}/block_device/{volume_id}	ecs:cloudServers:showServerBlockDevice	-
PUT /v1/{project_id}/cloudservers/{server_id}/block_device/{volume_id}	ecs:cloudServers:updateServerBlockDevice	-
POST /v1/{project_id}/cloudservers/{server_id}/changeos	ecs:cloudServers:changeOS	-
DELETE /v1/{project_id}/cloudservers/{server_id}/detachvolume/{volume_id}	ecs:cloudServers:detachVolume	-
POST /v1/{project_id}/cloudservers/{server_id}/metadata	ecs:cloudServers:updateMetadata	iam:agencies:pass
DELETE /v1/{project_id}/cloudservers/{server_id}/metadata/{key}	ecs:cloudServers:deleteMetadata	-
POST /v1/{project_id}/cloudservers/{server_id}/migrate	ecs:cloudServers:migrate	-
GET /v1/{project_id}/cloudservers/{server_id}/os-interface	ecs:cloudServers:listServerInterfaces	-
PUT /v1/{project_id}/cloudservers/{server_id}/os-reset-password	ecs:cloudServers:resetServerPwd	-
GET /v1/{project_id}/cloudservers/{server_id}/os-resetpwd-flag	ecs:cloudServers:showResetPasswordFlag	-
GET /v1/{project_id}/cloudservers/{server_id}/os-server-password	ecs:cloudServers:showServerPassword	-
DELETE /v1/{project_id}/cloudservers/{server_id}/os-server-password	ecs:cloudServers:deletePassword	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/cloudservers/{server_id}/os-volume_attachments	ecs:cloudServers:listServerVolumeAttachments	-
POST /v1/{project_id}/cloudservers/{server_id}/reinstallos	ecs:cloudServers:rebuild	-
POST /v2/{project_id}/cloudservers/{server_id}/reinstallos	ecs:cloudServers:rebuild	-
POST /v1/{project_id}/cloudservers/{server_id}/remote_console	ecs:cloudServers:vnc	-
POST /v1/{project_id}/cloudservers/{server_id}/resize	ecs:cloudServers:resize	-
GET /v1/{project_id}/cloudservers/detail?flavor={flavor}&name={name}&status={status}&limit={limit}&offset={offset}&not-tags={not-tags}&reservation_id={reservation_id}&enterprise_project_id={enterprise_project_id}&tags={tags}&ip={ip}	ecs:cloudServers:listServersDetails	-
PUT /v1/{project_id}/cloudservers/{server_id}	ecs:cloudServers:updateServer	-
POST /v1/{project_id}/cloudservers/{server_id}/actions/update-auto-terminate-time	ecs:cloudServers:setAutoTerminateTime	-
POST /v1/{project_id}/cloudservers/{server_id}/nics	ecs:cloudServers:addNics	-
POST /v1/{project_id}/cloudservers/{server_id}/nics/delete	ecs:cloudServerNics:delete	-
GET /v1/{project_id}/cloudservers/{server_id}/tags	ecs:cloudServers:showServerTags	-

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/cloudservers/{server_id}/tags/action	ecs:cloudServers:batchCreateServerTags	-
POST /v1/{project_id}/cloudservers/{server_id}/tags/action	ecs:cloudServers:batchDeleteServerTags	-
POST /v1/{project_id}/cloudservers/action	ecs:cloudServers:start	-
POST /v1/{project_id}/cloudservers/action	ecs:cloudServers:stop	-
POST /v1/{project_id}/cloudservers/action	ecs:cloudServers:reboot	-
GET /v1/{project_id}/cloudservers/flavors?availability_zone={availability_zone}&flavor_id={flavor_id}&limit={limit}&marker={marker}	ecs:cloudServerFlavors:get	-
GET /v1/{project_id}/cloudservers/limits	ecs:cloudServerQuotas:get	-
PUT /v1/{project_id}/cloudservers/{server_id}/os-reset-password	ecs:cloudServers:resetServerPwd	-
GET /v1/{project_id}/cloudservers/os-server-groups?limit={limit}&marker={marker}	ecs:cloudServers:listServerGroups	-
POST /v1/{project_id}/cloudservers/os-server-groups	ecs:cloudServers:createServerGroup	-
GET /v1/{project_id}/cloudservers/os-server-groups/{server_group_id}	ecs:cloudServers:showServerGroup	-
DELETE /v1/{project_id}/cloudservers/os-server-groups/{server_group_id}	ecs:cloudServers:deleteServerGroup	-
POST /v1/{project_id}/cloudservers/os-server-groups/{server_group_id}/action	ecs:cloudServers:addServerGroupMember	-

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/cloudservers/os-server-groups/{server_group_id}/action	ecs:cloudServers:deleteServerGroupMember	-
GET /v1/{project_id}/cloudservers/resize_flavors?instance_uuid={instance_uuid}&source_flavor_id={source_flavor_id}&source_flavor_name={source_flavor_name}	ecs:cloudServers:listResizeFlavors	-
GET /v1/{project_id}/cloudservers/tags	ecs:cloudServers:listServerTags	-
POST /v2/{project_id}/cloudservers/{server_id}/changeos	ecs:cloudServers:changeOS	-
PUT /v1/{project_id}/cloudservers/server-name	ecs:cloudServers:batchUpdateServersName	-
POST /v1/{project_id}/cloudservers/actions/change-charge-mode	ChangeServerChargeMode	• billing:order:pay • billing:subscription:renew
GET /v2/{domain_id}/auto-launch-groups	ecs:launchTemplates:list	-
DELETE /v2/{domain_id}/auto-launch-groups/{auto_launch_group_id}	ecs:launchTemplates:delete	-
POST /v2/{domain_id}/auto-launch-groups	ecs:launchTemplates:create	-
PUT /v2/{domain_id}/auto-launch-groups/{auto_launch_group_id}	ecs:launchTemplates:update	-
GET /v1/{project_id}/cloudservers/flavor-sell-policies?flavor_id={flavor_id}	ecs:cloudServerFlavors:get	-
GET /v1/{project_id}/cloudservers/{server_id}/autorecovery	ecs:cloudServers:getAutoRecovery	-
PUT /v1/{project_id}/cloudservers/{server_id}/autorecovery	ecs:cloudServers:setAutoRecovery	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-14中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

ECS定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-14 ECS 支持的资源类型

资源类型	URN
instance	ecs:<region>:<account-id>:instance:<server-id>
capacityReservations	ecs:<region>:<account-id>:capacityReservations:<capacity-reservation-id>

条件（Condition）

条件键（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如ecs:）仅适用于对应服务的操作，详情请参见表5-15。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
- 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，SCP才能生效。支持的运算符请参见：运算符。

ECS定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-15 ECS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
ecs:imageID	string	多值	根据请求参数中指定的镜像ID过滤访问。

5.10.1.2 裸金属服务器 BMS

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于BMS定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于BMS定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下BMS的相关操作。

表 5-16 BMS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
bms:servers:updateBaremetalServer	授予修改裸金属服务器的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
bms:servers:showBaremetalServerInterfaceAttachments	授予查询裸金属服务器网卡的权限。	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:resetServerPwd	授予一键重置裸金属服务器密码的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:showResetPasswordFlag	授予查询是否支持一键重置密码的权限。	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:showWindowsBaremetalServerPwd	授予获取Windows裸金属服务器密码的权限。	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:deletePassword	授予Windows裸金属服务器清除密码的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:showBaremetalServerVolumeInfo	授予查询裸金属服务器挂载的云硬盘信息的权限。	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
bms:servers:create	授予创建裸金属服务器的权限。	write	-	• g:EnterpriseProjectId • g:TagKeys • eip:AssociatePublicIp • bms:Flavorld • bms:VpcId • bms:VpcSubnetId • bms:KmsKeyId
bms:servers:showBaremetalServer	授予查询单个裸机详情的权限。	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:attachVolume	授予裸金属服务器挂载云硬盘的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • bms:KmsKeyId
bms:servers:detachVolume	授予裸金属服务器卸载指定云硬盘的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:updateMetadata	授予更新裸金属服务器元数据的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
bms:servers:reInstallOS	授予重装裸金属服务器操作系统的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • bms:KmsKeyId
bms:servers:showBaremetalServerTags	授予查询裸金属服务器标签的权限。	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:start	授予批量启动裸金属服务器的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:reboot	授予批量重启裸金属服务器的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:stop	授予批量关机裸金属服务器的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:list	授予查询裸金属服务器详情列表的权限。	list	-	g:EnterpriseProjectId
bms:serverFlavors:get	授予查询规格详情和规格扩展信息列表的权限。	list	-	-
bms:serverQuotas:get	授予查询租户配额限制的权限。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
bms:servers:batchCreateBaremetalServerTags	授予批量添加标签的权限。	write	instance*	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
bms:servers:batchDeleteBaremetalServerTags	授予批量删除标签的权限。	write	instance*	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
bms:servers:addNics	授予裸金属服务器绑定网卡的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • eip:AssociatePublicIp • bms:VpcSubnetId
bms:server:deleteNics	授予裸金属服务器解绑网卡的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:serialConsole	授予获取裸金属服务器远程登录地址的权限。	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:server:updateInterface	授予修改裸金属服务器网卡属性的权限。	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

BMS的API通常对应着一个或多个授权项。表5-17展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-17 API 与授权项的关系

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/baremetalservers/{server_id}	bms:servers:updateBaremetalServer	-
GET /v1/{project_id}/baremetalservers/{server_id}/os-interface	bms:servers:showBaremetalServerInterfaceAttachments	-
PUT /v1/{project_id}/baremetalservers/{server_id}/os-reset-password	bms:servers:resetServerPwd	-
GET /v1/{project_id}/baremetalservers/{server_id}/os-resetpwd-flag	bms:servers:showResetPasswordFlag	-
GET /v1/{project_id}/baremetalservers/{server_id}/os-server-password	bms:servers:showWindowsBaremetalServerPwd	-
DELETE /v1/{project_id}/baremetalservers/{server_id}/os-server-password	bms:servers:deletePassword	-
GET /v1/{project_id}/baremetalservers/{server_id}/os-volume_attachments	bms:servers:showBaremetalServerVolumeInfo	-
POST /v1/{project_id}/baremetalservers	bms:servers:create	-
GET /v1/{project_id}/baremetalservers/{server_id}	bms:servers:showBaremetalServer	-
POST /v1/{project_id}/baremetalservers/{server_id}/attachvolume	bms:servers:attachVolume	evs:volumes:use
DELETE /v1/{project_id}/baremetalservers/{server_id}/detachvolume/{attachment_id}	bms:servers:detachVolume	-
POST /v1/{project_id}/baremetalservers/{server_id}/metadata	bms:servers:updateMetadata	-
POST /v1/{project_id}/baremetalservers/{server_id}/reinstallos	bms:servers:reInstallOS	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/baremetalservers/{server_id}/tags	bms:servers:showBaremetalServerTags	-
POST /v1/{project_id}/baremetalservers/action	bms:servers:start	-
POST /v1/{project_id}/baremetalservers/action	bms:servers:reboot	-
POST /v1/{project_id}/baremetalservers/action	bms:servers:stop	-
GET /v1/{project_id}/baremetalservers/detail	bms:servers:list	-
GET /v1/{project_id}/baremetalservers/flavors	bms:serverFlavors:get	-
GET /v1/{project_id}/baremetalservers/limits	bms:serverQuotas:get	-
POST /v1/{project_id}/baremetalservers/{server_id}/tags/action	bms:servers:batchCreateBaremetalServerTags	-
POST /v1/{project_id}/baremetalservers/{server_id}/tags/action	bms:servers:batchDeleteBaremetalServerTags	-
POST /v1/{project_id}/baremetalservers/{server_id}/nics	bms:servers:addNics	-
POST /v1/{project_id}/baremetalservers/{server_id}/nics/delete	bms:server:deleteNics	-
POST /v1/{project_id}/baremetalservers/{server_id}/remote_console	bms:servers:serialConsole	-
PUT /v1/{project_id}/baremetalservers/{server_id}/os-interface/{port_id}	bms:server:updateInterface	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表3**中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

BMS定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-18 BMS 支持的资源类型

资源类型	URN
instance	bms:<region>:<account-id>:instance:<server-id>

- <region>：指定授权的区域，，表示授权在此区域进行相关操作。
- <account-id>：指定授权的用户账号ID，表示授权在此账号ID下进行相关操作。请在API凭证中获取账号ID。
- <server-id>：裸金属服务器ID，表示授权对此裸金属服务器进行相关操作。

条件（Condition）

条件（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如bms:）仅适用于对应服务的操作，详情请参见**表4**。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
- 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，SCP才能生效。支持的运算符请参见：运算符。

BMS定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-19 BMS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
bms:KmsKeyId	string	多值	根据请求参数中指定的加密密钥ID过滤访问。
bms:Flavorld	string	多值	根据请求参数中指定的规格ID过滤访问。
bms:VpcId	string	多值	根据请求参数中指定的网络ID过滤访问。

服务级条件键	类型	单值/多值	说明
bms:VpcSubnetId	string	多值	根据请求参数中指定的子网ID过滤访问。

5.10.1.3 镜像服务 IMS

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指示每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于IMS定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于IMS定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下IMS的相关操作。

表 5-20 IMS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
ims:images:list	查看所有镜像列表。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
ims:images:get	查看用户指定镜像详情。	read	image *	-
ims:images:create	创建镜像元数据。	write	-	• g:RequestTag/<tag-key> • g:TagKeys
ims:images:share	分享已经存在镜像。	permission_management	image *	ims:TargetOrgPaths
ims:images:copyInRegion	区域内复制已经存在镜像。	write	image *	ims:Encrypted
ims:images:copyCrossRegion	跨区域复制已经存在镜像。	write	image *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
ims:quotas:get	查询镜像配额。	read	-	-
ims:images:upload	上传镜像。	write	image *	-
ims:wholeImages:create	制作整机镜像。	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
ims:images:export	导出镜像。	read	image *	-
ims:dataImages:create	使用外部镜像文件制作数据镜像。	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
ims:serverImages:create	制作镜像。	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
ims:images:setTags	更新镜像标签。	tagging	image *	• g:RequestTag/<tag-key> • g:TagKeys

授权项	描述	访问级别	资源类型（*为必须）	条件键
ims:images:getTags	查询镜像标签。	read	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
ims:images:deleteImage	删除镜像。	write	image *	-
ims:images:updateImage	更新镜像信息。	write	image *	-
ims:images:listOsVersion	查看所有镜像支持的OS列表权限。	list	-	-
ims:images:getJob	查询异步任务进度。	read	-	-
ims:images:import	镜像导入。	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
ims:images:setOrDeleteTags	批量增加或删除镜像上标签。	write	-	• g:RequestTag/<tag-key> • g:TagKeys
ims:images:updateMemberStatus	更新镜像成员状态。	write	image *	-
ims:images:addMember	添加镜像成员。	write	image *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ims:images:deleteMember	删除镜像成员。	write	image *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ims:images:listImagesByTag	按标签查询镜像。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
ims:images:showImageTags	查询镜像标签。	read	image *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ims:images:listImageTags	查询项目标签。	list	-	-

IMS的API通常对应着一个或多个授权项。表5-21展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-21 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v2/cloudimages	ims:images:list	-
GET /v2/images/{image_id}	ims:images:get	-
POST /v2/images	ims:images:create	-
POST /v2/images/{image_id}/members	ims:images:share	ims:images:get
POST /v1/cloudimages/{image_id}/copy	ims:images:copyInRegion	ims:serverImages:create
POST /v1/cloudimages/{image_id}/cross_region_copy	ims:images:copyCrossRegion	-
GET /v1/cloudimages/quota	ims:quotas:get	-
PUT /v1/cloudimages/{image_id}/upload PUT /v2/images/{image_id}/file	ims:images:upload	• ims:images:get • ims:images:update
POST /v1/cloudimages/wholeimages/action	ims:wholeImages:create	-
POST /v1/cloudimages/{image_id}/file	ims:images:export	• obs:object:GetObject • obs:object:PutObject

API	对应的授权项	依赖的授权项
• POST /v2/cloudimages/quickimport/action（仅快速导入数据盘镜像需要此授权项） • POST /v1/cloudimages/dataimages/action	ims:dataImages:create	-
• PATCH /v2/cloudimages/{image_id}（仅企业项目迁移需要此授权项） • POST /v2/cloudimages/action • OST /v2/cloudimages/quickimport/action（仅快速导入系统盘镜像需要此授权项） • POST /v1/cloudimages/{image_id}/copy（仅开通企业项目用户需要此授权项）	ims:serverImages:create	-
PUT /v1/cloudimages/tags	ims:images:setTags	-
GET /v1/cloudimages/tags	ims:images:getTags	-
DELETE /v2/images/{image_id}	ims:images:deleteImage	-
• PATCH /v2/cloudimages/{image_id} • PATCH /v2/images/{image_id}	ims:images:updateImage	-
GET /v1/cloudimages/os_version	ims:images:listOsVersion	-
GET /v1/cloudimages/job/{job_id}	ims:images:getJob	-
POST /v2/cloudimages/quickimport/action	ims:images:import	• ims:dataImages:create • ims:serverImages:create
POST /v2/{project_id}/images/{image_id}/tags/action	ims:images:setOrDeleteTags	• ims:images:setTags • ims:images:deleteTags

API	对应的授权项	依赖的授权项
• PUT /v1/cloudimages/members • PUT /v2/images/{image_id}/members/{member_id}	ims:images:updateMemberStatus	-
POST /v1/cloudimages/members	ims:images:addMember	-
DELETE /v1/cloudimages/members	ims:images:deleteMember	-
POST /v2/{project_id}/images/resource_instances/action	ims:images:listImagesByTag	-
GET /v2/{project_id}/images/{image_id}/tags	ims:images:showImageTags	-
GET /v2/{project_id}/images/tags	ims:images:listImageTags	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-22中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

IMS定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-22 IMS 支持的资源类型

资源类型	URN
image	ims:<region>:<account-id>:image:<image-id>

- <region>：指定授权的区域，，表示授权在此区域进行相关操作。
- <account-id>：指定授权的用户账号ID，表示授权在此账号ID下进行相关操作。请在API凭证中获取账号ID。
- <image-id>：镜像ID，表示授权对此镜像进行相关操作。

说明

资源路径URN支持通配符号*表示所有。

条件（Condition）

条件（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀为服务缩写，如ims:）仅适用于对应服务的操作，详情请参见**表3**。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
  - 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，SCP才能生效。支持的运算符请参见：运算符。

IMS定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-23 ims 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
ims:TargetOrgPaths	string	多值	根据指定的共享账号的 Organizations Path 过滤访问。
ims:Encrypted	boolean	单值	根据镜像是否加密对镜像导入和复制等操作进行控制。
ims:TargetBucketOrgPaths	string	多值	根据指定的目标桶owner账号的 Organizations Path 过滤访问。
ims:OriginBucketOrgPaths	string	多值	根据指定的源桶owner账号账号的 Organizations Path 过滤访问。

5.10.2 网络

5.10.2.1 虚拟私有云 VPC

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于vpc定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

  关于vpc定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下vpc的相关操作。

表 5-24 vpc 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
vpc:vpcs:create	授予创建虚拟私有云权限。	write	vpc *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
vpc:vpcs:get	授予查询虚拟私有云详情权限。	read	vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId
vpc:vpcs:list	授予查询虚拟私有云列表权限。	list	vpc *	-
			-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
vpc:vpcs:update	授予更新虚拟私有云权限。	write	vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId
vpc:vpcs:delete	授予删除虚拟私有云权限。	write	vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId
vpc:subnets:create	授予创建子网权限。	write	subnet *	-
			vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId
			-	• g:RequestTag/<tag-key> • g:TagKeys
vpc:subnets:get	授予查询子网详情权限。	read	subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • g:EnterpriseProjectId
vpc:subnets:list	授予查询子网列表权限。	list	subnet *	-
			-	g:EnterpriseProjectId
vpc:subnets:update	授予更新子网权限。	write	subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
vpc:subnets:delete	授予删除子网权限。	write	subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • g:EnterpriseProjectId
vpc:quotas:list	授予查询资源配额权限。	list	-	-
vpc:privateIps:create	授予创建私有IP权限。	write	privateIp *	-
			subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId
vpc:privateIps:get	授予查询私有IP详情权限。	read	privateIp *	• vpc:PrivateIpId • vpc:SubnetId
vpc:privateIps:list	授予查询私有IP列表权限。	list	privateIp *	-
vpc:privateIps:delete	授予删除私有IP权限。	write	privateIp *	• vpc:PrivateIpId • vpc:SubnetId
vpc:securityGroups:create	授予创建安全组权限。	write	securityGroup *	-
			-	g:EnterpriseProjectId
vpc:securityGroups:get	授予查询安全组详情权限。	read	securityGroup *	• g:EnterpriseProjectId • vpc:SecurityGroupId
vpc:securityGroups:list	授予查询安全组列表权限。	list	securityGroup *	-
			-	g:EnterpriseProjectId
vpc:securityGroups:update	授予更新安全组权限。	write	securityGroup *	• g:EnterpriseProjectId • vpc:SecurityGroupId

授权项	描述	访问级别	资源类型（*为必须）	条件键
vpc:securityGroups:delete	授予删除安全组权限。	write	securityGroup *	• g:EnterpriseProjectId • vpc:SecurityGroupId
vpc:securityGroupRules:create	授予创建安全组规则权限。	write	securityGroupRule *	-
			securityGroup *	• g:EnterpriseProjectId • vpc:SecurityGroupId
vpc:securityGroupRules:get	授予查询安全组规则详情权限。	read	securityGroupRule *	• g:EnterpriseProjectId • vpc:SecurityGroupId
vpc:securityGroupRules:list	授予查询安全组规则列表权限。	list	-	g:EnterpriseProjectId
vpc:securityGroupRules:update	授予更新安全组规则权限。	write	securityGroupRule *	• g:EnterpriseProjectId • vpc:SecurityGroupId
vpc:securityGroupRules:delete	授予删除安全组规则权限。	write	securityGroupRule *	• g:EnterpriseProjectId • vpc:SecurityGroupId
vpc:ports:create	授予创建端口权限。	write	port *	-
			subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • g:EnterpriseProjectId
vpc:ports:get	授予查询端口详情权限。	read	port *	• vpc:SubnetId • vpc:PortId • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
vpc:ports:list	授予查询端口列表权限。	list	port *	-
			-	g:EnterpriseProjectId
vpc:ports:update	授予更新端口权限。	write	port *	• vpc:SubnetId • vpc:PortId • g:EnterpriseProjectId
vpc:ports:delete	授予删除端口权限。	write	port *	• vpc:SubnetId • vpc:PortId • g:EnterpriseProjectId
vpc:peerings:create	授予创建对等连接权限。	write	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:AccepterVpcOrgPath • vpc:AccepterVpcOwner
			vpc *	• g:ResourceTag/<tag-key> • vpc:VpcId
vpc:peerings:get	授予查询对等连接详情权限。	read	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:PeeringId
vpc:peerings:list	授予查询对等连接列表权限。	list	peering *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
vpc:peerings:accept	授予接受对等连接权限。	write	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:PeeringId • vpc:RequesterVpcOrgPath • vpc:RequesterVpcOwner
vpc:peerings:reject	授予拒绝对等连接权限。	write	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:PeeringId
vpc:peerings:update	授予更新对等连接权限。	write	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:PeeringId
vpc:peerings:delete	授予删除对等连接权限。	write	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:PeeringId
vpc:routeTables:create	授予创建路由表权限。	write	routeTable *	-
			vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId
vpc:routeTables:get	授予查询路由表详情权限。	read	routeTable *	• vpc:RouteTableId • vpc:VpcId • g:EnterpriseProjectId
vpc:routeTables:list	授予查询路由表列表权限。	list	routeTable *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	g:EnterpriseProjectId
vpc:routeTables:update	授予更新路由表权限。	write	routeTable *	• vpc:RouteTableId • vpc:VpcId • g:EnterpriseProjectId
vpc:routeTables:associate	授予关联路由表权限。	write	routeTable *	• vpc:RouteTableId • vpc:VpcId
			subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • g:EnterpriseProjectId
vpc:routeTables:delete	授予删除路由表权限。	write	routeTable *	• vpc:RouteTableId • vpc:VpcId • g:EnterpriseProjectId
vpc:flowLogs:create	授予创建流日志权限。	write	flowLog *	-
			port	vpc:PortId
			subnet	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId
			vpc	• g:ResourceTag/<tag-key> • vpc:VpcId
vpc:flowLogs:get	授予查询流日志列表或详情权限。	read	flowLog *	vpc:FlowLogId
vpc:flowLogs:list	授予查询流日志列表权限。	read	flowLog *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
vpc:flowLogs:update	授予更新流日志权限。	write	flowLog *	vpc:FlowLogId
vpc:flowLogs:delete	授予删除流日志权限。	write	flowLog *	vpc:FlowLogId
vpc:addressGroups:create	授予创建IP地址组权限。	write	addressGroup *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
vpc:addressGroups:get	授予查询IP地址组详情权限。	read	addressGroup *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:AddressGroupId
vpc:addressGroups:list	授予查询IP地址组列表权限。	list	addressGroup *	-
			-	g:EnterpriseProjectId
vpc:addressGroups:update	授予更新IP地址组权限。	write	addressGroup *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:AddressGroupId
vpc:addressGroups:delete	授予删除IP地址组权限。	write	addressGroup *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:AddressGroupId
vpc:firewalls:create	授予创建网络ACL权限。	write	firewall *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
vpc:firewalls:get	授予查询网络ACL详情权限。	read	firewall *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:FirewallId
vpc:firewalls:list	授予查询网络ACL列表权限。	list	firewall *	-
			-	g:EnterpriseProjectId
vpc:firewalls:update	授予更新网络ACL权限。	write	firewall *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:FirewallId • vpc:FirewallRuleDirection • vpc:FirewallRuleProtocol • vpc:FirewallRuleAction • vpc:FirewallRuleSourcePort • vpc:FirewallRuleDestinationPort • vpc:FirewallOperationType
			subnet	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
vpc:firewalls:delete	授予删除网络ACL权限。	write	firewall *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:FirewallId
vpc:vpcs:createTags	授予创建虚拟私有云资源标签权限。	tagging	vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId
			-	• g:RequestTag/<tag-key> • g:TagKeys
vpc:vpcs:listTags	授予查询虚拟私有云资源标签权限。	read	vpc *	-
vpc:vpcs:deleteTags	授予删除虚拟私有云资源标签权限。	tagging	vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId
			-	g:TagKeys
vpc:subnets:createTags	授予创建子网资源标签权限。	tagging	subnet *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId • vpc:SubnetId
			-	• g:RequestTag/<tag-key> • g:TagKeys
vpc:subnets:listTags	授予查询子网资源标签权限。	read	subnet *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
vpc:subnets:deleteTags	授予删除子网资源标签权限。	tagging	subnet *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId • vpc:SubnetId
			-	g:TagKeys
vpc:subNetworkInterfaces:create	授予创建辅助弹性网卡权限。	write	subNetworkInterface *	-
			subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId
vpc:subNetworkInterfaces:get	授予查询辅助弹性网卡详情权限。	read	subNetworkInterface *	• vpc:SubnetId • vpc:SubNetworkInterfaceId
vpc:subNetworkInterfaces:list	授予查询辅助弹性网卡列表权限。	list	subNetworkInterface *	-
vpc:subNetworkInterfaces:update	授予更新辅助弹性网卡权限。	write	subNetworkInterface *	• vpc:SubnetId • vpc:SubNetworkInterfaceId
vpc:subNetworkInterfaces:delete	授予删除辅助弹性网卡权限。	write	subNetworkInterface *	• vpc:SubnetId • vpc:SubNetworkInterfaceId
vpc:networks:create	授予创建网络权限。	write	network *	-
vpc:networks:get	授予查询网络详情权限。	read	network *	-
vpc:networks:list	授予查询网络列表权限。	list	network *	-
vpc:networks:update	授予更新网络权限。	write	network *	-
vpc:networks:delete	授予删除网络权限。	write	addressGroup *	-

vpc的API通常对应着一个或多个授权项。表5-25展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-25 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/vpcs	vpc:vpcs:create	-
GET /v1/{project_id}/vpcs/{vpc_id}	vpc:vpcs:get	-
GET /v1/{project_id}/vpcs	vpc:vpcs:list	-
PUT /v1/{project_id}/vpcs/{vpc_id}	vpc:vpcs:update	-
DELETE /v1/{project_id}/vpcs/{vpc_id}	vpc:vpcs:delete	-
POST /v1/{project_id}/subnets	vpc:subnets:create	-
GET /v1/{project_id}/subnets/{subnet_id}	vpc:subnets:get	-
GET /v1/{project_id}/subnets	vpc:subnets:list	-
PUT /v1/{project_id}/vpcs/{vpc_id}/subnets/{subnet_id}	vpc:subnets:update	-
DELETE /v1/{project_id}/vpcs/{vpc_id}/subnets/{subnet_id}	vpc:subnets:delete	-
GET /v1/{project_id}/quotas	vpc:quotas:list	-
POST /v1/{project_id}/privateips	vpc:privateIps:create	-
GET /v1/{project_id}/privateips/{privateip_id}	vpc:privateIps:get	-
GET /v1/{project_id}/subnets/{subnet_id}/privateips	vpc:privateIps:list	-
DELETE /v1/{project_id}/privateips/{privateip_id}	vpc:privateIps:delete	-
POST /v1/{project_id}/security-groups	vpc:securityGroups:create	-
GET /v1/{project_id}/security-groups/{security_group_id}	vpc:securityGroups:get	-
GET /v1/{project_id}/security-groups	vpc:securityGroups:list	-

API	对应的授权项	依赖的授权项
DELETE /v1/{project_id}/security-groups/{security_group_id}	vpc:securityGroups:delete	-
POST /v1/{project_id}/security-group-rules	vpc:securityGroupRules:create	-
GET /v1/{project_id}/security-group-rules/{security_group_rule_id}	vpc:securityGroupRules:get	-
GET /v1/{project_id}/security-group-rules	vpc:securityGroupRules:list	-
DELETE /v1/{project_id}/security-group-rules/{security_group_rule_id}	vpc:securityGroupRules:delete	-
POST /v1/{project_id}/ports	vpc:ports:create	-
GET /v1/{project_id}/ports/{port_id}	vpc:ports:get	-
GET /v1/{project_id}/ports	vpc:ports:list	-
PUT /v1/{project_id}/ports/{port_id}	vpc:ports:update	-
DELETE /v1/{project_id}/ports/{port_id}	vpc:ports:delete	-
POST /v2.0/vpc/peerings	vpc:peerings:create	-
PUT /v2.0/vpc/peerings/{peering_id}/accept	vpc:peerings:accept	-
PUT /v2.0/vpc/peerings/{peering_id}/reject	vpc:peerings:reject	-
GET /v2.0/vpc/peerings/{peering_id}	vpc:peerings:get	-
GET /v2.0/vpc/peerings	vpc:peerings:list	-
PUT /v2.0/vpc/peerings/{peering_id}	vpc:peerings:update	-
DELETE /v2.0/vpc/peerings/{peering_id}	vpc:peerings:delete	-
POST /v1/{project_id}/routetables	vpc:routeTables:create	-
GET /v1/{project_id}/routetables/{routetable_id}	vpc:routeTables:get	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/routetables	vpc:routeTables:list	-
PUT /v1/{project_id}/routetables/{routetable_id}	vpc:routeTables:update	-
POST /v1/{project_id}/routetables/{routetable_id}/action	vpc:routeTables:associate	-
POST 01 /v1/{project_id}/routetables/{routetable_id}/action	vpc:routeTables:associate	-
DELETE /v1/{project_id}/routetables/{routetable_id}	vpc:routeTables:delete	-
POST /v1/{project_id}/fl/flow_logs	vpc:flowLogs:create	-
GET /v1/{project_id}/fl/flow_logs/{flowlog_id}	vpc:flowLogs:get	-
GET /v1/{project_id}/fl/flow_logs	vpc:flowLogs:list	-
PUT /v1/{project_id}/fl/flow_logs/{flowlog_id}	vpc:flowLogs:update	-
DELETE /v1/{project_id}/fl/flow_logs/{flowlog_id}	vpc:flowLogs:delete	-
PUT /v3/{project_id}/vpc/vpcs/{vpc_id}/add-extend-cidr	vpc:vpcs:update	-
PUT /v3/{project_id}/vpc/vpcs/{vpc_id}/remove-extend-cidr	vpc:vpcs:update	-
PUT /v3/{project_id}/vpc/security-groups/{security_group_id}	vpc:securityGroups:update	-
POST /v3/{project_id}/vpc/address-groups	vpc:addressGroups:create	-
GET /v3/{project_id}/vpc/address-groups/{address_group_id}	vpc:addressGroups:get	-
GET /v3/{project_id}/vpc/address-groups	vpc:addressGroups:list	-
PUT /v3/{project_id}/vpc/address-groups/{address_group_id}	vpc:addressGroups:update	-

API	对应的授权项	依赖的授权项
DELETE /v3/{project_id}/vpc/address-groups/{address_group_id}	vpc:addressGroups:delete	-
DELETE /v3/{project_id}/vpc/address-groups/{address_group_id}/force	vpc:addressGroups:delete	-
POST /v2.0/{project_id}/vpcs/{vpc_id}/tags/action	vpc:vpcs:createTags	-
POST 01 /v2.0/{project_id}/vpcs/{vpc_id}/tags/action	vpc:vpcs:deleteTags	-
POST /v2.0/{project_id}/vpcs/{vpc_id}/tags	vpc:vpcs:createTags	-
POST /v2.0/{project_id}/vpcs/resource_instances/action	vpc:vpcs:listTags	-
GET /v2.0/{project_id}/vpcs/tags	vpc:vpcs:listTags	-
GET /v2.0/{project_id}/vpcs/{vpc_id}/tags	vpc:vpcs:listTags	-
DELETE /v2.0/{project_id}/vpcs/{vpc_id}/tags/{key}	vpc:vpcs:deleteTags	-
POST 01 /v2.0/{project_id}/subnets/{subnet_id}/tags/action	vpc:subnets:creatTags	-
POST /v2.0/{project_id}/subnets/{subnet_id}/tags/action	vpc:subnets:deleteTags	-
POST /v2.0/{project_id}/subnets/{subnet_id}/tags	vpc:subnets:creatTags	-
POST /v2.0/{project_id}/subnets/resource_instances/action	vpc:subnets:listTags	-
GET /v2.0/{project_id}/subnets/tags	vpc:subnets:listTags	-
GET /v2.0/{project_id}/subnets/{subnet_id}/tags	vpc:subnets:listTags	-
DELETE /v2.0/{project_id}/subnets/{subnet_id}/tags/{key}	vpc:subnets:deleteTags	-
PUT /v3/{project_id}/vpc/sub-network-interfaces/migrate	vpc:subNetworkInterfaces:update	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-26中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

vpc定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-26 vpc 支持的资源类型

资源类型	URN
vpc	vpc:<region>:<account-id>:vpc:<vpc-id>
subnet	vpc:<region>:<account-id>:subnet:<subnet-id>
privateIp	vpc:<region>:<account-id>:privateIp:<private-ip-id>
securityGroup	vpc:<region>:<account-id>:securityGroup:<security-group-id>
securityGroupRule	vpc:<region>:<account-id>:securityGroupRule:<security-group-rule-id>
port	vpc:<region>:<account-id>:port:<port-id>
peering	vpc:<region>:<account-id>:peering:<peering-id>
routeTable	vpc:<region>:<account-id>:routeTable:<route-table-id>
flowLog	vpc:<region>:<account-id>:flowLog:<flow-log-id>
addressGroup	vpc:<region>:<account-id>:addressGroup:<address-group-id>
firewall	vpc:<region>:<account-id>:firewall:<firewall-id>
subNetworkInterface	vpc:<region>:<account-id>:subNetworkInterface:<subNetworkInterface-id>
publicip	vpc:<region>:<account-id>:publicip:<publicip-id>
bandwidth	vpc:<region>:<account-id>:bandwidth:<bandwidth-id>
network	vpc:<region>:<account-id>:network:<network-id>

条件（Condition）

条件（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。

  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀为服务缩写，如vpc:）仅适用于对应服务的操作，详情请参见**表5-27**。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
- 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，SCP才能生效。支持的运算符请参见：运算符。

vpc定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-27 vpc 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
vpc:VpcId	string	多值	根据指定的虚拟私有云资源ID过滤访问。
vpc:SubnetId	string	多值	根据指定的子网资源ID过滤访问。
vpc:SecurityGroupId	string	多值	根据指定的安全组资源ID过滤访问。
vpc:PeeringId	string	多值	根据指定的对等连接资源ID过滤访问。
vpc:AccepterVpcId	string	多值	根据指定的接收方VPC资源ID过滤访问。
vpc:AccepterVpcOrgPath	string	多值	根据指定的对等连接接收方VPC资源所有者的OrgPath过滤访问。
vpc:AccepterVpcOwner	string	多值	根据指定的对等连接接收方VPC资源所有者的账号ID过滤访问。
vpc:RequesterVpcOrgPath	string	多值	根据指定的对等连接请求方VPC资源所有者的OrgPath过滤访问。
vpc:RequesterVpcOwner	string	多值	根据指定的对等连接请求方VPC资源所有者的账号ID过滤访问。
vpc:RequesterVpcId	string	多值	根据指定的请求方VPC资源ID过滤访问。

服务级条件键	类型	单值/多值	说明
vpc:RouteTableId	string	多值	根据指定的路由表资源ID过滤访问。
vpc:FlowLogId	string	多值	根据指定的流日志资源ID过滤访问。
vpc:AddressGroupId	string	多值	根据指定的IP地址组资源ID过滤访问。
vpc:FirewallId	string	多值	根据指定的网络ACL资源ID过滤访问。
vpc:PrivateIpId	string	多值	根据指定的私有IP资源ID过滤访问。
vpc:PortId	string	多值	根据指定的端口资源ID过滤访问。
vpc:SubNetworkInterfaceId	string	多值	根据指定的辅助弹性网卡资源ID过滤访问。
vpc:FirewallRuleDirection	string	多值	根据指定的网络ACL规则方向过滤访问，有效的条件值应为ingress、egress。
vpc:FirewallRuleProtocol	string	多值	根据指定的网络ACL规则协议过滤访问，有效的条件值应为tcp、udp、icmp、icmpv6、any。
vpc:FirewallRuleAction	string	多值	根据指定的网络ACL规则策略过滤访问，有效的条件值应为allow、deny。
vpc:FirewallRuleSourcePort	numeric	多值	根据指定的网络ACL规则源端口过滤访问。
vpc:FirewallRuleDestinationPort	numeric	多值	根据指定的网络ACL规则目的端口过滤访问。
vpc:FirewallOperationType	string	多值	根据指定的网络ACL操作类型过滤访问，有效的条件值应为updateAcl、associateSubnet、disassociateSubnet、insertRule、updateRule、removeRule。

5.10.2.2 弹性公网 IP EIP

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于EIP定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于EIP定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下EIP的相关操作。

表 5-28 EIP 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
eip:publicIps:create	授予申请弹性公网IP的权限。	write	publicip *	-
			-	g:EnterpriseProjectId
eip:publicIps:batchCreate	授予批量创建弹性公网IP的权限。	write	publicip *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
eip:publicIps:list	授予查询弹性公网IP列表的权限。	list	publicip *	-
			-	g:EnterpriseProjectId
eip:publicIps:count	授予查询弹性公网IP数量的权限。	list	publicip *	-
eip:publicIps:get	授予查询指定弹性公网IP的权限。	read	publicip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
eip:publicIps:update	授予更新弹性公网IP的权限。	write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:publicIps:enableNat64	授予使能弹性公网IP NAT64的权限。	write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:publicIps:disableNat64	授予使能弹性公网IP NAT64的权限。	write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:publicIps:associateInstance	授予将弹性公网IP绑定网卡的权限。	write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:publicIps:disassociateInstance	授予将弹性公网IP解绑网卡的权限。	write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
eip:publicIps:attachBandwidth	授予将弹性公网IP绑定带宽的权限。	write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			bandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:publicIps:detachBandwidth	授予将弹性公网IP从共享带宽中解绑的权限。	write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			bandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:publicIps:delete	授予删除弹性公网IP的权限。	write	publicip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
eip:publicIps:createTags	授予创建弹性IP资源标签权限。	tagging	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
eip:publicIps:listTags	授予查询弹性IP资源标签权限。	list	publicip *	-
eip:publicIps:deleteTags	授予删除弹性公网IP资源标签权限。	tagging	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	g:TagKeys
eip:bandwidths:insertPublicIps	授予共享带宽插入弹性公网IP的权限。	write	bandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
eip:bandwidths:removePublicIps	授予共享带宽移除弹性公网IP的权限。	write	bandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
eip:bandwidths:create	授予创建共享带宽的权限。	write	bandwidth *	-
			-	g:EnterpriseProjectId
eip:bandwidths:batchCreate	授予批量创建共享带宽的权限。	write	bandwidth *	-
eip:bandwidths:list	授予查询带宽列表的权限。	list	bandwidth *	-
			-	g:EnterpriseProjectId
eip:bandwidths:update	授予更新带宽的权限。	write	bandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:bandwidths:get	授予查询带宽的权限。	read	bandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
eip:bandwidths:delete	授予删除共享带宽的权限。	write	bandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
eip:bandwidthPkgs:list	授予查询带宽加油包列表的权限。	list	bandwidthPkg *	-
eip:publicipPools:get	授予查询公网IP池的权限。	read	publicipPool *	-
eip:vpcIgws:list	授予查询互联网网关列表的权限。	list	vpcIgw *	-
eip:vpcIgws:get	授予查询互联网网关的权限。	read	vpcIgw *	-
eip:vpcIgws:update	授予更新互联网网关的权限。	write	vpcIgw *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
eip:vpcIgws:delete	授予删除互联网网关的权限。	write	vpcIgw *	-
eip:vpcIgws:create	授予创建互联网网关的权限。	write	vpcIgw *	-
eip:globalEips:list	授予查询全域弹性公网IP列表的权限。	list	globalEip *	-
			-	g:EnterpriseProjectId
eip:globalEips:count	授予查询全域弹性公网IP数量的权限。	list	globalEip *	-
eip:globalEips:get	授予查询指定全域弹性公网IP的权限。	read	globalEip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
eip:globalEips:create	授予申请全域弹性公网IP的权限。	write	globalEip *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
eip:globalEips:updateGeip	授予更新全域弹性公网IP的权限。	write	globalEip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:globalEips:disassociateInstance	授予从全域弹性公网IP解绑实例的权限。	write	globalEip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:globalEips:associateInstance	授予给全域弹性公网IP绑定实例的权限。	write	globalEip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:globalEips:delete	授予删除全域弹性公网IP的权限。	write	globalEip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
eip:globalEips:attachBandwidth	授予将弹性公网IP绑定公网带宽的权限。	write	globalEip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:globalEips:detachBandwidth	授予将弹性公网IP从公网带宽中移除的权限。	write	globalEip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:globalEips:createTags	授予创建全域弹性IP资源标签权限。	tagging	globalEip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
eip:globalEips:getTags	授予查询全域弹性IP资源标签权限。	read	globalEip *	-
eip:globalEips:listTags	授予查询项目里所有全域弹性IP资源标签权限。	list	globalEip *	-
eip:globalEips:deleteTags	授予删除全域弹性公网IP资源标签权限。	tagging	globalEip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	g:TagKeys
eip:internetBandwidths:createTags	授予创建全域公网带宽资源标签权限。	tagging	internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	• g:RequestTag/<tag-key> • g:TagKeys
eip:internetBandwidths:getTags	授予查询全域公网带宽资源标签权限。	read	internetBandwidth *	-
eip:internetBandwidths:listTags	授予查询项目里所有全域公网带宽资源标签权限。	list	internetBandwidth *	-
eip:internetBandwidths:deleteTags	授予删除全域公网带宽资源标签权限。	tagging	internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	g:TagKeys
eip:internetBandwidths:list	授予查询全域公网带宽列表的权限。	list	internetBandwidth *	-
			-	g:EnterpriseProjectId
eip:internetBandwidths:count	授予查询全域公共带宽数量的权限。	list	internetBandwidth *	-
eip:internetBandwidths:get	授予查询指定全域公网带宽的权限。	read	internetBandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
eip:internetBandwidths:create	授予申请全域公网带宽的权限。	write	internetBandwidth *	-
			-	g:EnterpriseProjectId
eip:internetBandwidths:update	授予更新全域公网带宽的权限。	write	internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
eip:internetBandwidths:delete	授予删除全域公网带宽的权限。	write	internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:geipSegments:list	授予查询全域弹性公网IP段列表的权限。	list	geipSegment *	-
			-	g:EnterpriseProjectId
eip:geipSegments:count	授予查询全域弹性公网IP段数量的权限。	list	geipSegment *	-
eip:geipSegments:get	授予查询指定全域弹性公网IP段的权限。	read	geipSegment *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
eip:geipSegments:create	授予申请全域弹性公网IP段的权限。	write	geipSegment *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
eip:geipSegments:update	授予更新全域弹性公网IP段的权限。	write	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:geipSegments:disassociateInstance	授予从全域弹性公网IP段解绑实例的权限。	write	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:geipSegments:associateInstance	授予给全域弹性公网IP段绑定实例的权限。	write	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:geipSegments:delete	授予删除全域弹性公网IP段的权限。	write	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
eip:geipSegments:attachBandwidth	授予将全域弹性公网IP段绑定公网带宽的权限。	write	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:geipSegments:detachBandwidth	授予将全域弹性公网IP段从公网带宽中移除的权限。	write	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			internetBandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:geipSegments:createTags	授予创建全域弹性IP段资源标签权限。	tagging	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
eip:geipSegments:getTags	授予查询全域弹性IP段资源标签权限。	read	geipSegment *	-
eip:geipSegments:listTags	授予查询项目里所有全域弹性IP段资源标签权限。	list	geipSegment *	-
eip:geipSegments:deleteTags	授予删除全域弹性公网IP段资源标签权限。	tagging	geipSegment *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	g:TagKeys
eip:userDisclaimer:sign	授予签署免责条款的权限。	write	-	-
eip:userDisclaimer:cancel	授予撤销免责条款的权限。	write	-	-

EIP的API通常对应着一个或多个授权项。表5-29展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-29 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/publicips	eip:publicIps:create	-
POST /v2/{project_id}/batchpublicips	eip:publicIps:batchCreate	-
GET /v1/{project_id}/publicips	eip:publicIps:list	-
GET /v2/{project_id}/elasticips	eip:publicIps:count	-
GET /v2/{project_id}/publicip/instances	eip:publicIps:count	-
GET /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:get	-
PUT /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:update	-
POST /v2.0/{project_id}/publicips/change-to-period	eip:publicIps:update	bss:renewal:update
PATCH /v2/{project_id}/batchpublicips	eip:publicIps:disassociateInstance	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/associate-instance	eip:publicIps:associateInstance	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/disassociate-instance	eip:publicIps:disassociateInstance	-
POST /v3/{project_id}/eip/publicips/attach-share-bandwidth	eip:publicIps:attachBandwidth	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/attach-share-bandwidth	eip:publicIps:attachBandwidth	-
POST /v3/{project_id}/eip/publicips/detach-share-bandwidth	eip:publicIps:detachBandwidth	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/eip/publicips/{publicip_id}/detach-share-bandwidth	eip:publicIps:detachBandwidth	-
DELETE /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:delete	-
DELETE /v2/{project_id}/batchpublicips	eip:publicIps:delete	-
POST /v2.0/{project_id}/publicips/{publicip_id}/tags/action	eip:publicIps:createTags	-
POST 01 /v2.0/{project_id}/publicips/{publicip_id}/tags/action	eip:publicIps:deleteTags	-
POST /v2.0/{project_id}/publicips/{publicip_id}/tags	eip:publicIps:createTags	-
DELETE /v2.0/{project_id}/publicips/{publicip_id}/tags/{key}	eip:publicIps:deleteTags	-
POST /v2.0/{project_id}/publicips/resource_instances/action	eip:publicIps:listTags	-
GET /v2.0/{project_id}/publicips/tags	eip:publicIps:listTags	-
GET /v2.0/{project_id}/publicips/{publicip_id}/tags	eip:publicIps:listTags	-
POST /v2.0/{project_id}/bandwidths/{bandwidth_id}/insert	eip:bandwidths:insertPublicIps	-
POST /v2.0/{project_id}/bandwidths/{bandwidth_id}/remove	eip:bandwidths:removePublicIps	-
POST /v2.0/{project_id}/bandwidths	eip:bandwidths:create	-
POST /v2.0/{project_id}/batch-bandwidths	eip:bandwidths:batchCreate	-
GET /v1/{project_id}/bandwidths	eip:bandwidths:list	-
DELETE /v2.0/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:delete	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:get	-
PUT /v1/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:update	-
PUT /v2.0/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:update	-
POST /v2.0/{project_id}/bandwidths/change-to-period	eip:bandwidths:update	bss:renewal:update
GET /v2/{project_id}/bandwidthpkgs	eip:bandwidthPkgs:list	-
PUT /v2/{project_id}/bandwidthpkgs/{id}	eip:bandwidthPkgs:update	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/enable-nat64	eip:publicIps:enableNat64	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/disable-nat64	eip:publicIps:disableNat64	-
POST /v1/{project_id}/publicips	eip:publicIps:create	-
POST /v2/{project_id}/batchpublicips	eip:publicIps:batchCreate	-
GET /v1/{project_id}/publicips	eip:publicIps:list	-
GET /v2/{project_id}/elasticips	eip:publicIps:count	-
GET /v2/{project_id}/publicip/instances	eip:publicIps:count	-
GET /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:get	-
PUT /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:update	-
POST /v2.0/{project_id}/publicips/change-to-period	eip:publicIps:update	bss:renewal:update
PATCH /v2/{project_id}/batchpublicips	eip:publicIps:disassociateInstance	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/eip/publicips/{publicip_id}/associate-instance	eip:publicIps:associateInstance	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/disassociate-instance	eip:publicIps:disassociateInstance	-
POST /v3/{project_id}/eip/publicips/attach-share-bandwidth	eip:publicIps:attachBandwidth	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/attach-share-bandwidth	eip:publicIps:attachBandwidth	-
POST /v3/{project_id}/eip/publicips/detach-share-bandwidth	eip:publicIps:detachBandwidth	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/detach-share-bandwidth	eip:publicIps:detachBandwidth	-
DELETE /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:delete	-
DELETE /v2/{project_id}/batchpublicips	eip:publicIps:delete	-
POST /v2.0/{project_id}/publicips/{publicip_id}/tags/action	eip:publicIps:createTags	-
POST 01 /v2.0/{project_id}/publicips/{publicip_id}/tags/action	eip:publicIps:deleteTags	-
POST /v2.0/{project_id}/publicips/{publicip_id}/tags	eip:publicIps:createTags	-
DELETE /v2.0/{project_id}/publicips/{publicip_id}/tags/{key}	eip:publicIps:deleteTags	-
POST /v2.0/{project_id}/publicips/resource_instances/action	eip:publicIps:listTags	-
GET /v2.0/{project_id}/publicips/tags	eip:publicIps:listTags	-
GET /v2.0/{project_id}/publicips/{publicip_id}/tags	eip:publicIps:listTags	-

API	对应的授权项	依赖的授权项
POST /v2.0/{project_id}/bandwidths/{bandwidth_id}/insert	eip:bandwidths:insertPublicIps	-
POST /v2.0/{project_id}/bandwidths/{bandwidth_id}/remove	eip:bandwidths:removePublicIps	-
POST /v2.0/{project_id}/bandwidths	eip:bandwidths:create	-
POST /v2.0/{project_id}/batch-bandwidths	eip:bandwidths:batchCreate	-
GET /v1/{project_id}/bandwidths	eip:bandwidths:list	-
DELETE /v2.0/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:delete	-
GET /v1/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:get	-
PUT /v1/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:update	-
PUT /v2.0/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:update	-
POST /v2.0/{project_id}/bandwidths/change-to-period	eip:bandwidths:update	bss:renewal:update
GET /v2/{project_id}/bandwidthpkgs	eip:bandwidthPkgs:list	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/enable-nat64	eip:publicIps:enableNat64	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/disable-nat64	eip:publicIps:disableNat64	-
POST /v1/{project_id}/publicips	eip:publicIps:create	-
POST /v2/{project_id}/batchpublicips	eip:publicIps:batchCreate	-
GET /v1/{project_id}/publicips	eip:publicIps:list	-
GET /v2/{project_id}/elasticips	eip:publicIps:count	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/publicip/instances	eip:publicIps:count	-
GET /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:get	-
PUT /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:update	-
POST /v2.0/{project_id}/publicips/change-to-period	eip:publicIps:update	bss:renewal:update
PATCH /v2/{project_id}/batchpublicips	eip:publicIps:disassociateInstance	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/associate-instance	eip:publicIps:associateInstance	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/disassociate-instance	eip:publicIps:disassociateInstance	-
POST /v3/{project_id}/eip/publicips/attach-share-bandwidth	eip:publicIps:attachBandwidth	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/attach-share-bandwidth	eip:publicIps:attachBandwidth	-
POST /v3/{project_id}/eip/publicips/detach-share-bandwidth	eip:publicIps:detachBandwidth	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/detach-share-bandwidth	eip:publicIps:detachBandwidth	-
DELETE /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:delete	-
DELETE /v2/{project_id}/batchpublicips	eip:publicIps:delete	-
POST /v2.0/{project_id}/publicips/{publicip_id}/tags/action	eip:publicIps:createTags	-
POST 01 /v2.0/{project_id}/publicips/{publicip_id}/tags/action	eip:publicIps:deleteTags	-
POST /v2.0/{project_id}/publicips/{publicip_id}/tags	eip:publicIps:createTags	-

API	对应的授权项	依赖的授权项
DELETE /v2.0/{project_id}/publicips/{publicip_id}/tags/{key}	eip:publicIps:deleteTags	-
POST /v2.0/{project_id}/publicips/resource_instances/action	eip:publicIps:listTags	-
GET /v2.0/{project_id}/publicips/tags	eip:publicIps:listTags	-
GET /v2.0/{project_id}/publicips/{publicip_id}/tags	eip:publicIps:listTags	-
POST /v2.0/{project_id}/bandwidths/{bandwidth_id}/insert	eip:bandwidths:insertPublicIps	-
POST /v2.0/{project_id}/bandwidths/{bandwidth_id}/remove	eip:bandwidths:removePublicIps	-
POST /v2.0/{project_id}/bandwidths	eip:bandwidths:create	-
POST /v2.0/{project_id}/batch-bandwidths	eip:bandwidths:batchCreate	-
GET /v1/{project_id}/bandwidths	eip:bandwidths:list	-
DELETE /v2.0/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:delete	-
GET /v1/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:get	-
PUT /v1/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:update	-
PUT /v2.0/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:update	-
POST /v2.0/{project_id}/bandwidths/change-to-period	eip:bandwidths:update	bss:renewal:update
GET /v2/{project_id}/bandwidthpkgs	eip:bandwidthPkgs:list	-
PUT /v2/{project_id}/bandwidthpkgs/{id}	eip:bandwidthPkgs:update	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/eip/publicips/{publicip_id}/enable-nat64	eip:publicIps:enableNat64	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/disable-nat64	eip:publicIps:disableNat64	-
POST /v1/{project_id}/publicips	eip:publicIps:create	-
POST /v2/{project_id}/batchpublicips	eip:publicIps:batchCreate	-
GET /v1/{project_id}/publicips	eip:publicIps:list	-
GET /v2/{project_id}/elasticips	eip:publicIps:count	-
GET /v2/{project_id}/publicip/instances	eip:publicIps:count	-
GET /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:get	-
PUT /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:update	-
POST /v2.0/{project_id}/publicips/change-to-period	eip:publicIps:update	bss:renewal:update
PATCH /v2/{project_id}/batchpublicips	eip:publicIps:disassociateInstance	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/associate-instance	eip:publicIps:associateInstance	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/disassociate-instance	eip:publicIps:disassociateInstance	-
POST /v3/{project_id}/eip/publicips/attach-share-bandwidth	eip:publicIps:attachBandwidth	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/attach-share-bandwidth	eip:publicIps:attachBandwidth	-
POST /v3/{project_id}/eip/publicips/detach-share-bandwidth	eip:publicIps:detachBandwidth	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/eip/publicips/{publicip_id}/detach-share-bandwidth	eip:publicIps:detachBandwidth	-
DELETE /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:delete	-
DELETE /v2/{project_id}/batchpublicips	eip:publicIps:delete	-
POST /v2.0/{project_id}/publicips/{publicip_id}/tags/action	eip:publicIps:createTags	-
POST 01 /v2.0/{project_id}/publicips/{publicip_id}/tags/action	eip:publicIps:deleteTags	-
POST /v2.0/{project_id}/publicips/{publicip_id}/tags	eip:publicIps:createTags	-
DELETE /v2.0/{project_id}/publicips/{publicip_id}/tags/{key}	eip:publicIps:deleteTags	-
POST /v2.0/{project_id}/publicips/resource_instances/action	eip:publicIps:listTags	-
GET /v2.0/{project_id}/publicips/tags	eip:publicIps:listTags	-
GET /v2.0/{project_id}/publicips/{publicip_id}/tags	eip:publicIps:listTags	-
POST /v2.0/{project_id}/bandwidths/{bandwidth_id}/insert	eip:bandwidths:insertPublicIps	-
POST /v2.0/{project_id}/bandwidths/{bandwidth_id}/remove	eip:bandwidths:removePublicIps	-
POST /v2.0/{project_id}/bandwidths	eip:bandwidths:create	-
POST /v2.0/{project_id}/batch-bandwidths	eip:bandwidths:batchCreate	-
GET /v1/{project_id}/bandwidths	eip:bandwidths:list	-
DELETE /v2.0/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:delete	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:get	-
PUT /v1/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:update	-
PUT /v2.0/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:update	-
POST /v2.0/{project_id}/bandwidths/change-to-period	eip:bandwidths:update	bss:renewal:update
GET /v2/{project_id}/bandwidthpkgs	eip:bandwidthPkgs:list	-
PUT /v2/{project_id}/bandwidthpkgs/{id}	eip:bandwidthPkgs:update	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/enable-nat64	eip:publicIps:enableNat64	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/disable-nat64	eip:publicIps:disableNat64	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-30中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

EIP定义了以下可以在自定义SCP的Resource元素中使用的资源类型。

表 5-30 EIP 支持的资源类型

资源类型	URN
globalEip	eip:<region>:<account-id>:globalEip:<globalEip-id>
internetBandwidth	eip:<region>:<account-id>:internetBandwidth:<internetBandwidth-id>
bandwidthRule	eip:<region>:<account-id>:bandwidthRule:<bandwidthRule-id>
bandwidthPkg	eip:<region>:<account-id>:bandwidthPkg:<bandwidthPkg-id>

资源类型	URN
publicipPool	eip:<region>:<account-id>:publicipPool:<publicipPool-id>
vpcIgw	eip:<region>:<account-id>:vpcIgw:<vpcIgw-id>
geipSegment	eip:<region>:<account-id>:geipSegment:<geipSegment-id>
globalEip	eip:<region>:<account-id>:globalEip:<globalEip-id>
internetBandwidth	eip:<region>:<account-id>:internetBandwidth:<internetBandwidth-id>
bandwidthPkg	eip:<region>:<account-id>:bandwidthPkg:<bandwidthPkg-id>
publicipPool	eip:<region>:<account-id>:publicipPool:<publicipPool-id>
vpcIgw	eip:<region>:<account-id>:vpcIgw:<vpcIgw-id>
geipSegment	eip:<region>:<account-id>:geipSegment:<geipSegment-id>
globalEip	eip:<region>:<account-id>:globalEip:<globalEip-id>
internetBandwidth	eip:<region>:<account-id>:internetBandwidth:<internetBandwidth-id>
bandwidthRule	eip:<region>:<account-id>:bandwidthRule:<bandwidthRule-id>
bandwidthPkg	eip:<region>:<account-id>:bandwidthPkg:<bandwidthPkg-id>
publicipPool	eip:<region>:<account-id>:publicipPool:<publicipPool-id>
vpcIgw	eip:<region>:<account-id>:vpcIgw:<vpcIgw-id>
geipSegment	eip:<region>:<account-id>:geipSegment:<geipSegment-id>
globalEip	eip:<region>:<account-id>:globalEip:<globalEip-id>
internetBandwidth	eip:<region>:<account-id>:internetBandwidth:<internetBandwidth-id>
bandwidthRule	eip:<region>:<account-id>:bandwidthRule:<bandwidthRule-id>
bandwidthPkg	eip:<region>:<account-id>:bandwidthPkg:<bandwidthPkg-id>
publicipPool	eip:<region>:<account-id>:publicipPool:<publicipPool-id>

资源类型	URN
vpcIgw	eip:<region>:<account-id>:vpcIgw:<vpcIgw-id>
geipSegment	eip:<region>:<account-id>:geipSegment:<geipSegment-id>

条件（Condition）

EIP服务不支持在SCP中的条件键中配置服务级的条件键。EIP可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.2.3 NAT 网关 NAT

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于NAT定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于NAT定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下NAT的相关操作。

表 5-31 NAT 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
nat:privateNatGateways:list	授予权限以查询私网NAT网关列表。	list	privateGateway *	g:EnterpriseProjectId
nat:privateNatGateways:create	授予权限以创建私网NAT网关。	write	privateGateway *	-
			subnet *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
nat:privateNatGateways:delete	授予权限以删除指定的私网NAT网关。	write	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
nat:privateNatGateways:get	授予权限以查询指定的私网NAT网关。	read	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
nat:privateNatGateways:update	授予权限以更新指定的私网NAT网关。	write	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
nat:privateNatDnatRules:list	授予权限以查询私网NAT网关DNAT规则列表。	list	privateDnatRule *	g:EnterpriseProjectId
nat:privateNatDnatRules:create	授予权限以创建私网NAT网关DNAT规则。	write	privateGateway *	g:ResourceTag/<tag-key>
			privateDnatRule *	-
			privateTransitIp *	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			port	-
			-	g:EnterpriseProjectId
nat:privateNatDnatRules:delete	授予权限以删除指定的私网NAT网关DNAT规则。	write	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			privateDnatRule *	g:EnterpriseProjectId
nat:privateNatDnatRules:get	授予权限以查询指定的私网NAT网关DNAT规则。	read	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			privateDnatRule *	g:EnterpriseProjectId
nat:privateNatDnatRules:update	授予权限以更新指定的私网NAT网关DNAT规则。	write	privateGateway *	g:ResourceTag/<tag-key>
			privateDnatRule *	-
			privateTransitIp	g:ResourceTag/<tag-key>
			port	-
			-	g:EnterpriseProjectId
nat:privateNatSnatRules:list	授予权限以查询私网NAT网关SNAT规则列表。	list	privateSnatRule *	g:EnterpriseProjectId
nat:privateNatSnatRules:create	授予权限以创建私网NAT网关SNAT规则。	write	privateGateway *	g:ResourceTag/<tag-key>
			privateSnatRule *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			privateTransitIp *	g:ResourceTag/<tag-key>
			subnet	-
			-	g:EnterpriseProjectId
nat:privateNatSnatRules:delete	授予权限以删除指定的私网NAT网关SNAT规则。	write	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			privateSnatRule *	g:EnterpriseProjectId
nat:privateNatSnatRules:get	授予权限以查询指定的私网NAT网关SNAT规则。	read	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			privateSnatRule *	g:EnterpriseProjectId
nat:privateNatSnatRules:update	授予权限以更新指定的私网NAT网关SNAT规则。	write	privateGateway *	g:ResourceTag/<tag-key>
			privateSnatRule *	-
			privateTransitIp	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
nat:privateNatTransitIps:list	授予权限以查询私网NAT中转IP地址列表。	list	privateTransitIp *	g:EnterpriseProjectId
nat:privateNatTransitIps:create	授予权限以创建私网NAT中转IP地址。	write	privateTransitIp *	-
			subnet	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
nat:privateNatTransitIps:delete	授予权限以删除指定的私网NAT中转IP地址。	write	privateTransitIp *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
nat:privateNatTransitIps:get	授予权限以查询指定的私网NAT中转IP地址。	read	privateTransitIp *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
nat:natGateways:list	授予权限以查询公网NAT网关列表。	list	gateway *	g:EnterpriseProjectId
nat:natGateways:create	授予权限以创建公网NAT网关。	write	gateway *	-
			vpc *	-
			subnet *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
nat:natGateways:delete	授予权限以删除指定的公网NAT网关。	write	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
nat:natGateways:get	授予权限以查询指定的公网NAT网关。	read	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
nat:natGateways:update	授予权限以更新指定的公网NAT网关。	write	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
nat:dnatRules:list	授予权限以查询公网NAT网关DNAT规则列表。	list	dnatRule *	g:EnterpriseProjectId
nat:dnatRules:create	授予权限以创建公网NAT网关DNAT规则。	write	gateway *	g:ResourceTag/<tag-key>
			dnatRule *	-
			publicip	-
			globalEip	-
			port	-
			-	g:EnterpriseProjectId
nat:dnatRules:get	授予权限以查询指定的公网NAT网关DNAT规则。	read	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			dnatRule *	g:EnterpriseProjectId
nat:dnatRules:update	授予权限以更新指定的公网NAT网关DNAT规则。	write	gateway *	g:ResourceTag/<tag-key>
			dnatRule *	-
			publicip	-
			globalEip	-
			port	-
			-	g:EnterpriseProjectId
nat:dnatRules:delete	授予权限以删除指定的公网NAT网关DNAT规则。	write	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			dnatRule *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
nat:snatRules:list	授予权限以查询公网NAT网关SNAT规则列表。	list	snatRule *	g:EnterpriseProjectId
nat:snatRules:create	授予权限以创建公网NAT网关SNAT规则。	write	gateway *	g:ResourceTag/<tag-key>
			snatRule *	-
			publicip	-
			globalEip	-
			subnet	-
			-	g:EnterpriseProjectId
nat:snatRules:get	授予权限以查询指定的公网NAT网关SNAT规则。	read	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			snatRule *	g:EnterpriseProjectId
nat:snatRules:update	授予权限以更新指定的公网NAT网关SNAT规则。	write	gateway *	g:ResourceTag/<tag-key>
			snatRule *	-
			publicip	-
			globalEip	-
			-	g:EnterpriseProjectId
nat:snatRules:delete	授予权限以删除指定的公网NAT网关SNAT规则。	write	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			snatRule *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
nat:privateNatGateways:createTags	授予权限以创建私网NAT网关标签。	tagging	privateGateway *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
nat:privateNatGateways:deleteTags	授予权限以删除指定的私网NAT网关标签。	tagging	privateGateway *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
nat:privateNatGateways:listTags	授予权限以查询私网NAT网关标签。	list	privateGateway	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
nat:privateNatTransitIps:createTags	授予权限以创建私网NAT中转IP标签。	tagging	privateTransitIp *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
nat:privateNatTransitIps:deleteTags	授予权限以删除指定的私网NAT中转IP标签。	tagging	privateTransitIp *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
nat:privateNatTransitIps:listTags	授予权限以查询私网NAT中转IP标签。	list	privateTransitIp	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
nat:natGateways:createTags	授予权限以创建公网NAT网关标签。	tagging	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
nat:natGateways:deleteTags	授予权限以删除指定的公网NAT网关标签。	tagging	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
nat:natGateways:listTags	授予权限以查询公网NAT网关标签。	list	gateway	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

NAT的API通常对应着一个或多个授权项。表5-32展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-32 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/private-nat/gateways	nat:privateNatGateways:list	-
POST /v3/{project_id}/private-nat/gateways	nat:privateNatGateways:create	-
DELETE /v3/{project_id}/private-nat/gateways/{gateway_id}	nat:privateNatGateways:delete	-
GET /v3/{project_id}/private-nat/gateways/{gateway_id}	nat:privateNatGateways:get	-

API	对应的授权项	依赖的授权项
PUT /v3/{project_id}/private-nat/gateways/{gateway_id}	nat:privateNatGateways:update	-
GET /v3/{project_id}/private-nat/dnat-rules	nat:privateNatDnatRules:list	-
POST /v3/{project_id}/private-nat/dnat-rules	nat:privateNatDnatRules:create	-
DELETE /v3/{project_id}/private-nat/dnat-rules/{dnat_rule_id}	nat:privateNatDnatRules:delete	-
GET /v3/{project_id}/private-nat/dnat-rules/{dnat_rule_id}	nat:privateNatDnatRules:get	-
PUT /v3/{project_id}/private-nat/dnat-rules/{dnat_rule_id}	nat:privateNatDnatRules:update	-
GET /v3/{project_id}/private-nat/snat-rules	nat:privateNatSnatRules:list	-
POST /v3/{project_id}/private-nat/snat-rules	nat:privateNatSnatRules:create	-
DELETE /v3/{project_id}/private-nat/snat-rules/{snat_rule_id}	nat:privateNatSnatRules:delete	-
GET /v3/{project_id}/private-nat/snat-rules/{snat_rule_id}	nat:privateNatSnatRules:get	-
PUT /v3/{project_id}/private-nat/snat-rules/{snat_rule_id}	nat:privateNatSnatRules:update	-
GET /v3/{project_id}/private-nat/transit-ips	nat:privateNatTransitIps:list	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/private-nat/transit-ips	nat:privateNatTransitIps:create	-
DELETE /v3/{project_id}/private-nat/transit-ips/{transit_ip_id}	nat:privateNatTransitIps:delete	-
GET /v3/{project_id}/private-nat/transit-ips/{transit_ip_id}	nat:privateNatTransitIps:get	-
GET /v2/{project_id}/nat_gateways	nat:natGateways:list	-
POST /v2/{project_id}/nat_gateways	nat:natGateways:create	-
DELETE /v2/{project_id}/nat_gateways/{nat_gateway_id}	nat:natGateways:delete	-
GET /v2/{project_id}/nat_gateways/{nat_gateway_id}	nat:natGateways:get	-
PUT /v2/{project_id}/nat_gateways/{nat_gateway_id}	nat:natGateways:update	-
GET /v2/{project_id}/dnat_rules	nat:dnatRules:list	-
POST /v2/{project_id}/dnat_rules	nat:dnatRules:create	eip:publicIps:associateInstance
GET /v2/{project_id}/dnat_rules/{dnat_rule_id}	nat:dnatRules:get	-

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/dnat_rules/{dnat_rule_id}	nat:dnatRules:update	• eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
POST /v2/{project_id}/dnat_rules/batch	nat:dnatRules:create	eip:publicIps:associateInstance
DELETE /v2/{project_id}/nat_gateways/{nat_gateway_id}/dnat_rules/{dnat_rule_id}	nat:dnatRules:delete	eip:publicIps:disassociateInstance
GET /v2/{project_id}/snat_rules	nat:snatRules:list	-
POST /v2/{project_id}/snat_rules	nat:snatRules:create	eip:publicIps:associateInstance
GET /v2/{project_id}/snat_rules/{snat_rule_id}	nat:snatRules:get	-
PUT /v2/{project_id}/snat_rules/{snat_rule_id}	nat:snatRules:update	• eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
DELETE /v2/{project_id}/nat_gateways/{nat_gateway_id}/snat_rules/{snat_rule_id}	nat:snatRules:delete	eip:publicIps:disassociateInstance
POST /v3/{project_id}/private-nat-gateways/resource_instances/action	nat:privateNatGateways:listTags	-
POST /v3/{project_id}/private-nat-gateways/{resource_id}/tags/action	nat:privateNatGateways:createTags	nat:privateNatGateways:deleteTags

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/private-nat-gateways/{resource_id}/tags	nat:privateNatGateways:createTags	-
GET /v3/{project_id}/private-nat-gateways/{resource_id}/tags	nat:privateNatGateways:listTags	-
DELETE /v3/{project_id}/private-nat-gateways/{resource_id}/tags/{key}	nat:privateNatGateways:deleteTags	-
GET /v3/{project_id}/private-nat-gateways/tags	nat:privateNatGateways:listTags	-
POST /v3/{project_id}/transit-ips/resource_instances/action	nat:privateNatTransitIps:listTags	-
POST /v3/{project_id}/transit-ips/{resource_id}/tags/action	nat:privateNatTransitIps:createTags	nat:privateNatTransitIps:deleteTags
POST /v3/{project_id}/transit-ips/{resource_id}/tags	nat:privateNatTransitIps:createTags	-
GET /v3/{project_id}/transit-ips/{resource_id}/tags	nat:privateNatTransitIps:listTags	-
DELETE /v3/{project_id}/transit-ips/{resource_id}/tags/{key}	nat:privateNatTransitIps:deleteTags	-
GET /v3/{project_id}/transit-ips/tags	nat:privateNatTransitIps:listTags	-

API	对应的授权项	依赖的授权项
POST /v2.0/{project_id}/nat_gateways/resource_instances/action	nat:natGateways:listTags	-
POST /v2.0/{project_id}/nat_gateways/{nat_gateway_id}/tags/action	nat:natGateways:createTags	nat:natGateways:deleteTags
POST /v2.0/{project_id}/nat_gateways/{nat_gateway_id}/tags	nat:natGateways:createTags	-
GET /v2.0/{project_id}/nat_gateways/{nat_gateway_id}/tags	nat:natGateways:listTags	-
DELETE /v2.0/{project_id}/nat_gateways/{nat_gateway_id}/tags/{key}	nat:natGateways:deleteTags	-
GET /v2.0/{project_id}/nat_gateways/tags	nat:natGateways:listTags	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-33**中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

NAT定义了以下可以在自定义SCP的Resource元素中使用的资源类型。

表 5-33 NAT 支持的资源类型

资源类型	URN
snatRule	nat:<region>:<account-id>:snatRule:<snat-rule-id>
privateSnatRule	nat:<region>:<account-id>:privateSnatRule:<private-snat-rule-id>

资源类型	URN
port	vpc:<region>:<account-id>:port:<port-id>
privateGateway	nat:<region>:<account-id>:privateGateway:<private-gateway-id>
vpc	vpc:<region>:<account-id>:vpc:<vpc-id>
publicip	vpc:<region>:<account-id>:publicip:<publicip-id>
gateway	nat:<region>:<account-id>:gateway:<gateway-id>
privateTransitIp	nat:<region>:<account-id>:privateTransitIp:<private-transit-ip-id>
dnatRule	nat:<region>:<account-id>:dnatRule:<dnat-rule-id>
globalEip	eip:<region>:<account-id>:globalEip:<geip-id>
privateDnatRule	nat:<region>:<account-id>:privateDnatRule:<private-dnat-rule-id>
subnet	vpc:<region>:<account-id>:subnet:<subnet-id>

条件（Condition）

NAT服务不支持在SCP中的条件键中配置服务级的条件键。NAT可以使用适用于所有服务的全局条件键，请参考请参考全局条件键。

5.10.2.4 弹性负载均衡 ELB

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。

  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于ELB定义的资源类型的详细信息请参见**资源类型（Resource）**。

- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于ELB定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下ELB的相关操作。

表 5-34 ELB 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
elb:flavors:show	授予查询指定规格的详情。	read	flavor *	-
elb:flavors:list	授予查询规格详情列表的权限。	list	flavor *	-
elb:quotas:list	授予查询配额列表的权限。	list	-	-
elb:quotas:show	授予查询可以创建指定类型资源的最大数量的权限。	read	-	-
elb:availability-zones:list	授予查询可用区列表的权限。	list	availabilityZone *	-
			-	g:EnterpriseProjectId
elb:loadbalancers:list	授予查询负载均衡器实例列表。	list	loadbalancer *	-
			-	g:EnterpriseProjectId
elb:loadbalancers:show	授予获取负载均衡器实例详情的权限。	read	loadbalancer *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
elb:loadbalancers:create	授予创建负载均衡器实例的权限。	write	loadbalancer *	-
			subnet	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
elb:loadbalancers:update	授予更新负载均衡器实例的权限。	write	subnet	-
			loadbalancer *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
elb:loadbalancers:delete	授予删除负载均衡器实例的权限。	write	loadbalancer *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
elb:listeners:create	授予创建监听器的权限。	write	listener *	g:EnterpriseProjectId
			loadbalancer *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
elb:listeners:update	授予修改监听器的权限。	write	listener *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
elb:listeners:list	授予查询监听器列表的权限。	list	listener *	-
			-	g:EnterpriseProjectId
elb:listeners:show	授予获取监听器详情的权限。	read	listener *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
elb:listeners:delete	授予删除监听器的权限。	write	listener *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
elb:certificates:list	授予查询证书列表的权限。	list	certificate *	-
			-	g:EnterpriseProjectId
elb:certificates:show	授予获取证书详情的权限。	read	certificate *	-
elb:certificates:create	授予创建证书的权限。	write	certificate *	-
			-	g:EnterpriseProjectId
elb:certificates:update	授予修改证书的权限。	write	certificate *	-
elb:certificates:delete	授予删除证书的权限。	write	certificate *	-
elb:certificates:setPrivateKeyEcho	授予设置证书私钥回显开关的权限。	write	-	-
elb:certificates:getPrivateKeyEcho	授予查询证书私钥回显开关的权限。	write	-	-
elb:agreements:list	授予查询签署记录列表的权限。	list	agreement *	-
elb:agreements:show	授予获取签署信息详情的权限。	read	agreement *	-
elb:agreements:create	授予创建签署记录的权限。	write	agreement *	-
elb:agreements:update	授予修改签署记录的权限。	write	agreement *	-
elb:healthmonitors:create	授予创建健康检查的权限。	write	healthmonitor *	g:EnterpriseProjectId
			pool *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
elb:healthmonitors:update	授予修改健康检查的权限。	write	healthmonitor *	g:EnterpriseProjectId
elb:healthmonitors:delete	授予删除健康检查的权限。	write	healthmonitor *	g:EnterpriseProjectId
elb:healthmonitors:show	授予获取健康检查详情的权限。	read	healthmonitor *	g:EnterpriseProjectId
elb:healthmonitors:list	授予查询健康检查列表的权限。	list	healthmonitor *	-
			-	g:EnterpriseProjectId
elb:ipgroups:list	授予查询IP地址组列表的权限。	list	ipgroup *	-
			-	g:EnterpriseProjectId
elb:ipgroups:show	授予获取IP地址组详情的权限。	read	ipgroup *	-
elb:ipgroups:create	授予创建IP地址组的权限。	write	ipgroup *	-
			-	g:EnterpriseProjectId
elb:ipgroups:update	授予修改IP地址组的权限。	write	ipgroup *	-
elb:ipgroups:delete	授予删除IP地址组的权限。	write	ipgroup *	-
elb:l7policies:create	授予创建7层转发策略的权限。	write	listener *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			l7policy *	g:EnterpriseProjectId
			pool	g:EnterpriseProjectId
elb:l7policies:update	授予修改7层转发策略的权限。	write	l7policy *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
			listener	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			pool	g:EnterpriseProjectId
elb:l7policies:delete	授予删除7层转发策略的权限。	write	l7policy *	g:EnterpriseProjectId
elb:l7policies:show	授予获取转发策略详情的权限。	read	l7policy *	g:EnterpriseProjectId
elb:l7policies:list	授予查询转发策略的权限。	list	l7policy *	-
			-	g:EnterpriseProjectId
elb:l7rules:create	授予创建7层转发规则的权限。	write	l7rule *	g:EnterpriseProjectId
			l7policy *	g:EnterpriseProjectId
elb:l7rules:update	授予修改7层转发规则的权限。	write	l7rule *	g:EnterpriseProjectId
elb:l7rules:list	授予查询转发规则的权限。	list	l7policy *	-
			l7rule *	-
			-	g:EnterpriseProjectId
elb:l7rules:show	授予获取7层转发规则详情的权限。	read	l7rule *	g:EnterpriseProjectId
elb:l7rules:delete	授予删除7层转发规则的权限。	write	l7rule *	g:EnterpriseProjectId
elb:logtanks:list	授予查询云日志列表的权限。	list	logtank *	-
			-	g:EnterpriseProjectId
elb:logtanks:show	授予获取云日志详情的权限。	read	logtank *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
elb:logtanks:create	授予创建云日志的权限。	write	logtank *	g:EnterpriseProjectId
			loadbalancer *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
elb:logtanks:update	授予修改云日志的权限。	write	logtank *	g:EnterpriseProjectId
elb:logtanks:delete	授予删除云日志的权限。	write	logtank *	g:EnterpriseProjectId
elb:pools:list	授予查询后端服务器组列表的权限。	list	pool *	-
			-	g:EnterpriseProjectId
elb:pools:show	授予获取后端服务器组详情的权限。	read	pool *	g:EnterpriseProjectId
elb:pools:create	授予创建后端服务器组的权限。	write	loadbalancer	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			listener	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			pool *	g:EnterpriseProjectId
elb:pools:update	授予修改后端服务器组的权限。	write	pool *	g:EnterpriseProjectId
elb:pools:delete	授予删除后端服务器组的权限。	write	pool *	g:EnterpriseProjectId
elb:members:list	授予查询后端服务器列表的权限。	list	pool	-
			member *	-
			-	g:EnterpriseProjectId
elb:members:show	授予获取后端服务器详情的权限。	read	member *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
elb:members:create	授予创建后端服务器的权限。	write	member *	g:EnterpriseProjectId
			pool *	g:EnterpriseProjectId
			subnet	-
elb:members:update	授予修改后端服务器的权限。	write	member *	g:EnterpriseProjectId
elb:members:delete	授予删除后端服务器的权限。	write	member *	g:EnterpriseProjectId
elb:security-policies:list	授予查询安全策略的权限。	list	securityPolicy *	-
			-	g:EnterpriseProjectId
elb:security-policies:show	授予获取安全策略详情的权限。	read	securityPolicy *	-
elb:security-policies:create	授予创建安全策略的权限。	write	securityPolicy *	-
			-	g:EnterpriseProjectId
elb:security-policies:update	授予修改安全策略的权限。	write	securityPolicy *	-
elb:security-policies:delete	授予删除安全策略的权限。	write	securityPolicy *	-

ELB的API通常对应着一个或多个授权项。表5-35展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-35 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/elb/flavors	elb:flavors:list	-
GET /v3/{project_id}/elb/flavors/{flavor_id}	elb:flavors:show	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/elb/quotas/details	elb:quotas:list	-
GET /v3/{project_id}/elb/quotas	elb:quotas:show	-
POST /v3/{project_id}/elb/loadbalancers	elb:loadbalancers:create	-
DELETE /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}	elb:loadbalancers:delete	-
DELETE /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/force-elb	elb:loadbalancers:delete	-
GET /v3/{project_id}/elb/loadbalancers	elb:loadbalancers:list	-
GET /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}	elb:loadbalancers:show	-
GET /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/statuses	elb:loadbalancers:show	-
PUT /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}	elb:loadbalancers:update	-
POST /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/availability-zone/batch-remove	elb:loadbalancers:update	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/availability-zone/batch-add	elb:loadbalancers:update	-
POST /v3/{project_id}/elb/ipgroups	elb:ipgroups:create	-
DELETE /v3/{project_id}/elb/ipgroups/{ipgroup_id}	elb:ipgroups:delete	-
GET /v3/{project_id}/elb/ipgroups	elb:ipgroups:list	-
GET /v3/{project_id}/elb/ipgroups/{ipgroup_id}	elb:ipgroups:show	-
PUT /v3/{project_id}/elb/ipgroups/{ipgroup_id}	elb:ipgroups:update	-
POST /v3/{project_id}/elb/ipgroups/{ipgroup_id}/iplist/create-or-update	elb:ipgroups:update	-
POST /v3/{project_id}/elb/ipgroups/{ipgroup_id}/iplist/batch-delete	elb:ipgroups:update	-
POST /v3/{project_id}/elb/security-policies	elb:security-policies:create	-
DELETE /v3/{project_id}/elb/security-policies/{security_policy_id}	elb:security-policies:delete	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/elb/security-policies	elb:security-policies:list	-
GET /v3/{project_id}/elb/system-security-policies	elb:security-policies:list	-
GET /v3/{project_id}/elb/security-policies/{security_policy_id}	elb:security-policies:show	-
PUT /v3/{project_id}/elb/security-policies/{security_policy_id}	elb:security-policies:update	-
POST /v3/{project_id}/elb/pools/{pool_id}/members	elb:members:create	-
DELETE /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}	elb:members:delete	-
GET /v3/{project_id}/elb/pools/{pool_id}/members	elb:members:list	-
GET /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}	elb:members:show	-
PUT /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}	elb:members:update	-
POST /v3/{project_id}/elb/pools/{pool_id}/members/batch-update	elb:members:update	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/elb/pools/{pool_id}/members/batch-add	elb:members:create	-
POST /v3/{project_id}/elb/pools/{pool_id}/members/batch-delete	elb:members:delete	-
POST /v3/{project_id}/elb/pools	elb:pools:create	-
DELETE /v3/{project_id}/elb/pools/{pool_id}	elb:pools:delete	-
GET /v3/{project_id}/elb/pools	elb:pools:list	-
GET /v3/{project_id}/elb/pools/{pool_id}	elb:pools:show	-
PUT /v3/{project_id}/elb/pools/{pool_id}	elb:pools:update	-
POST /v3/{project_id}/elb/master-slave-pools	elb:pools:create	-
GET /v3/{project_id}/elb/master-slave-pools	elb:pools:list	-
GET /v3/{project_id}/elb/master-slave-pools/{pool_id}	elb:pools:show	-
DELETE /v3/{project_id}/elb/master-slave-pools/{pool_id}	elb:pools:delete	-
POST /v3/{project_id}/elb/listeners	elb:listeners:create	-

API	对应的授权项	依赖的授权项
DELETE /v3/{project_id}/elb/listeners/{listener_id}	elb:listeners:delete	-
DELETE /v3/{project_id}/elb/listeners/{listener_id}/force	elb:listeners:delete	-
GET /v3/{project_id}/elb/listeners	elb:listeners:list	-
GET /v3/{project_id}/elb/listeners/{listener_id}	elb:listeners:show	-
PUT /v3/{project_id}/elb/listeners/{listener_id}	elb:listeners:update	-
POST /v3/{project_id}/elb/healthmonitors	elb:healthmonitors:create	-
DELETE /v3/{project_id}/elb/healthmonitors/{healthmonitor_id}	elb:healthmonitors:delete	-
GET /v3/{project_id}/elb/healthmonitors	elb:healthmonitors:list	-
GET /v3/{project_id}/elb/healthmonitors/{healthmonitor_id}	elb:healthmonitors:show	-
PUT /v3/{project_id}/elb/healthmonitors/{healthmonitor_id}	elb:healthmonitors:update	-
GET /v3/{project_id}/elb/availability-zones	elb:availability-zones:list	-
GET /v3/{project_id}/elb/preoccupy-ip-num	elb:loadbalancers:show	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/elb/logtanks	elb:logtanks:create	-
DELETE /v3/{project_id}/elb/logtanks/{logtank_id}	elb:logtanks:delete	-
GET /v3/{project_id}/elb/logtanks	elb:logtanks:list	-
GET /v3/{project_id}/elb/logtanks/{logtank_id}	elb:logtanks:show	-
PUT /v3/{project_id}/elb/logtanks/{logtank_id}	elb:logtanks:update	-
POST /v3/{project_id}/elb/certificates	elb:certificates:create	-
DELETE /v3/{project_id}/elb/certificates/{certificate_id}	elb:certificates:delete	-
GET /v3/{project_id}/elb/certificates	elb:certificates:list	-
GET /v3/{project_id}/elb/certificates/{certificate_id}	elb:certificates:show	-
PUT /v3/{project_id}/elb/certificates/{certificate_id}	elb:certificates:update	-
POST /v3/{project_id}/elb/l7policies	elb:l7policies:create	-
DELETE /v3/{project_id}/elb/l7policies/{l7policy_id}	elb:l7policies:delete	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/elb/l7policies	elb:l7policies:list	-
GET /v3/{project_id}/elb/l7policies/{l7policy_id}	elb:l7policies:show	-
PUT /v3/{project_id}/elb/l7policies/{l7policy_id}	elb:l7policies:update	-
POST /v3/{project_id}/elb/l7policies/batch-update-priority	elb:l7policies:update	-
POST /v3/{project_id}/elb/l7policies/{l7policy_id}/rules	elb:l7rules:create	-
DELETE /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}	elb:l7rules:delete	-
GET /v3/{project_id}/elb/l7policies/{l7policy_id}/rules	elb:l7rules:list	-
GET /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}	elb:l7rules:show	-
PUT /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}	elb:l7rules:update	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-36**中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅

作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

ELB定义了以下可以在自定义SCP的Resource元素中使用的资源类型。

表 5-36 ELB 支持的资源类型

资源类型	URN
pool	elb:<region>:<account-id>:pool:<pool-id>
agreement	elb:<region>:<account-id>:agreement:<agreement-id>
loadbalancer	elb:<region>:<account-id>:loadbalancer:<loadbalancer-id>
certificate	elb:<region>:<account-id>:certificate:<certificate-id>
healthmonitor	elb:<region>:<account-id>:healthmonitor:<healthmonitor-id>
ipgroup	elb:<region>:<account-id>:ipgroup:<ipgroup-id>
securityPolicy	elb:<region>:<account-id>:securityPolicy:<security-policy-id>
logtank	elb:<region>:<account-id>:logtank:<logtank-id>
availabilityZone	elb:<region>:<account-id>:availabilityZone:<availability-zone-id>
member	elb:<region>:<account-id>:member:<pool-id>/<member-id>
l7policy	elb:<region>:<account-id>:l7policy:<l7policy-id>
l7rule	elb:<region>:<account-id>:l7rule:<l7policy-id>/<l7rule-id>
flavor	elb:<region>:<account-id>:flavor:<flavor-id>
subnet	vpc:<region>:<account-id>:subnet:<subnet-id>
listener	elb:<region>:<account-id>:listener:<listener-id>

条件（Condition）

ELB服务不支持在SCP中的条件键中配置服务级的条件键。ELB可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.2.5 VPC 终端节点 VPCEP

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于VPCEP定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

  关于VPCEP定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下VPCEP的相关操作。

表 5-37 VPCEP 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
vpcep:endpoints:create	授予指定服务创建VPC终端节点的权限。	write	endpoints *	• vpcep:VpceServiceName • vpcep:VpceServiceOrgPath • vpcep:VpceServiceOwner
			vpc *	-
			routeTable	-
			subnet	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
vpcep:endpoints:createInterface	授予指定服务创建接口型VPC终端节点的权限。	write	endpoints *	• vpcep:VpceServiceName • vpcep:VpceServiceOrgPath • vpcep:VpceServiceOwner
			subnet	vpcep:VpcId
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
vpcep:endpoints:delete	授予权限删除终端节点。	write	endpoints *	• g:ResourceTag/<tag-key> • vpcep:VpceServiceName
vpcep:endpoints:list	授予查询终端节点列表。	list	endpoints *	-
			-	g:EnterpriseProjectId
vpcep:endpoints:get	授予权限查询终端节点详情。	read	endpoints *	g:ResourceTag/<tag-key>
vpcep:endpoints:update	授予权限更新终端节点的白名单。	write	endpoints *	• vpcep:VpceServiceName • vpcep:VpceServiceOrgPath • vpcep:VpceServiceOwner • g:ResourceTag/<tag-key>
			routeTable	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			subnet	-
vpcep:endpoints:updateRouteTables	授予权限修改终端节点路由表。	write	endpoints *	g:ResourceTag/<tag-key>
			routeTable *	-
vpcep:endpoints:updatePolicy	授予权限修改终端节点策略。	write	endpoints *	g:ResourceTag/<tag-key>
vpcep:endpoints:deletePolicy	授予权限删除终端节点策略。	write	endpoints *	g:ResourceTag/<tag-key>
vpcep:endpointServices:create	授予权限创建终端节点服务。	write	endpointServices *	vpcep:VpceServicePrivateDnsName
			vpc *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
vpcep:endpointServices:list	授予权限查询终端节点服务列表。	list	endpointServices *	-
			-	g:EnterpriseProjectId
vpcep:endpointServices:get	授予权限查询终端节点服务详情。	read	endpointServices *	g:ResourceTag/<tag-key>
vpcep:endpointServices:update	授予权限修改终端节点服务。	write	endpointServices *	g:ResourceTag/<tag-key>
vpcep:endpointServices:delete	授予权限删除终端节点服务。	write	endpointServices *	g:ResourceTag/<tag-key>
vpcep:endpointServices:updateName	授予权限修改终端节点服务的名称。	write	endpointServices *	-
vpcep:endpointServices:describe	授予权限查询终端节点服务概要。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
vpcep:endpointServices:listPublic	授予权限查询公共终端节点服务列表。	list	endpointServices *	-
vpcep:endpointServices:listPermissions	授予权限查询终端节点服务的白名单列表。	list	endpointServices *	-
vpcep:endpointServices:updatePermissions	授予权限批量添加或移除终端节点服务的白名单。	permission_management	endpointServices *	-
			-	• vpcep:VpceEndpointOrgPath • vpcep:VpceEndpointOwner
vpcep:endpointServices:createPermissions	授予权限批量添加终端节点服务的白名单。	permission_management	endpointServices *	-
			-	• vpcep:VpceEndpointOrgPath • vpcep:VpceEndpointOwner
vpcep:endpointServices:deletePermissions	授予权限批量移除终端节点服务的白名单。	permission_management	endpointServices *	-
vpcep:endpointServices:updatePermissionsDescription	授予权限更新终端节点服务白名单描述。	write	endpointServices *	-
vpcep:endpointServices:listConnections	授予权限查询连接终端节点服务的连接列表。	list	endpointServices *	-
vpcep:endpointServices:updateConnections	授予权限接受或拒绝终端节点的连接。	write	endpointServices *	-
vpcep:endpointServices:updateConnectionDescription	授予权限更新终端节点连接描述。	write	endpointServices *	-
vpcep::listResourceTags	授予权限根据标签查询资源实例。	list	endpoints	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			endpointServices	-
vpcep::updateResourceTags	授予权限为指定Endpoint Service或Endpoint批量添加或删除标签。	tagging	endpoints	-
			endpointServices	-
vpcep::getProjectTags	授予权限查询租户资源标签。	read	endpoints	-
			endpointServices	-
vpcep::getResourceTags	授予权限查询租户下某个资源标签。	read	endpoints	-
			endpointServices	-
vpcep::listQuotas	授予权限查询用户的资源配额，包括终端节点服务和终端节点。	read	-	-
vpcep::listVersionDetails	授予权限查询VPC终端节点接口版本列表。	list	-	-
vpcep::listSpecifiedVersion	授予权限查询指定VPC终端节点接口版本信息。	list	-	-

VPCEP的API通常对应着一个或多个授权项。表5-38展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-38 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/vpc-endpoints	vpcep:endpoints:create	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/interface-vpc-endpoints	vpcep:endpoints:createInterface	-
DELETE /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}	vpcep:endpoints:delete	-
GET /v1/{project_id}/vpc-endpoints	vpcep:endpoints:list	-
GET /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}	vpcep:endpoints:get	-
PUT /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}	vpcep:endpoints:update	-
PUT /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}/routetables	vpcep:endpoints:updateRouteTables	-
PUT /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}/policy	vpcep:endpoints:updatePolicy	-
DELETE /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}/policy	vpcep:endpoints:deletePolicy	-
POST /v1/{project_id}/vpc-endpoint-services	vpcep:endpointServices:create	-
GET /v1/{project_id}/vpc-endpoint-services	vpcep:endpointServices:list	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}	vpcep:endpointServices:get	-
PUT /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}	vpcep:endpointServices:update	-
DELETE /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}	vpcep:endpointServices:delete	-
PUT /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/name	vpcep:endpointServices:updateName	-
GET /v1/{project_id}/vpc-endpoint-services/describe	vpcep:endpointServices:describe	-
GET /v1/{project_id}/vpc-endpoint-services/public	vpcep:endpointServices:listPublic	-
GET /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions	vpcep:endpointServices:listPermissions	-
POST /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions/action	vpcep:endpointServices:updatePermissions	-
POST /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions/batch-create	vpcep:endpointServices:createPermissions	-

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions/batch-delete	vpcep:endpointServices:deletePermissions	-
PUT /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions/{permission_id}	vpcep:endpointServices:updatePermissionsDescription	-
GET /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/connections	vpcep:endpointServices:listConnections	-
POST /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/connections/action	vpcep:endpointServices:updateConnections	-
PUT /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/connections/description	vpcep:endpointServices:updateConnectionDescription	-
POST /v1/{project_id}/{resource_type}/resource_instances/action	vpcep::listResourceTags	-
POST /v1/{project_id}/{resource_type}/{resource_id}/tags/action	vpcep::updateResourceTags	-
GET /v1/{project_id}/{resource_type}/tags	vpcep::getProjectTags	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/{resource_type}/{resource_id}/tags	vpcep::getResourceTags	-
GET /v1/{project_id}/quotas	vpcep::listQuotas	-
GET /	vpcep::listVersionDetails	-
GET /{version}	vpcep::listSpecifiedVersion	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-39中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

VPCEP定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-39 VPCEP 支持的资源类型

资源类型	URN
endpoints	vpcep:<region>:<account-id>:endpoints:<endpoint-id>
endpointServices	vpcep:<region>:<account-id>:endpointServices:<endpoint-service-id>

条件（Condition）

条件（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀为服务缩写，如vpcep:）仅适用于对应服务的操作，详情请参见表5-40。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
  - 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，SCP才能生效。支持的运算符请参见：运算符。

VPCEP定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-40 VPCEP 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
vpcep:VpceServiceName	string	单值	按照终端节点服务名称进行筛选。
vpcep:VpceServiceOwner	string	单值	按照终端节点服务所有者进行筛选。
vpcep:VpceServicePrivateDnsName	string	单值	按您传入的终端节点服DNS名称筛选访问权限。
vpcep:VpceServiceOrgPath	string	单值	按照终端节点服务所有者的组织路径进行筛选。
vpcep:VpceEndpointOrgPath	string	单值	按照终端节点所有者的组织路径进行筛选。
vpcep:VpceEndpointOwner	string	单值	按照终端节点所有者的账号进行筛选。
vpcep:VpcId	string	多值	根据指定的虚拟私有云资源ID过滤访问。

5.10.2.6 云专线 DC

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）也可以使用这些授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。

  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于DC定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于DC定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下DC的相关操作。

表 5-41 DC 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
dcaas:directConnect:create	授予创建物理连接。	write	directConnect *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dcaas:directConnect:update	授予更新指定物理连接信息。	write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:directConnect:delete	授予删除指定物理连接。只适用于按需计费物理连接，对于包周期购买的物理连接通过订单退订的方式删除指定物理连接。	write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:directConnect:get	授予查询指定物理连接详细信息。	read	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:directConnect:list	授予查询租户创建的所有物理连接。	list	directConnect *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	g:EnterpriseProjectId
dcaas:directConnect:createHostedDirectConnect	授予合作伙伴创建托管物理连接。	write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:directConnect:updateHostedDirectConnect	授予合作伙伴更新指定托管物理连接。	write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:directConnect:deleteHostedDirectConnect	授予合作伙伴删除指定托管物理连接。	write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:directConnect:getHostedDirectConnect	授予合作伙伴查询指定托管物理连接。	read	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:directConnect:listHostedDirectConnect	授予合作伙伴查询所有托管物理连接列表。	list	directConnect *	g:EnterpriseProjectId
dcaas:directConnect:createOnestopDirectConnect	授予创建一站式物理连接。	write	directConnect *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dcaas:directConnect:updateOnestopDirectConnect	授予更新指定一站式物理连接。	write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:directConnect:createOrder	授予创建订单用来购买物理连接。	write	directConnect *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dcaas:directConnect:updateOrder	授予更新指定订单，用于物理连接升配或降配。	write	directConnect *	-
dcaas:vgw:create	授予创建虚拟网关。	write	vgw *	-
			vpc	-
			instances	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
dcaas:vgw:update	授予更新指定虚拟网关的信息。	write	vgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:vgw:delete	授予删除指定的虚拟网关。	write	vgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:vgw:get	授予查询指定虚拟网关的详细信息。	read	vgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:vgw:list	授予查询虚拟网关列表。	list	vgw *	-
			-	g:EnterpriseProjectId
dcaas:vif:create	授予创建虚拟接口。	write	vif *	-
			directConnect	-
			lag	-
			vgw	-
			gdgw	-
			connectGateway	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			lgw	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
dcaas:vif:update	授予更新指定虚拟接口。	write	vif *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:vif:delete	授予删除指定虚拟接口。	write	vif *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:vif:get	授予查询指定虚拟接口。	read	vif *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:vif:list	授予查询指定租户所有虚拟接口列表。	list	vif *	-
			-	g:EnterpriseProjectId
dcaas:vif:updateVifExtendAttribute	授予更新指定虚拟接口扩展属性。	write	vif *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:vifPeer:create	授予创建虚拟接口对等体。	write	vifPeer *	-
			vif *	-
dcaas:vifPeer:update	授予更新指定虚拟接口对等体信息。	write	vifPeer *	-
dcaas:vifPeer:delete	授予删除指定虚拟接口对等体。	write	vifPeer *	-
dcaas:vifPeer:get	授予查询指定虚拟接口对等体。	read	vifPeer *	-
dcaas:vifPeer:list	授予查询虚拟接口对等体列表。	list	vifPeer *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dcaas:gdgw:create	授予创建全球接入网关实例。	write	gdgw *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
dcaas:gdgw:update	授予更新指定全球接入网关信息。	write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:gdgw:delete	授予删除指定的全球接入网关。	write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:gdgw:get	授予查询指定全球接入网关实例详情信息。	read	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:gdgw:list	授予查询全球接入网关列表。	list	gdgw *	-
			-	g:EnterpriseProjectId
dcaas:gdgw:createPeerlink	授予创建指定全球接入网关的关联连接。	write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:gdgw:updatePeerlink	授予更新指定全球接入网关的指定关联连接。	write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:gdgw:deletePeerlink	授予删除指定全球接入网关的指定对等连接。	write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:gdgw:getPeerlink	授予查询指定全球接入网关的指定关联连接。	read	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
dcaas:gdgw:listPeerlink	授予查询指定全球接入网关的所有关联连接列表。	list	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:connectGateway:create	授予权限以创建互联网关。	write	connectGateway *	-
dcaas:connectGateway:update	授予权限以更新互联网关。	write	connectGateway *	-
dcaas:connectGateway:delete	授予权限以删除互联网关。	write	connectGateway *	-
dcaas:connectGateway:get	授予权限以查询互联网关详情。	read	connectGateway *	-
dcaas:connectGateway:list	授予权限以查询互联网关列表。	list	connectGateway *	-
dcaas:connectGateway:listGlobalEip	授予权限以查询绑定的geip列表。	list	connectGateway *	-
dcaas:connectGateway:bindGlobalEip	授予权限以绑定geip。	write	connectGateway *	-
dcaas:connectGateway:unbindGlobalEip	授予权限以解绑定geip。	write	connectGateway *	-
dcaas:vif:switchoverTest	授予权限以进行倒换测试。	write	vif *	-
dcaas:vif:listSwitchoverTestRecord	授予权限以获取倒换测试执行记录。	list	vif *	-
dcaas:vif:getSwitchoverTestRecord	授予权限以获取单条倒换测试执行记录。	read	vif *	-
dcaas:resources:batchTagUntag	授予权限以批量增加删除云专线的资源标签。	tagging	directConnect	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			lag	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			vgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			vif	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			gdgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
dcaas:resources:listResourceTag	授予权限以查询云专线的资源标签。	list	directConnect	-
			lag	-
			vgw	-
			vif	-
			gdgw	-
dcaas:resources:listTag	授予权限以查询云专线某个资源类型的标签。	list	directConnect	-
			lag	-
			vgw	-
			vif	-
			gdgw	-
dcaas:resources:tag	授予权限以添加云专线的资源标签。	tagging	directConnect	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			lag	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			vgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			vif	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			gdgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
dcaas:resources:unTag	授予权限以删除云专线的资源标签。	tagging	directConnect	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			lag	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			vgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			vif	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			gdgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	g:TagKeys
dcaas:resources:listByTag	授予根据标签查询云专线资源列表权限。	list	directConnect	-
			lag	-
			vgw	-
			vif	-
			gdgw	-
dcaas:gdgw:listGdgwRouteTable	授予权限以获取专线全球网关的自定义路由表。	list	gdgw *	-
dcaas:gdgw:updateGdgwRouteTable	授予权限以更新专线全球网关的自定义路由表。	write	gdgw *	-
dcaas:quota:listVgwUsage	授予权限以获取专线的VPC下VGW配额。	list	-	-
dcaas:quota:listUsage	授予权限以获取专线的配额。	list	-	-
dcaas:lgw:create	授予创建本地网关权限。	write	lgw *	-
dcaas:lgw:update	授予更新本地网关权限。	write	lgw *	-
dcaas:lgw:delete	授予删除本地网关权限。	write	lgw *	-
dcaas:lgw:get	授予查询本地网关详情权限。	read	lgw *	-
dcaas:lgw:list	授予查询本地网关列表权限。	list	lgw *	-
dcaas:lgwTable:create	授予创建本地网关路由表权限。	write	lgwTable *	-
			lgw *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dcaas:lgwTable:update	授予更新本地网关路由表权限。	write	lgwTable *	-
dcaas:lgwTable:delete	授予删除本地网关路由表权限。	write	lgwTable *	-
dcaas:lgwTable:get	授予查询本地网关路由表详情权限。	read	lgwTable *	-
dcaas:lgwTable:list	授予查询本地网关路由表列表权限。	list	lgwTable *	-
dcaas:lgwTable:createLgwTableRoute	授予创建本地网关路由表路由权限。	write	lgwTable *	-
dcaas:lgwTable:updateLgwTableRoute	授予更新本地网关路由表路由权限。	write	lgwTable *	-
dcaas:lgwTable:deleteLgwTableRoute	授予删除本地网关路由表路由权限。	write	lgwTable *	-
dcaas:lgwTable:getLgwTableRoute	授予查询本地网关路由表路由详情权限。	read	lgwTable *	-
dcaas:lgwTable:listLgwTableRoute	授予查询本地网关路由表路由列表权限。	list	lgwTable *	-
dcaas:lgwTable:batchDeleteLgwTableRoute	授予批量删除本地网关路由表路由权限。	write	lgwTable *	-
dcaas:lgwTable:createLgwTableVpc	授予将本地网关路由表关联至虚拟私有云的权限。	write	lgwTable *	-
			vpc *	-
dcaas:lgwTable:updateLgwTableVpc	授予更新本地网关路由表虚拟私有云权限。	write	lgwTable *	-
dcaas:lgwTable:deleteLgwTableVpc	授予解除本地网关路由表与虚拟私有云关联的权限。	write	lgwTable *	-
dcaas:lgwTable:getLgwTableVpc	授予查询本地网关路由表虚拟私有云详情权限。	read	lgwTable *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dcaas:lgwTable:listLgwTableVpc	授予查询本地网关路由表虚拟私有云列表权限。	list	lgwTable *	-

DC的API通常对应着一个或多个授权项。表5-42展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-42 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/dcaas/direct-connects/{direct_connect_id}	dcaas:directConnect:get	-
GET /v3/{project_id}/dcaas/direct-connects	dcaas:directConnect:list	-
PUT /v3/{project_id}/dcaas/direct-connects/{direct_connect_id}	dcaas:directConnect:update	-
DELETE /v3/{project_id}/dcaas/direct-connects/{direct_connect_id}	dcaas:directConnect:delete	-
GET /v3/{project_id}/dcaas/hosted-connects/{hosted_connect_id}	dcaas:directConnect:getHostedDirectConnect	-
GET /v3/{project_id}/dcaas/hosted-connects	dcaas:directConnect:listHostedDirectConnect	-
POST /v3/{project_id}/dcaas/hosted-connects	dcaas:directConnect:createHostedDirectConnect	-
PUT /v3/{project_id}/dcaas/hosted-connects/{hosted_connect_id}	dcaas:directConnect:updateHostedDirectConnect	-

API	对应的授权项	依赖的授权项
DELETE /v3/{project_id}/dcaas/hosted-connects/{hosted_connect_id}	dcaas:directConnect:deleteHostedDirectConnect	-
GET /v3/{project_id}/dcaas/virtual-gateways/{virtual_gateway_id}	dcaas:vgw:get	-
GET /v3/{project_id}/dcaas/virtual-gateways	dcaas:vgw:list	-
PUT /v3/{project_id}/dcaas/virtual-gateways/{virtual_gateway_id}	dcaas:vgw:update	-
DELETE /v3/{project_id}/dcaas/virtual-gateways/{virtual_gateway_id}	dcaas:vgw:delete	-
POST /v3/{project_id}/dcaas/virtual-gateways	dcaas:vgw:create	er:instances:get vpc:vpcs:get
GET /v3/{project_id}/dcaas/virtual-interfaces/{virtual_interface_id}	dcaas:vif:get	-
GET /v3/{project_id}/dcaas/virtual-interfaces	dcaas:vif:list	-
PUT /v3/{project_id}/dcaas/virtual-interfaces/{virtual_interface_id}	dcaas:vif:update	-
DELETE /v3/{project_id}/dcaas/virtual-interfaces/{virtual_interface_id}	dcaas:vif:delete	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/dcaas/virtual-interfaces	dcaas:vif:create	-
PUT /v3/{project_id}/dcaas/vif-peers/{vif_peer_id}	dcaas:vifPeer:update	-
DELETE /v3/{project_id}/dcaas/vif-peers/{vif_peer_id}	dcaas:vifPeer:delete	-
POST /v3/{project_id}/dcaas/vif-peers	dcaas:vifPeer:create	-
POST /v3/{project_id}/dcaas/switchover-test	dcaas:vif:switchoverTest	-
GET /v3/{project_id}/dcaas/switchover-test	dcaas:vif:listSwitchoverTestRecord	-
GET /v3/{project_id}/dcaas/quotas	dcaas:quota:listUsage	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-43中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

DC定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-43 DC 支持的资源类型

资源类型	URN
instances	er:<region>:<account-id>:instances:<instance-id>
lgw	dcaas:<region>:<account-id>:lgw:<lgw-id>
vif	dcaas:<region>:<account-id>:vif:<vif-id>
lgwTable	dcaas:<region>:<account-id>:lgwTable:<lgwTable-id>
gdgw	dcaas:<region>:<account-id>:gdgw:<gdgw-id>

资源类型	URN
vifPeer	dcaas:<region>:<account-id>:vifPeer:<vifPeer-id>
vpc	vpc:<region>:<account-id>:vpc:<vpc-id>
vgw	dcaas:<region>:<account-id>:vgw:<vgw-id>
directConnect	dcaas:<region>:<account-id>:directConnect:<directConnect-id>
lag	dcaas:<region>:<account-id>:lag:<lag-id>
connectGateway	dcaas:<region>:<account-id>:connectGateway:<connectGateway-id>

条件（Condition）

DC服务不支持在SCP中的条件键中配置服务级的条件键。DC可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.3 容器

5.10.3.1 云容器引擎 CCE

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在策略语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于CCE定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。

- 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
- 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
- 如果此列条件键没有值（-），表示此操作不支持指定条件键。

关于CCE定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下CCE的相关操作。

表 5-44 CCE 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
cce:cluster:createCluster	授予创建集群的权限。	write	cluster *	• g:EnterpriseProjectId • g:TagKeys • g:RequestTag/<tag-key>
cce:cluster:delete	授予删除集群的权限。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:updateCluster	授予更新集群的权限。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:upgrade	授予执行集群版本升级的权限。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:start	授予唤醒休眠集群的权限。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:stop	授予对集群执行休眠操作的权限。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:list	授予查看集群详情列表的权限。	list	cluster *	-
cce:cluster:getCluster	授予查看用户指定集群详情的权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cce:cluster:getEndpoints	授予查看用户指定集群访问地址的权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cce:cluster:resize	授予对集群进行规格变更的权限。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:eipBinding	授予对集群绑定/解绑公网IP的权限。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:generateClientCredential	授予生成集群客户端访问凭据的权限。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:addTags	授予添加集群标签的权限。	tagging	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:TagKeys • g:RequestTag/<tag-key>
cce:cluster:removeTags	授予删除集群标签的权限。	tagging	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:TagKeys • g:RequestTag/<tag-key>
cce:cluster:getConfigurationTemplate	授予查询集群配置模板信息的权限。	read	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:cluster:getLogConfig	授予查询集群当前日志采集配置的权限。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
cce:cluster:updateLogConfig	授予更新集群日志采集配置的权限。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:partition:create	授予接入分区的权限。	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:partition:update	授予更新分区的权限。	write	cluster *	g:EnterpriseProjectId
cce:partition:get	授予查询指定分区详情的权限。	read	cluster *	g:EnterpriseProjectId
cce:partition:list	授予查看指定集群的分区列表。	list	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:nodepool:create	授予创建节点池的权限。	write	cluster *	• cce:ClusterId • evs:Encrypted • g:EnterpriseProjectId
cce:nodepool:delete	授予删除节点池的权限。	write	cluster *	g:EnterpriseProjectId
cce:nodepool:updateNodepool	授予更新节点池的权限。	write	cluster *	-
			-	• evs:Encrypted • g:EnterpriseProjectId
cce:nodepool:getNodepool	授予查询指定节点池详情的权限。	read	cluster *	g:EnterpriseProjectId
cce:nodepool:list	授予查看指定集群的节点池列表。	list	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:nodepool:getConfigurationTemplate	授予查询节点池配置模板的权限。	read	cluster *	g:EnterpriseProjectId
cce:nodepool:getConfiguration	授予查询节点池配置的权限。	read	cluster *	g:EnterpriseProjectId
cce:nodepool:updateConfiguration	授予更新节点池配置的权限。	write	cluster *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cce:node:createNode	授予创建节点的权限。	write	cluster *	• cce:ClusterId • evs:Encrypted • g:EnterpriseProjectId
cce:node:delete	授予删除节点的权限。	write	cluster *	g:EnterpriseProjectId
cce:node:update	授予更新节点的权限。	write	cluster *	g:EnterpriseProjectId
cce:node:getNode	授予查询指定节点详情的权限。	read	cluster *	g:EnterpriseProjectId
cce:node:list	授予查看指定集群的节点列表。	list	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:node:reset	授予重置节点的权限。	write	cluster *	• cce:ClusterId • evs:Encrypted • g:EnterpriseProjectId
cce:node:add	授予纳管节点的权限。	write	cluster *	• cce:ClusterId • evs:Encrypted • g:EnterpriseProjectId
cce:node:remove	授予释放节点的权限。	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:node:migrate	授予在集群间迁移节点的权限。	write	cluster *	• cce:nodeTransferSourceCluster • cce:nodeTransferTargetCluster • g:EnterpriseProjectId
cce:node:sync	授予同步节点基础设施资源状态的权限。	read	cluster *	g:EnterpriseProjectId
cce:quota:get	授予查询CCE服务相关资源配额的权限。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
cce:addonInstance:create	授予创建插件实例的权限。	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:addonInstance:delete	授予删除插件实例的权限。	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:addonInstance:update	授予更新插件实例的权限。	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:addonInstance:get	授予查询指定插件实例详情的权限。	read	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:addonInstance:list	授予查看指定集群的插件实例列表的权限。	list	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:addonInstance:rollback	授予回滚指定插件实例的权限。	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:chart:upload	授予上传应用模板的权限。	write	-	-
cce:chart:delete	授予删除应用模板的权限。	write	-	-
cce:chart:update	授予更新应用模板的权限。	write	-	-
cce:chart:listChart	授予查看应用模板详情列表的权限。	list	-	-
cce:chart:getChart	授予查看用户指定应用模板详情的权限。	read	-	-
cce:chart:download	授予查看用户下载应用模板的权限。	read	-	-
cce:chart:getQuota	授予查看应用模板配额的权限。	read	-	-
cce:release:create	授予创建应用实例的权限。	write	-	• cce:ClusterId • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cce:release:delete	授予删除应用实例的权限。	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:release:update	授予更新应用实例的权限。	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:release:get	授予查询指定应用实例详情的权限。	read	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:release:list	授予查看指定集群的应用实例列表的权限。	list	cluster *	• cce:ClusterId • g:EnterpriseProjectId

CCE的API通常对应着一个或多个授权项。表5-45展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-45 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /api/v3/projects/{project_id}/quotas	cce:quota:get	-
POST /api/v3/projects/{project_id}/clusters	cce:cluster:createCluster	-
DELETE /api/v3/projects/{project_id}/clusters/{cluster_id}	cce:cluster:delete	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}	cce:cluster:updateCluster	-

API	对应的授权项	依赖的授权项
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows	cce:cluster:upgrade	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows	cce:cluster:upgrade	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows/{upgrade_workflow_id}	cce:cluster:upgrade	-
PATCH /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows/{upgrade_workflow_id}	cce:cluster:upgrade	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade	cce:cluster:upgrade	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/retry	cce:cluster:upgrade	-

API	对应的授权项	依赖的授权项
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/tasks/{task_id}	cce:cluster:upgrade	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/continue	cce:cluster:upgrade	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/pause	cce:cluster:upgrade	-
GET /api/v3/clusterupgradefeaturegates	cce:cluster:upgrade	-
GET /api/v3/clusterupgradepaths	cce:cluster:upgrade	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/upgradeinfo	cce:cluster:upgrade	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/postcheck	cce:cluster:upgrade	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/precheck	cce:cluster:upgrade	-

API	对应的授权项	依赖的授权项
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/precheck/tasks	cce:cluster:upgrade	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/precheck/tasks/{task_id}	cce:cluster:upgrade	-
GET /api/v3.1/projects/{project_id}/clusters/{cluster_id}/operation/snapshot/tasks	cce:cluster:upgrade	-
POST /api/v3.1/projects/{project_id}/clusters/{cluster_id}/operation/snapshot	cce:cluster:upgrade	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/tasks	cce:cluster:upgrade	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/awake	cce:cluster:start	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/hibernate	cce:cluster:stop	-

API	对应的授权项	依赖的授权项
GET /api/v3/projects/{project_id}/clusters	cce:cluster:list	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}	cce:cluster:getCluster	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/openapi	cce:cluster:getEndpoints	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/resize	cce:cluster:resize	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/mastereip	cce:cluster:eipBinding	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/clustercert	cce:cluster:generateClientCredential	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/tags/create	cce:cluster:addTags	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/tags/delete	cce:cluster:removeTags	-

API	对应的授权项	依赖的授权项
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/configuration/detail	cce:cluster:getConfigurationTemplate	-
GET /api/v3/projects/{project_id}/cluster/{cluster_id}/log-configs	cce:cluster:getLogConfig	-
PUT /api/v3/projects/{project_id}/cluster/{cluster_id}/log-configs	cce:cluster:updateLogConfig	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/partitions	cce:partition:create	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/partitions/{partition_name}	cce:partition:update	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/partitions/{partition_name}	cce:partition:get	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/partitions	cce:partition:list	-

API	对应的授权项	依赖的授权项
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools	cce:nodepool:create	-
DELETE /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}	cce:nodepool:delete	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}	cce:nodepool:updateNodepool	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}	cce:nodepool:getNodepool	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools	cce:nodepool:list	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}/configuration/detail	cce:nodepool:getConfigurationTemplate	-

API	对应的授权项	依赖的授权项
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}/configuration	cce:nodepool:getConfiguration	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}/configuration	cce:nodepool:updateConfiguration	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes	cce:node:createNode	-
DELETE /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/{node_id}	cce:node:delete	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/{node_id}	cce:node:update	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/{node_id}	cce:node:getNode	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes	cce:node:list	-

API	对应的授权项	依赖的授权项
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/reset	cce:node:reset	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/add	cce:node:add	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/operation/remove	cce:node:remove	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/operation/migrateto/{target_cluster_id}	cce:node:migrate	-
GET /api/v2/projects/{project_id}/clusters/{cluster_id}/nodes/{node_id}/sync	cce:node:sync	-
POST /api/v3/addons	cce:addonInstance:create	-
DELETE /api/v3/addons/{id}	cce:addonInstance:delete	-
PUT /api/v3/addons/{id}	cce:addonInstance:update	-
GET /api/v3/addons/{id}	cce:addonInstance:get	-
GET /api/v3/addons	cce:addonInstance:list	-

API	对应的授权项	依赖的授权项
POST /api/v3/addons/{id}/operation/rollback	cce:addonInstance:rollback	-
POST /v2/charts	cce:chart:upload	-
DELETE /v2/charts/{chart_id}	cce:chart:delete	-
PUT /v2/charts/{chart_id}	cce:chart:update	-
GET /v2/charts/{chart_id}	cce:chart:getChart	-
GET /v2/charts	cce:chart:listChart	-
GET /v2/charts/{chart_id}/archive	cce:chart:download	-
GET /v2/charts/{project_id}/quotas	cce:chart:getQuota	-
POST /cce/cam/v3/clusters/{cluster_id}/releases	cce:release:create	-
DELETE /cce/cam/v3/clusters/{cluster_id}/namespace/{namespace}/releases/{name}	cce:release:delete	-
PUT /cce/cam/v3/clusters/{cluster_id}/namespace/{namespace}/releases/{name}	cce:release:update	-
GET /cce/cam/v3/clusters/{cluster_id}/namespace/{namespace}/releases/{name}	cce:release:get	-
GET /cce/cam/v3/clusters/{cluster_id}/releases	cce:release:list	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-46中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

CCE定义了以下可以在自定义SCP的Resource元素中使用的资源类型。

表 5-46 CCE 支持的资源类型

资源类型	URN
cluster	cce:<region>:<account-id>:cluster:<cluster-name>

条件（Condition）

条件（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如cce:）仅适用于对应服务的操作，详情请参见表5-47。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
- 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，SCP才能生效。支持的运算符请参见：运算符。

CCE定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-47 CCE 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
cce:ClusterId	string	单值	按照在请求中传递的集群ID筛选访问权限。
cce:nodeTransferSourceCluster	string	单值	按照节点迁移的源集群ID筛选访问权限。
cce:nodeTransferTargetCluster	string	单值	按照节点迁移的目的集群ID筛选访问权限。

5.10.3.2 容器镜像服务 SWR

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于SWR定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于SWR定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下SWR的相关操作。

表 5-48 SWR 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
swr:namespace:createNamespace	授予共享版仓库创建组织的权限。	write	namespace *	-
swr:namespace:deleteNamespace	授予共享版仓库删除组织的权限。	write	namespace *	-
swr:namespace:listNamespaces	授予共享版仓库查询组织列表的权限。	list	namespace *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
swr:namespace:getNamespace	授予共享版仓库获取组织详情的权限。	read	namespace *	-
swr:repo:createRepo	授予共享版仓库创建镜像仓库的权限。	write	repo *	-
swr:repo:deleteRepo	授予共享版仓库删除镜像仓库的权限。	write	repo *	-
swr:repo:listRepos	授予共享版仓库查询镜像仓库列表的权限。	list	repo *	-
swr:repo:listSharedRepos	授予共享版仓库查询共享镜像列表的权限。	list	repo *	-
swr:repo:getRepo	授予共享版仓库查询镜像仓库概要信息的权限。	read	repo *	-
swr:repo:updateRepo	授予共享版仓库更新镜像仓库的概要信息的权限。	write	repo *	-
swr:repo:deleteRepoTag	授予共享版仓库删除镜像仓库中指定tag的镜像的权限。	write	repo *	-
swr:repo:createRepoTag	授予共享版仓库创建镜像tag的权限。	write	repo *	-
swr:repo:listRepoTags	授予共享版仓库查询镜像tag列表的权限。	list	repo *	-
swr:repo:createRepoDomain	授予共享版仓库创建共享账号的权限。	permission_management	repo *	-
			-	• swr:TargetAccountId • swr:TargetOrgPath • swr:TargetOrgId

授权项	描述	访问级别	资源类型（*为必须）	条件键
swr:repo:deleteRepoDomain	授予共享版仓库删除共享账号的权限。	permission_management	repo *	-
swr:repo:listRepoDomains	授予共享版仓库获取共享账号列表的权限。	list	repo *	-
swr:repo:getRepoDomain	授予共享版仓库判断共享账号是否存在的权限。	read	repo *	-
swr:repo:updateRepoDomain	授予共享版仓库更新共享账号的权限。	permission_management	repo *	-
swr:repo:createRepoShare	授予共享版仓库创建镜像共享规则的权限。	permission_management	repo *	-
			-	• swr:TargetAccountId • swr:TargetOrgPath • swr:TargetOrgId
swr:repo:deleteRepoShare	授予共享版仓库删除镜像共享规则的权限。	permission_management	repo *	-
swr:repo:listRepoShares	授予共享版仓库获取镜像共享规则列表的权限。	list	repo *	-
swr:repo:getRepoShare	授予共享版仓库查看镜像共享规则的权限。	read	repo *	-
swr:repo:updateRepoShare	授予共享版仓库更新镜像共享规则的权限。	permission_management	repo *	-
swr:repo:createAutoSyncRepoJob	授予共享版仓库创建镜像自动同步任务的权限。	write	repo *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
swr:repo:createManualSyncRepoJob	授予共享版仓库手动同步镜像的权限。	write	repo *	-
swr:repo:deleteAutoSyncRepoJob	授予共享版仓库删除镜像自动同步任务的权限。	write	repo *	-
swr:repo:listAutoSyncRepoJobs	授予共享版仓库获取镜像自动同步任务列表的权限。	list	repo *	-
swr:repo:getSyncRepoJobInfo	授予共享版仓库获取镜像自动同步任务信息的权限。	read	repo *	-
swr:repo:createTrigger	授予共享版仓库创建触发器的权限。	write	repo *	-
swr:repo:deleteTrigger	授予共享版仓库删除触发器的权限。	write	repo *	-
swr:repo:listTriggers	授予共享版仓库获取镜像仓库下的触发器列表的权限。	list	repo *	-
swr:repo:getTrigger	授予共享版仓库获取触发器详情的权限。	read	repo *	-
swr:repo:updateTrigger	授予共享版仓库更新触发器配置的权限。	write	repo *	-
swr:repo:createRetention	授予共享版仓库创建镜像老化规则的权限。	write	repo *	-
swr:repo:deleteRetention	授予共享版仓库删除镜像老化规则的权限。	write	repo *	-
swr:repo:listRetentionHistories	授予共享版仓库获取镜像老化记录的权限。	list	repo *	-
swr:repo:listRetentions	授予共享版仓库获取镜像老化规则列表的权限。	list	repo *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
swr:repo:getRetention	授予共享版仓库获取镜像老化规则记录的权限。	read	repo *	-
swr:repo:updateRetention	授予共享版仓库修改镜像老化规则的权限。	write	repo *	-
swr::createLoginSecret	授予共享版仓库生成临时登录指令的权限。	write	-	-
swr::listQuotas	授予共享版仓库获取配额信息的权限。	list	-	-
swr::getDomainOverview	授予共享版仓库获取租户总览信息的权限。	read	-	-
swr::getDomainResourceReports	授予共享版仓库获取租户资源统计信息的权限。	read	-	-
swr:namespace:multipartUpload	授予共享版仓库分段上传镜像的权限。	write	namespace *	-
swr:namespace:createNamespaceAccess	授予共享版仓库创建组织权限的权限。	permission_management	namespace *	-
swr:namespace:deleteNamespaceAccess	授予共享版仓库删除组织权限的权限。	permission_management	namespace *	-
swr:namespace:getNamespaceAccess	授予共享版仓库查询组织权限的权限。	read	namespace *	-
swr:namespace:updateNamespaceAccess	授予共享版仓库更新组织权限的权限。	permission_management	namespace *	-
swr:repo:createRepoAccess	授予共享版仓库创建镜像权限的权限。	permission_management	repo *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
swr:repo:deleteRepoAccess	授予共享版仓库删除镜像权限的权限。	permission_management	repo *	-
swr:repo:getRepoAccess	授予共享版仓库查询镜像权限的权限。	read	repo *	-
swr:repo:updateRepoAccess	授予共享版仓库更新镜像权限的权限。	permission_management	repo *	-
swr:repo:upload	授予共享版仓库上传镜像的权限。	write	repo *	-
swr:repo:download	授予共享版仓库下载镜像的权限。	read	repo *	-

SWR的API通常对应着一个或多个授权项。表5-49展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-49 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v2/manage/namespaces	swr:namespace:createNamespace	-
DELETE /v2/manage/namespaces/{namespace}	swr:namespace:deleteNamespace	-
GET /v2/manage/namespaces	swr:namespace:listNamespaces	-
GET /v2/manage/namespaces/{namespace}	swr:namespace:getNamespace	-
POST /v2/manage/namespaces/{namespace}/repos	swr:repo:createRepo	-

API	对应的授权项	依赖的授权项
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}	swr:repo:deleteRepo	-
GET /v2/manage/repos	swr:repo:listRepos	-
GET /v2/manage/shared-repositories	swr:repo:listSharedRepos	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}	swr:repo:getRepo	-
PATCH /v2/manage/namespaces/{namespace}/repos/{repository}	swr:repo:updateRepo	-
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/tags/{tag}	swr:repo:deleteRepoTag	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/tags	swr:repo:listRepoTags	-
POST /v2/manage/namespaces/{namespace}/repositories/{repository}/access-domains	swr:repo:createRepoDomain	-
DELETE /v2/manage/namespaces/{namespace}/repositories/{repository}/access-domains/{access_domain}	swr:repo:deleteRepoDomain	-

API	对应的授权项	依赖的授权项
GET /v2/manage/namespaces/{namespace}/repositories/{repository}/access-domains	swr:repo:listRepoDomains	-
GET /v2/manage/namespaces/{namespace}/repositories/{repository}/access-domains/{access_domain}	swr:repo:getRepoDomain	-
PATCH /v2/manage/namespaces/{namespace}/repositories/{repository}/access-domains/{access_domain}	swr:repo:updateRepoDomain	-
POST /v2/manage/namespaces/{namespace}/repos/{repository}/shares	swr:repo:createRepoShare	-
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/shares/{share_id}	swr:repo:deleteRepoShare	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/shares	swr:repo:listRepoShares	-
PATCH /v2/manage/namespaces/{namespace}/repos/{repository}/shares/{share_id}	swr:repo:updateRepoShare	-
POST /v2/manage/namespaces/{namespace}/repos/{repository}/sync_repo	swr:repo:createAutoSyncRepoJob	• swr::createLoginSecret • swr:repo:download • swr:repo:upload

API	对应的授权项	依赖的授权项
POST /v2/manage/namespaces/{namespace}/repos/{repository}/sync_images	swr:repo:createManualSyncRepoJob	• swr::createLoginSecret • swr:repo:download • swr:repo:upload
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/sync_repo	swr:repo:deleteAutoSyncRepoJob	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/sync_repo	swr:repo:listAutoSyncRepoJobs	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/sync_job	swr:repo:getSyncRepoJobInfo	-
POST /v2/manage/namespaces/{namespace}/repos/{repository}/triggers	swr:repo:createTrigger	-
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/triggers/{trigger}	swr:repo:deleteTrigger	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/triggers	swr:repo:listTriggers	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/triggers/{trigger}	swr:repo:getTrigger	-
PATCH /v2/manage/namespaces/{namespace}/repos/{repository}/triggers/{trigger}	swr:repo:updateTrigger	-

API	对应的授权项	依赖的授权项
POST /v2/manage/namespaces/{namespace}/repos/{repository}/retentions	swr:repo:createRetention	-
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/retentions/{retention_id}	swr:repo:deleteRetention	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/retentions/histories	swr:repo:listRetentionHistories	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/retentions	swr:repo:listRetentions	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/retentions/{retention_id}	swr:repo:getRetention	-
PATCH /v2/manage/namespaces/{namespace}/repos/{repository}/retentions/{retention_id}	swr:repo:updateRetention	-
POST /v2/manage/utils/secret	swr::createLoginSecret	-
GET /v2/manage/projects/{project_id}/quotas	swr::listQuotas	-
POST /v2/manage/namespaces/{namespace}/access	swr:namespace:createNamespaceAccess	-

API	对应的授权项	依赖的授权项
DELETE /v2/manage/namespaces/{namespace}/access	swr:namespace:deleteNamespaceAccess	-
GET /v2/manage/namespaces/{namespace}/access	swr:namespace:getNamespaceAccess	-
PATCH /v2/manage/namespaces/{namespace}/access	swr:namespace:updateNamespaceAccess	-
POST /v2/manage/namespaces/{namespace}/repos/{repository}/access	swr:repo:createRepoAccess	-
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/access	swr:repo:deleteRepoAccess	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/access	swr:repo:getRepoAccess	-
PATCH /v2/manage/namespaces/{namespace}/repos/{repository}/access	swr:repo:updateRepoAccess	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-50**中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

SWR定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-50 SWR 支持的资源类型

资源类型	URN
repo	swr:<region>:<account-id>:repo:<namespace-name>/<repo-name>

资源类型	URN
namespace	swr:<region>:<account-id>:namespace:<namespace-name>

条件（Condition）

条件（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如SWR仅适用于对应服务的操作，详情请参见表5-51。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
- 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，SCP才能生效。支持的运算符请参见：运算符。

SWR定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-51 SWR 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
swr:TargetOrgPath	string	单值	按照共享目标账号所处的组织路径进行权限控制。
swr:TargetOrgId	string	单值	按照共享目标账号所处的组织Id进行权限控制。
swr:TargetAccountId	string	单值	按照共享目标账号Id进行权限控制。

5.10.4 大数据

5.10.4.1 数据湖探索 DLI

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

- 如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于DLI定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

  关于DLI定义的条件键的详细信息请参见**条件（Condition）**。

您可以在自定义SCP语句的Action元素中指定以下DLI的相关操作。

表 5-52 DLI 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
dli::operateAuth	授予数据湖探索权限管理权限。	permission_management	-	-
dli::listAuth	授予数据湖探索权限信息查询权限。	list	-	-
dli:variable:list	授予全局变量列表查询权限。	list	variable *	-
dli:variable:create	授予全局变量创建权限。	write	variable *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dli:variable:update	授予全局变量更新权限。	write	variable *	-
dli:variable:delete	授予全局变量删除权限。	write	variable *	-
dli:catalog:list	授予数据目录列表查询权限。	list	-	-
dli:catalog:bind	授予数据目录绑定权限。	write	-	-
dli:catalog:get	授予数据目录详情查询权限。	read	-	-
dli:queue:list	授予队列列表查询权限。	list	queue *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
dli:queue:create	授予队列创建权限。	write	queue *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dli:queue:get	授予队列详情查询权限。	read	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:update	授予队列更新权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:delete	授予队列删除权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
dli:queue:scale	授予队列扩缩容权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:checkConnection	授予地址连通性测试权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:getConnection	授予连通性结果查询权限。	read	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:listPlans	授予查询队列定时扩缩容计划列表权限。	list	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:createPlan	授予创建队列定时扩缩容计划权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:deletePlan	授予删除队列定时扩缩容计划权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:updatePlan	授予更新队列定时扩缩容计划权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:createProperty	授予新增队列配置权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
dli:queue:listProperties	授予查询队列配置列表权限。	list	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:updateProperty	授予更新队列配置权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:deleteProperty	授予删除队列配置权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:jobs:list	授予作业列表查询权限。	list	jobs *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
dli:queue:submitJob	授予队列作业提交权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:jobs:get	授予作业详情查询权限。	read	jobs *	g:ResourceTag/<tag-key>
dli:table:select	授予表查询权限。	read	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:table:insertInto	授予表数据插入权限。	write	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
dli:queue:cancelJob	授予队列作业取消权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:jobs:exportResult	授予作业导出结果权限。	read	jobs *	g:ResourceTag/<tag-key>
dli::checkSql	授予校验SQL语法权限。	write	-	-
dli:database:list	授予数据库列表查询权限。	list	database *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
dli:database:create	授予数据库创建权限。	write	database *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dli:database:update	授予数据库更新权限。	write	database *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:database:delete	授予数据库删除权限。	write	database *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:database:displayAllTables	授予数据库显示所有表权限。	list	database *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
dli:database:createTable	授予数据库创建表权限。	write	database *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:table:update	授予表更新权限。	write	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:table:describe	授予表结构显示权限。	read	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:table:delete	授予表删除权限。	write	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:table:showPartitions	授予表所有分区显示权限。	read	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:sqldefendrule:create	授予创建SQL防御规则权限。	write	-	-
dli:sqldefendrule:list	授予查询SQL防御规则列表权限。	list	-	-
dli:sqldefendrule:update	授予更新SQL防御规则权限。	write	-	-
dli:sqldefendrule:delete	授予删除SQL防御规则权限。	write	-	-
dli:sqldefendrule:get	授予查询SQL防御规则详情权限。	read	-	-
dli:resource:create	授予资源包创建权限。	write	resource *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	• g:RequestTag/<tag-key> • g:TagKeys
dli:resource:get	授予资源包详情查询权限。	read	resource *	g:ResourceTag/<tag-key>
dli:resource:delete	授予资源包删除权限。	write	resource *	g:ResourceTag/<tag-key>
dli:resource:list	授予资源包列表查询权限。	list	resource *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
dli:resource:update	授予资源包更新权限。	write	resource *	g:ResourceTag/<tag-key>
dli:jobs:update	授予作业更新权限。	write	jobs *	g:ResourceTag/<tag-key>
dli:jobs:delete	授予作业删除权限。	write	jobs *	g:ResourceTag/<tag-key>
dli:jobs:create	授予作业创建权限。	write	jobs *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
dli:jobs:startFlinkJob	授予作业启动权限。	write	jobs *	g:ResourceTag/<tag-key>
dli:jobs:stopFlinkJob	授予作业停止权限。	write	jobs *	g:ResourceTag/<tag-key>
dli:jobs:export	授予作业导出权限。	write	jobs *	g:ResourceTag/<tag-key>
dli::createEdgeChannel	授予创建IEF消息通道权限。	write	-	-
dli::reportEdgeJob	授予边缘Flink作业状态信息上报权限。	write	-	-
dli::callbackEdgeJobAction	授予边缘Flink作业Action状态回调权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dli::createEdgeSystemEvent	授予IEF系统事件上报权限。	write	-	-
dli:template:list	授予模板列表查询权限。	list	template *	-
dli:template:create	授予模板创建权限。	write	template *	-
dli:template:update	授予模板更新权限。	write	template *	-
dli:template:delete	授予模板删除权限。	write	template *	-
dli:template:get	授予模板详情查询权限。	read	template *	-
dli:elasticresourcepool:resourceManagement	授予弹性资源池管理资源权限。	write	elasticresourcepool *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:elasticresourcepool:list	授予弹性资源池列表查询权限。	list	elasticresourcepool *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
dli:elasticresourcepool:create	授予弹性资源池创建权限。	write	elasticresourcepool *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dli:elasticresourcepool:update	授予弹性资源池更新权限。	write	elasticresourcepool *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
dli:elasticresourcepool:delete	授予弹性资源池删除权限。	write	elasticresourcepool *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:elasticresourcepool:scale	授予弹性资源池扩缩容权限。	list	elasticresourcepool *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli::createLakehouse	授予lakehouse创建权限。	write	-	-
dli::getLakehouse	授予lakehouse查询权限。	read	-	-
dli:connection:list	授予查询经典型跨源连接列表权限。	list	-	• g:RequestTag/<tag-key> • g:TagKeys
dli:connection:create	授予创建经典型跨源连接权限。	write	-	• g:RequestTag/<tag-key> • g:TagKeys
dli:connection:get	授予查询经典型跨源连接权限。	read	-	-
dli:connection:delete	授予删除经典型跨源连接权限。	write	-	-
dli:edsconnection:get	授予增强型跨源详情查询权限。	read	edsconnection *	g:ResourceTag/<tag-key>
dli:edsconnection:update	授予增强型跨源更新权限。	write	edsconnection *	g:ResourceTag/<tag-key>
dli:edsconnection:delete	授予增强型跨源删除权限。	write	edsconnection *	g:ResourceTag/<tag-key>
dli:edsconnection:list	授予增强型跨源列表查询权限。	list	edsconnection *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	• g:RequestTag/<tag-key> • g:TagKeys
dli:edsconnection:create	授予增强型跨源创建权限。	write	edsconnection *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • dli:VpcId
dli:edsconnection:unbindQueue	授予增强型跨源解绑队列权限。	write	edsconnection *	g:ResourceTag/<tag-key>
dli:edsconnection:bindQueue	授予增强型跨源绑定队列权限。	write	edsconnection *	g:ResourceTag/<tag-key>
dli:datasourceauth:list	授予跨源认证列表查询权限。	list	datasourceauth *	-
dli:datasourceauth:update	授予安全认证信息更新权限。	write	datasourceauth *	-
dli:datasourceauth:create	授予安全认证信息创建权限。	write	datasourceauth *	-
dli:datasourceauth:delete	授予安全认证信息删除权限。	write	datasourceauth *	-
dli:edsconnection:deleteRoute	授予增强型跨源删除路由权限。	write	edsconnection *	g:ResourceTag/<tag-key>
dli:edsconnection:createRoute	授予增强型跨源创建路由权限。	write	edsconnection *	g:ResourceTag/<tag-key>
dli::getQuota	授予查询配额权限。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dli:queue:restart	授予队列重启权限。	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:table:insertOverwriteTable	授予表重写表数据权限。	write	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:catalog:unbind	授予数据目录解绑权限。	write	-	-
dli::listTags	授予标签获取列表权限。	list	-	-
dli::listResourcesByTag	授予标签查询资源列表权限。	list	-	• g:RequestTag/<tag-key> • g:TagKeys
dli::unTagResource	授予删除标签权限。	tagging	queue	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			resource	g:ResourceTag/<tag-key>
			database	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			elasticresourcepool	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			edsconnection	g:ResourceTag/<tag-key>
			jobs	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	• g:RequestTag/<tag-key> • g:TagKeys
dli::listTagsForResource	授予查询指定资源标签的权限。	list	queue	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			resource	g:ResourceTag/<tag-key>
			database	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			elasticresourcepool	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			edsconnection	g:ResourceTag/<tag-key>
			jobs	g:ResourceTag/<tag-key>
dli::createDownloader	授予创建下载任务权限。	write	-	-
dli::tagResource	创建资源标签	tagging	queue	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			resource	g:ResourceTag/<tag-key>
			database	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			elasticresourcepool	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			edsconnection	g:ResourceTag/<tag-key>
			jobs	g:ResourceTag/<tag-key>
dli:jobs:check	校验作业是否存在	read	-	-
dli:jobs:import	作业导入	write	jobs	-
dli:template:check	校验模板是否存在	read	-	-

DLI的API通常对应着一个或多个授权项。表5-53展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-53 API 与授权项的关系（OpenAPI）

API	对应的授权项	依赖的授权项
PUT /v1.0/{project_id}/queues/user-authorization	dli::operateAuth	-
PUT /v1.0/{project_id}/user-authorization	dli::operateAuth	-
GET /v1.0/{project_id}/databases/{database_name}/tables/{table_name}/users	dli::listAuth	-
GET /v1.0/{project_id}/databases/{database_name}/tables/{table_name}/users/{user_name}	dli::listAuth	-
GET /v1.0/{project_id}/databases/{database_name}/users	dli::listAuth	-
GET /v1.0/{project_id}/queues/{queue_name}/users	dli::listAuth	-
GET /v1.0/{project_id}/authorization/privileges	dli::listAuth	-
PUT /v1.0/{project_id}/authorization	dli::operateAuth	-

API	对应的授权项	依赖的授权项
GET /v1.0/{project_id}/variables	dli:variable:list	-
POST /v1.0/{project_id}/variables	dli:variable:create	-
PUT /v1.0/{project_id}/variables/{var_name}	dli:variable:update	-
DELETE /v1.0/{project_id}/variables/{var_name}	dli:variable:delete	-
GET /v3/{project_id}/catalogs	dli:catalog:list	-
POST /v3/{project_id}/catalogs/action	dli:catalog:bind	dli:catalog:unbind
GET /v3/{project_id}/catalogs/{catalog_name}	dli:catalog:get	-
GET /v1.0/{project_id}/queues	dli:queue:list	-
POST /v1.0/{project_id}/queues	dli:queue:create	-
GET /v1.0/{project_id}/queues/{queue_name}	dli:queue:get	-
PUT /v1.0/{project_id}/queues/{queue_name}	dli:queue:update	-
DELETE /v1.0/{project_id}/queues/{queue_name}	dli:queue:delete	-
PUT /v1.0/{project_id}/queues/{queue_name}/action	dli:queue:scale	dli:queue:restart
POST /v1.0/{project_id}/queues/{queue_name}/connection-test	dli:queue:checkConnection	-
GET /v1.0/{project_id}/queues/{queue_name}/connection-test/{task_id}	dli:queue:getConnection	-
GET /v1/{project_id}/queues/{queue_name}/plans	dli:queue:listPlans	-
POST /v1/{project_id}/queues/{queue_name}/plans	dli:queue:createPlan	-
POST /v1/{project_id}/queues/{queue_name}/plans/batch-delete	dli:queue:deletePlan	-
PUT /v1.0/{project_id}/queues/{queue_name}	dli:queue:updatePlan	-
DELETE /v1/{project_id}/queues/{queue_name}/plans/{plan_id}	dli:queue:deletePlan	-
POST /v3/{project_id}/queues/{queue_name}/properties	dli:queue:createProperty	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/queues/{queue_name}/properties	dli:queue:listProperties	-
PUT /v3/{project_id}/queues/{queue_name}/properties	dli:queue:updateProperty	-
DELETE /v3/{project_id}/queues/{queue_name}/properties	dli:queue:deleteProperty	-
GET /v1.0/{project_id}/jobs	dli:jobs:list	-
POST /v1.0/{project_id}/jobs/submit-job	dli:queue:submitJob	-
GET /v1.0/{project_id}/jobs/{job_id}/status	dli:jobs:get	-
GET /v1.0/{project_id}/jobs/{job_id}/detail	dli:jobs:get	-
DELETE /v1.0/{project_id}/jobs/{job_id}	dli:queue:cancelJob	-
GET /v1.0/{project_id}/jobs/{job_id}/preview	dli:jobs:get	-
POST /v1.0/{project_id}/jobs/check-sql	dli::checkSql	-
GET /v1/{project_id}/jobs/{job_id}/progress	dli:jobs:get	-
POST /v1/{project_id}/sql-defend-rules	dli:sqldefendrule:create	-
GET /v1/{project_id}/sql-defend-rules	dli:sqldefendrule:list	-
PUT /v1/{project_id}/sql-defend-rules/{rule_id}	dli:sqldefendrule:update	-
DELETE /v1/{project_id}/sql-defend-rules/{rule_id}	dli:sqldefendrule:delete	-
GET /v1/{project_id}/sql-defend-rules/{rule_id}	dli:sqldefendrule:get	-
POST /v1.0/{project_id}/streaming/jobs/{job_id}/import-savepoint	dli:jobs:update	-
POST /v1.0/{project_id}/streaming/jobs/{job_id}/savepoint	dli:jobs:update	-
GET /v1.0/{project_id}/streaming/jobs/{job_id}	dli:jobs:get	-

API	对应的授权项	依赖的授权项
DELETE /v1.0/{project_id}/streaming/jobs/{job_id}	dli:jobs:delete	-
GET /v1.0/{project_id}/streaming/jobs	dli:jobs:list	-
POST /v1.0/{project_id}/streaming/sql-jobs	dli:jobs:create	-
PUT /v1.0/{project_id}/streaming/sql-jobs/{job_id}	dli:jobs:update	-
POST /v1.0/{project_id}/streaming/flink-jobs	dli:jobs:create	-
PUT /v1.0/{project_id}/streaming/flink-jobs/{job_id}	dli:jobs:update	-
POST /v1.0/{project_id}/streaming/jobs/run	dli:jobs:startFlinkJob	dli:queue:submitJob
POST /v1.0/{project_id}/streaming/jobs/stop	dli:jobs:stopFlinkJob	dli:queue:cancelJob
POST /v1.0/{project_id}/streaming/jobs/delete	dli:jobs:delete	-
GET /v1.0/{project_id}/streaming/jobs/{job_id}/execute-graph	dli:jobs:get	-
POST /v1.0/{project_id}/streaming/jobs/export	dli:jobs:export	-
POST /v1.0/{project_id}/streaming/jobs/import	dli:jobs:import	-
POST /v3/{project_id}/streaming/jobs/{job_id}/gen-graph	dli:jobs:get	-
GET /v1.0/{project_id}/streaming/job-templates	dli:template:list	-
POST /v1.0/{project_id}/streaming/job-templates	dli:template:create	-
PUT /v1.0/{project_id}/streaming/job-templates/{template_id}	dli:template:update	-
DELETE /v1.0/{project_id}/streaming/job-templates/{template_id}	dli:template:delete	-
POST /v1.0/{project_id}/sqls	dli:template:create	-
GET /v1.0/{project_id}/sqls	dli:template:list	-
GET /v1.0/{project_id}/sqls/sample	dli:template:list	-

API	对应的授权项	依赖的授权项
PUT /v1.0/{project_id}/sqls/{template_id}	dli:template:update	-
POST /v1.0/{project_id}/sqls-deletion	dli:template:delete	-
POST /v3/{project_id}/templates	dli:template:create	-
GET /v3/{project_id}/templates	dli:template:list	-
PUT /v3/{project_id}/templates/{template_id}	dli:template:update	-
GET /v3/{project_id}/templates/{template_id}	dli:template:get	-
GET /v2.0/{project_id}/batches	dli:jobs:list	-
POST /v2.0/{project_id}/batches	dli:queue:submitJob	-
GET /v2.0/{project_id}/batches/{batch_id}	dli:jobs:get	-
DELETE /v2.0/{project_id}/batches/{batch_id}	dli:queue:cancelJob	-
GET /v2.0/{project_id}/batches/{batch_id}/log	dli:jobs:get	-
GET /v2.0/{project_id}/batches/{batch_id}/state	dli:jobs:get	-
POST /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/notebook/action	dli:elasticresourcepool:resourceManagement	-
POST /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/notebook/instances	dli:elasticresourcepool:resourceManagement	-
GET /v3/{project_id}/elastic-resource-pools	dli:elasticresourcepool:list	-
POST /v3/{project_id}/elastic-resource-pools	dli:elasticresourcepool:create	-
PUT /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}	dli:elasticresourcepool:update	-
DELETE /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}	dli:elasticresourcepool:delete	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/queues	dli:elasticresourcepool:resourceManagement	-
POST /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/queues	dli:elasticresourcepool:resourceManagement	• dli:queue:create • dli:queue:delete
PUT /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/queues/{queue_name}	dli:elasticresourcepool:resourceManagement	-
GET /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/scale-records	dli:elasticresourcepool:scale	-
POST /v3/{project_id}/orders/elastic-resource-pools	dli:elasticresourcepool:create	-
POST /v3/{project_id}/orders/elastic-resource-pools/specification-change	dli:elasticresourcepool:scale	-
POST /v3/{project_id}/lakehouse	dli::createLakehouse	-
GET /v3/{project_id}/lakehouse	dli::getLakehouse	-
GET /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}	dli:edsconnection:get	-
PUT /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}	dli:edsconnection:update	-
DELETE /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}	dli:edsconnection:delete	-
GET /v2.0/{project_id}/datasource/enhanced-connections	dli:edsconnection:list	-
POST /v2.0/{project_id}/datasource/enhanced-connections	dli:edsconnection:create	-
POST /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}/disassociate-queue	dli:edsconnection:unbindQueue	-
POST /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}/associate-queue	dli:edsconnection:bindQueue	-

API	对应的授权项	依赖的授权项
GET /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}/privileges	dli::listAuth	-
GET /v3/{project_id}/datasource/auth-infos	dli:datasourceauth:list	-
PUT /v3/{project_id}/datasource/auth-infos	dli:datasourceauth:update	-
POST /v3/{project_id}/datasource/auth-infos	dli:datasourceauth:create	-
DELETE /v3/{project_id}/datasource/auth-infos/{auth_info_name}	dli:datasourceauth:delete	-
POST /v3/{project_id}/datasource/enhanced-connections/{connection_id}/routes	dli:edsconnection:deleteRoute	-
DELETE /v3/{project_id}/datasource/enhanced-connections/{connection_id}/routes/{name}	dli:edsconnection:createRoute	-
GET /v3/{project_id}/quotas	dli::getQuota	-
GET /v3/{project_id}/datasource/auth-infos	dli:datasourceauth:list	-
PUT /v3/{project_id}/datasource/auth-infos	dli:datasourceauth:update	-
POST /v3/{project_id}/datasource/auth-infos	dli:datasourceauth:create	-
DELETE /v3/{project_id}/datasource/auth-infos/{auth_info_name}	dli:datasourceauth:delete	-
POST /v3/{project_id}/datasource/enhanced-connections/{connection_id}/routes	dli:edsconnection:createRoute	-
DELETE /v3/{project_id}/datasource/enhanced-connections/{connection_id}/routes/{name}	dli:edsconnection:deleteRoute	-
GET /v3/{project_id}/{resource_type}/tags	dli::listTags	-
POST /v3/{project_id}/{resource_type}/resource-instances/filter	dli::listResourcesByTag	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/{resource_type}/resource-instances/count	dli::listResourcesByTag	-
POST /v3/{project_id}/{resource_type}/{resource_id}/tags/delete	dli::unTagResource	-
GET /v3/{project_id}/{resource_type}/{resource_id}/tags	dli::listTagsForResource	-

表 5-54 API 与授权项的关系（控制台操作相关）

API	对应的授权项	依赖的授权项
GET /v1.0/{project_id}/logs/transfer	dli::getLogTransfer	-
POST /v1.0/{project_id}/logs/history	dli::getLog	-
POST /v1.0/{project_id}/logs/runtime	dli::getLog	-
GET /v1.0/{project_id}/logs/pods	dli::getLog	-
GET /v1.0/{project_id}/logs/pods/{pod_name}	dli::getLog	-
PUT /v1.0/{project_id}/databases/{database_name}/name	dli:database:update	-
POST /v1/{project_id}/streaming/jobs/check	dli:jobs:check	-
POST /v1/{project_id}/streaming/sql/validate	dli::checkSql	-
GET /v1/{project_id}/streaming/jobs/{job_id}/log	dli:jobs:get	-
GET /v1/{project_id}/streaming/jobs/{job_id}/log/{tm_id}	dli:jobs:get	-
GET /v1/{project_id}/streaming/jobs/{job_id}/submitlog	dli:jobs:get	-
POST /v1/{project_id}/streaming/templates/check	dli:template:check	-
GET /v1.0/{project_id}/databases/{database_name}/projects	dli::listAuth	-

API	对应的授权项	依赖的授权项
GET /v1.0/{project_id}/databases/{database_name}/tables/{table_name}/projects	dli::listAuth	-
GET /v1.0/{project_id}/databases/{database_name}/tables/{table_name}/projects/{projectId}	dli::listAuth	-
GET /v1.0/{project_id}/databases/{database_name}/projects/{projectId}	dli::listAuth	-
GET /v1.0/{project_id}/databases/{database_name}/tables/{table_name}/columns/{column_name}/projects/{projectId}	dli::listAuth	-
POST /v1.0/{project_id}/logs/transfer	dli::createLogTransfer	-
POST /v1.0/{project_id}/orders/queues	dli:queue:create	-
PUT /v1.0/{project_id}/orders/queues	dli:queue:scale	-
PUT /v3/{project_id}/queues/{queue_name}/scale-range	dli:queue:scale	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-55中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

DLI定义了以下可以在自定义SCP的Resource元素中使用的资源类型。

表 5-55 DLI 支持的资源类型

资源类型	URN
variable	dli:<region>:<account-id>:variable:<variable-name-with-prefix>
queue	dli:<region>:<account-id>:queue:<queue-name-with-prefix>
jobs	dli:<region>:<account-id>:jobs:<job-id-with-prefix>

资源类型	URN
table	dli:<region>:<account-id>:table:<table-name-with-prefix>
database	dli:<region>:<account-id>:database:<database-name-with-prefix>
resource	dli:<region>:<account-id>:resource:<resource-name-with-prefix>
template	dli:<region>:<account-id>:template:<template-name-with-prefix>
elasticresourcepool	dli:<region>:<account-id>:elasticresourcepool:<elasticresourcepool-name-with-prefix>
edsconnection	dli:<region>:<account-id>:edsconnection:<edsconnection-id-with-prefix>
datasourceauth	dli:<region>:<account-id>:datasourceauth:<datasourceauth-name-with-prefix>

条件（Condition）

条件（Condition）是自定义SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀为服务缩写，如dli:）仅适用于对应服务的操作，详情请参见**表5-56**。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
- 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，SCP才能生效。支持的运算符请参见：运算符。

DLI定义了以下可以在自定义SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-56 DLI 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
dli:VpcId	string	单值	根据虚拟网络ID筛选访问权限。

5.10.5 CDN 与智能边缘

5.10.5.1 内容分发网络 CDN

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在策略语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于CDN定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在策略语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于CDN定义的条件键的详细信息请参见**条件（Condition）**。

您可以在策略语句的Action元素中指定以下CDN的相关操作。

表 5-57 CDN 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
cdn:statistics:queryStats	授予权限查询域名统计数据。	list	domain *	g:EnterpriseProjectId
cdn:statistics:downloadExcel	授予权限下载域名统计数据。	list	domain *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cdn:log:queryLogs	授予权限查询日志数据。	read	domain *	g:EnterpriseProjectId
cdn:charge:modifyChargeMode	授予权限创建或者修改计费模式。	write	-	-
cdn:charge:queryChargeMode	授予权限查询计费模式。	list	-	-
cdn:statistics:querySubscriptionTasks	授予权限查询运营报表。	list	-	-
cdn:statistics:createSubscriptionTasks	授予权限创建运营报表。	write	domain *	-
cdn:statistics:updateSubscriptionTasks	授予权限修改运营报表。	write	domain *	-
cdn:statistics:deleteSubscriptionTasks	授予权限删除运营报表。	write	-	-
cdn:configuration:queryDomainList	授予权限查询域名信息列表。	list	domain *	g:EnterpriseProjectId
cdn:configuration:queryDomains	授予权限查询域名。	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:modifyDomainConfigs	授予权限修改域名配置信息。	write	domain *	g:EnterpriseProjectId
cdn:configuration:modifyOriginConfInfo	授予权限修改域名源站信息配置。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:log:queryLogs	授予权限查询日志数据。	read	domain *	g:EnterpriseProjectId
cdn:statistics:queryStats	授予权限查询域名统计数据。	list	domain *	g:EnterpriseProjectId
cdn:configuration:queryDomainList	授予权限查询域名信息列表。	list	domain *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cdn:configuration:createDomains	授予权限创建域名。	write	domain *	g:EnterpriseProjectId
cdn:configuration:queryDomains	授予权限查询域名。	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:deleteDomains	授予权限删除域名相关信息。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:disableDomains	授予权限禁用域名。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:enableDomains	授予权限启用域名。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:modifyOriginServerInfo	授予权限修改域名源站信息。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:modifyOriginConfInfo	授予权限修改域名源站信息配置。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:queryOriginConfInfo	授予权限查询域名源站配置信息。	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:modifyReferConf	授予权限修改refer白名单配置。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:queryReferConf	授予权限查询refer白名单配置。	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cdn:configuration:queryIpAcl	授予权限查询ip黑白名单。	list	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:modifyIpAcl	授予权限修改ip黑白名单。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:queryCacheRule	授予权限查询域名缓存规则。	list	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:modifyCacheRule	授予权限修改域名缓存规则。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:modifyHttpsConf	授予权限修改域名证书配置。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:queryHttpsConf	授予权限查询域名https配置。	read	domain	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:queryIpInfo	授予权限查ip归属信息。	list	-	-
cdn:configuration:createResHeader	授予权限创建响应头信息。	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:queryResponseHeaderList	授予权限查询响应头信息。	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:batchModifyHttpsConf	授予权限批量修改域名证书配置。	write	domain *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cdn:configuration:queryTags	授予权限查询域名标签列表。	list	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:modifyTags	授予权限修改资源标签。	tagging	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
cdn:configuration:deleteTags	授予权限删除资源标签。	tagging	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
cdn:configuration:refreshCache	授予权限刷新缓存。	write	-	g:EnterpriseProjectId
cdn:configuration:queryRefreshAndPreheatHistoryTask	授予权限查询刷新预热任务记录信息。	list	-	-
cdn:configuration:queryCacheHistoryTask	授予权限查询缓存历史任务信息。	list	-	-
cdn:configuration:preheatCache	授予权限修改预热相关配置。	write	-	g:EnterpriseProjectId
cdn:configuration:queryQuota	授予权限查询当前用户域名、刷新文件、刷新目录和预热的配额。	list	-	-

CDN的API通常对应着一个或多个授权项。**表5-58**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-58 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1.0/cdn/domains	cdn:configuration:queryDomainList	-
POST /v1.0/cdn/domains	cdn:configuration:createDomains	-
DELETE /v1.0/cdn/domains/{domain_id}	cdn:configuration:deleteDomains	-
PUT /v1.0/cdn/domains/{domain_id}/disable	cdn:configuration:disableDomains	-
PUT /v1.0/cdn/domains/{domain_id}/enable	cdn:configuration:enableDomains	-
GET /v1.0/cdn/ip-info	cdn:configuration:queryIpInfo	-
PUT /v1.0/cdn/domains/{domain_id}/private-bucket-access	cdn:configuration:modifyOriginConfInfo	-
PUT /v1.0/cdn/domains/config-https-info	cdn:configuration:batchModifyHttpsConf	-
GET /v1.0/cdn/domains/https-certificate-info	cdn:configuration:queryDomainList	-

API	对应的授权项	依赖的授权项
PUT /v1.1/cdn/configuration/domains/{domain_name}/configs	cdn:configuration:modifyOriginConfInfo	• cdn:configuration:modifyBusinessType • cdn:configuration:modifyOriginServerInfo • cdn:configuration:modifyBackSourceUrlConfig • cdn:configuration:modifyHttpsConf • cdn:configuration:modifyCacheRule • cdn:configuration:modifyReferConf • cdn:configuration:modifyIpAcl • cdn:configuration:modifyUserAgent • cdn:configuration:modifyUrlAuth • cdn:configuration:createResHeader • cdn:configuration:modifyErrorCodeRedirectRule • cdn:configuration:modifyVideoSeek • cdn:configuration:modifyRemoteAuth • cdn:configuration:modifyServiceArea
GET /v1.1/cdn/configuration/domains/{domain_name}/configs	cdn:configuration:queryDomains	-
GET /v1.0/cdn/configuration/tags	cdn:configuration:queryTags	-
POST /v1.0/cdn/configuration/tags	cdn:configuration:modifyTags	-
POST /v1.0/cdn/configuration/tags/batch-delete	cdn:configuration:deleteTags	-

API	对应的授权项	依赖的授权项
POST /v1.0/cdn/content/refresh-tasks	cdn:configuration:refreshCache	-
POST /v1.0/cdn/content/preheating-tasks	cdn:configuration:preheatCache	-
GET /v1.0/cdn/historytasks	cdn:configuration:queryCacheHistoryTask	-
GET /v1.0/cdn/historytasks/{history_tasks_id}/detail	cdn:configuration:queryCacheHistoryTask	-
GET /v1.0/cdn/contentgateway/url-tasks	cdn:configuration:queryRefreshAndPreheatHistoryTask	-
GET /v1.0/cdn/quota	cdn:configuration:queryQuota	-
GET /v1.0/cdn/statistics/top-url	cdn:statistics:queryStats	-
GET /v1.0/cdn/statistics/domain-location-stats	cdn:statistics:queryStats	-
GET /v1.0/cdn/statistics/domain-stats	cdn:statistics:queryStats	-
GET /v1.0/cdn/logs	cdn:log:queryLogs	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-59**中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

CDN定义了以下可以在自定义SCP的Resource元素中使用的资源类型。

表 5-59 CDN 支持的资源类型

资源类型	URN
domain	cdn::<account-id>:domain:<domain-name>

条件（Condition）

CDN服务不支持在SCP中的条件键中配置服务级的条件键。CDN可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.6 数据库

5.10.6.1 云数据库 RDS

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于RDS定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于RDS定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下RDS的相关操作。

表 5-60 RDS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
rds:task:listAll	授予获取任务信息的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
rds:tag:list	授予查询项目标签的权限。	list	-	-
rds:param:listAll	授予获取参数模板列表的权限。	list	-	-
rds:param:listInstanceParamHistories	授予查询实例参数修改历史列表的权限。	list	-	-
rds:databaseUser:list	授予查询数据库用户列表的权限。	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:database:list	授予查询数据库列表的权限。	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:backup:list	授予获取备份列表的权限。	list	-	-
rds:log:setSlowLogSensitiveStatus	授予慢日志明文显示的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:enableSecondLevelMonitoring	授予开启秒级监控的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:tde	授予开启tde的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:openReadonly	授予设置只读参数的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifySynchronizeModel	授予设置主备实例数据同步方式的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
rds:instance:modifyStrategy	授予主备实例倒换策略的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifySSL	授予关闭或开启SSL的权限。	permission_management	-	-
rds:instance:modifyForceSwitch	授予开启强切高可用的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:setAutoEnlargePolicy	授予设置自动扩容策略的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifyBackupPolicy	授予设置自动备份策略的权限。	permission_management	instance	g:EnterpriseProjectId rds:BackupEnabled g:ResourceTag/<tag-key>
rds:instance:extendSpace	授予扩容数据库实例的磁盘空间的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:shrinkSpace	授予缩小数据库实例的磁盘空间的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:database:shrink	授予收缩数据库的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:binlog:setPolicy	授予设置binlog策略的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
rds:auditlog:operate	授予设置审计日志策略的权限。	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getParameter	授予获取指定实例的参数模板的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:param:get	授予获取指定参数模板参数的权限。	read	-	-
rds:instance:getSecondLevelMonitoringConfig	授予查询秒级监控配置的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:log:getErrorLogs	授予查询数据库错误日志的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:log:getSlowLogs	授予查询慢日志的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:log:download	授予日志下载的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:log:setLogSwitchover	授予查询主备切换日志的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getAutoEnlargePolicy	授予查询自动扩容策略的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getBackupPolicy	授予查询备份策略的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
rds:instance:getDBProxy	授予查询数据库代理信息的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getDnsName	授予查询实例域名的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getMsdtcHosts	授予查询MSDTC的hosts的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getProxyFlavors	授予查询数据库代理可变更规格的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getReplicaStatus	授予查询实例复制状态的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getRestoreTime	授予查询实例的可恢复时间段的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:listAll	授予查询数据库实例列表的权限。	read	-	-
rds:instance:get	授予查询数据库单个实例详情的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getEip	授予查实例绑定公网IP信息的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:update	授予修改实例相关信息的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
rds:instance:updateQuota	授予修改项目配额的权限。	read	-	-
rds:instance:listQuotas	授予查询资源配额的权限。	read	-	-
rds:instance:deleteTag	授予批量删除标签的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
			-	g:RequestTag/<tag-key> g:TagKeys
rds:instance:createTag	授予批量增加标签的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
			-	g:RequestTag/<tag-key> g:TagKeys
rds:binlog:get	授予获取binlog的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:binlog:download	授予下载binlog的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:backup:download	授予获取备份下载链接的权限。	read	-	-
rds:auditlog:list	授予实例获取审计日志列表的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:auditlog:download	授予生成审计日志下载链接的权限。	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
rds:instance:listDatabaseVersion	授予查询数据库版本信息的权限。	read	-	-
rds:instance:listFlavors	授予查询规格列表的权限。	read	-	-
rds:instance:listStorageType	授予查询数据库磁盘类型的权限。	read	-	-
rds:coldTable:query	授予冷热分离查询的权限。	read	-	-
rds:task:delete	授予删除任务中心任务的权限。	write	-	-
rds:password:update	授予修改数据库密码的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:param:save	授予保存参数组的权限。	write	-	-
rds:param:reset	授予重置参数组的权限。	write	-	-
rds:param:updateTemplate	授予修改参数模板参数的权限。	write	-	-
rds:instance:updateParameter	授予修改指定实例的参数的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:param:delete	授予删除参数模板的权限。	write	-	-
rds:param:createTemplate	授予创建参数模板的权限。	write	-	-
rds:param:copy	授予复制参数模板的权限。	write	-	-
rds:param:apply	授予应用参数模板的权限。	write	-	-
rds:instance:tableRestore	授予表级恢复的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
rds:instance:switchover	授予手动主备切换的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:singleToHa	授予单机转主备实例的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:haToSingle	授予主备转单机实例的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:setRecycleBin	授予设置回收站策略的权限。	write	-	-
rds:instance:restoreInPlace	授予恢复到已有或当前实例。	write	-	-
rds:instance:restart	授予重启数据库实例的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:stop	授予停止实例的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:start	授予开启实例的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifySpec	授予变更数据库实例的规格的权限。	write	-	-
rds:instance:modifySecurityGroup	授予修改安全组的权限。	write	-	-
rds:instance:modifyPublicAccess	授予绑定和解绑弹性公网IP的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
rds:instance:modifyProxy	授予开启/关闭数据库代理的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifyPort	授予修改端口的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifyIp	授予修改内网IP的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifyHost	授予修改主机权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:updateDnsName	授予修改域名的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:SetMsdtcHosts	授予添加MSDTC主机的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:updateOpsWindow	授予设置实例可维护时间窗的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:updateName	授予修改实例名称的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:updateRemark	授予修改实例备注的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
rds:instance:upgradeDatabaseVersion	授予升级数据库版本的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:deleteInstance	授予删除数据库实例。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:deleteNode	授予删除数据库节点。	write	-	-
rds:instance:createDns	授予创建内网DNS的权限。	write	-	-
rds:instance:create	授予创建数据库实例的权限。	write	-	rds:Encrypted rds:BackupEnabled g:RequestTag/<tag-key> g:TagKeys g:EnterpriseProjectId
rds:instance:batchTableRestore	授予批量表级时间点恢复的权限。	write	-	-
rds:databaseUser:update	授予修改数据库用户名备注的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:databaseUser:drop	授予删除数据库用户的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:databaseUser:create	授予创建数据库用户的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:databasePrivilege:revoke	授予解除数据库账号权限的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
rds:databasePrivilege:grant	授予数据库账号或用户的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:database:drop	授予删除数据库的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:database:update	授予修改数据库的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:database:createDatabase	授予创建数据库的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:binlog:merge	授予合并binlog的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:binlog:delete	授予删除binlog的权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:backup:delete	授予删除手动备份的权限。	write	-	-
rds:backup:create	授予创建手动备份的权限。	write	-	-
rds:instance:buildDrRelation	授予配置灾备实例容灾能力权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifyDRRole	授予灾备升主权限。	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:ltsConfig:update	授予配置日志转存LTS能力权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
rds:coldTable:operate	授予冷热分离操作的权限。	write	-	-

RDS的API通常对应着一个或多个授权项。表5-61展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-61 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/jobs?id={id}	rds:task:listAll	-
GET /v3/{project_id}/tags	rds:tag:list	-
GET /v3/{project_id}/configurations	rds:param:listAll	-
GET /v3/{project_id}/instances/{instance_id}/configuration-histories?offset={offset}&limit={limit}&start_time={start_time}&end_time={end_time}&param_name={param_name}	rds:param:listInstanceParamHistories	-
GET /v3/{project_id}/instances/{instance_id}/db_user/detail?page={page}&limit={limit}	rds:databaseUser:list	-
GET /v3/{project_id}/instances/{instance_id}/database/detail?page={page}&limit={limit}	rds:database:list	-
GET /v3/{project_id}/backups?instance_id={instance_id}	rds:backup:list	-
PUT /v3/{project_id}/instances/{instance_id}/slowlog-sensitization/{status}	rds:log:setSlowLogSensitiveStatus	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/second-level-monitor	rds:instance:enableSecondLevelMonitoring	-
PUT /v3/{project_id}/instances/{instance_id}/tde	rds:instance:tde	-
PUT /v3/{project_id}/instances/{instance_id}/readonly-status	rds:instance:openReadonly	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/failover/mode	rds:instance:modifySynchronizeModel	-

API	对应的授权项	依赖的授权项
PUT /v3/{*project_id*}/instances/{*instance_id*}/failover/strategy	rds:instance:modifyStrategy	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/ssl	rds:instance:modifySSL	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:modifyForceSwitch	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/disk-auto-expansion	rds:instance:setAutoEnlargePolicy	-
PUT /v3/{project_id}/instances/{instance_id}/backups/policy	rds:instance:modifyBackupPolicy	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:extendSpace	-
POST /v3/{project_id}/instances/{instance_id}/db_shrink	rds:database:shrink	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/binlog/clear-policy	rds:binlog:setPolicy	-
PUT /v3/{project_id}/instances/{instance_id}/auditlog-policy	rds:auditlog:operate	-
GET /v3/{project_id}/instances/{instance_id}/configurations	rds:instance:getParameter	-
GET /v3/{project_id}/configurations/{config_id}	rds:param:get	-
GET /v3/{*project_id*}/instances/{*instance_id*}/second-level-monitor	rds:instance:getSecondLevelMonitoringConfig	-
POST /v3/{project_id}/instances/{instance_id}/error-logs	rds:log:getErrorLogs	-
POST /v3/{project_id}/instances/{instance_id}/slow-logs	rds:log:getSlowLogs	-
POST /v3/{project_id}/instances/{instance_id}/slowlog-download	rds:log:download	-
GET /v3/{*project_id*}/instances/{*instance_id*}/disk-auto-expansion	rds:instance:getAutoEnlargePolicy	-
GET /v3/{project_id}/instances/{instance_id}/backups/policy	rds:instance:getBackupPolicy	-
GET /v3/{*project_id*}/instances/{*instance_id*}/proxy	rds:instance:getDBProxy	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/instances/{instance_id}/dns	rds:instance:getDnsName	-
GET /v3/{project_id}/instances/{instance_id}/msdtc/hosts?offset={offset}&limit={limit}	rds:instance:getMsdtcHosts	-
GET /v3/{project_id}/flavors/{database_name}?version_name={version_name}&spec_code={spec_code}	rds:instance:getProxyFlavors	-
GET /v3/{project_id}/instances/{instance_id}/replication/status	rds:instance:getReplicaStatus	-
GET /v3/{project_id}/instances/{instance_id}/restore-time?date={date}	rds:instance:getRestoreTime	-
GET /v3/{project_id}/instances	rds:instance:listAll	-
GET /v3/{project_id}/instances?id={id}&name={name}&type={type}&datastore_type={datastore_type}&vpc_id={vpc_id}&subnet_id={subnet_id}&offset={offset}&limit={limit}&tags={key}={value}	rds:instance:get	-
GET https://{*Endpoint*}/v3/{project_id}/quotas	rds:instance:listQuotas	-
POST /v3/{project_id}/instances/{instance_id}/tags/action	rds:instance:deleteTag	-
POST /v3/{project_id}/instances/{instance_id}/tags/action	rds:instance:createTag	-
GET /v3/{*project_id*}/instances/{*instance_id*}/binlog/clear-policy	rds:binlog:get	-
GET /v3/{project_id}/backup-files?backup_id={backup_id}	rds:backup:download	-
GET /v3/{project_id}/instances/{instance_id}/auditlog?start_time={start_time}&end_time={end_time}&offset={offset}&limit={limit}	rds:auditlog:list	-
POST /v3/{project_id}/instances/{instance_id}/auditlog-links	rds:auditlog:download	-
GET /v3/{*project_id*}/datastores/{*database_name*}	rds:instance:listDatabaseVersion	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/flavors/{database_name}?version_name={version_name}&spec_code={spec_code}	rds:instance:listFlavors	-
GET /v3/{project_id}/storage-type/{database_name}?version_name={version_name}&ha_mode={ha_mode}	rds:instance:listStorageType	-
POST /v3/{*project_id*}/instances/{*instance_id*}/password	rds:password:update	-
PUT /v3/{*project_id*}/configurations/{config_id}	rds:param:updateTemplate	-
PUT /v3.1/{project_id}/instances/{instance_id}/configurations	rds:instance:updateParameter	-
DELETE /v3/{project_id}/configurations/{config_id}	rds:param:delete	-
POST /v3/{project_id}/configurations	rds:param:createTemplate	-
POST /v3/{project_id}/configurations/{config_id}/copy	rds:param:copy	-
PUT /v3.1/{*project_id*}/configurations/{config_id}/apply	rds:param:apply	-
POST /v3.1/{project_id}/instances/{instance_id}/restore/tables	rds:instance:tableRestore	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/failover	rds:instance:switchover	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:singleToHa	-
PUT /v3/{project_id}/instances/recycle-policy	rds:instance:setRecycleBin	-
POST /v3/{project_id}/instances	rds:instance:restoreInPlace	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:restart	-
POST /v3/{project_id}/instances/{instance_id}/action/shutdown	rds:instance:stop	-
POST /v3/{project_id}/instances/{instance_id}/action/startup	rds:instance:start	-

API	对应的授权项	依赖的授权项
POST /v3/{*project_id*}/instances/{*instance_id*}/action	rds:instance:modifySpec	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/security-group	rds:instance:modifySecurityGroup	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/public-ip	rds:instance:modifyPublicAccess	-
POST /v3/{*project_id*}/instances/{*instance_id*}/proxy	rds:instance:modifyProxy	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/port	rds:instance:modifyPort	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/ip	rds:instance:modifyIp	-
PUT /v3/{project_id}/instances/{instance_id}/modify-dns	rds:instance:updateDnsName	-
POST /v3/{project_id}/instances/{instance_id}/msdtc/host	rds:instance:SetMsdtcHosts	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/ops-window	rds:instance:updateOpsWindow	-
PUT /v3/{project_id}/instances/{instance_id}/name	rds:instance:updateName	-
PUT /v3/{project_id}/instances/{instance_id}/alias	rds:instance:updateRemark	-
POST /v3/{project_id}/instances/{instance_id}/db-upgrade	rds:instance:upgradeDatabaseVersion	-
DELETE /v3/{project_id}/instances/{instance_id}	rds:instance:deleteInstance	-
POST /v3/{project_id}/instances/{instance_id}/create-dns	rds:instance:createDns	-
POST /v3/{project_id}/instances	rds:instance:create	-
PUT /v3/{project_id}/instances/{instance_id}/db-users/{user_name}/comment	rds:databaseUser:update	-
DELETE /v3/{project_id}/instances/{instance_id}/db_user/{user_name}	rds:databaseUser:drop	-
POST /v3/{project_id}/instances/{instance_id}/db_user	rds:databaseUser:create	-
DELETE /v3/{project_id}/instances/{instance_id}/db_privilege	rds:databasePrivilege:revoke	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/instances/{instance_id}/db_privilege	rds:databasePrivilege:grant	-
DELETE /v3/{project_id}/instances/{instance_id}/database/{db_name}	rds:database:drop	-
POST /v3/{project_id}/instances/{instance_id}/database	rds:database:createDatabase	-
DELETE /v3/{project_id}/backups/{backup_id}	rds:backup:delete	-
POST /v3/{project_id}/backups	rds:backup:create	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:buildDrRelation	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:modifyDRRole	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表3中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

RDS定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-62 RDS 支持的资源类型

资源类型	URN
instance	rds:<region>:<account-id>:instance:<instance-id>

条件（Condition）

条件（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如rds:）仅适用于对应服务的操作，详情请参见**表5-63**。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请

求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。

- 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，SCP才能生效。支持的运算符请参见：运算符。

RDS定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-63 RDS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
rds:Encrypted	Boolean	单值	按照请求参数中传递的是否开启磁盘加密标签键筛选访问权限。
rds:BackupEnabled	Boolean	单值	按照请求参数中传递的是否开启备份策略标签键筛选访问权限。

5.10.6.2 文档数据库服务 DDS

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于DDS定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

关于DDS定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下DDS的相关操作。

表 5-64 DDS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
dds:instance:setSsl	授予切换SSL开关的权限。	permission_management	instance	-
dds:instance:unbindEIP	授予解绑弹性公网IP的权限。	write	-	-
dds:instance:migrateAz	授予实例迁移可用区的权限。	write	-	-
dds:instance:listMigrateAz	授予查询实例可迁移的可用区列表的权限。	list	-	-
dds:instance:updateIp	授予修改内网IP地址的权限。	write	instance	-
dds:instance:bindEIP	授予绑定弹性公网IP的权限。	write	-	-
dds:instance:resetPassword	授予重置数据库用户密码的权限。	write	instance	-
dds:instance:checkPassword	授予检查数据库密码的权限。	read	instance	-
dds:instance:updatePort	授予修改数据库端口的权限。	write	instance	-
dds:backup:download	授予下载备份文件的权限。	read	instance	-
dds:instance:setAuditLogPolicy	授予设置审计日志策略的权限。	permission_management	instance	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dds:instance:getAuditLogPolicy	授予查看审计日志策略的权限。	list	instance	-
dds:instance:listAuditLog	授予查看审计日志的权限。	list	instance	-
dds:instance:listSlowLog	授予查看慢日志的权限。	list	instance	-
dds:instance:downloadSlowLog	授予下载慢日志的权限。	read	instance	-
dds:instance:listErrorLog	授予查看错误日志的权限。	list	instance	-
dds:instance:downloadErrorLog	授予下载错误日志的权限。	read	instance	-
dds:configuration:delete	授予删除参数组的权限。	write	-	g:EnterpriseProjectId
dds:configuration:update	授予修改参数组中参数值的权限。	write	-	g:EnterpriseProjectId
dds:backup:listAll	授予查询备份列表的权限。	list	-	-
dds:instance:updateConfiguration	授予修改实例或实例节点的参数组配置的权限。	write	instance	-
dds:instance:applyConfiguration	授予应用参数配置到实例或实例节点的权限。	write	-	-
dds:instance:createIp	授予创建IP的权限。	write	-	-
dds:backup:delete	授予删除备份的权限。	write	-	-
dds:instance:updateSecurityGroup	授予变更实例安全组的权限。	write	instance	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dds:configuration:listAll	授予查询参数组列表的权限。	list	-	g:EnterpriseProjectId
dds:instance:getConfiguration	授予查询实例参数配置的权限。	read	instance	-
dds:configuration:get	授予查询参数配置详情的权限。	read	-	g:EnterpriseProjectId
dds:instance:updateSpec	授予变更实例规格的权限。	write	instance	-
dds:instance:getSecondLevelMonitoringConfig	授予查询秒级监控配置的权限。	read	instance	-
dds:instance:setSecondLevelMonitoringConfig	授予开启秒级监控的权限。	write	instance	-
dds:instance:switchover	授予切换主备节点的权限。	write	instance	-
dds:instance:extendVolume	授予扩容实例存储容量的权限。	write	instance	-
dds:instance:listAll	授予查询数据库实例列表的权限。	list	-	-
dds:instance:setRecyclePolicy	授予设置实例回收备份策略的权限。	write	-	-
dds:instance:getRecyclePolicy	授予查看实例回收备份策略的权限。	read	-	-
dds:instance:listRecycleInstances	授予查询回收站实例列表的权限。	list	-	-
dds:instance:getUpgradeDuration	授予查询数据库补丁升级预估时长的权限。	read	instance	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dds:instance:getDiskUsage	授予查询磁盘使用率的权限。	read	instance	-
dds:configuration:listAppliedHistory	授予查询参数模板被应用历史的权限。	list	-	-
dds:configuration:listUpdatedHistory	授予查询参数模板修改历史的权限。	list	-	-
dds:configuration:compare	授予比较两个参数模板之间差异的权限。	read	-	-
dds:configuration:copy	授予复制参数模板的权限。	write	-	-
dds:configuration:reset	授予重置参数模板的权限。	write	-	-
dds:instance:getSslCertDownloadAddress	授予获取下载ssl证书地址的权限。	read	instance	-
dds:instance:addNode	授予扩容实例节点数量的权限。	write	instance	-
dds:instance:deleteEnlargeFailedNode	授予删除扩容失败的实例节点的权限。	write	instance	-
dds:task:listAll	授予查询任务列表的权限。	list	-	-
dds:task:getDetail	授予查询任务详情的权限。	read	-	-
dds:instance:restart	授予重启数据库实例的权限。	write	instance	-
dds:instance:deleteAuditLog	授予删除审计日志的权限。	write	instance	-
dds:instance:delete	授予删除数据库实例的权限。	write	instance	-
dds:instance:updateName	授予修改实例名称的权限。	write	instance	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dds:instance:updateRemark	授予修改实例备注的权限。	write	instance	-
dds:instance:setTag	授予批量添加或删除指定实例标签的权限。	tagging	instance	-
dds:instance:listTags	授予查询指定实例的标签信息的权限。	read	-	-
dds:instance:setBackupPolicy	授予设置自动备份策略的权限。	write	-	dds:BackupEnabled
dds:instance:getBackupPolicy	授予查询自动备份策略的权限。	read	-	-
dds:configuration:create	授予创建参数组的权限。	write	-	g:EnterpriseProjectId
dds:instance:setSlowLogPlaintextStatus	授予切换慢日志明文显示开关的权限。	permission_management	instance	-
dds:instance:getSlowLogPlaintextStatus	授予查看慢日志明文开关状态的权限。	read	instance	-
dds:instance:downloadAuditLog	授予下载审计日志的权限。	read	instance	-
dds:instance:create	授予创建数据库实例的权限。	write	-	dds:Encrypted dds:BackupEnabled
dds:instance:restore	授予备份恢复原实例的权限。	write	-	-
dds:backup:getRestoreTimeList	授予查询实例可恢复时间段的权限。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dds:backup:getRestoreCollections	授予获取可恢复的数据库集合列表的权限。	list	-	-
dds:backup:getRestoreDatabases	授予获取可恢复的数据库列表的权限。	list	-	-
dds:instance:getConnectionStatistics	授予查询实例连接数统计信息的权限。	read	instance	-
dds:instance:getQuotas	授予查询配额的权限。	read	-	-
dds:instance:createDatabaseUser	授予创建数据库用户的权限。	write	instance	-
dds:instance:getDatabaseUser	授予查询数据库用户列表的权限。	read	instance	-
dds:instance:deleteDatabaseUser	授予删除数据库用户的权限。	write	instance	-
dds:instance:createDatabaseRole	授予创建数据库角色的权限。	write	instance	-
dds:instance:deleteDatabaseRole	授予删除数据库角色的权限。	write	instance	-
dds:instance:getDatabaseRole	授予查询数据库角色列表的权限。	read	instance	-
dds:instance:setSourceSubnet	授予网段配置的权限。	write	instance	-
dds:instance:upgradeDatabaseVersion	授予升级数据库版本的权限。	write	instance	-
dds:backup:create	授予创建数据库实例手动备份的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dds:instance:deleteSession	授予删除节点会话的权限。	write	-	-
dds:instance:listSession	授予查询节点会话列表的权限。	list	-	-
dds:instance:getShardingBalancer	授予查询集群实例负载均衡的权限。	read	instance	-
dds:instance:setShardingBalancer	授予设置集群实例负载均衡的权限。	write	instance	-
dds:instance:setBalancerWindow	授予设置集群均衡活动时间窗的权限。	write	instance	-
dds:instance:updateOpsWindow	授予设置实例可维护时间窗的权限。	write	instance	-
dds:instance:listFlavors	授予查询规格列表的权限。	read	-	-
dds:instance:listStorageType	授予查询数据库磁盘类型的权限。	read	-	-
dds:instance:listDatabaseVersion	授予查询数据库版本信息的权限。	read	-	-
dds:tag:listAll	授予查询项目下所有标签信息的权限。	list	-	-
dds:instance:reduceNode	授予缩容集群实例的节点数量的权限。	write	instance	-
dds:instance:createDomainName	授予创建DNS的权限。	write	-	-
dds:instance:updateDomainName	授予修改DNS名称的权限。	write	-	-
dds:instance:updateReplicaSetName	授予修改数据库复制集名称的权限。	write	instance	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dds:instance:getDetail	授予查询实例详情的权限。	read	instance	-
dds:instance:getNodeList	授予查询实例节点列表的权限。	read	instance	-
dds:instance:updateTag	授予修改实例标签的权限。	tagging	instance	-
dds:instance:deleteTag	授予删除实例标签的权限。	tagging	instance	-
dds:backup:get	授予查询备份信息的权限。	read	-	-
dds:offsiteBackup:listRegion	授予获取指定实例异地备份区域的权限。	read	-	-
dds:offsiteBackup:listInstance	授予获取异地备份实例的权限。	read	-	-
dds:offsiteBackup:listAll	授予获取异地备份列表的权限。	read	-	-
dds:instance:saveLogConfig	授予批量保存日志配置的权限。	write	-	-
dds:instance:deleteLogConfig	授予批量删除日志配置的权限。	write	-	-

DDS的API通常对应着一个或多个授权项。表5-65展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-65 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/instances	dds:instance:create vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get vpc:ports:get	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/instances?id={id}&name={name}&mode={mode}&datastore_type={datastore_type}&vpc_id={vpc_id}&subnet_id={subnet_id}&offset={offset}&limit={limit}	dds:instance:listAll	-
DELETE /v3/{project_id}/instances/{instance_id}	dds:instance:delete	-
POST /v3/{project_id}/instances/{instance_id}/restart	dds:instance:restart	-
POST /v3/{project_id}/instances/{instance_id}/enlarge-volume	dds:instance:extendVolume	-
POST /v3/{project_id}/instances/{instance_id}/enlarge	dds:instance:addNode vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get vpc:ports:get	-
POST /v3/{project_id}/instances/{instance_id}/resize	dds:instance:updateSpec	-
POST /v3/{project_id}/instances/{instance_id}/switchover	dds:instance:switchover	-
POST/v3/{project_id}/instances/{instance_id}/switch-ssl	dds:instance:setSSL	-
PUT /v3/{project_id}/instances/{instance_id}/modify-name	dds:instance:updateName	-
POST /v3/{project_id}/instances/{instance_id}/modify-port	dds:instance:updatePort	-
POST /v3/{project_id}/instances/{instance_id}/modify-security-group	dds:instance:updateSecurityGroup	-
POST /v3/{project_id}/nodes/{node_id}/bind-eip	dds:instance:bindEIP	-
POST /v3/{project_id}/nodes/{node_id}/unbind-eip	dds:instance:unbindEIP	-
POST /v3/{project_id}/instances/{instance_id}/modify-internal-ip	dds:instance:updateIp	-
POST /v3/{project_id}/instances/{instance_id}/create-ip	dds:instance:createIp	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/instances/{instance_id}/migrate/az	dds:instance:listMigrateAz	-
POST /v3/{project_id}/instances/{instance_id}/migrate	dds:instance:migrateAz	-
GET /v3/{project_id}/nodes/{node_id}/sessions	dds:instance:lisSession	-
POST /v3/{project_id}/nodes/{node_id}/session	dds:instance:deleteSession	-
GET /v3/{projectId}/instances/{instance_id}/conn-statistics	dds:instance:getConnectionStatistics	-
POST /v3/{project_id}/backups	dds:backup:create	-
DELETE /v3/{project_id}/backups/{backups_id}	dds:backup:delete	-
GET /v3/{project_id}/backups?instance_id={instance_id}&backup_id={backup_id}&backup_type={backup_type}&offset={offset}&limit={limit}&begin_time={begin_time}&end_time={end_time}&mode={mode}	dds:backup:listAll	-
GET /v3/{project_id}/instances/{instance_id}/backups/policy	dds:instance:getBackupPolicy	-
PUT /v3/{project_id}/instances/{instance_id}/backups/policy	dds:instance:setBackupPolicy	-
POST /v3/{project_id}/instances	dds:instance:create vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get vpc:ports:get	-
GET /v3/{projectId}/backups/download-file	dds:backup:download	-
GET /v3/{project_id}/instances/{instance_id}/restore-time	dds:backup:getRestoreTimeList	-
GET /v3/{project_id}/instances/{instance_id}/restore-database	dds:backup:getRestoreDatabases	-
GET /v3/{project_id}/instances/{instance_id}/restore-collection	dds:backup:getRestoreCollections	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/instances/recovery	dds:backup:restore	-
POST /v3/{project_id}/instances/{instance_id}/restore/collections	dds:backup:restore	-
GET /v3/{project_id}/configurations	dds:configuration:listAll	-
PUT /v3/{project_id}/configurations	dds:configuration:create	-
DELETE /v3/{project_id}/configurations/{config_id}	dds:configuration:delete	-
GET /v3/{projectId}/configurations/{configId}	dds:configuration:get	-
PUT /v3/{project_id}/configurations/{config_id}	dds:configuration:update	-
PUT /v3/{project_id}/configurations/{config_id}/apply	dds:instance:applyConfiguration	-
GET /v3/{project_id}/instances/{instance_id}/configurations	dds:instance:getConfiguration	-
PUT /v3/{project_id}/instances/{instance_id}/configurations	dds:instance:updateConfiguration	-
GET /v3/{project_id}/instances/{instance_id}/slowlog	dds:instance:listSlowLog	-
POST /v3/{project_id}/instances/{instance_id}/slowlog-download	dds:instance:downloadSlowLog	-
GET /v3/{project_id}/instances/{instance_id}/errorlog	dds:instance:listErrorLog	-
POST /v3/{project_id}/instances/{instance_id}/errorlog-download	dds:instance:downloadErrorLog	-
POST /v3/{project_id}/instances/{instance_id}/auditlog-policy	dds:instance:setAuditLogPolicy	-
GET /v3/{project_id}/instances/{instance_id}/auditlog-policy	dds:instance:getAuditLogPolicy	-
GET /v3/{project_id}/instances/{instance_id}/auditlog	dds:instance:listAuditLog	-
POST /v3/{project_id}/instances/{instance_id}/auditlog-links	dds:instance:downloadAuditLog	-
POST /v3/{project_id}/instances/{instance_id}/tags/action	dds:instance:setTag	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/instances/{instance_id}/tags	dds:instance:listTags	-
POST /v3/{project_id}/instances/{instance_id}/db-user	dds:instance:createDatabaseUser	-
POST /v3/{project_id}/instances/{instance_id}/db-role	dds:instance:createDatabaseRole	-
DELETE /v3/{project_id}/instances/{instance_id}/db-user	dds:instance:deleteDatabaseUser	-
DELETE /v3/{project_id}/instances/{instance_id}/db-role	dds:instance:deleteDatabaseRole	-
PUT /v3/{project_id}/instances/{instance_id}/reset-password	dds:instance:resetPasswd	-
GET /v3/{project_id}/instances/{instance_id}/db-user/detail? offset={offset}&limit={limit}&user_name={user_name }&db_name={db_name}	dds:instance:getDatabaseUser	-
GET /v3/{project_id}/instances/{instance_id}/db-roles? role_name={role_name}&db_name={db_name}&offset={offset}&limit={limit}	dds:instance:getDatabaseRole	-
GET /v3/{project_id}/instances/{instance_id}/balancer	dds:instance:getShardingBalancer	-
PUT /v3/{project_id}/instances/{instance_id}/balancer/{action}	dds:instance:setShardingBalancer	-
PUT /v3/{project_id}/instances/{instance_id}/balancer/active-window	dds:instance:setBalancerWindow	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-66**中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

DDS定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-66 DDS 支持的资源类型

资源类型	URN	条件键
instanceName	dds:<region>:<account-id>:instanceName:<instance-name>	- g:EnterpriseProjectId - g:ResourceTag/<tag-key>

条件（Condition）

条件（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，组织将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀为服务缩写，如DDS:）仅适用于对应服务的操作，详情请参见**表5-67**。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
- 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，SCP才能生效。支持的运算符请参见：运算符。

DDS定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-67 DDS 支持的服务级条件键

服务级条件键	类型	说明
dds:Encrypted	boolean	按照请求参数中传递的是否开启磁盘加密标签键筛选访问权限。
dds:BackupEnabled	boolean	按照请求参数中传递的是否开启备份策略标签键筛选访问权限。

5.10.7 安全与合规

5.10.7.1 DDoS 防护 AAD

5.10.7.1.1 原生基础防护 Anti-DDoS

Organizations服务中的服务控制策略（Service Control Policies，以下简称SCP）可以使用这些授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP策略语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于Anti-DDoS定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP策略语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于Anti-DDoS定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP策略语句的Action元素中指定以下Anti-DDoS的相关操作。

表 5-68 Anti-DDoS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
anti-ddos:task:list	授予查询Anti-DDoS任务权限。	list	-	-
anti-ddos:quota:list	授予查询配额权限。	list	-	-
anti-ddos:optionalDefensePolicy:list	授予查询Anti-DDoS配置可选范围权限。	list	-	-
anti-ddos:logConfig:update	授予更新云日志服务配置权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
anti-ddos:logConfig:get	授予查询云日志服务配置权限。	read	-	-
anti-ddos:ip:updateDefensePolicy	授予更新Anti-DDoS服务权限。	write	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:ip:untagResource	授予批量删除标签权限。	write	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:ip:tagResource	授予批量添加标签权限。	write	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:ip:listTagsForResource	授予查询资源标签列表权限。	list	ip *	-
anti-ddos:ip:listDefenseStatuses	授予查询EIP防护状态列表权限。	list	ip *	-
anti-ddos:ip:getWeeklyReport	授予查询周防护统计情况权限。	read	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:ip:getDefenseStatus	授予查询指定EIP防护状态权限。	read	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:ip:getDefensePolicy	授予查询Anti-DDoS服务权限。	read	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:ip:getDailyTrafficReport	授予查询指定EIP防护流量权限。	read	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
anti-ddos:ip:getDailyEventReport	授予查询指定EIP异常事件权限。	read	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:ip:enableDefensePolicy	授予开通Anti-DDoS服务权限。	write	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:ip:disableDefensePolicy	授予关闭Anti-DDoS服务权限。	write	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:defaultDefensePolicy:get	授予查询Anti-DDoS默认防护策略权限。	read	-	-
anti-ddos:defaultDefensePolicy:delete	授予删除Anti-DDoS默认防护策略权限。	write	-	-
anti-ddos:defaultDefensePolicy:create	授予配置Anti-DDoS默认防护策略权限。	write	-	-
anti-ddos:alertConfig:update	授予更新告警配置信息权限。	write	-	-
anti-ddos:alertConfig:get	授予查询告警配置信息权限。	read	-	-

Anti-DDoS的API通常对应着一个或多个授权项。表5-69展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-69 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/query-task-status	anti-ddos:task:list	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/antiddos/quotas	anti-ddos:quota:list	-
GET /v1/{project_id}/antiddos/query-config-list	anti-ddos:optionalDefensePolicy:list	-
PUT /v1/{project_id}/antiddos/lts-config	anti-ddos:logConfig:update	-
GET /v1/{project_id}/antiddos/lts-config	anti-ddos:logConfig:get	-
PUT /v1/{project_id}/antiddos/{floating_ip_id}	anti-ddos:ip:updateDefensePolicy	-
DELETE /v1/{project_id}/antiddos-ip/{resource_id}/tags/delete	anti-ddos:ip:untagResource	-
POST /v1/{project_id}/antiddos-ip/{resource_id}/tags/create	anti-ddos:ip:tagResource	-
GET /v1/{project_id}/antiddos-ip/{resource_id}/tags	anti-ddos:ip:listTagsForResource	-
GET /v1/{project_id}/antiddos-ip/tags	anti-ddos:ip:listTagsForResource	-
GET /v1/{project_id}/antiddos	anti-ddos:ip:listDefenseStatuses	-
POST /v1/{project_id}/antiddos-ip/resource-instances/count	anti-ddos:ip:listDefenseStatuses	-

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/antiddos-ip/resource-instances/filter	anti-ddos:ip:listDefenseStatuses	-
GET /v1/{project_id}/antiddos/weekly	anti-ddos:ip:getWeeklyReport	-
GET /v1/{project_id}/antiddos/weekly-export	anti-ddos:ip:getWeeklyReport	-
GET /v1/{project_id}/antiddos/{floating_ip_id}/status	anti-ddos:ip:getDefenseStatus	-
GET /v1/{project_id}/antiddos/{floating_ip_id}	anti-ddos:ip:getDefensePolicy	-
GET /v1/{project_id}/antiddos/queryIsEnabledResult/query	anti-ddos:ip:getDefensePolicy	-
GET /v1/{project_id}/antiddos/{floating_ip_id}/daily	anti-ddos:ip:getDailyTrafficReport	-
GET /v1/{project_id}/antiddos/{floating_ip_id}/daily-export	anti-ddos:ip:getDailyTrafficReport	-
GET /v1/{project_id}/antiddos/{floating_ip_id}/logs	anti-ddos:ip:getDailyEventReport	-
POST /v1/{project_id}/antiddos/{floating_ip_id}	anti-ddos:ip:enableDefensePolicy	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/antiddos/immediate_protection	anti-ddos:ip:enableDefensePolicy	-
DELETE /v1/{project_id}/antiddos/{floating_ip_id}	anti-ddos:ip:disableDefensePolicy	-
GET /v1/{project_id}/antiddos/{floating_ip_id}/closeAndReason	anti-ddos:ip:disableDefensePolicy	-
GET /v1/{project_id}/antiddos/default/config	anti-ddos:defaultDefensePolicy:get	-
DELETE /v1/{project_id}/antiddos/default/config	anti-ddos:defaultDefensePolicy:delete	-
POST /v1/{project_id}/antiddos/default/config	anti-ddos:defaultDefensePolicy:create	-
POST /v2/{project_id}/warnalert/alertconfig/update	anti-ddos:alertConfig:update	-
GET /v2/{project_id}/warnalert/alertconfig/query	anti-ddos:alertConfig:get	-

资源类型（Resource）

资源类型（Resource）表示SCP策略所作用的资源。如**表5-70**中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP策略语句中指定该资源的URN，SCP策略仅作用于此资源；如未指定，Resource默认为“*”，则SCP策略将应用到所有资源。您也可以在SCP策略中设置条件，从而指定资源类型。

Anti-DDoS定义了以下可以在自定义SCP策略的Resource元素中使用的资源类型。

表 5-70 Anti-DDoS 支持的资源类型

资源类型	URN
ip	anti-ddos:<region>:<account-id>:ip:<ip-id>

条件（Condition）

Anti-DDoS服务不支持在SCP策略中的条件键中配置服务级的条件键。

Anti-DDoS可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.7.1.2 DDoS 高防 AAD

Organizations服务中的服务控制策略（Service Control Policies，以下简称SCP）可以使用这些授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP《组织服务用户指南》的“创建SCP”章节。

操作（Action）

操作（Action）即为SCP策略中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP策略中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP策略语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于AAD定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP策略语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于AAD定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP策略语句的Action元素中指定以下AAD的相关操作。

表 5-71 AAD 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
aad:alarmConfig:create	授予创建告警设置的权限。	write	alarmConfig *	-
aad:alarmConfig:put	授予修改告警设置的权限。	write	alarmConfig *	-
aad:alarmConfig:get	授予查询告警设置的权限。	read	alarmConfig *	-
aad:alarmConfig:delete	授予删除告警设置的权限。	write	alarmConfig *	-
aad:certificate:delete	授予删除证书的权限。	write	certificate *	-
aad:certificate:list	授予查询证书列表的权限。	list	certificate *	-
aad:certificate:set	授予修改域名对应证书的权限。	write	certificate *	-
			domain *	g:EnterpriseProjectId
aad:dashboard:delete	授予删除报表日志配置的权限。	write	-	-
aad:dashboard:get	授予获取报表数据和日志配置的权限。	read	-	-
aad:dashboard:set	授予修改报表日志配置的权限。	write	-	-
aad:domain:create	授予添加防护域名的权限。	write	domain *	g:EnterpriseProjectId
aad:domain:delete	授予删除防护域名的权限。	write	domain *	g:EnterpriseProjectId
aad:domain:get	授予查询防护域名详情的权限。	read	domain *	g:EnterpriseProjectId
aad:domain:list	授予查询域名列表的权限。	list	domain *	g:EnterpriseProjectId
aad:domain:put	授予修改域名防护属性的权限。	write	domain *	g:EnterpriseProjectId
aad:forwardingRule:create	授予添加转发规则的权限。	write	forwardingRule *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
aad:forwardingRule:delete	授予删除转发规则的权限。	write	forwardingRule *	g:EnterpriseProjectId
aad:forwardingRule:get	授予查询转发规则的权限。	read	forwardingRule *	g:EnterpriseProjectId
aad:forwardingRule:list	授予导出转发规则的权限。	list	forwardingRule *	g:EnterpriseProjectId
aad:forwardingRule:put	授予修改转发规则中的回源IP的权限。	write	forwardingRule *	g:EnterpriseProjectId
aad:instance:create	授予创建实例的权限。	write	instance *	g:EnterpriseProjectId
aad:instance:get	授予查询实例属性的权限。	read	instance *	g:EnterpriseProjectId
aad:instance:list	授予查询实例列表的权限。	list	instance *	g:EnterpriseProjectId
aad:instance:put	授予修改实例属性的权限。	write	instance *	g:EnterpriseProjectId
aad:policy:create	授予添加防护规则的权限。	write	policy *	g:EnterpriseProjectId
aad:policy:delete	授予删除防护规则的权限。	write	policy *	g:EnterpriseProjectId
aad:policy:get	授予查询防护规则详情的权限。	read	policy *	g:EnterpriseProjectId
aad:policy:list	授予查询防护规则列表的权限。	list	policy *	g:EnterpriseProjectId
aad:policy:put	授予修改防护规则的权限。	write	policy *	g:EnterpriseProjectId
aad:quotas:get	授予查询防护规格的权限。	read	-	-
aad:whiteBlackIpRule:create	授予添加防护黑白名单的权限。	write	whiteBlackIpRule *	g:EnterpriseProjectId
aad:whiteBlackIpRule:delete	授予删除防护黑白名单的权限。	write	whiteBlackIpRule *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
aad:whiteBlackIpRule:list	授予查询防护黑白名单列表的权限。	list	whiteBlackIpRule *	g:EnterpriseProjectId
aad:protectedIp:put	授予修改防护对象标签的权限。	write	-	-
aad:protectedIp:list	授予查询防护对象列表的权限。	list	-	-
aad:package:put	授予修改防护包的权限。	write	package *	-
aad:package:list	授予查询防护包列表的权限。	list	package *	-
aad:block:put	授予解封IP的权限。	write	-	-
aad:block:list	授予查询封堵ip列表的权限。	list	-	-
aad:block:get	授予查询封堵和解封信息的权限。	read	-	-
aad:alarmConfig:create	授予创建告警设置的权限。	write	alarmConfig *	-
aad:alarmConfig:put	授予修改告警设置的权限。	write	alarmConfig *	-
aad:alarmConfig:get	授予查询告警设置的权限。	read	alarmConfig *	-
aad:alarmConfig:delete	授予删除告警设置的权限。	write	alarmConfig *	-
aad:certificate:delete	授予删除证书的权限。	write	certificate *	-
aad:certificate:list	授予查询证书列表的权限。	list	certificate *	-
aad:certificate:set	授予修改域名对应证书的权限。	write	certificate *	-
			domain *	g:EnterpriseProjectId
aad:dashboard:delete	授予删除报表日志配置的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
aad:dashboard:get	授予获取报表数据和日志配置的权限。	read	-	-
aad:dashboard:set	授予修改报表日志配置的权限。	write	-	-
aad:domain:create	授予添加防护域名的权限。	write	domain *	g:EnterpriseProjectId
aad:domain:delete	授予删除防护域名的权限。	write	domain *	g:EnterpriseProjectId
aad:domain:get	授予查询防护域名详情的权限。	read	domain *	g:EnterpriseProjectId
aad:domain:list	授予查询域名列表的权限。	list	domain *	g:EnterpriseProjectId
aad:domain:put	授予修改域名防护属性的权限。	write	domain *	g:EnterpriseProjectId
aad:forwardingRule:create	授予添加转发规则的权限。	write	forwardingRule *	g:EnterpriseProjectId
aad:forwardingRule:delete	授予删除转发规则的权限。	write	forwardingRule *	g:EnterpriseProjectId
aad:forwardingRule:get	授予查询转发规则的权限。	read	forwardingRule *	g:EnterpriseProjectId
aad:forwardingRule:list	授予导出转发规则的权限。	list	forwardingRule *	g:EnterpriseProjectId
aad:forwardingRule:put	授予修改转发规则中的回源IP的权限。	write	forwardingRule *	g:EnterpriseProjectId
aad:instance:create	授予创建实例的权限。	write	instance *	g:EnterpriseProjectId
aad:instance:get	授予查询实例属性的权限。	read	instance *	g:EnterpriseProjectId
aad:instance:list	授予查询实例列表的权限。	list	instance *	g:EnterpriseProjectId
aad:instance:put	授予修改实例属性的权限。	write	instance *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
aad:policy:create	授予添加防护规则的权限。	write	policy *	g:EnterpriseProjectId
aad:policy:delete	授予删除防护规则的权限。	write	policy *	g:EnterpriseProjectId
aad:policy:get	授予查询防护规则详情的权限。	read	policy *	g:EnterpriseProjectId
aad:policy:list	授予查询防护规则列表的权限。	list	policy *	g:EnterpriseProjectId
aad:policy:put	授予修改防护规则的权限。	write	policy *	g:EnterpriseProjectId
aad:quotas:get	授予查询防护规格的权限。	read	-	-
aad:whiteBlackIpRule:create	授予添加防护黑白名单的权限。	write	whiteBlackIpRule *	g:EnterpriseProjectId
aad:whiteBlackIpRule:delete	授予删除防护黑白名单的权限。	write	whiteBlackIpRule *	g:EnterpriseProjectId
aad:whiteBlackIpRule:list	授予查询防护黑白名单列表的权限。	list	whiteBlackIpRule *	g:EnterpriseProjectId
aad:protectedIp:put	授予修改防护对象标签的权限。	write	-	-
aad:protectedIp:list	授予查询防护对象列表的权限。	list	-	-
aad:package:put	授予修改防护包的权限。	write	package *	-
aad:package:list	授予查询防护包列表的权限。	list	package *	-
aad:block:put	授予解封IP的权限。	write	-	-
aad:block:list	授予查询封堵ip列表的权限。	list	-	-
aad:block:get	授予查询封堵和解封信息的权限。	read	-	-

AAD的API通常对应着一个或多个授权项。表5-72展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-72 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/cad/alart/config	aad:alarmConfig:create	-
POST /v1/cnad/alarm-config	aad:alarmConfig:put	-
DELETE /v1/cnad/alarm-config	aad:alarmConfig:delete	-
GET /v1/{project_id}/cad/alart/list	aad:alarmConfig:get	-
GET /v1/cnad/alarm-config	aad:alarmConfig:get	-
DELETE /v1/aad/certificate/del	aad:certificate:delete	-
GET /v1/{project_id}/cad/domains/certificatelist	aad:certificate:list	-
GET /v1/aad/certificate-details	aad:certificate:list	-
POST /v1/{project_id}/cad/domains/certificate	aad:certificate:set	-
POST /v1/aad/configs/lts/delete	aad:dashboard:delete	-
GET /v1/{project_id}/cad/ddosinfo/events_type	aad:dashboard:get	-
GET /v1/aad/configs/lts_region	aad:dashboard:get	-
GET /v1/aad/configs/lts	aad:dashboard:get	-
GET /v1/{project_id}/waf/event/timeline	aad:dashboard:get	-
GET /v1/{project_id}/waf/event/request/peak	aad:dashboard:get	-
GET /v1/{project_id}/waf/event/attack/type	aad:dashboard:get	-
GET /v1/{project_id}/waf/event/attack/source/num	aad:dashboard:get	-
GET /v1/{project_id}/waf/event/attack/source	aad:dashboard:get	-
GET /v1/{project_id}/cad/instances/flow_pps	aad:dashboard:get	-
GET /v1/{project_id}/cad/instances/flow_bps	aad:dashboard:get	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/cad/instances/events	aad:dashboard:get	-
GET /v1/{project_id}/cad/ddosinfo/peak	aad:dashboard:get	-
POST /v1/aad/configs/lts	aad:dashboard:set	-
POST /v1/{project_id}/aad/domains	aad:domain:create	-
POST /v1/{project_id}/cad/domains/del	aad:domain:delete	-
GET /v1/{project_id}/aad/domains/{domain_id}/service-config	aad:domain:get	-
GET /v1/{project_id}/cad/domains/ports	aad:domain:list	-
GET /v1/{project_id}/cad/domains/name	aad:domain:get	-
GET /v1/{project_id}/cad/domains/line/{enterprise_project_id}	aad:domain:list	-
GET /v1/{project_id}/cad/domains/instances	aad:domain:get	-
GET /v1/{project_id}/cad/domains/brief	aad:domain:get	-
GET /v1/{project_id}/aad/domains/waf-list	aad:domain:list	-
GET /v1/{project_id}/cad/domains	aad:domain:list	-
POST /v1/{project_id}/aad/domains/{domain_id}/service-config	aad:domain:put	-
POST /v1/{project_id}/cad/domains/switch	aad:domain:put	-
POST /v1/{project_id}/cad/domains/cnameDispatchSwitch	aad:domain:put	-
POST /v1/{project_id}/cad/domains/cname/switch	aad:domain:put	-
POST /v1/{project_id}/cad/instances/protocol_rule	aad:forwardingRule:create	-
POST /v1/{project_id}/cad/instances/protocol_rule/import	aad:forwardingRule:create	-

API	对应的授权项	依赖的授权项
DELETE /v1/{project_id}/cad/instances/protocol_rule/{rule_id}	aad:forwardingRule:delete	-
POST /v1/{project_id}/cad/instances/protocol_rule/batchdel	aad:forwardingRule:delete	-
GET /v1/{project_id}/cad/instances/rules	aad:forwardingRule:get	-
GET /v1/{project_id}/cad/instances/protocol_rule/export	aad:forwardingRule:list	-
PUT /v1/{project_id}/cad/instances/protocol_rule/{rule_id}	aad:forwardingRule:put	-
POST /v1/{project_id}/cad/instances/cad_open	aad:instance:create	-
GET /v1/{project_id}/cad/products	aad:instance:create	-
GET /v1/{project_id}/{resource_type}/{resource_id}/tags	aad:instance:get	-
GET /v1/{project_id}/cad/upgradeproducts/{instance_id}	aad:instance:get	-
GET /v1/{project_id}/cad/instances/detail/{instance_id}	aad:instance:get	-
GET /v1/{project_id}/aad/instances/brief-list	aad:instance:list	-
GET /v1/{project_id}/cad/sourceip	aad:instance:list	-
GET /v1/{project_id}/cad/instances	aad:instance:list	-
POST /v1/{project_id}/{resource_type}/{resource_id}/tags/action	aad:instance:put	-
POST /v1/{project_id}/cad/instances/cad_spec_upgrade	aad:instance:put	-
PUT /v1/{project_id}/cad/instances/{instance_id}/name	aad:instance:put	-
PUT /v1/{project_id}/cad/instances/{instance_id}/elastic/{ip_id}	aad:instance:put	-
POST /v1/{project_id}/aad/policies/waf/cc	aad:policy:create	-
POST /v1/cnad/policies	aad:policy:create	-

API	对应的授权项	依赖的授权项
DELETE /v1/{project_id}/aad/policies/waf/cc/{rule_id}	aad:policy:delete	-
DELETE /v1/cnad/policies/{policy_id}	aad:policy:delete	-
GET /v1/{project_id}/cad/flowblock	aad:policy:get	-
GET /v1/cnad/policies/{policy_id}	aad:policy:get	-
GET /v1/{project_id}/aad/policies/waf/cc	aad:policy:list	-
GET /v1/cnad/policies	aad:policy:list	-
PUT /v1/{project_id}/aad/policies/waf/cc/{rule_id}	aad:policy:put	-
POST /v1/{project_id}/cad/flowblock/udp	aad:policy:put	-
POST /v1/{project_id}/cad/flowblock/foreign	aad:policy:put	-
POST /v1/cnad/policies/{policy_id}/ip-list/add	aad:policy:put	-
POST /v1/cnad/policies/{policy_id}/bind	aad:policy:put	-
POST /v1/cnad/policies/{policy_id}/ip-list/delete	aad:policy:put	-
POST /v1/cnad/policies/{policy_id}/unbind	aad:policy:put	-
PUT /v1/cnad/policies/{policy_id}	aad:policy:put	-
GET /v1/{project_id}/aad/quotas/domain-port	aad:quotas:get	-
GET /v1/{project_id}/scc/waf/quota	aad:quotas:get	-
GET /v1/{project_id}/cad/quotas	aad:quotas:get	-
GET /v1/{project_id}/cad/ip/quotas	aad:quotas:get	-
GET /v1/{project_id}/cad/bwlist/quota	aad:quotas:get	-
GET /v1/{project_id}/aad/user-configs	aad:quotas:get	-
POST /v1/{project_id}/cad/bwlist	aad:whiteBlackIpRule:create	-

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/cad/bwlist/delete	aad:whiteBlackIpRule:delete	-
GET /v1/{project_id}/cad/bwlist	aad:whiteBlackIpRule:list	-
PUT /v1/cnad/protected-ips/tags	aad:protectedIp:put	-
GET /v1/cnad/protected-ips	aad:protectedIp:list	-
POST /v1/cnad/packages/{package_id}/protected-ips	aad:package:put	-
PUT /v1/cnad/packages/{package_id}/name	aad:package:put	-
GET /v1/cnad/packages	aad:package:list	-
GET /v1/cnad/packages/{package_id}/unbound-protected-ips	aad:package:list	-
POST /v1/unblockservice/{domain_id}/unblock	aad:block:put	-
GET /v1/unblockservice/{domain_id}/block-list	aad:block:list	-
GET /v1/unblockservice/{domain_id}/unblock-quota-statistics	aad:block:get	-
GET /v1/unblockservice/{domain_id}/block-statistics	aad:block:get	-
GET /v1/unblockservice/{domain_id}/unblock-record	aad:block:get	-
GET /v1/{project_id}/cad/instances/{instance_id}/elastic_count/{ip_id}	aad:instance:get	-
GET /v1/{project_id}/cad/instances/{data_center}/elastic/{line}/{ip_id}	aad:instance:get	-
GET /v1/aad/remain-vip-number	aad:quotas:get	-
GET /v1/aad/instance/connection-num	aad:dashboard:get	-
PUT /v1/{project_id}/cad/instances/{instance_id}/pp-switch	aad:instance:put	-
GET /v1/aad-service/ces/{domain_id}/dims-info	aad:instance:list	-

API	对应的授权项	依赖的授权项
GET /v1/aad-service/ces/v2/{domain_id}/instances	aad:instance:list	-
GET /v1/{project_id}/cad/instances/security-statistics	aad:instance:list	-
GET /v1/aad/domain/instances/rules	aad:domain:list	-
POST /v1/aad/policy/modify	aad:policy:put	-
POST /v1/aad/geoip	aad:policy:put	-
GET /v1/aad/geoip	aad:policy:get	-
DELETE /v1/aad/geoip/{ruleId}	aad:policy:delete	-
PUT /v1/aad/geoip/{ruleId}	aad:policy:put	-
POST /v1/aad/whiteip	aad:policy:put	-
GET /v1/aad/whiteip	aad:policy:get	-
DELETE /v1/aad/whiteip	aad:policy:delete	-
POST /v1/aad/custom	aad:policy:put	-
GET /v1/aad/custom	aad:policy:get	-
PUT /v1/aad/custom/{ruleId}	aad:policy:put	-
DELETE /v1/aad/custom/{ruleId}	aad:policy:delete	-
GET /v1/aad/policy/details	aad:policy:get	-
POST /v1/aad/cc/intelligent/modify	aad:policy:put	-
GET /v1/aad/geoip/map	aad:policy:get	-
GET /v1/aad/instances/{instance_id}/{ip}/ddos-statistics	aad:dashboard:get	-
GET /v1/aad/protected-domains/{domain_id}	aad:domain:get	-
GET /v1/aad/protected-domains	aad:domain:list	-
PUT /v1/aad/protected-domains/{domain_id}	aad:domain:put	-
POST /v1/aad/instances/{instance_id}/{ip}/rules/batch-create	aad:forwardingRule:create	-

API	对应的授权项	依赖的授权项
POST /v1/aad/instances/{instance_id}/{ip}/rules/batch-delete	aad:forwardingRule:delete	-
GET /v1/aad/instances/{instance_id}/{ip}/rules	aad:forwardingRule:list	-
PUT /v1/aad/instances/{instance_id}/{ip}/rules/{rule_id}	aad:forwardingRule:put	-
GET /v1/aad/instances	aad:instance:list	-

资源类型（Resource）

资源类型（Resource）表示SCP策略所作用的资源。如表5-73中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP策略语句中指定该资源的URN，SCP策略仅作用于此资源；如未指定，Resource默认为“*”，则SCP策略将应用到所有资源。您也可以在SCP策略中设置条件，从而指定资源类型。

AAD定义了以下可以在自定义SCP策略的Resource元素中使用的资源类型。

表 5-73 AAD 支持的资源类型

资源类型	URN
forwardingRule	aad::<account-id>:forwardingRule:<forwarding-rule-id>
package	aad::<account-id>:package:<package-id>
policy	aad::<account-id>:policy:<policy-id>
alarmConfig	aad::<account-id>:alarmConfig:<alarm-config-id>
domain	aad::<account-id>:domain:<domain-id>
certificate	aad::<account-id>:certificate:<certificate-id>
instance	aad::<account-id>:instance:<instance-id>
whiteBlackIpRule	aad::<account-id>:whiteBlackIpRule:<white-black-ip-rule-id>

条件（Condition）

AAD服务不支持在SCP策略中的条件键中配置服务级的条件键。

AAD可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.7.2 主机安全服务 HSS

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于HSS定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

  关于HSS定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下HSS的相关操作。

表 5-74 HSS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:host:addHostsGroup	授予权限以创建服务器组。	write	host *	g:EnterpriseProjectId
hss:ars:addPWLPolicyHost	授予权限以进行白名单策略添加主机。	write	host *	g:EnterpriseProjectId
hss:rasp:addRaspPolicy	授予权限以添加防护策略。	write	-	g:EnterpriseProjectId
hss:safetyReport:addSecurityReport	授予权限以创建或复制新报告。	write	-	g:EnterpriseProjectId
hss:wtp:addTimingOffConfigInfo	授予权限以添加定时关闭防护配置。	write	host *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:wtp:addWtpHostProtectDirInfo	授予权限以增加防护目录。	write	host *	g:EnterpriseProjectId
hss:wtp:addWtpPrivilegedProcessInfo	授予权限以添加特权进程。	write	host *	g:EnterpriseProjectId
hss:setting:changeAutoKillVirusStatus	授予权限以开启或关闭程序自动隔离查杀。	write	-	g:EnterpriseProjectId
hss:event:changeBlockedIp	授予权限以解除拦截。	write	host *	g:EnterpriseProjectId
hss:setting:changeMalwareCollectStatus	授予权限以开启或关闭恶意软件云查样本收集配置。	write	-	g:EnterpriseProjectId
hss:ars:changePWLPolicy	授予权限以修改白名单策略。	write	-	g:EnterpriseProjectId
hss:ars:changePWLPolicyProcessStatus	授予权限以标记进程白名单策略识别进程。	write	-	g:EnterpriseProjectId
hss:safetyReport:changeSecurityReport	授予权限以修改报告。	write	-	g:EnterpriseProjectId
hss:ars:createPWLPolicy	授予权限以创建白名单策略。	write	host *	-
			-	g:EnterpriseProjectId
hss:ars:deletePWLPolicy	授予权限以删除白名单策略。	write	-	g:EnterpriseProjectId
hss:ars:deletePWLPolicyHost	授予权限以进行白名单策略删除主机。	write	host *	g:EnterpriseProjectId
hss:antiransomware:deleteRansomwareDuplicationInfo	授予权限以删除备份副本。	write	-	g:EnterpriseProjectId
hss:antiransomware:deleteRansomwareProtectionPolicy	授予权限以删除防护策略。	write	-	g:EnterpriseProjectId
hss:rasp:deleteRaspPolicy	授予权限以删除防护策略。	write	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:safetyReport:deleteSecurityReport	授予权限以删除报告。	write	-	g:EnterpriseProjectId
hss:wtp:deleteTimingOffConfigInfo	授予权限以删除定时关闭防护配置。	write	host *	g:EnterpriseProjectId
hss:wtp:deleteWtpBackupHostInfo	授予权限以删除远端备份服务器。	write	host *	g:EnterpriseProjectId
hss:wtp:deleteWtpHostProtectDirInfo	授予权限以删除防护目录。	write	host *	g:EnterpriseProjectId
hss:wtp:deleteWtpPrivilegedProcessInfo	授予权限以删除特权进程。	write	host *	g:EnterpriseProjectId
hss:setting:getAgentInstallScript	授予权限以查询agent安装脚本。	read	-	g:EnterpriseProjectId
hss:setting:getAlarmConfig	授予权限以查询告警配置。	read	-	g:EnterpriseProjectId
hss:rasp:getAppRaspSwitchStatus	授予权限以查询应用防护开启状态。	read	host *	g:EnterpriseProjectId
hss:setting:getAutoKillVirusStatus	授予权限以查询程序自动隔离查杀状态。	read	-	g:EnterpriseProjectId
hss:container:getContainerNodeStatistics	授予权限以查询容器节点防护总览数据。	read	-	g:EnterpriseProjectId
hss:keyfile:getFileStatistic	授予权限以获取服务器文件统计信息。	read	-	g:EnterpriseProjectId
hss:setting:getMalwareCollectStatus	授予权限以查询恶意软件云查样本收集配置开关状态。	read	-	g:EnterpriseProjectId
hss:setting:getMalwareReminders	授予权限以获取提示信息配置。	read	-	g:EnterpriseProjectId
hss:securitycheck:getManualSecurityCheckStatus	授予权限以查询手动体检状态和进度。	read	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:overview:getOverviewAssetGroupsStatistics	授予权限以获取业务组分布统计，并识别一般资产、重要资产、核心资产。	read	-	g:EnterpriseProjectId
hss:overview:getOverviewAssetOsStatistics	授予权限以获取操作系统分布统计。	read	-	g:EnterpriseProjectId
hss:overview:getOverviewAssetStatistics	授予权限以获取资产统计，包含主机、容器、镜像。	read	-	g:EnterpriseProjectId
hss:overview:getOverviewAttckMitre	授予权限以调查响应-ATT&CK攻击路径矩阵。	read	-	g:EnterpriseProjectId
hss:overview:getOverviewDefenseStatistics	授予权限以获取主动防御统计。	read	-	g:EnterpriseProjectId
hss:overview:getOverviewProtectionStatusStatistics	授予权限以查询当前云负载的防护状态。	read	-	g:EnterpriseProjectId
hss:overview:getOverviewQuotaStatistics	授予权限以获取主机安全统计。	read	-	g:EnterpriseProjectId
hss:overview:getOverviewRiskLists	授予权限以查询风险列表。	read	-	g:EnterpriseProjectId
hss:overview:getOverviewRiskManageStatistics	授予权限以获取风险管理，包含风险趋势和类型统计。	read	-	g:EnterpriseProjectId
hss:overview:getOverviewRiskScore	授予权限以查询风险评分结果。	read	-	g:EnterpriseProjectId
hss:overview:getOverviewRiskStatistics	授予权限以查询风险统计，安全风险、安全告警、主动防御。	read	-	g:EnterpriseProjectId
hss:overview:getOverviewTrialsStatistics	授予权限以试用主机风险统计。	read	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:antiransomware:getRansomwareBackupInfoByBackupId	授予权限以查询指定备份信息。	read	-	g:EnterpriseProjectId
hss:antiransomware:getRansomwareHSSBackupPolicyInfo	授予权限以查询备份策略信息。	read	-	g:EnterpriseProjectId
hss:antiransomware:getRansomwareBackupStatistics	授予权限以查询备份统计信息。	read	-	g:EnterpriseProjectId
hss:antiransomware:getRansomwareProtectionStatistics	授予权限以查询防护统计信息。	read	-	g:EnterpriseProjectId
hss:antiransomware:getRansomwareVaultInfo	授予权限以查询备份存储库信息。	read	-	g:EnterpriseProjectId
hss:rasp:getRaspPolicyDetail	授予权限以查询防护策略详情。	read	-	g:EnterpriseProjectId
hss:rasp:getRaspProtectStatistics	授予权限以获取防护数据统计。	read	-	g:EnterpriseProjectId
hss:wtp:getRaspSwitchStatus	授予权限以查询动态网页防篡改开启状态。	read	host *	g:EnterpriseProjectId
hss:securitycheck:getSecurityCheckConfig	授予权限以查询安全体检定时配置信息。	read	-	g:EnterpriseProjectId
hss:securitycheck:getSecurityCheckHostReport	授予权限以查询指定服务器的安全体检报告。	read	host *	g:EnterpriseProjectId
hss:securitycheck:getSecurityCheckOverview	授予权限以查询安全体检概览信息。	read	-	g:EnterpriseProjectId
hss:securitycheck:getSecurityCheckStatistic	授予权限以查询安全体检统计信息。	read	-	g:EnterpriseProjectId
hss:safetyReport:getSecurityReport	授予权限以查询安全报告内容。	read	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:safetyReport:getSecurityReportSubscription	授予权限以查询报告订阅的内容。	read	-	g:EnterpriseProjectId
hss:wtp:getTimingOffStatusInfo	授予权限以查询定时关闭防护开关状态。	read	host *	g:EnterpriseProjectId
hss:wtp:getWtpDashboardProtectStatistics	授予权限以查询防护数据统计。	read	-	g:EnterpriseProjectId
hss:wtp:getWtpDirectory	授予权限以查询动态网页防篡改的Tomcat bin目录。	read	host *	g:EnterpriseProjectId
hss:wtp:getWtpDirectoryMonitorOnlyStatus	授予权限以查询只监控不修复开关状态。	read	host *	g:EnterpriseProjectId
hss:wtp:getWtpPrivilegedProcessesChildStatus	授予权限以展示特权进程子进程可信状态。	read	host *	g:EnterpriseProjectId
hss:wtp:getWtpRemoteBackupHostInfo	授予权限以查询远端备份服务器信息。	read	host *	g:EnterpriseProjectId
hss:setting:listAgentVersion	授予权限以查询agent版本信息列表。	list	-	g:EnterpriseProjectId
hss:container:listContainerNodes	授予权限以查询容器节点列表。	list	-	g:EnterpriseProjectId
hss:keyfile:listFileEvents	授予权限以获取变更文件列表。	list	-	g:EnterpriseProjectId
hss:keyfile:listFileHostEventDetails	授予权限以获取某个服务器变更文件信息。	list	host *	g:EnterpriseProjectId
hss:keyfile:listFileHosts	授予权限以获取云服务器变更列表。	list	-	g:EnterpriseProjectId
hss:host:listHostGroups	授予权限以查询服务器组列表。	list	-	g:EnterpriseProjectId
hss:setting:listLoginCommonIp	授予权限以查询常用登录IP信息。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:setting:listLoginCommonLocation	授予权限以查询常用登录地信息。	list	-	g:EnterpriseProjectId
hss:setting:listLoginWhiteIp	授予权限以查询登录IP白名单。	list	-	g:EnterpriseProjectId
hss:policy:listPolicyGroup	授予权限以查询策略组列表。	list	-	g:EnterpriseProjectId
hss:asset:listPortHost	授予权限以查询资产指纹-端口-服务器列表。	list	-	g:EnterpriseProjectId
hss:asset:listProcessesHost	授予权限以查询资产指纹-进程-服务器列表。	list	-	g:EnterpriseProjectId
hss:ars:listPWLEvent	授予权限以查询进程白名单事件。	list	-	g:EnterpriseProjectId
hss:ars:listPwlPolicy	授予权限以查询进程白名单策略列表。	list	-	g:EnterpriseProjectId
hss:ars:listPwlPolicyHost	授予权限以查询进程白名单策略关联主机列表。	list	-	g:EnterpriseProjectId
hss:ars:listPwlPolicyProcess	授予权限以查询进程白名单策略识别进程。	list	-	g:EnterpriseProjectId
hss:antiransomware:listRansomwareBackedupByHostId	授予权限以查询备份列表。	list	host *	g:EnterpriseProjectId
hss:antiransomware:listRansomwareOperationLogsByVaultName	授予权限以查询备份恢复任务列表。	list	-	g:EnterpriseProjectId
hss:antiransomware:listRansomwareProtectionOptionalServer	授予权限以查询可选防护服务器列表。	list	-	g:EnterpriseProjectId
hss:antiransomware:listRansomwareProtectionPolicy	授予权限以查询防护策略列表。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:antiransomware:listRansomwareProtectionServer	授予权限以查询勒索防护服务器列表。	list	-	g:EnterpriseProjectId
hss:rasp:listRaspCheckFeatureRule	授予权限以查询检测规则列表。	list	-	g:EnterpriseProjectId
hss:rasp:listRaspEvents	授予权限以查询应用防护事件列表。	list	-	g:EnterpriseProjectId
hss:rasp:listRaspPolicies	授予权限以查询防护策略列表。	list	-	g:EnterpriseProjectId
hss:rasp:listRaspProtectionServers	授予权限以查询防护服务器列表。	list	-	g:EnterpriseProjectId
hss:securitycheck:listSecurityCheckHostReportHistory	授予权限以查询指定服务器的安全体检历史报告列表。	list	host *	g:EnterpriseProjectId
hss:securitycheck:listSecurityCheckHostResult	授予权限以查询多服务器的安全体检结果列表。	list	-	g:EnterpriseProjectId
hss:safetyReport:listSecurityReport	授予权限以查询报告总览页列表。	list	-	g:EnterpriseProjectId
hss:safetyReport:listSecurityReportHistoryPeriod	授予权限以查询历史报告统计周期列表。	list	-	g:EnterpriseProjectId
hss:safetyReport:listSecurityReportSendingRecord	授予权限以查询报告发送记录列表。	list	-	g:EnterpriseProjectId
hss:wtp:listTimingOffConfigInfo	授予权限以查询定时关闭防护配置列表。	list	host *	g:EnterpriseProjectId
hss:setting:listTwoFactorLoginHost	授予权限以查询双因子主机列表。	list	-	g:EnterpriseProjectId
hss:wtp:listWtpBackupHostsInfo	授予权限以查询远端备份服务器。	list	-	g:EnterpriseProjectId
hss:wtp:listWtpHostProtectDirInfo	授予权限以查询主机防护目录。	list	host *	g:EnterpriseProjectId
hss:wtp:listWtpHostProtectHistoryInfo	授予权限以查询主机静态网页防篡改防护动态。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:wtp:listWtpHostRaspProtectHistoryInfo	授予权限以查询主机动态网页防篡改防护动态。	list	-	g:EnterpriseProjectId
hss:wtp:listWtpPrivilegedProcessesInfo	授予权限以查询特权进程配置。	list	host *	g:EnterpriseProjectId
hss:wtp:listWtpProtectHost	授予权限以查询防护列表。	list	-	g:EnterpriseProjectId
hss:setting:modifyLoginCommonIp	授予权限以添加、编辑或删除常用登录IP地址。	write	host *	g:EnterpriseProjectId
hss:setting:modifyLoginCommonLocation	授予权限以添加、编辑或删除常用登录地。	write	host *	g:EnterpriseProjectId
hss:setting:modifyLoginWhiteIp	授予权限以添加、编辑或删除登录IP白名单。	write	host *	g:EnterpriseProjectId
hss:ars:operatePWLEvent	授予权限以处理事件。	write	-	g:EnterpriseProjectId
hss:ars:relearnPWLPolicy	授予权限以进行白名单策略重新学习。	write	host *	g:EnterpriseProjectId
hss:overview:resetOverviewRiskScore	授予权限以重置风险评分，重新体检。	write	-	g:EnterpriseProjectId
hss:antiransomware:restoreRansomwareDuplicationInfo	授予权限以备份恢复。	write	-	g:EnterpriseProjectId
hss:safetyReport:sendSecurityReport	授予权限以发送安全报告。	write	-	g:EnterpriseProjectId
hss:setting:setAlarmConfig	授予权限以设置提示信息配置。	write	-	g:EnterpriseProjectId
hss:setting:setMalwareReminders	授予权限以设置提示信息配置。	write	-	g:EnterpriseProjectId
hss:wtp:setRemoteWtpBackupInfo	授予权限以开启关闭远端备份。	write	host *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:wtp:setTimingOffSwitchInfo	授予权限以设置定时关闭防护开关状态。	write	host *	g:EnterpriseProjectId
hss:setting:setTwoFactorLoginConfig	授予权限以设置双因子登录配置。	write	host *	g:EnterpriseProjectId
hss:wtp:setWtpDirectoryMonitorOnlyStatus	授予权限以设置只监控不修复开关状态。	write	host *	g:EnterpriseProjectId
hss:wtp:setWtpPrivilegedProcessesChildStatus	授予权限以设置特权进程子进程可信状态。	write	host *	g:EnterpriseProjectId
hss:wtp:setWtpProtectionStatusInfo	授予权限以开启关闭网页防篡改防护。	write	host *	g:EnterpriseProjectId
hss:wtp:setWtpProtectSwitch	授予权限以开启/关闭动态网页防篡改防护。	write	host *	g:EnterpriseProjectId
hss:wtp:setWtpScheduledProtectionDateOffConfigInfo	授予权限以设置自动关闭防护的频率周期。	write	host *	g:EnterpriseProjectId
hss:securitycheck:startManualSecurityCheck	授予权限以启动手动体检。	write	-	g:EnterpriseProjectId
hss:antiransomware:startRansomwareBackupSingle	授予权限以开启单台服务器备份功能。	write	host *	g:EnterpriseProjectId
hss:antiransomware:startRansomwareProtection	授予权限以开启勒索病毒防护。	write	host *	g:EnterpriseProjectId
hss:antiransomware:startRansomwareProtectionSingle	授予权限以开启单台服务器勒索防护。	write	host *	g:EnterpriseProjectId
hss:securitycheck:stopManualSecurityCheck	授予权限以取消手动体检。	write	-	g:EnterpriseProjectId
hss:antiransomware:stopRansomwareProtection	授予权限以关闭勒索病毒防护。	write	host *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:container:switchContainerProtectStatus	授予权限以切换防护状态。	write	host *	g:EnterpriseProjectId
hss:ars:switchPWLPolicyHost	授予权限以开启/关闭主机白名单策略。	write	host *	g:EnterpriseProjectId
hss:rasp:switchRasp	授予权限以开启/关闭应用防护。	write	host *	g:EnterpriseProjectId
hss:safetyReport:switchSecurityReportStatus	授予权限以修改安全报告开关。	write	-	g:EnterpriseProjectId
hss:wtp:switchWtpHostProtectDirInfo	授予权限以开启/关闭目录防护。	write	host *	g:EnterpriseProjectId
hss:host:uninstallAgents	授予权限以卸载Agent。	write	host *	g:EnterpriseProjectId
hss:setting:updateAlarmConfig	授予权限以设置告警配置。	write	-	g:EnterpriseProjectId
hss:antiransomware:updateRansomwareBackupPolicyInfo	授予权限以修改备份策略。	write	-	g:EnterpriseProjectId
hss:antiransomware:updateRansomwareProtectionPolicy	授予权限以修改防护策略。	write	-	g:EnterpriseProjectId
hss:rasp:updateRaspPolicy	授予权限以修改防护策略。	write	-	g:EnterpriseProjectId
hss:securitycheck:updateSecurityCheckConfig	授予权限以修改安全体检定时配置信息。	write	-	g:EnterpriseProjectId
hss:wtp:updateTimingOffConfigInfo	授予权限以修改定时关闭防护配置。	write	host *	g:EnterpriseProjectId
hss:wtp:updateWtpBackupHostInfo	授予权限以添加或修改远端备份服务器。	write	host *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:wtp:updateWtpDirectoryInfo	授予权限以修改动态网页防篡改的Tomcat bin目录。	write	host *	g:EnterpriseProjectId
hss:wtp:updateWtpHostProtectDirInfo	授予权限以修改防护目录。	write	host *	g:EnterpriseProjectId
hss:wtp:updateWtpPrivilegedProcessInfo	授予权限以修改特权进程。	write	host *	g:EnterpriseProjectId
hss:asset:addValuesLevel	授予权限以关联资产管理-主机管理-资产重要性。	write	host *	g:EnterpriseProjectId
hss:asset:batchModifyPortStatus	授予权限以修改端口状态。	write	host *	g:EnterpriseProjectId
hss:asset:deleteToolConditionHistory	授予权限以清除工具的搜索记录（运营工具）。	write	-	g:EnterpriseProjectId
hss:asset:executeTool	授予权限以工具执行搜索（运营工具）。	write	-	g:EnterpriseProjectId
hss:asset:getAccountTop	授予权限以获取资产管理-概览-账户Top。	read	-	g:EnterpriseProjectId
hss:asset:getAgentStatisticsStatus	授予权限以获取资产管理-概览-资产状态-主机Agent状态。	read	-	g:EnterpriseProjectId
hss:asset:getAssetStatistic	授予权限以获取资产统计信息，账号、端口、进程等。	read	-	g:EnterpriseProjectId
hss:asset:getAssetType	授予权限以获取资产管理-概览-资产状态-资产分布。	read	-	g:EnterpriseProjectId
hss:asset:getAutoLaunchTop	授予权限以获取资产管理-概览-自启动项Top。	read	-	g:EnterpriseProjectId
hss:asset:getCommonPort	授予权限以呈现某一端口详细信息。	read	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:asset:getContainerProtectionStatus	授予权限以获取资产管理-概览-资产状态-容器节点防护状态。	read	-	g:EnterpriseProjectId
hss:asset:getCoreConfFileTop	授予权限以获取资产管理-概览-关键配置Top。	read	-	g:EnterpriseProjectId
hss:asset:getEnvironmentTop	授予权限以获取资产管理-概览-环境变量Top。	read	-	g:EnterpriseProjectId
hss:asset:getHostAssetManualCollectStatus	授予权限以获取单主机资产指纹立即采集接口的运行状态。	read	host *	g:EnterpriseProjectId
hss:asset:getHostProtectionStatus	授予权限以获取资产管理-概览-资产状态-Agent状态。	read	-	g:EnterpriseProjectId
hss:asset:getJarPackageTop	授予权限以获取资产管理-概览-jar包Top。	read	-	g:EnterpriseProjectId
hss:asset:getKernelModuleTop	授予权限以获取资产管理-概览-内核模块Top。	read	-	g:EnterpriseProjectId
hss:asset:getOsStatisticsInfo	授予权限以获取资产管理-概览-资产状态-操作系统统计信息。	read	-	g:EnterpriseProjectId
hss:asset:getPorcessTop	授予权限以获取资产管理-概览-进程Top。	read	-	g:EnterpriseProjectId
hss:asset:getPortTop	授予权限以获取资产管理-概览-端口Top。	read	-	g:EnterpriseProjectId
hss:asset:getQuotaStatisticsInfo	授予权限以获取资产管理-概览-资产状态-防护配额统计信息。	read	-	g:EnterpriseProjectId
hss:asset:getSoftwareTop	授予权限以获取资产管理-概览-软件Top。	read	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:asset:getWebAppAndServiceTop	授予权限以获取资产管理-概览-WebAppAndServiceTop。	read	-	g:EnterpriseProjectId
hss:asset:getWebAppTop	授予权限以获取资产管理-概览-Web应用Top。	read	-	g:EnterpriseProjectId
hss:asset:getWebFrameworkTop	授予权限以获取资产管理-概览-Web框架Top。	read	-	g:EnterpriseProjectId
hss:asset:getWebServiceTop	授予权限以获取资产管理-概览-Web服务Top。	read	-	g:EnterpriseProjectId
hss:asset:getWebSiteTop	授予权限以获取资产管理-概览-Web站点Top。	read	-	g:EnterpriseProjectId
hss:asset:listAppChangeHistories	授予权限以获取资产指纹-软件信息-历史变动记录。	list	-	g:EnterpriseProjectId
hss:asset:listApps	授予权限以获取单主机资产指纹-软件。	list	-	g:EnterpriseProjectId
hss:asset:listAppStatistics	授予权限以获取资产指纹-软件信息。	list	-	g:EnterpriseProjectId
hss:asset:listAutoLaunchChangeHistories	授予权限以获取资产指纹-自启动项-历史变动记录。	list	-	g:EnterpriseProjectId
hss:asset:listAutoLaunchs	授予权限以获取单主机资产指纹-自启动项。	list	-	g:EnterpriseProjectId
hss:asset:listAutoLaunchStatistics	授予权限以获取资产指纹-自启动项信息。	list	-	g:EnterpriseProjectId
hss:asset:listCoreConfFileHostInfo	授予权限以获取资产管理-资产指纹-系统关键配置文件的服务器列表。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:asset:listCoreConfFileInfo	授予权限以获取资产管理-主机管理-指纹类型-关键配置。	list	host *	g:EnterpriseProjectId
hss:asset:listCoreConfFileStatistics	授予权限以获取资产管理-资产指纹-系统关键配置文件左侧树。	list	-	g:EnterpriseProjectId
hss:asset:listEnvironmentHostInfo	授予权限以获取资产管理-资产指纹-环境变量的服务器列表（资产指纹右侧服务器列表）。	list	-	g:EnterpriseProjectId
hss:asset:listEnvironmentInfo	授予权限以获取资产管理-主机管理-指纹类型-环境变量。	list	host *	g:EnterpriseProjectId
hss:asset:listEnvironmentStatistics	授予权限以获取资产管理-资产指纹-环境变量文件左侧树。	list	-	g:EnterpriseProjectId
hss:asset:listJarPackageHostInfo	授予权限以获取资产管理-资产指纹-Jar包的服务器列表。	list	-	g:EnterpriseProjectId
hss:asset:listJarPackageInfo	授予权限以获取资产管理-主机管理-指纹类型-Jar包。	list	host *	g:EnterpriseProjectId
hss:asset:listJarPackageStatistics	授予权限以获取资产管理-资产指纹-Jar包左侧树。	list	-	g:EnterpriseProjectId
hss:asset:listKernelModuleHostInfo	授予权限以获取资产管理-资产指纹-内核模块的服务器列表。	list	-	g:EnterpriseProjectId
hss:asset:listKernelModuleInfo	授予权限以获取资产管理-主机管理-指纹类型-内核模块。	list	host *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:asset:listKernelModuleStatistics	授予权限以获取资产管理-资产指纹-内核模块左侧树。	list	-	g:EnterpriseProjectId
hss:asset:listPorts	授予权限以获取单主机资产指纹-开放端口信息。	list	host *	g:EnterpriseProjectId
hss:asset:listPortStatistics	授予权限以获取资产指纹-开放端口信息。	list	-	g:EnterpriseProjectId
hss:asset:listProcesses	授予权限以获取进程列表。	list	host *	g:EnterpriseProjectId
hss:asset:listProcessStatistics	授予权限以获取资产指纹-进程信息。	list	-	g:EnterpriseProjectId
hss:asset:listResult	授予权限以获取执行结果（运营工具）。	list	-	g:EnterpriseProjectId
hss:asset:listTool	授予权限以获取工具列表（运营工具）。	list	-	g:EnterpriseProjectId
hss:asset:listToolConditionHistory	授予权限以获取工具的搜索记录（运营工具）。	list	-	g:EnterpriseProjectId
hss:asset:listUserChangeHistories	授予权限以获取账户变动历史记录信息。	list	-	g:EnterpriseProjectId
hss:asset:listUserGroup	授予权限以获取用户组列表。	list	-	g:EnterpriseProjectId
hss:asset:listUsers	授予权限以获取资产的账号列表。	list	-	g:EnterpriseProjectId
hss:asset:listUserStatistics	授予权限以获取资产指纹-账号信息。	list	-	g:EnterpriseProjectId
hss:asset:listWebAppAndServices	授予权限以获取资产管理-资产指纹-右侧WebAppAndService资产信息。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:asset:listWebAppAndServiceStatistics	授予权限以获取资产管理-资产指纹-左侧WebAppAndService名称树信息。	list	-	g:EnterpriseProjectId
hss:asset:listWebAppHostInfo	授予权限以获取资产管理-资产指纹-Web应用的服务器列表。	list	-	g:EnterpriseProjectId
hss:asset:listWebAppInfo	授予权限以获取资产管理-主机管理-指纹类型-Web应用。	list	host *	g:EnterpriseProjectId
hss:asset:listWebAppStatistics	授予权限以获取资产管理-资产指纹-Web应用左侧树。	list	-	g:EnterpriseProjectId
hss:asset:listWebFrameworkHostInfo	授予权限以获取资产管理-资产指纹-Web框架的服务器列表。	list	-	g:EnterpriseProjectId
hss:asset:listWebFrameworkInfo	授予权限以获取资产管理-主机管理-指纹类型-Web框架。	list	host *	g:EnterpriseProjectId
hss:asset:listWebFrameworkStatistics	授予权限以获取资产管理-资产指纹-Web框架左侧树。	list	-	g:EnterpriseProjectId
hss:asset:listWebServiceHostInfo	授予权限以获取资产管理-资产指纹-Web服务的服务器列表。	list	-	g:EnterpriseProjectId
hss:asset:listWebServiceInfo	授予权限以获取资产管理-主机管理-指纹类型-Web服务。	list	host *	g:EnterpriseProjectId
hss:asset:listWebServiceStatistics	授予权限以获取资产管理-资产指纹-Web服务左侧树。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:asset:listWebSiteHostInfo	授予权限以获取资产管理-资产指纹-Web站点的服务器列表。	list	-	g:EnterpriseProjectId
hss:asset:listWebSiteInfo	授予权限以获取资产管理-主机管理-指纹类型-Web站点。	list	host *	g:EnterpriseProjectId
hss:asset:listWebSiteStatistics	授予权限以获取资产管理-资产指纹-Web站点左侧树。	list	-	g:EnterpriseProjectId
hss:asset:runHostAssetManualCollect	授予权限以立即采集单主机资产指纹。	write	host *	g:EnterpriseProjectId
hss:baseline:addSecurityCheckPolicyGroup	授予权限以新建配置检测策略信息。	write	-	g:EnterpriseProjectId
hss:baseline:changeCheckRuleState	授予权限以对未通过的配置检查项进行忽略/取消忽略/修复/验证操作。	write	baseline *	g:EnterpriseProjectId
hss:baseline:deleteSecurityCheckPolicyGroup	授予权限以删除指定配置检测策略信息。	write	-	g:EnterpriseProjectId
hss:baseline:exportSecurityCheckReport	授予权限以按查询结果导出配置检测报告。	list	-	g:EnterpriseProjectId
hss:baseline:getBaselineOverview	授予权限以查询基线检查的统计数据信息。	read	-	g:EnterpriseProjectId
hss:baseline:getBaselineScanStatus	授予权限以查询基线检查任务进度。	read	-	g:EnterpriseProjectId
hss:baseline:getBaselineStatistic	授予权限以查询基线检查的统计数据信息，包括弱口令，口令复杂度，配置检测。	read	-	g:EnterpriseProjectId
hss:baseline:getCheckRuleDetail	授予权限以查询配置检查项检测报告。	read	baseline *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:baseline:getCheckRuleFixFailDetail	授予权限以查询检查项修复失败原因。	read	baseline *	g:EnterpriseProjectId
hss:baseline:getDefaultSecurityCheckPolicy	授予权限以查询配置检测策略的默认基线信息。	read	-	g:EnterpriseProjectId
hss:baseline:getDefaultSecurityCheckPolicyDetails	授予权限以查询基线的详细检查项。	read	-	g:EnterpriseProjectId
hss:baseline:getRiskConfigDetail	授予权限以查询指定安全配置项的检查结果。	read	-	g:EnterpriseProjectId
hss:baseline:listCheckRuleHost	授予权限以查询配置检查项影响到的服务器列表。	list	baseline *	g:EnterpriseProjectId
hss:baseline:listPasswordComplexity	授予权限以查询口令复杂度策略检测报告。	list	-	g:EnterpriseProjectId
hss:baseline:listRiskConfigCheckRules	授予权限以查询指定安全配置项的检查项列表。	list	-	g:EnterpriseProjectId
hss:baseline:listRiskConfigHosts	授予权限以查询指定安全配置项的受影响服务器列表。	list	-	g:EnterpriseProjectId
hss:baseline:listRiskConfigs	授予权限以查询租户的服务器安全配置检测结果列表。	list	-	g:EnterpriseProjectId
hss:baseline:listSecurityCheckPolicyGroup	授予权限以查询配置检测策略组列表。	list	-	g:EnterpriseProjectId
hss:baseline:listWeakPasswordUsers	授予权限以查询弱口令检测结果列表。	list	-	g:EnterpriseProjectId
hss:baseline:runBaselineDetect	授予权限以手动检测：对策略中选择的主机，进行配置检测和弱口令检测。	write	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:baseline:updateSecurityCheckPolicyGroup	授予权限以修改指定配置检测策略信息。	write	-	g:EnterpriseProjectId
hss:event:addLoginWhiteList	授予权限以添加登录白名单。	write	-	g:EnterpriseProjectId
hss:event:batchChangeEvent	授予权限以批量处理告警事件。	write	-	g:EnterpriseProjectId
hss:event:changeEvent	授予权限以处理告警事件。	write	event *	g:EnterpriseProjectId
hss:event:changeIsolatedFile	授予权限以恢复已隔离文件。	write	host *	g:EnterpriseProjectId
hss:event:exportAlarmWhiteList	授予权限以导出告警白名单。	list	-	g:EnterpriseProjectId
hss:event:exportEmergency	授予权限以导出应急恶意程序接口。	list	-	g:EnterpriseProjectId
hss:event:getEmergencyStatistics	授予权限以获取应急事件统计信息。	read	-	g:EnterpriseProjectId
hss:event:getEventAttackTag	授予权限以查询攻击标识分布统计列表。	read	-	g:EnterpriseProjectId
hss:event:getEventSeverity	授予权限以查询威胁等级统计列表。	read	-	g:EnterpriseProjectId
hss:event:getEventStatistics	授予权限以查询告警事件统计。	read	-	g:EnterpriseProjectId
hss:event:getMalwareInfo	授予权限以获取突发恶意程序详情列表。	read	event *	g:EnterpriseProjectId
hss:event:handleMalwareEvent	授予权限以处理恶意程序。	write	event *	g:EnterpriseProjectId
hss:event:importAlarmWhiteList	授予权限以导入告警白名单。	write	-	g:EnterpriseProjectId
hss:event:isolateOperateEmergency	授予权限以开启或关闭隔离箱。	write	-	g:EnterpriseProjectId
hss:event:listAlarmWhiteList	授予权限以查询告警白名单列表。	list	-	g:EnterpriseProjectId
hss:event:listBlockedIp	授予权限以查询已拦截IP列表。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:event:listEventOperates	授予权限以查询事件支持的处理类型。	list	-	g:EnterpriseProjectId
hss:event:listEventTopRisk	授予权限以查询TOP10事件类型统计列表。	list	-	g:EnterpriseProjectId
hss:event:listEventType	授予权限以查询事件类型统计列表。	list	-	g:EnterpriseProjectId
hss:event:listFileIsolateList	授予权限以获取突发恶意程序隔离文件列表。	list	-	g:EnterpriseProjectId
hss:event:listIsolatedFile	授予权限以查询已隔离文件列表。	list	-	g:EnterpriseProjectId
hss:event:listLoginWhiteList	授予权限以查询登录白名单列表。	list	-	g:EnterpriseProjectId
hss:event:listMalware	授予权限以获取突发恶意程序事件列表。	list	-	g:EnterpriseProjectId
hss:event:listSecurityEvents	授予权限以查入侵事件列表。	list	-	g:EnterpriseProjectId
hss:event:recoverIsolateFile	授予权限以恢复文件隔离箱。	write	-	g:EnterpriseProjectId
hss:event:removeAlarmWhiteList	授予权限以删除告警白名单。	write	-	g:EnterpriseProjectId
hss:event:removeLoginWhiteList	授予权限以删除登录白名单。	write	-	g:EnterpriseProjectId
hss:host:associateHostAssetValue	授予权限以关联资产重要性。	write	host *	g:EnterpriseProjectId
hss:host:associateHostsGroup	授予权限以分配到组。	write	host *	g:EnterpriseProjectId
hss:host:batchInstallAgent	授予权限以批量安装agent。	write	host *	g:EnterpriseProjectId
hss:host:changeHostsGroup	授予权限以编辑服务器组。	write	-	g:EnterpriseProjectId
hss:host:deleteHostsGroup	授予权限以删除服务器组。	write	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:host:getHostsStatistics	授予权限以统计服务器数据。	read	-	g:EnterpriseProjectId
hss:host:listFirewallStatus	授予权限以查询主机是否开启防火墙。	read	host *	g:EnterpriseProjectId
hss:host:listHostGroupAssetValue	授予权限以查询资产重要性的服务器组列表。	list	-	g:EnterpriseProjectId
hss:host:listHostsRisk	授予权限以获取ECS风险状况。	read	host *	g:EnterpriseProjectId
hss:host:listHostStatus	授予权限以查询云服务器列表。	list	-	g:EnterpriseProjectId
hss:host:listHostsUpgrade	授予权限以获取主机的升级状态。	read	host *	-
			-	g:EnterpriseProjectId
hss:host:manualCheckVul	授予权限以手动检测漏洞。	write	-	g:EnterpriseProjectId
hss:host:switchFirewallStatus	授予权限以修改防火墙授权状态。	write	host *	g:EnterpriseProjectId
hss:host:switchHostsProtectStatus	授予权限以切换防护状态。	write	host *	g:EnterpriseProjectId
hss:host:upgradeAgent	授予权限以升级Agent1.0到2.0。	write	host *	-
			-	g:EnterpriseProjectId
hss:host:upgradeAgents	授予权限以升级Agent。	write	host *	g:EnterpriseProjectId
hss:image:batchScanLocalImage	授予权限以进行本地镜像扫描。	write	-	g:EnterpriseProjectId
hss:image:batchScanPrivateImage	授予权限以批量扫描私有镜像仓库镜像。	write	-	g:EnterpriseProjectId
hss:image:getImageFilesStat	授予权限以查询镜像文件统计信息。	read	-	g:EnterpriseProjectId
hss:image:getImageLocalVulOverview	授予权限以查询本地漏洞概览信息。	read	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:image:getImageVulOverview	授予权限以查询仓库漏洞概览信息。	read	-	g:EnterpriseProjectId
hss:image:listCfgCheckAffectedImage	授予权限以查询租户镜像未通过基线项所影响的镜像列表。	list	-	g:EnterpriseProjectId
hss:image:listGlobalCfgCheck	授予权限以查询租户全量配置检测统计结果。	list	-	g:EnterpriseProjectId
hss:image:listGlobalMalware	授予权限以查询租户恶意文件列表。	list	-	g:EnterpriseProjectId
hss:image:listGlobalVul	授予权限以查询租户的漏洞信息。	list	-	g:EnterpriseProjectId
hss:image:listImageApps	授予权限以查询镜像软件列表。	list	-	g:EnterpriseProjectId
hss:image:listImageAppVul	授予权限以查询软件漏洞列表。	list	-	g:EnterpriseProjectId
hss:image:listImageCfgCheck	授予权限以查询单个镜像的配置基线检测结果。	list	-	g:EnterpriseProjectId
hss:image:listImageFiles	授予权限以查询镜像无归属文件列表。	list	-	g:EnterpriseProjectId
hss:image:listImageLocal	授予权限以查询本地镜像列表。	list	-	g:EnterpriseProjectId
hss:image:listImageMalware	授予权限以查询镜像恶意文件列表。	list	-	g:EnterpriseProjectId
hss:image:listImageNamespace	授予权限以查询镜像namespace信息。	list	-	g:EnterpriseProjectId
hss:image:listImageRepository	授予权限以查询私有镜像仓库镜像列表。	list	-	g:EnterpriseProjectId
hss:image:listImageVul	授予权限以查询镜像的漏洞信息。	list	-	g:EnterpriseProjectId
hss:image:listInstanceImageVul	授予权限以查询企业镜像的漏洞信息。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:image:listLocalImageApp	授予权限以查询本地镜像软件列表。	list	-	g:EnterpriseProjectId
hss:image:listLocalImageAppVuls	授予权限以查询本地镜像某软件的软件漏洞列表。	list	-	g:EnterpriseProjectId
hss:image:listLocalImageContainers	授予权限以查询本地镜像的容器信息。	list	-	g:EnterpriseProjectId
hss:image:listLocalImageHosts	授予权限以查询本地镜像的主机信息。	list	-	g:EnterpriseProjectId
hss:image:listLocalImageMalware	授予权限以查询本地镜像的恶意文件信息。	list	-	g:EnterpriseProjectId
hss:image:listLocalImageVuls	授予权限以查询本地镜像的漏洞信息。	list	-	g:EnterpriseProjectId
hss:image:listLocalVulRepoImage	授予权限以查询本地镜像漏洞影响的镜像和容器信息。	list	-	g:EnterpriseProjectId
hss:image:listPrivateImageRepository	授予权限以查询私有镜像仓库镜像列表。	list	-	g:EnterpriseProjectId
hss:image:listSharedImageRepository	授予权限以查询共享镜像仓库镜像列表。	list	-	g:EnterpriseProjectId
hss:image:listVulCve	授予权限以查询漏洞对应cve信息。	list	-	g:EnterpriseProjectId
hss:image:listVulRepoImage	授予权限以查询单个漏洞影响的镜像仓库中的镜像信息。	list	-	g:EnterpriseProjectId
hss:image:runImageScan	授予权限以扫描镜像。	write	-	g:EnterpriseProjectId
hss:image:runImageSynchronizeTask	授予权限以从SWR服务同步自由镜像列表。	write	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:image:runSwrImageScan	授予权限以更新并扫描SWR镜像,提供swr访问。	write	-	g:EnterpriseProjectId
hss:image:sharedImageSynchronization	授予权限以从swr更新他人共享镜像。	write	-	g:EnterpriseProjectId
hss:policy:addPolicyGroup	授予权限以复制主机策略组。	write	policy *	g:EnterpriseProjectId
hss:policy:associatePolicyGroup	授予权限以部署策略。	write	policy *	g:EnterpriseProjectId
			host *	g:EnterpriseProjectId
hss:policy:changePolicyDetail	授予权限以修改策略内容。	write	policy *	g:EnterpriseProjectId
hss:policy:changePolicyGroup	授予权限以修改策略组相关内容。	write	policy *	g:EnterpriseProjectId
hss:policy:deletePolicyGroup	授予权限以删除策略组。	write	policy *	g:EnterpriseProjectId
hss:policy:getPolicyDetail	授予权限以查询指定策略详细信息。	read	policy *	g:EnterpriseProjectId
hss:policy:listPolicyGroupDetail	授予权限以查询策略组策略信息列表。	list	policy *	g:EnterpriseProjectId
hss:quota:addResourceInstanceTag	授予权限以单个资源添加资源标签。	tagging	-	• g:RequestTag/<tag-key> • g:TagKeys
hss:quota:batchCreateTags	授予权限以批量创建标签。	write	-	• g:RequestTag/<tag-key> • g:TagKeys
hss:quota:batchDeleteTags	授予权限以批量删除标签。	write	-	• g:RequestTag/<tag-key> • g:TagKeys
hss:quota:cancelHostsQuota	授予权限以解绑配额。	write	-	-
hss:quota:changeTmsResourceTagInfo	授予权限以批量添加删除资源标签。	write	-	• g:RequestTag/<tag-key> • g:TagKeys

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:quota:countResourceInstances	授予权限以通过标签过滤购买的资源数量。	list	-	• g:RequestTag/<tag-key> • g:TagKeys
hss:quota:dealOrder	授予权限以订购HSS。	write	-	-
hss:quota:deleteResourceInstanceTag	授予权限以删除单个资源下的标签。	tagging	-	• g:RequestTag/<tag-key> • g:TagKeys
hss:quota:filterResourceInstanceList	授予权限以通过标签过滤购买的资源列表。	list	-	• g:RequestTag/<tag-key> • g:TagKeys
hss:quota:getResourceInstanceTag	授予权限以查询单个资源的资源标签。	read	-	-
hss:quota:getResourceQuotas	授予权限以查询配额信息。	read	-	-
hss:quota:getTmsResourceTagsInfo	授予权限以查询资源标签。	read	-	-
hss:quota:listProjectTags	授予权限以查询租户当前项目下所有用过的标签。	list	-	-
hss:quota:listQuotasDetail	授予权限以查询配额详情。	list	-	-
hss:quota:listResourceIds	授予权限以批量查询配额ID信息。	list	-	-
hss:quota:listTmsResourceInstancesInfo	授予权限以查询资源实例。	list	-	• g:RequestTag/<tag-key> • g:TagKeys
hss:quota:upgradeOrder	授予权限以变更规格。	write	-	-
hss:vulnerability:changeVulStatus	授予权限以修改漏洞的状态。	write	host *	g:EnterpriseProjectId
hss:vulnerability:exportEmergencyVulnerabilities	授予权限以导出应急漏洞。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:vulnerability:exportVulsList	授予权限以导出漏洞及漏洞影响的主机的相关信息。	list	-	g:EnterpriseProjectId
hss:vulnerability:getCmsVulDetail	授予权限以查询webcms漏洞基本信息。	read	-	g:EnterpriseProjectId
hss:vulnerability:getEmergencySummary	授予权限以查询应急事件总览。	read	-	g:EnterpriseProjectId
hss:vulnerability:getEmergencyVulDetail	授予权限以查询应急事件漏洞详情。	read	-	g:EnterpriseProjectId
hss:vulnerability:getLinuxVulDetail	授予权限以查询linux漏洞基本信息。	read	-	g:EnterpriseProjectId
hss:vulnerability:getVulCheckStatus	授予权限以查询主机漏洞的扫描状态。	read	-	g:EnterpriseProjectId
hss:vulnerability:getVulSummary	授予权限以查询漏洞统计信息。	read	-	g:EnterpriseProjectId
hss:vulnerability:getWindosVulDetail	授予权限以查询windows漏洞基本信息。	read	-	g:EnterpriseProjectId
hss:vulnerability:getWindowsVulNum	授予权限以查询主机windows漏洞的数量。	list	-	g:EnterpriseProjectId
hss:vulnerability:listEmergencyVul	授予权限以查询应急事件漏洞。	list	-	g:EnterpriseProjectId
hss:vulnerability:listHostVuls	授予权限以查询单台服务器漏洞信息。	list	host *	g:EnterpriseProjectId
hss:vulnerability:listHostVulSummary	授予权限以查询服务器统计信息和风险服务器TOP5。	list	-	g:EnterpriseProjectId
hss:vulnerability:listTopVulSummary	授予权限以查询漏洞TOP5。	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulHosts	授予权限以查询单个漏洞影响的云服务器信息。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:vulnerability:listVulnerabilities	授予权限以查询漏洞列表。	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulRepairFailedDetail	授予权限以查询漏洞修复失败信息。	list	host *	g:EnterpriseProjectId
hss:vulnerability:listVulTypeSummary	授予权限以查询漏洞类型分布。	list	-	g:EnterpriseProjectId
hss:vulnerability:operateEmergency	授予权限以操作应急事件漏洞。	write	-	g:EnterpriseProjectId
hss:host:getScanStatus	授予权限以查询手动检测状态。	read	host *	g:EnterpriseProjectId
hss:host:setManualDetect	授予权限以下发手动检测。	write	host *	g:EnterpriseProjectId
hss::getTrustServiceStatus	授予权限以获取可信服务状态。	read	-	-
hss::enableTrustService	授予权限以开启可信服务。	permission_management	-	-
hss::validateAdmin	授予权限以校验当前账号是否是管理员账号（包含组织管理员和委托管理员）。	tagging	-	-
hss::listAccounts	授予权限以展示多账号列表。	list	-	-
hss::batchAddAccounts	授予权限以批量添加账号。	write	-	-
hss::deleteAccount	授予权限以删除账号。	write	-	-
hss::listOrganizationTree	授予权限以展示多账号树形结构。	list	-	-
hss::listDelegatedAccounts	授予权限以查询已委托账号树形结构。	list	-	-
hss:antiransomware:listBackupVaults	授予权限以查询备份存储库列表。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:antiransomware:listRansomwareProtectionNodes	授予权限以查询勒索防护服务器列表。	list	-	g:EnterpriseProjectId
hss:antiransomware:getBackupsStatistics	授予权限以查询备份统计信息。	list	-	g:EnterpriseProjectId
hss:antiransomware:startSingleBackup	授予权限以开启单台服务器备份功能。	write	host *	-
			-	g:EnterpriseProjectId
hss:antiransomware:getBackupPolicyInfo	授予权限以查询单个备份策略信息。	read	-	g:EnterpriseProjectId
hss:hostGroup:getOutsideGroupStatus	授予权限以查询是否支持创建数据中心服务器组。	read	-	g:EnterpriseProjectId
hss:hostGroup:getOutsideHostGroup	授予权限以查询线下数据中心服务器组。	read	-	g:EnterpriseProjectId
hss:hostGroup:addOutsideHostGroup	授予权限以创建线下数据中心服务器组。	write	-	g:EnterpriseProjectId
hss:hostGroup:changeOutsideHostGroup	授予权限以编辑线下数据中心服务器组。	write	-	g:EnterpriseProjectId
hss:images:listImageTag	授予权限以查询镜像tag版本列表。	list	-	g:EnterpriseProjectId
hss:images:listImageSensitive	授予权限以查询镜像的敏感信息。	list	-	g:EnterpriseProjectId
hss:images:getFilePathWhiteDetail	授予权限以查询镜像的敏感信息文件路径白名单。	read	-	g:EnterpriseProjectId
hss:images:changeFilePathWhiteDetail	授予权限以修改镜像的敏感信息文件路径白名单。	write	-	g:EnterpriseProjectId
hss:images:changeSensitiveInfo	授予权限以操作处理敏感信息。	write	-	g:EnterpriseProjectId
hss:event:listTopEventType	授予权限以查询TOP5事件类型统计列表。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:vulnerability:getVulScanPolicy	授予权限以查询漏洞扫描策略。	read	-	-
hss:vulnerability:changeVulScanPolicy	授予权限以修改漏洞扫描策略。	write	host *	-
hss:vulnerability:listVulWhiteList	授予权限以查询漏洞白名单列表。	list	-	g:EnterpriseProjectId
hss:vulnerability:getVulWhiteListDetail	授予权限以查询漏洞白名单详情。	read	-	g:EnterpriseProjectId
hss:vulnerability:changeVulWhiteList	授予权限以修改漏洞白名单。	write	host *	-
			-	g:EnterpriseProjectId
hss:vulnerability:deleteVulWhiteList	授予权限以删除漏洞白名单。	write	-	-
hss:vulnerability:addVulWhiteList	授予权限以添加漏洞白名单。	write	host *	-
			-	g:EnterpriseProjectId
hss:vulnerability:listVulWhiteListVulOptions	授予权限以查询添加白名单时的漏洞选项。	list	-	-
hss:vulnerability:listVulScanTask	授予权限以查询漏洞扫描任务列表。	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulScanTaskHost	授予权限以查询漏洞扫描任务对应的主机列表。	list	-	g:EnterpriseProjectId
hss:vulnerability:rescanVulScanTask	授予权限以重新扫描之前漏洞扫描任务中的主机。	write	host *	-
			-	g:EnterpriseProjectId
hss:vulnerability:getVulScanTaskStatistics	授予权限以查询漏洞扫描任务的统计数据。	read	-	g:EnterpriseProjectId
hss:vulnerability:listHostVulStatistics	授予权限以查询漏洞管理统计数据。	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulHostApps	授予权限以查询漏洞受影响服务器详情-软件列表。	list	host *	-
			-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:vulnerability:listVulHostProcess	授予权限以查询漏洞受影响服务器详情-进程列表。	list	host *	-
			-	g:EnterpriseProjectId
hss:vulnerability:listVulHandleHistory	授予权限以查询漏洞历史处置记录。	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulHostHosts	授予权限以查询漏洞主机列表。	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulHostVuls	授予权限以查询紧急修复/未完成修复漏洞。	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulHostHandleVuls	授予权限以查询今日处理漏洞/累计处理漏洞。	list	-	g:EnterpriseProjectId
hss:image:listImageNonCompliantApp	授予权限以查询镜像的不合规软件信息。	list	-	g:EnterpriseProjectId
hss:image:batchExportSWRVulList	授予权限以swr镜像仓库漏洞批量导出。	write	-	g:EnterpriseProjectId
hss:image:batchExportLocalVulList	授予权限以本地镜像漏洞批量导出。	write	-	g:EnterpriseProjectId
hss:image:getExtendedWeakPassword	授予权限以查询镜像的自定义弱口令。	list	-	g:EnterpriseProjectId
hss:image:changeExtendedWeakPassword	授予权限以修改镜像的自定义弱口令。	write	-	g:EnterpriseProjectId
hss:image:listImageBasicImage	授予权限以查询镜像的基础镜像信息。	list	-	g:EnterpriseProjectId
hss:image:listImagePwdComplexity	授予权限以查询镜像口令复杂度策略检测报告。	list	-	g:EnterpriseProjectId
hss:image:listImageWeakPwdUsers	授予权限以查询镜像弱口令检测结果列表。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:image:listImageRiskConfigs	授予权限以查询镜像安全配置检测结果列表。	list	-	g:EnterpriseProjectId
hss:image:listImageRiskConfigCheckRules	授予权限以查询镜像指定安全配置项的检查项列表。	list	-	g:EnterpriseProjectId
hss:image:getImageRiskConfigDetail	授予权限以查询镜像指定安全配置项的检查结果。	read	-	g:EnterpriseProjectId
hss:image:getImageCheckRuleDetail	授予权限以查询镜像配置检查项检测报告。	read	-	g:EnterpriseProjectId
hss:image:getImageBaselineStatistic	授予权限以查询基线检查的统计数据信息，包括弱口令，口令复杂度，配置检测。	read	-	g:EnterpriseProjectId
hss:event:addSystemUserWhiteList	授予权限以添加系统用户白名单。	write	-	g:EnterpriseProjectId
hss:event:updateSystemUserWhiteList	授予权限以修改系统用户白名单。	write	-	g:EnterpriseProjectId
hss:event:listSystemUserWhiteList	授予权限以查询系统用户白名单。	list	-	g:EnterpriseProjectId
hss:event:removeSystemUserWhiteList	授予权限以删除系统用户白名单。	write	-	g:EnterpriseProjectId
hss:container:saveClusters	授予权限以同步集群信息。	write	-	g:EnterpriseProjectId
hss:container:listClusterInfo	授予权限以查询Kubernetes集群列表。	list	-	g:EnterpriseProjectId
hss:container:listPodInfo	授予权限以查询pod基本信息列表。	list	-	g:EnterpriseProjectId
hss:container:showPodDetail	授予权限以查询pod详细信息。	read	-	g:EnterpriseProjectId
hss:container:listContainerInfo	授予权限以查询容器基本信息列表。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:container:showContainerDetail	授予权限以查询容器详细信息。	list	-	g:EnterpriseProjectId
hss:container:listServiceInfo	授予权限以查询Kubernetes服务列表。	list	-	g:EnterpriseProjectId
hss:container:showServiceDetail	授予权限以查询Kubernetes服务详情。	read	-	g:EnterpriseProjectId
hss:container:listEndpointInfo	授予权限以查询kubernetes端点列表。	list	-	g:EnterpriseProjectId
hss:container:showEndpointDetail	授予权限以查询Kubernetes端点详情。	read	-	g:EnterpriseProjectId
hss:container:listDeployments	授予权限以查询Kubernetes无状态负载列表。	list	-	g:EnterpriseProjectId
hss:container:listStatefulSets	授予权限以查询Kubernetes有状态负载列表。	list	-	g:EnterpriseProjectId
hss:container:listDaemonSets	授予权限以查询Kubernetes守护进程列表。	list	-	g:EnterpriseProjectId
hss:container:listJobs	授予权限以查询kubernetes普通任务列表。	list	-	g:EnterpriseProjectId
hss:container:listCronJobs	授予权限以查询Kubernetes定时任务列表。	list	-	g:EnterpriseProjectId
hss:vulnerability:showVulAffectedStatics	授予权限以统计漏洞受影响服务器数量。	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulHandleTask	授予权限以查询漏洞处置任务列表。	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulHandleTaskDetail	授予权限以查询漏洞处置任务的详情列表。	list	-	g:EnterpriseProjectId
hss:container:isolateK8sContainer	授予权限以修改容器的运行状态。	write	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:container:getNetworkStatistics	授予权限以查询容器防火墙统计状态。	list	-	g:EnterpriseProjectId
hss:container:getClusters	授予权限以查询集群列表。	list	-	g:EnterpriseProjectId
hss:container:getClusterNetworkInfo	授予权限以查询集群网络信息。	read	-	g:EnterpriseProjectId
hss:container:getClusterPolicyList	授予权限以查询容器网络策略列表。	list	-	g:EnterpriseProjectId
hss:container:deletePolicy	授予权限以删除容器网络策略。	write	-	g:EnterpriseProjectId
hss:container:createPolicy	授予权限以创建容器网络策略。	write	-	g:EnterpriseProjectId
hss:container:updatePolicy	授予权限以更新容器网络策略。	write	-	g:EnterpriseProjectId
hss:container:syncClusterPolicyList	授予权限以同步容器网络策略。	read	-	g:EnterpriseProjectId
hss:container:syncClusterList	授予权限以同步集群命名空间信息。	read	-	g:EnterpriseProjectId
hss:container:getNamespaceList	授予权限以查询集群命名空间列表。	list	-	g:EnterpriseProjectId
hss:container:getNodeList	授予权限以查询集群节点列表。	list	-	g:EnterpriseProjectId
hss:container:syncClusterNodeList	授予权限以同步集群节点。	read	-	g:EnterpriseProjectId
hss:vulnerability:getVulScanTaskEstimatedTime	授予权限以查询漏洞扫描的预估时间。	read	-	g:EnterpriseProjectId
hss:antiransomware:addRansomwareProtectionPolicy	授予权限以添加勒索防护策略。	write	-	g:EnterpriseProjectId
hss:antiransomware:associateBackupPolicy	授予权限以将备份策略绑定存储库。	write	-	g:EnterpriseProjectId
hss:antiransomware:listBackupPolicy	授予权限以查询备份策略列表。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:antiransomware:associateProtectionPolicy	授予权限以切换勒索防护策略。	write	-	g:EnterpriseProjectId
hss:antiransomware:batchStartProtection	授予权限以开启勒索防护。	write	-	g:EnterpriseProjectId
hss:event:getEventAttCk	授予权限以查询ATT&CK攻击阶段统计列表。	list	event *	-
			-	g:EnterpriseProjectId
hss:event:downloadEventSourceFile	授予权限以下载告警源文件。	list	event *	-
			-	g:EnterpriseProjectId
hss:overview:showSecurityScore	授予权限以查询安全评分。	list	-	g:EnterpriseProjectId
hss:overview:listSecurityRisk	授予权限以查询安全风险列表。	list	-	g:EnterpriseProjectId
hss:overview:showQuotaHostStatistics	授予权限以查询主机配额统计信息。	list	-	g:EnterpriseProjectId
hss:overview:showAgentStatistics	授予权限以查询agent待升级，在线离线数量。	list	-	g:EnterpriseProjectId
hss:overview:showHotInformation	授予权限以查询热点资讯。	list	-	g:EnterpriseProjectId
hss:overview:showSecurityRisk	授予权限以查询安全风险信息。	list	-	g:EnterpriseProjectId
hss:overview:showProtectStatistics	授予权限以查询守护天数，病毒库更新时间，漏洞库更新时间，各模块累计次数。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:overview:showStatistics	授予权限以查询勒索病毒防治开启数量，应用防护开启数量，网页防篡改开启数量，双因子认证开启数量，支持双因子认证开启数量，隔离文件数量。	list	-	g:EnterpriseProjectId
hss:event:listEventHandleHistory	授予权限以查询历史事件处置列表。	list	event *	-
			-	g:EnterpriseProjectId
hss:image:listSwrImageRepository	授予权限以查询swr镜像仓库镜像列表。	list	-	g:EnterpriseProjectId
hss:image:batchScanSwrImage	授予权限以镜像仓库镜像批量扫描。	write	-	g:EnterpriseProjectId
hss:image:vulnerabilities	授予权限以查询镜像的漏洞信息。	list	-	g:EnterpriseProjectId
hss:image:listVulnerabilityCve	授予权限以漏洞对应cve信息。	list	-	g:EnterpriseProjectId
hss:image:listImageRiskConfigRules	授予权限以查询镜像指定安全配置项的检查项列表。	list	-	g:EnterpriseProjectId
hss:image:runImageSynchronize	授予权限以从SWR服务同步镜像列表。	write	-	g:EnterpriseProjectId
hss:event:listEventForensic	授予权限以查询事件取证信息。	list	event *	-
			-	g:EnterpriseProjectId
hss:event:listSimilarHandledEvents	授予权限以查询相似已处置的告警记录。	list	event *	-
			-	g:EnterpriseProjectId
hss:event:listSameEvent	授予权限以查询相同告警。	list	event *	-
			-	g:EnterpriseProjectId
hss:container:getPolicies	授予权限以查询策略列表。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:container:getPolicyDetail	授予权限以查询策略详情。	list	-	g:EnterpriseProjectId
hss:container:getOverview	授予权限以查询集群防护总览。	list	-	g:EnterpriseProjectId
hss:container:getProtectEvents	授予权限以查询集群防护事件。	list	-	g:EnterpriseProjectId
hss:container:getProtectClusters	授予权限以查询集群防护信息。	list	-	g:EnterpriseProjectId
hss:container:changeProtectStatus	授予权限以改变集群防护状态。	write	-	g:EnterpriseProjectId
hss:container:addWhiteImage	授予权限以加入镜像白名单。	write	-	g:EnterpriseProjectId
hss:container:listDefaultPolicy	授予权限以查询默认策略模板。	list	-	g:EnterpriseProjectId
hss:container:listProtectionItem	授予权限以查询防护范围。	list	-	g:EnterpriseProjectId
hss:vulnerability:getVulBackupStatistics	授予权限以查询漏洞处理对应主机的备份相关统计信息。	read	-	g:EnterpriseProjectId
hss:vulnerability:ListVulHostVaults	授予权限以查询漏洞处理对应的主机存储库的列表。	list	-	g:EnterpriseProjectId
hss:vulnerability:ListVulHostBackups	授予权限以查询可回滚的备份列表。	list	host *	g:EnterpriseProjectId
hss:vulnerability:RestoreVulHostBackup	授予权限以用备份进行回滚。	write	-	g:EnterpriseProjectId
hss:event:exportEvent	授予权限以导出事件告警。	write	event *	-
			-	g:EnterpriseProjectId
hss:event:queryExportTask	授予权限以查询导出事件告警任务。	read	event *	-
			-	g:EnterpriseProjectId
hss:event:downloadEvent	授予权限以下载事件告警。	read	event *	-
			-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:ars:createAppWhitelistPolicy	授予权限以创建应用进程白名单策略。	write	host *	-
			-	g:EnterpriseProjectId
hss:ars:listAppWhitelistPolicy	授予权限以查询应用进程白名单策略列表。	list	-	g:EnterpriseProjectId
hss:ars:changeAppWhitelistPolicy	授予权限以修改应用进程白名单策略。	write	host *	-
			-	g:EnterpriseProjectId
hss:ars:deleteAppWhitelistPolicy	授予权限以删除应用进程白名单策略。	write	-	g:EnterpriseProjectId
hss:ars:showAppWhitelistPolicy	授予权限以查询应用进程白名单策略信息。	list	-	g:EnterpriseProjectId
hss:ars:switchAppWhitelistPolicyHost	授予权限以修改应用进程白名单策略防护状态。	write	host *	-
			-	g:EnterpriseProjectId
hss:ars:addAppWhitelistPolicyHost	授予权限以添加主机到应用进程白名单策略。	write	host *	-
			-	g:EnterpriseProjectId
hss:ars:listAppWhitelistPolicyHost	授予权限以查询应用进程白名单策略的主机列表。	list	-	g:EnterpriseProjectId
hss:ars:deleteAppWhitelistPolicyHost	授予权限以删除应用进程白名单策略的主机。	write	host *	-
			-	g:EnterpriseProjectId
hss:ars:listAppWhitelistHostStatus	授予权限以查询应用进程白名单策略的可选服务器列表。	list	-	g:EnterpriseProjectId
hss:ars:listAppWhitelistPolicyProcess	授予权限以查询应用进程白名单策略的进程列表。	list	-	g:EnterpriseProjectId
hss:ars:changeAppWhitelistPolicyProcessStatus	授予权限以修改应用进程白名单策略的进程可信状态。	write	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:ars:addAppWhitelistPolicyProcess	授予权限以添加进程到应用进程白名单策略。	write	host *	-
			-	g:EnterpriseProjectId
hss:ars:listAppWhitelistPolicyProcessExtend	授予权限以查询应用进程白名单策略的进程扩展列表。	list	host *	-
			-	g:EnterpriseProjectId
hss:ars:exportAppWhitelistPolicyProcess	授予权限以导出应用进程白名单策略的进程列表。	list	host *	-
			-	g:EnterpriseProjectId
hss:ars:switchAppWhitelistPolicyLearnStatus	授予权限以修改应用进程白名单策略学习状态。	write	host *	-
			-	g:EnterpriseProjectId
hss:ars:showAppWhitelistAgentStatics	授予权限以查询不支持应用进程控制功能的旗舰版主机数量。	list	-	g:EnterpriseProjectId
hss:ars:listAppWhitelistEvent	授予权限以查询应用进程控制的可疑进程事件列表。	list	-	g:EnterpriseProjectId
hss:container:deleteSelfBuildK8sClusterDaemonsetInfo	授予权限以删除询自建集群daemonset。	write	-	g:EnterpriseProjectId
hss:container:saveSelfBuildK8sClusterDaemonsetInfo	授予权限以保存自建集群daemonset。	write	-	g:EnterpriseProjectId
hss:container:showSelfBuildK8sClusterDaemonsetInfo	授予权限以查询自建集群daemonset。	read	-	g:EnterpriseProjectId
hss:container:listSelfBuildK8sClusterInfo	授予权限以查询自建Kubernetes集群列表。	list	-	g:EnterpriseProjectId
hss:container:createDaemonset	授予权限以创建CCE集群daemonset。	write	-	g:EnterpriseProjectId
hss:vulnerability:listVulRepairCmds	授予权限以查询漏洞修复命令。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:vulnerability:listUrgentVulnerabilities	授予权限以查询应急漏洞列表。	list	-	g:EnterpriseProjectId
hss:antivirus:createAntivirusTask	授予权限以创建病毒查杀任务。	write	host *	-
			-	g:EnterpriseProjectId
hss:antivirus:listAntivirusTask	授予权限以查询病毒查杀任务列表。	list	-	g:EnterpriseProjectId
hss:antivirus:switchAntivirusTask	授予权限以取消病毒查杀任务。	write	host *	-
			-	g:EnterpriseProjectId
hss:antivirus:listAntivirusHost	授予权限以查询病毒查杀可选服务器列表。	list	-	g:EnterpriseProjectId
hss:antivirus:createAntivirusPolicy	授予权限以创建自定义查杀策略。	write	host *	-
			-	g:EnterpriseProjectId
hss:antivirus:listAntivirusPolicy	授予权限以查询自定义查杀策略列表。	list	-	g:EnterpriseProjectId
hss:antivirus:listAntivirusResult	授予权限以查询病毒查杀结果列表。	list	-	g:EnterpriseProjectId
hss:antivirus:operateAntivirusResult	授予权限以处置病毒查杀结果。	write	-	g:EnterpriseProjectId
hss:antivirus:exportAntivirusResult	授予权限以导出病毒查杀结果。	write	-	g:EnterpriseProjectId
hss:antivirus:showAntivirusStatistic	授予权限以查询病毒查杀统计信息。	list	-	g:EnterpriseProjectId
hss:image:showImageFullScanProgress	授予权限以查询镜像全量扫描进展。	list	-	g:EnterpriseProjectId
hss:host:changeHostIgnoreStatus	授予权限以忽略或取消忽略主机。	write	host *	-
			-	g:EnterpriseProjectId
hss:host:listIgnoreHosts	授予权限以查询已忽略主机。	list	host *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	g:EnterpriseProjectId
hss:image:batchExportBaselineTask	授予权限以导出镜像基线检查结果。	write	-	g:EnterpriseProjectId
hss:image:showImageSecurityReportStatistic	授予权限以查询镜像安全报告导出统计。	write	-	g:EnterpriseProjectId
hss:vulnerability:exportVuls	授予权限以创建漏洞导出任务。	write	-	g:EnterpriseProjectId
hss:exportTask:queryExportTask	授予权限以查询导出任务。	list	-	g:EnterpriseProjectId
hss:file:downloadExportedFile	授予权限以下载文件。	list	-	g:EnterpriseProjectId
hss:image:listGlobalVulnerabilities	授予权限以查询租户的漏洞信息。	list	-	g:EnterpriseProjectId
hss:image:listVulnerabilityImages	授予权限以查询单个漏洞影响的镜像仓库中的镜像信息。	list	-	g:EnterpriseProjectId
hss:setting:getPluginInstallScript	授予权限以查询服务器安装的插件信息。	list	-	g:EnterpriseProjectId
hss:setting:getPluginList	授予权限以查询插件安装指南信息。	list	-	g:EnterpriseProjectId
hss:setting:getAutoOpenQuotaStatus	授予权限以查询自动绑定配额开关状态。	read	-	g:EnterpriseProjectId
hss:setting:changeAutoOpenQuotaStatus	授予权限以修改自动绑定配额开关状态。	write	-	g:EnterpriseProjectId
hss:image:batchExportSWRVulTask	授予权限以导出swr镜像漏洞结果。	write	-	g:EnterpriseProjectId
hss:image:batchExportLocalVulTask	授予权限以导出本地镜像漏洞结果。	write	-	g:EnterpriseProjectId
hss:vulnerability:exportVulReport	授予权限以导出html格式的漏洞报告。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
hss:vulnerability:getVulReportData	授予权限以获取pdf漏洞报告的数据。	list	-	g:EnterpriseProjectId
hss:setting:getAgentAutoUpgradeStatus	授予权限以查询agent自动升级开关状态。	read	-	g:EnterpriseProjectId
hss:setting:changeAgentAutoUpgradeStatus	授予权限以修改agent自动升级开关状态。	write	-	g:EnterpriseProjectId
hss:quota:showProductdataOfferingInfos	授予权限以查询商品信息。	list	-	g:EnterpriseProjectId
hss:image:listLocalImageAppInfo	授予权限以查询本地镜像软件列表。	list	-	g:EnterpriseProjectId
hss:image:listLocalImageAppVulnerabilities	授予权限以查询本地镜像单个软件漏洞列表。	list	-	g:EnterpriseProjectId

HSS的API通常对应着一个或多个授权项。表5-75展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-75 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v5/{project_id}/host-management/groups	hss:host:addHostsGroup	eps:enterpriseProjects:list
PUT /v5/{project_id}/event/blocked-ip	hss:event:changeBlockedIp	eps:enterpriseProjects:list
GET /v5/{project_id}/backup/policy	hss:antiransomware:getRansomwareHSSBackupPolicyInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/container/nodes	hss:container:listContainerNodes	eps:enterpriseProjects:list

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/host-management/groups	hss:host:listHostGroups	eps:enterpriseProjects:list
GET /v5/{project_id}/policy/groups	hss:policy:listPolicyGroup	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/ports/detail	hss:asset:listPortHost	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/processes/detail	hss:asset:listProcessesHost	eps:enterpriseProjects:list
GET /v5/{project_id}/ransomware/protection/policy	hss:antiransomware:listRansomwareProtectionPolicy	eps:enterpriseProjects:list
GET /v5/{project_id}/ransomware/server	hss:antiransomware:listRansomwareProtectionServer	eps:enterpriseProjects:list
GET /v5/{project_id}/webtamper/static/protect-history	hss:wtp:listWtpHostProtectHistoryInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/webtamper/rasp/protect-history	hss:wtp:listWtpHostRaspProtectHistoryInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/webtamper/hosts	hss:wtp:listWtpProtectHost	• eps:enterpriseProjects:list • vpc:ports:list
POST /v5/{project_id}/webtamper/static/status	hss:wtp:setWtpProtectionStatusInfo	eps:enterpriseProjects:list
POST /v5/{project_id}/webtamper/rasp/status	hss:wtp:setWtpProtectSwitch	eps:enterpriseProjects:list
POST /v5/{project_id}/ransomware/protection/open	hss:antiransomware:startRansomwareProtection	eps:enterpriseProjects:list

API	对应的授权项	依赖的授权项
POST /v5/{project_id}/ransomware/protection/close	hss:antiransomware:stopRansomwareProtection	eps:enterpriseProjects:list
PUT /v5/{project_id}/backup/policy	hss:antiransomware:updateRansomwareBackupPolicyInfo	eps:enterpriseProjects:list
PUT /v5/{project_id}/ransomware/protection/policy	hss:antiransomware:updateRansomwareProtectionPolicy	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/statistics	hss:asset:getAssetStatistic	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/app/change-history	hss:asset:listAppChangeHistories	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/apps	hss:asset:listApps	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/app/statistics	hss:asset:listAppStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/auto-launch/change-history	hss:asset:listAutoLaunchChangeHistories	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/auto-launchs	hss:asset:listAutoLaunchs	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/auto-launch/statistics	hss:asset:listAutoLaunchStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/midwares/detail	hss:asset:listJarPackageHostInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/midwares	hss:asset:listJarPackageStatistics	eps:enterpriseProjects:list

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/asset/ports	hss:asset:listPorts	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/port/statistics	hss:asset:listPortStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/process/statistics	hss:asset:listProcessStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/user/change-history	hss:asset:listUserChangeHistories	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/users	hss:asset:listUsers	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/user/statistics	hss:asset:listUserStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/check-rule/detail	hss:baseline:getCheckRuleDetail	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/risk-config/{check_name}/detail	hss:baseline:getRiskConfigDetail	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/password-complexity	hss:baseline:listPasswordComplexity	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/risk-config/{check_name}/check-rules	hss:baseline:listRiskConfigCheckRules	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/risk-config/{check_name}/hosts	hss:baseline:listRiskConfigHosts	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/risk-configs	hss:baseline:listRiskConfigs	eps:enterpriseProjects:list

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/baseline/weak-password-users	hss:baseline:listWeakPasswordUsers	eps:enterpriseProjects:list
POST /v5/{project_id}/event/operate	hss:event:changeEvent	eps:enterpriseProjects:list
PUT /v5/{project_id}/event/isolated-file	hss:event:changeIsolatedFile	eps:enterpriseProjects:list
GET /v5/{project_id}/event/white-list/alarm	hss:event:listAlarmWhiteList	eps:enterpriseProjects:list
GET /v5/{project_id}/event/blocked-ip	hss:event:listBlockedIp	eps:enterpriseProjects:list
GET /v5/{project_id}/event/isolated-file	hss:event:listIsolatedFile	eps:enterpriseProjects:list
GET /v5/{project_id}/event/events	hss:event:listSecurityEvents	eps:enterpriseProjects:list
PUT /v5/{project_id}/host-management/groups	hss:host:changeHostsGroup	eps:enterpriseProjects:list
DELETE /v5/{project_id}/host-management/groups	hss:host:deleteHostsGroup	eps:enterpriseProjects:list
GET /v5/{project_id}/host-management/hosts	hss:host:listHostStatus	• eps:enterpriseProjects:list • vpc:ports:list • eip:publicIps:list
POST /v5/{project_id}/host-management/protection	hss:host:switchHostsProtectStatus	eps:enterpriseProjects:list
POST /v5/{project_id}/policy/deploy	hss:policy:associatePolicyGroup	eps:enterpriseProjects:list

API	对应的授权项	依赖的授权项
POST /v5/{project_id}/{resource_type}/{resource_id}/tags/create	hss:quota:batchCreateTags	eps:enterpriseProjects:list
DELETE /v5/{project_id}/{resource_type}/{resource_id}/tags/{key}	hss:quota:deleteResourceInstanceTag	eps:enterpriseProjects:list
GET /v5/{project_id}/billing/quotas	hss:quota:getResourceQuotas	eps:enterpriseProjects:list
GET /v5/{project_id}/billing/quotas-detail	hss:quota:listQuotasDetail	eps:enterpriseProjects:list
PUT /v5/{project_id}/vulnerability/status	hss:vulnerability:changeVulStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/vulnerability/host/{host_id}	hss:vulnerability:listHostVuls	eps:enterpriseProjects:list
GET /v5/{project_id}/vulnerability/hosts	hss:vulnerability:listVulHosts	eps:enterpriseProjects:list
GET /v5/{project_id}/vulnerability/vulnerabilities	hss:vulnerability:listVulnerabilities	eps:enterpriseProjects:list
GET /v5/{project_id}/vulnerability/scan-policy	hss:vulnerability:getVulScanPolicy	-
PUT /v5/{project_id}/vulnerability/scan-policy	hss:vulnerability:changeVulScanPolicy	-
GET /v5/{project_id}/vulnerability/scan-tasks	hss:vulnerability:listVulScanTask	-

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/vulnerability/scan-task/{task_id}/hosts	hss:vulnerability:listVulScanTaskHost	-
GET /v5/{project_id}/vulnerability/statistics	hss:vulnerability:listHostVulStatistics	-
GET /v5/{project_id}/image/baseline/risk-configs	hss:image:listImageRiskConfigs	-
GET /v5/{project_id}/image/baseline/check-rule/detail	hss:image:getImageCheckRuleDetail	-
GET /v5/{project_id}/image/swr-repository	hss:image:listSwrImageRepository	-
POST /v5/{project_id}/image/batch-scan	hss:image:batchScanSwrImage	-
GET /v5/{project_id}/image/{image_id}/vulnerabilities	hss:image:vulnerabilities	-
GET /v5/{project_id}/image/vulnerability/{vul_id}/cve	hss:image:listVulnerabilityCve	-
GET /v5/{project_id}/image/baseline/risk-configs/{check_name}/rules	hss:image:listImageRiskConfigRules	-
POST /v5/{project_id}/image/synchronize	hss:image:runImageSynchronize	-
GET /v5/{project_id}/product/productdata/offering-infos	hss:quota:showProductdataOfferingInfos	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-76中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

HSS定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-76 HSS 支持的资源类型

资源类型	URN
host	hss:<region>:<account-id>:host:<host-id>
event	hss:<region>:<account-id>:event:<event-id>
baseline	hss:<region>:<account-id>:baseline:<type>/<check_rule_id>
policy	hss:<region>:<account-id>:policy:<resource-type>/<type-id>

条件（Condition）

HSS服务不支持在SCP中的条件键中配置服务级的条件键。

HSS可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.7.3 安全云脑 SecMaster

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。

- 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

关于SecMaster定义的资源类型的详细信息请参见**资源类型（Resource）**。

- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

关于SecMaster定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下SecMaster的相关操作。

表 5-77 SecMaster 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
secmaster:playbook:get	授予权限获取剧本详情。	read	playbook *	-
secmaster:playbook:create	授予权限创建剧本。	write	playbook *	-
secmaster:playbook:delete	授予权限删除剧本。	write	playbook *	-
secmaster:playbook:update	授予权限更新剧本。	write	playbook *	-
secmaster:playbook:list	授予权限获取剧本列表。	list	playbook *	-
secmaster:playbook:getStatistics	授予权限获取剧本统计数据。	read	playbook *	-
secmaster:playbook:getMonitor	授予权限获取剧本运行监控数据。	read	playbook *	-
secmaster:playbook:copyVersion	授予权限克隆剧本版本。	write	playbook *	-
secmaster:playbook:approve	授予权限审核剧本。	write	playbook *	-
secmaster:playbook:listApproves	授予权限查询审核列表。	list	playbook *	-
secmaster:playbook:listInstances	授予权限查询实例列表。	list	playbook *	-
secmaster:playbook:getInstanceAuditlog	授予权限查询实例审计日志列表。	list	playbook *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
secmaster:playbook:createVersion	授予权限创建剧本版本。	write	playbook *	-
secmaster:playbook:createVersionRule	授予权限创建剧本版本规则。	write	playbook *	-
secmaster:playbook:createVersionAction	授予权限创建剧本版本动作。	write	playbook *	-
secmaster:playbook:getVersion	授予权限获取剧本版本。	read	playbook *	-
secmaster:playbook:getVersionRule	授予权限获取剧本版本规则。	read	playbook *	-
secmaster:playbook:deleteVersion	授予权限删除剧本版本。	write	playbook *	-
secmaster:playbook:deleteVersionRule	授予权限删除剧本版本规则。	write	playbook *	-
secmaster:playbook:deleteVersionAction	授予权限删除剧本版本动作。	write	playbook *	-
secmaster:playbook:updateVersion	授予权限更新剧本版本。	write	playbook *	-
secmaster:playbook:updateVersionRule	授予权限更新剧本版本规则。	write	playbook *	-
secmaster:playbook:updateVersionAction	授予权限更新剧本版本动作。	write	playbook *	-
secmaster:playbook:listVersions	授予权限获取剧本版本列表。	list	playbook *	-
secmaster:playbook:listVersionActions	授予权限获取剧本版本动作列表。	list	playbook *	-
secmaster:playbook:getInstance	授予权限查询实例详情。	read	playbook *	-
secmaster:playbook:getInstanceTopology	授予权限查询实例拓扑详情。	read	playbook *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
secmaster:playbook:operateInstance	授予权限操作剧本实例。	write	playbook *	-
secmaster:workflow:list	授予权限查询流程列表。	list	workflow *	-
secmaster:workflow:get	授予权限获取流程的详情。	read	workflow *	-
secmaster:workflow:delete	授予权限删除流程。	write	workflow *	-
secmaster:workflow:create	授予权限创建流程。	write	workflow *	-
secmaster:workflow:update	授予权限更新流程。	write	workflow *	-
secmaster:workflow:listVersions	授予权限获取流程版本的列表。	list	workflow *	-
secmaster:workflow:getVersion	授予权限获取流程的版本详情。	read	workflow *	-
secmaster:workflow:deleteVersion	授予权限删除流程的版本。	write	workflow *	-
secmaster:workflow:createVersion	授予权限创建流程版本。	write	workflow *	-
secmaster:workflow:updateVersion	授予权限更新流程的版本。	write	workflow *	-
secmaster:workflow:approveVersion	授予权限审核流程版本。	write	workflow *	-
secmaster:workflow:validate	授予权限校验流程的版本。	write	workflow *	-
secmaster:workflow:simulate	授予权限更新流程版本调试结果。	write	workflow *	-
secmaster:workflow:getInstance	授予权限流程实例拓扑图。	read	workflow *	-
secmaster:workflow:operateInstance	授予权限更新或创建流程实例。	write	workflow *	-
secmaster:connection:list	授予权限查询资产连接列表。	list	connection *	-
secmaster:connection:create	授予权限创建资产连接。	write	connection *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
secmaster:connection:get	授予权限获取资产连接详情。	read	connection *	-
secmaster:connection:delete	授予权限删除资产连接。	write	connection *	-
secmaster:connection:update	授予权限更新资产连接。	write	connection *	-
secmaster:workspace:list	授予权限查询工作空间列表。	list	workspace *	-
secmaster:workspace:create	授予权限创建工作空间。	write	workspace *	-
secmaster:workspace:update	授予权限更新工作空间。	write	workspace *	-
secmaster:workspace:get	授予权限获取工作空间详情。	read	workspace *	-
secmaster:workspace:delete	授予权限删除工作空间。	write	workspace *	-
secmaster:task:list	授予权限查询待办列表。	list	task *	-
secmaster:task:create	授予权限创建待办。	write	task *	-
secmaster:task:update	授予权限更新待办。	write	task *	-
secmaster:task:get	授予权限获取待办详情。	read	task *	-
secmaster:indicator:get	授予权限获取情报详情。	read	indicator *	-
secmaster:indicator:create	授予权限创建情报。	write	indicator *	-
secmaster:indicator:update	授予权限更新情报。	write	indicator *	-
secmaster:indicator:delete	授予权限删除情报。	write	indicator *	-
secmaster:indicator:list	授予权限查询情报列表。	read	indicator *	-
secmaster:indicator:listTypes	授予权限查询情报类型列表。	list	indicator *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
secmaster:indicator:bindLayout	授予权限绑定情报类型与布局关联。	write	indicator *	-
secmaster:alert:get	授予权限获取告警详情。	read	alert *	-
secmaster:alert:create	授予权限创建告警。	write	alert *	-
secmaster:alert:update	授予权限更新告警。	write	alert *	-
secmaster:alert:list	授予权限搜索告警列表。	list	alert *	-
secmaster:alert:delete	授予权限删除告警。	write	alert *	-
secmaster:alert:batchOrders	授予权限告警转事件。	list	alert *	-
secmaster:alert:listTypes	授予权限查询告警类型列表。	list	alert *	-
secmaster:alert:listCategories	授予权限查询告警类别列表。	list	alert *	-
secmaster:alert:createType	授予权限创建告警类型。	write	alert *	-
secmaster:alert:updateType	授予权限修改告警类型。	write	alert *	-
secmaster:alert:deleteType	授予权限删除告警类型。	write	alert *	-
secmaster:alert:enableType	授予权限启用/禁用告警类型。	write	alert *	-
secmaster:alert:bindLayout	授予权限绑定告警类型与布局关联。	write	alert *	-
secmaster:incident:get	授予权限获取事件详情。	read	incident *	-
secmaster:incident:create	授予权限创建事件。	write	incident *	-
secmaster:incident:update	授予权限更新事件。	write	incident *	-
secmaster:incident:list	授予权限搜索事件列表。	list	incident *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
secmaster:incident:listTypes	授予权限获取事件的类型列表。	list	incident *	-
secmaster:incident:delete	授予权限删除事件。	write	incident *	-
secmaster:incident:listCategories	授予权限查询事件类别列表。	list	incident *	-
secmaster:incident:createType	授予权限创建事件类型。	write	incident *	-
secmaster:incident:updateType	授予权限修改事件类型。	write	incident *	-
secmaster:incident:deleteType	授予权限删除事件类型。	write	incident *	-
secmaster:incident:enableType	授予权限启用/禁用事件类型。	write	incident *	-
secmaster:incident:bindLayout	授予权限绑定事件类型与布局的关联。	write	incident *	-
secmaster:dataobject:createRelation	授予权限创建对象关系。	write	dataobject *	-
secmaster:dataobject:deleteRelation	授予权限删除对象关系。	write	dataobject *	-
secmaster:dataobject:listRelation	授予权限搜索对象关系列表。	list	dataobject *	-
secmaster:vulnerability:listGroup	授予权限查询漏洞组列表。	list	vulnerability *	-
secmaster:vulnerability:getGroup	授予权限获取漏洞组详情。	read	vulnerability *	-
secmaster:vulnerability:exportGroup	授予权限导出漏洞组列表。	list	vulnerability *	-
secmaster:vulnerability:listType	授予权限查询漏洞类型列表。	list	vulnerability *	-
secmaster:vulnerability:bindLayout	授予权限绑定漏洞类型与布局关联。	write	vulnerability *	-
secmaster:vulnerability:createType	授予权限创建漏洞类型。	write	vulnerability *	-
secmaster:vulnerability:updateType	授予权限修改漏洞类型。	write	vulnerability *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
secmaster:vulnerability:deleteType	授予权限删除漏洞类型。	write	vulnerability *	-
secmaster:vulnerability:enableType	授予权限启用/禁用漏洞类型。	write	vulnerability *	-
secmaster:subscription:deletePostPaidOrder	授予权限删除按需订单。	write	-	-
secmaster:subscription:createPostPaidOrder	授予权限创建按需订单。	write	-	-
secmaster:subscription:createPrePaidOrder	授予权限创建包周期订单。	write	-	-
secmaster:subscription:getVersion	授予权限查看订购版本。	read	-	-
secmaster:metric:getResult	授予权限查看指标结果。	read	metric *	-
secmaster:metric:listResults	授予权限列出指标结果。	list	metric *	-
secmaster:metric:listHits	授予权限列出指标Hits结果。	list	metric *	-
secmaster:agency:get	授予权限查看委托。	read	-	-
secmaster:agency:create	授予权限创建委托。	write	-	-
secmaster:resource:getStatistics	授予权限查看资源统计。	read	resource *	-
secmaster:resource:list	授予权限列出资源。	list	resource *	-
secmaster:resource:import	授予权限导入资源。	write	resource *	-
secmaster:resource:getTemplate	授予权限获取资源导入模板。	read	resource *	-
secmaster:report:list	授予权限列出报告。	list	report *	-
secmaster:report:get	授予权限查看报告。	read	report *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
secmaster:report:create	授予权限创建报告。	write	report *	-
secmaster:report:update	授予权限更新报告。	write	report *	-
secmaster:report:delete	授予权限删除报告。	write	report *	-
secmaster:emergencyVulnerability:updateReadStatus	授予权限设置应急漏洞读取状态。	write	emergencyVulnerability *	-
secmaster:emergencyVulnerability:list	授予权限列出应急漏洞。	list	emergencyVulnerability *	-
secmaster:emergencyVulnerability:export	授予权限导出应急漏洞。	read	emergencyVulnerability *	-
secmaster:dataspace:list	授予权限查询数据空间列表。	list	dataspace *	-
secmaster:dataspace:create	授予权限创建数据空间。	write	dataspace *	-
secmaster:dataspace:get	授予权限查询数据空间详情。	read	dataspace *	-
secmaster:dataspace:update	授予权限更新数据空间。	write	dataspace *	-
secmaster:dataspace:delete	授予权限删除数据空间。	write	dataspace *	-
secmaster:pipe:list	授予权限查询数据管道列表。	list	pipe *	-
secmaster:pipe:create	授予权限创建数据管道。	write	pipe *	-
secmaster:pipe:get	授予权限查询数据管道详情。	read	pipe *	-
secmaster:pipe:update	授予权限更新数据管道。	write	pipe *	-
secmaster:pipe:delete	授予权限删除数据管道。	write	pipe *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
secmaster:pipe:getIndex	授予权限查询数据管道索引。	read	pipe *	-
secmaster:pipe:updateIndex	授予权限更新数据管道索引。	write	pipe *	-
secmaster:pipe:getConsumption	授予权限查询数据管道消费。	read	pipe *	-
secmaster:pipe:createConsumption	授予权限创建数据管道消费。	write	pipe *	-
secmaster:pipe:deleteConsumption	授予权限删除数据管道消费。	write	pipe *	-
secmaster:search:listLogs	授予权限查询数据。	list	workspace *	-
secmaster:search:listHistograms	授予权限查询数据分布直方图。	list	workspace *	-
secmaster:search:createAnalysis	授予权限执行分析。	write	workspace *	-
secmaster:searchCondition:list	授予权限查询检索条件列表。	list	searchCondition *	-
secmaster:searchCondition:create	授予权限创建检索条件。	write	searchCondition *	-
secmaster:searchCondition:get	授予权限查询检索条件详情。	read	searchCondition *	-
secmaster:searchCondition:update	授予权限更新检索条件。	write	searchCondition *	-
secmaster:searchCondition:delete	授予权限删除检索条件。	write	searchCondition *	-
secmaster:alertRule:list	授予权限查询告警模型。	list	alertRule *	-
secmaster:alertRule:create	授予权限创建告警模型。	write	alertRule *	-
secmaster:alertRule:get	授予权限查询告警模型详情。	read	alertRule *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
secmaster:alertRule:update	授予权限修改告警模型。	write	alertRule *	-
secmaster:alertRule:delete	授予权限删除告警模型。	write	alertRule *	-
secmaster:alertRule:enable	授予权限启用告警模型。	write	alertRule *	-
secmaster:alertRule:disable	授予权限停用告警模型。	write	alertRule *	-
secmaster:alertRule:listMetrics	授予权限查询告警模型总览。	list	alertRule *	-
secmaster:alertRule:createSimulation	授予权限模拟告警模型。	write	alertRule *	-
secmaster:alertRuleTemplate:list	授予权限查询告警模板。	list	alertRuleTemplate *	-
secmaster:alertRuleTemplate:get	授予权限查询告警模板详情。	read	alertRuleTemplate *	-
secmaster:alertRuleTemplate:listMetrics	授予权限查询告警模板总览。	list	alertRuleTemplate *	-
secmaster:dataclass:create	授予权限创建数据类。	write	dataclass *	-
secmaster:dataclass:update	授予权限更新数据类。	write	dataclass *	-
secmaster:dataclass:delete	授予权限删除数据类。	write	dataclass *	-
secmaster:dataclass:get	授予权限获取数据类详情。	read	dataclass *	-
secmaster:dataclass:list	授予权限查询数据类列表。	list	dataclass *	-
secmaster:dataclass:createField	授予权限创建字段。	write	dataclass *	-
secmaster:dataclass:updateField	授予权限更新字段。	write	dataclass *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
secmaster:dataclass:deleteField	授予权限删除字段。	write	dataclass *	-
secmaster:dataclass:getField	授予权限获取字段详情。	read	dataclass *	-
secmaster:dataclass:listFields	授予权限查询字段列表。	list	dataclass *	-
secmaster:dataclass:getType	授予权限获取类型详情。	read	dataclass *	-
secmaster:dataclass:listTypes	授予权限查询类型列表。	list	dataclass *	-
secmaster:mapping:update	授予权限更新分类映射状态。	write	mapping *	-
secmaster:mapping:list	授予权限搜索分类映射列表。	list	mapping *	-
secmaster:mapping:getDatasource	授予权限获取分类映射数据源。	read	mapping *	-
secmaster:mapping:listFunctions	授予权限获取分类映射函数。	list	mapping *	-
secmaster:mapping:delete	授予权限删除分类映射。	write	mapping *	-
secmaster:mapping:copy	授予权限复制分类映射。	write	mapping *	-
secmaster:mapping:createClassifier	授予权限创建分类。	write	mapping *	-
secmaster:mapping:updateClassifier	授予权限更新分类。	write	mapping *	-
secmaster:mapping:getClassifier	授予权限获取分类信息。	read	mapping *	-
secmaster:mapping:deleteClassifier	授予权限删除分类。	write	mapping *	-
secmaster:mapping:createMapper	授予权限创建映射。	write	mapping *	-
secmaster:mapping:updateMapper	授予权限更新映射。	write	mapping *	-
secmaster:mapping:listMappers	授予权限查询映射列表。	list	mapping *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
secmaster:mapping:getMapper	授予权限获取映射信息。	read	mapping *	-
secmaster:mapping:deleteMapper	授予权限删除映射。	write	mapping *	-
secmaster:layout:listBusinessTypes	授予权限获取布局类型列表。	list	layout *	-
secmaster:layout:list	授予权限查询布局列表。	list	layout *	-
secmaster:layout:create	授予权限创建布局。	write	layout *	-
secmaster:layout:delete	授予权限删除布局。	write	layout *	-
secmaster:layout:update	授予权限更新布局。	write	layout *	-
secmaster:layout:get	授予权限查询布局。	read	layout *	-
secmaster:layout:createTemplate	授予权限另存为模板。	write	layout *	-
secmaster:layout:createField	授予权限创建布局字段。	write	layout *	-
secmaster:layout:listFields	授予权限获取布局字段列表。	list	layout *	-
secmaster:layout:getField	授予权限获取布局字段详情。	read	layout *	-
secmaster:layout:updateFiled	授予权限更新布局字段。	write	layout *	-
secmaster:layout:deleteField	授予权限删除布局字段。	write	layout *	-
secmaster:layout:listWizards	授予权限获取页面。	list	layout *	-
secmaster:layout:createWizard	授予权限创建页面。	write	layout *	-
secmaster:layout:getWizard	授予权限获取页面详情。	read	layout *	-
secmaster:layout:deleteWizard	授予权限删除页面。	write	layout *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
secmaster:layout:updateWizard	授予权限更新页面。	write	layout *	-
secmaster:catalogue:list	授予权限目录列表查询。	list	catalogue *	-
secmaster:catalogue:update	授予权限更新目录。	write	catalogue *	-
secmaster:playbook:export	授予权限导出剧本。	read	playbook *	-
secmaster:playbook:import	授予权限导入剧本。	write	playbook *	-
secmaster:indicator:downloadTemplate	授予权限下载指标模板。	read	indicator *	-
secmaster:indicator:export	授予权限导出指标。	read	indicator *	-
secmaster:indicator:import	授予权限导入指标。	write	indicator *	-
secmaster:table:list	授予权限查询表。	list	table *	-
secmaster:table:create	授予权限创建表。	write	table *	-
secmaster:table:get	授予权限查询表详情。	read	table *	-
secmaster:table:update	授予权限修改表。	write	table *	-
secmaster:table:delete	授予权限删除表。	write	table *	-
secmaster:table:createLock	授予权限锁止表。	write	table *	-
secmaster:table:deleteLock	授予权限解锁表。	write	table *	-
secmaster:table:listMetrics	授予权限查询表总览。	list	table *	-
secmaster:table:updateSchema	授予权限设计表。	write	table *	-

SecMaster的API通常对应着一个或多个授权项。表5-78展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-78 API 与操作项的关系

API	对应的操作项	依赖的操作项
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}	secmaster:playbook:get	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks	secmaster:playbook:create	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}	secmaster:playbook:delete	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}	secmaster:playbook:update	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks	secmaster:playbook:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/statistics	secmaster:playbook:getStatistics	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}/monitor	secmaster:playbook:getMonitor	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/clone	secmaster:playbook:copyVersion	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/approve	secmaster:playbook:approve	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/approval	secmaster:playbook:listApproves	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances	secmaster:playbook:listInstances	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/auditlogs	secmaster:playbook:getInstanceAuditlog	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions	secmaster:playbook:createVersion	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/rules	secmaster:playbook:createVersionRule	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/actions	secmaster:playbook:createVersionAction	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}	secmaster:playbook:getVersion	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/rules/{rule_id}	secmaster:playbook:getVersionRule	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}	secmaster:playbook:deleteVersion	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/rules/{rule_id}	secmaster:playbook:deleteVersionRule	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/actions/{action_id}	secmaster:playbook:deleteVersionAction	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}	secmaster:playbook:updateVersion	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/rules/{rule_id}	secmaster:playbook:updateVersionRule	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/actions/{action_id}	secmaster:playbook:updateVersionAction	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}/versions	secmaster:playbook:listVersions	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/actions	secmaster:playbook:listVersionActions	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}	secmaster:playbook:getInstance	-

API	对应的操作项	依赖的操作项
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}/topology	secmaster:playbook:getInstanceTopology	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}/operation	secmaster:playbook:operateInstance	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows	secmaster:workflow:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}	secmaster:workflow:get	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}	secmaster:workflow:delete	-
GET /v1/{project_id}/workspacesPOST /v1/{project_id}/workspaces/{workspace_id}/soc/workflows	secmaster:workflow:create	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}	secmaster:workflow:update	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions	secmaster:workflow:listVersions	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions/{version_id}	secmaster:workflow:getVersion	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions/{version_id}	secmaster:workflow:deleteVersion	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions	secmaster:workflow:createVersion	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions/{version_id}	secmaster:workflow:updateVersion	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions/{version_id}/approval	secmaster:workflow:approveVersion	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/validation	secmaster:workflow:validate	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions/{version_id}/debug/result	secmaster:workflow:simulate	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/instances/{instance_id}/topology	secmaster:workflow:getInstance	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/instances	secmaster:workflow:operateInstance	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/assetcredentials	secmaster:connection:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/assetcredentials	secmaster:connection:create	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/assetcredentials/{asset_id}	secmaster:connection:get	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/assetcredentials/{asset_id}	secmaster:connection:delete	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/assetcredentials/{asset_id}	secmaster:connection:update	-
GET /v1/{project_id}/workspaces	secmaster:workspace:list	-
POST /v1/{project_id}/workspaces	secmaster:workspace:create	-
PUT /v1/{project_id}/workspaces/{workspace_id}	secmaster:workspace:update	-
GET /v1/{project_id}/workspaces/v1/{project_id}/workspaces/{workspace_id}	secmaster:workspace:get	-
DELETE /v1/{project_id}/workspaces/{workspace_id}	secmaster:workspace:delete	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/tasks	secmaster:task:list	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/workspaces/{workspace_id}/soc/tasks	secmaster:task:create	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/tasks/{task_id}	secmaster:task:update	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/tasks/{task_id}	secmaster:task:get	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/{indicator_id}	secmaster:indicator:get	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators	secmaster:indicator:create	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/{indicator_id}	secmaster:indicator:update	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/{indicator_id}	secmaster:indicator:delete	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/search	secmaster:indicator:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/types	secmaster:indicator:listTypes	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/types/layout	secmaster:indicator:bindLayout	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/{alert_id}	secmaster:alert:get	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts	secmaster:alert:create	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/{alert_id}	secmaster:alert:update	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/search	secmaster:alert:list	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/alerts	secmaster:alert:delete	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/batch-order	secmaster:alert:batchOrders	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types	secmaster:alert:listTypes	-

API	对应的操作项	依赖的操作项
GET /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types/category	secmaster:alert:listCategories	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types	secmaster:alert:createType	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types/{dataclass_type_id}	secmaster:alert:updateType	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types	secmaster:alert:deleteType	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types/enable	secmaster:alert:enableType	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types/layout	secmaster:alert:bindLayout	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/{incident_id}	secmaster:incident:get	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents	secmaster:incident:create	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/{incident_id}	secmaster:incident:update	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/search	secmaster:incident:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types	secmaster:incident:listTypes	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/incidents	secmaster:incident:delete	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types/category	secmaster:incident:listCategories	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types	secmaster:incident:createType	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types/{dataclass_type_id}	secmaster:incident:updateType	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types	secmaster:incident:deleteType	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/incidents/enable	secmaster:incident:enableType	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types/layout	secmaster:incident:bindLayout	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}	secmaster:dataobject:createRelation	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}	secmaster:dataobject:deleteRelation	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}/search	secmaster:dataobject:listRelation	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerability/search	secmaster:vulnerability:listGroup	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerability/{vul_id}	secmaster:vulnerability:getGroup	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerability/export	secmaster:vulnerability:exportGroup	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types	secmaster:vulnerability:listType	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types/layout	secmaster:vulnerability:bindLayout	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types	secmaster:vulnerability:createType	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types/{dataclass_type_id}	secmaster:vulnerability:updateType	-

API	对应的操作项	依赖的操作项
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types	secmaster:vulnerability:deleteType	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types/enable	secmaster:vulnerability:enableType	-
DELETE /v1/{project_id}/subscriptions/orders	secmaster:subscription:deletePostPaidOrder	-
POST /v1/{project_id}/subscriptions/orders	secmaster:subscription:createPostPaidOrder	-
POST /v1/{project_id}/subscriptions/orders/{order_id}	secmaster:subscription:createPrePaidOrder	-
GET /v1/{project_id}/subscriptions/version	secmaster:subscription:getVersion	-
GET /v1/{project_id}/workspaces/{workspace_id}/sa/metrics/{metric_id}/result	secmaster:metric:getResult	-
POST /v1/{project_id}/workspaces/{workspace_id}/sa/metrics/results	secmaster:metric:listResults	-
POST /v1/{project_id}/workspaces/{workspace_id}/sa/metrics/hits	secmaster:metric:listHits	-
GET /v1/{project_id}/agency	secmaster:agency:get	-
POST /v1/{project_id}/agency	secmaster:agency:create	-
GET /v1/{project_id}/workspaces/{workspace_id}/resource-statistics	secmaster:resource:getStatistics	-
GET /v1/{project_id}/workspaces/{workspace_id}/resources	secmaster:resource:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/sa/resources/import	secmaster:resource:import	-
GET /v1/{project_id}/workspaces/{workspace_id}/sa/resource/template	secmaster:resource:getTemplate	-
GET /v1/{project_id}/workspaces/{workspace_id}/sa/reports	secmaster:report:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/sa/reports/{report_id}	secmaster:report:get	-
POST /v1/{project_id}/workspaces/{workspace_id}/sa/reports	secmaster:report:create	-

API	对应的操作项	依赖的操作项
PUT /v1/{project_id}/workspaces/{workspace_id}/sa/reports/{report_id}	secmaster:report:update	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/sa/reports/{report_id}	secmaster:report:delete	-
POST /v1/{project_id}/workspaces/{workspace_id}/sa/vulnerability/read-status	secmaster:emergencyVulnerability:updateReadStatus	-
GET /v1/{project_id}/workspaces/{workspace_id}/sa/vulnerability/list	secmaster:emergencyVulnerability:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/sa/vulnerability/export	secmaster:emergencyVulnerability:export	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces	secmaster:dataspace:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces	secmaster:dataspace:create	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces/{dataspace_id}	secmaster:dataspace:get	-
PUT /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces/{dataspace_id}	secmaster:dataspace:update	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces/{dataspace_id}	secmaster:dataspace:delete	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/pipes	secmaster:pipe:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/pipes	secmaster:pipe:create	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}	secmaster:pipe:get	-
PUT /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}	secmaster:pipe:update	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}	secmaster:pipe:delete	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}/index	secmaster:pipe:getIndex	-

API	对应的操作项	依赖的操作项
PUT /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}/index	secmaster:pipe:updateIndex	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}/consumption	secmaster:pipe:getConsumption	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}/consumption	secmaster:pipe:createConsumption	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}/consumption	secmaster:pipe:deleteConsumption	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/search/logs	secmaster:search:listLogs	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/search/histograms	secmaster:search:listHistograms	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/search/analysis	secmaster:search:createAnalysis	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/search/conditions	secmaster:searchCondition:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/search/conditions	secmaster:searchCondition:create	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/search/conditions/{condition_id}	secmaster:searchCondition:get	-
PUT /v1/{project_id}/workspaces/{workspace_id}/siem/search/conditions/{condition_id}	secmaster:searchCondition:update	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/search/conditions/{condition_id}	secmaster:searchCondition:delete	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules	secmaster:alertRule:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules	secmaster:alertRule:create	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/{rule_id}	secmaster:alertRule:get	-

API	对应的操作项	依赖的操作项
PUT /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/{rule_id}	secmaster:alertRule:update	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules	secmaster:alertRule:delete	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/enable	secmaster:alertRule:enable	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/disable	secmaster:alertRule:disable	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/metrics	secmaster:alertRule:listMetrics	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/simulation	secmaster:alertRule:createSimulation	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/templates	secmaster:alertRuleTemplate:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/templates/{template_id}	secmaster:alertRuleTemplate:get	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/templates/metrics	secmaster:alertRuleTemplate:listMetrics	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses	secmaster:dataclass:create	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}	secmaster:dataclass:update	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}	secmaster:dataclass:delete	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}	secmaster:dataclass:get	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses	secmaster:dataclass:list	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields	secmaster:dataclass:createField	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields/{field_id}	secmaster:dataclass:updateField	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields	secmaster:dataclass:deleteField	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields/{field_id}	secmaster:dataclass:getField	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields	secmaster:dataclass:listFields	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/types/{dataclass_type_id}	secmaster:dataclass:getType	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/types	secmaster:dataclass:listTypes	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/{mapping_id}/status	secmaster:mapping:update	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/search	secmaster:mapping:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/data-source	secmaster:mapping:getDatasource	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/functions	secmaster:mapping:listFunctions	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/{mapping_id}	secmaster:mapping:delete	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/{mapping_id}/clone	secmaster:mapping:copy	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/classifiers	secmaster:mapping:createClassifier	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/classifiers/{classifier_id}	secmaster:mapping:updateClassifier	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/classifiers/{classifier_id}	secmaster:mapping:getClassifier	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/classifiers/{classifier_id}	secmaster:mapping:deleteClassifier	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/mappers	secmaster:mapping:createMapper	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/mappers/{mapper_id}	secmaster:mapping:updateMapper	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/mappers/search	secmaster:mapping:listMappers	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/mappers/{mapper_id}	secmaster:mapping:getMapper	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/mappers/{mapper_id}	secmaster:mapping:deleteMapper	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/business-type	secmaster:layout:listBusinessTypes	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/search	secmaster:layout:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/layouts	secmaster:layout:create	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/layouts	secmaster:layout:delete	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}	secmaster:layout:update	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}	secmaster:layout:get	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/template	secmaster:layout:createTemplate	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/fields	secmaster:layout:createField	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/fields	secmaster:layout:listFields	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/fields/{field_id}	secmaster:layout:getField	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/fields/{field_id}	secmaster:layout:updateFiled	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/fields	secmaster:layout:deleteField	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/wizards	secmaster:layout:listWizards	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/wizards	secmaster:layout:createWizard	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/wizards/{wizard_id};/v1/{project_id}/workspaces/{workspace_id}/soc/layouts/wizards	secmaster:layout:getWizard	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/wizards/{wizard_id}	secmaster:layout:deleteWizard	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/wizards	secmaster:layout:updateWizard	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/catalogues/search;/v1/{project_id}/workspaces/{workspace_id}/soc/catalogues	secmaster:catalogue:list	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/catalogues/{catalogue_id}	secmaster:catalogue:update	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/export	secmaster:playbook:export	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/import	secmaster:playbook:import	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/template/download	secmaster:indicator:downloadTemplate	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/export	secmaster:indicator:export	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/import	secmaster:indicator:import	-
GET /v2/{project_id}/workspaces/{workspace_id}/siem/tables	secmaster:table:list	-
-POST /v2/{project_id}/workspaces/{workspace_id}/siem/tables	secmaster:table:create	-
GET /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}	secmaster:table:get	-
PUT /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}	secmaster:table:update	-
DELETE /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}	secmaster:table:delete	-
POST /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}/lock	secmaster:table:createLock	-
DELETE /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}/lock	secmaster:table:deleteLock	-
GET /v2/{project_id}/workspaces/{workspace_id}/siem/tables/metrics	secmaster:table:listMetrics	-
PUT /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}/schema	secmaster:table:updateSchema	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-79**中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

SecMaster定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-79 SecMaster 支持的资源类型

资源类型	URN
workspace	secmaster:<region>:<account-id>:workspace:<workspace-id>
playbook	secmaster:<region>:<account-id>:playbook:<workspace-id>/<playbook-id>
workflow	secmaster:<region>:<account-id>:workflow:<workspace-id>/<workflow-id>
connection	secmaster:<region>:<account-id>:connection:<workspace-id>/<connection-id>
task	secmaster:<region>:<account-id>:task:<workspace-id>/<task-id>
indicator	secmaster:<region>:<account-id>:indicator:<workspace-id>/<indicator-id>
alert	secmaster:<region>:<account-id>:alert:<workspace-id>/<alert-id>
incident	secmaster:<region>:<account-id>:incident:<workspace-id>/<incident-id>
dataobject	secmaster:<region>:<account-id>:dataobject:<workspace-id>/<dataobject-id>
metric	secmaster:<region>:<account-id>:metric:<workspace-id>/<metric-id>
resource	secmaster:<region>:<account-id>:resource:<workspace-id>/<resource-id>
report	secmaster:<region>:<account-id>:report:<workspace-id>/<report-id>
emergencyVulnerability	secmaster:<region>:<account-id>:emergencyVulnerability:<workspace-id>/<emergency-vulnerability-id>
dataspace	secmaster:<region>:<account-id>:dataspace:<workspace-id>/<dataspace-id>
pipe	secmaster:<region>:<account-id>:pipe:<workspace-id>/<pipe-id>
alertRule	secmaster:<region>:<account-id>:alertRule:<workspace-id>/<alertRule-id>
vulnerability	secmaster:<region>:<account-id>:vulnerability:<workspace-id>/<vulnerability-id>

资源类型	URN
alertRuleTemplate	secmaster:<region>:<account-id>:alertRuleTemplate:<workspace-id>/<alertRuleTemplate-id>
searchCondition	secmaster:<region>:<account-id>:searchCondition:<workspace-id>/<searchCondition-id>
dataclass	secmaster:<region>:<account-id>:dataclass:<workspace-id>/<dataclass-id>
mapping	secmaster:<region>:<account-id>:mapping:<workspace-id>/<mapping-id>
layout	secmaster:<region>:<account-id>:layout:<workspace-id>/<layout-id>
catalogue	secmaster:<region>:<account-id>:catalogue:<workspace-id>/<catalogue-id>
table	secmaster:<region>:<account-id>:table:<workspace-id>/<table-id>

条件（Condition）

SecMaster服务不支持在SCP中的条件键中配置服务级的条件键。SecMaster可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.7.4 云防火墙 CFW

Organizations服务中的服务控制策略（Service Control Policies，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。

  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于CFW定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于CFW定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下CFW的相关操作。

表 5-80 CFW 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
cfw:acl:createAclRule	授予创建acl规则的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:deleteAclRule	授予删除acl规则的权限。	write	acl *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:deleteHitCount	授予删除acl规则命中次数的权限。	write	acl *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listDomainParseServers	授予查询域名解析服务器列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getDomainParseResult	授予解析域名的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cfw:acl:getExportStatus	授予查询acl规则导出状态的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:getImportStatus	授予查询acl规则导入状态的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:getImportTemplate	授予获取acl规则导入模板的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:listAclRules	授予查询acl规则列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:listAclTags	授予查询acl规则标签列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:updateAclRule	授予更新acl规则的权限。	write	acl *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:updateAclRuleAction	授予更新acl规则动作的权限。	write	acl *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateDomainParseServer	授予更新域名解析服务器的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:setPriority	授予设置acl规则优先级的权限。	write	acl *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:blackWhiteList:create	授予创建黑白名单的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:blackWhiteList:delete	授予删除黑白名单的权限。	write	blackWhiteList *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:blackWhiteList:list	授予列出黑白名单列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:blackWhiteList:update	授予更新黑白名单的权限。	write	blackWhiteList *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:domainGroup:update	授予更新域名组的权限。	write	domainGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:domainGroup:create	授予创建域名组的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:domainGroup:delete	授予删除域名组的权限。	write	domainGroup *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:domainGroup:list	授予列出域名组列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:eip:count	授予查询弹性公网IP数量的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:eip:list	授予列出弹性公网IP列表的权限。	list	instance *	g:ResourceTag/<tag-key>
cfw:eip:updateProtectStatus	授予修改弹性公网IP防护状态的权限。	write	eip *	-
			-	g:EnterpriseProjectId
cfw:instance:checkNameRepeat	授予检查云防火墙名称是否重复。	read	-	-
cfw:instance:listAdvanceIpsRules	授予查询云防火墙高级ips规则列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listUsedEr	授予查询已使用er列表的权限。	list	-	-
cfw:instance:listUsedInspectionVpc	授予查询已使用inspectionVpc列表的权限。	list	-	-
cfw:instance:addLogConfig	授予添加云防火墙日志配置的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateCustomRule	授予更新云防火墙用户自定义ips的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cfw:instance:updateCustomRuleAction	授予更新云防火墙用户自定义ips动作的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateLogConfig	授予更新云防火墙LTS日志配置的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:createInstance	授予创建云防火墙的权限。	write	instance *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
cfw:instance:deletePostPaidInstance	授予删除按需计费云防火墙的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:createCaptureTask	授予创建云防火墙抓包任务的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:createCustomRule	授予创建云防火墙自定义IPS规则的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:createTags	授予创建云防火墙标签的权限。	tagging	instance *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cfw:instance:deleteInstance	授予删除云防火墙实例的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cfw:instance:deleteCaptureTask	授予删除云防火墙抓包任务的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:deleteCustomRule	授予删除云防火墙用户自定义IPS规则的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:deleteLogSearchHistory	授予删除云防火墙日志搜索历史的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:deleteTags	授予删除云防火墙标签的权限。	tagging	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	g:TagKeys
cfw:instance:exportLog	授予导出日志的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listInstanceByTags	授予按标签查询云防火墙实例的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	g:TagKeys
cfw:instance:getBaseVersion	授予查询基础版云防火墙的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getCaptureTaskResult	授予查询云防火墙抓包任务结果的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getCustomRule	授予查询云防火墙自定义IPS规则详情的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cfw:instance:getDomainParseServerStatus	授予查询云防火墙域名服务器状态的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getIpsMode	授予查询云防火墙IPS防护模式的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getIpsStatus	授予查询云防火墙IPS状态的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getLogConfig	授予查询云防火墙LTS日志配置的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getMaxCapturePacketNum	授予查询云防火墙用户最大抓包数量的权限。	read	-	-
cfw:instance:getPolicyStatistics	授予查询云防火墙防护策略统计信息的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listProjectTags	授予查询云防火墙项目标签列表的权限。	list	-	-
cfw:instance:getRegionDb	授予查询云防火墙地理位置库的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listInstanceTags	授予查询云防火墙实例标签列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listInstance	授予查询云防火墙列表的权限。	list	instance *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
cfw:instance:getInstance	授予查询云防火墙详情的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listAccessControlLog	授予查询云防火墙访问控制日志列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listAttackLog	授予查询云防火墙攻击日志列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listCaptureTask	授予查询云防火墙抓包任务列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listCustomRule	授予查询云防火墙用户自定义IPS列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getEw	授予查询云防火墙东西向墙的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listFlowLog	授予展示云防火墙流量日志列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listIpsRule	授予展示云防火墙IPS规则列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listProtectedVpc	授予查询云防火墙防护vpc列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cfw:instance:updateIpsMode	授予更新云防火墙IPS防护模式的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateAdvanceIpsRule	授予更新云防火墙高级ips规则的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateIpsRuleAction	授予更新云防火墙IPS规则模式的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateIpsStatus	授予更新云防火墙IPS状态的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateEwProtectedStatus	授予更新云防火墙东西向防火墙防护状态的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:saveTags	授予替换云防火墙标签的权限。	tagging	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
cfw:instance:startBaseVersion	授予开通云防火墙基础版的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:stopBaseVersion	授予关闭云防火墙基础版的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cfw:instance:stopCaptureTask	授予停止云防火墙抓包任务的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateAlarmConfig	授予更新云防火墙告警配置的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getAlarmConfig	授予查询云防火墙告警配置的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:upgradeInstance	授予升级云防火墙的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateName	授予更新云防火墙名称的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getAccessControlLogStatistics	授予查询云防火墙访问控制日志统计信息的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getAttackLogStatistics	授予查询云防火墙攻击日志统计信息的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getLogSearchHistory	授予查询云防火墙日志搜索历史的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getEngineLogStatistics	授予查询云防火墙引擎日志统计信息的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cfw:instance:getFlowLogStatistics	授予查询云防火墙流量日志统计信息的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getIpLogStatistics	授予查询云防火墙IP日志统计信息的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:updateIpGroupMember	授予更新云防火墙地址组成员的权限。	write	ipGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:createIpGroup	授予修改云防火墙地址组成员的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:createIpGroupMember	授予创建云防火墙地址组成员的权限。	write	ipGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:deleteIpGroup	授予删除云防火墙地址组的权限。	write	ipGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:deleteIpGroupMember	授予删除云防火墙地址组成员的权限。	write	ipGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:getIpGroup	授予查询云防火墙地址组的权限。	read	ipGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cfw:ipGroup:listIpGroups	授予查询云防火墙地址组列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:listIpGroupMember	授予查询云防火墙地址组列表的权限。	list	ipGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:updateIpGroup	授予更新云防火墙地址组的权限。	write	ipGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:updateServiceGroupMember	授予修改云防火墙服务组成员的权限。	write	serviceGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:create	授予创建云防火墙服务组成员的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:createServiceGroupMember	授予创建云防火墙服务组成员的权限。	write	serviceGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:delete	授予删除云防火墙服务组的权限。	write	serviceGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cfw:serviceGroup:deleteServiceGroupMember	授予删除云防火墙服务组成员的权限。	write	serviceGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:get	授予查询云防火墙服务组的权限。	read	serviceGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:list	授予查询云防火墙服务组列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:listServiceGroupMember	授予查询云防火墙服务组列表的权限。	list	serviceGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:update	授予更新云防火墙服务组的权限。	write	serviceGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:enableMultiAccount	授予开启云防火墙多账号管理的权限。	write	-	-
cfw:instance:listAccounts	授予查看多账号列表的权限。	list	-	-
cfw:instance:listOrganizationTree	授予查看组织树的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
cfw:instance:addAccount	授予添加账号的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:deleteAccount	授予删除账号的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getProtectedVpc	授予查看防火墙防护vpc详情的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:deleteProtectedVpc	授予删除防火墙防护vpc的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:addProtectedVpc	授予添加防火墙防护vpc的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateProtectedVpc	授予更新防火墙防护vpc的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateAntiVirusStatus	授予更新云防火墙反病毒状态的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getAntiVirusStatus	授予查看云防火墙反病毒状态的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateAntiVirusRule	授予更新云防火墙反病毒规则的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cfw:instance:getAntiVirusRule	授予查看云防火墙反病毒规则的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

CFW的API通常对应着一个或多个授权项。表5-81展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-81 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/cfw/logs/flow	cfw:instance:listFlowLog	-
GET /v1/{project_id}/cfw/logs/access-control	cfw:instance:listAccessControlLog	-
GET /v1/{project_id}/cfw/logs/attack	cfw:instance:listAttackLog	-
PUT /v1/{project_id}/cfw/logs/configuration	cfw:instance:updateLogConfig	-
POST /v1/{project_id}/firewall/east-west	cfw:instance:createInstance	• er:instances:list • er:attachments:list • er:attachments:create • vpc:vpcs:list • vpc:subnets:get • vpc:subnets:create • vpc:routeTables:list • vpc:routeTables:update • vpc:quotas:list • nat:natGateways:list
DELETE /v2/{project_id}/firewall/{resource_id}	cfw:instance:deleteInstance	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/firewall/east-west	cfw:instance:getEw	• er:attachments:list • vpc:vpcs:list • nat:natGateways:list
GET /v1/{project_id}/dns/servers	cfw:instance:listDomainParseServers	-
PUT /v1/{project_id}/dns/servers	cfw:instance:updateDomainParseServer	-
PUT /v1/{project_id}/domain-set/{set_id}	cfw:domainGroup:update	-
DELETE /v1/{project_id}/domain-set/{set_id}	cfw:domainGroup:delete	-
GET /v1/{project_id}/domain-sets	cfw:domainGroup:list	-
DELETE /v1/{project_id}/address-items	cfw:ipGroup:deleteIpGroupMember	-
GET /v1/{project_id}/address-sets/{set_id}	cfw:ipGroup:getIpGroup	-
GET /v1/{project_id}/address-items	cfw:ipGroup:listIpGroupMember	-
GET /v1/{project_id}/address-sets	cfw:ipGroup:listIpGroups	-
DELETE /v1/{project_id}/domain-set/domains/{set_id}	cfw:domainGroup:delete	-
GET /v1/{project_id}/service-items	cfw:serviceGroup:listServiceGroupMember	-
DELETE /v1/{project_id}/service-items/{item_id}	cfw:serviceGroup:deleteServiceGroupMember	-

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/black-white-list	cfw:blackWhiteList:create	-
DELETE /v1/{project_id}/service-sets/{set_id}	cfw:serviceGroup:delete	-
POST /v1/{project_id}/firewalls/list	cfw:instance:listInstance	-
PUT /v1/{project_id}/service-sets/{set_id}	cfw:serviceGroup:update	-
POST /v1/{project_id}/eip/protect	cfw:eip:updateProtectStatus	-
POST /v1/{project_id}/domain-set	cfw:domainGroup:create	-
GET /v1/{project_id}/firewall/exist	cfw:instance:getInstance	-
DELETE /v1/{project_id}/acl-rule	cfw:acl:deleteAclRule	-
GET /v1/{project_id}/domain/parse/{domain_name}	cfw:instance:listDomainParseServers	-
POST /v1/{project_id}/acl-rule/count	cfw:acl:listAclRules	-
DELETE /v1/{project_id}/address-sets/{set_id}	cfw:ipGroup:deleteIpGroup	-
POST /v1/{project_id}/firewall/east-west/protect	cfw:instance:updateEwProtectedStatus	-
POST /v1/{project_id}/domain-set/domains/{set_id}	cfw:domainGroup:create	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/service-sets	cfw:serviceGroup:list	-
GET /v2/{project_id}/cfw-acl/tags	cfw:acl:listAclTags	-
POST /v1/{project_id}/service-set	cfw:serviceGroup:create	-
DELETE /v1/{project_id}/service-items	cfw:serviceGroup:deleteServiceGroupMember	-
POST /v1/{project_id}/ips/switch	cfw:instance:updateIpsStatus	-
POST /v1/{project_id}/ips/protect	cfw:instance:updateIpsMode	-
GET /v1/{project_id}/service-sets/{set_id}	cfw:serviceGroup:get	-
DELETE /v1/{project_id}/acl-rule/count	cfw:acl:deleteHitCount	-
PUT /v1/{project_id}/address-sets/{set_id}	cfw:ipGroup:updateIpGroup	-
DELETE /v1/{project_id}/acl-rule/{acl_rule_id}	cfw:acl:deleteAclRule	-
PUT /v1/{project_id}/acl-rule/action	cfw:acl:updateAclRuleAction	-
POST /v1/{project_id}/address-set	cfw:ipGroup:createIpGroup	-
PUT /v1/{project_id}/black-white-list/{list_id}	cfw:blackWhiteList:update	-

API	对应的授权项	依赖的授权项
DELETE /v1/{project_id}/address-items/{item_id}	cfw:ipGroup:deleteIpGroupMember	-
GET /v1/{project_id}/ips/switch	cfw:instance:getIpsStatus	-
PUT /v1/{project_id}/acl-rule/{acl_rule_id}	cfw:acl:updateAclRule	-
GET /v1/{project_id}/vpcs/protection	cfw:instance:listProtectedVpc	-
GET /v1/{project_id}/eip-count/{object_id}	cfw:eip:count	-
GET /v1/{project_id}/black-white-lists	cfw:blackWhiteList:list	-
GET /v1/{project_id}/eips/protect	cfw:eip:list	-
DELETE /v1/{project_id}/black-white-list/{list_id}	cfw:blackWhiteList:delete	-
GET /v1/{project_id}/acl-rules	cfw:acl:listAclRules	-
GET /v1/{project_id}/domain-set/domains/{domain_set_id}	cfw:domainGroup:list	-
POST /v1/{project_id}/acl-rule	cfw:acl:createAclRule	-
PUT /v1/{project_id}/acl-rule/order/{acl_rule_id}	cfw:acl:setPriority	-
POST /v1/{project_id}/address-items	cfw:ipGroup:createIpGroupMember	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/ips/protect	cfw:instance:getIpsMode	-
POST /v1/{project_id}/service-items	cfw:serviceGroup:createServiceGroupMember	-
GET /v1/{project_id}/cfw/logs/configuration	cfw:instance:getLogConfig	-
POST /v1/{project_id}/cfw/logs/configuration	cfw:instance:updateLogConfig	-
POST /v2/{project_id}/firewall	cfw:instance:createInstance	-
GET /v3/{project_id}/jobs/{job_id}	cfw:instance:listInstance	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-82中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

CFW定义了以下可以在自定义SCP的Resource元素中使用的资源类型。

表 5-82 CFW 支持的资源类型

资源类型	URN
instance	cfw:<region>:<account-id>:instance:<fwInstance-id>
acl	cfw:<region>:<account-id>:acl:<acl-id>
ipGroup	cfw:<region>:<account-id>:ipGroup:<ipGroup-id>
serviceGroup	cfw:<region>:<account-id>:serviceGroup:<serviceGroup-id>
blackWhiteList	cfw:<region>:<account-id>:blackWhiteList:<blackWhiteList-id>
domainGroup	cfw:<region>:<account-id>:domainGroup:<domainGroup-id>
eip	cfw:<region>:<account-id>:eip:<eip-id>

条件（Condition）

CFW服务不支持在SCP中的条件键中配置服务级的条件键。

CFW可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.7.5 云证书管理服务 CCM

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “**访问级别**”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “**资源类型**”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于PCA定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “**条件键**”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于PCA定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下PCA的相关操作。

表 5-83 PCA 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
pca:ca:create	授予权限创建私有CA。	write	ca *	-
			-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
pca:ca:delete	授予权限删除私有CA。	write	ca *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
pca:ca:disable	授予权限禁用私有CA。	write	ca *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
pca:ca:enable	授予权限启用私有CA。	write	ca *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
pca:ca:export	授予权限导出私有CA证书。	read	ca *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
pca:ca:getCsr	授予权限导出私有CA的证书签名请求（CSR）。	read	ca *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
pca:ca:import	授予权限导入证书作为私有CA证书。	write	ca *	-
			-	g:EnterpriseProjectId
pca:ca:activate	授予权限激活私有CA。	write	ca *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
pca:ca:list	授予权限查询私有CA列表。	list	ca *	-
			-	g:EnterpriseProjectId
pca:ca:restore	授予权限恢复私有CA。	write	ca *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
pca:ca:revoke	授予权限吊销私有CA。	write	ca *	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	g:EnterpriseProjectId
pca:ca:get	授予权限查询私有CA详情。	read	ca *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
pca:ca:quota	授予权限查询私有CA配额。	read	-	-
pca:ca:createTag	授予权限创建或更新私有CA标签。	tagging	ca *	g:ResourceTag/<tag-key>
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
pca:ca:deleteTag	授予权限删除私有CA标签。	tagging	ca *	g:ResourceTag/<tag-key>
			-	• g:EnterpriseProjectId • g:TagKeys
pca:ca:listTags	授予权限查询私有CA的标签列表。	list	ca *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
pca:ca:listAllTags	授予权限查询用户的私有CA标签列表。	list	ca *	-
pca:ca:listByTag	授予权限根据标签查询私有CA列表。	list	ca *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
pca:ca:issueCert	授予权限签发私有证书。	write	ca *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	• g:EnterpriseProjectId • pca:CommonName
pca:ca:issueCertByCsr	授予权限根据证书签名请求（CSR）签发私有证书。	write	ca *	-
			-	• g:EnterpriseProjectId • pca:CommonName
pca:cert:delete	授予权限删除私有证书。	write	-	g:EnterpriseProjectId
pca:cert:export	授予权限导出私有证书。	read	-	g:EnterpriseProjectId
pca:cert:list	授予权限查询私有证书列表。	list	-	g:EnterpriseProjectId
pca:ca:revokeCert	授予权限吊销私有证书。	write	ca *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
pca:cert:get	授予权限查询私有证书详情。	read	-	g:EnterpriseProjectId
pca:cert:quota	授予权限查询私有证书配额。	read	-	-
pca:cert:createTag	授予权限创建或更新私有证书标签。	tagging	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
pca:cert:deleteTag	授予权限删除私有证书标签。	tagging	-	• g:EnterpriseProjectId • g:TagKeys
pca:cert:listTags	授予权限查询私有证书的标签列表。	list	-	g:EnterpriseProjectId
pca:cert:listAllTags	授予权限查询用户的私有证书标签列表。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
pca:cert:listByTag	授予权限根据标签查询私有证书列表。	list	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
pca:ca:disableCrl	授予权限禁用CRL。	write	ca *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
pca:ca:enableCrl	授予权限启用CRL。	write	ca *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId

PCA的API通常对应着一个或多个授权项。**表 PCA API与授权项的关系**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-84 PCA API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/private-certificate-authorities	pca:ca:create	-
POST /v1/private-certificate-authorities/order	pca:ca:create	-
DELETE /v1/private-certificate-authorities/{ca_id}	pca:ca:delete	-
POST /v1/private-certificate-authorities/{ca_id}/disable	pca:ca:disable	-
POST /v1/private-certificate-authorities/{ca_id}/enable	pca:ca:enable	-

API	对应的授权项	依赖的授权项
POST /v1/private-certificate-authorities/{ca_id}/export	pca:ca:export	-
GET /v1/private-certificate-authorities/{ca_id}/csr	pca:ca:getCsr	-
POST /v1/private-certificate-authorities/{ca_id}/import	pca:ca:import	-
POST /v1/private-certificate-authorities/{ca_id}/activate	pca:ca:activate	-
GET /v1/private-certificate-authorities	pca:ca:list	-
POST /v1/private-certificate-authorities/{ca_id}/restore	pca:ca:restore	-
POST /v1/private-certificate-authorities/{ca_id}/revoke	pca:ca:revoke	-
GET /v1/private-certificate-authorities/{ca_id}	pca:ca:get	-
GET /v1/private-certificate-authorities/quotas	pca:ca:quota	-
POST /v1/private-certificate-authorities/{ca_id}/tags/create	pca:ca:createTag	-
DELETE /v1/private-certificate-authorities/{ca_id}/tags/delete	pca:ca:deleteTag	-

API	对应的授权项	依赖的授权项
POST /v1/private-certificate-authorities/{ca_id}/tags	pca:ca:createTag	-
GET /v1/private-certificate-authorities/{ca_id}/tags	pca:ca:listTags	-
GET /v1/private-certificate-authorities/tags	pca:ca:listAllTags	-
POST /v1/private-certificate-authorities/resource-instances/filter	pca:ca:listByTag	-
POST /v1/private-certificates	pca:ca:issueCert	-
POST /v1/private-certificates/csr	pca:ca:issueCertByCsr	-
DELETE /v1/private-certificates/{certificate_id}	pca:cert:delete	-
POST /v1/private-certificates/{certificate_id}/export	pca:cert:export	-
GET /v1/private-certificates	pca:cert:list	-
POST /v1/private-certificates/{certificate_id}/revoke	pca:ca:revokeCert	-
GET /v1/private-certificates/{certificate_id}	pca:cert:get	-
GET /v1/private-certificates/quotas	pca:cert:quota	-
POST /v1/private-certificates/{certificate_id}/tags/create	pca:cert:createTag	-

API	对应的授权项	依赖的授权项
DELETE /v1/private-certificates/{certificate_id}/tags/delete	pca:cert:deleteTag	-
POST /v1/private-certificates/{certificate_id}/tags	pca:cert:createTag	-
GET /v1/private-certificates/{certificate_id}/tags	pca:cert:listTags	-
GET /v1/private-certificates/tags	pca:cert:listAllTags	-
POST /v1/private-certificates/resource-instances/filter	pca:cert:listByTag	-
POST /v1/private-certificate-authorities/{ca_id}/crl/disable	pca:ca:disableCrl	-
POST /v1/private-certificate-authorities/{ca_id}/crl/enable	pca:ca:enableCrl	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表 PCA支持的资源类型**中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的策略语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

PCA定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-85 PCA 支持的资源类型

资源类型	URN
ca	pca:<region>:<account-id>:ca:<ca-id>

条件（Condition）

条件（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：请参考全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如pca:）仅适用于对应服务的操作，详情请参见**表 PCA支持的服务级条件键**。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
- 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，SCP才能生效。支持的运算符请参见：运算符。

PCA定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-86 PCA 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
pca:CommonName	string	单值	根据请求参数中的证书通用名称过滤访问。

5.10.7.6 SSL 证书管理 SCM

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “**访问级别**”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “**资源类型**”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。

- 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

关于SCM定义的资源类型的详细信息请参见**资源类型（Resource）**。

- “**条件键**”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于SCM定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下SCM的相关操作。

表 5-87 SCM 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
scm:cert:subscribe	授予权限购买证书。	write	cert *	-
			-	g:EnterpriseProjectId
scm:cert:update	授予权限更新证书。	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:delete	授予权限删除证书。	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:apply	授予权限请求证书。	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:revoke	授予权限吊销证书。	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:cancel	授予权限取消证书请求。	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:reissue	授予权限重签证书。	write	cert *	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	g:EnterpriseProjectId
scm:cert:push	授予权限推送证书。	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:import	授予权限导入证书。	write	cert *	-
			-	g:EnterpriseProjectId
scm:cert:export	授予权限导出证书。	read	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:upload	授予权限上传证书。	write	cert *	-
			-	g:EnterpriseProjectId
scm:cert:download	授予权限下载证书。	read	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:save	授予权限补全证书信息。	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:addDomain	授予权限追加域名。	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:expandQuota	授予权限扩容证书配额。	write	-	g:EnterpriseProjectId
scm:cert:renew	授予权限续费证书。	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:unsubscribe	授予权限退订证书。	write	cert *	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	g:EnterpriseProjectId
scm:cert:autoRenew	授予权限开启证书自动续费。	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:list	授予权限查询证书列表。	list	cert *	-
			-	g:EnterpriseProjectId
scm:cert:get	授予权限查询证书详情。	read	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:getApplicationInfo	授予权限查询证书补全信息。	read	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:listPushHistory	授予权限查询推送记录。	list	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:getDomainValidation	授予权限查询域名验证信息。	read	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:checkDomain	授予权限验证证书域名。	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:listDeployedResources	授予权限获取证书关联资源。	list	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:deletePrivacyAuthorization	授予权限取消隐私授权。	write	cert *	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	g:EnterpriseProjectId
scm:cert:enableAutoDeploy	授予权限自动部署证书。	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:listAutoDeployedResources	授予权限查询自动部署的证书列表。	list	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:listCertificatesByTag	授予权限根据标签查询证书列表。	list	cert *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
scm:cert:createTag	授予权限创建或更新标签。	tagging	cert *	g:ResourceTag/<tag-key>
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
scm:cert:listTagsByCertificate	授予权限查询证书的标签列表。	list	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:listAllTags	授予权限查询所有的标签列表。	list	cert *	-
scm:cert:seekHelp	授予权限发送求助邮件。	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:uploadAuthentication	授予权限上传认证信息。	write	cert *	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	g:EnterpriseProjectId
scm::createCsr	授予权限创建CSR。	write	-	-
scm::listCsr	授予权限查询CSR列表。	list	-	-
scm::getCsr	授予权限查询CSR详情。	read	-	-
scm::getCsrPrivateKey	授予权限获取CSR私钥。	read	-	-
scm::updateCsr	授予权限更新CSR。	write	-	-
scm::deleteCsr	授予权限删除CSR。	write	-	-
scm::uploadCsr	授予权限上传CSR。	write	-	-
scm::createDomainMonitor	授予权限创建需要监控的域名。	write	-	-
scm::updateDomainMonitor	授予权限更新需要监控的域名。	write	-	-
scm::updateDomainMonitorSwitch	授予权限打开或关闭域名的监控开关。	write	-	-
scm::deleteDomainMonitor	授予权限删除需要监控的域名。	write	-	-
scm::getDomainMonitor	授予权限查询需要监控的域名详情。	read	-	-
scm::listDomainMonitors	授予权限查询需要监控的域名列表。	list	-	-
scm:cert:operateNotification	授予权限操作证书通知配置。	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm::orderDomainMonitor	授予权限下单需要监控的域名配额。	write	-	-
scm:cert:deployResources	授予权限部署证书至其他服务资源。	write	cert *	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	g:EnterpriseProjectId
scm:cert:listDeployResourcesHistory	授予权限查询证书的部署历史记录。	list	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:getDeployQuota	授予权限获取证书的部署配额。	read	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId

SCM的API通常对应着一个或多个授权项。**表 SCM API与授权项的关系**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-88 SCM API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3/scm/certificates	scm:cert:list	-
POST /v3/scm/certificates/import	scm:cert:import	-
GET /v3/scm/certificates/{certificate_id}	scm:cert:get	-
POST /v3/scm/certificates/{certificate_id}/export	scm:cert:export	-
POST /v3/scm/certificates/{certificate_id}/push	scm:cert:push	-
DELETE /v3/scm/certificates/{certificate_id}	scm:cert:delete	-
POST /v3/scm/certificates/{certificate_id}/read	scm:cert:getApplicationInfo	-

API	对应的授权项	依赖的授权项
POST /v3/scm/domain/monitor/subscribe	scm::orderDomainMonitor	-
PUT /v3/scm/domain/monitor/change	scm::orderDomainMonitor	-
POST /v3/scm/certificates/{certificate_id}/deploy	scm:cert:deployResources	-
GET /v3/scm/certificates/{certificate_id}/deploy-history	scm:cert:listDeployResourcesHistory	-
GET /v3/scm/certificates/{certificate_id}/deploy-quota	scm:cert:getDeployQuota	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表 scm支持的资源类型**中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的策略语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

SCM定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-89 SCM 支持的资源类型

资源类型	URN
cert	scm:<region>:<account-id>:cert:<cert-id>

条件（Condition）

SCM服务不支持在SCP中的条件键中配置服务级的条件键。SCM可以使用适用于所有服务的全局条件键，请参考请参考全局条件键。

5.10.8 IoT 物联网

5.10.8.1 设备接入 IoTDA

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于IoTDA定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于IoTDA定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下IoTDA的相关操作。

表 5-90 IoTDA 支持的授权项

授权项	描述	访问级别	资源类型	条件键
iotda:products:create	创建产品	write	app	g:EnterpriseProjectId
iotda:products:queryList	查询产品列表	list	app	g:EnterpriseProjectId
iotda:products:query	查询产品	read	app	g:EnterpriseProjectId
iotda:products:modify	修改产品	write	app	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型	条件键
iotda:products:delete	删除产品	write	app	g:EnterpriseProjectId
iotda:devices:register	创建设备	write	app	g:EnterpriseProjectId
iotda:devices:queryList	查询设备列表	list	app	g:EnterpriseProjectId
iotda:devices:query	查询设备	read	app	g:EnterpriseProjectId
iotda:devices:modify	修改设备	write	app	g:EnterpriseProjectId
iotda:devices:delete	删除设备	write	app	g:EnterpriseProjectId
iotda:devices:resetSecret	重置设备密钥	write	app	g:EnterpriseProjectId
iotda:devices:freeze	冻结设备	write	app	g:EnterpriseProjectId
iotda:devices:unfreeze	解冻设备	write	app	g:EnterpriseProjectId
iotda:devices:resetFingerprint	重置设备指纹	write	app	g:EnterpriseProjectId
iotda:devices:queryList	灵活搜索设备列表	list	app	g:EnterpriseProjectId
iotda:messages:send	下发设备消息	write	app	g:EnterpriseProjectId
iotda:messages:queryList	查询设备消息	list	app	g:EnterpriseProjectId
iotda:messages:query	查询指定消息id的消息	read	app	g:EnterpriseProjectId
iotda:message:broadcast	下发广播消息	write	app	g:EnterpriseProjectId
iotda:commands:send	下发设备命令	write	app	g:EnterpriseProjectId
iotda:asynccommands:send	下发异步设备命令	write	app	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型	条件键
iotda:asynccommands:query	查询指定id的命令	read	app	g:EnterpriseProjectId
iotda:properties:modify	修改设备属性	write	app	g:EnterpriseProjectId
iotda:properties:query	查询设备属性	read	app	g:EnterpriseProjectId
iotda:shadow:query	查询设备影子数据	read	app	g:EnterpriseProjectId
iotda:shadow:config	配置设备影子预期数据	write	app	g:EnterpriseProjectId
iotda:amqpqueue:create	创建AMQP队列	write	-	g:EnterpriseProjectId
iotda:amqpqueue:queryList	查询AMQP列表	list	-	g:EnterpriseProjectId
iotda:amqpqueue:query	查询单个AMQP队列	read	-	g:EnterpriseProjectId
iotda:amqpqueue:delete	删除AMQP队列	write	-	g:EnterpriseProjectId
iotda:accesscode:create	生成接入凭证	write	-	g:EnterpriseProjectId
iotda:routingrules:create	创建规则触发条件	write	app	g:EnterpriseProjectId
iotda:routingrules:queryList	查询规则条件列表	list	app	g:EnterpriseProjectId
iotda:routingrules:query	查询规则条件	read	app	g:EnterpriseProjectId
iotda:routingrules:modify	修改规则触发条件	write	app	g:EnterpriseProjectId
iotda:routingrules:delete	删除规则触发条件	write	app	g:EnterpriseProjectId
iotda:routingactions:create	创建规则动作	write	app	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型	条件键
iotda:routingactions:queryList	查询规则动作列表	list	app	g:EnterpriseProjectId
iotda:routingactions:query	查询规则动作	read	app	g:EnterpriseProjectId
iotda:routingactions:modify	修改规则动作	write	app	g:EnterpriseProjectId
iotda:routingactions:delete	删除规则动作	write	app	g:EnterpriseProjectId
iotda:rules:create	创建规则	write	-	g:EnterpriseProjectId
iotda:rules:queryList	查询规则列表	list	-	g:EnterpriseProjectId
iotda:rules:modify	修改规则	write	-	g:EnterpriseProjectId
iotda:rules:query	查询规则	read	-	g:EnterpriseProjectId
iotda:rules:delete	删除规则	write	-	g:EnterpriseProjectId
iotda:rules:modifyStatus	修改规则状态	write	-	g:EnterpriseProjectId
iotda:group:create	添加设备组	write	app	g:EnterpriseProjectId
iotda:group:queryList	查询设备组列表	list	app	g:EnterpriseProjectId
iotda:group:query	查询设备组	read	app	g:EnterpriseProjectId
iotda:group:modify	修改设备组	write	app	g:EnterpriseProjectId
iotda:group:delete	删除设备组	write	app	g:EnterpriseProjectId
iotda:group:addDevice	管理设备组中的设备	write	app	g:EnterpriseProjectId
iotda:group:queryDeviceList	查询设备组设备列表	list	app	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型	条件键
iotda:tags:bind	绑定标签	tagging	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
iotda:tags:unbind	解绑标签	tagging	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
iotda:tags:queryResourceList	按标签查询资源	list	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
iotda:apps:queryList	查询资源空间列表	list	app	g:EnterpriseProjectId
iotda:app:create	创建资源空间	write	app	g:EnterpriseProjectId
iotda:apps:query	查询资源空间	read	app	g:EnterpriseProjectId
iotda:apps:delete	删除资源空间	write	app	g:EnterpriseProjectId
iotda:batchtasks:create	创建批量任务	write	-	g:EnterpriseProjectId
iotda:batchtasks:queryList	查询批量任务列表	list	-	g:EnterpriseProjectId
iotda:batchtasks:query	查询批量任务	read	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型	条件键
iotda:batchtasks:retry	批量任务重试	write	-	g:EnterpriseProjectId
iotda:batchtasks:stop	批量任务停止	write	-	g:EnterpriseProjectId
iotda:batchtasks:delete	删除批量任务	write	-	g:EnterpriseProjectId
iotda:batchtaskfiles:create	上传批量任务文件	write	-	g:EnterpriseProjectId
iotda:batchtaskfiles:queryList	查询批量任务文件列表	list	-	g:EnterpriseProjectId
iotda:batchtaskfiles:delete	删除批量任务文件	write	-	g:EnterpriseProjectId
iotda:certificates:upload	上传设备CA证书	write	app	g:EnterpriseProjectId
iotda:certificates:queryList	获取设备CA证书列表	list	app	g:EnterpriseProjectId
iotda:certificates:delete	删除设备CA证书	write	app	g:EnterpriseProjectId
iotda:certificates:check	验证设备CA证书	write	app	g:EnterpriseProjectId
iotda:otapackages:create	创建OTA升级包	write	-	g:EnterpriseProjectId
iotda:otapackages:queryList	查询OTA升级包列表	list	-	g:EnterpriseProjectId
iotda:otapackages:query	获取OTA升级包详情	read	-	g:EnterpriseProjectId
iotda:otapackages:delete	删除OTA升级包	write	-	g:EnterpriseProjectId
iotda:tunnel:queryList	查询隧道列表	list	-	g:EnterpriseProjectId
iotda:tunnel:create	创建设备隧道	write	-	g:EnterpriseProjectId
iotda:tunnel:delete	删除设备隧道	write	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型	条件键
iotda:tunnel:query	查询隧道详情	read	-	g:EnterpriseProjectId
iotda:tunnel:update	修改设备隧道	write	-	g:EnterpriseProjectId

IoTDA的API通常对应着一个或多个授权项。**表2 API与授权项的关系**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-91 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v5/iot/{project_id}/products	iotda:products:create	-
GET /v5/iot/{project_id}/products	iotda:products:queryList	-
GET /v5/iot/{project_id}/products/{product_id}	iotda:products:query	-
PUT /v5/iot/{project_id}/products/{product_id}	iotda:products:modify	-
DELETE /v5/iot/{project_id}/products/{product_id}	iotda:products:delete	-
POST /v5/iot/{project_id}/devices	iotda:devices:register	-
GET /v5/iot/{project_id}/devices	iotda:devices:queryList	-
GET /v5/iot/{project_id}/devices/{device_id}	iotda:devices:query	-
PUT /v5/iot/{project_id}/devices/{device_id}	iotda:devices:modify	-
DELETE /v5/iot/{project_id}/devices/{device_id}	iotda:devices:delete	-
POST /v5/iot/{project_id}/devices/{device_id}/action	iotda:devices:resetSecret	-
POST /v5/iot/{project_id}/devices/{device_id}/freeze	iotda:devices:freeze	-
POST /v5/iot/{project_id}/devices/{device_id}/unfreeze	iotda:devices:unfreeze	-
POST /v5/iot/{project_id}/devices/{device_id}/reset-fingerprint	iotda:devices:resetFingerprint	-

API	对应的授权项	依赖的授权项
POST /v5/iot/{project_id}/search/query-devices	iotda:devices:queryList	-
POST /v5/iot/{project_id}/devices/{device_id}/messages	iotda:messages:send	-
GET /v5/iot/{project_id}/devices/{device_id}/messages	iotda:messages:queryList	-
GET /v5/iot/{project_id}/devices/{device_id}/messages/{message_id}	iotda:messages:query	-
POST /v5/iot/{project_id}/broadcast-messages	iotda:message:broadcast	-
POST /v5/iot/{project_id}/devices/{device_id}/commands	iotda:commands:send	-
POST /v5/iot/{project_id}/devices/{device_id}/async-commands	iotda:asynccommands:send	-
GET /v5/iot/{project_id}/devices/{device_id}/async-commands/{command_id}	iotda:asynccommands:query	-
PUT /v5/iot/{project_id}/devices/{device_id}/properties	iotda:properties:modify	-
GET /v5/iot/{project_id}/devices/{device_id}/properties	iotda:properties:query	-
GET /v5/iot/{project_id}/devices/{device_id}/shadow	iotda:shadow:query	-
PUT /v5/iot/{project_id}/devices/{device_id}/shadow	iotda:shadow:config	-
POST /v5/iot/{project_id}/amqp-queues	iotda:amqpqueue:create	-
GET /v5/iot/{project_id}/amqp-queues	iotda:amqpqueue:queryList	-
GET /v5/iot/{project_id}/amqp-queues/{queue_id}	iotda:amqpqueue:query	-
DELETE /v5/iot/{project_id}/amqp-queues/{queue_id}	iotda:amqpqueue:delete	-
POST /v5/iot/{project_id}/auth/accesscode	iotda:accesscode:create	-
POST /v5/iot/{project_id}/routing-rule/rules	iotda:routingrules:create	-

API	对应的授权项	依赖的授权项
GET /v5/iot/{project_id}/routing-rule/rules	iotda:routingrules:queryList	-
GET /v5/iot/{project_id}/routing-rule/rules/{rule_id}	iotda:routingrules:query	-
PUT /v5/iot/{project_id}/routing-rule/rules/{rule_id}	iotda:routingrules:modify	-
DELETE /v5/iot/{project_id}/routing-rule/rules/{rule_id}	iotda:routingrules:delete	-
POST /v5/iot/{project_id}/routing-rule/actions	iotda:routingactions:create	-
GET /v5/iot/{project_id}/routing-rule/actions	iotda:routingactions:queryList	-
GET /v5/iot/{project_id}/routing-rule/actions/{action_id}	iotda:routingactions:query	-
PUT /v5/iot/{project_id}/routing-rule/actions/{action_id}	iotda:routingactions:modify	-
DELETE /v5/iot/{project_id}/routing-rule/actions/{action_id}	iotda:routingactions:delete	-
POST /v5/iot/{project_id}/rules	iotda:rules:create	-
GET /v5/iot/{project_id}/rules	iotda:rules:queryList	-
PUT /v5/iot/{project_id}/rules/{rule_id}	iotda:rules:modify	-
GET /v5/iot/{project_id}/rules/{rule_id}	iotda:rules:query	-
DELETE /v5/iot/{project_id}/rules/{rule_id}	iotda:rules:delete	-
PUT /v5/iot/{project_id}/rules/{rule_id}/status	iotda:rules:modifyStatus	-
POST /v5/iot/{project_id}/device-group	iotda:group:create	-
GET /v5/iot/{project_id}/device-group	iotda:group:queryList	-
GET /v5/iot/{project_id}/device-group/{group_id}	iotda:group:query	-
PUT /v5/iot/{project_id}/device-group/{group_id}	iotda:group:modify	-
DELETE /v5/iot/{project_id}/device-group/{group_id}	iotda:group:delete	-
POST /v5/iot/{project_id}/device-group/{group_id}/action	iotda:group:addDevice	-

API	对应的授权项	依赖的授权项
GET /v5/iot/{project_id}/device-group/{group_id}/devices	iotda:group:queryDeviceList	-
POST /v5/iot/{project_id}/tags/bind-resource	iotda:tags:bind	-
POST /v5/iot/{project_id}/tags/unbind-resource	iotda:tags:unbind	-
POST /v5/iot/{project_id}/tags/query-resources	iotda:tags:queryResourceList	-
GET /v5/iot/{project_id}/apps	iotda:apps:queryList	-
POST /v5/iot/{project_id}/apps	iotda:app:create	-
GET /v5/iot/{project_id}/apps/{app_id}	iotda:apps:query	-
DELETE /v5/iot/{project_id}/apps/{app_id}	iotda:apps:delete	-
POST /v5/iot/{project_id}/batchtasks	iotda:batchtasks:create	-
GET /v5/iot/{project_id}/batchtasks	iotda:batchtasks:queryList	-
GET /v5/iot/{project_id}/batchtasks/{task_id}	iotda:batchtasks:query	-
POST /v5/iot/{project_id}/batchtasks/{task_id}/retry	iotda:batchtasks:retry	-
POST /v5/iot/{project_id}/batchtasks/{task_id}/stop	iotda:batchtasks:stop	-
DELETE /v5/iot/{project_id}/batchtasks/{task_id}	iotda:batchtasks:delete	-
POST /v5/iot/{project_id}/batchtask-files	iotda:batchtaskfiles:create	-
GET /v5/iot/{project_id}/batchtask-files	iotda:batchtaskfiles:queryList	-
DELETE /v5/iot/{project_id}/batchtask-files/{file_id}	iotda:batchtaskfiles:delete	-
POST /v5/iot/{project_id}/certificates	iotda:certificates:upload	-
GET /v5/iot/{project_id}/certificates	iotda:certificates:queryList	-
DELETE /v5/iot/{project_id}/certificates/{certificate_id}	iotda:certificates:delete	-
POST /v5/iot/{project_id}/certificates/{certificate_id}/action	iotda:certificates:check	-

API	对应的授权项	依赖的授权项
POST /v5/iot/{project_id}/ota-upgrades/packages	iotda:otapackages:create	-
GET /v5/iot/{project_id}/ota-upgrades/packages	iotda:otapackages:queryList	-
GET /v5/iot/{project_id}/ota-upgrades/packages/{package_id}	iotda:otapackages:query	-
DELETE /v5/iot/{project_id}/ota-upgrades/packages/{package_id}	iotda:otapackages:delete	-
GET /v5/iot/{project_id}/tunnels	iotda:tunnel:queryList	-
POST /v5/iot/{project_id}/tunnels	iotda:tunnel:create	-
DELETE /v5/iot/{project_id}/tunnels/{id}	iotda:tunnel:delete	-
GET /v5/iot/{project_id}/tunnels/{id}	iotda:tunnel:query	-
PUT /v5/iot/{project_id}/tunnels/{id}	iotda:tunnel:update	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-92中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

表 5-92 IoTDA 支持的资源类型

资源类型	URN
app	iotda:<region>:<account-id>:app:<app-id>
instance	iotda:<region>:<account-id>:instance:<instance-id>

条件（Condition）

IoTDA服务不支持在SCP中的条件键中配置服务级的条件键。

IoTDA可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.9 应用中间件

5.10.9.1 分布式缓存服务 DCS

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于DCS定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于DCS定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下DCS的相关操作。

表 5-93 DCS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
dcs:instance:create	授予权限以创建缓存实例。	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys • dcs:backupEnabled

授权项	描述	访问级别	资源类型（*为必须）	条件键
dcs:instance:list	授予权限以查询缓存列表。	list	-	g:EnterpriseProjectId
dcs:instance:exportListFile	授予权限以下载导出的缓存实例列表文件。	list	-	-
dcs:instance:delete	授予权限以删除缓存实例。	write	instance	g:EnterpriseProjectId
dcs:instance:get	授予权限以查询缓存实例。	read	instance *	g:EnterpriseProjectId
dcs:instance:modify	授予权限以修改缓存实例。	write	instance *	• g:EnterpriseProjectId • dcs:backupEnabled
dcs:instance:scale	授予权限以扩容缓存实例。	write	instance *	g:EnterpriseProjectId
dcs:instance:swap	授予权限以执行缓存实例主备倒换。	write	instance *	g:EnterpriseProjectId
dcs:instance:modifyAuthInfo	授予权限以修改缓存实例密码。	write	instance *	g:EnterpriseProjectId
dcs:instance:modifyStatus	授予权限以重启缓存实例或清空缓存实例数据。	write	instance *	g:EnterpriseProjectId
dcs:instance:getConfiguration	授予权限以查询实例配置参数。	read	instance *	g:EnterpriseProjectId
dcs:instance:modifyConfiguration	授予权限以修改缓存实例配置参数。	write	instance *	g:EnterpriseProjectId
dcs:instance:deleteDataBackupFile	授予权限以删除缓存实例备份数据。	write	instance *	g:EnterpriseProjectId
dcs:instance:restoreData	授予权限以恢复缓存实例数据。	write	instance *	g:EnterpriseProjectId
dcs:instance:getDataRestoreLog	授予权限以查询实例恢复记录。	read	instance *	g:EnterpriseProjectId
dcs:instance:downloadBackupData	授予权限以获取实例备份文件下载链接。	read	instance *	g:EnterpriseProjectId
dcs:instance:backupData	授予权限以备份缓存实例数据。	write	instance *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
dcs:instance:getDataBackupLog	授予权限以查询实例备份记录。	read	instance *	g:EnterpriseProjectId
dcs:migrationTask:create	授予权限以创建数据迁移任务。	write	-	-
dcs:migrationTask:list	授予权限以查询数据迁移任务列表。	list	-	-
dcs:migrationTask:delete	授予权限以删除数据迁移任务。	write	migrationTask	-
dcs:migrationTask:get	授予权限以查询数据迁移任务。	read	migrationTask *	-
dcs:migrationTask:modify	授予权限以配置、停止数据迁移任务。	write	migrationTask *	-
dcs:instance:listBigKey	授予权限以查询实例大key列表。	list	instance *	g:EnterpriseProjectId
dcs:instance:getBigKey	授予权限以查询实例大key详情。	read	instance *	g:EnterpriseProjectId
dcs:instance:deleteBigKeyScanTask	授予权限以删除实例大key扫描任务。	write	instance	g:EnterpriseProjectId
dcs:instance:updateBigKeyAutoScanConfig	授予权限以修改实例大key扫描任务配置。	write	instance *	g:EnterpriseProjectId
dcs:instance:getBigKeyAutoScanConfig	授予权限以查询实例大key扫描任务配置。	read	instance *	g:EnterpriseProjectId
dcs:instance:analyzeHotKey	授予权限以执行实例热key分析。	write	instance *	g:EnterpriseProjectId
dcs:instance:listHotKey	授予权限以查询实例热key列表。	list	instance *	g:EnterpriseProjectId
dcs:instance:getHotKey	授予权限以查询实例热key详情。	read	instance *	g:EnterpriseProjectId
dcs:instance:deleteHotKeyScanTask	授予权限以删除实例热key扫描任务。	write	instance	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
dcs:instance:updateHotKeyAutoScanConfig	授予权限以修改实例热key扫描任务配置。	write	instance *	g:EnterpriseProjectId
dcs:instance:getHotKeyAutoScanConfig	授予权限以查询实例热key扫描任务配置。	read	instance *	g:EnterpriseProjectId
dcs:instance:analyzeExpiredKey	授予权限以执行实例过期key分析。	write	instance *	g:EnterpriseProjectId
dcs:instance:getAutoExpiredKeyScanTask	授予权限以查询过期key扫描任务。	read	instance *	-
dcs:instance:updateExpiredKeyScanConfig	授予权限以修改实例过期key扫描任务配置。	write	instance *	g:EnterpriseProjectId
dcs:instance:getExpiredKeyScanConfig	授予权限以查询实例过期key扫描任务配置。	read	instance *	g:EnterpriseProjectId
dcs:slowlog:list	授予权限以查询慢日志列表。	list	instance *	g:EnterpriseProjectId
dcs:aclaccount:create	授予权限以创建ACL账号。	write	instance *	-
dcs:aclaccount:list	授予权限以查询ACL账户列表。	list	instance *	-
dcs:aclaccount:modify	授予权限以修改ACL账号密码。	write	instance *	-
dcs:aclaccount:delete	授予权限以删除ACL账号。	write	instance *	-
dcs:whitelist:modify	授予权限以设置IP白名单分组。	write	instance *	-
dcs:whitelist:list	授予权限以查询指定实例的IP白名单。	list	instance *	-
dcs:instance:getBackgroundTask	授予权限以查询后台任务列表。	read	instance *	g:EnterpriseProjectId
dcs:instance:deleteBackgroundTask	授予权限以删除后台任务。	write	instance *	g:EnterpriseProjectId
dcs:instance:createDiagnosisTask	授予权限以诊断实例。	write	instance *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
dcs:instance:listDiagnosisTask	授予权限以查询实例诊断任务列表。	list	instance *	g:EnterpriseProjectId
dcs:instance:getDiagnosisTask	授予权限以查询实例诊断详情。	read	instance *	g:EnterpriseProjectId
dcs:instance:deleteDiagnosisTask	授予权限以删除诊断记录。	write	instance *	g:EnterpriseProjectId
dcs:template:list	授予权限以查询参数模板列表。	list	-	-
dcs:template:create	授予权限以创建自定义模板。	write	-	-
dcs:template:get	授予权限以查询参数模板。	read	-	-
dcs:template:modify	授予权限以修改自定义参数模板。	write	-	-
dcs:template:delete	授予权限以删除自定义参数模板。	write	-	-
dcs:tag:list	授予权限以查询租户所有标签。	list	-	-
dcs:tag:modify	授予权限以批量添加或删除标签。	write	instance *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
dcs:tag:get	授予权限以查询单个实例标签。	read	instance *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
dcs:redisLog:get	授予权限以获取日志下载链接。	read	instance *	-
dcs:quota:get	授予权限以查询租户配额。	read	-	-
dcs:instance:webcli	授予权限以使用WebCli连接Redis实例。	write	instance *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dcs:clientIpTrans:modify	授予权限以开启或关闭客户端ip透传。	write	instance *	-
dcs:clients:list	授予权限以查询Redis会话列表。	read	instance *	-
dcs:clients:kill	授予权限以Kill Redis会话。	write	instance *	-
dcs:ssl:get	授予权限以获取SSL证书信息。	read	instance *	-
dcs:ssl:modify	授予权限以修改SSL开关配置。	write	instance *	-
dcs:job:get	授予权限以获取前置任务检查结果。	read	-	-
dcs:task:list	授予权限以获取后台任务列表。	list	-	-
dcs:task:delete	授予权限以删除后台任务记录。	write	-	-

DCS的API通常对应着一个或多个授权项。表5-94展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-94 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/instances	dcs:instance:list	-
DELETE /v2/{project_id}/instances	dcs:instance:delete	• vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:subnets:get
GET /v2/{project_id}/instances/{instance_id}	dcs:instance:get	-

API	对应的授权项	依赖的授权项
DELETE /v2/{project_id}/instances/{instance_id}	dcs:instance:delete	• vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:subnets:get
PUT /v2/{project_id}/instances/{instance_id}	dcs:instance:modify	• vpc:ports:get • vpc:ports:update
POST /v2/{project_id}/instances/{instance_id}/resize	dcs:instance:scale	• vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:subnets:get • vpc:securityGroupRules:get • vpc:securityGroups:get
POST /v2/{project_id}/instances/{instance_id}/resize/check-job	dcs:instance:scale	-
POST /v2/{project_id}/instances/{instance_id}/swap	dcs:instance:swap	-
PUT /v2/{project_id}/instances/{instance_id}/password	dcs:instance:modifyAuthInfo	-
POST /v2/{project_id}/instances/{instance_id}/password/reset	dcs:instance:modifyAuthInfo	-
GET /v2/{project_id}/instances/status	dcs:instance:list	-

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/instances/status	dcs:instance:modifyStatus	-
GET /v2/{project_id}/instances/statistic	dcs:instance:list	-
POST /v2/{project_id}/instances/{instance_id}/groups/{group_id}/replications/{node_id}/slave-priority	dcs:instance:modify	-
DELETE /v2/{project_id}/instances/{instance_id}/groups/{group_id}/replications/{node_id}/remove-ip	dcs:instance:delete	-
GET /v2/{project_id}/instance/{instance_id}/groups	dcs:instance:get	-
GET /v2/{project_id}/instances/{instance_id}/configs	dcs:instance:getConfiguration	-
PUT /v2/{project_id}/instances/{instance_id}/configs	dcs:instance:modifyConfiguration	-
PUT /v2/{project_id}/instances/{instance_id}/async-configs	dcs:instance:modifyConfiguration	-

API	对应的授权项	依赖的授权项
DELETE /v2/{project_id}/instances/{instance_id}/backups/{backup_id}	dcs:instance:deleteDataBackupFile	-
POST /v2/{project_id}/instances/{instance_id}/restores	dcs:instance:restoreData	-
GET /v2/{project_id}/instances/{instance_id}/restores	dcs:instance:getDataRestoreLog	-
POST /v2/{project_id}/instances/{instance_id}/backups/{backup_id}/links	dcs:instance:downloadBackupData	-
POST /v2/{project_id}/instances/{instance_id}/backups	dcs:instance:backupData	-
GET /v2/{project_id}/instances/{instance_id}/backups	dcs:instance:getDataBackupLog	-
POST /v2/{project_id}/migration-task	dcs:migrationTask:create	-
GET /v2/{project_id}/migration-tasks	dcs:migrationTask:list	-
DELETE /v2/{project_id}/migration-tasks/delete	dcs:migrationTask:delete	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/migration-task/{task_id}	dcs:migrationTask:get	-
POST /v2/{project_id}/migration-task/{task_id}/stop	dcs:migrationTask:modify	-
GET /v2/{project_id}/migration-task/{task_id}/stats	dcs:migrationTask:get	-
POST /v2/{project_id}/migration/instance	dcs:migrationTask:create	-
POST /v2/{project_id}/migration/{task_id}/task	dcs:migrationTask:modify	-
POST /v2/{project_id}/migration-task/batch-stop	dcs:migrationTask:modify	-
POST /v2/{project_id}/migration-task/{task_id}/sync-stop	dcs:migrationTask:modify	-
GET /v2/{project_id}/dcs/tags	dcs:tag:list	-
POST /v2/{project_id}/dcs/{instance_id}/tags/action	dcs:tag:modify	-
GET /v2/{project_id}/instances/{instance_id}/tags	dcs:tag:get	-
GET /v2/{project_id}/instances/{instance_id}/bigkey-tasks	dcs:instance:listBigKey	-

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/instances/{instance_id}/bigkey/autoscan	dcs:instance:updateBigKeyAutoScanConfig	-
GET /v2/{project_id}/instances/{instance_id}/bigkey/autoscan	dcs:instance:getBigKeyAutoScanConfig	-
POST /v2/{project_id}/instances/{instance_id}/hotkey-task	dcs:instance:analyzeHotKey	-
GET /v2/{project_id}/instances/{instance_id}/hotkey-tasks	dcs:instance:listHotKey	-
GET /v2/{project_id}/instances/{instance_id}/hotkey-task/{hotkey_id}	dcs:instance:getHotKey	-
DELETE /v2/{project_id}/instances/{instance_id}/hotkey-task/{hotkey_id}	dcs:instance:deleteHotKeyScanTask	-
PUT /v2/{project_id}/instances/{instance_id}/hotkey/autoscan	dcs:instance:updateHotKeyAutoScanConfig	-
GET /v2/{project_id}/instances/{instance_id}/hotkey/autoscan	dcs:instance:getHotKeyAutoScanConfig	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/instances/{instance_id}/scan-expire-keys-task	dcs:instance:analyzeExpiredKey	-
GET /v2/{project_id}/instances/{instance_id}/auto-expire/histories	dcs:instance:getAutoExpiredKeyScanTask	-
POST /v2/{project_id}/instances/{instance_id}/auto-expire/scan	dcs:instance:analyzeExpiredKey	-
GET /v2/{project_id}/instances/{instance_id}/scan-expire-keys/autoscan-config	dcs:instance:getExpiredKeyScanConfig	-
PUT /v2/{project_id}/instances/{instance_id}/scan-expire-keys/autoscan-config	dcs:instance:updateExpiredKeyScanConfig	-
GET /v2/{project_id}/instances/{instance_id}/slowlog	dcs:slowlog:list	-
GET /v2/{project_id}/instances/{instance_id}/redislog	dcs:redisLog:get	-
POST /v2/{project_id}/instances/{instance_id}/redislog	dcs:redisLog:get	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/instances/{instance_id}/redislog/{id}/links	dcs:redisLog:get	-
POST /v2/{project_id}/instances/{instance_id}/accounts	dcs:aclaccount:create	-
GET /v2/{project_id}/instances/{instance_id}/accounts	dcs:aclaccount:list	-
PUT /v2/{project_id}/instances/{instance_id}/accounts/{account_id}/password/modify	dcs:aclaccount:modify	-
PUT /v2/{project_id}/instances/{instance_id}/accounts/{account_id}/password/reset	dcs:aclaccount:modify	-
PUT /v2/{project_id}/instances/{instance_id}/accounts/{account_id}	dcs:aclaccount:modify	-
PUT /v2/{project_id}/instances/{instance_id}/accounts/{account_id}/role	dcs:aclaccount:modify	-

API	对应的授权项	依赖的授权项
DELETE /v2/{project_id}/instances/{instance_id}/accounts/{account_id}	dcs:aclaccount:delete	-
PUT /v2/{project_id}/instance/{instance_id}/whitelist	dcs:whitelist:modify	-
GET /v2/{project_id}/instance/{instance_id}/whitelist	dcs:whitelist:list	-
GET /v2/{project_id}/instances/{instance_id}/tasks	dcs:instance:getBackgroundTask	-
DELETE /v2/{project_id}/instances/{instance_id}/tasks/{task_id}	dcs:instance:deleteBackgroundTask	-
GET /v2/{project_id}/quota	dcs:quota:get	-
GET /v2/{project_id}/dims/monitored-objects/{instance_id}	dcs:instance:get	-
GET /v2/{project_id}/dims/monitored-objects	dcs:instance:list	-
POST /v2/{project_id}/instances/{instance_id}/diagnosis	dcs:instance:createDiagnosisTask	-
GET /v2/{project_id}/instances/{instance_id}/diagnosis	dcs:instance:listDiagnosisTask	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/diagnosis/{report_id}	dcs:instance:getDiagnosisTask	-
DELETE /v2/{project_id}/instances/{instance_id}/diagnosis	dcs:instance:deleteDiagnosisTask	-
GET /v2/{project_id}/config-templates	dcs:template:list	-
POST /v2/{project_id}/config-templates	dcs:template:create	-
GET /v2/{project_id}/config-templates/{template_id}	dcs:template:get	-
DELETE /v2/{project_id}/config-templates/{template_id}	dcs:template:delete	-
PUT /v2/{project_id}/config-templates/{template_id}	dcs:template:modify	-
GET /v2/{project_id}/instances-logical-nodes	dcs:instance:list	-
GET /v2/{project_id}/instances/{instance_id}/config-histories	dcs:instance:get	-
PUT /v2/{project_id}/instances/{instance_id}/bandwidth	dcs:instance:modify	-

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/instances/{instance_id}/async-swap	dcs:instance:swap	-
GET /v2/{project_id}/instances/{instance_id}/operations	dcs:instance:get	-
POST /v2/{project_id}/instances/{instance_id}/webcli/auth	dcs:instance:webcli	-
POST /v2/{project_id}/instances/{instance_id}/webcli/command	dcs:instance:webcli	-
POST /v2/{project_id}/instances/{instance_id}/webcli/logout	dcs:instance:webcli	-
PUT /v2/{project_id}/{instance_id}/client-ip-transparent-transmission	dcs:clientIpTrans:modify	-
GET /v2/{project_id}/instances/{instance_id}/bigkey-task/{bigkey_id}	dcs:instance:getBigKey	-
DELETE /v2/{project_id}/instances/{instance_id}/bigkey-task/{bigkey_id}	dcs:instance:deleteBigKeyScanTask	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/instances/{instance_id}/clients	dcs:clients:list	-
GET /v2/{project_id}/instances/{instance_id}/clients	dcs:clients:list	-
POST /v2/{project_id}/instances/{instance_id}/clients/kill	dcs:clients:kill	-
POST /v2/{project_id}/instances/{instance_id}/clients/kill-all	dcs:clients:kill	-
GET /v2/{project_id}/instances/{instance_id}/config-histories/{history_id}	dcs:instance:get	-
GET /v2/{project_id}/instances/{instance_id}/deletable-replication	dcs:instance:scale	-
POST /v2/{project_id}/instances/export	dcs:instance:list	-
GET /v2/{project_id}/instance/{instance_id}/groups/{group_id}/group-nodes-state	dcs:instance:get	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/instance/{instance_id}/groups/{group_id}/replications/{node_id}/async-switchover	dcs:instance:swap	-
GET /v2/{project_id}/instances/{instance_id}/ssl	dcs:ssl:get	-
PUT /v2/{project_id}/instances/{instance_id}/ssl	dcs:ssl:modify	-
POST /v2/{project_id}/instances/{instance_id}/ssl-certs/download	dcs:ssl:modify	-
GET /v2/{project_id}/instances/{instance_id}/tasks/{task_id}/progress	dcs:instance:getBackgroundTask	-
GET /v2/{project_id}/instances/export-job	dcs:instance:exportListFile	-
GET /v2/{project_id}/jobs/{job_id}	dcs:job:get	-
PUT /v2/{project_id}/migration-task/{task_id}	dcs:migrationTask:modify	-
POST /v2/{project_id}/migration-task/{task_id}/exchange-ip	dcs:migrationTask:modify	-
GET /v2/{project_id}/tasks	dcs:task:list	-

API	对应的授权项	依赖的授权项
DELETE /v2/{project_id}/tasks/{task_id}	dcs:task:delete	-
GET /v2/{project_id}/migration-task/{task_id}/logs	dcs:migrationTask:get	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-95中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

DCS定义了以下可以在自定义SCP的Resource元素中使用的资源类型。

表 5-95 DCS 支持的资源类型

资源类型	URN
instance	dcs:<region>:<account-id>:instance:<instance-id>
migrationTask	dcs:<region>:<account-id>:migrationTask:<task-id>

条件（Condition）

条件（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。 详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如dcs:）仅适用于对应服务的操作，详情请参见表5-96。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
- 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，SCP才能生效。支持的运算符请参见：运算符。

DCS定义了以下可以在自定义SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-96 DCS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
dcs:backupEnabled	boolean	单值	对DCS实例开启自动备份进行权限控制。

5.10.9.2 微服务引擎 CSE

Organizations服务中的服务控制策略（Service Control Policies，以下简称SCP）也可以使用这些授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于CSE定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于CSE定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下CSE的相关操作。

表 5-97 CSE 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
cse:config:upload	授予上传微服务配置权限	write	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
cse:config:download	授予下载微服务配置权限	write	-	g:EnterpriseProjectId
cse:namespace:list	授予查看命名空间资源列表权限	list	-	-
cse:namespace:get	授予查看命名空间资源权限	read	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:namespace:create	授予创建命名空间资源权限	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:TagKeys
cse:namespace:update	授予修改命名空间资源权限	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:namespace:delete	授予删除命名空间资源权限	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:policy:list	授予查看治理策略列表权限	list	-	-
cse:policy:get	授予查看治理策略信息权限	read	-	-
cse:policy:create	授予创建治理策略权限	write	-	-
cse:policy:update	授予修改治理策略权限	write	-	-
cse:policy:delete	授予删除治理策略权限	write	-	-
cse:engine:get	授予查看引擎信息权限	read	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:engine:list	授予查询引擎信息列表权限	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
cse:engine:modify	授予变更引擎权限	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:engine:create	授予创建引擎权限	write	-	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:TagKeys
cse:engine:upgrade	授予升级引擎权限	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:engine:delete	授予删除引擎权限	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:engine:tagResource	授予添加引擎标签的权限	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:engine:unTagResource	授予删除引擎标签的权限	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:engine:listTags	授予查询项目下所有引擎标签的权限	list	-	-
cse:engine:listTagsForResource	授予查询引擎标签的权限	list	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:engine:listResourcesByTag	授予通过标签查询引擎列表的权限	list	-	g:TagKeys

CSE的API通常对应着一个或多个授权项。表5-98展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-98 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/enginemgr/engines/{engine_id}	cse:engine:get	-
PUT /v2/{project_id}/enginemgr/engines/{engine_id}/actions	cse:engine:modify	-
GET /v2/{project_id}/enginemgr/engines/{engine_id}/jobs/{job_id}	cse:engine:get	-
GET /v2/{project_id}/enginemgr/engines	cse:engine:list	-
POST /v1/{project_id}/kie/download	cse:config:download	-
POST /v1/{project_id}/kie/file	cse:config:upload	-
GET /v1/{project_id}/kie/kv	cse:namespace:get	-
POST /v1/{project_id}/kie/kv	cse:namespace:update	-
DELETE /v1/{project_id}/kie/kv	cse:namespace:update	-
PUT /v1/{project_id}/kie/kv/{kv_id}	cse:namespace:update	-
DELETE /v1/{project_id}/kie/kv/{kv_id}	cse:namespace:update	-
GET /v1/{project_id}/nacos/v1/console/namespaces	cse:namespace:get	-
DELETE /v1/{project_id}/nacos/v1/console/namespaces	cse:namespace:delete	-
POST /v1/{project_id}/nacos/v1/console/namespaces	cse:namespace:create	-

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/nacos/v1/console/namespaces	cse:namespace:update	-
POST /v2/{project_id}/enginemgr/engines	cse:engine:create	-
GET /v2/{project_id}/enginemgr/engines/{engine_id}	cse:engine:get	-
DELETE /v2/{project_id}/enginemgr/engines/{engine_id}	cse:engine:delete	-
PUT /v2/{project_id}/enginemgr/engines/{engine_id}/resize	cse:engine:modify	-
PUT /v2/{project_id}/enginemgr/engines/{engine_id}/config	cse:engine:modify	-
PUT /v2/{project_id}/enginemgr/engines/{engine_id}/upgrade	cse:engine:upgrade	-
GET /v3/{project_id}/govern/governance/{kind}	cse:policy:list	-
POST /v3/{project_id}/govern/governance/{kind}	cse:policy:create	-
DELETE /v3/{project_id}/govern/governance/{kind}/{policy_id}	cse:policy:delete	-
GET /v3/{project_id}/govern/governance/{kind}/{policy_id}	cse:policy:get	-
PUT /v3/{project_id}/govern/governance/{kind}/{policy_id}	cse:policy:update	-
GET /v3/{project_id}/govern/governance/display	cse:policy:list	-

API	对应的授权项	依赖的授权项
DELETE /v3/{project_id}/govern/route-rule/microservices/{service_name}	cse:policy:delete	-
PUT /v3/{project_id}/govern/route-rule/microservices/{service_name}	cse:policy:update	-
GET /v3/{project_id}/govern/route-rule/microservices/{service_name}	cse:policy:get	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表3中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

CSE定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-99 CSE 支持的资源类型

资源类型	URN
namespace	cse:<region>:<account-id>:namespace:<engine-id>/<namespace-id>
policy	cse:<region>:<account-id>:policy:<namespace-id>/<policy-name>
engine	cse:<region>:<account-id>:engine:<engine-id>

条件（Condition）

CSE服务不支持在SCP中的条件键中配置服务级的条件键。

CSE可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.10 开发与运维

5.10.10.1 应用管理与运维平台 ServiceStage

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于ServiceStage定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于ServiceStage定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下ServiceStage的相关操作。

表 5-100 ServiceStage 支持的授权项

授权项	描述	访问级别	资源类型	条件键
servicestage:app:getApplication	授予用户查看指定应用权限	read	app	• g:EnterpriseProjectId • g:ResourceTag
servicestage:app:createApplication	授予用户创建应用权限	write	app	• g:EnterpriseProjectId • g:RequestTag • g:TagKeys

授权项	描述	访问级别	资源类型	条件键
servicestage:app:modifyApplication	授予用户更新应用权限	write	app	• g:EnterpriseProjectId • g:ResourceTag • g:RequestTag • g:TagKeys
servicestage:app:deleteApplication	授予用户删除应用权限	write	app	• g:EnterpriseProjectId • g:ResourceTag
servicestage:app:listApplication	授予用户查看应用列表权限	list	-	-
servicestage:app:getConfiguration	授予用户查看应用配置权限	read	app	• g:ResourceTag • g:EnterpriseProjectId
servicestage:app:deleteConfiguration	授予用户删除应用配置权限	write	app	• g:EnterpriseProjectId • g:ResourceTag
servicestage:app:modifyConfiguration	授予用户更新应用配置权限	write	app	• g:EnterpriseProjectId • g:ResourceTag
servicestage:app:getComponent	授予用户查看指定应用组件权限	read	app	• g:EnterpriseProjectId • g:ResourceTag
servicestage:app:createComponent	授予用户创建应用组件权限	write	app	• g:ResourceTag • g:EnterpriseProjectId
servicestage:app:modifyComponent	授予用户更新应用组件权限	write	app	• g:ResourceTag • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型	条件键
servicestage:app:deleteComponent	授予用户删除应用组件权限	write	app	• g:ResourceTag • g:EnterpriseProjectId
servicestage:app:listComponent	授予用户查看应用组件列表权限	list	-	-
servicestage:environment:create	授予用户创建环境权限	write	environment	• g:EnterpriseProjectId • g:RequestTag • g:TagKeys
servicestage:environment:get	授予用户查看环境信息权限	read	environment	• g:ResourceTag • g:EnterpriseProjectId
servicestage:environment:list	授予用户查看环境列表权限	list	-	-
servicestage:environment:modify	授予用户更新环境权限	write	environment	• g:ResourceTag • g:EnterpriseProjectId • g:RequestTag • g:TagKeys
servicestage:environment:delete	授予用户删除环境权限	write	environment	• g:ResourceTag • g:EnterpriseProjectId
servicestage:environment:tag	授予TMS用户创建环境标签权限	tagging	environment	• g:ResourceTag • g:EnterpriseProjectId • g:RequestTag • g:TagKeys

授权项	描述	访问级别	资源类型	条件键
servicestage:app:tag	授予TMS用户创建应用标签权限	tagging	app	• g:ResourceTag • g:EnterpriseProjectId • g:RequestTag • g:TagKeys
servicestage:environment:listResourcesByTag	授予TMS用户通过标签查询环境资源权限	read	environment	• g:RequestTag • g:TagKeys
servicestage:app:listResourcesByTag	授予TMS用户通过标签查询应用资源权限	read	app	• g:RequestTag • g:TagKeys
servicestage:environment:unTagResource	授予TMS用户删除环境资源标签权限	tagging	environment	• g:ResourceTag • g:RequestTag • g:EnterpriseProjectId • g:TagKeys
servicestage:app:unTagResource	授予TMS用户删除应用资源标签权限	tagging	app	• g:ResourceTag • g:EnterpriseProjectId • g:RequestTag • g:TagKeys
servicestage:environment:listTags	授予TMS用户查询环境资源标签列表权限	read	-	-
servicestage:app:listTags	授予TMS用户查询应用资源标签列表权限	read	-	-
servicestage:pipeline:get	授予用户查看流水线权限	read	pipeline	-
servicestage:pipeline:create	授予用户创建流水线权限	write	pipeline	-

授权项	描述	访问级别	资源类型	条件键
servicestage:pipeline:modify	授予用户更新流水线权限	write	pipeline	-
servicestage:pipeline:delete	授予用户删除流水线权限	write	pipeline	-
servicestage:pipeline:list	授予用户查看流水线列表权限	list	-	-
servicestage:assembling:runtimeList	授予用户查看技术栈列表权限	read	-	-
servicestage:assembling:getInfo	授予用户查看构建信息权限	list	-	-
servicestage:assembling:create	授予用户创建构建任务权限	write	assembling	-
servicestage:assembling:modify	授予用户更新构建任务权限	write	assembling	-
servicestage:assembling:delete	授予用户删除构建任务权限	write	assembling	-
servicestage:assembling:list	授予用户查看构建任务列表权限	list	-	-
servicestage:repositoryAuth:list	授予用户获取仓库授权列表权限	list	-	-
servicestage:repositoryAuth:get	授予用户获取仓库授权权限	read	repositoryAuth	-
servicestage:repositoryAuth:create	授予用户创建仓库授权权限	write	repositoryAuth	-
servicestage:repositoryAuth:delete	授予用户删除仓库授权权限	write	repositoryAuth	-

授权项	描述	访问级别	资源类型	条件键
servicestage:environment:listTagsForResource	授予eps用户查询环境资源标签列表权限	read	environment	• g:ResourceTag • g:EnterpriseProjectId
servicestage:app:listTagsForResource	授予eps用户查询应用资源标签列表权限	read	app	• g:ResourceTag • g:EnterpriseProjectId

ServiceStage的API通常对应着一个或多个授权项。表5-101展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-101 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/cas/metadata/runtimes	servicestage:app:listApplication	-
GET /v2/{project_id}/cas/metadata/flavors	servicestage:app:listApplication	-
POST /v2/{project_id}/cas/environments	servicestage:environment:create	-
GET /v2/{project_id}/cas/environments	servicestage:environment:list	-
PUT /v2/{project_id}/cas/environments/{environment_id}	servicestage:environment:modify	-
DELETE /v2/{project_id}/cas/environments/{environment_id}	servicestage:environment:delete	-
GET /v2/{project_id}/cas/environments/{environment_id}	servicestage:environment:get	-
PATCH /v2/{project_id}/cas/environments/{environment_id}/resources	servicestage:environment:modify	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/cas/applications	servicestage:app:createApplication	-
GET /v2/{project_id}/cas/applications	servicestage:app:listApplication	-
PUT /v2/{project_id}/cas/applications/{application_id}	servicestage:app:modifyApplication	-
DELETE /v2/{project_id}/cas/applications/{application_id}	servicestage:app:deleteApplication	-
GET /v2/{project_id}/cas/applications/{application_id}	servicestage:app:getApplication	-
PUT /v2/{project_id}/cas/applications/{application_id}/configuration	servicestage:app:modifyConfiguration	-
DELETE /v2/{project_id}/cas/applications/{application_id}/configuration	servicestage:app:deleteConfiguration	-
GET /v2/{project_id}/cas/applications/{application_id}/configuration	servicestage:app:getConfiguration	-
POST /v2/{project_id}/cas/applications/{application_id}/components	servicestage:app:createComponent	servicestage:assembling:getInfo servicestage:assembling:create
GET /v2/{project_id}/cas/applications/{application_id}/components	servicestage:app:listComponent	-
PUT /v2/{project_id}/cas/applications/{application_id}/components/{component_id}	servicestage:app:modifyComponent	-

API	对应的授权项	依赖的授权项
DELETE /v2/{project_id}/cas/applications/{application_id}/components/{component_id}	servicestage:app:deleteComponent	-
GET /v2/{project_id}/cas/applications/{application_id}/components/{component_id}	servicestage:app:getComponent	-
POST /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances	servicestage:app:createComponent	servicestage:assembling:getInfo servicestage:assembling:create
GET /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances	servicestage:app:listComponent	-
POST /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}/action	servicestage:app:modifyComponent	-
PUT /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}	servicestage:app:modifyComponent	-
DELETE /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}	servicestage:app:deleteComponent	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}	servicestage:app:getComponent	-
GET /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}/snapshots	servicestage:app:getComponent	-
GET /v2/{project_id}/cas/jobs/{job_id}	servicestage:app:listApplication	-
POST /v3/{project_id}/cas/environments	servicestage:environment:create	-
GET /v3/{project_id}/cas/environments	servicestage:environment:list	-
PUT /v3/{project_id}/cas/environments/{environment_id}	servicestage:environment:modify	-
DELETE /v3/{project_id}/cas/environments/{environment_id}	servicestage:environment:delete	-
GET /v3/{project_id}/cas/environments/{environment_id}	servicestage:environment:get	-
PUT /v3/{project_id}/cas/environments/{environment_id}/resources	servicestage:environment:modify	-
GET /v3/{project_id}/cas/environments/{environment_id}/resources	servicestage:environment:list	-
POST /v3/{project_id}/cas/applications	servicestage:app:createApplication	-
GET /v3/{project_id}/cas/applications	servicestage:app:listApplication	-

API	对应的授权项	依赖的授权项
PUT /v3/{project_id}/cas/applications/{application_id}	servicestage:app:modifyApplication	-
GET /v3/{project_id}/cas/applications/{application_id}	servicestage:app:getApplication	-
GET /v3/{project_id}/cas/applications/{application_id}/configuration	servicestage:app:getConfiguration	-
PUT /v3/{project_id}/cas/applications/{application_id}/configuration	servicestage:app:modifyConfiguration	-
DELETE /v3/{project_id}/cas/applications/{application_id}/configuration	servicestage:app:deleteConfiguration	-
POST /v3/{project_id}/cas/applications/{application_id}/components	servicestage:app:createComponent	servicestage:assembling:getInfo servicestage:assembling:create
GET /v3/{project_id}/cas/applications/{application_id}/components	servicestage:app:listComponent	-
GET /v3/{project_id}/cas/components	servicestage:app:listComponent	-
PUT /v3/{project_id}/cas/applications/{application_id}/components/{component_id}	servicestage:app:modifyComponent	-
DELETE /v3/{project_id}/cas/applications/{application_id}/components/{component_id}	servicestage:app:deleteComponent	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/cas/applications/{application_id}/components/{component_id}	servicestage:app:getComponent	-
POST /v3/{project_id}/cas/applications/{application_id}/components/{component_id}/action	servicestage:app:modifyComponent	-
GET /v3/{project_id}/cas/applications/{application_id}/components/{component_id}/records	servicestage:app:listComponent	-
GET /v3/{project_id}/cas/runtimestacks	servicestage:app:listApplication	-
GET /v1/{project_id}/git/auths	servicestage:repositoryAuth:list	-
GET /v1/{project_id}/git/auths/{repo_type}/redirect	servicestage:repositoryAuth:get	-
POST /v1/{project_id}/git/auths/{repo_type}/oauth	servicestage:repositoryAuth:create	-
POST /v1/{project_id}/git/auths/{repo_type}/personal	servicestage:repositoryAuth:create	-
POST /v1/{project_id}/git/auths/{repo_type}/password	servicestage:repositoryAuth:create	-
DELETE /v1/{project_id}/git/auths/{name}	servicestage:repositoryAuth:delete	-
GET /v2/{project_id}/servicestage-environment/{environment_id}/tags	servicestage:environment:listTagsForResource	-
GET /v2/{project_id}/servicestage-application/{app_id}/tags	servicestage:app:listTagsForResource	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-102中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

ServiceStage定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-102 ServiceStage 支持的资源类型

资源类型	URN
app	servicestage:<region>:<account-id>:app:<app-id>
environment	servicestage:<region>:<account-id>:environment:<environment-id>
pipeline	servicestage:<region>:<account-id>:pipeline:<pipeline-id>
assembling	servicestage:<region>:<account-id>:assembling:<assembling-id>
repositoryAuth	servicestage:<region>:<account-id>:repositoryAuth:<repositoryAuth-id>

条件（Condition）

ServiceStage服务不支持在SCP中的条件键中配置服务级的条件键。

ServiceStage可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.10.2 软件开发生产线 CodeArts

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。

- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于CodeArts控制台定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于CodeArts控制台定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下CodeArts控制台的相关操作。

表 5-103 CodeArts 控制台支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
codearts:projectman:viewUsage	授予权限以在控制台查询项目管理服务资源用量。	read	-	-
codearts:codehub:viewUsage	授予权限以在控制台查询代码托管服务资源用量。	read	-	-
codearts:cloudbuild:viewUsage	授予权限以在控制台查询编译构建服务资源用量。	read	-	-
codearts:codecheck:viewUsage	授予权限以在控制台查询代码检查服务资源用量。	read	-	-
codearts:cloudtest:viewUsage	授予权限以在控制台查询云测-测试管理服务资源用量。	read	-	-
codearts:apitest:viewUsage	授予权限以在控制台查询云测-接口测试服务资源用量。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
codearts:cloudrelease:viewUsage	授予权限以在控制台查询发布服务资源用量。	read	-	-
codearts:cloudide:viewUsage	授予权限以在控制台查询CloudIDE服务资源用量。	read	-	-
codearts:classroom:viewUsage	授予权限以在控制台查询Classroom服务资源用量。	read	-	-
codearts:monthlyPackage:changeSpecification	授予权限以在控制台变更软件开发平台套餐规格。	write	-	-
codearts:monthlyPackage:subscribe	授予权限以在控制台订购软件开发平台套餐。	write	-	-
codearts:projectman:subscribeService	授予权限以在控制台开通按需项目管理服务。	write	-	-
codearts:codehub:subscribeService	授予权限以在控制台开通按需代码托管服务。	write	-	-
codearts:cloudbuild:subscribeService	授予权限以在控制台开通按需编译构建服务。	write	-	-
codearts:codecheck:subscribeService	授予权限以在控制台开通按需代码检查服务。	write	-	-
codearts:cloudtest:subscribeService	授予权限以在控制台开通按需云测-测试管理服务。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
codearts:apitest:subscribeService	授予权限以在控制台开通按需云测-接口测试服务。	write	-	-
codearts:cloudrelease:subscribeService	授予权限以在控制台开通按需发布服务。	write	-	-
codearts:package:subscribeService	授予权限以在控制台开通按需服务组合。	write	-	-
codearts:cloudide:subscribeService	授予权限以在控制台开通按需CloudIDE服务。	write	-	-
codearts:classroom:subscribeService	授予权限以在控制台开通按需Classroom服务。	write	-	-
codearts:projectman:unsubscribeService	授予权限以在控制台取消开通按需项目管理服务。	write	-	-
codearts:codehub:unsubscribeService	授予权限以在控制台取消开通按需代码托管服务。	write	-	-
codearts:cloudbuild:unsubscribeService	授予权限以在控制台取消开通按需编译构建服务。	write	-	-
codearts:codecheck:unsubscribeService	授予权限以在控制台取消开通按需代码检查服务。	write	-	-
codearts:cloudtest:unsubscribeService	授予权限以在控制台取消开通按需云测-测试管理服务。	write	-	-
codearts:apitest:unsubscribeService	授予权限以在控制台取消开通按需云测-接口测试服务。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
codearts:cloudrelease:unsubscribeService	授予权限以在控制台取消开通按需发布服务。	write	-	-
codearts:package:unsubscribeService	授予权限以在控制台取消开通按需服务组合。	write	-	-
codearts:cloudide:unsubscribeService	授予权限以在控制台取消开通按需CloudIDE服务。	write	-	-
codearts:classroom:unsubscribeService	授予权限以在控制台取消开通按需Classroom服务。	write	-	-
codearts:authorization:list	授予权限以在控制台查看租户授权列表。	list	-	-
codearts:payPerUsePackage:listResourceDetail	授予权限以在控制台查看按需套餐包资源详情。	list	-	-
codearts:monthlyPackage:listResourceDetail	授予权限以在控制台查看软件开发平台套餐资源详情。	list	-	-
codearts:projectman:listResourceDetail	授予权限以在控制台查看项目管理资源列表详情。	list	-	-
codearts:codehub:listResourceDetail	授予权限以在控制台查看仓库托管资源列表详情。	list	-	-
codearts:cloudbuild:listResourceDetail	授予权限以在控制台查看构建资源列表详情。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
codearts:codecheck:listResourceDetail	授予权限以在控制台查看代码检查资源列表详情。	list	-	-
codearts:cloudtest:listResourceDetail	授予权限以在控制台查看云测-测试管理资源列表详情。	list	-	-
codearts:cloudrelease:listResourceDetail	授予权限以在控制台查看发布资源列表详情。	list	-	-
codearts:cloudide:listResourceDetail	授予权限以在控制台查看CloudIDE资源列表详情。	list	-	-
codearts:classroom:listResourceDetail	授予权限以在控制台查看Classroom资源列表详情。	list	-	-
codearts:agileDevopsTrainingServices:listResourceDetail	授予权限以在控制台查看敏捷与DevOps培训服务资源列表详情。	list	-	-
codearts:projectman:listSubscriptionHistory	授予权限以在控制台查看项目管理服务开通记录。	list	-	-
codearts:codehub:listSubscriptionHistory	授予权限以在控制台查看代码托管服务开通记录。	list	-	-
codearts:cloudbuild:listSubscriptionHistory	授予权限以在控制台查看编译构建服务开通记录。	list	-	-
codearts:codecheck:listSubscriptionHistory	授予权限以在控制台查看代码检查服务开通记录。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
codearts:cloudtest:listSubscriptionHistory	授予权限以在控制台查看云测-测试管理服务开通记录。	list	-	-
codearts:apitest:listSubscriptionHistory	授予权限以在控制台查看云测-接口测试服务开通记录。	list	-	-
codearts:cloudrelease:listSubscriptionHistory	授予权限以在控制台查看发布服务开通记录。	list	-	-
codearts:package:listSubscriptionHistory	授予权限以在控制台查看按需服务组合开通记录。	list	-	-
codearts:cloudide:listSubscriptionHistory	授予权限以在控制台查看CloudIDE服务开通记录。	list	-	-
codearts:classroom:listSubscriptionHistory	授予权限以在控制台查看Classroom服务开通记录。	list	-	-
codearts:authorization:create	授予权限以在控制台新增企业账户授权。	permissions	-	-
codearts:authorization:cancel	授予权限以在控制台取消企业账户授权。	permissions	-	-
codearts:authorization:update	授予权限以在控制台同意或拒绝企业账户授权。	permissions	-	-

资源类型（Resource）

CodeArts控制台不支持在SCP中的资源中指定资源进行权限控制。如需允许访问CodeArts控制台，请在SCP的Resource元素中使用通配符号*，表示SCP将应用到所有资源。

条件（Condition）

CodeArts控制台不支持在SCP中的条件键中配置服务级的条件键。

CodeArts控制台可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.10.3 流水线 Codearts Pipeline

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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帐号时，并没有直接对组织单元或成员帐号授予操作权限，而是规定了成员帐号或组织单元包含的成员帐号的授权范围。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的操作项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于CodeartsPipeline定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该操作项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该操作项资源类型列没有值（-），则表示条件键对整个操作项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

  关于CodeartsPipeline定义的条件键的详细信息请参见**条件（Condition）**。

您可以在自定义SCP语句的Action元素中指定以下CodeartsPipeline的相关操作。

表 5-104 CodeartsPipeline 支持的操作项

操作项	描述	访问级别	资源类型（*为必须）	条件键
codeartspipeline:pipelinetemplate:create	授予权限以创建流水线模板。	write	-	-

操作项	描述	访问级别	资源类型（*为必须）	条件键
codeartspipeline:pipelinetemplate:update	授予权限以更新流水线模板。	write	-	-
codeartspipeline:pipelinetemplate:delete	授予权限以删除流水线模板。	write	-	-
codeartspipeline:pipelinetemplate:get	授予权限以查看流水线模板。	read	-	-
codeartspipeline:pipelinetemplate:list	授予权限以查看流水线模板列表。	list	-	-
codeartspipeline:rule:create	授予权限以创建规则。	write	-	-
codeartspipeline:rule:update	授予权限以更新规则。	write	-	-
codeartspipeline:rule:delete	授予权限以删除规则。	write	-	-
codeartspipeline:rule:get	授予权限以查看规则。	read	-	-
codeartspipeline:rule:list	授予权限以查看规则列表。	list	-	-
codeartspipeline:strategy:create	授予权限以创建策略。	write	-	-
codeartspipeline:strategy:update	授予权限以更新策略。	write	-	-
codeartspipeline:strategy:delete	授予权限以删除策略。	write	-	-
codeartspipeline:strategy:get	授予权限以查看策略。	read	-	-
codeartspipeline:strategy:list	授予权限以查看策略列表。	list	-	-

操作项	描述	访问级别	资源类型（*为必须）	条件键
codeartspipeline:extension:create	授予权限以创建插件。	write	-	-
codeartspipeline:extension:update	授予权限以更新插件。	write	-	-
codeartspipeline:extension:delete	授予权限以删除插件。	write	-	-
codeartspipeline:extension:get	授予权限以查看插件。	read	-	-
codeartspipeline:extension:list	授予权限以查看插件列表。	list	-	-

CodeartsPipeline的API通常对应着一个或多个操作项。表5-105展示了API与操作项的关系，以及该API需要依赖的操作项。

表 5-105 API 与操作项的关系

API	对应的操作项	依赖的操作项
POST /v5/{tenant_id}/api/pipeline-templates	codeartspipeline:pipelinetemplate:create	-
PUT /v5/{tenant_id}/api/pipeline-templates/{template_id}	codeartspipeline:pipelinetemplate:update	-
DELETE /v5/{tenant_id}/api/pipeline-templates/{template_id}	codeartspipeline:pipelinetemplate:delete	-
GET /v5/{tenant_id}/api/pipeline-templates/{template_id}	codeartspipeline:pipelinetemplate:get	-
POST /v5/{tenant_id}/api/pipeline-templates/list	codeartspipeline:pipelinetemplate:list	-

API	对应的操作项	依赖的操作项
POST /v2/{domain_id}/rules/create	codeartspipeline:rule:create	-
PUT /v2/{domain_id}/rules/{rule_id}/update	codeartspipeline:rule:update	-
DELETE /v2/{domain_id}/rules/{rule_id}/delete	codeartspipeline:rule:delete	-
GET /v2/{domain_id}/rules/{rule_id}/detail	codeartspipeline:rule:get	-
GET /v2/{domain_id}/rules/query	codeartspipeline:rule:list	-
POST /v2/{domain_id}/tenant/rule-sets/create	codeartspipeline:strategy:create	-
PUT /v2/{domain_id}/tenant/rule-sets/{rule_set_id}/update	codeartspipeline:strategy:update	-
DELETE /v2/{domain_id}/tenant/rule-sets/{rule_set_id}/delete	codeartspipeline:strategy:delete	-
GET /v2/{domain_id}/tenant/rule-sets/{rule_set_id}/detail	codeartspipeline:strategy:get	-
GET /v2/{project_id}/rule-sets/{rule_set_id}/gray/detail	codeartspipeline:strategy:get	-
GET /v2/{domain_id}/tenant/rule-sets/query	codeartspipeline:strategy:list	-
GET /v2/{project_id}/rule-sets/query	codeartspipeline:strategy:list	-

API	对应的操作项	依赖的操作项
PUT /v2/{domain_id}/tenant/rule-sets/{rule_set_id}/switch	codeartspipeline:strategy:update	-
POST /v1/{domain_id}/agent-plugin/create	codeartspipeline:extension:create	-
POST /v1/{domain_id}/agent-plugin/create-draft	codeartspipeline:extension:create	-
POST /v1/{domain_id}/publisher/create	codeartspipeline:extension:create	-
POST /v1/{domain_id}/agent-plugin/edit-draft	codeartspipeline:extension:update	-
POST /v1/{domain_id}/agent-plugin/publish-draft	codeartspipeline:extension:update	-
POST /v1/{domain_id}/agent-plugin/update-info	codeartspipeline:extension:update	-
POST /v1/{domain_id}/agent-plugin/publish-plugin-bind	codeartspipeline:extension:update	-
POST /v1/{domain_id}/agent-plugin/publish-plugin	codeartspipeline:extension:update	-
POST /v1/{domain_id}/common/upload-plugin-icon	codeartspipeline:extension:update	-
POST /v1/{domain_id}/common/upload-publisher-icon	codeartspipeline:extension:update	-
DELETE /v1/{domain_id}/agent-plugin/delete-draft	codeartspipeline:extension:delete	-

API	对应的操作项	依赖的操作项
GET /v1/{domain_id}/publisher/query-all	codeartspipeline:extension:list	-
GET /v1/{domain_id}/publisher/optional-publisher	codeartspipeline:extension:list	-
POST /v1/{domain_id}/relation/stage-plugins	codeartspipeline:extension:list	-
GET /v1/{domain_id}/relation/plugin/single	codeartspipeline:extension:list	-
POST /v1/{domain_id}/agent-plugin/query-all	codeartspipeline:extension:list	-
POST /v1/{domain_id}/agent-plugin/plugin-metrics	codeartspipeline:extension:get	-
POST /v1/{domain_id}/agent-plugin/plugin-input	codeartspipeline:extension:get	-
POST /v1/{domain_id}/agent-plugin/plugin-output	codeartspipeline:extension:get	-
GET /v1/{domain_id}/agent-plugin/query	codeartspipeline:extension:list	-
GET /v1/{domain_id}/agent-plugin/detail	codeartspipeline:extension:get	-
GET /v1/{domain_id}/agent-plugin/all-version	codeartspipeline:extension:list	-
DELETE /v1/{domain_id}/publisher/delete	codeartspipeline:extension:delete	-

API	对应的操作项	依赖的操作项
POST /v1/{domain_id}/publisher/detail	codeartspipeline:extension:get	-
POST /v3/{domain_id}/extension/info/add	codeartspipeline:extension:create	-
POST /v3/{domain_id}/extension/info/update	codeartspipeline:extension:update	-
DELETE /v3/{domain_id}/extension/info/delete	codeartspipeline:extension:delete	-
POST /v3/{domain_id}/extension/upload	codeartspipeline:extension:update	-
GET /v3/{domain_id}/extension/detail	codeartspipeline:extension:get	-
POST /v1/{domain_id}/relation/plugins	codeartspipeline:extension:list	-

资源类型（Resource）

CodeartsPipeline服务不支持在SCP中的资源中指定资源进行权限控制。如需允许访问CodeartsPipeline服务，请在SCP的Resource元素中使用通配符号*，表示SCP将应用到所有资源。

条件（Condition）

CodeartsPipeline服务不支持在SCP中的条件键中配置服务级的条件键。
CodeartsPipeline可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.11 管理与监管

5.10.11.1 消息通知服务 SMN

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于SMN定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

  关于SMN定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下SMN的相关操作。

表 5-106 SMN 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
smn:topic:create	授予创建主题的权限。	write	topic *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
smn:topic:listTopic	授予查询主题列表的权限。	list	topic *	-
			-	g:EnterpriseProjectId
smn:topic:updateTopic	授予更新主题信息的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
smn:topic:get	授予查询主题详情的权限。	read	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:delete	授予删除主题的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:listAttributes	授予查询主题策略的权限。	list	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:deleteAttribute	授予删除主题策略的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:updateAttribute	授予更新主题策略的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• smn:TargetOrgPath • smn:TargetOrgId • smn:TargetAccountId
smn:topic:subscribe	授予主题下创建订阅的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• smn:Protocol • smn:Endpoint
smn:topic:listSubscriptionsByTopic	授予查询指定主题的订阅列表的权限。	list	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
smn:topic:listSubscriptions	授予查询所有主题的订阅列表的权限。	list	topic *	-
smn:topic:deleteSubscription	授予删除指定主题下的订阅的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:updateSubscription	授予更新指定主题下的订阅的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:publish	授予发送消息的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:template:create	授予创建模板的权限。	write	template *	-
smn:template:listTemplates	授予查询模板列表的权限。	list	template *	-
smn:template:update	授予修改模板的权限。	write	template *	-
smn:template:get	授予查询模板详情的权限。	read	template *	-
smn:template:delete	授予删除模板的权限。	write	template *	-
smn:tag:create	授予指定主题创建标签的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
smn:tag:delete	授予删除主题标签的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	• g:RequestTag/<tag-key> • g:TagKeys
smn:tag:batchModify	授予批量修改主题标签的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
smn:tag:list	授予查询主题标签的权限。	read	topic *	g:ResourceTag/<tag-key>
smn:topic:createLogTank	授予为主题关联日志组和日志流的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:listLogTank	授予查询主题的日志组和日志流的权限。	list	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:updateLogTank	授予更新主题的日志组和日志流的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:deleteLogTank	授予解除主题的日志组和日志流关系的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

SMN的API通常对应着一个或多个授权项。表5-107展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-107 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/notifications/topics	smn:topic:create	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/notifications/topics	smn:topic:listTopic	-
PUT /v2/{project_id}/notifications/topics/{topic_urn}	smn:topic:updateTopic	-
GET /v2/{project_id}/notifications/topics/{topic_urn}	smn:topic:get	-
DELETE /v2/{project_id}/notifications/topics/{topic_urn}	smn:topic:delete	-
GET /v2/{project_id}/notifications/topics/{topic_urn}/attributes	smn:topic:listAttributes	-
DELETE /v2/{project_id}/notifications/topics/{topic_urn}/attributes	smn:topic:deleteAttribute	-
PUT /v2/{project_id}/notifications/topics/{topic_urn}/attributes/{name}	smn:topic:updateAttribute	-
DELETE /v2/{project_id}/notifications/topics/{topic_urn}/attributes/{name}	smn:topic:deleteAttribute	-
POST /v2/{project_id}/notifications/topics/{topic_urn}/subscriptions	smn:topic:subscribe	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/notifications/topics/{topic_urn}/subscriptions	smn:topic:listSubscriptionsByTopic	-
PUT /v2/{project_id}/notifications/topics/{topic_urn}/subscriptions/{subscription_urn}	smn:topic:updateSubscription	-
DELETE /v2/{project_id}/notifications/subscriptions/{subscription_urn}	smn:topic:deleteSubscription	-
GET /v2/{project_id}/notifications/subscriptions	smn:topic:listSubscriptions	-
POST /v2/{project_id}/notifications/topics/{topic_urn}/publish	smn:topic:publish	-
POST /v2/{project_id}/notifications/message_template	smn:template:create	-
GET /v2/{project_id}/notifications/message_template	smn:template:listTemplates	-
PUT /v2/{project_id}/notifications/message_template/{message_template_id}	smn:template:update	-
GET /v2/{project_id}/notifications/message_template/{message_template_id}	smn:template:get	-

API	对应的授权项	依赖的授权项
DELETE /v2/{project_id}/notifications/message_template/{message_template_id}	smn:template:delete	-
POST /v2/{project_id}/{resource_type}/{resource_id}/tags	smn:tag:create	-
GET /v2/{project_id}/{resource_type}/{resource_id}/tags	smn:tag:list	-
POST /v2/{project_id}/{resource_type}/{resource_id}/tags/action	smn:tag:batchModify	• smn:tag:create • smn:tag:delete
DELETE /v2/{project_id}/{resource_type}/{resource_id}/tags/{key}	smn:tag:delete	-
GET /v2/{project_id}/{resource_type}/tags	smn:tag:list	-
POST /v2/{project_id}/{resource_type}/resource_instances/action	smn:tag:list	-
GET /v2/{project_id}/notifications/topics/{topic_urn}/logtanks	smn:topic:listLogTank	-
POST /v2/{project_id}/notifications/topics/{topic_urn}/logtanks	smn:topic:createLogTank	-

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/notifications/topics/{topic_urn}/logtanks/{logtank_id}	smn:topic:updateLogTank	-
DELETE /v2/{project_id}/notifications/topics/{topic_urn}/logtanks/{logtank_id}	smn:topic:deleteLogTank	-
POST /v2/{project_id}/notifications/subscriptions/filter_polices	smn:topic:updateSubscription	-
PUT /v2/{project_id}/notifications/subscriptions/filter_polices	smn:topic:updateSubscription	-
DELETE /v2/{project_id}/notifications/subscriptions/filter_polices	smn:topic:updateSubscription	-
POST /v2/{project_id}/notifications/topics/{topic_urn}/subscriptions/from-subscription-users	smn:topic:subscribe	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-108**中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

SMN定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-108 SMN 支持的资源类型

资源类型	URN
topic	smn:<region>:<account-id>:topic:<topic-id>
template	smn:<region>:<account-id>:template:<template-id>

条件（Condition）

条件（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀为服务缩写，如smn:）仅适用于对应服务的操作，详情请参见**表5-109**。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
- 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，SCP才能生效。支持的运算符请参见：运算符。

SMN定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-109 SMN 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
smn:TargetOrgPath	string	单值	主题策略授权的组织路径。
smn:TargetOrgId	string	单值	主题策略授权的组织ID。
smn:TargetAccountId	string	单值	主题策略授权的账号ID。
smn:Protocol	string	单值	订阅终端协议。
smn:Endpoint	string	单值	订阅终端地址。

5.10.11.2 云日志服务 LTS

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于LTS定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于LTS定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下LTS的相关操作。

表 5-110 LTS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
lts:logGroup:deleteLogGroup	授予权限以删除指定日志组。	write	logGroup *	-
lts:logGroup:listLogGroup	授予权限以查询日志组列表。	list	-	-
lts:logGroup:createLogGroup	授予权限以创建日志组。	write	-	-
lts:logGroup:updateLogGroup	授予权限以修改指定日志组。	write	logGroup *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
lts:logStream:listLogStream	授予权限以查询日志流列表。	list	logGroup *	-
lts:logStream:deleteLogStream	授予权限以删除指定日志流。	write	logStream *	-
lts:logStream:createLogStream	授予权限以创建日志流。	write	logGroup *	-
lts:logStream:searchLog	授予权限以查询日志。	list	logStream *	-
lts:logStream:searchStructLog	授予权限以查询结构化日志。	list	logStream *	-
lts:logStream:searchLogHistogram	授予权限以查询日志直方图。	list	logStream *	-
lts:transfer:createTransfer	授予权限以创建转储任务。	write	-	-
lts:transfer:deleteTransfer	授予权限以删除转储任务。	write	transfer *	-
lts:transfer:listTransfer	授予权限以查询日志转储任务列表。	list	-	-
lts:transfer:updateTransfer	授予权限以修改转储任务。	write	transfer *	-
lts:transfer:registerDmsKafkaInstance	授予权限以注册DmsKafka实例。	write	-	-
lts:configCenter:updateOverCollectSwitch	授予权限以修改超额采集开关。	write	-	-
lts:structConfig:createStructConfig	授予权限以创建LTS结构化配置。	write	logStream *	-
lts:structConfig:deleteStructConfig	授予权限以删除LTS结构化配置。	write	logStream *	-
lts:structConfig:getStructConfig	授予权限以查询LTS结构化配置。	read	logStream *	-
lts:structConfig:listStructTemplate	授予权限以查询结构化模板列表。	list	-	-
lts:structConfig:updateStructConfig	授予权限以修改LTS结构化配置。	write	logStream *	-
lts:mappingRule:create	授予权限以创建映射规则。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
lts:mappingRule:delete	授予权限以删除映射规则。	write	-	-
lts:mappingRule:get	授予权限以查看映射规则详情。	read	-	-
lts:mappingRule:list	授予权限以查询映射规则列表。	list	-	-
lts:mappingRule:update	授予权限以修改映射规则。	write	-	-
lts:logStream:getHistorySql	授予权限以查看日志流历史sql。	read	logStream *	-
lts:alarmRule:createSqlAlarmRule	授予权限以创建sql告警规则的规则。	write	-	-
lts:alarmRule:deleteSqlAlarmRule	授予权限以删除sql告警规则。	write	alarmRule *	-
lts:alarmRule:updateSqlAlarmRule	授予权限以修改sql告警规则。	write	alarmRule *	-
lts:alarmRule:listSqlAlarmRule	授予权限以查看sql告警规则。	list	-	-
lts:alarmRule:createWordAlarmRule	授予权限以创建关键词告警规则。	write	-	-
lts:alarmRule:deleteWordAlarmRule	授予权限以删除关键词告警规则。	write	alarmRule *	-
lts:alarmRule:updateWordAlarmRule	授予权限以修改关键词告警规则。	write	alarmRule *	-
lts:alarmRule:listWordAlarmRule	授予权限以查看关键词告警规则。	list	-	-
lts:alarm:cleanAlarm	授予权限以删除告警。	write	-	-
lts:alarm:listAlarm	授予权限以查看警列表。	list	-	-
lts:logStream:listChart	授予权限以查询日志流图表。	list	-	-
lts:alarmNoticeTemplate:create	授予权限以创建告警通知模板。	write	-	-
lts:alarmNoticeTemplate:update	授予权限以修改告警通知模板。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
lts:alarmNoticeTemplate:delete	授予权限以删除告警通知模板。	write	-	-
lts:alarmNoticeTemplate:list	授予权限以查询告警通知模板列表。	list	-	-
lts:alarmNoticeTemplate:get	授予权限以查询告警通知模板详情。	read	-	-
lts:hostGroup:create	授予权限以创建主机组。	write	-	-
lts:hostGroup:delete	授予权限以删除主机组。	write	hostGroup *	-
lts:host:list	授予权限以查询主机列表。	list	-	-
lts:hostGroup:list	授予权限以查询主机组列表。	list	accessConfig *	-
lts:hostGroup:update	授予权限以修改主机组。	write	hostGroup *	-
lts:accessConfig:create	授予权限以创建日志接入。	write	logStream *	-
lts:accessConfig:delete	授予权限以删除日志接入。	write	accessConfig *	-
lts:accessConfig:list	授予权限以查询日志接入列表。	list	-	-
lts:accessConfig:update	授予权限以修改日志接入。	write	accessConfig *	-
			hostGroup	-
lts:tag:create	授予权限以创建标签。	write	-	-
lts:tag:delete	授予权限以删除标签。	write	-	-
lts:logStream:createQuickQuery	授予权限以创建快速查询。	write	logStream *	-
lts:logStream:deleteQuickQuery	授予权限以删除快速查询。	write	logStream *	-
lts:logStream:listQuickQuery	授予权限以查询快速查询列表。	list	logGroup *	-
lts:logFavorite:create	授予权限以创建日志收藏。	write	logStream *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
lts:logFavorite:delete	授予权限以删除日志收藏。	write	-	-
lts:dashboardGroup:create	授予权限以创建仪表盘分组。	write	-	-
lts:dashboard:create	授予权限以创建仪表盘。	write	-	-
lts:trafficStatistic:get	授予权限以获取资源统计详情。	read	-	-
lts:tokenizer:get	授予权限以获取已配置的分词符。	read	-	-
lts:tokenizer:create	授予权限以保存分词符。	write	-	-
lts:tokenizer:preview	授予权限以预览分词符。	read	-	-
lts:usageAlarm:update	授予权限以打开或者关闭使用量预警。	write	-	-
lts:csvTable:list	授予权限以获取关联数据源配置信息表。	list	-	-
lts:csvTable:upload	授予权限以上传csv文件。	write	-	-
lts:csvTable:get	授予权限以预览关联数据和查看关联数据源信息。	read	-	-
lts:csvTable:create	授予权限以创建关联数据源。	write	-	-
lts:csvTable:update	授予权限以更新关联数据源。	write	-	-
lts:csvTable:delete	授予权限以删除关联数据源。	write	-	-
lts:scheduledSql:create	授予权限以创建定时sql。	write	-	-
lts:scheduledSql:delete	授予权限以删除定时sql。	write	-	-
lts:scheduledSql:update	授予权限以修改定时sql。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
lts:scheduledSql:list	授予权限以获取定时sql列表。	list	-	-
lts:scheduledSql:get	授予权限以获取定时sql详情。	read	-	-
lts:scheduledSql:retry	授予权限以重试执行实例。	write	-	-
lts:transfer:getDisList	授予权限以获取Dis通道列表。	list	-	-
lts:transfer:listKafkaInstance	授予权限以获取kafka列表。	list	-	-
lts:transfer:updateKafkaInstance	授予权限以更新kafka信息。	write	-	-
lts:transfer:deleteKafkaInstance	授予权限以删除kafka信息。	write	-	-
lts:transfer:listKafkaAuthorization	授予权限以查询用户配置kafka授权列表。	list	-	-
lts:transfer:createKafkaAuthorization	授予权限以增加用户配置kafka授权列表。	write	-	-
lts:transfer:deleteKafkaAuthorization	授予权限以删除用户配置kafka授权列表。	write	-	-
lts:transfer:getTransfer	授予权限以获取转储任务的信息。	read	transfer *	-
lts:transfer:getDwsInfo	授予权限以查询租户的dws信息。	read	-	-
lts:transfer:registerDwsCluster	授予权限以注册dws集群。	write	-	-
lts:hostGroup:getHost	授予权限以通过查询条件获取所有主机。	read	-	-
lts:hostGroup:get	授予权限以通过查询条件获取单个主机组加入的所有配置。	read	-	-
lts:accessConfig:get	授予权限以获取单个采集配置。	read	accessConfig *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
lts:logFavorite:list	授予权限以获取收藏列表。	list	-	-
lts:logFavorite:update	授予权限以修改收藏。	write	logStream *	-
lts:logGroup:getLogGroup	授予权限以查询日志组。	read	logGroup *	-
lts:IndexConfig:list	授予权限以查询索引。	list	logGroup *	-
lts:IndexConfig:create	授予权限以创建索引。	write	logGroup *	-
lts:structConfig:listStructConfig	授予权限以获取日志流结构化信息。	list	logStream *	-
lts:logStream:updateLogStream	授予权限以修改日志流。	write	logStream *	-
lts:logStream:getRealtimeLog	授予权限以获取实时日志。	read	logStream *	-
lts:logStream:getLogStream	授予权限以查询日志流信息。	read	logStream *	-
lts:logStream:createLogFilterRules	授予权限以创建日志清洗规则。	write	logStream *	-
lts:logStream:updateLogFilterRules	授予权限以修改日志清洗规则。	write	logStream *	-
lts:logStream:deleteLogFilterRules	授予权限以删除日志清洗规则。	write	logStream *	-
lts:logStream:listLogFilterRules	授予权限以查询日志清洗规则。	list	logStream *	-
lts:logStream:getQuickQuery	授予权限以查看快速查询。	list	logStream *	-
lts:logStream:updateQuickQuery	授予权限以修改快速查询。	write	logStream *	-
lts:logStream:searchLogContext	授予权限以查询日志上下文。	read	logStream *	-
lts:structConfig:getCustomTemplate	授予权限以查询用户自定义模板。	read	-	-
lts:structConfig:createCustomTemplate	授予权限以创建用户自定义模板。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
lts:structConfig:updateCustomTemplate	授予权限以修改用户自定义模板。	write	-	-
lts:structConfig:deleteCustomTemplate	授予权限以删除用户自定义模板。	write	-	-
lts:structConfig:listCustomTemplate	授予权限以查询用户自定义模板列表。	read	-	-
lts:structConfig:smartExtra	授予权限以智能提取结构化字段。	write	-	-
lts:logStream:getAggrResult	授予权限以获取快速分析结果。	read	logStream *	-
lts:logStream:getAggr	授予权限以查询快速分析聚合器。	read	-	-
lts:logStream:createAggr	授予权限以创建快速分析聚合器。	write	-	-
lts:logStream:deleteAggr	授予权限以删除快速分析聚合器。	write	-	-
lts:logStream:getQuickAnalysisAggValue	授予权限以获取数值类型的快速分析结果。	read	logStream *	-
lts:logStream:getWordFreqConfig	授予权限以查询用户已创建的快速分析字段。	read	logStream *	-
lts:logStream:refreshWordFreqConfig	授予权限以修改快速分析字段。	write	logStream *	-
lts:logCrux:list	授予权限以查询日志聚类信息。	list	-	-
lts:logCrux:get	授予权限以获取日志聚类开关信息。	read	-	-
lts:logCrux:enable	授予权限以开启日志聚类开关。	write	-	-
lts:logCrux:disable	授予权限以关闭日志聚类开关。	write	-	-
lts:logStream:updateChart	授予权限以更新用户日志看板。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
lts:logStream:createChart	授予权限以创建用户日志看板。	write	-	-
lts:logStream:deleteChart	授予权限以删除用户日志看板。	write	logStream *	-
lts:logStream:getChart	授予权限以获取用户日志看板。	read	logStream *	-
lts:dashboard:deleteChart	授予权限以删除图表。	write	dashboard *	-
lts:dashboard:listCharts	授予权限以展示仪表盘层级的图表。	list	-	-
lts:dashboard:updateChart	授予权限以移动图表。	write	dashboard *	-
lts:dashboard:getDashboard	授予权限以查询用户日志仪表盘。	read	-	-
lts:dashboardGroup:getDashboardsGroup	授予权限以查询用户日志仪表盘分组。	read	-	-
lts:dashboardGroup:updateDashboardsGroup	授予权限以修改用户日志仪表盘分组。	write	-	-
lts:dashboardGroup:deleteDashboardsGroup	授予权限以更新用户日志仪表盘分组。	write	-	-
lts:dashboard:CreateDashBoard	授予权限以根据日志仪表盘模板批量创建仪表盘。	write	-	-
lts:dashboard:CreateDashBoardTemplate	授予权限以创建用户日志仪表盘模板。	write	-	-
lts:dashboard:getDashBoardTemplate	授予权限以查询用户日志仪表盘模板。	read	-	-
lts:dashboard:updateDashBoardTemplate	授予权限以修改用户日志仪表盘模板。	write	-	-
lts:dashboard:deleteDashBoardTemplate	授予权限以删除用户日志仪表盘模板。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
lts:dashboardGroup:createLogDashboardTemplateGroup	授予权限以创建仪表盘模板分组。	write	-	-
lts:dashboardGroup:updateLogDashboardTemplateGroup	授予权限以修改仪表盘模板分组。	write	-	-
lts:dashboardGroup:deleteLogDashboardTemplateGroup	授予权限以删除用户日志仪表盘模板分组。	write	-	-
lts:dashboard:listFilter	授予权限以查询仪表盘过滤器。	list	dashboard *	-
lts:dashboard:createFilter	授予权限以创建仪表盘过滤器。	write	dashboard *	-
lts:dashboard:updateFilter	授予权限以修改仪表盘过滤器。	write	dashboard *	-
lts:dashboard:deleteFilter	授予权限以删除仪表盘过滤器。	write	dashboard *	-
lts:alarmRule:listAlarmRules	授予权限以查询告警规则列表。	list	-	-
lts:alarmRule:getKeywordsAlarmRule	授予权限以查询关键词告警规则。	read	alarmRule *	-
lts:alarmRule:getSqlAlarmRule	授予权限以查询sql告警规则。	read	alarmRule *	-
lts:alarm:listAlarmStatistic	授予权限以查询sql告警数据。	list	-	-
lts:dashboard:update	授予权限以修改用户日志仪表盘。	write	-	-
lts:dashboard:delete	授予权限以删除用户日志仪表盘。	write	-	-
lts:logSearch:list	授予权限以获取集群列表，命名空间，组件，实例，日志，节点，日志文件页面组件列表，文件列表。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
lts:logSearch:getTime	授予权限以获取后端节点当前时间。	read	-	-
lts:logSearch:getLogContext	授予权限以获取日志上下文。	read	-	-
lts:logSearch:exportLogs	授予权限以下载日志。	write	-	-
lts:ageingTime:get	授予权限以获取配额管理。	list	-	-
lts:ageingTime:update	授予权限以修改配额管理。	write	-	-
lts:logConfigPath:list	授予权限以查询VM日志路径配置。	list	-	-
lts:logConfigPath:create	授予权限以新建VM日志路径配置。	write	-	-
lts:structRule:get	授予权限以获取结构化规则。	read	-	-
lts:structRule:create	授予权限以创建结构化规则。	write	-	-
lts:structRule:delete	授予权限以删除结构化规则。	write	-	-
lts:structRule:regex	授予权限以结构化提取。	write	-	-
lts:logPail:list	授予权限以查询日志桶、桶内日志和日志柱状图。	list	-	-
lts:structSql:list	授予权限以查询结构化日志。	list	-	-
lts:logPail:create	授予权限以添加日志桶。	write	-	-
lts:logPail:update	授予权限以修改日志桶。	list	-	-
lts:logPail:delete	授予权限以删除日志桶。	write	-	-
lts:storageRelation:list	授予权限以查询当前租户下的转储关系。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
lts:storageRelation:delete	授予权限以删除当前租户下的转储关系。	write	-	-
lts:storage:batchAction	授予权限以周期性批量启停。	write	-	-
lts:logPailDump:create	授予权限以添加日志转储。	write	-	-
lts:statisticsRule:list	授予权限以查询统计规则。	list	-	-
lts:statisticsRule:create	授予权限以创建统计规则。	write	-	-
lts:statisticsRule:update	授予权限以修改统计规则。	write	-	-
lts:statisticsRule:delete	授予权限以删除统计规则。	write	-	-
lts:transfer:listKafkaInstanceTopic	授予权限以获取用户kafka所有topic。	list	-	-
lts:logPackage:create	授予权限以购买资源包。	write	-	-
lts:consumerGroup:create	授予权限以创建消费组。	write	-	-
lts:consumerGroup:delete	授予权限以删除消费组。	write	-	-
lts:consumerGroup:list	授予权限以查询消费组列表。	list	-	-
lts:consumerGroup:get	授予权限以查询消费组详情。	read	-	-
lts:consumerGroup:update	授予权限以修改消费组。	write	-	-
lts:logStream:get	授予权限以获取日志流详情。	read	-	-
lts:agency:listGroupAndStream	授予权限以获取委托方日志组日志流列表。	list	-	-
lts:agency:listEps	授予权限以获取委托方EPS列表。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
lts:agency:listStructConfig	授予权限以获取委托方结构化配置。	list	-	-
lts:logConverge:get	授予权限以获取多账号日志汇聚配置。	read	-	-
lts:logConverge:update	授予权限以更新多账号日志汇聚配置。	write	-	-
lts:logManager:createAggr	授予权限以创建快速分析聚合器。	write	logStream *	-
lts:logManager:createAggrs	授予权限以批量创建快速分析聚合器。	write	logStream *	-
lts:logManager:deleteAggr	授予权限以删除快速分析聚合器。	write	logStream *	-
lts:logManager:deleteAggrs	授予权限以批量删除快速分析聚合器。	write	logStream *	-
lts:logmanager:createLogFilter	授予权限以创建日志清洗规则。	write	logStream *	-
lts:logmanager:listLogFilters	授予权限以查看日志清洗规则。	read	logStream *	-
lts:logmanager:updateLogFilters	授予权限以修改日志清洗规则。	write	logStream *	-
lts:logmanager:deleteLogFilters	授予权限以删除日志清洗规则。	write	logStream *	-
lts:structConfig:regex	授予权限以正则结构化示例日志。	write	-	-

LTS的API通常对应着一个或多个授权项。表5-111展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-111 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/groups	lts:logGroup:createLogGroup	-

API	对应的授权项	依赖的授权项
DELETE /v2/{project_id}/groups/{log_group_id}	lts:logGroup:deleteLogGroup	-
GET /v2/{project_id}/groups	lts:logGroup:listLogGroup	-
POST /v2/{project_id}/groups/{log_group_id}	lts:logGroup:updateLogGroup	-
POST /v2/{project_id}/groups/{log_group_id}/streams	lts:logStream:createLogStream	-
PUT /v2/{project_id}/groups/{log_group_id}/streams-ttl/{log_stream_id}	lts:logStream:updateLogStream	-
DELETE /v2/{project_id}/groups/{log_group_id}/streams/{log_stream_id}	lts:logStream:deleteLogStream	-
GET /v2/{project_id}/groups/{log_group_id}/streams	lts:logStream:listLogStream	-
GET /v2/{project_id}/log-streams	lts:logStream:listLogStream	-
POST /v2/{project_id}/lts/keyword-count	lts:logStream:searchLogHistogram	-
POST /v2/{project_id}/groups/{log_group_id}/streams/{log_stream_id}/content/query	lts:logStream:searchLog	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/groups/{log_group_id}/streams/{log_stream_id}/struct-content/query	lts:logStream:searchStructLog	-
POST /v2/{project_id}/streams/{log_stream_id}/struct-content/query	lts:logStream:searchStructLog	-
POST /v2/{project_id}/log-dump/obs	lts:transfer:createTransfer	• obs:bucket:PutBucketAcl • obs:bucket:GetBucketAcl • obs:bucket:HeadBucket
POST /v2/{project_id}/transfers	lts:transfer:createTransfer	• obs:bucket:PutBucketAcl • obs:bucket:GetBucketAcl • obs:bucket:GetEncryptionConfiguration • obs:bucket:HeadBucket • dis:streams:list • dis:streamPolicies:list
DELETE /v2/{project_id}/transfers	lts:transfer:deleteTransfer	-
GET /v2/{project_id}/transfers	lts:transfer:listTransfer	-
POST /v2/{project_id}/lts/dms/kafka-instance	lts:transfer:registerDmsKafkaInstance	dms:instance:list
PUT /v2/{project_id}/transfers	lts:transfer:updateTransfer	• obs:bucket:PutBucketAcl • obs:bucket:GetBucketAcl • obs:bucket:GetEncryptionConfiguration • obs:bucket:HeadBucket • dis:streams:list • dis:streamPolicies:list

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/collection/disable	lts:configCenter:updateOverCollectSwitch	-
POST /v2/{project_id}/collection/enable	lts:configCenter:updateOverCollectSwitch	-
POST /v3/{project_id}/lts/struct/template	lts:structConfig:createStructConfig	-
POST /v2/{project_id}/lts/struct/template	lts:structConfig:createStructConfig	-
DELETE /v2/{project_id}/lts/struct/template	lts:structConfig:deleteStructConfig	-
GET /v3/{project_id}/lts/struct/customtemplate/list	lts:structConfig:listStructTemplate	-
GET /v3/{project_id}/lts/struct/customtemplate	lts:structConfig:listStructTemplate	-
GET /v2/{project_id}/lts/struct/template	lts:structConfig:getStructConfig	-
PUT /v3/{project_id}/lts/struct/template	lts:structConfig:updateStructConfig	-
PUT /v2/{project_id}/lts/struct/template	lts:structConfig:updateStructConfig	-
POST /v2/{project_id}/lts/aom-mapping	lts:mappingRule:create	-
DELETE /v2/{project_id}/lts/aom-mapping	lts:mappingRule:delete	-
GET /v2/{project_id}/lts/aom-mapping/{rule_id}	lts:mappingRule:get	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/lts/aom-mapping	lts:mappingRule:list	-
PUT /v2/{project_id}/lts/aom-mapping	lts:mappingRule:update	-
GET /v2/{project_id}/lts/notifications/topics	lts:alarmNoticeTemplate:list	smn:topic:list
POST /v2/{project_id}/lts/alarms/sql-alarm-rule	lts:alarmRule:createSqlAlarmRule	-
DELETE /v2/{project_id}/lts/alarms/sql-alarm-rule/{sql_alarm_rule_id}	lts:alarmRule:deleteSqlAlarmRule	-
GET /v2/{project_id}/lts/alarms/sql-alarm-rule	lts:alarmRule:listSqlAlarmRule	-
PUT /v2/{project_id}/lts/alarms/status	lts:alarmRule:updateSqlAlarmRule	-
PUT /v2/{project_id}/lts/alarms/sql-alarm-rule	lts:alarmRule:updateSqlAlarmRule	-
POST /v2/{project_id}/lts/alarms/keywords-alarm-rule	lts:alarmRule:createWordAlarmRule	-
DELETE /v2/{project_id}/lts/alarms/keywords-alarm-rule/{keywords_alarm_rule_id}	lts:alarmRule:deleteWordAlarmRule	-
GET /v2/{project_id}/lts/alarms/keywords-alarm-rule	lts:alarmRule:listWordAlarmRule	-

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/lts/alarms/keywords-alarm-rule	lts:alarmRule:updateWordAlarmRule	-
POST /v2/{project_id}/{domain_id}/lts/alarms/sql-alarm/clear	lts:alarm:cleanAlarm	-
POST /v2/{project_id}/{domain_id}/lts/alarms/sql-alarm/query	lts:alarm:listAlarm	-
GET /v2/{project_id}/groups/{log_group_id}/streams/{log_stream_id}/charts	lts:logStream:listChart	-
POST /v2/{project_id}/{domain_id}/lts/events/notification/templates	lts:alarmNoticeTemplate:create	-
DELETE /v2/{project_id}/{domain_id}/lts/events/notification/templates	lts:alarmNoticeTemplate:delete	-
POST /v2/{project_id}/{domain_id}/lts/events/notification/templates/view	lts:alarmNoticeTemplate:list	-
GET /v2/{project_id}/{domain_id}/lts/events/notification/templates	lts:alarmNoticeTemplate:list	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/{domain_id}/lts/events/notification/template/{template_name}	lts:alarmNoticeTemplate:get	-
PUT /v2/{project_id}/{domain_id}/lts/events/notification/templates	lts:alarmNoticeTemplate:update	-
POST /v3/{project_id}/lts/host-group	lts:hostGroup:create	-
DELETE /v3/{project_id}/lts/host-group	lts:hostGroup:delete	-
POST /v3/{project_id}/lts/host-list	lts:host:list	• aom:icmgr:get • aom:icmgr:list
POST /v3/{project_id}/lts/host-group-list	lts:hostGroup:list	-
PUT /v3/{project_id}/lts/host-group	lts:hostGroup:update	-
POST /v3/{project_id}/lts/access-config	lts:accessConfig:create	-
DELETE /v3/{project_id}/lts/access-config	lts:accessConfig:delete	-
POST /v3/{project_id}/lts/access-config-list	lts:accessConfig:list	-
PUT /v3/{project_id}/lts/access-config	lts:accessConfig:update	-
POST /v1/{project_id}/{resource_type}/{resource_id}/tags/action	lts:tag:create	-

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/groups/{group_id}/topics/{topic_id}/search-criterias	lts:logStream:createQuickQuery	-
DELETE /v1.0/{project_id}/groups/{group_id}/topics/{topic_id}/search-criterias	lts:logStream:deleteQuickQuery	-
GET /v1.0/{project_id}/groups/{group_id}/topics/{topic_id}/search-criterias	lts:logStream:listQuickQuery	-
GET /v2/{project_id}/lts/history-sql	lts:logStream:getHistorySql	-
GET /v1.0/{project_id}/lts/groups/{group_id}/search-criterias	lts:logStream:listQuickQuery	-
POST /v1.0/{project_id}/lts/favorite	lts:logFavorite:create	-
DELETE /v1.0/{project_id}/lts/favorite/{fav_res_id}	lts:logFavorite:delete	-
POST /v2/{project_id}/dashboard	lts:dashboard:create	-
POST /v2/{project_id}/lts/dashboard-group	lts:dashboardGroup:create	-
POST /v2/{project_id}/lts/timeline-traffic-statistics	lts:trafficStatistic:get	-
POST /v2/{project_id}/lts/topn-traffic-statistics	lts:trafficStatistic:get	-

资源类型（Resource）

资源类型（Resource）表示份SCP所作用的资源。如表5-112中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

LTS定义了以下可以在自定义SCP的Resource元素中使用的资源类型。

表 5-112 LTS 支持的资源类型

资源类型	URN
logStream	lts:<region>:<account-id>:logStream:<group_id>/<stream_id>
logGroup	lts:<region>:<account-id>:logGroup:<group_id>
dashboard	lts:<region>:<account-id>:dashboard:<dashboard_id>
accessConfig	lts:<region>:<account-id>:accessConfig:<config_id>
alarmRule	lts:<region>:<account-id>:alarmRule:<alarm_rule_id>
transfer	lts:<region>:<account-id>:transfer:<transfer_id>
hostGroup	lts:<region>:<account-id>:hostGroup:<host_group_id>

条件（Condition）

LTS服务不支持在SCP中的条件键中配置服务级的条件键。LTS可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.11.3 统一身份认证 IAM

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。

  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于IAM定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于IAM定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下IAM的相关操作。其中，不带V5后缀的授权项用于控制IAM旧版控制台的访问，带V5后缀的授权项用于控制IAM新版控制台的访问。

表 5-113 IAM 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
iam::listAccessKeys	授予列举永久访问密钥的权限。	list	-	-
iam::createAccessKey	授予创建永久访问密钥的权限。	write	-	-
iam::getAccessKey	授予查询永久访问密钥的权限。	read	-	-
iam::updateAccessKey	授予修改永久访问密钥的权限。	write	-	-
iam::deleteAccessKey	授予删除永久访问密钥的权限。	write	-	-
iam:projects:list	授予列举项目的权限。	list	-	-
iam:projects:create	授予创建项目的权限。	write	-	-
iam:projects:listForUser	授予列举指定用户项目的权限。	list	-	-
iam:projects:update	授予修改项目的权限。	write	-	-
iam:groups:list	授予列举用户组的权限。	list	-	-
iam:groups:create	授予创建用户组的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
iam:groups:get	授予查询用户组的权限。	read	-	-
iam:groups:delete	授予删除用户组的权限。	write	-	-
iam:groups:update	授予修改用户组的权限。	write	-	-
iam:groups:removeUser	授予从用户组中移除用户的权限。	write	-	-
iam:groups:listUsers	授予列举指定用户组中用户的权限。	list	-	-
iam:groups:checkUser	授予查询用户是否在用户组中的权限。	read	-	-
iam:groups:addUser	授予添加用户到用户组的权限。	write	-	-
iam:users:create	授予创建用户的权限。	write	-	-
iam:users:get	授予查询用户的权限。	read	-	-
iam:users:update	授予修改用户的权限。	write	-	-
iam:users:list	授予列举用户的权限。	list	-	-
iam:users:delete	授予删除用户的权限。	write	-	-
iam:users:listGroups	授予列举指定用户所属用户组的权限。	list	-	-
iam:users:listVirtualMFADevices	授予列举指定用户所属虚拟MFA设备的权限。	list	-	-
iam:users:createVirtualMFADevice	授予创建虚拟MFA设备密钥的权限。	write	-	-
iam:users:deleteVirtualMFADevice	授予删除虚拟MFA设备的权限。	write	-	-
iam:users:getVirtualMFADevice	授予查询虚拟MFA设备的权限。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
iam:users:bindVirtualMFADevice	授予绑定虚拟MFA设备的权限。	write	-	-
iam:users:unbindVirtualMFADevice	授予解绑虚拟MFA设备的权限。	write	-	-
iam:identityProviders:list	授予列举身份提供商的权限。	list	-	-
iam:identityProviders:get	授予查询身份提供商的权限。	read	-	-
iam:identityProviders:create	授予创建身份提供商的权限。	write	-	-
iam:identityProviders:delete	授予删除身份提供商的权限。	write	-	-
iam:identityProviders:update	授予修改身份提供商的权限。	write	-	-
iam:identityProviders:listMappings	授予列举身份提供商映射关系的权限。	list	-	-
iam:identityProviders:getMapping	授予查询身份提供商映射关系的权限。	read	-	-
iam:identityProviders:createMapping	授予创建身份提供商映射关系的权限。	write	-	-
iam:identityProviders:deleteMapping	授予删除身份提供商映射关系的权限。	write	-	-
iam:identityProviders:updateMapping	授予修改身份提供商映射关系的权限。	write	-	-
iam:identityProviders:listProtocols	授予列举身份提供商协议的权限。	list	-	-
iam:identityProviders:getProtocol	授予查询身份提供商协议的权限。	read	-	-
iam:identityProviders:createProtocol	授予创建身份提供商协议的权限。	write	-	-
iam:identityProviders:deleteProtocol	授予删除身份提供商协议的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
iam:identityProviders:updateProtocol	授予修改身份提供商协议的权限。	write	-	-
iam:identityProviders:getSAMLMetadata	授予查询身份提供商SAML metadata文件的权限。	read	-	-
iam:identityProviders:createSAMLMetadata	授予创建身份提供商SAML metadata文件的权限。	write	-	-
iam:identityProviders:getOIDCConfig	授予查询身份提供商OIDC配置的权限。	read	-	-
iam:identityProviders:createOIDCConfig	授予创建身份提供商OIDC配置的权限。	write	-	-
iam:identityProviders:updateOIDCConfig	授予修改身份提供商OIDC配置的权限。	write	-	-
iam:securityPolicies:getProtectPolicy	授予查询操作保护策略的权限。	read	-	-
iam:securityPolicies:updateProtectPolicy	授予修改操作保护策略的权限。	write	-	-
iam:securityPolicies:getPasswordPolicy	授予查询密码策略的权限。	read	-	-
iam:securityPolicies:updatePasswordPolicy	授予修改密码策略的权限。	write	-	-
iam:securityPolicies:getLoginPolicy	授予查询登录策略的权限。	read	-	-
iam:securityPolicies:updateLoginPolicy	授予修改登录策略的权限。	write	-	-
iam:securityPolicies:getConsoleAclPolicy	授予查询控制台访问策略的权限。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
iam:securityPolicies:updateConsoleAclPolicy	授予修改控制台访问策略的权限。	write	-	-
iam:securityPolicies:getApiAclPolicy	授予查询接口访问策略的权限。	read	-	-
iam:securityPolicies:updateApiAclPolicy	授予修改接口访问策略的权限。	write	-	-
iam:users:listLoginProtectSettings	授予列举租户下用户登录保护设置的权限。	list	-	-
iam:users:getLoginProtectSetting	授予查询登录保护设置的权限。	read	-	-
iam:users:updateLoginProtectSetting	授予修改登录保护设置的权限。	write	-	-
iam:quotas:list	授予列举配额的权限。	list	-	-
iam:quotas:listForProject	授予查询项目配额的权限。	list	-	-
iam:agencies:pass	授予向云服务传递委托的权限。	permission_management	agency *	-
iam:roles:list	授予查询权限列表的权限。	list	-	-
iam:roles:get	授予查询权限详情的权限。	read	-	-
iam::listRoleAssignments	授予查询租户授权记录的权限。	list	-	-
iam:groups:listRolesOnDomain	授予查询全局服务中用户组权限的权限。	list	-	-
iam:groups:listRolesOnProject	授予查询项目服务中用户组权限的权限。	list	-	-
iam:groups:grantRoleOnDomain	授予为用户组授予全局服务权限的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
iam:groups:grantRoleOnProject	授予为用户组授予项目级服务权限的权限。	write	-	-
iam:groups:checkRoleOnDomain	授予查询用户组是否拥有全局服务权限的权限。	read	-	-
iam:groups:checkRoleOnProject	授予查询用户组是否拥有项目服务权限的权限。	read	-	-
iam:groups:listRoles	授予查询用户组的所有权限的权限。	list	-	-
iam:groups:checkRole	授予查询用户组是否拥有指定权限的权限。	read	-	-
iam:groups:revokeRole	授予移除用户组指定权限的权限。	write	-	-
iam:groups:revokeRoleOnDomain	授予移除用户组的全局服务权限的权限。	write	-	-
iam:groups:revokeRoleOnProject	授予移除用户组的项目服务权限的权限。	write	-	-
iam:groups:grantRole	授予为用户组授予指定权限的权限。	write	-	-
iam:roles:create	授予创建自定义策略的权限。	write	-	-
iam:roles:update	授予修改自定义策略的权限。	write	-	-
iam:roles:delete	授予删除自定义策略的权限。	write	-	-
iam:agencies:list	授予列出委托的权限。	list	-	-
iam:agencies:get	授予查询指定委托详情的权限。	read	-	-
iam:agencies:create	授予创建委托的权限。	write	-	-
iam:agencies:update	授予修改委托的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
iam:agencies:delete	授予删除委托的权限。	write	-	-
iam:agencies:listRolesOnDomain	授予查询委托拥有的全局服务权限的权限。	list	-	-
iam:agencies:listRolesOnProject	授予查询委托拥有的指定项目权限的权限。	list	-	-
iam:agencies:grantRoleOnDomain	授予为委托授予全局服务权限的权限。	write	-	-
iam:agencies:grantRoleOnProject	授予为委托授予项目服务权限的权限。	write	-	-
iam:agencies:checkRoleOnDomain	授予查询委托是否拥有全局服务权限的权限。	read	-	-
iam:agencies:checkRoleOnProject	授予查询委托是否拥有项目服务权限的权限。	read	-	-
iam:agencies:revokeRoleOnDomain	授予移除委托的全局服务权限的权限。	write	-	-
iam:agencies:revokeRoleOnProject	授予移除委托的项目服务权限的权限。	write	-	-
iam:agencies:listRoles	授予查询委托的所有权限的权限。	list	-	-
iam:agencies:grantRole	授予为委托授予指定权限的权限。	write	-	-
iam:agencies:checkRole	授予查询委托是否拥有指定权限的权限。	read	-	-
iam:agencies:revokeRole	授予移除委托的指定权限的权限。	write	-	-
iam::listGroupsAssignedEnterpriseProject	授予查询企业项目关联的用户组的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
iam:groups:listRolesOnEnterpriseProject	授予查询企业项目已关联用户组的权限的权限。	list	-	-
iam:groups:grantRoleOnEnterpriseProject	授予基于用户组为企业项目授权的权限。	write	-	-
iam:groups:revokeRoleOnEnterpriseProject	授予删除企业项目关联的用户组权限的权限。	write	-	-
iam:groups:listAssignedEnterpriseProjects	授予查询用户组直接关联的企业项目的权限。	list	-	-
iam:users:listAssignedEnterpriseProjects	授予查询用户直接关联的企业项目的权限。	list	-	-
iam::listUsersAssignedEnterpriseProject	授予查询企业项目直接关联用户的权限。	list	-	-
iam:users:listRolesOnEnterpriseProject	授予查询企业项目直接关联用户权限的权限。	list	-	-
iam:users:grantRoleOnEnterpriseProject	授予基于用户为企业项目授权的权限。	write	-	-
iam:users:revokeRoleOnEnterpriseProject	授予删除企业项目直接关联用户的权限的权限。	write	-	-
iam:agencies:grantRoleOnEnterpriseProject	授予基于委托为企业项目授权的权限。	write	-	-
iam:agencies:revokeRoleOnEnterpriseProject	授予删除企业项目关联的委托的权限的权限。	write	-	-
iam:mfa:listVirtualMFADevicesV5	授予列举虚拟MFA设备的权限。	list	mfa *	-
iam:mfa:createVirtualMFADeviceV5	授予创建虚拟MFA设备的权限。	write	mfa *	-
iam:mfa:deleteVirtualMFADeviceV5	授予删除虚拟MFA设备的权限。	write	mfa *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
iam:mfa:enableV5	授予启用虚拟MFA设备的权限。	write	mfa *	-
iam:mfa:disableV5	授予禁用虚拟MFA设备的权限。	write	mfa *	-
iam:securitypolicies:getPasswordPolicyV5	授予获取密码策略信息的权限。	read	-	-
iam:securitypolicies:updatePasswordPolicyV5	授予修改密码策略的权限。	write	-	-
iam:securitypolicies:getLoginPolicyV5	授予获取登录策略信息的权限。	read	-	-
iam:securitypolicies:updateLoginPolicyV5	授予修改登录策略的权限。	write	-	-
iam:credentials:listCredentialsV5	授予权限以列举IAM用户的永久访问密钥。	list	user *	g:ResourceTag/<tag-key>
iam:credentials:showAccessKeyLastUsedV5	授予获取指定永久访问密钥最后一次使用时间的权限。	read	user *	g:ResourceTag/<tag-key>
iam:credentials:createCredentialV5	授予为IAM用户创建永久访问密钥的权限。	write	user *	g:ResourceTag/<tag-key>
iam:credentials:updateCredentialV5	授予为IAM用户修改永久访问密钥的权限。	write	user *	g:ResourceTag/<tag-key>
iam:credentials:deleteCredentialV5	授予为IAM用户删除永久访问密钥的权限。	write	user *	g:ResourceTag/<tag-key>
iam:users:changePasswordV5	授予IAM用户修改自己密码的权限。	write	user *	g:ResourceTag/<tag-key>
iam:users:showLoginProfileV5	授予获取IAM用户登录信息的权限。	read	user *	g:ResourceTag/<tag-key>
iam:users:createLoginProfileV5	授予为IAM用户创建登录信息的权限。	write	user *	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
iam:users:updateLoginProfileV5	授予为IAM用户修改登录信息的权限。	write	user *	g:ResourceTag/<tag-key>
iam:users:deleteLoginProfileV5	授予为IAM用户删除登录信息的权限。	write	user *	g:ResourceTag/<tag-key>
iam:users:listUsersV5	授予列举IAM用户的权限。	list	user *	-
iam:users:getUserV5	授予获取IAM用户信息的权限。	read	user *	g:ResourceTag/<tag-key>
iam:users:showUserLastLoginV5	授予获取IAM用户最后一次登录时间的权限。	read	user *	g:ResourceTag/<tag-key>
iam:users:createUserV5	授予创建IAM用户的权限。	write	user *	-
iam:users:updateUserV5	授予修改IAM用户的权限。	write	user *	g:ResourceTag/<tag-key>
iam:users:deleteUserV5	授予删除IAM用户的权限。	write	user *	g:ResourceTag/<tag-key>
iam:groups:listGroupsV5	授予列举用户组的权限。	list	group *	-
iam:groups:getGroupV5	授予获取用户组信息的权限。	read	group *	-
iam:groups:createGroupV5	授予创建用户组的权限。	write	group *	-
iam:groups:updateGroupV5	授予修改用户组的权限。	write	group *	-
iam:groups:deleteGroupV5	授予删除用户组的权限。	write	group *	-
iam:permissions:addUserToGroupV5	授予添加IAM用户到用户组的权限。	write	group *	-
iam:permissions:removeUserFromGroupV5	授予从用户组中移除IAM用户的权限。	write	group *	-
iam:policies:listV5	授予列举身份策略的权限。	list	policy *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
iam:policies:getV5	授予获取身份策略信息的权限。	read	policy *	-
iam:policies:createV5	授予创建自定义身份策略的权限。	permission_management	policy *	-
iam:policies:deleteV5	授予删除自定义身份策略的权限。	permission_management	policy *	-
iam:policies:listVersionsV5	授予列举身份策略版本的权限。	list	policy *	-
iam:policies:getVersionV5	授予获取身份策略版本信息的权限。	read	policy *	-
iam:policies:createVersionV5	授予为自定义身份策略创建新版本的权限。	permission_management	policy *	-
iam:policies:deleteVersionV5	授予为自定义身份策略删除版本的权限。	permission_management	policy *	-
iam:policies:setDefaultVersionV5	授予设置自定义身份策略默认版本的权限。	permission_management	policy *	-
iam:agencies:attachPolicyV5	授予为委托或信任委托附加身份策略的权限。	permission_management	agency *	g:ResourceTag/<tag-key>
			-	iam:PolicyURN
iam:groups:attachPolicyV5	授予为用户组附加身份策略的权限。	permission_management	group *	-
			-	iam:PolicyURN
iam:users:attachPolicyV5	授予为IAM用户附加身份策略的权限。	permission_management	user *	g:ResourceTag/<tag-key>
			-	iam:PolicyURN

授权项	描述	访问级别	资源类型（*为必须）	条件键
iam:agencies:detachPolicyV5	授予为委托或信任委托分离身份策略的权限。	permission_management	agency *	g:ResourceTag/<tag-key>
			-	iam:PolicyURN
iam:groups:detachPolicyV5	授予为用户组分离身份策略的权限。	permission_management	group *	-
			-	iam:PolicyURN
iam:users:detachPolicyV5	授予为IAM用户分离身份策略的权限。	permission_management	user *	g:ResourceTag/<tag-key>
			-	iam:PolicyURN
iam:policies:listEntitiesV5	授予权限以列举附加在身份策略上的所有实体。	list	policy *	-
iam:agencies:listAttachedPoliciesV5	授予权限以列举委托或信任委托附加的身份策略。	list	agency *	g:ResourceTag/<tag-key>
iam:groups:listAttachedPoliciesV5	授予权限以列举用户组附加的身份策略。	list	group *	-
iam:users:listAttachedPoliciesV5	授予权限以列举IAM用户附加的身份策略。	list	user *	g:ResourceTag/<tag-key>
iam:agencies:createServiceLinkedAgencyV5	授予创建服务关联委托的权限以允许云服务代表您执行操作。	write	agency *	-
			-	iam:ServicePrincipal
iam:agencies:deleteServiceLinkedAgencyV5	授予删除服务关联委托的权限。	write	agency *	g:ResourceTag/<tag-key>
			-	iam:ServicePrincipal
iam:agencies:getServiceLinkedAgencyDeletionStatusV5	授予获取服务关联委托删除状态的权限。	read	agency *	-
iam:agencies:listV5	授予列举委托及信任委托的权限。	list	agency *	-
iam:agencies:getV5	授予获取委托或信任委托信息的权限。	read	agency *	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
iam:agencies:createV5	授予创建信任委托的权限。	write	agency *	-
iam:agencies:updateV5	授予修改信任委托的权限。	write	agency *	g:ResourceTag/<tag-key>
iam:agencies:deleteV5	授予删除信任委托的权限。	write	agency *	g:ResourceTag/<tag-key>
iam:agencies:updateTrustPolicyV5	授予修改信任委托信任策略的权限。	write	agency *	g:ResourceTag/<tag-key>
iam::listTagsForResourceV5	授予列举资源标签的权限。	list	agency	g:ResourceTag/<tag-key>
			user	g:ResourceTag/<tag-key>
iam::tagForResourceV5	授予设置资源标签的权限。	tagging	agency	g:ResourceTag/<tag-key>
			user	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
iam::untagForResourceV5	授予删除资源标签的权限。	tagging	agency	g:ResourceTag/<tag-key>
			user	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
iam::getAccountSummaryV5	授予获取此账号中IAM实体使用情况和IAM配额的摘要信息的权限。	list	-	-
iam::getAsymmetricSignatureSwitchV5	授予获取临时令牌非对称签名开关状态的权限。	read	-	-
iam::setAsymmetricSignatureSwitchV5	授予设置临时令牌非对称签名开关状态的权限。	write	-	-

IAM的API通常对应着一个或多个授权项。表5-114展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-114 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3.0/OS-CREDENTIAL/credentials	iam::listAccessKeys	-
POST /v3.0/OS-CREDENTIAL/credentials	iam::createAccessKey	-
GET /v3.0/OS-CREDENTIAL/credentials/{access_key}	iam::getAccessKey	-
PUT /v3.0/OS-CREDENTIAL/credentials/{access_key}	iam::updateAccessKey	-
DELETE /v3.0/OS-CREDENTIAL/credentials/{access_key}	iam::deleteAccessKey	-
GET /v3.0/OS-QUOTA/domains/{domain_id}	iam:quotas:list	-
GET /v3.0/OS-QUOTA/projects/{project_id}	iam:quotas:listForProject	-
GET /v3/projects	iam:projects:list	-
POST /v3/projects	iam:projects:create	-
GET /v3/users/{user_id}/projects	iam:projects:listForUser	-
PATCH /v3/projects/{project_id}	iam:projects:update	-
PUT /v3-ext/projects/{project_id}	iam:projects:update	-
GET /v3/groups	iam:groups:list	-
POST /v3/groups	iam:groups:create	-
GET /v3/groups/{group_id}	iam:groups:get	-

API	对应的授权项	依赖的授权项
DELETE /v3/groups/{group_id}	iam:groups:delete	-
PATCH /v3/groups/{group_id}	iam:groups:update	-
GET /v3/groups/{group_id}/users	iam:groups:listUsers	-
HEAD /v3/groups/{group_id}/users/{user_id}	iam:groups:checkUser	-
PUT /v3/groups/{group_id}/users/{user_id}	iam:groups:addUser	-
DELETE /v3/groups/{group_id}/users/{user_id}	iam:groups:removeUser	-
POST /v3.0/OS-USER/users	iam:users:create	-
GET /v3.0/OS-USER/users/{user_id}	iam:users:get	-
PUT /v3.0/OS-USER/users/{user_id}	iam:users:update	-
PUT /v3.0/OS-USER/users/{user_id}/info	iam:users:update	-
GET /v3/users	iam:users:list	-
POST /v3/users	iam:users:create	-
GET /v3/users/{user_id}	iam:users:get	-
DELETE /v3/users/{user_id}	iam:users:delete	-
PATCH /v3/users/{user_id}	iam:users:update	-
GET /v3/users/{user_id}/groups	iam:users:listGroups	-
GET /v3.0/OS-MFA/virtual-mfa-devices	iam:users:listVirtualMFADevices	-

API	对应的授权项	依赖的授权项
POST /v3.0/OS-MFA/virtual-mfa-devices	iam:users:createVirtualMFADevice	-
DELETE /v3.0/OS-MFA/virtual-mfa-devices	iam:users:deleteVirtualMFADevice	-
GET /v3.0/OS-MFA/users/{user_id}/virtual-mfa-device	iam:users:getVirtualMFADevice	-
PUT /v3.0/OS-MFA/mfa-devices/bind	iam:users:bindVirtualMFADevice	-
PUT /v3.0/OS-MFA/mfa-devices/unbind	iam:users:unbindVirtualMFADevice	-
GET /v3.0/OS-USER/login-protects	iam:users:listLoginProtectSettings	-
GET /v3.0/OS-USER/users/{user_id}/login-protect	iam:users:getLoginProtectSetting	-
PUT /v3.0/OS-USER/users/{user_id}/login-protect	iam:users:updateLoginProtectSetting	-
GET /v3/OS-FEDERATION/identity_providers	iam:identityProviders:list	-
GET /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:get	-
PUT /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:create	-
DELETE /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:delete	-
PATCH /v3/OS-FEDERATION/identity_providers/{id}	iam:identityProviders:update	-

API	对应的授权项	依赖的授权项
GET /v3/OS-FEDERATION/mappings	iam:identityProviders:listMappings	-
GET /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:getMapping	-
PUT /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:createMapping	-
DELETE /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:deleteMapping	-
PATCH /v3/OS-FEDERATION/mappings/{id}	iam:identityProviders:updateMapping	-
GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols	iam:identityProviders:listProtocols	-
GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:getProtocol	-
PUT /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:createProtocol	-
DELETE /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:deleteProtocol	-
PATCH /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:updateProtocol	-

API	对应的授权项	依赖的授权项
GET /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata	iam:identityProviders:getSAMLMetadata	-
POST /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata	iam:identityProviders:createSAMLMetadata	-
GET /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config	iam:identityProviders:getOIDCConfig	-
POST /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config	iam:identityProviders:createOIDCConfig	-
PUT /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config	iam:identityProviders:updateOIDCConfig	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy	iam:securityPolicies:getProtectPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy	iam:securityPolicies:updateProtectPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy	iam:securityPolicies:getPasswordPolicy	-

API	对应的授权项	依赖的授权项
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy	iam:securityPolicies:updatePasswordPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy	iam:securityPolicies:getLoginPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy	iam:securityPolicies:updateLoginPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy	iam:securityPolicies:getConsoleAclPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy	iam:securityPolicies:updateConsoleAclPolicy	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy	iam:securityPolicies:getApiAclPolicy	-
PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy	iam:securityPolicies:updateApiAclPolicy	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-115**中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

IAM定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-115 IAM 支持的资源类型

资源类型	URN
policy	iam::<account-id>:policy:<policy-name-with-path>
agency	iam::<account-id>:agency:<agency-name-with-path>
user	iam::<account-id>:user:<user-name>
group	iam::<account-id>:group:<group-name>
mfa	iam::<account-id>:mfa:<mfa-name>

条件（Condition）

条件（Condition）是自定义SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀为服务缩写，如iam:）仅适用于对应服务的操作，详情请参见表5-116。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
- 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，SCP才能生效。支持的运算符请参见：运算符。

IAM定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-116 IAM 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
iam:PolicyURN	string	单值	按照身份策略的URN筛选访问权限。
iam:ServicePrincipal	string	单值	按照服务关联委托传递的云服务对应的服务标识筛选访问权限。

5.10.11.4 安全令牌服务 STS

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于STS定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于STS定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下STS的相关操作。

表 5-117 STS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
sts:agencies:assume	授予权限以获取一组可用来访问您通常无法访问的资源的临时安全凭证。	write	agency *	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	• sts:ExternalId • sts:SourceIdentity • sts:TransitiveTagKeys • sts:AgencySessionName • g:RequestTag/<tag-key> • g:TagKeys • g:SourceAccount • g:SourceUrn
sts::decodeAuthorizationMessage	授予权限以从为响应请求而返回的编码消息中解码有关请求授权状态的其他信息。	write	-	-
sts::setSourceIdentity	授予在 STS 会话上设置源身份的权限。	write	agency *	g:ResourceTag/<tag-key>
			-	sts:SourceIdentity
sts::tagSession	授予权限以将标签添加至 STS 会话。	tagging	agency *	g:ResourceTag/<tag-key>
			-	• sts:TransitiveTagKeys • g:RequestTag/<tag-key> • g:TagKeys
sts::getServiceBearerToken	授予权限获取一个绑定至某服务的 Bearer Token。	write	-	• sts:DurationTimes • sts:ServiceName

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-118**中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

STS定义了以下可以在自定义SCP的Resource元素中使用的资源类型。

表 5-118 STS 支持的资源类型

资源类型	URN
agency	iam::<account-id>:agency:<agency-name-with-path>
assumed-agency	sts::<account-id>:assumed-agency:<agency-name>/<session-name>

条件（Condition）

条件（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀通常为服务缩写，如sts:）仅适用于对应服务的操作，详情请参见表4。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
- 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，SCP才能生效。支持的运算符请参见：运算符。

STS定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-119 STS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
sts:ExternalId	string	单值	按您代入另一个账户中的角色时所需的唯一标识符筛选访问权限。
sts:SourceIdentity	string	单值	按照在请求中传递的源身份筛选访问权限。
sts:TransitiveTagKeys	string	多值	按照在请求中传递的可传递标签键筛选访问权限。
sts:AgencySessionName	string	单值	按您代入角色时所需的角色会话名称筛选访问权限。

服务级条件键	类型	单值/多值	说明
sts:DurationTimes	numeric	单值	按照创建 Bearer Token 的持续时间筛选访问权限。
sts:ServiceName	string	单值	按照创建 Bearer Token 的服务名筛选访问权限。

5.10.11.5 资源编排服务 RFS

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于资源编排服务 （RFS）定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于资源编排服务 （RFS）定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下资源编排服务 （RFS）的相关操作。

表 5-120 资源编排服务 （ RFS ）支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
rf:privateTemplate:list	授予权限列举project下所有的私有模板。	list	privateTemplate *	-
rf:privateTemplate:create	授予权限创建私有模板。	write	privateTemplate *	-
rf:privateTemplate:delete	授予权限删除私有模板。	write	privateTemplate *	-
rf:privateTemplate:showMetadata	授予权限展示私有模板的信息。	read	privateTemplate *	-
rf:privateTemplate:updateMetadata	授予权限更新私有模板元数据。	write	privateTemplate *	-
rf:privateTemplate:listVersions	授予权限展示私有模板下所有模板版本信息。	list	privateTemplate *	-
rf:privateTemplate:createVersion	授予权限创建新的私有模板版本。	write	privateTemplate *	-
rf:privateTemplate:showVersionContent	授予权限获取私有模板的版本内容。	read	privateTemplate *	-
rf:privateTemplate:deleteVersion	授予权限删除私有模板的版本。	write	privateTemplate *	-
rf:privateTemplate:showVersionMetadata	授予权限获取私有模板版本的元数据。	read	privateTemplate *	-
rf:stack:create	授予权限创建堆栈。	write	stack *	-
rf:stack:deploy	授予权限部署堆栈。	write	stack *	-
rf:stack:list	授予权限查询堆栈列表。	list	stack *	-
rf:stack:getMetadata	授予权限获取堆栈元数据信息。	read	stack *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
rf:stack:delete	授予权限删除堆栈。	write	stack *	-
rf:stack:getTemplate	授予权限获取堆栈模板。	read	stack *	-
rf:stack:listEvents	授予权限查询堆栈部署事件列表。	list	stack *	-
rf:stack:listResources	授予权限查询堆栈资源信息列表。	list	stack *	-
rf:stack:listOutputs	授予权限查询堆栈输出列表。	list	stack *	-
rf:stack:createExecutionPlan	授予权限创建执行计划。	write	stack *	-
rf:stack:getExecutionPlanMetadata	授予权限获取执行计划元数据信息。	read	stack *	-
rf:stack:getExecutionPlan	授予权限获取执行计划信息。	read	stack *	-
rf:stack:applyExecutionPlan	授予权限应用执行计划。	write	stack *	-
rf:stack:listExecutionPlans	授予权限查询执行计划信息列表。	list	stack *	-
rf:stack:deleteExecutionPlan	授予权限删除执行计划。	write	stack *	-
rf:stack:continueRollback	授予权限继续回滚堆栈。	write	stack *	-
rf:stack:continueDeploy	授予权限继续部署堆栈。	write	stack *	-
rf:stack:estimateExecutionPlanPrice	授予权限预估执行计划价格。	read	stack *	-
rf:stack:update	授予权限更新堆栈。	write	stack *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
rf:stackSet:create	授予权限创建资源栈集。	write	stackSet *	-
rf:stackSet:list	授予权限查询资源栈集列表。	list	stackSet *	-
rf:stackSet:showTemplate	授予权限获取资源栈集模板。	read	stackSet *	-
rf:stackSet:showMetadata	授予权限获取资源栈集元数据信息。	read	stackSet *	-
rf:stackSet:deploy	授予权限部署资源栈集。	write	stackSet *	-
rf:stackSet:delete	授予权限删除资源栈集。	write	stackSet *	-
rf:stackSet:update	授予权限更新资源栈集。	write	stackSet *	-
rf:stackSet:listStackInstances	授予权限查询资源栈实例列表。	list	stackSet *	-
rf:stackSet:createStackInstances	授予权限创建资源栈实例。	write	stackSet *	-
rf:stackSet:deleteStackInstances	授予权限删除资源栈实例。	write	stackSet *	-
rf:stackSet:showOperationMetadata	授予权限获取资源栈集操作元数据信息。	read	stackSet *	-
rf:stackSet:listOperations	授予权限查询资源栈集操作信息列表。	list	stackSet *	-

资源编排服务（RFS）的API通常对应着一个或多个授权项。**表5-121**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-121 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/templates	rf:privateTemplate:list	-
POST /v1/{project_id}/templates	rf:privateTemplate:create	-
DELETE /v1/{project_id}/templates/{template_name}	rf:privateTemplate:delete	-
GET /v1/{project_id}/templates/{template_name}/metadata	rf:privateTemplate:showMetadata	-
PATCH /v1/{project_id}/templates/{template_name}/metadata	rf:privateTemplate:updateMetadata	-
GET /v1/{project_id}/templates/{template_name}/versions	rf:privateTemplate:listVersions	-
POST /v1/{project_id}/templates/{template_name}/versions	rf:privateTemplate:createVersion	-
GET /v1/{project_id}/templates/{template_name}/versions/{version_id}	rf:privateTemplate:showVersionContent	-
DELETE /v1/{project_id}/templates/{template_name}/versions/{version_id}	rf:privateTemplate:deleteVersion	-
GET /v1/{project_id}/templates/{template_name}/versions/{version_id}/metadata	rf:privateTemplate:showVersionMetadata	-
POST /v1/{project_id}/stacks	rf:stack:create	• kms:cmk:decryptDataKey • iam:agencies:pass

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/stacks/{stack_name}/deployments	rf:stack:deploy	kms:cmk:decryptDataKey
GET /v1/{project_id}/stacks	rf:stack:list	-
GET /v1/{project_id}/stacks/{stack_name}/metadata	rf:stack:getMetadata	-
DELETE /v1/{project_id}/stacks/{stack_name}	rf:stack:delete	-
GET /v1/{project_id}/stacks/{stack_name}/templates	rf:stack:getTemplate	-
GET /v1/{project_id}/stacks/{stack_name}/events	rf:stack:listEvents	-
GET /v1/{project_id}/stacks/{stack_name}/resources	rf:stack:listResources	-
GET /v1/{project_id}/stacks/{stack_name}/outputs	rf:stack:listOutputs	-
POST /v1/{project_id}/stacks/{stack_name}/execution-plans	rf:stack:createExecutionPlan	kms:cmk:decryptDataKey
GET /v1/{project_id}/stacks/{stack_name}/execution-plans/{execution_plan_name}/metadata	rf:stack:getExecutionPlanMetadata	-
GET /v1/{project_id}/stacks/{stack_name}/execution-plans/{execution_plan_name}	rf:stack:getExecutionPlan	-
POST /v1/{project_id}/stacks/{stack_name}/execution-plans/{execution_plan_name}	rf:stack:applyExecutionPlan	-
GET /v1/{project_id}/stacks/{stack_name}/execution-plans	rf:stack:listExecutionPlans	-

API	对应的授权项	依赖的授权项
DELETE /v1/{project_id}/stacks/{stack_name}/execution-plans/{execution_plan_name}	rf:stack:deleteExecutionPlan	-
POST /v1/{project_id}/stacks/{stack_name}/rollbacks	rf:stack:continueRollback	-
POST /v1/{project_id}/stacks/{stack_name}/continuations	rf:stack:continueDeploy	-
GET /v1/{project_id}/stacks/{stack_name}/execution-plans/{execution_plan_name}/prices	rf:stack:estimateExecutionPlanPrice	bss:discount:view
PATCH /v1/{project_id}/stacks/{stack_name}	rf:stack:update	iam:agencies:pass
POST /v1/stack-sets	rf:stackSet:create	iam:agencies:pass
GET /v1/stack-sets	rf:stackSet:list	-
GET /v1/stack-sets/{stack_set_name}/templates	rf:stackSet:showTemplate	-
GET /v1/stack-sets/{stack_set_name}/metadata	rf:stackSet:showMetadata	-
POST /v1/stack-sets/{stack_set_name}/deployments	rf:stackSet:deploy	-
DELETE /v1/stack-sets/{stack_set_name}	rf:stackSet:delete	-
PATCH /v1/stack-sets/{stack_set_name}	rf:stackSet:update	iam:agencies:pass
GET /v1/stack-sets/{stack_set_name}/stack-instances	rf:stackSet:listStackInstances	-
GET /v1/stack-sets/{stack_set_name}/operations/{stack_set_operation_id}/metadata	rf:stackSet:showOperationMetadata	-

API	对应的授权项	依赖的授权项
GET /v1/stack-sets/{stack_set_name}/operations	rf:stackSet:listOperations	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表3中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

资源编排服务 （RFS）定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-122 资源编排服务 （RFS）支持的资源类型

资源类型	URN
privateTemplate	rf:<region>:<account-id>:privateTemplate:<template-name>
stack	rf:<region>:<account-id>:stack:<stack-name>
stackSet	rf:<region>:<account-id>:stackSet:<stack-set-name>/<stack-set-id>

条件（Condition）

资源编排服务 （RFS）服务不支持在SCP中的条件键中配置服务级的条件键。

资源编排服务 （RFS）可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.11.6 IAM 身份中心

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在策略语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于IAM身份中心定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于IAM身份中心定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下IAM身份中心的相关操作。

表 5-123 IAM 身份中心支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
IdentityCenter:permissionSet:create	授予创建权限集的权限。	write	instance *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
IdentityCenter:permissionSet:attachManagedPolicy	授予将系统身份策略添加到权限集的权限。	permission_management	instance *	-
			permissionSet *	-
IdentityCenter:permissionSet:detachManagedPolicy	授予从指定权限集中分离添加的系统身份策略的权限。	permission_management	instance *	-
			permissionSet *	-
IdentityCenter:permissionSet:update	授予更新指定实例的权限集的权限。	permission_management	instance *	-
			permissionSet *	-
IdentityCenter:permissionSet:delete	授予删除指定实例的权限集的权限。	write	instance *	-
			permissionSet *	-

授权项	描述	访问级别	资源类型（* 为必须）	条件键
IdentityCenter:permissionSet:list	授予列出指定实例的权限集的权限。	list	instance *	-
IdentityCenter:permissionSet:listAccountsForProvisioned	授予列出指定权限集已授权的所有账号的权限。	list	permissionSet *	-
			instance *	-
IdentityCenter:permissionSet:listProvisioningStatus	授予列出指定实例的权限集授权请求的处理状态的权限。	list	instance *	-
IdentityCenter:permissionSet:listManagedPolicies	授予列出添加到指定权限集的系统身份策略的权限。	list	instance *	-
			permissionSet *	-
IdentityCenter:permissionSet:listProvisionedToAccount	授予列出授权给指定账号的所有权限集的权限。	list	account *	-
			instance *	-
IdentityCenter:permissionSet:describeProvisioningStatus	授予获取权限集授权请求的处理状态详细信息的权限。	read	instance *	-
IdentityCenter:permissionSet:describe	授予获取指定实例的权限集详细信息的权限。	read	instance *	-
			permissionSet *	-
IdentityCenter:permissionSet:provision	授予将指定权限集授权给指定目标的权限。	write	account *	-
			instance *	-
			permissionSet *	-
IdentityCenter:instance:getIdentityCenterStatus	授予查询IAM身份中心服务状态的权限。	read	-	-
IdentityCenter:instance:registerRegion	授予注册region的权限。	write	-	-
IdentityCenter:instance:describeRegisteredRegions	授予查询IAM身份中心已开通的region的权限。	read	-	-

授权项	描述	访问级别	资源类型（* 为必须）	条件键
IdentityCenter:instance:startIdentityCenter	授予开通IAM身份中心的权限。	write	-	-
IdentityCenter:instance:deleteIdentityCenter	授予关闭IAM身份中心的权限。	write	-	-
IdentityCenter:instance:list	授予查询IAM身份中心实例列表的权限。	list	-	-
IdentityCenter:accountAssignment:create	授予使用指定权限集为指定账号分配对主体的访问权限的权限。	write	instance *	-
			account *	-
			permissionSet *	-
IdentityCenter:accountAssignment:delete	授予使用指定权限集从指定账号删除主体访问权限的权限。	write	instance *	-
			account *	-
			permissionSet *	-
IdentityCenter:accountAssignment:list	授予列出具有指定权限集的指定账号的受让人的权限。	list	instance *	-
			account *	-
			permissionSet *	-
IdentityCenter:accountAssignment:describeDeletionStatus	授予获取分配删除请求的处理状态详细信息的权限。	read	instance *	-
IdentityCenter:accountAssignment:describeCreationStatus	授予获取分配创建请求的处理状态详细信息的权限。	read	instance *	-
IdentityCenter:accountAssignment:listCreationStatus	授予列出指定IAM身份中心实例的账号分配创建请求的处理状态的权限。	list	instance *	-
IdentityCenter:accountAssignment:listDeletionStatus	授予列出指定IAM身份中心实例的账号分配删除请求的处理状态的权限。	list	instance *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
IdentityCenter:accountAssignment:listProfileAssociation	授予查询账号、权限集关联的所有用户或用户组的权限。	read	-	-
IdentityCenter:accountAssignment:disassociationProfile	授予解除用户或用户组绑定的所有授权的权限。	write	-	-
IdentityCenter:instance:listIdentityStoreAssociations	授予查询关联到IAM身份中心的身份源详细信息的权限。	read	-	-
IdentityCenter:ssoConfiguration:update	授予更新当前IAM身份中心实例配置的权限。	write	-	-
IdentityCenter:ssoConfiguration:describe	授予获取当前IAM身份中心实例配置的权限。	read	-	-
IdentityCenter:mfaDevices:describeManagementSettings	授予获取MFA管理设置信息的权限。	read	-	-
IdentityCenter:mfaDevices:updateManagementSettings	授予更新MFA管理设置信息的权限。	write	-	-
IdentityCenter:instance:createAlias	授予为指定的身份源创建别名的权限。	write	-	-
IdentityCenter:user:create	授予创建用户的权限。	write	-	-
IdentityCenter:user:list	授予查询用户列表的权限。	read	-	-
IdentityCenter:user:describe	授予查询用户详情的权限。	read	-	-
IdentityCenter:user:describeUsers	授予批量获取用户详情的权限。	read	-	-
IdentityCenter:user:update	授予更新用户的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
IdentityCenter:user:delete	授予删除用户的权限。	write	-	-
IdentityCenter:user:getUserId	授予获取用户ID的权限。	read	-	-
IdentityCenter:user:enableUser	授予启用用户的权限。	write	-	-
IdentityCenter:user:disableUser	授予停用用户的权限。	write	-	-
IdentityCenter:group:create	授予创建用户组的权限。	write	-	-
IdentityCenter:group:list	授予查询用户组列表的权限。	read	-	-
IdentityCenter:group:describe	授予查询用户组详情的权限。	read	-	-
IdentityCenter:group:describeGroups	授予批量获取用户组详情的权限。	read	-	-
IdentityCenter:group:update	授予更新用户组的权限。	write	-	-
IdentityCenter:group:delete	授予删除用户组的权限。	write	-	-
IdentityCenter:group:getGroupId	授予获取用户组Id的权限。	read	-	-
IdentityCenter:groupMembership:create	授予绑定用户与用户组的权限。	write	-	-
IdentityCenter:groupMemberships:list	授予查询用户组的所有成员的权限。	read	-	-
IdentityCenter:groupMembership:listForMember	授予查询用户加入的所有用户组的权限。	read	-	-
IdentityCenter:groupMembership:describe	授予查询绑定关系详情的权限。	read	-	-
IdentityCenter:groupMembership:delete	授予解绑用户和用户组的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
IdentityCenter:groupMembership:getGroupMembershipId	授予查询绑定关系ID的权限。	read	-	-
IdentityCenter:groupMembership:isMembershipInGroup	授予查询用户是否绑定在用户组的权限。	read	-	-
IdentityCenter:externalIdp:create	授予创建外部身份提供商的权限。	write	-	-
IdentityCenter:externalIdp:list	授予获取外部身份提供商身份源配置的权限。	read	-	-
IdentityCenter:externalIdp:enable	授予启用外部身份提供商的权限。	write	-	-
IdentityCenter:externalIdp:disable	授予停用外部身份提供商的权限。	write	-	-
IdentityCenter:externalIdp:getSpConfiguration	授予获取IAM身份中心服务提供商配置的权限。	read	-	-
IdentityCenter:externalIdp:update	授予更新外部身份提供商配置的权限。	write	-	-
IdentityCenter:externalIdp:delete	授予删除外部身份提供商配置的权限。	write	-	-
IdentityCenter:externalIdp:importCertificate	授予导入证书的权限。	write	-	-
IdentityCenter:externalIdp:deleteCertificate	授予删除证书的权限。	write	-	-
IdentityCenter:externalIdp:listCertificates	授予获取证书列表的权限。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
IdentityCenter:externalIdp:createProvisioningTenant	授予创建Tenant的权限。	write	-	-
IdentityCenter:externalIdp:listProvisioningTenant	授予查询Tenant列表的权限。	read	-	-
IdentityCenter:externalIdp:deleteProvisioningTenant	授予删除Tenant的权限。	write	-	-
IdentityCenter:externalIdp:createBearerToken	授予创建Bearer Token的权限。	write	-	-
IdentityCenter:externalIdp:listBearerTokens	授予查询Bearer Token列表的权限。	read	-	-
IdentityCenter:externalIdp:deleteBearerToken	授予删除Bearer Token的权限。	write	-	-
IdentityCenter:user:updatePassword	授予通过电子邮件发送密码重置链接或者生成一次性密码的方式为用户更新密码的权限。	write	-	-
IdentityCenter:user:deleteUserMfaDevice	授予为指定用户删除MFA设备的权限。	write	-	-
IdentityCenter:user:updateMfaDevice	授予更新MFA设备信息的权限。	write	-	-
IdentityCenter:user:listMfaDevice	授予查询MFA设备列表的权限。	read	-	-
IdentityCenter:user:registerVirtualMfaDevice	授予开始虚拟MFA设备创建过程的权限。	write	-	-
IdentityCenter:user:verifyEmail	授予验证用户电子邮件地址的权限。	write	-	-

IAM身份中心的API通常对应着一个或多个授权项。表5-124展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-124 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/instances/{instance_id}/permission-sets	IdentityCenter:permissionSet:create	organizations:delegatedAdministrators:list
POST /v1/instances/{instance_id}/permission-sets/{permission_set_id}/attach-managed-policy	IdentityCenter:permissionSet:attachManagedPolicy	• iam:policies:get • organizations:delegatedAdministrators:list
POST /v1/instances/{instance_id}/permission-sets/{permission_set_id}/detach-managed-policy	IdentityCenter:permissionSet:detachManagedPolicy	organizations:delegatedAdministrators:list
PUT /v1/instances/{instance_id}/permission-sets/{permission_set_id}	IdentityCenter:permissionSet:update	organizations:delegatedAdministrators:list
DELETE /v1/instances/{instance_id}/permission-sets/{permission_set_id}	IdentityCenter:permissionSet:delete	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/permission-sets	IdentityCenter:permissionSet:list	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}/accounts	IdentityCenter:permissionSet:listAccountsForProvisioned	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/permission-sets/provisioning-statuses	IdentityCenter:permissionSet:listProvisioningStatus	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}/managed-policies	IdentityCenter:permissionSet:listManagedPolicies	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/permission-sets/provisioned-to-accounts	IdentityCenter:permissionSet:listProvisionedToAccount	organizations:delegatedAdministrators:list

API	对应的授权项	依赖的授权项
GET /v1/instances/{instance_id}/permission-sets/provisioning-status/{request_id}	IdentityCenter:permissionSet:describeProvisioningStatus	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}	IdentityCenter:permissionSet:describe	organizations:delegatedAdministrators:list
POST /v1/instances/{instance_id}/permission-sets/{permission_set_id}/provision	IdentityCenter:permissionSet:provision	organizations:delegatedAdministrators:list
GET /v1/instances	IdentityCenter:instance:list	organizations:delegatedAdministrators:list
POST /v1/instances/{instance_id}/account-assignments/create	IdentityCenter:accountAssignment:create	organizations:delegatedAdministrators:list
POST /v1/instances/{instance_id}/account-assignments/delete	IdentityCenter:accountAssignment:delete	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/account-assignments	IdentityCenter:accountAssignment:list	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/account-assignments/deletion-status/{request_id}	IdentityCenter:accountAssignment:describeDeletionStatus	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/account-assignments/creation-status/{request_id}	IdentityCenter:accountAssignment:describeCreationStatus	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/account-assignments/creation-statuses	IdentityCenter:accountAssignment:listCreationStatus	organizations:delegatedAdministrators:list
GET /v1/instances/{instance_id}/account-assignments/deletion-statuses	IdentityCenter:accountAssignment:listDeletionStatus	organizations:delegatedAdministrators:list
POST /v1/identity-stores/{identity_store_id}/users	IdentityCenter:user:create	organizations:delegatedAdministrators:list
GET /v1/identity-stores/{identity_store_id}/users	IdentityCenter:user:list	organizations:delegatedAdministrators:list

API	对应的授权项	依赖的授权项
GET /v1/identity-stores/{identity_store_id}/users/{user_id}	IdentityCenter:user:describe	organizations:delegatedAdministrators:list
PUT /v1/identity-stores/{identity_store_id}/users/{user_id}	IdentityCenter:user:update	organizations:delegatedAdministrators:list
DELETE /v1/identity-stores/{identity_store_id}/users/{user_id}	IdentityCenter:user:delete	organizations:delegatedAdministrators:list
POST /v1/identity-stores/{identity_store_id}/users/retrieve-user-id	IdentityCenter:user:getUserId	organizations:delegatedAdministrators:list
POST /v1/identity-stores/{identity_store_id}/groups	IdentityCenter:group:create	organizations:delegatedAdministrators:list
GET /v1/identity-stores/{identity_store_id}/groups	IdentityCenter:group:list	organizations:delegatedAdministrators:list
GET /v1/identity-stores/{identity_store_id}/groups/{group_id}	IdentityCenter:group:describe	organizations:delegatedAdministrators:list
PUT /v1/identity-stores/{identity_store_id}/groups/{group_id}	IdentityCenter:group:update	organizations:delegatedAdministrators:list
DELETE /v1/identity-stores/{identity_store_id}/groups/{group_id}	IdentityCenter:group:delete	organizations:delegatedAdministrators:list
POST /v1/identity-stores/{identity_store_id}/groups/retrieve-group-id	IdentityCenter:group:getGroupId	organizations:delegatedAdministrators:list
POST /v1/identity-stores/{identity_store_id}/group-memberships	IdentityCenter:groupMembership:create	organizations:delegatedAdministrators:list
GET /v1/identity-stores/{identity_store_id}/group-memberships	IdentityCenter:groupMemberships:list	organizations:delegatedAdministrators:list
GET /v1/identity-stores/{identity_store_id}/group-memberships-for-member	IdentityCenter:groupMembership:listForMember	organizations:delegatedAdministrators:list

API	对应的授权项	依赖的授权项
GET /v1/identity-stores/{identity_store_id}/group-memberships/{membership_id}	IdentityCenter:groupMembership:describe	organizations:delegatedAdministrators:list
DELETE /v1/identity-stores/{identity_store_id}/group-memberships/{membership_id}	IdentityCenter:groupMembership:delete	organizations:delegatedAdministrators:list
POST /v1/identity-stores/{identity_store_id}/group-memberships/retrieve-group-membership-id	IdentityCenter:groupMembership:getGroupMembershipId	organizations:delegatedAdministrators:list
POST /v1/identity-stores/{identity_store_id}/is-member-in-groups	IdentityCenter:groupMembership:isMembershipInGroup	organizations:delegatedAdministrators:list

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-125中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的策略语句中指定该资源的URN，策略仅作用于此资源；如未指定，Resource默认为“*”，则策略将应用到所有资源。您也可以在策略中设置条件，从而指定资源类型。

IAM身份中心定义了以下可以在策略的Resource元素中使用的资源类型。

表 5-125 IAM 身份中心支持的资源类型

资源类型	URN
instance	IdentityCenter::<management-account-id>:instance:<instance-id>
account	IdentityCenter::<management-account-id>:account:<account-id>
permissionSet	IdentityCenter::<management-account-id>:permissionSet:<instance-id>/<permission-set-id>

条件（Condition）

IAM身份中心服务不支持在SCP中的条件键中配置服务级的条件键。

IAM身份中心可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.11.7 组织 Organizations

Organizations服务中的服务控制策略（Service Control Policies，以下简称SCP）可以使用以下这些授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “访问级别”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “资源类型”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于Organizations定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

  关于Organizations定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下Organizations的相关操作。

表 5-126 Organizations 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
organizations:organizations:create	授予创建组织的权限。	write	-	-
organizations:organizations:get	授予查询所属组织信息的权限。	read	-	-
organizations:organizations:delete	授予删除组织的权限。	write	-	-
organizations:organizations:leave	授予离开当前组织的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
organizations:roots:list	授予列出组织的根的权限。	list	-	-
organizations:ous:create	授予创建组织单元的权限。	write	ou	g:ResourceTag/<tag-key>
			root	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
organizations:ous:list	授予列举组织单元的权限。	list	-	-
organizations:ous:get	授予查询有关组织单元的信息的权限。	read	ou *	g:ResourceTag/<tag-key>
organizations:ous:update	授予更改组织单元名称的权限。	write	ou *	g:ResourceTag/<tag-key>
organizations:ous:delete	授予删除组织单元的权限。	write	ou *	g:ResourceTag/<tag-key>
organizations:accounts:create	授予创建账号的权限。	write	-	• g:RequestTag/<tag-key> • g:TagKeys
organizations:accounts:list	授予列出组织中的账号的权限。	list	-	-
organizations:accounts:get	授予查询账号信息的权限。	read	account *	g:ResourceTag/<tag-key>
organizations:accounts:remove	授予移除指定的账号的权限。	write	account *	g:ResourceTag/<tag-key>
organizations:accounts:move	授予移动账号的权限。	write	account *	g:ResourceTag/<tag-key>
organizations:accounts:invite	授予邀请账号加入组织的权限。	write	-	• g:RequestTag/<tag-key> • g:TagKeys
organizations:createAccountStatuses:list	授予列出创建账号的状态的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
organizations:createAccountStatuses:get	授予查询有关创建账号状态的信息的权限。	read	-	-
organizations:handshakes:get	授予查询邀请相关信息的权限。	read	handshake *	-
organizations:handshakes:accept	授予接受邀请的权限。	write	handshake *	-
organizations:handshakes:decline	授予拒绝邀请的权限。	write	handshake *	-
organizations:handshakes:cancel	授予取消邀请的权限。	write	handshake *	-
organizations:receivedHandshakes:list	授予列出收到的邀请的权限。	list	-	-
organizations:handshakes:list	授予列出发送的邀请的权限。	list	-	-
organizations:trustedServices:enable	授予启用可信服务的权限。	write	-	organizations:ServicePrincipal
organizations:trustedServices:disable	授予禁用受信任服务的权限。	write	-	organizations:ServicePrincipal
organizations:trustedServices:list	授予列出组织的可信服务列表的权限。	list	-	-
organizations:delegatedAdministrators:register	授予注册作为服务委托管理员的权限。	write	account *	g:ResourceTag/<tag-key>
			-	organizations:ServicePrincipal
organizations:delegatedAdministrators:deregister	授予注销服务的委托管理员的权限。	write	account *	g:ResourceTag/<tag-key>
			-	organizations:ServicePrincipal
organizations:delegatedServices:list	授予列出指定账号是其委托管理员的服务的权限。	list	account *	g:ResourceTag/<tag-key>
organizations:delegatedAdministrators:list	授予列出此组织中指定为委托管理员的账号的权限。	list	-	organizations:ServicePrincipal

授权项	描述	访问级别	资源类型（*为必须）	条件键
organizations:policies:create	授予创建策略的权限。	write	-	• g:RequestTag/<tag-key> • g:TagKeys
organizations:policies:list	授予列出策略的权限。	list	-	-
organizations:policies:get	授予查询策略相关信息的权限。	read	policy *	g:ResourceTag/<tag-key>
organizations:policies:update	授予更新策略的权限。	write	policy *	g:ResourceTag/<tag-key>
organizations:policies:delete	授予删除策略的权限。	write	policy *	g:ResourceTag/<tag-key>
organizations:policies:enable	授予在根中启用策略类型的权限。	write	root *	g:ResourceTag/<tag-key>
organizations:policies:disable	授予禁用根中的策略类型的权限。	write	root *	g:ResourceTag/<tag-key>
organizations:policies:attach	授予将策略跟实体绑定的权限。	write	policy *	g:ResourceTag/<tag-key>
			account	g:ResourceTag/<tag-key>
			ou	g:ResourceTag/<tag-key>
			root	g:ResourceTag/<tag-key>
organizations:policies:detach	授予将策略跟实体解绑的权限。	write	policy *	g:ResourceTag/<tag-key>
			account	g:ResourceTag/<tag-key>
			ou	g:ResourceTag/<tag-key>
			root	g:ResourceTag/<tag-key>
organizations:attachedEntities:list	授予列出跟指定策略绑定的所有实体的权限。	list	policy *	g:ResourceTag/<tag-key>
organizations:tags:list	授予列出绑定到指定资源的标签的权限。	list	account	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			ou	g:ResourceTag/<tag-key>
			root	g:ResourceTag/<tag-key>
			policy	g:ResourceTag/<tag-key>
organizations:resources:tag	授予为指定资源添加标签的权限。	tagging	account	g:ResourceTag/<tag-key>
			ou	g:ResourceTag/<tag-key>
			root	g:ResourceTag/<tag-key>
			policy	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
organizations:resources:untag	授予从指定资源中删除指定主键标签的权限。	tagging	account	g:ResourceTag/<tag-key>
			ou	g:ResourceTag/<tag-key>
			root	g:ResourceTag/<tag-key>
			policy	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
organizations:entities:list	授予列出组织中的根、组织单元和账号的权限。	list	-	-
organizations:services:list	授予列出所有可以与组织服务集成的云服务的权限。	list	-	-
organizations:tagPolicyServices:list	授予列出被添加到标签策略强制执行的资源类型。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
organizations:effectivePolicies:get	授予查询账号指定策略类型的有效策略的权限。	read	-	-
organizations:resources:listByTag	授予列出所有资源类型及标签信息查询实例的权限。	list	-	-
organizations:resources:countByTag	授予列出资源类型及标签信息查询实例数量的权限。	list	-	-
organizations:resources:list	授予列出项目标签的权限。	list	-	-
organizations:quotas:list	授予列出租户组织配额的权限。	list	-	-

Organizations的API通常对应着一个或多个授权项。表5-127展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-127 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/organizations	organizations:organizations:create	iam:agencies:createServiceLinkedAgency
GET /v1/organizations	organizations:organizations:get	-
DELETE /v1/organizations	organizations:organizations:delete	-
POST /v1/organizations/leave	organizations:organizations:leave	-
GET /v1/organizations/roots	organizations:roots:list	-
POST /v1/organizations/organizational-units	organizations:ous:create	organizations:resources:tag
GET /v1/organizations/organizational-units	organizations:ous:list	-

API	对应的授权项	依赖的授权项
GET /v1/organizations/organizational-units/{organizational_unit_id}	organizations:ous:get	-
PATCH /v1/organizations/organizational-units/{organizational_unit_id}	organizations:ous:update	-
DELETE /v1/organizations/organizational-units/{organizational_unit_id}	organizations:ous:delete	-
POST /v1/organizations/accounts	organizations:accounts:create	organizations:resources:tag
GET /v1/organizations/accounts	organizations:accounts:list	-
GET /v1/organizations/accounts/{account_id}	organizations:accounts:get	-
POST /v1/organizations/accounts/{account_id}/remove	organizations:accounts:remove	-
POST /v1/organizations/accounts/{account_id}/move	organizations:accounts:move	-
POST /v1/organizations/accounts/invite	organizations:accounts:invite	organizations:resources:tag
GET /v1/organizations/create-account-status	organizations:createAccountStatuses:list	-

API	对应的授权项	依赖的授权项
GET /v1/organizations/create-account-status/{create_account_status_id}	organizations:createAccountStatuses:get	-
GET /v1/organizations/handshakes/{handshake_id}	organizations:handshakes:get	-
POST /v1/received-handshakes/{handshake_id}/accept	organizations:handshakes:accept	iam:agencies:createServiceLinkedAgency
POST /v1/received-handshakes/{handshake_id}/decline	organizations:handshakes:decline	-
POST /v1/organizations/handshakes/{handshake_id}/cancel	organizations:handshakes:cancel	-
GET /v1/received-handshakes	organizations:receivedHandshakes:list	-
GET /v1/organizations/handshakes	organizations:handshakes:list	-
POST /v1/organizations/trusted-services/enable	organizations:trustedServices:enable	-
POST /v1/organizations/trusted-services/disable	organizations:trustedServices:disable	-
GET /v1/organizations/trusted-services	organizations:trustedServices:list	-

API	对应的授权项	依赖的授权项
POST /v1/organizations/delegated-administrators/register	organizations:delegatedAdministrators:register	-
POST /v1/organizations/delegated-administrators/deregister	organizations:delegatedAdministrators:deregister	-
GET /v1/organizations/accounts/{account_id}/delegated-services	organizations:delegatedServices:list	-
GET /v1/organizations/delegated-administrators	organizations:delegatedAdministrators:list	-
POST /v1/organizations/policies	organizations:policies:create	organizations:resources:tag
GET /v1/organizations/policies	organizations:policies:list	-
GET /v1/organizations/policies/{policy_id}	organizations:policies:get	-
PATCH /v1/organizations/policies/{policy_id}	organizations:policies:update	-
DELETE /v1/organizations/policies/{policy_id}	organizations:policies:delete	-
POST /v1/organizations/policies/enable	organizations:policies:enable	-
POST /v1/organizations/policies/disable	organizations:policies:disable	-

API	对应的授权项	依赖的授权项
POST /v1/organizations/policies/{policy_id}/attach	organizations:policies:attach	-
POST /v1/organizations/policies/{policy_id}/detach	organizations:policies:detach	-
GET /v1/organizations/policies/{policy_id}/attached-entities	organizations:attachedEntities:list	-
GET /v1/organizations/resources/{resource_id}/tags	organizations:tags:list	-
POST /v1/organizations/resources/{resource_id}/tag	organizations:resources:tag	-
POST /v1/organizations/resources/{resource_id}/untag	organizations:resources:untag	-
GET /v1/organizations/entities	organizations:entities:list	-
GET /v1/organizations/services	organizations:services:list	-
GET /v1/organizations/tag-policy-services	organizations:tagPolicyServices:list	-
GET /v1/organizations/entities/effective-policies	organizations:effectivePolicies:get	-
GET /v1/organizations/{resource_type}/{resource_id}/tags	organizations:tags:list	-

API	对应的授权项	依赖的授权项
POST /v1/organizations/{resource_type}/{resource_id}/tags/create	organizations:resources:tag	-
POST /v1/organizations/{resource_type}/{resource_id}/tags/delete	organizations:resources:untag	-
POST /v1/organizations/{resource_type}/resource-instances/filter	organizations:resources:listByTag	-
POST /v1/organizations/{resource_type}/resource-instances/count	organizations:resources:countByTag	-
GET /v1/organizations/{resource_type}/tags	organizations:resources:list	-
GET /v1/organizations/quotas	organizations:quotas:list	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-128中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

Organizations定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-128 Organizations 支持的资源类型

资源类型	URN
handshake	organizations::<management-account-id>:handshake:<organization-id>/<handshake-id>
ou	organizations::<management-account-id>:ou:<organization-id>/<organization-unit-id>

资源类型	URN
organization	organizations::<management-account-id>:organization:<organization-id>
root	organizations::<management-account-id>:root:<organization-id>/<root-id>
account	organizations::<management-account-id>:account:<organization-id>/<account-id>
policy	organizations::<management-account-id>:policy:<organization-id>/<policy-type>/<policy-id>
builtinpolicy	organizations::system:policy:<policy-type>/<policy-id>

条件（Condition）

条件（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀为服务缩写，如organizations:）仅适用于对应服务的操作，详情请参见**表5-129**。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
- 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，SCP才能生效。支持的运算符请参见：运算符。

Organizations定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-129 Organizations 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
organizations:ServicePrincipal	string	单值	根据指定的服务主体的名称过滤访问。

5.10.11.8 资源访问管理 RAM

Organizations服务中的服务控制策略（Service Control Policies，以下简称SCP）可以使用以下这些授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于RAM定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

  关于RAM定义的条件键的详细信息请参见**条件（Condition）**。

您可以在自定义SCP语句的Action元素中指定以下RAM的相关操作。

表 5-130 RAM 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
ram:permissions:list	授予列出RAM权限的权限。	list	permission *	-
ram:permissions:get	授予获取RAM权限内容的权限。	read	permission *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
ram:resourceShares:create	授予使用提供的资源和/或委托人创建资源共享的权限。	write	-	• g:RequestTag/<tag-key> • g:TagKeys • ram:RequestedResourceType • ram:ResourceUrn • ram:Principal • ram:TargetOrgPaths • ram:RequestedAllowExternalPrincipals
ram:resourceShares:search	授予从提供的列表获取一组资源共享，或获取具有指定状态的资源共享的权限。	read	-	• g:TagKeys
ram:resourceShares:update	授予更新资源共享属性的权限。	write	resourceShare*	• g:ResourceTag/<tag-key> • ram:AllowExternalPrincipals
			-	ram:RequestedAllowExternalPrincipals
ram:resourceShares:delete	授予删除资源共享的权限。	write	resourceShare*	• g:ResourceTag/<tag-key> • ram:AllowExternalPrincipals
ram:resourceShares:associate	授予将资源和/或委托人与资源共享关联的权限。	write	resourceShare*	• g:ResourceTag/<tag-key> • ram:AllowExternalPrincipals

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	• ram:RequestedResourceType • ram:ResourceUrn • ram:Principal • ram:TargetOrgPaths
ram:resourceShares:disassociate	授予取消资源和/或委托人与资源共享关联的权限。	write	resourceShare *	• g:ResourceTag/<tag-key> • ram:AllowExternalPrincipals
			-	• ram:RequestedResourceType • ram:ResourceUrn • ram:Principal • ram:TargetOrgPaths
ram:resourceShares:searchResourceShareAssociations	授予从提供的列表中获取一组资源共享关联，或者获取具有指定类型的指定状态的资源共享关联的权限。	read	-	-
ram:resourceShares:associatePermission	授予将权限与资源共享关联的权限。	write	resourceShare *	g:ResourceTag/<tag-key>
			-	ram:PermissionUrn
ram:resourceShares:disassociatePermission	授予取消权限与资源共享关联的权限。	write	resourceShare *	g:ResourceTag/<tag-key>
			-	ram:PermissionUrn
ram:resourceShares:listAssociatedPermissions	授予列出与资源共享关联权限的权限。	list	resourceShare *	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
ram:resourceShares:tag	授予标记指定资源共享的权限。	tagging	resourceShare *	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
ram:resourceShares:untag	授予取消标记指定资源共享的权限。	tagging	resourceShare *	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
ram:resourceShares:listTags	授予查询资源共享标签的权限。	list	-	-
ram:resourceShares:listResourceSharesByTag	授予根据标签查询资源共享列表的权限。	list	-	• g:TagKeys
ram:resourceShares:searchResourceShareCountByTag	授予根据标签查询资源共享数量的权限。	read	-	• g:TagKeys
ram:sharedResources:search	授予列出您添加到资源共享的资源或与您共享的资源的权限。	list	-	-
ram:sharedPrincipals:search	授予列出您与之共享资源或与您共享了资源的委托人的权限。	list	-	-
ram:resourceShareInvitations:accept	授予接受指定资源共享接受的权限。	write	resourceShareInvitation *	-
			-	ram:ShareOwnerAccountId
ram:resourceShareInvitations:reject	授予拒绝指定资源共享邀请的权限。	write	resourceShareInvitation *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	ram:ShareOwnerAccountId
ram:resourceShareInvitations:search	授予按指定邀请ID或资源共享ID获取资源共享邀请的权限。	read	-	-
ram:resourceShares:enableSharingWithOrganization	授予开启组织资源共享的权限。	permission_management	-	-
ram:resourceShares:disableSharingWithOrganization	授予关闭组织资源共享的权限。	permission_management	-	-
ram:resourceShares:searchEnableSharingWithOrganization	授予查询是否开启组织资源共享的权限。	read	-	-
ram:sharedResources:searchDistinctResource	授予列出您添加到资源共享的不同资源或与您共享的不同资源的权限。	list	-	-
ram:sharedPrincipals:searchDistinctPrincipal	授予列出您与之共享资源或与您共享了资源的不同委托人的权限。	list	-	-
ram:resourceShares:listQuota	授予查询资源共享配额权限。	list	-	-
ram:resourceTypes:list	授予查询云服务资源类型权限。	list	-	-
ram:permission:listVersions	授予获取RAM指定权限所有版本的权限。	list	-	-

RAM的API通常对应着一个或多个授权项。**表5-131**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-131 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1/permissions	ram:permissions:list	-
GET /v1/permissions/{permission_id}	ram:permissions:get	-
POST /v1/resource-shares	ram:resourceShares:create	-
POST /v1/resource-shares/search	ram:resourceShares:search	-
PUT /v1/resource-shares/{resource_share_id}	ram:resourceShares:update	-
DELETE /v1/resource-shares/{resource_share_id}	ram:resourceShares:delete	-
POST /v1/resource-shares/{resource_share_id}/associate	ram:resourceShares:associate	-
POST /v1/resource-shares/{resource_share_id}/disassociate	ram:resourceShares:disassociate	-
POST /v1/resource-share-associations/search	ram:resourceShares:searchResourceShareAssociations	-
POST /v1/resource-shares/{resource_share_id}/associate-permission	ram:resourceShares:associatePermission	-
POST /v1/resource-shares/{resource_share_id}/disassociate-permission	ram:resourceShares:disassociatePermission	-
GET /v1/resource-shares/{resource_share_id}/associated-permissions	ram:resourceShares:listAssociatedPermissions	-

API	对应的授权项	依赖的授权项
POST /v1/resource-shares/{resource_share_id}/tags/create	ram:resourceShares:tag	-
POST /v1/resource-shares/{resource_share_id}/tags/delete	ram:resourceShares:untag	-
GET /v1/resource-shares/tags	ram:resourceShares:listTags	-
POST /v1/resource-shares/resource-instances/filter	ram:resourceShares:listResourceSharesByTag	-
POST /v1/resource-shares/resource-instances/count	ram:resourceShares:searchResourceShareCountByTag	-
POST /v1/shared-resources/search	ram:sharedResources:search	-
POST /v1/shared-principals/search	ram:sharedPrincipals:search	-
POST /v1/resource-share-invitations/{resource_share_invitation_id}/accept	ram:resourceShareInvitations:accept	-
POST /v1/resource-share-invitations/{resource_share_invitation_id}/reject	ram:resourceShareInvitations:reject	-
POST /v1/resource-share-invitations/search	ram:resourceShareInvitations:search	-
POST /v1/organization-share/enable	ram:resourceShares:enableSharingWithOrganization	-
POST /v1/organization-share/disable	ram:resourceShares:disableSharingWithOrganization	-
GET /v1/organization-share	ram:resourceShares:searchEnableSharingWithOrganization	-

API	对应的授权项	依赖的授权项
POST /v1/shared-resources/search-distinct-resource	ram:sharedResources:searchDistinctResource	-
POST /v1/shared-principals/search-distinct-principal	ram:sharedPrincipals:searchDistinctPrincipal	-
GET /v1/resource-shares/quotas	ram:resourceShares:listQuota	-
GET /v1/resource-types	ram:resourceTypes:list	-
GET /v1/permissions/{permission_id}/versions	ram:permission:listVersions	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-132中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

RAM定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-132 RAM 支持的资源类型

资源类型	URN
permission	ram::system:permission:<permission-id>
resourceShare	ram::<account-id>:resourceShare:<resource-share-id>
resourceShareInvitation	ram::<account-id>:resourceShareInvitation:<resource-share-invitation-id>

条件（Condition）

条件（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀为服务缩写，如ram:）仅适用于对应服务的操作，详情请参见表5-133。

  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。

- 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，SCP才能生效。支持的运算符请参见：运算符。

RAM定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-133 RAM 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
ram:RequestedResourceType	string	多值	根据指定的资源类型过滤访问。
ram:ResourceUrn	string	多值	根据具有指定URN的资源过滤访问。
ram:Principal	string	多值	根据指定使用者的格式过滤访问。
ram:TargetOrgPaths	string	多值	根据指定使用者所在的组织路径过滤访问。
ram:PermissionUrn	string	单值	根据指定的权限URN过滤访问。
ram:ShareOwnerAccountId	string	单值	根据拥有的资源共享的特定账户过滤访问。例如，您可以使用此条件键指定可以根据资源共享所有者的账户ID接受或拒绝资源共享邀请。
ram:AllowExternalPrincipals	boolean	单值	按允许或者拒绝与外部使用者共享的资源共享过滤访问。例如，如果操作只能在允许与外部使用者共享的资源共享上执行，请指定true。外部使用者是指在其组织之外的账号。
ram:RequestedAllowExternalPrincipals	boolean	单值	根据指定的allow_external_principals过滤访问。外部使用者是指在其组织之外的账号。

5.10.11.9 企业项目管理 EPS

Organizations服务中的服务控制策略（Service Control Policies，以下简称SCP）可以使用以下这些授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于EPS定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

  关于EPS定义的条件键的详细信息请参见**条件（Condition）**。

您可以在自定义SCP语句的Action元素中指定以下EPS的相关操作。

表 5-134 EPS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
eps:enterpriseProjects:list	授予权限以查看企业项目列表。	list	enterpriseProject *	-
eps:enterpriseProjects:create	授予权限以创建企业项目。	write	enterpriseProject *	-
eps:enterpriseProjects:update	授予权限以修改企业项目。	write	enterpriseProject *	-
eps:enterpriseProjects:enable	授予权限以启用企业项目。	write	enterpriseProject *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
eps:enterpriseProjects:disable	授予权限以停用企业项目。	write	enterpriseProject *	-
eps:resources:list	授予权限以查看企业项目资源列表。	list	enterpriseProject *	-
eps:resources:add	授予权限将资源迁入至企业项目。	write	enterpriseProject *	-
eps:resources:remove	授予权限将资源从企业项目迁出。	write	enterpriseProject *	-

EPS的API通常对应着一个或多个授权项。表5-135展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-135 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1.0/enterprise-projects	eps:enterpriseProjects:list	-
POST /v1.0/enterprise-projects	eps:enterpriseProjects:create	-
PUT /v1.0/enterprise-projects/{enterprise_project_id}	eps:enterpriseProjects:update	-
POST /v1.0/enterprise-projects/{enterprise_project_id}/action	eps:enterpriseProjects:enable	-
POST /v1.0/enterprise-projects/{enterprise_project_id}/action	eps:enterpriseProjects:disable	-
POST /v1.0/enterprise-projects/{enterprise_project_id}/resources/filter	eps:resources:list	-

API	对应的授权项	依赖的授权项
POST /v1.0/enterprise-projects/{enterprise_project_id}/resources-migrate	eps:resources:add	eps:resources:remove
POST /v1.0/enterprise-projects/{enterprise_project_id}/resources-migrate	eps:resources:remove	eps:resources:add

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-136中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

EPS定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-136 EPS 支持的资源类型

资源类型	URN
enterpriseProject	eps::<account-id>:enterpriseProject:<enterprise-project-id>

条件（Condition）

EPS服务不支持在SCP中的条件键中配置服务级的条件键。

EPS可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.11.10 标签管理服务 TMS

Organizations服务中的服务控制策略（Service Control Policies，以下简称SCP）可以使用以下这些授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于TMS定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

  关于TMS定义的条件键的详细信息请参见**条件（Condition）**。

您可以在自定义SCP语句的Action元素中指定以下TMS的相关操作。

表 5-137 TMS 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
tms:predefineTags:list	授予权限以查询预定义标签列表。	list	-	-
tms:predefineTags:create	授予权限以创建预定义标签。	write	-	-
tms:predefineTags:update	授予权限以更新预定义标签。	write	-	-
tms:predefineTags:delete	授予权限以删除预定义标签。	write	-	-
tms:resourceTags:list	授予权限以查询资源标签列表。	list	-	-
tms:resourceTags:create	授予权限以创建资源标签。	write	-	-
tms:resourceTags:delete	授予权限以删除资源标签。	write	-	-
tms:resources:list	授予权限以查询资源列表。	list	-	-
tms:tagKeys:list	授予权限以查询标签key列表。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
tms:tagValues:list	授予权限以查询标签values列表。	list	-	-

TMS的API通常对应着一个或多个授权项。表5-138展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-138 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1.0/predefine_tags	tms:predefineTags:list	-
POST /v1.0/predefine_tags/action	tms:predefineTags:create	-
PUT /v1.0/predefine_tags	tms:predefineTags:update	-
POST /v1.0/predefine_tags/action	tms:predefineTags:delete	-
GET /v2.0/resources/{resource_id}/tags	tms:resourceTags:list	-
POST /v1.0/resource-tags/batch-create	tms:resourceTags:create	-
POST /v1.0/resource-tags/batch-delete	tms:resourceTags:delete	-
POST /v1.0/resource-instances/filter	tms:resources:list	-
GET /v1.0/tag-keys	tms:tagKeys:list	-
GET /v1.0/tag-values	tms:tagValues:list	-

资源类型（Resource）

TMS服务不支持在SCP中的资源中指定资源进行权限控制。如需允许访问TMS服务，请在SCP的Resource元素中使用通配符号*，表示SCP将应用到所有资源。

条件（Condition）

TMS服务不支持在SCP中的条件键中配置服务级的条件键。

TMS可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.11.11 配置审计 Config

Organizations服务中的服务控制策略（Service Control Policies，以下简称SCP）可以使用以下这些授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于Config定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列没有值（-），表示此操作不支持指定条件键。

  关于Config定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下Config的相关操作。

表 5-139 Config 支持的授权项

授权项	描述	访问级别	资源类型（* 为必须）	条件键
rms:organizationConformancePacks:create	授予权限创建组织合规规则包。	write	-	-
rms:organizationConformancePacks:get	授予权限查看组织合规规则包。	read	organizationConformancePacks *	-
rms:organizationConformancePacks:delete	授予权限删除组织合规规则包。	write	organizationConformancePacks *	-

授权项	描述	访问级别	资源类型（* 为必须）	条件键
rms:organizationConformancePacks:list	授予权限查询组织合规规则包列表。	list	-	-
rms:conformancePacks:create	授予权限创建合规规则包。	write	-	-
rms:conformancePacks:get	授予权限查看合规规则包。	read	conformancePacks *	-
rms:conformancePacks:delete	授予权限删除合规规则包。	write	conformancePacks *	-
rms:conformancePacks:list	授予权限查询合规规则包列表。	list	-	-
rms:storedQueries:create	授予权限保存新的高级查询语句。	write	-	-
rms:storedQueries:update	授予权限更新已存在的高级查询语句。	write	storedQueries *	-
rms:storedQueries:delete	授予权限删除已存在的高级查询语句。	write	storedQueries *	-
rms:storedQueries:get	授予权限查看已存在的高级查询语句详情。	read	storedQueries *	-
rms:storedQueries:list	授予权限查看已存在的高级查询语句列表。	list	-	-
rms:policyAssignments:create	授予权限创建新的合规规则以评估你的资源。	write	-	-
rms:policyAssignments:update	授予权限更新已存在的合规规则以评估你的资源。	write	policyAssignments *	-
rms:policyAssignments:delete	授予权限删除已存在的合规规则和相应的评估状态结果。	write	policyAssignments *	-
rms:policyAssignments:get	授予权限查看已存在的合规规则详情。	read	policyAssignments *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
rms:organizationPolicyAssignments:put	授予权限对整个组织创建或更新合规规则以评估你的资源。	write	-	-
rms:organizationPolicyAssignments:delete	授予权限删除指定的组织合规规则和组织内所有成员账号的合规评估状态结果。	write	organizationPolicyAssignments *	-
rms:organizationPolicyAssignments:get	授予权限查看组织合规规则详情。	read	organizationPolicyAssignments *	-
rms:organizationPolicyAssignments:list	授予权限查看组织合规规则列表。	list	-	-
rms:policyStates:get	授予权限查看合规规则评估状态结果列表。	read	-	-
rms:policyStates:runEvaluation	授予权限运行指定的合规规则以评估你的资源。	write	-	-
rms:policyStates:update	授予权限FunctionGraph函数将评估结果传输到Config。	write	-	-
rms:aggregators:create	授予权限创建聚合器聚合指定租户资源。	write	-	-
rms:aggregators:update	授予权限更新已存在的聚合器。	write	aggregators *	-
rms:aggregators:delete	授予权限删除指定聚合器并删除被聚合的租户资源。	write	aggregators *	-
rms:aggregators:list	授予权限查看已存在的聚合器列表。	list	-	-
rms:aggregators:get	授予权限查看已存在的聚合器详情。	read	aggregators *	-

授权项	描述	访问级别	资源类型（* 为必须）	条件键
rms:aggregatorResources:list	授予权限查看已被聚合的资源。	list	-	-
rms:aggregatorResources:runQuery	授予权限执行高级查询语句返回被聚合的资源属性。	list	-	-
rms:aggregatorResources:get	授予权限查看用户指定被聚合的资源详情。	read	-	-
rms:aggregationAuthorizations:create	授予权限创建聚合授权。	write	aggregationAuthorizations *	-
			-	rms:AuthorizedAccountOrgPath
rms:aggregationAuthorizations:list	授予权限查看已存在的聚合授权列表。	list	-	-
rms:aggregationAuthorizations:delete	授予权限删除已存在聚合授权并删除被聚合的租户资源。	write	aggregationAuthorizations *	-
			-	rms:AuthorizedAccountOrgPath
rms:aggregationRequests:delete	授予权限删除来自其他账号的聚合请求。	write	-	-
rms:aggregationRequests:list	授予权限查看来自其他账号的聚合请求列表。	list	-	-
rms:trackerConfig:put	授予权限创建或更新资源记录器配置以记录指定资源类型的资源历史数据。	write	-	-
rms:trackerConfig:delete	授予权限删除资源记录器配置以停止记录指定资源类型的资源历史数据。	write	-	-

授权项	描述	访问级别	资源类型（* 为必须）	条件键
rms:trackerConfig:get	授予权限查看资源记录器配置。	read	-	-
rms:schemas:list	授予权限查看高级查询资源Schema。	list	-	-
rms:policyDefinitions:get	授予权限查看预定义合规策略。	list	-	-
rms:resources:getHistory	授予权限查看指定资源的历史配置数据。	list	-	-
rms:resources:getRelation	授予权限查看资源关系。	list	-	-
rms:resources:get	授予权限查看用户指定的资源详情。	read	-	-
rms:resources:list	授予权限查看用户所有的资源列表。	list	-	-
rms:resources:runQuery	授予权限执行高级查询语句。	list	-	-
rms:resources:summarize	授予权限查看用户的资源概况。	list	-	-
rms::tagResource	授予权限批量创建资源标签。	tagging	policyAssignments	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
rms::unTagResource	授予权限批量删除资源标签。	tagging	policyAssignments	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys

授权项	描述	访问级别	资源类型（* 为必须）	条件键
rms::listTagsForResource	授予权限查询资源标签。	list	policyAssignments	g:ResourceTag/<tag-key>
rms::listTags	授予权限查询项目标签。	list	-	-
rms::listResourcesByTag	授予权限查询资源实例。	list	-	g:TagKeys

Config的API通常对应着一个或多个授权项。表5-140展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-140 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/resource-manager/organizations/{organization_id}/conformance-packs	rms:organizationConformancePacks:create	• organizations:organizations:get • organizations:accounts:list • organizations:delegatedAdministrators:list • organizations:trustedServices:enable • organizations:trustedServices:list
DELETE /v1/resource-manager/organizations/{organization_id}/conformance-packs/{conformance_pack_id}	rms:organizationConformancePacks:delete	organizations:organizations:get
GET /v1/resource-manager/organizations/{organization_id}/conformance-packs	rms:organizationConformancePacks:list	organizations:organizations:get

API	对应的授权项	依赖的授权项
GET /v1/resource-manager/organizations/{organization_id}/conformance-packs/{conformance_pack_id}	rms:organizationConformancePacks:get	organizations:organizations:get
GET /v1/resource-manager/organizations/{organization_id}/conformance-packs/statuses	rms:organizationConformancePacks:list	organizations:organizations:get
GET /v1/resource-manager/organizations/{organization_id}/conformance-packs/detailed-statuses	rms:organizationConformancePacks:get	organizations:organizations:get
POST /v1/resource-manager/domains/{domain_id}/conformance-packs	rms:conformancePacks:create	• rf:stack:createStack • rf:stack:getStackMetadata • rf:stack:listStackResources
DELETE /v1/resource-manager/domains/{domain_id}/conformance-packs/{conformance_pack_id}	rms:conformancePacks:delete	• rf:stack:deleteStack • rf:stack:getStackMetadata
GET /v1/resource-manager/domains/{domain_id}/conformance-packs/{conformance_pack_id}	rms:conformancePacks:get	-
GET /v1/resource-manager/domains/{domain_id}/conformance-packs/{conformance_pack_id}/compliance	rms:conformancePacks:get	-

API	对应的授权项	依赖的授权项
GET /v1/resource-manager/domains/{domain_id}/conformance-packs/{conformance_pack_id}/compliance/details	rms:conformancePacks:get	-
GET /v1/resource-manager/domains/{domain_id}/conformance-packs	rms:conformancePacks:list	-
GET /v1/resource-manager/domains/{domain_id}/conformance-packs/compliance/summary	rms:conformancePacks:list	-
GET /v1/resource-manager/domains/{domain_id}/conformance-packs/scores	rms:conformancePacks:list	-
POST /v1/resource-manager/domains/{domain_id}/stored-queries	rms:storedQueries:create	-
PUT /v1/resource-manager/domains/{domain_id}/stored-queries/{query_id}	rms:storedQueries:update	-
DELETE /v1/resource-manager/domains/{domain_id}/stored-queries/{query_id}	rms:storedQueries:delete	-
GET /v1/resource-manager/domains/{domain_id}/stored-queries/{query_id}	rms:storedQueries:get	-
GET /v1/resource-manager/domains/{domain_id}/stored-queries	rms:storedQueries:list	-

API	对应的授权项	依赖的授权项
PUT /v1/resource-manager/domains/{domain_id}/policy-assignments	rms:policyAssignments:create	-
DELETE /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}	rms:policyAssignments:delete	-
GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}	rms:policyAssignments:get	-
GET /v1/resource-manager/domains/{domain_id}/policy-assignments	rms:policyAssignments:get	-
PUT /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}	rms:policyAssignments:update	-
POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/disable	rms:policyAssignments:update	-
POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/enable	rms:policyAssignments:update	-

API	对应的授权项	依赖的授权项
PUT /v1/resource-manager/organizations/{organization_id}/policy-assignments	rms:organizationPolicyAssignments:put	• organizations:organizations:get • organizations:accounts:list • organizations:delegatedAdministrators:list • organizations:trustedServices:enable • organizations:trustedServices:list
GET /v1/resource-manager/organizations/{organization_id}/policy-assignments	rms:organizationPolicyAssignments:list	organizations:organizations:get
GET /v1/resource-manager/organizations/{organization_id}/policy-assignments/{organization_policy_assignment_id}	rms:organizationPolicyAssignments:get	organizations:organizations:get
GET /v1/resource-manager/organizations/{organization_id}/policy-assignment-statuses	rms:organizationPolicyAssignments:list	organizations:organizations:get
GET /v1/resource-manager/organizations/{organization_id}/policy-assignment-detailed-status	rms:organizationPolicyAssignments:list	organizations:organizations:get
DELETE /v1/resource-manager/organizations/{organization_id}/policy-assignments/{organization_policy_assignment_id}	rms:organizationPolicyAssignments:delete	organizations:organizations:get

API	对应的授权项	依赖的授权项
GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/policy-states	rms:policyStates:get	-
GET /v1/resource-manager/domains/{domain_id}/policy-states	rms:policyStates:get	-
GET /v1/resource-manager/domains/{domain_id}/resources/{resource_id}/policy-states	rms:policyStates:get	-
POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/policy-states/run-evaluation	rms:policyStates:runEvaluation	-
GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/policy-states/evaluation-state	rms:policyStates:get	-
PUT /v1/resource-manager/domains/{domain_id}/policy-states	rms:policyStates:update	-
PUT /v1/resource-manager/domains/{domain_id}/aggregators	rms:aggregators:create	-
PUT /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}	rms:aggregators:update	-

API	对应的授权项	依赖的授权项
DELETE /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}	rms:aggregators:delete	-
GET /v1/resource-manager/domains/{domain_id}/aggregators	rms:aggregators:list	-
GET /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}	rms:aggregators:get	-
GET /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}/aggregator-sources-status	rms:aggregators:get	-
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-states/compliance-summary	rms:aggregatorResources:list	-
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-assignments/compliance	rms:aggregatorResources:list	-
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-states/compliance-details	rms:aggregatorResources:list	-

API	对应的授权项	依赖的授权项
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-assignment/detail	rms:aggregatorResources:list	-
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-resource-config	rms:aggregatorResources:get	-
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/aggregate-discovered-resources	rms:aggregatorResources:list	-
POST /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}/run-query	rms:aggregatorResources:runQuery	-
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/aggregate-discovered-resource-counts	rms:aggregatorResources:list	-
GET /v1/resource-manager/domains/{domain_id}/aggregators/aggregation-authorization	rms:aggregationAuthorizations:list	-

API	对应的授权项	依赖的授权项
PUT /v1/resource-manager/domains/{domain_id}/aggregators/aggregation-authorization	rms:aggregationAuthorizations:create	-
DELETE /v1/resource-manager/domains/{domain_id}/aggregators/aggregation-authorization/{authorized_account_id}	rms:aggregationAuthorizations:delete	-
DELETE /v1/resource-manager/domains/{domain_id}/aggregators/pending-aggregation-request/{requester_account_id}	rms:aggregationRequests:delete	-
GET /v1/resource-manager/domains/{domain_id}/aggregators/pending-aggregation-request	rms:aggregationRequests:list	-
PUT /v1/resource-manager/domains/{domain_id}/tracker-config	rms:trackerConfig:put	-
DELETE /v1/resource-manager/domains/{domain_id}/tracker-config	rms:trackerConfig:delete	-
GET /v1/resource-manager/domains/{domain_id}/tracker-config	rms:trackerConfig:get	-

API	对应的授权项	依赖的授权项
GET /v1/resource-manager/domains/{domain_id}/schemas	rms:schemas:list	-
GET /v1/resource-manager/policy-definitions	rms:policyDefinitions:get	-
GET /v1/resource-manager/policy-definitions/{policy_definition_id}	rms:policyDefinitions:get	-
GET /v1/resource-manager/domains/{domain_id}/resources/{resource_id}/history	rms:resources:getHistory	-
GET /v1/resource-manager/domains/{domain_id}/all-resources/{resource_id}/relations	rms:resources:getRelation	-
GET /v1/resource-manager/domains/{domain_id}/provider/{provider}/type/{type}/resources/{resource_id}	rms:resources:get	-
GET /v1/resource-manager/domains/{domain_id}/all-resources	rms:resources:list	-
GET /v1/resource-manager/domains/{domain_id}/provider/{provider}/type/{type}/resources	rms:resources:list	-
POST /v1/resource-manager/domains/{domain_id}/run-query	rms:resources:runQuery	-

API	对应的授权项	依赖的授权项
GET /v1/resource-manager/domains/{domain_id}/all-resources/summary	rms:resources:list	-
GET /v1/resource-manager/domains/{domain_id}/all-resources/tags	rms:resources:list	-
GET /v1/resource-manager/domains/{domain_id}/all-resources/count	rms:resources:list	-
GET /v1/resource-manager/domains/{domain_id}/all-resources/{resource_id}	rms:resources:get	-
GET /v1/resource-manager/domains/{domain_id}/resources/{resource_id}/relations	rms:resources:summarize	-
GET /v1/resource-manager/domains/{domain_id}/tracked-resources	rms:resources:list	-
GET /v1/resource-manager/domains/{domain_id}/tracked-resources/count	rms:resources:list	-
GET /v1/resource-manager/domains/{domain_id}/tracked-resources/tags	rms:resources:list	-
GET /v1/resource-manager/domains/{domain_id}/tracked-resources/summary	rms:resources:list	-

API	对应的授权项	依赖的授权项
GET /v1/resource-manager/domains/{domain_id}/tracked-resources/{resource_id}	rms:resources:get	-
POST /v1/resource-manager/{resource_type}/{resource_id}/tags/create	rms::tagResource	-
POST /v1/resource-manager/{resource_type}/{resource_id}/tags/delete	rms::unTagResource	-
GET /v1/resource-manager/{resource_type}/{resource_id}/tags	rms::listTagsForResource	-
GET /v1/resource-manager/{resource_type}/tags	rms::listTags	-
POST /v1/resource-manager/{resource_type}/resource-instances/count	rms::listResourcesByTag	-
POST /v1/resource-manager/{resource_type}/resource-instances/filter	rms::listResourcesByTag	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-141**中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

Config定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-141 Config 支持的资源类型

资源类型	URN
conformancePacks	rms::<account-id>:conformancePacks:<conformance-pack-id>
storedQueries	rms::<account-id>:storedQueries:<query-id>
policyAssignments	rms::<account-id>:policyAssignments:<policy-assignment-id>
organizationPolicyAssignments	rms::<account-id>:organizationPolicyAssignments:<organization-id>/<organization-policy-assignments-id>
organizationConformancePacks	rms::<account-id>:organizationConformancePacks:<organization-id>/<organization-conformance-pack-id>
aggregators	rms::<account-id>:aggregators:<aggregator-id>
aggregationAuthorizations	rms::<account-id>:aggregationAuthorizations:<authorized-account-id>

条件（Condition）

条件（Condition）是SCP生效的特定条件，包括条件键和运算符。

- 条件键表示SCP语句的Condition元素中的键值。根据适用范围，分为全局级条件键和服务级条件键。
  - 全局级条件键（前缀为g:）适用于所有操作，在鉴权过程中，云服务不需要提供用户身份信息，系统将自动获取并鉴权。详情请参见：全局条件键。
  - 服务级条件键（前缀为服务缩写，如config:）仅适用于对应服务的操作，详情请参见**表5-142**。
  - 单值/多值表示API调用时请求中与条件关联的值数。单值条件键在API调用时的请求中最多包含一个值，多值条件键在API调用时请求可以包含多个值。例如：g:SourceVpce是单值条件键，表示仅允许通过某个VPC终端节点发起请求访问某资源，一个请求最多包含一个VPC终端节点ID值。g:TagKeys是多值条件键，表示请求中携带的所有标签的key组成的列表，当用户在调用API请求时传入标签可以传入多个值。
- 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，SCP才能生效。支持的运算符请参见：运算符。

Config定义了以下可以在SCP的Condition元素中使用的条件键，您可以使用这些条件键进一步细化SCP语句应用的条件。

表 5-142 Config 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
rms:AuthorizedAccountOrgPath	string	单值	根据指定的资源聚合授权账号的Organizations Path过滤访问。

5.10.11.12 访问分析 IAM Access Analyzer

Organizations服务中的服务控制策略（Service Control Policy，以下简称SCP）可以使用以下授权项元素设置访问控制策略。

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- **“访问级别”**列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- **“资源类型”**列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于IAM Access Analyzer定义的资源类型的详细信息请参见**资源类型（Resource）**。
- **“条件键”**列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于IAM Access Analyzer定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下IAM Access Analyzer的相关操作。

表 5-143 IAM Access Analyzer 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
AccessAnalyzer:analyzer:create	授予创建分析器的权限。	write	analyzer *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
AccessAnalyzer:analyzer:get	授予查询分析器的权限。	read	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:list	授予查询分析器列表的权限。	list	analyzer *	-
AccessAnalyzer:analyzer:delete	授予删除分析器的权限。	write	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:scan	授予启动分析器扫描的权限。	write	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:getFinding	授予查询分析结果的权限。	read	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:listFindings	授予查询分析结果列表的权限。	list	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:updateFindings	授予更新分析结果的权限。	write	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer::tagResource	授予给资源添加标签的权限。	tagging	analyzer *	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
AccessAnalyzer::untagResource	授予给资源删除标签的权限。	tagging	analyzer *	g:ResourceTag/<tag-key>
			-	g:TagKeys
AccessAnalyzer:archiveRule:create	授予创建存档规则的权限。	write	archiveRule *	-
AccessAnalyzer:archiveRule:get	授予查询存档规则的权限。	read	archiveRule *	-
AccessAnalyzer:archiveRule:list	授予查询存档规则列表的权限。	list	archiveRule *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
AccessAnalyzer:archiveRule:update	授予更新存档规则的权限。	write	archiveRule *	-
AccessAnalyzer:archiveRule:delete	授予删除存档规则的权限。	write	archiveRule *	-
AccessAnalyzer:archiveRule:apply	授予应用存档规则的权限。	write	archiveRule *	-
AccessAnalyzer:analyzer:createPreview	授予创建访问分析预览的权限。	write	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:getPreview	授予查询访问分析预览的权限。	read	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:listPreviews	授予查询访问分析预览列表的权限。	list	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:listPreviewFindings	授予查询访问分析预览分析结果列表的权限。	list	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer::validatePolicy	授予验证策略的权限。	read	-	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表3中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

IAM Access Analyzer定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-144 IAM Access Analyzer 支持的资源类型

资源类型	URN
analyzer	AccessAnalyzer:<region>:<account-id>:analyzer:<analyzer-id>
archiveRule	AccessAnalyzer:<region>:<account-id>:archiveRule:<analyzer-id>/<archive-rule-id>

条件（Condition）

IAM Access Analyzer服务不支持在SCP中的条件键中配置服务级的条件键。IAM Access Analyzer可以使用适用于所有服务的全局条件键，请参考全局条件键。

5.10.11.13 云审计服务 CTS

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。

本章节介绍组织服务中SCP使用的元素，这些元素包含了操作（Action）、资源（Resource）和条件（Condition）。

如何使用这些元素编辑SCP自定义策略，请参考创建SCP。

操作（Action）

操作（Action）即为SCP中支持的授权项。

- “**访问级别**”列描述如何对操作进行分类（list、read和write等）。此分类可帮助您了解在SCP中相应操作对应的访问级别。
- “**资源类型**”列指每个操作是否支持资源级权限。
  - 资源类型支持通配符号*表示所有。如果此列没有值（-），则必须在SCP语句的Resource元素中指定所有资源类型（“*”）。
  - 如果该列包含资源类型，则必须在具有该操作的语句中指定该资源的URN。
  - 资源类型列中必需资源在表中用星号（*）标识，表示使用此操作必须指定该资源类型。

  关于cts定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “**条件键**”列包括了可以在SCP语句的Condition元素中支持指定的键值。
  - 如果该授权项资源类型列存在值，则表示条件键仅对列举的资源类型生效。
  - 如果该授权项资源类型列没有值（-），则表示条件键对整个授权项生效。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

  关于cts定义的条件键的详细信息请参见**条件（Condition）**。

您可以在SCP语句的Action元素中指定以下cts的相关操作。

表 5-145 cts 支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
cts:trace:list	授予查询审计事件权限。	list	-	-
cts:tracker:create	授予创建追踪器的权限。	write	-	-
cts:tracker:list	授予查询追踪器权限。	list	-	-
cts:tracker:update	授予更新追踪器的权限。	write	tracker	-
cts:tracker:delete	授予删除追踪器的权限。	write	tracker	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
cts:quota:get	授予查询追踪器配额权限。	read	-	-
cts:notification:create	授予创建通知规则权限。	write	-	-
cts:notification:update	授予更新关键操作通知权限。	write	notification	-
cts:notification:list	授予查询关键操作通知权限。	list	-	-
cts:notification:delete	授予删除通知规则权限。	write	notification	-
cts:tag:create	授予创建资源标签的权限。	tagging	tracker	-
			-	• g:TagKeys • g:RequestTag/<tag-key>
cts:tag:delete	授予删除资源标签的权限。	tagging	tracker	-
			-	• g:TagKeys • g:RequestTag/<tag-key>
cts:notification:listOperation	授予查询所有操作列表的权限。	list	-	-
cts:trace:listTraceUser	授予查询所有操作用户列表的权限。	list	-	-
cts:trace:listResource	授予查询所有事件资源类型列表的权限。	list	-	-
cts:trace:list	授予查询审计事件权限。	list	-	-
cts:tracker:create	授予创建追踪器的权限。	write	-	-
cts:tracker:list	授予查询追踪器权限。	list	-	-
cts:tracker:update	授予更新追踪器的权限。	write	tracker	-
cts:tracker:delete	授予删除追踪器的权限。	write	tracker	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
cts:quota:get	授予查询追踪器配额权限。	read	-	-
cts:notification:create	授予创建通知规则权限。	write	-	-
cts:notification:update	授予更新关键操作通知权限。	write	notification	-
cts:notification:list	授予查询关键操作通知权限。	list	-	-
cts:notification:delete	授予删除通知规则权限。	write	notification	-
cts:tag:create	授予创建资源标签的权限。	tagging	tracker	-
			-	• g:TagKeys • g:RequestTag/<tag-key>
cts:tag:delete	授予删除资源标签的权限。	tagging	tracker	-
			-	• g:TagKeys • g:RequestTag/<tag-key>
cts:notification:listOperation	授予查询所有操作列表的权限。	list	-	-
cts:trace:listTraceUser	授予查询所有操作用户列表的权限。	list	-	-
cts:trace:listResource	授予查询所有事件资源类型列表的权限。	list	-	-

cts的API通常对应着一个或多个授权项。表5-146展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-146 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/traces	cts:trace:list	-
GET /v3/{project_id}/quotas	cts:quota:get	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/tracker	cts:tracker:create	• lts:topics:list • lts:topics:create • lts:groups:list • lts:groups:create • obs:bucket:CreateBucket • obs:bucket:HeadBucket • obs:bucket:GetLifecycleConfiguration • obs:bucket:PutLifecycleConfiguration • obs:bucket:GetBucketAcl • obs:bucket:PutBucketAcl • kms:cmk:list
PUT /v3/{project_id}/tracker	cts:tracker:update	• lts:topics:list • lts:topics:create • lts:groups:list • lts:groups:create • obs:bucket:CreateBucket • obs:bucket:HeadBucket • obs:bucket:GetLifecycleConfiguration • obs:bucket:PutLifecycleConfiguration • obs:bucket:GetBucketAcl • obs:bucket:PutBucketAcl • kms:cmk:list
GET /v3/{project_id}/trackers	cts:tracker:list	-
DELETE /v3/{project_id}/trackers	cts:tracker:delete	-
POST /v3/{project_id}/notifications	cts:notification:create	• smn:topic:listTopic • iam:users:listUsers • iam:groups:listGroups
PUT /v3/{project_id}/notifications	cts:notification:update	• smn:topic:listTopic • iam:users:listUsers • iam:groups:listGroups

API	对应的授权项	依赖的授权项
DELETE /v3/{project_id}/notifications	cts:notification:delete	-
GET /v3/{project_id}/notifications/{notification_type}	cts:notification:list	-
POST /v3/{project_id}/{resource_type}/{resource_id}/tags/create	cts:tag:create	-
DELETE /v3/{project_id}/{resource_type}/{resource_id}/tags/delete	cts:tag:delete	-
GET /v3/{domain_id}/resources	cts:trace:listResource	-
GET /v3/{project_id}/operations	cts:notification:listOperation	-
GET /v3/{project_id}/user-resources	cts:trace:listTraceUser	-
POST /v3/{domain_id}/checkbucket	cts:tracker:list	obs:bucket:ListAllMyBuckets
GET /v3/{project_id}/traces	cts:trace:list	-
GET /v3/{project_id}/quotas	cts:quota:get	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/tracker	cts:tracker:create	• lts:topics:list • lts:topics:create • lts:groups:list • lts:groups:create • obs:bucket:CreateBucket • obs:bucket:HeadBucket • obs:bucket:GetLifecycleConfiguration • obs:bucket:PutLifecycleConfiguration • obs:bucket:GetBucketAcl • obs:bucket:PutBucketAcl • kms:cmk:list
PUT /v3/{project_id}/tracker	cts:tracker:update	• lts:topics:list • lts:topics:create • lts:groups:list • lts:groups:create • obs:bucket:CreateBucket • obs:bucket:HeadBucket • obs:bucket:GetLifecycleConfiguration • obs:bucket:PutLifecycleConfiguration • obs:bucket:GetBucketAcl • obs:bucket:PutBucketAcl • kms:cmk:list
GET /v3/{project_id}/trackers	cts:tracker:list	-
DELETE /v3/{project_id}/trackers	cts:tracker:delete	-
POST /v3/{project_id}/notifications	cts:notification:create	• smn:topic:listTopic • iam:users:listUsers • iam:groups:listGroups
PUT /v3/{project_id}/notifications	cts:notification:update	• smn:topic:listTopic • iam:users:listUsers • iam:groups:listGroups

API	对应的授权项	依赖的授权项
DELETE /v3/{project_id}/notifications	cts:notification:delete	-
GET /v3/{project_id}/notifications/{notification_type}	cts:notification:list	-
POST /v3/{project_id}/{resource_type}/{resource_id}/tags/create	cts:tag:create	-
DELETE /v3/{project_id}/{resource_type}/{resource_id}/tags/delete	cts:tag:delete	-
GET /v3/{domain_id}/resources	cts:trace:listResource	-
GET /v3/{project_id}/operations	cts:notification:listOperation	-
GET /v3/{project_id}/user-resources	cts:trace:listTraceUser	-
POST /v3/{domain_id}/checkbucket	cts:tracker:list	obs:bucket:ListAllMyBuckets

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-147中的某些操作指定了可以在该操作指定的资源类型，则必须在具有该操作的SCP语句中指定该资源的URN，SCP仅作用于此资源；如未指定，Resource默认为“*”，则SCP将应用到所有资源。您也可以在SCP中设置条件，从而指定资源类型。

cts定义了以下可以在自定义SCP的Resource元素中使用的资源类型。

表 5-147 cts 支持的资源类型

资源类型	URN
tracker	cts:<region>:<account-id>:tracker:<tracker-id>

资源类型	URN
notification	cts:<region>:<account-id>:notification:<notification-id>

条件（Condition）

cts服务不支持在SCP中的条件键中配置服务级的条件键。cts可以使用适用于所有服务的全局条件键，请参考全局条件键。

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。
- 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。

运算符	说明
@@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 标签策略快速入门

背景信息

本章节为您介绍如何快速地使用标签策略来规范资源标签的操作。

首次使用标签策略时，建议您先将一个简单的标签策略绑定至资源较少的测试账号中，待测试成功且您已完全了解标签策略的影响后，再继续使用更多复杂的标签策略，将其扩展至组织的根、OU或更多账号。

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。

步骤2 在组织中**启用标签策略**。

步骤3 **创建标签策略**。

首次使用建议创建一个简单的标签策略，例如：

1. 定义标签键为“ABC”。
2. 使用标签键的大小写形式来定义合规性，也就是说为资源添加的标签的键为“ABC”则符合规范，添加“abc”、“Abc”等其他大小写形式的标签则为不合规，标签策略将阻止不合规标签的添加操作。
3. 添加执行标签策略的资源类型，例如云监控服务的告警规则（ces:alarm），表示此标签策略仅对组织成员账号这一资源类型生效。当前支持标签策略的云服务和资源类型请参见：**支持标签策略的云服务**。

当您为此资源添加不合规的标签时，标签策略将阻止此操作，您必须将标签修改至符合标签策略规范才可以添加成功。

图 6-1 创建标签策略

步骤4 将创建的标签策略绑定至一个资源较少的可用于测试的成员账号中，具体请参见**绑定标签策略**。

图 6-2 绑定标签策略

步骤5 使用此成员账号登录华为云，进入云监控服务控制台，创建告警规则并为其添加标签，验证标签策略是否生效。

1. 为告警规则添加标签“ABC”，标签添加成功。
2. 为告警规则添加标签“abc”，界面提示此标签校验不合规，需修改后再次提交，表示标签策略已生效且验证无误。

图 6-3 添加不合规标签

注意

当您在创建资源时添加不合规的标签，标签策略将阻止标签添加操作，同时资源也无法创建成功；

当您为已创建的资源添加不合规标签时，标签策略仅会阻止标签添加操作，不会对资源产生影响。

----结束

6.4 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华为云，进入华为云Organizations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 6-4 启用标签策略

步骤3 在弹窗中勾选确认框，然后单击“启用”，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华为云，进入华为云Organizations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 6-5 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

6.5 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，制定规则。

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华为云，进入华为云Organizations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 6-6 进入标签策略管理页

步骤3 单击“创建”，进入标签策略创建页面。

图 6-7 单击创建

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 6-8 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”。

图 6-9 添加资源类型

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 6-10 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 6-11 添加标签

步骤7 单击右下角“保存”后，如跳转到标签策略列表，则标签策略创建成功。

----结束

6.6 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 进入华为云Organizations控制台，进入组织管理页面。

步骤2 在左侧导航栏，选择“组织管理”。

步骤3 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4 在右侧详细信息下，选择“策略”页签。

步骤5 单击“标签策略”左边的。

步骤6 单击“查看有效标签策略”，如图6-12所示。

图 6-12 查看有效标签策略

步骤7 在JSON视图查看有效标签策略内容。

----结束

6.7 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华为云，进入华为云Organizations控制台。

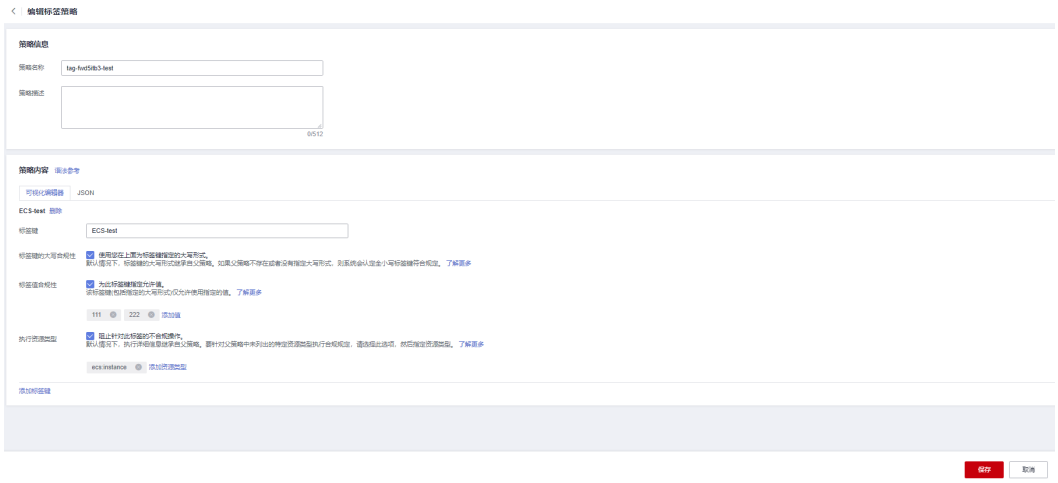
步骤2 进入策略管理页，单击“标签策略”，进入标签策略列表。

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。

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。

图 6-13 编辑标签策略



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华为云，进入华为云Organizations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 单击弹窗中的“确定”，完成标签策略删除。

图 6-14 删除标签策略

----结束

6.8 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。

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”。

图 6-15 绑定标签策略

步骤4 在弹窗中选择要添加的策略后，单击“绑定”，完成策略绑定。

----结束

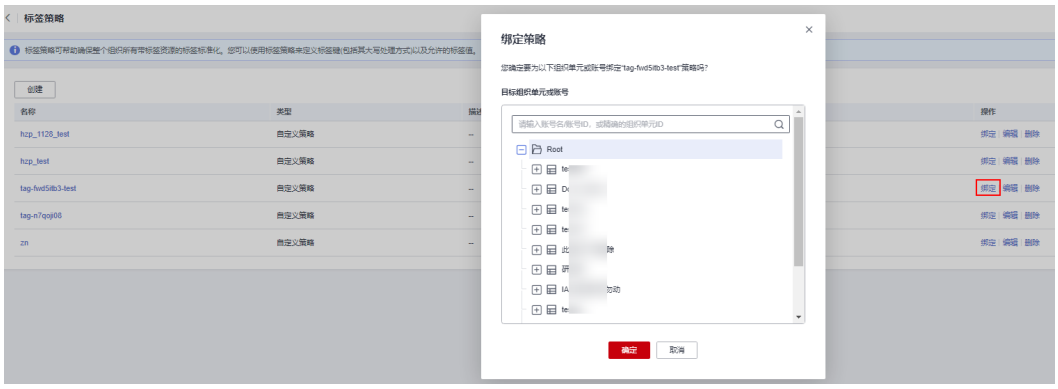
方式二：

步骤1 在Organizations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。

图 6-16 绑定标签策略



步骤4 单击“确定”，完成策略绑定。

----结束

解绑标签策略

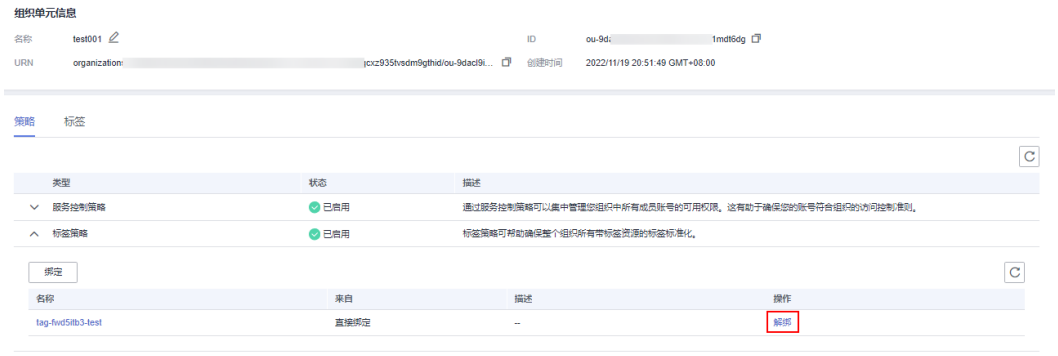
方式一：

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 6-17 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Organizations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”。

图 6-18 解绑标签策略

步骤5 单击“确定”，完成策略解绑。

----结束

6.9 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）
API网关（APIG）	实例（instance）
弹性伸缩（AS）	弹性伸缩组（scalingGroup）

服务名称	资源类型
裸金属服务器（BMS）	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）
内容分发网络（CDN）	域名（domain）
云监控服务（CES）	告警规则（alarm）
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）
数据库安全服务（DBSS）	审计实例（auditInstance）
云专线（DCAAS）	• 物理连接（directconnect） • 全球专线接入网关（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）
分布式消息服务（DMS）	• Kafka实例（kafka） • RabbitMQ实例（rocketmq） • 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）
弹性云服务器（ECS）	实例（instance）

服务名称	资源类型
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 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）
NAT网关（NAT）	• 公网NAT网关（gateway） • 私网NAT网关（privateGateway） • 中转IP（privateTransitIp） • 中转子网（transitSubnet）
私有证书管理服务（PCA）	私有CA（ca）
云数据库（RDS）	实例 (instances)
SSL证书管理服务（SCM）	证书（cert）

服务名称	资源类型
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）
VPC终端节点（VPCEP）	• 终端节点服务（endpointServices） • 终端节点（endpoints）

6.10 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
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

区域名称	区域
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华为云，进入华为云Organizations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”。

图 7-1 启用可信服务

步骤3 在弹窗中单击“确定”，完成可信服务启用。

----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华为云，进入华为云Organizations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 在弹窗中单击“确定”，完成可信服务禁用。

----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华为云，进入华为云Organizations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	相关文档
配置审计（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的所有成员账号中。	是	• 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	启用与组织共享资源

服务名称	功能简介	是否支持委托管理员	相关文档
云审计（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	组织追踪器
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	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	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	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	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	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	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	账号管理
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的访问权限。	是	什么是IAM身份中心

服务名称	功能简介	是否支持委托管理员	相关文档
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	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	创建托管

7.4 添加、查看和取消委托管理员

- 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

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。

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”。

图 7-3 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”，完成设置。

----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华为云，进入华为云Organizations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”。

图 7-4 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。

----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华为云，进入华为云Organizations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 7-5 取消委托

步骤4 单击弹窗中的“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：

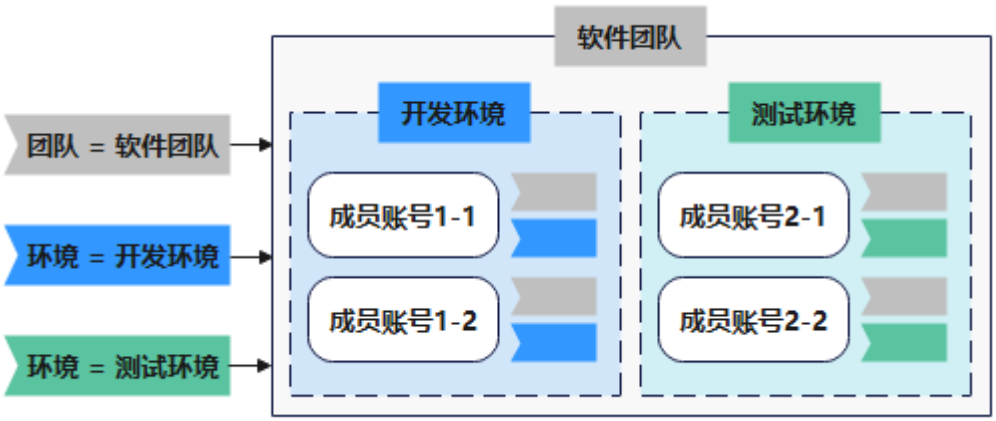
- 在创建OU、账号、SCP和标签策略时，可以添加标签。
- 根、OU、账号、SCP和标签策略创建完成后，可以在各自的详情页面添加、修改、查看、删除标签。

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

8.2.1 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

为根、OU和账号添加标签的方法类似，以OU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”。

图 8-2 添加标签

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。

----结束

8.2.2 添加策略标签

操作场景

Organizations支持为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华为云，进入华为云Organizations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。

图 8-3 进入策略详情

步骤4 选择“标签”页签，单击“添加”。

图 8-4 策略添加标签

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”，完成策略的标签添加。

----结束

8.3 修改标签

8.3.1 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 单击要修改标签操作列的“编辑”。

步骤4 在弹窗中输入新的标签值，单击“确定”，完成标签修改。

----结束

8.3.2 修改策略标签

操作场景

Organizations支持修改SCP自定义策略和标签策略标签。

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华为云，进入华为云Organizations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。

图 8-5 进入策略详情

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”，完成策略的标签修改。

----结束

8.4 查看标签

8.4.1 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，查看组织单元的标签信息，包括“标签键”和“标签值”。

----结束

8.4.2 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华为云，进入华为云Organizations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。

图 8-6 进入策略详情

步骤4 选择“标签”页签，即可查看当前策略的所有标签。

----结束

8.5 删除标签

8.5.1 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。

----结束

8.5.2 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华为云，进入华为云Organizations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。

图 8-7 进入策略详情

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 单击弹窗中的“确定”，完成标签删除。

----结束

9 审计

9.1 支持审计的关键操作

通过云审计服务，您可以记录与Organizations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	Organizations	CreateOrganizations
关闭组织	Organizations	DeleteOrganizations
退出组织	Organizations	LeaveOrganizations
创建组织单元	OrganizationsUnit	CreateOrganizationsalUnit
修改组织单元	OrganizationsUnit	UpdateOrganizationsalUnit
删除组织单元	OrganizationsUnit	DeleteOrganizationsalUnit
邀请账号	Account	InviteAccount
移动账号	Account	MoveAccount
移除账号	Account	RemoveAccount
接受邀请	Handshake	AcceptHandshake
拒绝邀请	Handshake	DeclineHandshake
取消邀请	Handshake	CancelHandshake
启用可信服务	TrustedService	EnableTrustedService
禁用可信服务	TrustedService	DisableTrustedService

操作名称	资源类型	事件名称
设置委托管理员	DelegatedAdministrator	RegisterDelegatedAdministrator
取消委托管理员	DelegatedAdministrator	DeregisterDelegatedAdministrator
创建策略	Policy	CreatePolicy
修改策略	Policy	UpdatePolicy
删除策略	Policy	DeletePolicy
启用策略类型	Policy	EnablePolicyType
禁用策略类型	Policy	DisablePolicyType
绑定策略	Policy	AttachPolicy
解绑策略	Policy	DetachPolicy
添加标签	Tag	TagResource
删除标签	Tag	UntagResource

9.2 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：

- **在新版事件列表查看审计事件**
- **在旧版事件列表查看审计事件**

使用限制

- 单账号跟踪的事件可以通过云审计控制台查询。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。
- 用户通过云审计控制台只能查询最近7天的操作记录。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)，才可在OBS桶里面查看历史文件。否则，您将无法追溯7天以前的操作记录。
- 云上操作后，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。

在新版事件列表查看审计事件

1. 登录管理控制台。

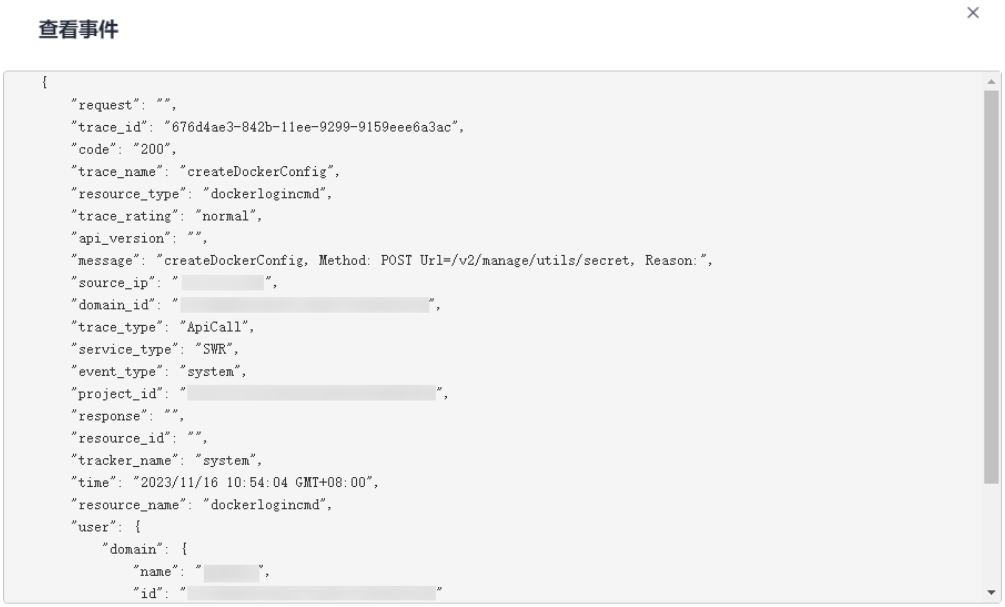
2. 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
   - 事件名称：输入事件的名称。
   - 事件ID：输入事件ID。
   - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
   - 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
   - 云服务：在下拉框中选择对应的云服务名称。
   - 资源类型：在下拉框中选择对应的资源类型。
   - 操作用户：在下拉框中选择一个或多个具体的操作用户。
   - 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
     - normal：表示操作成功。
     - warning：表示操作失败。
     - incident：表示比操作失败更严重的情况，例如引起其他故障等。
   - 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近1周内任意时间段的操作事件。
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。
6. 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。
7. （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。

在旧版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“管理与监管 > 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. 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。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
   - 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。
6. 选择完查询条件后，单击“查询”。
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。
8. 在需要查看的事件左侧，单击 展开该记录的详细信息。

9. 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。



10. 关于事件结构的关键字段详解，请参见《云审计服务用户指南》中的事件结构和事件样例。
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。

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. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 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

4. 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”。

11 修订记录

时间	修订记录
2024-03-14	第六次正式发布。 本次变更说明如下： ● 组织（Organizations）云服务正式商用。 ● 新增“标签策略快速入门”章节。 ● 新增“支持标签策略的区域”章节。 ● 新增“SCP授权参考”章节。 ● 新增“查看账号记录”章节。 ● 新增“关闭账号”章节。
2024-01-18	第五次正式发布。 本次变更说明如下： ● 新增“SCP示例”章节。 ● 新增“支持SCP的区域”章节。
2023-11-15	第四次正式发布。 本次变更说明如下： 新增“创建账号”章节。
2023-03-30	第三次正式发布。 本次变更说明如下： 上线标签策略特性相关内容。
2023-03-01	第二次正式发布。 本次变更说明如下： ● “绑定和解绑SCP”章节新增“约束与限制”。 ● 更新“支持SCP的服务”和“已对接组织的可信服务”。 ● 删除邀请的账号需要为企业子账号的相关描述。
2023-01-16	第一次正式发布。