组织

用户指南

文档版本	01
发布日期	2025-02-21

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。例如管理账号有两个IAM用户，一个IAM用户可以创建和删除组织单元，一个IAM用户只能查看组织单元。
- 给管理账号中不同职能部门的员工创建IAM用户，让员工拥有唯一和独立安全凭证访问华为云，并使用Organizations云服务资源，提高账号安全性。
- 将Organizations云服务资源委托给更专业、高效的其他华为云账号或者云服务，这些华为云账号或者云服务可以根据权限进行代运维。

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

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

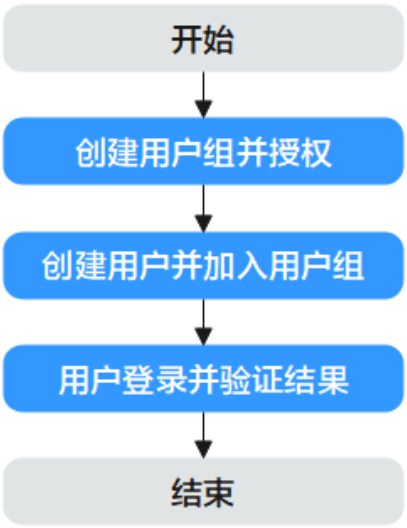
前提条件

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

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

示例流程

图 1-1 给用户授予 Organizations 权限流程



1. 创建用户组并授权

   在IAM控制台创建用户组，授予Organizations云服务只读权限“Organizations ReadOnlyAccess”。
2. 创建用户并加入用户组

   在IAM控制台创建用户，并将其加入1中创建的用户组。
3. 用户登录并验证权限

   使用新创建的用户登录控制台，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。

----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 2-2 管理账号查看组织信息

管理账号查看根信息

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

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

----结束

管理账号查看 OU 信息

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

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

----结束

管理账号查看账号信息

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

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

----结束

成员账号查看组织信息

以成员账号的身份登录华为云，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 2-3 删除组织

----结束

3 OU 管理

3.1 OU 概述

什么是 OU

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

本章节将为您介绍如下内容：

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

3.2 创建 OU

您可以在组织的根下创建OU。OU最深可嵌套至5层。创建OU请执行以下步骤。

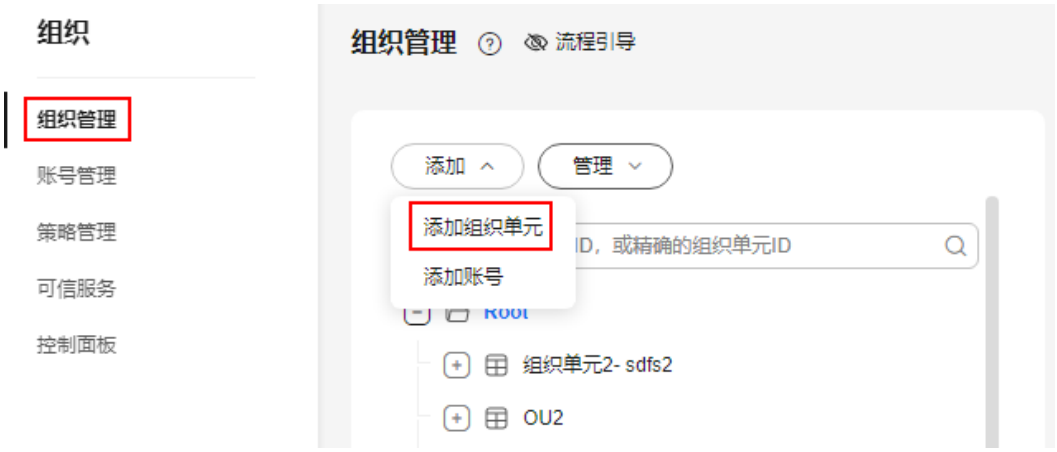
步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

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

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

步骤3 单击组织结构树上方的“添加”，单击“添加组织单元”。

图 3-1 添加组织单元



步骤4 在弹窗中填写组织单元名称。

步骤5 （可选）为组织单元添加标签。

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

标签的设置说明如表3-1所示。

表 3-1 标签说明

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

步骤6 然后单击“确定”，完成OU创建。

----结束

3.3 修改 OU

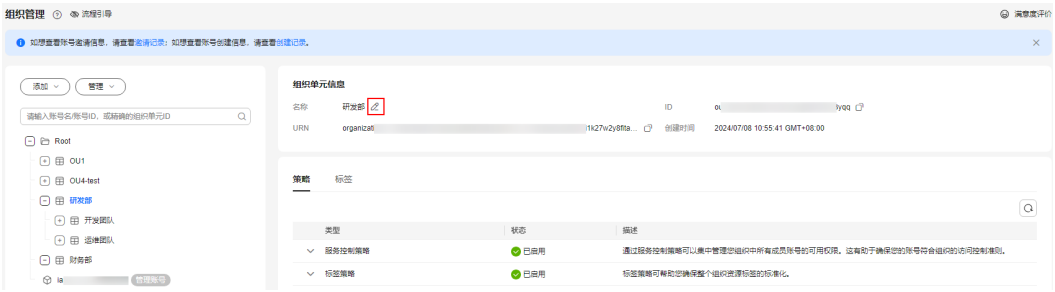
OU创建后，您可以随时修改OU的名称、标签和策略，其中修改标签和策略的详细步骤请参见：**标签管理**和**绑定和解绑SCP**。

操作步骤

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

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

图 3-2 修改 OU 名称



步骤3 在编辑框中修改OU名称，然后单击 保存，完成OU重命名。

----结束

3.4 查看 OU 详细信息

OU创建后，您可以随时查看OU的详细信息，具体请参见如下步骤。

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

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

图 3-3 查看组织单元详细信息

----结束

3.5 删除 OU

当您不再需要某个OU时，可以删除OU。

说明

只能删除资源为空的OU，被删除的OU中不能嵌套子OU，不能包含账号。

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

步骤2 选中要删除的OU，单击组织结构树上方的“管理”。

步骤3 单击“删除组织单元”，在弹窗中单击“确定”，完成OU删除。

图 3-4 删除组织单元

----结束

4 账号管理

4.1 账号概述

组织中的账号

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

表 4-1 账号分类

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

加入组织的影响

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

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

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

本章将为您介绍如下内容，以帮助您管理组织中的账号：

- **邀请账号加入组织**，包括管理账号创建邀请、管理您已发出的邀请，以及成员账号接受或拒绝邀请。
- **创建账号**，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。
- **移动账号**，将账号从一个OU移动到另外一个OU。
- **查看账号详细信息**，包括账号名称、ID、加入时间、归属组织单元、绑定的策略、标签和委托服务。
- **移除成员账号**，管理账号从组织中移除成员账号。
- **查看账号记录**，组织的管理账号可在账号管理页查看账号列表、邀请记录、创建记录及其相关信息，还可以进行邀请、创建、关闭、移动、移除账号以及取消邀请等操作。

4.2 邀请账号加入组织

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

说明

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

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

本章节包含如下内容：

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

向账号发送邀请

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

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

步骤2 单击组织结构树上方的“添加”，单击“添加账号”。

图 4-1 添加账号

步骤3 在弹窗中，选择“邀请现有账号”，输入邀请账号的账号名或账号ID。

如何获取账号名和账号ID请参见：获取账号名和ID。

图 4-2 邀请现有账号

步骤4 （可选）为账号添加标签。

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

标签的设置说明如**表4-2**所示。

表 4-2 标签说明

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

步骤5 单击“确定”，即可向受邀账号发出邀请。

----结束

管理组织的待处理邀请

登录到管理账号后，您可以查看和管理组织创建的邀请，具体步骤如下。

步骤1 以组织管理员或管理账号的身份登录华为云，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 此时界面会向您展示邀请列表。接受邀请则单击对应邀请操作列的“接受”，拒绝邀请则单击对应邀请操作列的“拒绝”。

图 4-4 接受或拒绝邀请

----结束

4.3 创建账号

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

本章节包含如下内容：

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

约束与限制

- 组织管理员最多可以同时创建5个账号。
- 创建账号时绑定的邮箱不可以与其他账号重复。
- 在组织中创建的账号仅支持通过委托切换角色和IAM身份中心进行登录。
- 通过组织云服务创建的账号，财务默认托管于组织管理账号。

注意

创建账号时请确保输入的邮箱的正确性。

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，账号描述根据需要选择输入。注意，创建的账号名称不能与已有账号名称重复。

系统会默认提供委托名，可以保持默认，或者进行自定义修改。

图 4-6 新建账号

步骤5 （可选）为账号添加标签。

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

标签的设置说明如表4-3所示。

表 4-3 标签说明

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

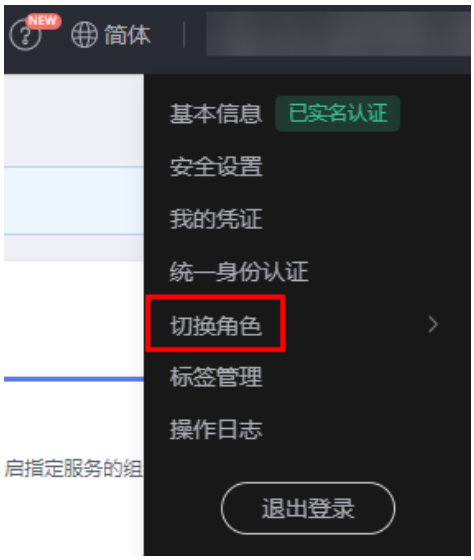
步骤6 单击“确定”，创建成功的账号将会显示在列表中。

----结束

通过委托登录创建的账号

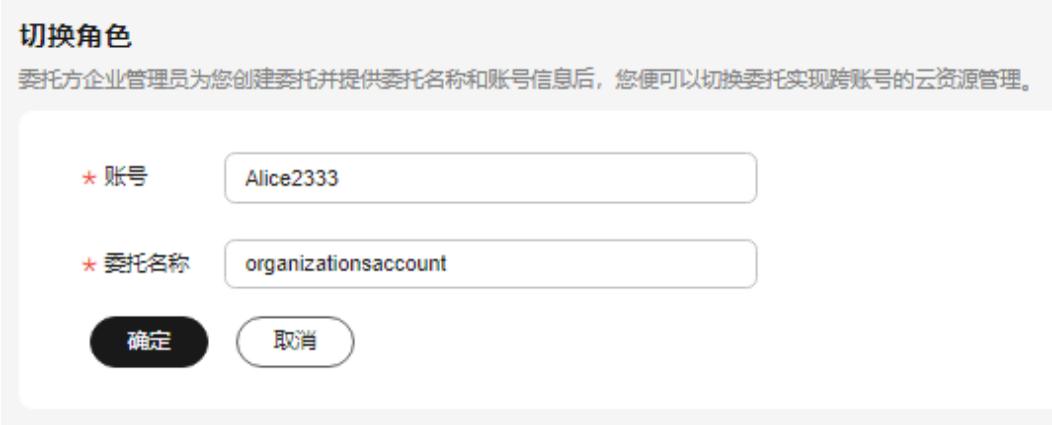
步骤1 鼠标移动至右上方的用户名，选择“切换角色”。

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

操作步骤

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

步骤2 选中要关闭的账号。单击组织结构树上方的“管理”，选择“关闭账号”。

图 4-9 关闭账号

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

步骤4 单击“确定”，完成账号关闭。

----结束

4.5 移动账号

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

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

步骤2 选中要移动的账号。单击组织结构树上方的管理，选择“移动账号”。

图 4-10 移动账号

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

----结束

4.6 查看账号详细信息

您可以随时查看组织内账号的详细信息，具体请参见如下步骤。

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

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

图 4-11 查看账号详情

----结束

4.7 移除成员账号

移除须知

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

- 在组织中创建的账号被移除组织或主动退出组织时，该账号创建成功的时间需大于七个自然日。
- 在组织中创建的账号被移除组织或主动退出组织时，需先将其转换为华为云账号。如何转换请参见将资源账号转为云账号。
- 邀请加入组织的账号为华为云账号时才支持移除组织或主动退出组织，详情请参见资源账号与华为云账号的差异。
- 已设置为委托管理员的账号无法从组织中移除或主动退出组织，需先**取消委托管理员**。
- 在组织中创建账号时默认创建的IAM委托，账号离开组织后并不会自动删除，组织管理账号可继续通过此委托访问成员账号的数据，如需终止组织管理账号的此访问权限，需成员账号手动删除委托。
- 在组织中创建的账号离开组织后，不会改变该账号与组织管理账号的财务托管模式。邀请加入组织的账号离开组织后，不会改变该账号原有的财务关系。如需调整请参见解除关联子账号。
- 当某个成员账号离开组织后，组织策略施加的权限限制将不再影响该账号，这意味着该账号可能拥有比之前更多的权限。当组织已启用可信服务，成员账号离开组织后将无法再使用该服务与组织集成的相关功能。
- 当成员账号离开组织时，所有附加到该账号的标签都将被删除。

移除账号

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

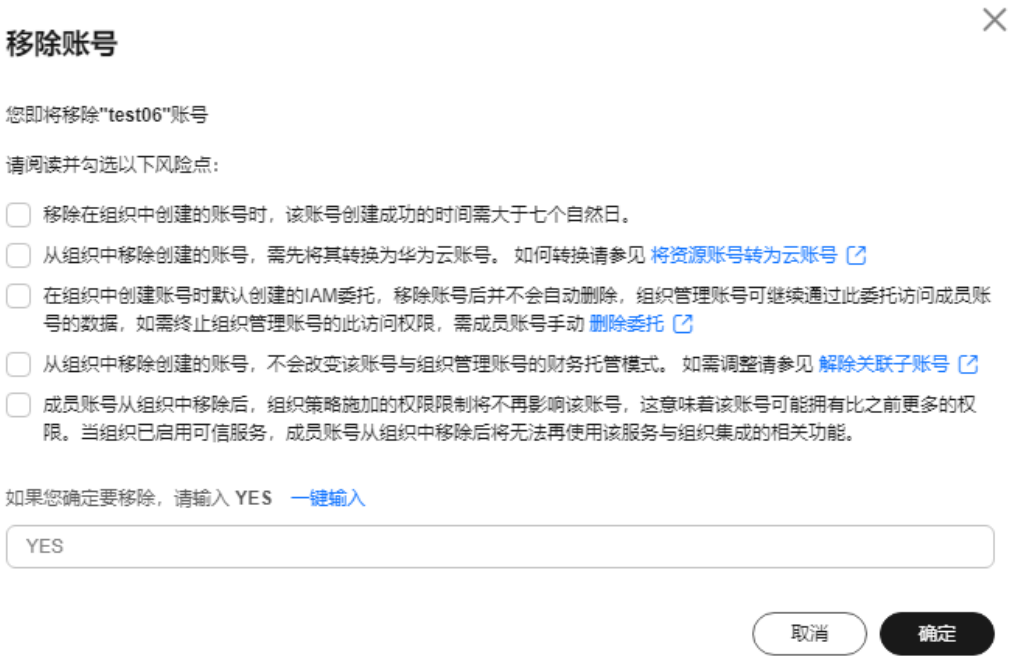
步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要移除的账号。单击组织结构树上方的管理，选择“移除账号”。

图 4-12 移除账号

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

图 4-13 确认移除账号



----结束

成员账号退出组织

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

已设置为委托管理员的账号无法退出组织，如需退出请先**取消委托管理员**。

步骤1 以成员账号的身份登录华为云，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”，在弹窗中阅读退出组织的注意事项后，输入“YES”，单击“确认”，完成退出组织操作。

图 4-14 确认退出组织

----结束

4.8 查看账号记录

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管理控制台，进入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不支持关闭操作。

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

图 4-15 账号列表

----结束

查看邀请记录

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入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 4-16 邀请记录

----结束

查看创建记录

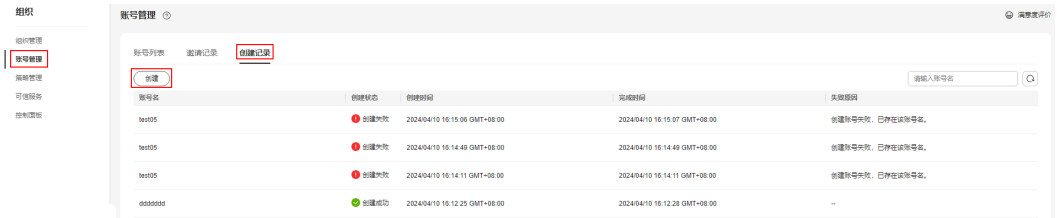
步骤1 以组织管理员或管理账号的身份登录管理控制台，进入Organizations控制台。

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。

步骤3 在列表左上方单击“创建”，可进行创建新账号加入组织的操作。

图 4-17 创建记录



----结束

5 服务控制策略管理

5.1 服务控制策略介绍

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

本节将从以下几方面为您介绍SCP：

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

测试 SCP 的影响

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

⚠ 注意

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

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

不受 SCP 限制的任务

您无法使用SCP来限制以下任务：

- 组织管理账号及其IAM用户执行的任何操作。
- 使用服务关联委托执行的任何操作。
- 由不支持SCP的云服务对支持SCP的云服务发起的API调用请求，将不受SCP限制。当前支持SCP的云服务和区域请参见：**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，在大多数场景下将不受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。现有的SCP系统策略请参见：**SCP系统策略列表**。

- **自定义策略**

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

权限控制原理

- **划定权限边界**

  SCP不直接进行授权，只划定权限边界。将SCP绑定到组织单元或者成员账号时，并没有直接对组织单元或成员账号授予操作权限，而是规定了成员账号或组织单元包含的成员账号的授权范围。IAM策略授予权限的有效性受SCP限制，只有在SCP允许范围内的权限才能生效。SCP禁止的权限操作，即便授予IAM用户权限，用户也不能执行相关操作。

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

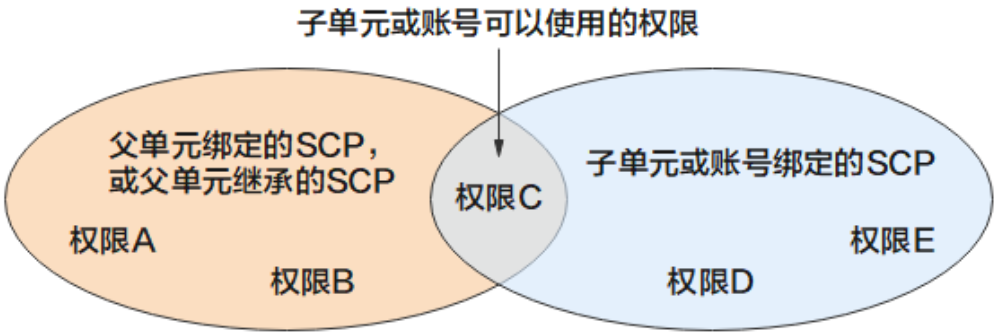
- **交集有效**

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

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

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

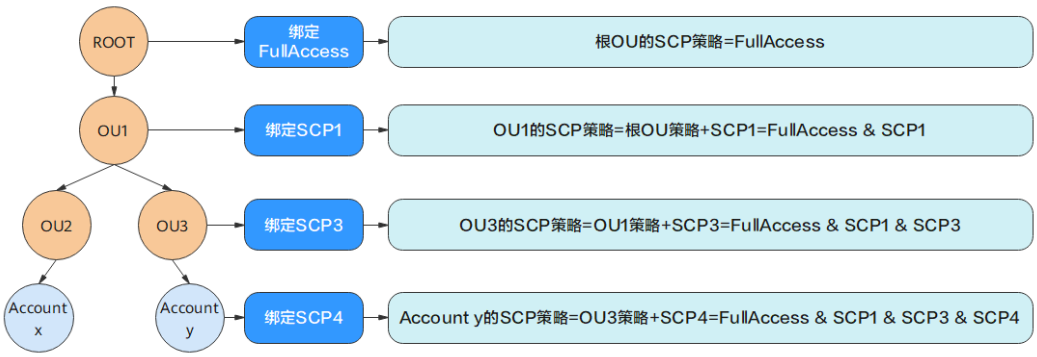
图 5-1 SCP 原理图



- **筛选继承**

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

图 5-2 SCP 继承规则



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

- 添加拒绝策略。拒绝策略会使用默认附加到每个OU和账号上的FullAccess SCP。此SCP将覆盖默认的隐式Deny，并明确允许所有权限从根组织单元传递到每个账号，除非创建并附加到相应OU或账号的其他SCP明确了拒绝权限。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

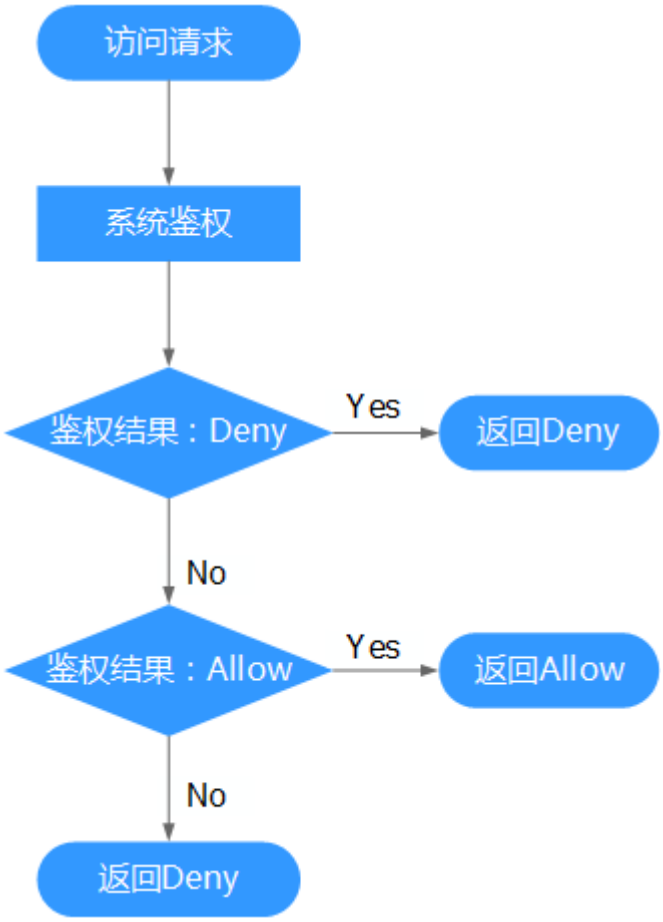
Effect（效果）包含两种：Allow（允许）和Deny（拒绝），分别表示允许或拒绝执行某操作的权限。

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"
      ]
    }
  }
 }
]
}
```

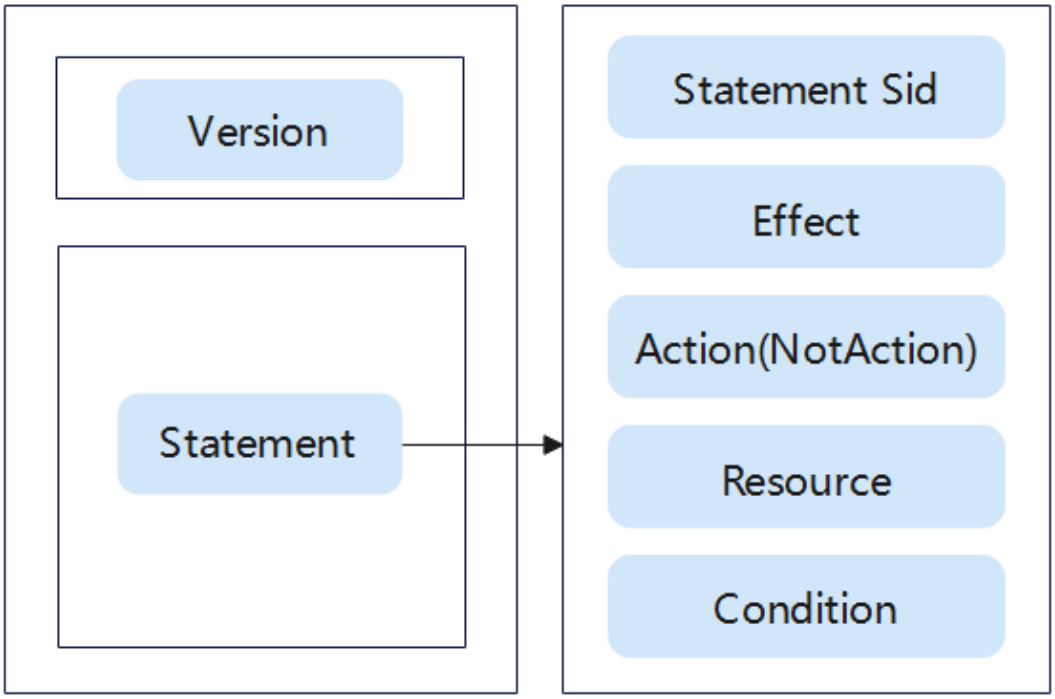
说明

SCP的语法与IAM身份策略的语法一致。

策略结构

策略结构包括Version（策略版本号）和Statement（策略权限语句）两部分，其中Statement元素的值可以是多个对象组成的数组，表示不同的权限约束。

图 5-4 策略结构



策略参数

策略参数包含Version和Statement两部分，下面介绍策略参数详细说明。

表 5-1 策略参数说明

参数	是否必选	含义	值
Version	必选	策略的版本。	5.0（不可自定义）

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

参数		是否必选	含义	值
	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。
	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："ecs:*:*:instance:*"：表示所有的ECS实例。

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。
- 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**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	字符串数组	用于控制跨服务访问。当身份主体向云服务发起访问时，该服务可能会转发身份主体的访问请求至其他服务，g:CalledVia包含服务转发访问的请求链中代表身份主体发出请求的服务列表。如服务转发身份主体的访问时，此条件键存在；如身份主体直接访问，则此条件键不存在。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，即第一个转发身份主体访问的服务。
g:CalledViaLast	字符串	与g:CalledVia相同，该属性特指g:CalledVia属性中的最后一个元素，即最后一个转发身份主体访问的服务。
g:CurrentTime	时间	接收到请求的时间。以ISO 8601格式表示，例如：2012-11-11T23:59:59Z。示例参见2。
g:DomainName	字符串	指请求者的账号名称。
g:DomainId	字符串	指请求者的账号ID。
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。当请求指定了具体的企业项目ID或访问的资源属于具体的企业项目时，如该API所对应授权项（Action）支持g:EnterpriseProjectId，则此条件键存在。此条件键为鉴权场景下使用的条件键，并非过滤条件，即不会过滤出符合该条件键所指定的企业项目下的资源。示例参见3。
g:MFAPresent	布尔值	指是否使用MFA多因素认证方式获取STS Security Token。仅在使用MFA认证登录控制台访问或使用MFA获取的委托会话发出请求时，此条件键为true。仅在STS Security Token发出请求时，此条件键存在。示例参考见4。
g:MFAAge	数值	指通过MFA多因素认证方式获取的STS Security Token的生效时长。仅在使用MFA认证登录控制台访问，或使用MFA获取的委托会话发出请求时，此条件键存在。单位为秒。
g:PrincipalAccount	字符串	与g:DomainId属性完全一致。
g:PrincipalUrn	字符串	指请求者身份主体的URN。不同身份类型的URN格式如下： IAM用户：iam::<domain-id>:user:<user-name> IAM委托会话：sts::<domain-id>:assumed-agency:<agency-name>/<session-name> 虚拟联邦用户：sts::<domain-id>:external-user:<idp-id>/<session-name> 示例参见5。

全局条件键	类型	说明
g:PrincipalIsRootUser	布尔值	指请求者身份主体是否是IAM根用户。所有请求中都会携带该属性。
g:PrincipalIsService	布尔值	指请求者身份主体是否是云服务，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	指请求者身份主体所属的组织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，仅在请求者存在所属组织时，此条件键存在。示例参见6。
g:PrincipalOrgManagementAccountId	字符串	指请求者身份主体所属组织的管理账号ID，仅在请求者存在所属组织时，此条件键存在。示例参见7。
g:PrincipalOrgPath	字符串	指请求者身份主体所属组织中的路径，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，仅在请求者存在所属组织时，此条件键存在。示例参见8。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	指请求者的身份主体名称，仅在请求者为云服务时，此条件键存在。示例参见9。
g:PrincipalTag/<tag-key>	字符串	指请求者身份主体携带的标签，标签键<tag-key>不区分大小写，仅请求者为带有标签的IAM用户、带有标签的信任委托、或带有会话标签的委托会话时，此条件键存在。示例参见10。
g:PrincipalType	字符串	指请求者的身份主体类型，共有三种类型：User、AssumedAgency、ExternalUser。当以IAM用户访问时，该属性取值为User；当以IAM委托会话访问时，取值为AssumedAgency；当以虚拟联邦用户访问时，取值为ExternalUser。
g:Referer	字符串	指请求携带的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。
g:RequestedRegion	字符串	指请求的目标区域（Region）。请求的目标云服务是区域级服务时，设置为对应的区域ID以进行控制，例如cn-north-4。仅在请求为部分区域级服务时，此条件键存在。
g:RequestTag/<tag-key>	字符串	指请求中携带的标签，标签键<tag-key>不区分大小写。当请求者在调用API时传入了标签（例如给资源添加标签的API、创建资源同时支持传入标签的API等），可以通过此条件键检查此请求是否包含对应标签。仅在支持g:RequestTag/<tag-key>的授权项（Action）中，当前请求的API传入标签时，此条件键存在。更多内容请参见SCP授权参考。示例参见11。

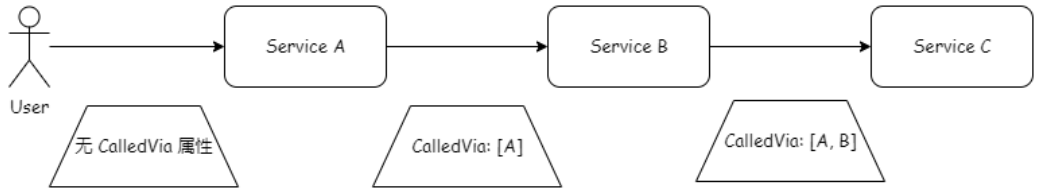
全局条件键	类型	说明
g:ResourceAccount	字符串	指请求所访问的资源的属主账号ID，仅在支持资源细粒度授权服务的授权项（Action）中，此条件键存在。更多内容请参见**SCP授权参考**。示例参见**12**。
g:ResourceOrgId	字符串	指请求所访问的资源的属主账号所在的组织ID。仅在支持资源细粒度鉴权的授权项（Action）中，且资源属主账号在组织内时，此条件键存在。更多内容请参见**SCP授权参考**。示例参见**13**。
g:ResourceOrgPath	字符串	指请求所访问的资源的属主账号在组织中的路径。仅在支持资源细粒度鉴权的授权项（Action）中，且资源属主账号在组织内时，此条件键存在。更多内容请参见**SCP授权参考**。示例参见**14**。
g:ResourceTag/<tag-key>	字符串	指请求所访问的资源身上携带的标签，标签键<tag-key>不区分大小写。用户可以通过该属性控制只能访问带有特定标签的资源。仅在支持g:ResourceTag/<tag-key>的授权项（Action）中，当前访问资源携带标签，此条件键存在。更多内容请参见**SCP授权参考**。示例参见**15**。
g:SecureTransport	布尔值	指请求是否使用了SSL协议。
g:SourceAccount	字符串	指云服务跨服务访问场景下，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。仅在支持g:SourceAccount的授权项（Action）中，此条件键存在。仅应在Principal是服务主体的资源策略中使用此条件键。示例参见**16**。
g:SourceUrn	字符串	指云服务跨服务访问场景下，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。仅在支持g:SourceUrn的授权项（Action）中，此条件键存在。仅应在Principal是服务主体的资源策略中使用此条件键。示例参见**17**。
g:SourceIdentity	字符串	指用户第一次通过STS服务的AssumeAgency API获取IAM临时凭据时指定其中的source_identity字段，且在后续的委托切换中不可再更改。仅在指定了source_identity的STS Security Token版本发出请求时，此条件键存在。示例参见**18**。
g:SourceIp	IP	指发起请求的源IP地址，专指来自公网的请求源IP。示例参见**19**。 **说明** 如果请求是从VPC内发起并经过VPC终端节点时，则会使用g:VpcSourceIp来取代g:SourceIp。如果不是通过VPC终端节点发起访问时，此条件键存在，但仅当通过公网发起访问时，该条件键可以作为有效的访问控制条件。云服务使用委托代表用户身份不经过公网发起访问时，此条件键不生效。

全局条件键	类型	说明
g:SourceVpc	字符串	指请求来源的VPC ID。仅当请求从VPC内部通过VPC终端节点访问云服务类型的VPC终端节点服务时，此条件键存在。
g:SourceVpce	字符串	指发起请求使用的VPC终端节点ID。仅当请求从VPC内部通过VPC终端节点访问云服务类型的VPC终端节点服务时，此条件键存在。示例参见20。
g:TagKeys	字符串数组	指请求中携带的所有标签的key组成的列表。仅在支持g:TagKeys的授权项（Action）中，当前请求的API传入标签时，此条件键存在。
g:TokenIssueTime	时间	指访问凭据中的STS Security Token的签发时间。仅在STS Security Token发出请求时，此条件键存在。
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	指请求者的身份主体ID，不同身份类型的ID格式如下： IAM用户：<user-id> IAM委托会话：<agency-id>:<session-name> 虚拟联邦用户：<idp-id>:<session-name>
g:UserName	字符串	IAM用户名。仅当请求者为IAM用户时，此条件键存在。
g:UserId	字符串	IAM用户ID。仅当请求者为IAM用户时，此条件键存在。
g:ViaService	布尔值	指该请求是否是由云服务代表身份主体转发访问发起的，当且仅当g:CalledVia属性非空时，该属性值为true。仅在STS Security Token发出请求时，此条件键存在。
g:VpcSourceIp	IP	指从VPC内发起的请求的源IP地址。仅当请求从VPC内部通过VPC终端节点访问云服务类型的VPC终端节点服务时，此条件键存在。

1. **g:CalledVia**

   用户身份主体请求服务A，服务A以用户身份主体请求服务B，服务B以用户身份主体请求服务C。在服务A收到的请求中，因为是用户身份主体直接请求，不会包含g:CalledVia属性；在服务B收到的请求中，因为是服务A代表用户身份主体发起，所以g:CalledVia会包含服务A的服务主体；在服务C收到的请求中g:CalledVia属性会包含服务A和服务B的服务主体，并且顺序与转发访问的请求链顺序一致，此时g:CalledViaFirst为服务A的服务主体，g:CalledViaLast则为服务B的服务主体，通过g:CalledViaFirst和g:CalledViaLast两个条件键可指定由哪个服务在转发访问链中第一个及最后一个调用。

图 5-5 g:CalledVia 使用场景



说明

用户通过管理控制台对云服务发起请求时，其CalledVia中将包含service.console。

示例：表示不允许通过管理控制台发起的请求调用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:EnterpriseProjectId**

   示例：此条件键为鉴权场景下使用的条件键，如下策略表示限制用户通过企业项目过滤查询虚拟私有云的访问执行操作：不允许用户请求GET /v1/{project_id}/vpcs时指定enterprise_project_id为xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx，即请求为/v1/{project_id}/vpcs?enterprise_project_id=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx时不可访问。

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

```
            "vpc:vpcs:list"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringEquals": {
                "g:EnterpriseProjectId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
            }
        }
    }]
}
```

说明

需要注意的是，g:EnterpriseProjectId并非过滤条件，即不会过滤出符合该条件键所指定的企业项目下的资源。仍以请求GET /v1/{project_id}/vpcs为例，当enterprise_project_id为all_granted_eps时，其接口行为是查询当前用户所有企业项目绑定的虚拟私有云。此时如用户已配置如上策略，接口将不会列出用户在策略中编写的g:EnterpriseProjectId所对应的企业项目下的虚拟私有云列表。

4. **g:MFAPresent**

   g:MFAPresent仅在STS Security Token版本发出请求时存在，如使用永久凭据发起请求等场景则此条件键不存在。

   示例：表示用户可以通过该属性控制云服务API仅能被经过多因素认证的身份调用。需注意搭配IfExists后缀以包括永久凭据发起请求此类g:MFAPresent条件键不存在的场景。

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "*"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "BoolIfExists": {
                "g:MFAPresent": "false"
            }
        }
    }]
}
```

5. **g:PrincipalUrn**

   示例：将以下SCP绑定至账号，不允许用户yyy创建资源共享实例。

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "ram:resourceShares:create"
        ],
        "Condition": {
            "StringEquals": {
                "g:PrincipalUrn": "iam::xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx:user:yyy"
            }
        }
    }]
}
```

6. **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-xxxxxxxxxx"

                }
            }
        }
    ]
}
```

7. **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xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx时视为匹配。

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

8. **g:PrincipalOrgPath**

   示例：表示条件键Condition在请求者账号属于组织单元ou-qqq时视为匹配。

```
{
    "Condition": {
        "StringMatch": {
            "g:PrincipalOrgPath": "o-xxx/r-yyy/ou-zzz/ou-qqq/*"
        }
    }
}
```

   示例：表示条件键Condition在请求者账号属于组织单元ou-qqq下任意子OU时视为匹配。

```
{
    "Condition": {
        "StringMatch": {
            "g:PrincipalOrgPath": "o-xxx/r-yyy/ou-zzz/ou-qqq/ou-*"
        }
    }
}
```

9. **g:PrincipalServiceName**

   示例：表示条件键Condition在请求者是RAM服务时视为匹配。

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

10. **g:PrincipalTag/<tag-key>**

    示例：表示当IAM用户上携带了{"department": "hr"}标签时，不允许访问IAM相关API。

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



```
        "Action": [
            "iam:*"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringEquals": {
                "g:PrincipalTag/department": "hr"
            }
        }
    }]
}
```

11. **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"
                }
            }
        }
    ]
}
```

12. **g:ResourceAccount**

    示例：表示拒绝用户使用指定用户以外的KMS密钥解密数据。

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "kms:cmk:decryptData"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "g:ResourceAccount": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
            }
        }
    }]
}
```

13. **g:ResourceOrgId**

    示例：表示拒绝用户使用指定组织以外的KMS密钥解密数据。

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "kms:cmk:decryptData"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
```



```
            "g:ResourceOrgId": "o-xxxxxxxx"
         }
      }
   }]
}
```

14. **g:ResourceOrgPath**

    示例：表示不允许用户用组织单元ou-qqq内账号的KMS密钥解密数据。

```
{
   "Version": "5.0",
   "Statement": [{
      "Effect": "Deny",
      "Action": [
         "kms:cmk:decryptData"
      ],
      "Resource": [
         "*"
      ],
      "Condition": {
         "StringMatch": {
            "g:ResourceOrgPath": "o-xxx/r-yyy/ou-zzz/ou-qqq/*"
         }
      }
   }]
}
```

    示例：表示不允许用户用组织单元ou-qqq下子OU内账号的KMS密钥解密数据。

```
{
   "Version": "5.0",
   "Statement": [{
      "Effect": "Deny",
      "Action": [
         "kms:cmk:decryptData"
      ],
      "Resource": [
         "*"
      ],
      "Condition": {
         "StringMatch": {
            "g:ResourceOrgPath": "o-xxx/r-yyy/ou-zzz/ou-qqq/ou-*"
         }
      }
   }]
}
```

15. **g:ResourceTag/<tag-key>**

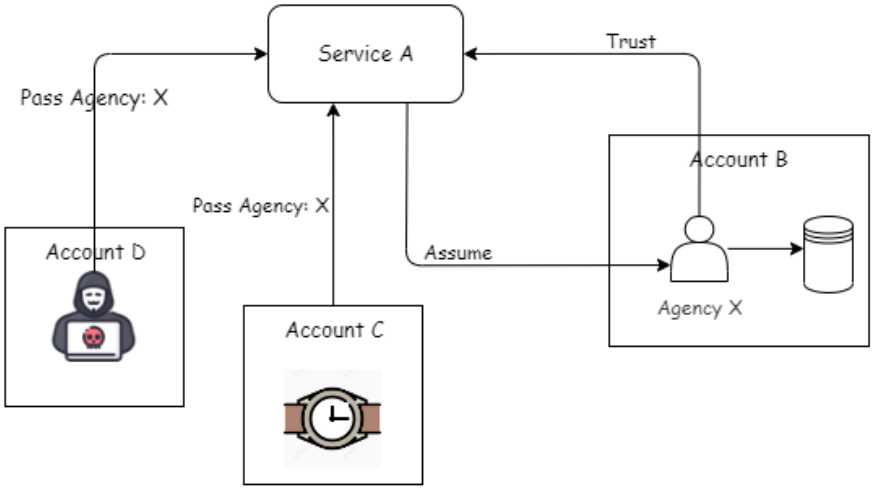
    示例：表示策略禁止用户修改带有{"team": "engineering"}标签的资源共享实例。

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


16. **g:SourceAccount**

    示例：Service A是一个用于记录活动的服务，能帮助用户（Account B）把其设备（Account C）触发的活动日志转储到用户指定的OBS桶里。为了能让Service A正常向桶中写入数据，Account B的管理员会为Service A创建一个委托/信任委托X来操作自己账号下的OBS桶。当用户（Account B）或某个设备（Account C）接入了Service A并触发请求后，Service A切换获取指定委托/信任委托X的临时身份凭据，然后向桶中写入数据。

    图 5-6 混淆代理

    由于委托/信任委托X的名字并非保密内容，如果攻击者（Account D）获取到了委托名并以同样的方式触发Service A，则其活动记录会被错误地记录在用户的OBS桶里。请注意，攻击者利用Service A的委托，间接地修改了用户的OBS桶，Service A的行为即被称为混淆代理。

    g:SourceAccount用于控制云服务为了哪个账号访问此次资源。以下策略仅允许Service A为xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx或yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy切换至对应委托的会话。

```
{
    "Version": "5.0",
    "Statement": [{
        "Principal": {
            "Service": [
                "Service.A"
            ]
        },
        "Action": [
            "sts:agencies:assume"
        ],
        "Condition": {
            "StringEquals": {
                "g:sourceAccount": [
                    "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
                    "yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy"
                ]
            }
        }
    }]
}
```

17. **g:SourceUrn**

    与g:SourceAccount相同，该条件键也用于解决混淆代理问题。假设用户设备（xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx）的资源定义分为手表（watch）和手环

（bracelet）两种，每种都有若干个。g:SourceUrn用于控制云服务为了哪个资源访问此次资源。以下策略表示仅允许Service A为符合条件的手表或手环切换至对应委托的会话。

```
{
   "Version": "5.0",
   "Statement": [{
      "Principal": {
         "Service": [
            "Service.A"
         ]
      },
      "Action": [
         "sts:agencies:assume"
      ],
      "Condition": {
         "StringEquals": {
            "g:sourceUrn": [
               "alarm:*:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx:watch:*",
               "alarm:*:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx:bracelet:*"
            ]
         }
      }
   }]
}
```

18. **g:SourceIdentity**

    示例：表示不允许source_identity为yyyyy的身份切换该委托。

```
{
   "Version": "5.0",
   "Statement": [{
      "Effect": "Deny",
      "Principal": {
         "IAM": [
            "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
         ]
      },
      "Action": [
         "sts:agencies:assume"
      ],
      "Condition": {
         "StringEquals": {
            "g:SourceIdentity": "yyyyy"
         }
      }
   }]
}
```

19. **g:SourceIp**

    示例：将以下策略绑定至账号，当该账号源IP地址在xxx.xx.xx.0/24范围内时，不允许通过编程或控制台访问KMS。

    须知

    源IP地址需要为公网IP，请勿在该条件键中包含内网地址。

```
{
   "Version": "5.0",
   "Statement": [{
      "Effect": "Deny",
      "Action": [
         "kms:cmk:decryptData"
      ],
      "Resource": [
```



```
            "*"
        ],
        "Condition": {
            "IpAddress": {
                "g:SourceIp": "xxx.xx.xx.0/24"
            }
        }
    }]
}
```

需注意：初始请求上下文中的g:SourceIp、g:SourceVpce、g:SourceVpc、g:VpcSourceIp不会在服务代表身份主体转发访问的后续请求中继续传递，因此使用这些条件键控制访问权限时，可能导致云服务需代表身份主体转发访问的请求被拒绝。实际场景中，建议使用g:CalledVia以允许转发访问请求。

例外：身份主体由控制台发起的公网访问可视为身份主体直接由公网进行编程访问，因此由控制台代表身份主体转发访问的此次请求中将包含有初始的g:SourceIp。

示例：将以下策略绑定至账号，拒绝该账号源IP地址在xxx.xx.xx.0/24范围外时，通过编程或控制台访问KMS；同时该策略允许云服务代表身份主体转发访问请求，即不会禁用其他云服务访问KMS。

```
{
    "Version": "5.0",
    "Statement": [{
            "Effect": "Deny",
            "Action": [
                "kms:cmk:decryptData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "NotIpAddress": {
                    "g:SourceIp": "xxx.xx.xx.0/24"
                },
                "Bool": {
                    "g:ViaService": "false"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [
                "kms:cmk:decryptData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "NotIpAddress": {
                    "g:SourceIp": "xxx.xx.xx.0/24"
                },
                "StringEqualsIfExists": {
                    "g:CalledViaFirst": "service.console",
                    "g:CalledViaLast": "service.console"
                }
            }
        }
    ]
}
```

20. **g:SourceVpce**

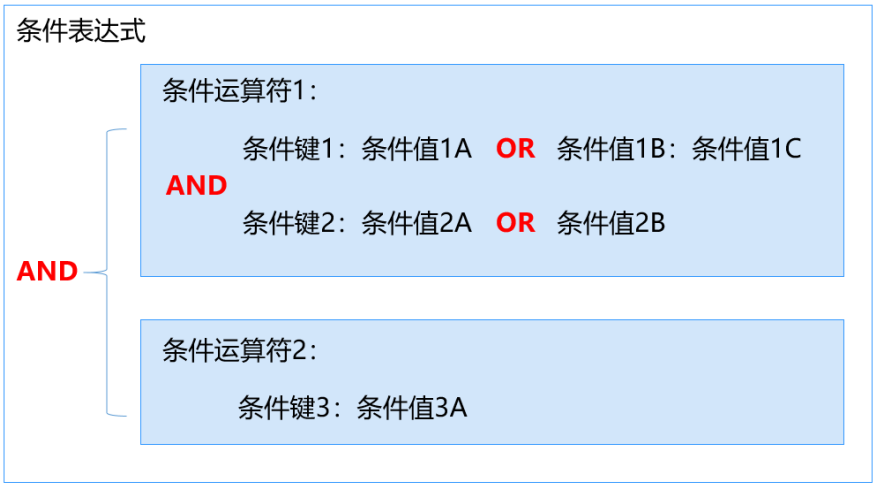
    示例：将以下策略绑定至账号，拒绝该账号通过VPC终端节点 "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" 外的方式访问KMS；同时该策略允许云服务代表身份主体转发访问请求。


```
{
   "Version": "5.0",
   "Statement": [{
      "Effect": "Deny",
      "Action": [
         "kms:cmk:decryptData"
      ],
      "Resource": [
         "*"
      ],
      "Condition": {
         "StringNotEquals": {
            "g:SourceVpce": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
         },
         "Bool": {
            "g:ViaService": "false"
         }
      }
   }]
}
```

- 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 5-7 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。
	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的请求者删除和修改资源共享实例。

```
{
   "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管理控制台，进入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”。

步骤3 在弹窗中勾选确认框，然后单击“确定”，完成SCP功能启用。

图 5-8 启用 SCP

----结束

禁用 SCP

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

注意

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

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入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 5-9 禁用 SCP

步骤3 在弹窗中单击“确定”，完成SCP功能禁用。

----结束

5.3 创建 SCP

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

操作步骤

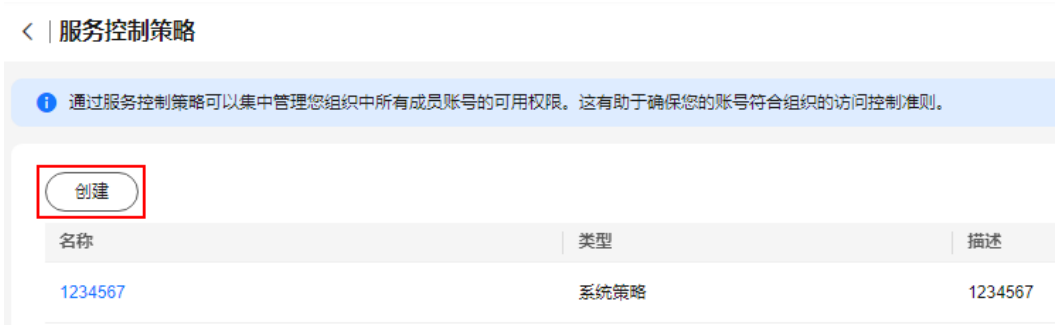
步骤1 以组织管理员或管理账号的身份登录管理控制台，进入Organizations控制台。

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 5-10 进入 SCP 管理页

步骤3 单击“创建”，进入SCP创建页面。

图 5-11 创建 SCP



步骤4 输入策略名称。新创建的策略名称不能与已有策略名称重复。

（可选）输入策略描述。

步骤5 在策略内容左侧可以直接编写JSON格式的策略内容。

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

说明

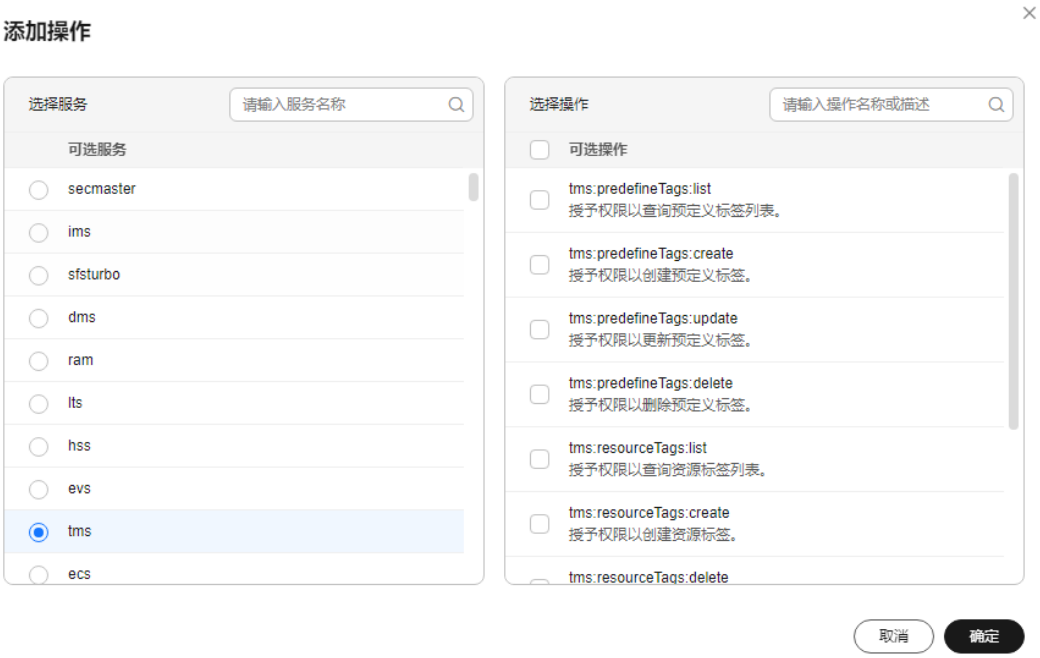
自定义策略版本号（Version）固定为5.0，不可修改。

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。

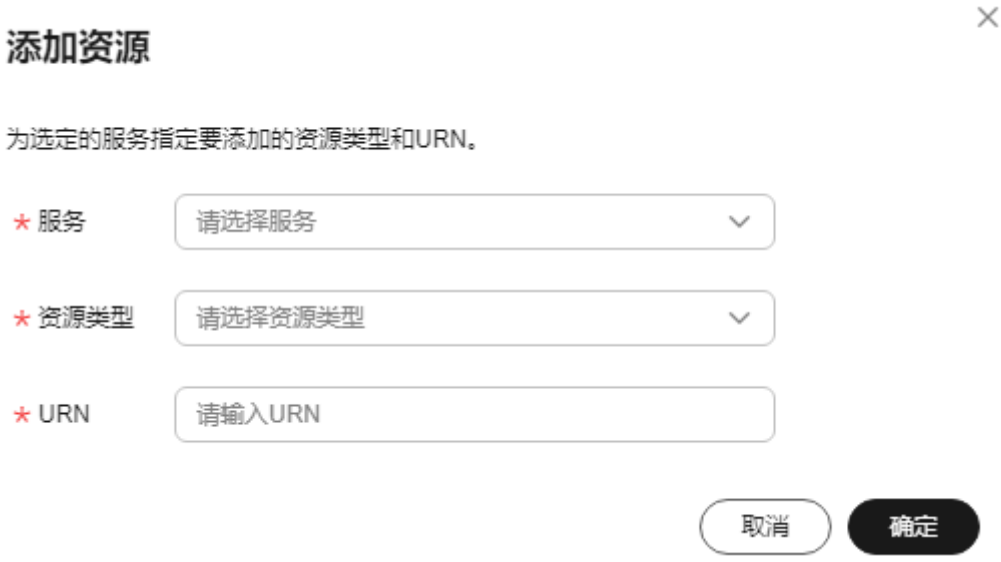
- 添加操作：单击“+”号，可以选择服务的操作项进行添加，添加成功的操作项会自动显示在Action元素下。如**图5-12**所示。

图 5-12 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5-13所示。

图 5-13 添加资源



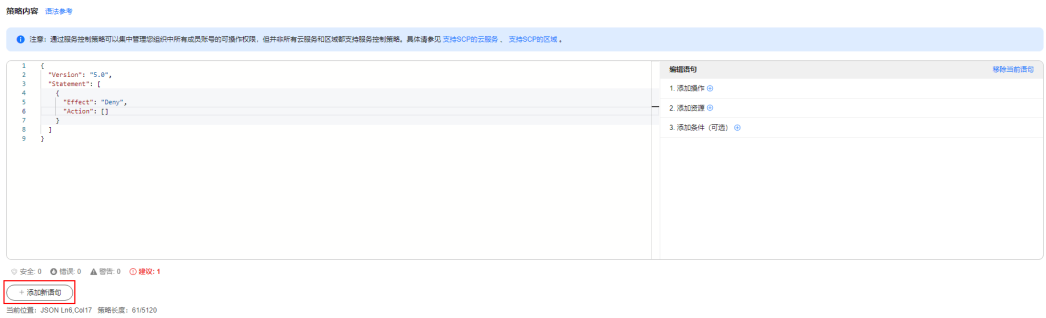
- 添加条件（可选）：单击“+”号，添加条件键和运算符，规定策略生效的条件。如图5-14所示。

图 5-14 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 5-15 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 5-16 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管理控制台，进入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”，在弹窗中输入“确认”，单击“确定”。

图 5-17 修改 SCP

步骤4 进入编辑策略页面，按需修改“策略名称”和“策略描述”。如#org_03_0036/fig977144619493所示。

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管理控制台，进入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 5-18 删除 SCP

----结束

5.5 绑定和解绑 SCP

管理账号可以为根、OU和账号绑定和解绑SCP。

约束与限制

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

绑定 SCP

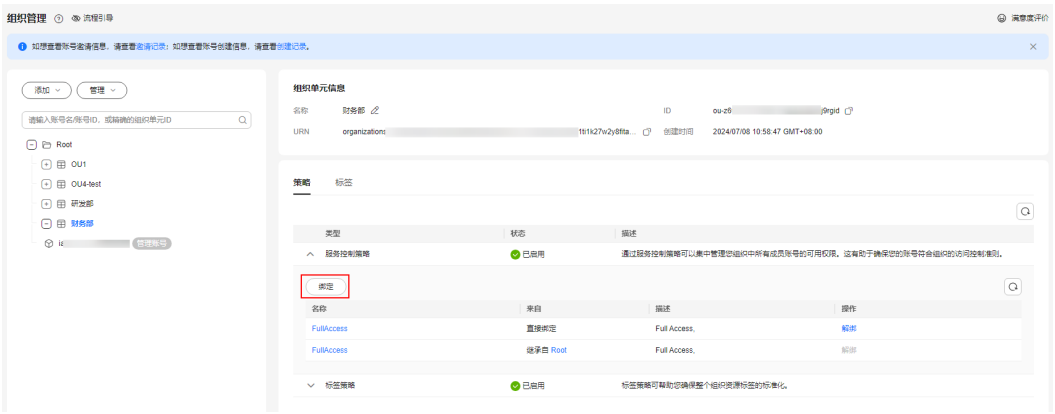
方式一：

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 5-19 绑定 SCP



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

图 5-20 绑定 SCP

----结束

解绑 SCP

方法一：

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

步骤2 选中要解绑SCP的OU或者账号。

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

步骤4 在弹窗中输入“确认”，单击“确定”，完成策略解绑。

图 5-21 解绑 SCP

说明

OU和账号至少直接绑定一个SCP，最后一个直接绑定策略，不可解绑。

----结束

方式二：

步骤1 在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”。

图 5-22 解绑 SCP

步骤5 在弹窗中输入“确认”，单击“确定”，完成策略解绑。

图 5-23 解绑 SCP

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

```
{
    "Version":"5.0",
    "Statement":[
        {
            "Effect":"Deny",
            "Action":["ecs:*:*"],
            "Resource":["*"],
            "Condition":{
                "StringEquals":{
                    "g:RequestedRegion":"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的云服务同时也支持IAM的身份策略。

计算

序号	服务名称	相关文档
1	弹性云服务器（ECS）	弹性云服务器 ECS
2	裸金属服务（BMS）	裸金属服务器 BMS
3	镜像服务（IMS）	镜像服务 IMS
4	弹性伸缩（AS）	弹性伸缩 AS

存储

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

网络

序号	服务名称	相关文档
1	虚拟私有云（VPC）	虚拟私有云 VPC
2	弹性公网IP（EIP）	弹性公网IP EIP
3	NAT网关（NAT）	NAT网关 NAT
4	弹性负载均衡（ELB）	弹性负载均衡 ELB
5	VPC终端节点（VPCEP）	VPC终端节点 VPCEP
6	云专线（DC）	云专线 DC
7	企业路由器（ER）	企业路由器 ER

序号	服务名称	相关文档
8	全球加速服务（GA）	全球加速服务 GA
9	云连接（CC）	云连接 CC

容器

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

大数据

序号	服务名称	相关文档
1	数据湖探索（DLI）	数据湖探索 DLI
2	数据治理中心（DataArts Studio）	数据治理中心 DataArts Studio
3	数据仓库服务 GaussDB（DWS）	数据仓库服务 GaussDB（DWS）
4	MapReduce服务（MRS）	MapReduce服务 MRS
5	云搜索服务（CSS）	云搜索服务 CSS

CDN 与智能边缘

序号	服务名称	相关文档
1	内容分发网络（CDN）	内容分发网络 CDN

数据库

序号	服务名称	相关文档
1	云数据库（RDS）	云数据库 RDS
2	文档数据库服务（DDS）	文档数据库服务 DDS
3	云数据库 GaussDB	云数据库 GaussDB
4	数据复制服务（DRS）	数据复制服务 DRS
5	云数据库 TaurusDB	云数据库 TaurusDB

安全与合规

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

IoT 物联网

序号	服务名称	相关文档
1	设备接入（IoTDA）	设备接入 IoTDA

应用中间件

序号	服务名称	相关文档
1	分布式缓存服务（DCS）	分布式缓存服务 DCS
2	微服务引擎（CSE）	微服务引擎 CSE
3	API网关（APIG）	API网关 APIG

开发与运维

序号	服务名称	相关文档
1	应用管理与运维平台（Servicestage）	应用管理与运维平台 ServiceStage
2	软件开发生产线（CodeArts）	软件开发生产线 CodeArts
3	流水线（CodeArts Pipeline）	流水线 Codearts Pipeline
4	性能测试 CodeArts PerfTest	性能测试 CodeArts PerfTest

企业应用

序号	服务名称	相关文档
1	云解析服务（DNS）	云解析服务 DNS
2	云桌面（Workspace）	云桌面 Workspace

管理与监管

序号	服务名称	相关文档
1	消息通知服务（SMN）	消息通知服务 SMN
2	云日志服务（LTS）	云日志服务 LTS
3	统一身份认证（IAM）	统一身份认证 IAM
4	安全令牌服务（STS）	安全令牌服务 STS
5	资源编排服务（RFS）	资源编排服务 RFS
6	IAM身份中心（IdentityCenter）	IAM身份中心
7	组织（Organizations）	组织 Organizations
8	资源访问管理（RAM）	资源访问管理 RAM
9	企业项目管理服务 （EPS）	企业项目管理 EPS
10	标签管理服务（TMS）	标签管理服务 TMS
11	配置审计（Config）（原 资源管理服务 RMS）	配置审计 Config
12	访问分析（AccessAnalyzer）	访问分析 IAM Access Analyzer
13	云审计服务（CTS）	云审计服务 CTS
14	资源治理中心（RGC）	资源治理中心 RGC
15	应用运维管理（AOM）	应用运维管理 AOM

序号	服务名称	相关文档
16	云监控服务 （ CES ）	云监控服务 CES

用户服务

序号	服务名称	相关文档
1	费用中心	费用中心
2	成本中心	成本中心
3	账号中心	账号中心
4	企业中心	企业中心
5	消息中心	消息中心
6	客户运营能力	客户运营能力

迁移

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

5.9 支持 SCP 的区域

当前支持使用SCP的区域如下表所示：

说明

支持SCP的区域与支持IAM身份策略的区域相同。

表 5-10 支持 SCP 的区域

区域名称	区域代码
亚太-新加坡	ap-southeast-3
亚太-曼谷	ap-southeast-2
亚太-雅加达	ap-southeast-4
华东-上海一	cn-east-3
华东-上海二	cn-east-2

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

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 5-11 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 • ecs:FlavorId • ecs:VpcId • ecs:SubnetId • ecs:PortId • ecs:KmsKeyId • eip:AssociatePublicIp • ecs:AvailabilityZone • evs:Encrypted • cbr:VaultId • ecs:SSHKeyPairName • ecs:SupportAgentType • ecs:ImageSupportAgentType • ecs:ImageType • ecs:OsVersion • ecs:OsType • ecs:ImagePlatform
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 *	ecs:FlavorId -

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:KmsKeyId • ecs:VolumeId 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:KmsKeyId • ecs:VolumeId evs:Encrypted
ecs:cloudServers:listServerBlockDevices	授予查询弹性云服务器磁盘信息的权限。	list	instance *	-
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:KmsKeyId • ecs:SSHKeyPairName • ecs:ImageType • ecs:OsVersion • ecs:OsType • ecs:ImagePlatform
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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:KmsKeyId • ecs:SSHKeyPairName 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 *	• eip:AssociatePublicIp • ecs:SubnetId • ecs:PortId -

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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5-12展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-12 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:associateInstance • iam:agencies:pass • eip:bandwidths:insertPublicIps

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/cloudservers	ecs:cloudServers:createServers	• eip:publicIps:create • eip:publicIps:associateInstance • iam:agencies:pass • eip:bandwidths:insertPublicIps
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	-
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

API	对应的授权项	依赖的授权项
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	-
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	-
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	-

API	对应的授权项	依赖的授权项
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}/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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/cloudservers/actions/change-charge-mode	ChangeServerChargeMode	• billing:order:pay • billing:subscription:renew
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5-13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 5-13 ECS 支持的资源类型

资源类型	URN
instance	ecs:<region>:<account-id>:instance:<server-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5-14。
  - 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 5-14 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。
ecs:FlavorId	string	多值	根据请求参数中指定的规格ID过滤访问。
ecs:VpcId	string	多值	根据请求参数中指定的网络ID过滤访问。
ecs:SubnetId	string	多值	根据请求参数中指定的子网ID过滤访问。
ecs:KmsKeyId	string	多值	根据请求参数中指定的加密密钥ID过滤访问。
ecs:ServerId	string	单值	根据云服务器ID过滤访问。
ecs:SSHKeyPairName	string	单值	根据请求参数中指定的SSH密钥对的名称过滤访问。
ecs:AvailabilityZone	string	单值	根据请求参数中指定的可用区名称过滤访问。
ecs:PortId	string	多值	根据请求参数中指定的portId过滤访问。
ecs:SupportAgentType	string	多值	根据请求中指定的agent类型过滤访问。
ecs:ImageSupportAgentType	string	多值	根据请求中指定的镜像支持的agent类型过滤访问。
ecs:VolumeId	string	单值	根据请求中指定的卷ID过滤访问。
ecs:ImageType	string	单值	根据请求中指定镜像的类型过滤访问（如：公共镜像、私有镜像、共享镜像、市场镜像）。
ecs:OsType	string	单值	根据请求中指定镜像的操作系统类型过滤访问（如：Linux、Windows）。

服务级条件键	类型	单值/多值	说明
ecs:OsVersion	string	单值	根据请求中指定镜像的操作系统版本过滤访问（如：CentOS 7.3 64bit）。
ecs:ImagePlatform	string	单值	根据请求中指定镜像的平台过滤访问（如：Windows、Ubuntu、Red Hat、SUSE、CentOS）。

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 5-15 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>
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 • g:RequestTag/<tag-key> • eip:AssociatePublicIp • bms:Flavorld • bms:VpcId • bms:SubnetId • bms:KmsKeyId • evs:Encrypted • bms:ImageId • bms:SSHKeyPairName • bms:AvailabilityZone • bms:VolumeType
bms:servers:showBaremetalServer	授予查询单个裸机详情的权限。	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: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 • evs:Encrypted • bms:VolumeType • bms:VolumeId
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>
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 • evs:Encrypted • bms:SSHKeyPairName
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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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:SubnetId
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5-16展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-16 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	-

API	对应的授权项	依赖的授权项
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	eip:publicIps:create eip:publicIps:associateInstance iam:agencies:pass eip:bandwidths:insertPublicIps -
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	-
GET /v1/{project_id}/baremetalservers/{server_id}/tags	bms:servers:showBaremetalServerTags	-
POST /v1/{project_id}/baremetalservers/action	bms:servers:start	-

API	对应的授权项	依赖的授权项
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 5-17 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 5-18 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。
bms:SubnetId	string	多值	根据请求参数中指定的子网ID过滤访问。

服务级条件键	类型	单值/多值	说明
bms:ImageId	string	单值	根据请求参数中指定的镜像ID过滤访问。
bms:SSHKeyPairName	string	单值	按请求中的keyName参数筛选访问。
bms:AvailabilityZone	string	单值	按请求中的availabilityZone参数筛选访问。
bms:VolumeType	string	多值	根据云硬盘的类型过滤访问。
bms:VolumeId	string	单值	根据指定的卷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 5-19 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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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的标签。	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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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5-20展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-20 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	-

API	对应的授权项	依赖的授权项
POST /v1/cloudimages/{image_id}/file	ims:images:export	• obs:object:GetObject • obs:object:PutObject
• 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 • POST /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	ims:images:get
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

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/images/{image_id}/tags/action	ims:images:setOrDeleteTags	• ims:images:setTags • ims:images:deleteTags
• 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5-21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 5-21 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。

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 5-22 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。

5.10.1.4 弹性伸缩 AS

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AS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AS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AS的相关操作。

表 5-23 AS 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
as:scalingGroup:create	授予创建弹性伸缩组的权限。	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys • as:ScalingConfigId • as:VpcId • as:VpcSubnetId • as:ElbPoolId • as:MaxInstanceSize • as:MinInstanceSize

授权项	描述	访问级别	资源类型（*为必须）	条件键
as:scalingGroup:delete	授予删除弹性伸缩组的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:list	授予查询弹性伸缩组列表的权限。	list	-	g:EnterpriseProjectId
as:scalingGroup:get	授予查询弹性伸缩组详情的权限。	read	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:update	授予修改弹性伸缩组的权限。	write	-	• g:EnterpriseProjectId • as:ScalingConfigId • as:VpcSubnetId • as:ElbPoolId • as:MaxInstanceSize • as:MinInstanceSize
as:scalingGroup:resume	授予启用弹性伸缩组的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:pause	授予停用弹性伸缩组的权限。	write	scalingGroup*	• 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
as:scalingConfig:create	授予创建弹性伸缩配置的权限。	write	-	• as:EcsInstanceId • as:EcsInstanceType • as:EcsFlavorId • as:ImageId • as:ImsDiskImageId • as:CbrDiskSnapshotId • as:EcsServerGroupId • as:EvsEncrypted • as:KmsKeyId • as:EvsVolumeType • as:KpsSSHKeyPairName • as:AssociatePublicIp
as:scalingConfig:delete	授予删除弹性伸缩配置的权限。	write	scalingConfig*	-
as:scalingConfig:batchDelete	授予批量删除弹性伸缩配置的权限。	write	scalingConfig*	-
as:scalingConfig:list	授予查询弹性伸缩配置列表的权限。	list	scalingConfig*	-
as:scalingConfig:get	授予查询弹性伸缩配置详情的权限。	read	scalingConfig*	-
as:scalingGroup:batchAddInstances	授予批量添加弹性伸缩实例的权限。	write	scalingGroup*	• 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
as:scalingGroup:batchRemoveInstances	授予批量移除弹性伸缩实例的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:batchSetInstancesProtect	授予批量设置弹性伸缩实例保护的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:batchSetInstancesUnprotect	授予批量取消弹性伸缩实例保护的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:batchSetInstancesStandby	授予批量设置弹性伸缩实例备用的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:batchSetInstancesExitStandby	授予批量设置弹性伸缩实例取消备用的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:deleteInstance	授予移除弹性伸缩实例的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:listInstances	授予查询弹性伸缩实例列表的权限。	list	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingPolicy:create	授予创建弹性伸缩策略的权限。	write	-	g:EnterpriseProjectId
as:scalingPolicy:list	授予查询弹性伸缩策略列表的权限。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
as:scalingPolicy:get	授予查询弹性伸缩策略详情的权限。	read	scalingPolicy*	g:EnterpriseProjectId
as:scalingPolicy:update	授予修改弹性伸缩策略的权限。	write	-	g:EnterpriseProjectId
as:scalingPolicy:delete	授予删除弹性伸缩策略的权限。	write	scalingPolicy*	g:EnterpriseProjectId
as:scalingPolicy:execute	授予手动执行弹性伸缩策略的权限。	write	scalingPolicy*	g:EnterpriseProjectId
as:scalingPolicy:resume	授予启用弹性伸缩策略的权限。	write	scalingPolicy*	g:EnterpriseProjectId
as:scalingPolicy:pause	授予停用弹性伸缩策略的权限。	write	scalingPolicy*	g:EnterpriseProjectId
as:scalingPolicy:batchPause	授予批量停用弹性伸缩策略的权限。	write	scalingPolicy*	g:EnterpriseProjectId
as:scalingPolicy:batchResume	授予批量启用弹性伸缩策略的权限。	write	scalingPolicy*	g:EnterpriseProjectId
as:scalingPolicy:batchDelete	授予批量删除弹性伸缩策略的权限。	write	scalingPolicy*	g:EnterpriseProjectId
as:scalingPolicy:listAll	授予查询租户弹性伸缩策略列表的权限。	list	-	g:EnterpriseProjectId
as:scalingGroup:listActivityLogs	授予查询伸缩活动日志列表的权限。	list	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingPolicy:listExecuteLogs	授予查询伸缩策略执行日志列表的权限。	list	scalingPolicy*	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
as::tagResource	授予创建标签的权限。	tagging	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
as::untagResource	授予删除标签的权限。	tagging	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
as::listTags	授予查询所有资源标签列表的权限。	list	-	-
as::listTagsForResource	授予查询指定资源标签的权限。	list	-	g:EnterpriseProjectId
as::listResourcesByTag	授予根据标签查询资源的权限。	list	-	• g:RequestTag/<tag-key> • g:TagKeys
as:scalingGroup:createLifecycleHook	授予创建生命周期挂钩的权限。	write	-	g:EnterpriseProjectId
as:scalingGroup:listLifecycleHooks	授予查询生命周期挂钩列表的权限。	list	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:getLifecycleHook	授予查询生命周期挂钩详情的权限。	read	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:updateLifecycleHook	授予修改生命周期挂钩的权限。	write	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
as:scalingGroup:deleteLifecycleHook	授予删除生命周期挂钩的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:callbackInstanceHook	授予生命周期挂钩回调的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:listInstanceHooks	授予查询实例挂起信息列表权限。	list	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:createNotification	授予创建通知的权限。	write	-	g:EnterpriseProjectId
as:scalingGroup:listNotifications	授予查询通知列表的权限。	list	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:deleteNotification	授予删除通知的权限。	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:getQuotas	授予查询伸缩实例和伸缩策略配额的权限。	read	-	g:EnterpriseProjectId
as::listQuotas	授予查询伸缩实例和伸缩策略配额的权限。	read	-	-

AS的API通常对应着一个或多个授权项。表5-24展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-24 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /autoscaling-api/v1/{project_id}/scaling_group	as:scalingGroup:create	-
DELETE /autoscaling-api/v1/{project_id}/scaling_group/{scaling_group_id}	as:scalingGroup:delete	-
GET /autoscaling-api/v1/{project_id}/scaling_group	as:scalingGroup:list	-
GET /autoscaling-api/v1/{project_id}/scaling_group/{scaling_group_id}	as:scalingGroup:get	-
PUT /autoscaling-api/v1/{project_id}/scaling_group/{scaling_group_id}	as:scalingGroup:update	-
POST /autoscaling-api/v1/{project_id}/scaling_group/{scaling_group_id}/action	as:scalingGroup:resume	-
POST /autoscaling-api/v1/{project_id}/scaling_group/{scaling_group_id}/action	as:scalingGroup:pause	-
POST /autoscaling-api/v1/{project_id}/scaling_configurationCreateScalingConfig	as:scalingConfig:create	-
DELETE /autoscaling-api/v1/{project_id}/scaling_configuration/{scaling_configuration_id}	as:scalingConfig:delete	-
POST /autoscaling-api/v1/{project_id}/scaling_configurations	as:scalingConfig:batchDelete	-
GET /autoscaling-api/v1/{project_id}/scaling_configuration	as:scalingConfig:list	-
GET /autoscaling-api/v1/{project_id}/scaling_configuration/{scaling_configuration_id}	as:scalingConfig:get	-

API	对应的授权项	依赖的授权项
POST /autoscaling-api/v1/{project_id}/scaling_group_instance/{scaling_group_id}/action	• as:scalingGroup:batchAddInstances • as:scalingGroup:batchSetInstancesProtect • as:scalingGroup:batchRemoveInstances • as:scalingGroup:batchSetInstancesStandby • as:scalingGroup:batchSetInstancesUnprotect • as:scalingGroup:batchSetInstancesExitStandby	-
DELETE /autoscaling-api/v1/{project_id}/scaling_group_instance/{instance_id}	as:scalingGroup:deleteInstance	-
GET /autoscaling-api/v1/{project_id}/scaling_group_instance/{scaling_group_id}/list	as:scalingGroup:listInstances	-
POST /autoscaling-api/v1/{project_id}/scaling_policy	as:scalingPolicy:create	-
GET /autoscaling-api/v1/{project_id}/scaling_policy/{scaling_group_id}/list	as:scalingPolicy:list	-
GET /autoscaling-api/v1/{project_id}/scaling_policy/{scaling_policy_id}	as:scalingPolicy:get	-
PUT /autoscaling-api/v1/{project_id}/scaling_policy/{scaling_policy_id}	as:scalingPolicy:update	-
DELETE /autoscaling-api/v1/{project_id}/scaling_policy/{scaling_policy_id}	as:scalingPolicy:delete	-
POST /autoscaling-api/v1/{project_id}/scaling_policy/{scaling_policy_id}/action	• as:scalingPolicy:resume • as:scalingPolicy:pause • as:scalingPolicy:execute	-
POST /autoscaling-api/v1/{project_id}/scaling_policies/action	as:scalingPolicy:batchDelete as:scalingPolicy:batchPause as:scalingPolicy:batchResume	-

API	对应的授权项	依赖的授权项
POST /autoscaling-api/v2/{project_id}/scaling_policy	as:scalingPolicy:create	-
GET /autoscaling-api/v2/{project_id}/scaling_policy	as:scalingPolicy:listAll	-
GET /autoscaling-api/v2/{project_id}/scaling_policy/{scaling_resource_id}/list	as:scalingPolicy:list	-
GET /autoscaling-api/v2/{project_id}/scaling_policy/{scaling_policy_id}	as:scalingPolicy:get	-
PUT /autoscaling-api/v2/{project_id}/scaling_policy/{scaling_policy_id}	as:scalingPolicy:update	-
GET /autoscaling-api/v1/{project_id}/scaling_activity_log/{scaling_group_id}	as:scalingGroup:listActivityLogs	-
GET /autoscaling-api/v2/{project_id}/scaling_activity_log/{scaling_group_id}	as:scalingGroup:listActivityLogs	-
GET /autoscaling-api/v1/{project_id}/scaling_policy_execute_log/{scaling_policy_id}	as:scalingPolicy:listExecuteLogs	-
POST /autoscaling-api/v1/{project_id}/{resource_type}/{resource_id}/tags/action	as::tagResource	-
POST /autoscaling-api/v1/{project_id}/{resource_type}/{resource_id}/tags/action	as::untagResource	-
GET /autoscaling-api/v1/{project_id}/{resource_type}/tags	as::listTags	-
GET /autoscaling-api/v1/{project_id}/{resource_type}/{resource_id}/tags	as::listTagsForResource	-
POST /autoscaling-api/v1/{project_id}/{resource_type}/resource_instances/action	as::listResourcesByTag	-

API	对应的授权项	依赖的授权项
POST /autoscaling-api/v1/{project_id}/scaling_lifecycle_hook/{scaling_group_id}	as:scalingGroup:createLifecycleHook	-
GET /autoscaling-api/v1/{project_id}/scaling_lifecycle_hook/{scaling_group_id}/list	as:scalingGroup:listLifecycleHooks	-
GET /autoscaling-api/v1/{project_id}/scaling_lifecycle_hook/{scaling_group_id}/{lifecycle_hook_name}	as:scalingGroup:getLifecycleHook	-
PUT /autoscaling-api/v1/{project_id}/scaling_lifecycle_hook/{scaling_group_id}/{lifecycle_hook_name}	as:scalingGroup:updateLifecycleHook	-
DELETE /autoscaling-api/v1/{project_id}/scaling_lifecycle_hook/{scaling_group_id}/{lifecycle_hook_name}	as:scalingGroup:deleteLifecycleHook	-
PUT /autoscaling-api/v1/{project_id}/scaling_instance_hook/{scaling_group_id}/callback	as:scalingGroup:callbackInstanceHook	-
GET /autoscaling-api/v1/{project_id}/scaling_instance_hook/{scaling_group_id}/list	as:scalingGroup:listInstanceHooks	-
PUT /autoscaling-api/v1/{project_id}/scaling_notification/{scaling_group_id}	as:scalingGroup:createNotification	-
DELETE /autoscaling-api/v1/{project_id}/scaling_notification/{scaling_group_id}/{topic_urn}	as:scalingGroup:deleteNotification	-
GET /autoscaling-api/v1/{project_id}/scaling_notification/{scaling_group_id}	as:scalingGroup:listNotifications	-

API	对应的授权项	依赖的授权项
GET /autoscaling-api/v1/{project_id}/quotas/{scaling_group_id}	as:scalingGroup:getQuotas	-
GET /autoscaling-api/v1/{project_id}/quotas	as::listQuotas	-

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。

AS定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-25 AS 支持的资源类型

资源类型	URN
scalingGroup	as:<region>:<account-id>:scalingGroup:<scaling-group-id>
scalingConfig	as:<region>:<account-id>:scalingConfig:<scaling-config-id>
scalingPolicy	as:<region>:<account-id>:scalingPolicy:<scaling-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as:）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。

AS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 5-26 AS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
as:ScalingConfigId	String	单值	指定特定伸缩配置创建虚拟机。
as:VpcId	String	单值	限制虚拟机使用的VPC ID。
as:VpcSubnetId	String	多值	限制虚拟机使用的子网 ID。
as:ElbPoolId	String	多值	限制虚拟机加入的ELB后端服务器组ID。
as:MaxInstanceSize	Integer	单值	限制伸缩组的最大实例数。
as:MinInstanceSize	Integer	单值	限制伸缩组的最小实例数。
as:EcsInstanceId	String	单值	限制指定已有实例创建伸缩配置。
as:EcsInstanceType	String	单值	限制创建虚拟机的类型：竞价or按需。
as:EcsFlavorId	String	多值	限制创建虚拟机使用的规格Id。
as:ImageId	String	单值	限制创建虚拟机使用的镜像Id。
as:ImsDiskImageId	String	多值	限制创建虚拟机使用的磁盘镜像Id。
as:CbrDiskSnapshotId	String	多值	限制创建虚拟机使用的磁盘云备份ID。
as:EcsServerGroupId	String	单值	限制创建虚拟机使用的云服务器组ID。
as:EvsEncrypted	Boolean	单值	限制是否支持磁盘加密。
as:KmsKeyId	String	多值	限制磁盘加密使用的密钥ID。
as:EvsVolumeType	String	多值	限制创建虚拟机使用的磁盘类型。
as:KpsSSHKeyPairName	String	单值	限制创建虚拟机使用的keypair名称。

服务级条件键	类型	单值/多值	说明
as:AssociatePublicIp	Boolean	单值	限制虚拟机使用eip。

5.10.2 存储

5.10.2.1 云备份 CBR

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。IAMSCP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。

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cbr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cbr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cbr的相关操作。

表 5-27 cbr 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
cbr:tasks:list	授予查询任务列表权限。	list	task *	-
			-	g:EnterpriseProjectId
cbr:tasks:get	授予查询单个任务权限。	read	task *	g:EnterpriseProjectId
cbr:member:create	授予添加备份成员权限。	permission_management	backup *	g:EnterpriseProjectId
			-	cbr:TargetOrgPaths
cbr:member:update	授予更新备份成员状态权限。	write	backup *	g:EnterpriseProjectId
cbr:member:get	授予获取备份成员详情权限。	read	backup *	g:EnterpriseProjectId
cbr:member:list	授予获取备份成员列表权限。	list	backup *	-
cbr:member:delete	授予删除指定备份成员权限。	permission_management	backup *	g:EnterpriseProjectId
cbr:vaults:showCheckpoint	授予查询备份还原点权限。	read	-	-
cbr:vaults:showSummary	授予查询存储库总览权限。	list	-	-
cbr:vaults:replicate	授予复制备份还原点权限。	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:backup	授予创建备份还原点权限。	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:sync	授予同步备份还原点权限。	write	vault *	• 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
cbr:vaults:create	授予创建存储库权限。	write	vault *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • cbr:PolicyId
cbr:vaults:get	授予查询指定存储库权限。	read	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:list	授予查询存储库列表权限。	list	vault *	-
			-	g:EnterpriseProjectId
cbr:vaults:update	授予修改存储库权限。	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:delete	授予删除存储库权限。	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:removeResources	授予移除资源权限。	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:addResources	授予添加资源权限。	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:setResources	授予设置存储库资源权限。	write	vault *	• 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
cbr:vaults:associatePolicy	授予设置存储库策略权限。	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:dissociatePolicy	授予解除存储库策略权限。	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:listExternalVaults	授予查询其他区域的存储库列表权限。	list	vault *	-
cbr:vaults:migrateResources	授予迁移资源权限。	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:backups:sync	授予同步备份权限。	write	vault *	g:EnterpriseProjectId
cbr:backups:get	授予查询指定备份权限。	read	backup *	g:EnterpriseProjectId
cbr:backups:showMetadata	授予查询备份元数据权限。	read	backup *	g:EnterpriseProjectId
cbr:backups:list	授予查询所有备份权限。	list	backup *	-
			-	g:EnterpriseProjectId
cbr:backups:delete	授予删除备份权限。	write	backup *	g:EnterpriseProjectId
cbr:backups:replicate	授予复制备份权限。	write	backup *	g:EnterpriseProjectId
cbr:backups:restore	授予备份恢复权限。	write	backup *	g:EnterpriseProjectId
cbr:backups:update	授予更新备份权限。	write	backup *	g:EnterpriseProjectId
cbr:policies:list	授予查询策略列表权限。	list	policy *	-
cbr:policies:create	授予创建策略权限。	write	policy *	-
			-	cbr:EnabledPolicy

授权项	描述	访问级别	资源类型（*为必须）	条件键
cbr:policies:get	授予查询单个策略权限。	read	policy *	-
cbr:policies:update	授予修改策略权限。	write	policy *	-
			-	cbr:EnabledPolicy
cbr:policies:delete	授予删除策略权限。	write	policy *	-
cbr:vaults:listProtectables	授予查询可保护资源权限。	list	-	g:EnterpriseProjectId
cbr:vaults:getProtectables	授予查询指定可保护资源权限。	read	-	-
cbr:backups:queryReplicationCapability	授予查询复制能力权限。	list	-	-
cbr:backups:checkAgent	授予查询agent状态权限。	read	-	-
cbr:vaults:listResourceInstances	授予查询存储库资源实例权限。	list	vault *	-
cbr:vaults:bulkCreateOrDeleteTags	授予批量添加删除存储库资源标签权限。	write	vault *	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cbr:vaults:setTags	授予添加存储库资源标签权限。	write	vault *	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cbr:vaults:deleteTags	授予删除存储库资源标签权限。	write	vault *	g:ResourceTag/<tag-key>
			-	g:TagKeys
cbr:vaults:getTags	授予查询存储库资源标签权限。	read	vault *	g:ResourceTag/<tag-key>
cbr:vaults:listProjectTags	授予查询存储库项目标签权限。	list	vault *	-
cbr:backups:listStorageUsage	授予查询容量统计权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
cbr:vaults:updateOrder	授予变更权限。	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:agents:addPath	授予新增备份路径权限。	write	agent *	-
cbr:agents:get	授予查询指定客户端权限。	read	agent *	-
cbr:agents:update	授予修改客户端权限。	write	agent *	-
cbr:agents:register	授予注册客户端权限。	write	agent *	-
cbr:agents:delete	授予移除客户端权限。	write	agent *	-
cbr:agents:removePath	授予移除备份路径权限。	write	agent *	-
cbr:agents:list	授予查询客户端列表权限。	list	agent *	-
cbr:backups:migratesCreate	授予租户迁移权限。	write	-	-
cbr:backups:migratesIndex	授予查询迁移权限。	read	-	-
cbr:organizationPolicies:create	授予创建组织策略权限。	write	-	-
cbr:organizationPolicies:listPolicyDetail	授予查询组织策略部署状态列表权限。	read	-	-
cbr:organizationPolicies:delete	授予删除组织策略权限。	write	-	-
cbr:organizationPolicies:update	授予修改组织策略权限。	write	-	-
cbr:organizationPolicies:list	授予查询组织策略列表权限。	list	-	-
cbr:organizationPolicies:get	授予查询单个组织策略权限。	read	-	-

cbr的API通常对应着一个或多个授权项。表5-28展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-28 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}/operation-logs	cbr:tasks:list	-
GET /v3/{project_id}/operation-logs/{operation_log_id}	cbr:tasks:get	-
POST /v3/{project_id}/backups/{backup_id}/members	cbr:member:create	-
PUT /v3/{project_id}/backups/{backup_id}/members/{member_id}	cbr:member:update	-
GET /v3/{project_id}/backups/{backup_id}/members/{member_id}	cbr:member:get	-
GET /v3/{project_id}/backups/{backup_id}/members	cbr:member:list	-
DELETE /v3/{project_id}/backups/{backup_id}/members/{member_id}	cbr:member:delete	-
GET /v3/{project_id}/checkpoints/{checkpoint_id}	cbr:vaults:showCheckpoint	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/vaults/summary	cbr:vaults:showSummary	-
POST /v3/{project_id}/checkpoints/replicate	cbr:vaults:replicate	-
POST /v3/{project_id}/checkpoints	cbr:vaults:backup	• ecs:cloudServers:listServersDetails • evs:volumes:list
POST /v3/{project_id}/checkpoints/sync	cbr:vaults:sync	-
POST /v3/{project_id}/vaults	cbr:vaults:create	• ecs:cloudServers:listServersDetails • evs:volumes:list
POST /v3/{project_id}/vaults/order	cbr:vaults:create	• ecs:cloudServers:listServersDetails • evs:volumes:list
GET /v3/{project_id}/vaults/{vault_id}	cbr:vaults:get	-
GET /v3/{project_id}/vaults	cbr:vaults:list	-
PUT /v3/{project_id}/vaults/{vault_id}	cbr:vaults:update	-
PUT /v3/{project_id}/vaults/batch-update	cbr:vaults:update	-
DELETE /v3/{project_id}/vaults/{vault_id}	cbr:vaults:delete	-
POST /v3/{project_id}/vaults/{vault_id}/removeresources	cbr:vaults:removeResources	-
POST /v3/{project_id}/vaults/{vault_id}/addresources	cbr:vaults:addResources	• ecs:cloudServers:listServersDetails • evs:volumes:list

API	对应的授权项	依赖的授权项
PUT /v3/{project_id}/vaults/{vault_id}/set-resources	cbr:vaults:setResources	-
POST /v3/{project_id}/vaults/{vault_id}/associatepolicy	cbr:vaults:associatePolicy	-
POST /v3/{project_id}/vaults/{vault_id}/dissociatepolicy	cbr:vaults:dissociatePolicy	-
GET /v3/{project_id}/vaults/external	cbr:vaults:listExternalVaults	-
POST /v3/{project_id}/vaults/{vault_id}/migrateresources	cbr:vaults:migrateResources	-
POST /v3/{project_id}/backups/sync	cbr:backups:sync	-
GET /v3/{project_id}/backups/{backup_id}	cbr:backups:get	-
GET /v3/{project_id}/backups/{backup_id}/metadata	cbr:backups:showMetadata	-
GET /v3/{project_id}/backups	cbr:backups:list	-
DELETE /v3/{project_id}/backups/{backup_id}	cbr:backups:delete	-
POST /v3/{project_id}/backups/{backup_id}/replicate	cbr:backups:replicate	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/backups/{backup_id}/restore	cbr:backups:restore	• ecs:cloudServers:listServersDetails • evs:volumes:list
PUT /v3/{project_id}/backups/{backup_id}	cbr:backups:update	-
GET /v3/{project_id}/policies	cbr:policies:list	-
POST /v3/{project_id}/policies	cbr:policies:create	-
GET /v3/{project_id}/policies/{policy_id}	cbr:policies:get	-
PUT /v3/{project_id}/policies/{policy_id}	cbr:policies:update	-
DELETE /v3/{project_id}/policies/{policy_id}	cbr:policies:delete	-
GET /v3/{project_id}/protectables/{protectable_type}/instances	cbr:vaults:listProtectables	• ecs:cloudServers:listServersDetails • evs:volumes:list
GET /v3/{project_id}/protectables/{protectable_type}/instances/{instance_id}	cbr:vaults:getProtectables	• ecs:cloudServers:listServersDetails • evs:volumes:list
GET /v3/{project_id}/replication-capabilities	cbr:backups:queryReplicationCapability	-
POST /v3/{project_id}/agent/check	cbr:backups:checkAgent	-
POST /v3/{project_id}/vault/resource_instances/action	cbr:vaults:listResourceInstances	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/vault/{vault_id}/tags/action	cbr:vaults:bulkCreateOrDeleteTags	-
POST /v3/{project_id}/vault/{vault_id}/tags	cbr:vaults:setTags	-
DELETE /v3/{project_id}/vault/{vault_id}/tags/{key}	cbr:vaults:deleteTags	-
GET /v3/{project_id}/vault/{vault_id}/tags	cbr:vaults:getTags	-
GET /v3/{project_id}/vault/tags	cbr:vaults:listProjectTags	-
GET /v3/{project_id}/storage_usage	cbr:backups:listStorageUsage	-
PUT /v3/{project_id}/orders/{order_id}	cbr:vaults:updateOrder	-
POST /v3/{project_id}/agents/{agent_id}/add-path	cbr:agents:addPath	-
GET /v3/{project_id}/agents/{agent_id}	cbr:agents:get	-
PUT /v3/{project_id}/agents/{agent_id}	cbr:agents:update	-
POST /v3/{project_id}/agents	cbr:agents:register	-
DELETE /v3/{project_id}/agents/{agent_id}	cbr:agents:delete	-
POST /v3/{project_id}/agents/{agent_id}/remove-path	cbr:agents:removePath	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/agents	cbr:agents:list	-
POST /v3/migrates	cbr:backups:migratesCreate	-
GET /v3/migrates	cbr:backups:migratesIndex	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-29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。

cbr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 5-29 cbr 支持的资源类型

资源类型	URN
vault	cbr:<region>:<account-id>:vault:<vault-id>
policy	cbr:<region>:<account-id>:policy:<policy-id>
task	cbr:<region>:<account-id>:task:<task-id>
backup	cbr:<region>:<account-id>:backup:<backup-id>
agent	cbr:<region>:<account-id>:agent:<agent-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cbr:）仅适用于对应服务的操作，详情请参见表5-30。
  - 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。

cbr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 5-30 cbr 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
cbr:TargetOrgPaths	string	单值	cbr服务添加备份成员API请求中指定的目标账号所属的组织路径。
cbr:VaultId	string	单值	根据请求参数中指定的存储库ID过滤访问。
cbr:PolicyId	string	单值	根据请求参数中指定的策略ID过滤访问。
cbr:EnabledPolicy	boolean	单值	根据策略是否开启过滤访问。

5.10.2.2 云硬盘 EVS

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EVS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EVS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EVS的相关操作。

表 5-31 EVS 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
evs:volumes:create	授予创建云硬盘的权限。	write	volume *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • evs:Encrypted • cbr:VaultId
evs:volumes:list	授予查询云硬盘列表的权限。	list	-	g:EnterpriseProjectId
evs:volumes:get	授予查询云硬盘的权限。	read	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:volumes:delete	授予删除云硬盘的权限。	write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:volumes:update	授予更新云硬盘的权限。	write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:volumes:resize	授予扩容云硬盘的权限。	write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:volumes:modifyQos	授予修改云硬盘QoS的权限。	write	volume *	• 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
evs:volumes:revert	授予从回收站还原云硬盘的权限。	write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:recycle_policy:get	授予查询回收站策略的权限。	read	-	-
evs:recycle_policy:update	授予更新回收站策略的权限。	write	-	-
evs:volumes:changeChargeMode	授予变更云硬盘计费模式的权限。	write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:snapshots:create	授予创建云硬盘快照的权限。	write	snapshot *	-
			volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:snapshots:list	授予查询云硬盘快照列表的权限。	list	-	g:EnterpriseProjectId
evs:snapshots:get	授予查询云硬盘快照的权限。	read	-	g:EnterpriseProjectId
evs:snapshots:delete	授予删除云硬盘快照的权限。	write	-	g:EnterpriseProjectId
evs:snapshots:update	授予更新云硬盘快照的权限。	write	-	g:EnterpriseProjectId
evs:snapshots:rollback	授予回滚快照到云硬盘的权限。	write	-	g:EnterpriseProjectId
evs:types:get	授予查询云硬盘类型的权限。	read	-	-
evs:quotas:get	授予查询云硬盘配额的权限。	read	-	-
evs:volumes:tagResource	授予添加云硬盘标签的权限。	write	volume *	• 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
			-	• g:RequestTag/<tag-key> • g:TagKeys
evs:volumes:unTagResource	授予删除云硬盘标签的权限。	write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	g:TagKeys
evs:volumes:listTags	授予查询项目下所有云硬盘标签的权限。	list	-	-
evs:volumes:listTagsForResource	授予查询云硬盘标签的权限。	read	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:volumes:listResourcesByTag	授予通过标签查询云硬盘实例列表的权限。	list	-	g:TagKeys
evs:volumes:use	授予ECS、BMS使用磁盘的权限。	write	-	g:EnterpriseProjectId

EVS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
POST /v2.1/{project_id}/cloudvolumes	evs:volumes:create	billing:order:pay
POST /v2/{project_id}/cloudvolumes	evs:volumes:create	-
POST /v3/{project_id}/cloudvolumes	evs:volumes:create	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/cloudvolumes/detail	evs:volumes:list	-
GET /v2/{project_id}/cloudvolumes/{volume_id}	evs:volumes:get	-
DELETE /v2/{project_id}/cloudvolumes/{volume_id}	evs:volumes:delete	-
PUT /v2/{project_id}/cloudvolumes/{volume_id}	evs:volumes:update	-
POST /v2.1/{project_id}/cloudvolumes/{volume_id}/action	evs:volumes:resize	billing:order:pay
POST /v5/{project_id}/volumes/batch-extend	evs:volumes:resize	billing:order:pay
POST /v2/{project_id}/cloudvolumes/{volume_id}/action	evs:volumes:resize	-
PUT /v5/{project_id}/cloudvolumes/{volume_id}/qos	evs:volumes:modifyQos	-
POST /v2/{project_id}/cloudvolumes/unsubscribe	evs:volumes:delete	billing:subscription:unsubscribe
POST /v2/{project_id}/cloudvolumes/change-charge-mode	evs:volumes:changeChargeMode	• billing:order:pay • billing:subscription:renew
POST /v2/{project_id}/cloudsnapshots	evs:snapshots:create	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/cloudsnapshots/detail	evs:snapshots:list	-
GET /v2/{project_id}/cloudsnapshots/{snapshot_id}	evs:snapshots:get	-
DELETE /v2/{project_id}/cloudsnapshots/{snapshot_id}	evs:snapshots:delete	-
PUT /v2/{project_id}/cloudsnapshots/{snapshot_id}	evs:snapshots:update	-
POST /v2/{project_id}/cloudsnapshots/{snapshot_id}/rollback	evs:snapshots:rollback	-
POST /v2/{project_id}/cloudvolumes/{volume_id}/tags/action	evs:volumes:tagResource	-
POST 01 /v2/{project_id}/cloudvolumes/{volume_id}/tags/action	evs:volumes:unTagResource	-
GET /v2/{project_id}/cloudvolumes/tags	evs:volumes:listTags	-
GET /v2/{project_id}/cloudvolumes/{volume_id}/tags	evs:volumes:listTagsForResource	-
POST /v2/{project_id}/cloudvolumes/resource_instances/action	evs:volumes:listResourcesByTag	-

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。

EVS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 EVS 支持的资源类型

资源类型	URN
imageCache	evs:<region>:<account-id>:imageCache:<imageCache-id>
snapshot	evs:<region>:<account-id>:snapshot:<snapshot-id>
volume	evs:<region>:<account-id>:volume:<volume-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evs:）仅适用于对应服务的操作，详情请参见表5-34。
  - 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。

EVS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 5-34 EVS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
evs:Encrypted	boolean	单值	根据云硬盘是否加密过滤访问。
evs:KmsKeyId	string	单值	根据云硬盘的密钥ID过滤访问。

服务级条件键	类型	单值/多值	说明
evs:ImageId	string	单值	根据镜像ID过滤访问。
evs:BackupId	string	单值	根据备份ID过滤访问。
evs:SnapshotId	string	单值	根据快照ID过滤访问。
evs:AvailabilityZone	string	单值	根据云硬盘的可用区过滤访问。
evs:SourceAvailabilityZone	string	单值	根据源AZ过滤访问。
evs:VolumeType	string	单值	根据云硬盘的类型过滤访问。
evs:VolumeSize	numeric	单值	根据云硬盘的大小过滤访问。
evs:VolumeIops	numeric	单值	根据云硬盘的IOPS过滤访问。
evs:VolumeThroughput	numeric	单值	根据云硬盘的吞吐量过滤访问。
evs:ChargingMode	string	单值	根据云硬盘的计费模式过滤访问。
evs:ServerServiceType	string	单值	根据云服务器服务类型过滤访问。
evs:VolumeId	string	单值	根据云硬盘ID过滤访问。

5.10.2.3 高性能弹性文件服务 SFS Turbo

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SFS Turbo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SFS Turbo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SFS Turbo的相关操作。

表 5-35 sfsturbo 支持的授权项

操作项	描述	访问级别	资源类型（*为必须）	条件键
sfsturbo:shares:createShare	授予创建弹性文件系统的权限。	write	shares *	• g:EnterpriseProjectId • g:TagKeys • g:RequestTag/<tag-key> • sfsturbo:CryptKeyId • cbr:VaultId
sfsturbo:shares:deleteShare	授予删除弹性文件系统的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:getAllShares	授予查询弹性文件系统列表的权限。	list	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
sfsturbo:shares:getShare	授予查询弹性文件系统的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

操作项	描述	访问级别	资源类型（*为必须）	条件键
sfsturbo:shares:extendShare	授予扩容弹性文件系统的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateHpcShare	授予更新弹性文件系统的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateShareSecurityGroup	授予修改文件系统绑定的安全组的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:addTag	授予创建弹性文件系统共享标签的权限。	tagging	shares *	• g:ResourceTag/<tag-key> • g:TagKeys
sfsturbo:shares:getTag	授予查询弹性文件系统共享标签的权限。	read	shares *	g:EnterpriseProjectId
sfsturbo:shares:deleteTag	授予删除弹性文件系统共享标签的权限。	tagging	shares *	• g:ResourceTag/<tag-key> • g:TagKeys
sfsturbo:shares:batchResTag	授予批量添加弹性文件系统共享标签的权限。	tagging	shares *	• g:ResourceTag/<tag-key> • g:TagKeys
sfsturbo:shares:getAllTag	授予查询弹性文件系统共享标签列表的权限。	list	-	g:EnterpriseProjectId
sfsturbo:shares:renameShare	授予修改弹性文件系统名称的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createDataRepositoryTask	授予创建弹性文件系统数据存储库任务的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

操作项	描述	访问级别	资源类型（*为必须）	条件键
sfsturbo:shares:deleteDataRepositoryTask	授予删除弹性文件系统数据存储库任务的权限。	write	shares *	• g:ResourceTag/<tag-key> g:EnterpriseProjectId
sfsturbo:shares:getDataRepositoryTask	授予查询弹性文件系统数据存储库任务的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:getAllDataRepositoryTasks	授予查询弹性文件系统数据存储库任务列表的权限。	list	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:getAZInfo	授予查询当前地区可用区信息的权限。	read	-	-
sfsturbo:shares:getQuota	授予查询弹性文件系统配额的权限。	read	-	-
sfsturbo:shares:getFlavors	授予查询弹性文件系统规格的权限。	read	-	-
sfsturbo:shares:checkShareName	授予检查弹性文件系统名称的权限。	read	-	-
sfsturbo:shares:showFsDir	授予查询弹性文件系统目录的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deleteFsDir	授予删除弹性文件系统目录的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createFsDirQuota	授予创建弹性文件系统目录配额的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showFsDirQuota	授予查询弹性文件系统目录配额的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

操作项	描述	访问级别	资源类型（*为必须）	条件键
sfsturbo:shares:deleteFsDirQuota	授予删除弹性文件系统目录配额的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateFsDirQuota	授予更新弹性文件系统目录配额的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:batchCreateFsDirQuotas	授予批量创建弹性文件系统目录配额的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:listFsDirQuotas	授予查询弹性文件系统目录配额列表的权限。	list	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:batchDeleteFsDirQuotas	授予批量删除弹性文件系统目录配额的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:batchUpdateFsDirQuotas	授予批量更新弹性文件系统目录配额的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showFsDirUsage	授予查询弹性文件系统目录资源使用情况的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createFsAsyncTask	授予创建弹性文件系统异步任务的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showFsAsyncTask	授予查询弹性文件系统异步任务详情的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

操作项	描述	访问级别	资源类型（*为必须）	条件键
sfsturbo:shares:listFsAsyncTasks	授予查询弹性文件系统异步任务列表的权限。	list	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deleteFsAsyncTask	授予删除弹性文件系统异步任务的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createBackendTarget	授予创建弹性文件系统后端存储库的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showBackendTargetInfo	授予查询弹性文件系统后端存储库详情的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:listBackendTargets	授予查询弹性文件系统后端存储库列表的权限。	list	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deleteBackendTarget	授予删除弹性文件系统后端存储库的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateObsTargetPolicy	授予修改弹性文件系统与OBS 后端存储库之间自动数据流转策略的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateObsTargetAttributes	授予修改弹性文件系统后端存储库属性的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:listPermRules	授予查询弹性文件系统权限规则列表的权限。	list	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

操作项	描述	访问级别	资源类型（*为必须）	条件键
sfsturbo:shares:showPermRule	授予查询弹性文件系统权限规则详情的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createPermRule	授予创建弹性文件系统权限规则的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updatePermRule	授予修改文件系统权限规则的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deletePermRule	授予删除弹性文件系统权限规则的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showLdap	授予查询弹性文件系统LDAP配置的权限。	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createLdap	授予创建弹性文件系统LDAP配置的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateLdap	授予修改文件系统LDAP配置的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deleteLdap	授予删除弹性文件系统LDAP配置的权限。	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:getJob	授予查询弹性文件系统任务详情的权限。	read	-	-

SFS Turbo的API通常对应着一个或多个授权项。**表5-36**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-36 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}/sfs-turbo/shares	sfsturbo:shares:createShare	• billing:order:pay • billing:contract:viewDiscount • vpc:vpcs:get • vpc:subnets:get • vpc:securityGroups:get • vpc:securityGroups:create • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:securityGroupRules:get • vpc:securityGroupRules:create • vpc:quotas:list • cbr:backups:get • cbr:vaults:addResources • evs:types:get • kms:cmk:listGrants • kms:cmk:createGrant • kms:cmk:get • sfsturbo:shares:getAZInfo • sfsturbo:shares:getQuota • sfsturbo:shares:getFlavors • sfsturbo:shares:checkShareName • eps:enterpriseProjects:list
GET /v1/{project_id}/sfs-turbo/shares/detail	sfsturbo:shares:getAllShares	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}	sfsturbo:shares:getShare	-

API	对应的授权项	依赖的授权项
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}	sfsturbo:shares:deleteShare	• vpc:ports:get • vpc:ports:delete • vpc:securityGroupRules:delete • vpc:securityGroups:delete
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/action	sfsturbo:shares:extendShare	• billing:order:pay • vpc:vpcs:get • vpc:subnets:get • vpc:ports:get • vpc:ports:create • vpc:ports:update
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/action	sfsturbo:shares:updateShareSecurityGroup	• vpc:ports:update • vpc:securityGroups:get • vpc:securityGroupRules:create • vpc:securityGroupRules:delete
POST /v1/{project_id}/sfs-turbo/{share_id}/tags	sfsturbo:shares:addTag	-
GET /v1/{project_id}/sfs-turbo/{share_id}/tags	sfsturbo:shares:getTag	-
DELETE /v1/{project_id}/sfs-turbo/{share_id}/tags/{key}	sfsturbo:shares:deleteTag	-
POST /v1/{project_id}/sfs-turbo/{share_id}/tags/action	sfsturbo:shares:batchResTag	-
GET /v1/{project_id}/sfs-turbo/tags	sfsturbo:shares:getAllTag	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/action	sfsturbo:shares:renameShare	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/{feature}/tasks	sfsturbo:shares:createFsAsyncTask	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/{feature}/tasks	sfsturbo:shares:listFsAsyncTasks	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/{feature}/tasks/{task_id}	sfsturbo:shares:showFsAsyncTask	-
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/{feature}/tasks/{task_id}	sfsturbo:shares:deleteFsAsyncTask	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/targets	sfsturbo:shares:createBackendTarget	• obs:bucket:putBucketPolicy • vpc:ports:get • vpc:ports:create • vpc:subnets:get
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/targets	sfsturbo:shares:listBackendTargets	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/targets/{target_id}	sfsturbo:shares:showBackendTargetInfo	-
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/targets/{target_id}	sfsturbo:shares:deleteBackendTarget	-
POST /v1/{project_id}/sfs-turbo/{share_id}/hpc-cache/task	sfsturbo:shares:createDataRepositoryTask	obs:bucket:headBucket
GET /v1/{project_id}/sfs-turbo/{share_id}/hpc-cache/task/{task_id}	sfsturbo:shares:getDataRepositoryTask	-
GET /v1/{project_id}/sfs-turbo/{share_id}/hpc-cache/tasks	sfsturbo:shares:getAllDataRepositoryTasks	-
PUT /v1/{project_id}/sfs-turbo/shares/{share_id}	sfsturbo:shares:updateHpcShare	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-quota	sfsturbo:shares:createFsDirQuota	-

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-quota	sfsturbo:shares:updateFsDirQuota	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-quota	sfsturbo:shares:showFsDirQuota	-
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-quota	sfsturbo:shares:deleteFsDirQuota	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir	sfsturbo:shares:createFsDir	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir	sfsturbo:shares:showFsDir	-
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir	sfsturbo:shares:deleteFsDir	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-usage	sfsturbo:shares:showFsDirUsage	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules	sfsturbo:shares:createPermRule	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules	sfsturbo:shares:listPermRules	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules/{rule_id}	sfsturbo:shares:showPermRule	-
PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules/{rule_id}	sfsturbo:shares:updatePermRule	-
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules/{rule_id}	sfsturbo:shares:deletePermRule	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/ldap	sfsturbo:shares:createLdap	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/ldap	sfsturbo:shares:showLdap	-
PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/ldap	sfsturbo:shares:updateLdap	-
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/ldap	sfsturbo:shares:deleteLdap	-
GET /v1/{project_id}/sfs-turbo/jobs/{job_id}	sfsturbo:shares:getJob	-
DELETE /v1/{project_id}/sfs-turbo/{share_id}/hpc-cache/task/{task_id}	sfsturbo:shares:deleteDataRepositoryTask	-
PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/targets/{target_id}/policy	sfsturbo:shares:updateObsTargetPolicy	-
PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/targets/{target_id}/attributes	sfsturbo:shares:updateObsTargetAttributes	-

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。

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

表 5-37 sfsturbo 支持的资源类型

资源类型	URN	条件键
shares	shares *	• 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，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sfsturbo:）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。

SFS Turbo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 5-38 sfsturbo 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
sfsturbo:CryptKeyId	string	单值	根据请求参数中指定的密钥 ID 过滤访问

5.10.3 网络

5.10.3.1 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 5-39 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
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			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
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
			-	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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
			-	• 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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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5-40展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-40 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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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:createTags	-
POST /v2.0/{project_id}/subnets/{subnet_id}/tags/action	vpc:subnets:deleteTags	-
POST /v2.0/{project_id}/subnets/{subnet_id}/tags	vpc:subnets:createTags	-
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	-
POST /v3/{project_id}/vpc/sub-network-interfaces	vpc:subNetworkInterfaces:create	-
POST /v3/{project_id}/vpc/sub-network-interfaces/batch-create	vpc:subNetworkInterfaces:create	-
GET /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}	vpc:subNetworkInterfaces:get	-
GET /v3/{project_id}/vpc/sub-network-interfaces	vpc:subNetworkInterfaces:list	-
GET /v3/{project_id}/vpc/sub-network-interfaces/count	vpc:subNetworkInterfaces:list	-
PUT /v3/{project_id}/vpc/sub-network-interfaces/migrate	vpc:subNetworkInterfaces:update	-
PUT /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}	vpc:subNetworkInterfaces:update	-
DELETE /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}	vpc:subNetworkInterfaces:delete	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-41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 5-41 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>
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5-42。
  - 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 5-42 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。
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。

服务级条件键	类型	单值/多值	说明
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: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。

5.10.3.2 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 5-43 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 *	-
			-	• 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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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>
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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			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
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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的API通常对应着一个或多个授权项。表5-44展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-44 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v2.0/{project_id}/publicips	eip:publicIps:create	-
POST /v1/{project_id}/publicips	eip:publicIps:create	-
POST /v2/{project_id}/batchpublicips	eip:publicIps:batchCreate	-
GET /v1/{project_id}/publicips	eip:publicIps:list	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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
GET /v3/{project_id}/eip/publicip-pools/{publicip_pool_id}	eip:publicipPools:get	-
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5-45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 5-45 EIP 支持的资源类型

资源类型	URN
bandwidthPkg	eip:<region>:<account-id>:bandwidthPkg:<bandwidthPkg-id>
publicipPool	eip:<region>:<account-id>:publicipPool:<publicipPool-id>
publicip	eip:<region>:<account-id>:publicip:<publicip-id>
bandwidth	eip:<region>:<account-id>:bandwidth:<bandwidth-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。

5.10.3.3 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 5-46 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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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>
			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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			private DnatRule *	g:EnterpriseProjectId
nat:privateNatDnatRules:update	授予权限以更新指定的私网NAT网关DNAT规则。	write	private Gateway *	g:ResourceTag/<tag-key>
			private DnatRule *	-
			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	private Gateway *	g:ResourceTag/<tag-key>
			privateSnatRule *	-
			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	private Gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			privateSnatRule *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-
			-	• 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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
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>
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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5-47展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-47 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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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5-48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 5-48 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>
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。

5.10.3.4 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 5-49 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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • elb:AssociatePublicips
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:AssociatePublicips

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
			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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
elb:security-policies:show	授予获取安全策略详情的权限。	read	security Policy *	-
elb:security-policies:create	授予创建安全策略的权限。	write	security Policy *	-
			-	g:EnterpriseProjectId
elb:security-policies:update	授予修改安全策略的权限。	write	security Policy *	-
elb:security-policies:delete	授予删除安全策略的权限。	write	security Policy *	-

ELB的API通常对应着一个或多个授权项。表5-50展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-50 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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

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

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
GET /v3/{project_id}/elb/l7policies	elb:l7policies:list	-
GET /v3/{project_id}/elb/l7policies/{l7policy_id}	elb:l7policies:show	-

API	对应的授权项	依赖的授权项
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5-51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 5-51 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）

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elb:）仅适用于对应服务的操作，详情请参见表5-52。
  - 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：条件键。

ELB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 5-52 ELB 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
elb:AssociatePublicips	boolean	单值	根据创建或修改负载均衡器时是否涉及创建或绑定公网操作筛选访问权限。若要完全限制弹性负载均衡器的公网访问，则需要同时使用弹性公网IP的相关Action进行策略管理。

5.10.3.5 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 5-53 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	-
			-	• 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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			routeTable	-
			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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
vpcep:endpointServices:describe	授予权限查询终端节点服务概要。	read	-	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
vpcep::listResourceTags	授予权限根据标签查询资源实例。	list	endpoints	-
			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::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5-54展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-54 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	-
DELETE /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}	vpcep:endpoints:delete	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
POST /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions/batch-delete	vpcep:endpointServices:deletePermissions	-

API	对应的授权项	依赖的授权项
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	-
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5-55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。

VPCEP定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-55 VPCEP 支持的资源类型

资源类型	URN
routeTable	vpc:<region>:<account-id>:routeTable:<route-table-id>
vpc	vpc:<region>:<account-id>:vpc:<vpc-id>
endpointServices	vpcep:<region>:<account-id>:endpointServices:<endpoint-service-id>
subnet	vpc:<region>:<account-id>:subnet:<subnet-id>
endpoints	vpcep:<region>:<account-id>:endpoints:<endpoint-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5-56。
  - 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。

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 5-56 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。

服务级条件键	类型	单值/多值	说明
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。

5.10.3.6 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 5-57 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 *	-
			-	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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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	-

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
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	-
			lgw	-
			-	• g:EnterpriseProjectId • 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
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 *	-
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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>
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:vif:switchoverTest	授予权限以进行倒换测试。	write	vif *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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>
			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	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			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>
			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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			vgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			vif	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			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	-	-

DC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 /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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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5-59**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。

DC定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-59 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>
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。

5.10.3.7 企业路由器 ER

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er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er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er的相关操作。

表 5-60 er 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	别名
er:instances:get	授予查询实例详情权限。	read	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:instances:create	授予创建实例权限。	write	instances *	g:EnterpriseProjectId	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
er:instances:list	授予查询实例列表权限。	list	instances *	-	-
er:instances:update	授予更新实例权限。	write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:instances:delete	授予删除实例权限。	write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:instances:createVpcAttachment	授予创建VPC连接权限。	write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:create
er:instances:showVpcAttachment	授予查询VPC连接详情权限。	read	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:get
er:instances:listVpcAttachments	授予查询VPC连接列表权限。	list	instances *	-	er:attachments:list

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
er:instances:updateVpcAttachment	授予更新VPC连接权限。	write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:update
er:instances:deleteVpcAttachment	授予删除VPC连接权限。	write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:delete
er:commonAttachments:get	授予查询连接详情权限。	read	attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:get
er:commonAttachments:list	授予查询连接列表权限。	list	attachments *	-	er:attachments:list
er:commonAttachments:update	授予更新连接权限。	write	attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:update
er:routeTables:get	授予查询路由表详情权限。	read	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:routeTables:create	授予创建路由表权限。	write	routeTables *	-	-
			instances *	• 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	别名
			-	• g:RequestTag/<tag-key> • g:TagKeys	
er:routeTables:list	授予查询路由表列表权限。	list	routeTables *	-	-
er:routeTables:update	授予更新路由表权限。	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:routeTables:delete	授予删除路由表权限。	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:routeTables:associate	授予将连接和路由表关联的权限。	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:associations:associate
			attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:routeTables:disassociate	授予解除连接和路由表关联的权限。	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:associations:disassociate
			attachments *	• 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	别名
er:routeTables:listAssociations	授予查询关联列表的权限。	list	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:associations:list
er:routeTables:enablePropagation	授予允许连接将路由传播到传播路由表的权限。	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:propagations:enable
			attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:routeTables:disablePropagation	授予禁止连接将路由传播到指定传播路由表的权限。	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:propagations:disable
			attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:routeTables:listPropagations	授予查询传播列表的权限。	list	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:propagations:list
er:staticRoutes:list	授予查询静态路由列表的权限。	list	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:list

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
er:staticRoutes:create	授予创建静态路由的权限。	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:create
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:effectiveRoutes:list	授予查询有效路由列表的权限。	list	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:list
er:staticRoutes:delete	授予删除静态路由的权限。	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:delete
er:staticRoutes:update	授予更新静态路由的权限。	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:update
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:staticRoutes:get	授予查询静态路由的权限。	read	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:get

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
er:tags:singleCreate	授予创建资源标签的权限。	write	routeTables	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:tags:create
			instances	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:tags:delete	授予删除资源标签的权限。	write	routeTables	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			instances	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:tags:batchOperation	授予批量创建资源标签的权限。	write	routeTables	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:tags:create

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			instances	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:tags:get	授予查询特定资源的标签的权限。	read	routeTables	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			instances	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:tags:list	授予查询资源标签列表的权限。	list	-	-	-
er:quotas:list	授予查询资源配额的权限。	list	-	-	-
er:flowLogs:create	授予创建流日志的权限。	write	instances *	• 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	别名
			attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			flowLogs *	-	
er:flowLogs:list	授予查询流日志列表的权限。	list	flowLogs *	-	-
er:flowLogs:get	授予查询流日志的权限。	read	flowLogs *	-	-
er:flowLogs:update	授予更新流日志的权限。	write	flowLogs *	-	-
er:flowLogs:delete	授予删除流日志的权限。	write	flowLogs *	-	-
er:flowLogs:enable	授予开启流日志的权限。	write	flowLogs *	-	-
er:flowLogs:disable	授予关闭流日志的权限。	write	flowLogs *	-	-

er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
POST /v3/{project_id}/enterprise-router/instances	er:instances:create	-
PUT /v3/{project_id}/enterprise-router/instances/{er_id}	er:instances:update	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/enterprise-router/instances/{er_id}	er:instances:get	-
GET /v3/{project_id}/enterprise-router/instances	er:instances:list	-
DELETE /v3/{project_id}/enterprise-router/instances/{er_id}	er:instances:delete	-
POST /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments	er:instances:createVpcAttachment	-
PUT /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments/{vpc_attachment_id}	er:instances:updateVpcAttachment	-
GET /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments/{vpc_attachment_id}	er:instances:showVpcAttachment	-
GET /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments	er:instances:listVpcAttachments	-
DELETE /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments/{vpc_attachment_id}	er:instances:deleteVpcAttachment	-

API	对应的授权项	依赖的授权项
PUT /v3/{project_id}/enterprise-router/{er_id}/attachments/{attachment_id}	er:commonAttachments:update	-
GET /v3/{project_id}/enterprise-router/{er_id}/attachments/{attachment_id}	er:commonAttachments:get	-
GET /v3/{project_id}/enterprise-router/{er_id}/attachments	er:commonAttachments:list	-
POST /v3/{project_id}/enterprise-router/{er_id}/route-tables	er:routeTables:create	-
PUT /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}	er:routeTables:update	-
GET /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}	er:routeTables:get	-
GET /v3/{project_id}/enterprise-router/{er_id}/route-tables	er:routeTables:list	-
DELETE /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}	er:routeTables:delete	-
POST /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/associate	er:routeTables:associate	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/associations	er:routeTables:listAssociations	-
POST /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/disassociate	er:routeTables:disassociate	-
POST /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/enable-propagations	er:routeTables:enablePropagation	-
GET /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/propagations	er:routeTables:listPropagations	-
POST /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/disable-propagations	er:routeTables:disablePropagation	-
POST /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/static-routes	er:staticRoutes:create	-
PUT /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/static-routes/{route_id}	er:staticRoutes:update	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/static-routes/{route_id}	er:staticRoutes:get	-
GET /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/static-routes	er:staticRoutes:list	-
GET /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/routes	er:effectiveRoutes:list	-
DELETE /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/static-routes/{route_id}	er:staticRoutes:delete	-
GET /v3/{project_id}/{resource_type}/tags	er:tags:list	-
GET /v3/{project_id}/{resource_type}/{resource_id}/tags	er:tags:get	-
POST /v3/{project_id}/{resource_type}/{resource_id}/tags	er:tags:singleCreate	-
POST /v3/{project_id}/{resource_type}/{resource_id}/tags/action	er:tags:batchOperation	-

API	对应的授权项	依赖的授权项
DELETE /v3/{project_id}/{resource_type}/{resource_id}/tags/{key}	er:tags:delete	-
GET /v3/{project_id}/enterprise-router/quotas	er:quotas:list	-
POST /v3/{project_id}/enterprise-router/{er_id}/flow-logs	er:flowLogs:create	-
GET /v3/{project_id}/enterprise-router/{er_id}/flow-logs	er:flowLogs:list	-
GET /v3/{project_id}/enterprise-router/{er_id}/flow-logs/{flow_log_id}	er:flowLogs:get	-
PUT /v3/{project_id}/enterprise-router/{er_id}/flow-logs/{flow_log_id}	er:flowLogs:update	-
DELETE /v3/{project_id}/enterprise-router/{er_id}/flow-logs/{flow_log_id}	er:flowLogs:delete	-
POST /v3/{project_id}/enterprise-router/{er_id}/flow-logs/{flow_log_id}/enable	er:flowLogs:enable	-
POST /v3/{project_id}/enterprise-router/{er_id}/flow-logs/{flow_log_id}/disable	er:flowLogs:disable	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-62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。

er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 5-62 er 支持的资源类型

资源类型	URN
instances	er:<region>:<account-id>:instances:<instance-id>
routeTables	er:<region>:<account-id>:routeTables:<route-table-id>
flowLogs	er:<region>:<account-id>:flowFlogs:<flow-log-id>
attachments	er:<region>:<account-id>:attachments:<attachment-id>

条件（Condition）

er服务不支持在SCP中的条件键中配置服务级的条件键。

er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。

5.10.3.8 全球加速服务 GA

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GA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GA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GA的相关操作。

表 5-63 GA 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
ga:accelerator:list	授予查询加速器列表权限。	list	accelerator *	-
ga:accelerator:create	授予创建加速器权限。	write	accelerator *	g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
ga:accelerator:get	授予查询加速器详情权限。	read	accelerator *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ga:accelerator:update	授予更新加速器权限。	write	accelerator *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ga:accelerator:delete	授予删除加速器权限。	write	accelerator *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ga:listener:list	授予查询监听器列表权限。	list	listener *	-
ga:listener:create	授予创建监听器权限。	write	listener *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
ga:listener:get	授予查询监听器详情权限。	read	listener *	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
ga:listener:update	授予更新监听器权限。	write	listener *	g:ResourceTag/<tag-key>
ga:listener:delete	授予删除监听器权限。	write	listener *	g:ResourceTag/<tag-key>
ga:endpointgroup:list	授予查询终端节点组列表权限。	list	endpointgroup *	-
ga:endpointgroup:create	授予创建终端节点组权限。	write	endpointgroup *	-
			-	ga:RequestRegionId
ga:endpointgroup:get	授予查询终端节点组详情权限。	read	endpointgroup *	ga:RegionId
ga:endpointgroup:update	授予更新终端节点组权限。	write	endpointgroup *	ga:RegionId
ga:endpointgroup:delete	授予删除终端节点组权限。	write	endpointgroup *	ga:RegionId
ga:endpoint:list	授予查询终端节点列表权限。	list	endpoint *	-
ga:endpoint:create	授予创建终端节点权限。	write	endpoint *	-
			-	• ga:RequestResourceType • ga:RequestResourceId • ga:RequestIpAddress • ga:RequestDomainName
ga:endpoint:get	授予查询终端节点详情权限。	read	endpoint *	• ga:ResourceType • ga:ResourceId • ga:IpAddress • ga:DomainName

授权项	描述	访问级别	资源类型（*为必须）	条件键
ga:endpoint:update	授予更新终端节点权限。	write	endpoint *	• ga:ResourceType • ga:ResourceId • ga:IpAddress • ga:DomainName
ga:endpoint:delete	授予删除终端节点权限。	write	endpoint *	• ga:ResourceType • ga:ResourceId • ga:IpAddress • ga:DomainName
ga:healthcheck:list	授予查询健康检查列表权限。	list	healthcheck *	-
ga:healthcheck:create	授予创建健康检查权限。	write	healthcheck *	-
ga:healthcheck:get	授予查询健康检查详情权限。	read	healthcheck *	-
ga:healthcheck:update	授予更新健康检查权限。	write	healthcheck *	-
ga:healthcheck:delete	授予删除健康检查权限。	write	healthcheck *	-
ga:tag:create	授予批量创建资源的标签权限。	tagging	accelerator	g:ResourceTag/<tag-key>
			listener	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
ga:tag:delete	授予批量删除资源的标签权限。	tagging	accelerator *	g:ResourceTag/<tag-key>
			listener *	g:ResourceTag/<tag-key>
			-	g:TagKeys
ga:tag:get	授予查询资源的标签权限。	read	accelerator	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			listener	g:ResourceTag/<tag-key>
ga:tag:list	授予查询标签列表的权限。	list	-	-
ga::listResourcesByTag	授予通过标签查询资源实例列表的权限。	list	-	g:TagKeys
ga:ipgroup:list	授予查询IP地址组列表权限。	list	ipgroup *	-
ga:ipgroup:create	授予创建IP地址组权限。	write	ipgroup *	-
ga:ipgroup:get	授予查询IP地址组详情权限。	read	ipgroup *	-
ga:ipgroup:update	授予更新IP地址组权限。	write	ipgroup *	-
ga:ipgroup:delete	授予删除IP地址组权限。	write	ipgroup *	-
ga:ipgroup:addIps	授予为IP地址组批量添加IP权限。	write	ipgroup *	-
ga:ipgroup:removeIps	授予为IP地址组批量删除IP权限。	write	ipgroup *	-
ga:ipgroup:associateListener	授予为IP地址组绑定监听器权限。	write	ipgroup *	-
ga:ipgroup:disassociateListener	授予为IP地址组解绑监听器权限。	write	ipgroup *	-
ga::listByoipPools	授予查询自带IP（BYOIP）地址池列表权限。	list	-	-
ga:logtank:list	授予查询云日志列表的权限。	list	logtank *	-
ga:logtank:create	授予创建云日志的权限。	write	logtank *	-
ga:logtank:get	授予获取云日志详情的权限。	read	logtank *	-
ga:logtank:update	授予修改云日志的权限。	write	logtank *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
ga:logtank:delete	授予删除云日志的权限。	write	logtank *	-

GA的API通常对应着一个或多个授权项。表5-64展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-64 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v1/accelerators	ga:accelerator:list	-
POST /v1/accelerators	ga:accelerator:create	-
GET /v1/accelerators/{accelerator_id}	ga:accelerator:get	-
PUT /v1/accelerators/{accelerator_id}	ga:accelerator:update	-
DELETE /v1/accelerators/{accelerator_id}	ga:accelerator:delete	-
GET /v1/listeners	ga:listener:list	-
POST /v1/listeners	ga:listener:create	-
GET /v1/listeners/{listener_id}	ga:listener:get	-
PUT /v1/listeners/{listener_id}	ga:listener:update	-
DELETE /v1/listeners/{listener_id}	ga:listener:delete	-
GET /v1/endpoint-groups	ga:endpointgroup:list	-
POST /v1/endpoint-groups	ga:endpointgroup:create	-

API	对应的授权项	依赖的授权项
GET /v1/endpoint-groups/{endpoint_group_id}	ga:endpointgroup:get	-
PUT /v1/endpoint-groups/{endpoint_group_id}	ga:endpointgroup:update	-
DELETE /v1/endpoint-groups/{endpoint_group_id}	ga:endpointgroup:delete	-
GET /v1/endpoint-groups/{endpoint_group_id}/endpoints	ga:endpoint:list	-
POST /v1/endpoint-groups/{endpoint_group_id}/endpoints	ga:endpoint:create	-
GET /v1/endpoint-groups/{endpoint_group_id}/endpoints/{endpoint_id}	ga:endpoint:get	-
PUT /v1/endpoint-groups/{endpoint_group_id}/endpoints/{endpoint_id}	ga:endpoint:update	-
DELETE /v1/endpoint-groups/{endpoint_group_id}/endpoints/{endpoint_id}	ga:endpoint:delete	-
GET /v1/health-checks	ga:healthcheck:list	-
POST /v1/health-checks	ga:healthcheck:create	-
GET /v1/health-checks/{health_check_id}	ga:healthcheck:get	-
PUT /v1/health-checks/{health_check_id}	ga:healthcheck:update	-

API	对应的授权项	依赖的授权项
DELETE /v1/health-checks/{health_check_id}	ga:healthcheck:delete	-
POST /v1/{resource_type}/{resource_id}/tags/create	ga:tag:create	-
DELETE /v1/{resource_type}/{resource_id}/tags/delete	ga:tag:delete	-
GET /v1/{resource_type}/{resource_id}/tags	ga:tag:get	-
POST /v1/{resource_type}/resource-instances/filter	ga::listResourcesByTag	-
POST /v1/{resource_type}/resource-instances/count	ga::listResourcesByTag	-
GET /v1/{resource_type}/tags	ga:tag:list	-
GET /v1/ip-groups	ga:ipgroup:list	-
POST /v1/ip-groups	ga:ipgroup:create	-
GET /v1/ip-groups/{ip_group_id}	ga:ipgroup:get	-
PUT /v1/ip-groups/{ip_group_id}	ga:ipgroup:update	-
DELETE /v1/ip-groups/{ip_group_id}	ga:ipgroup:delete	-
POST /v1/ip-groups/{ip_group_id}/add-ips	ga:ipgroup:addIps	-
POST /v1/ip-groups/{ip_group_id}/remove-ips	ga:ipgroup:removeIps	-

API	对应的授权项	依赖的授权项
POST /v1/ip-groups/{ip_group_id}/associate-listener	ga:ipgroup:associateListener	-
POST /v1/ip-groups/{ip_group_id}/disassociate-listener	ga:ipgroup:disassociateListener	-
GET /v1/byoip-pools	ga::listByoipPools	-
GET /v1/logtanks	ga:logtank:list	-
POST /v1/logtanks	ga:logtank:create	-
GET /v1/logtanks/{logtank_id}	ga:logtank:get	-
PUT /v1/logtanks/{logtank_id}	ga:logtank:update	-
DELETE /v1/logtanks/{logtank_id}	ga:logtank:delete	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-65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。

GA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 5-65 GA 支持的资源类型

资源类型	URN
ipgroup	ga::<account-id>:ipgroup:<ipgroup-id>
endpoint	ga::<account-id>:endpoint:<endpoint-id>
accelerator	ga::<account-id>:accelerator:<accelerator-id>
logtank	ga::<account-id>:logtank:<logtank-id>
listener	ga::<account-id>:listener:<listener-id>
healthcheck	ga::<account-id>:healthcheck:<healthcheck-id>
endpointgroup	ga::<account-id>:endpointgroup:<endpointgroup-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ga:）仅适用于对应服务的操作，详情请参见表5-66。
  - 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。

GA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 5-66 GA 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
ga:RequestRegionId	string	单值	按照在请求中传递的地域ID筛选访问权限。
ga:RequestResourceType	string	单值	按照在请求中传递的资源类型筛选访问权限。
ga:RequestResourceId	string	单值	按照在请求中传递的资源ID筛选访问权限。
ga:RequestIpAddress	string	单值	按照在请求中传递的IP地址筛选访问权限。
ga:RequestDomainName	string	单值	按照在请求中传递的域名筛选访问权限。
ga:RegionId	string	单值	按照终端节点组的地域筛选访问权限。
ga:ResourceType	string	单值	按照终端节点的资源类型筛选访问权限。
ga:ResourceId	string	单值	按照终端节点的资源ID筛选访问权限。
ga:IpAddress	string	单值	按照终端节点的IP地址筛选访问权限。
ga:DomainName	string	单值	按照终端节点的域名筛选访问权限。

5.10.3.9 云连接 CC

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CC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CC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CC的相关操作。

表 5-67 CC 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
cc:cloudConnections:create	授予创建云连接权限。	write	cloudConnection *	-
			-	• g:EnterpriseProjectId • 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
cc:cloudConnections:delete	授予删除云连接权限。	write	cloudConnection *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:cloudConnections:update	授予更新云连接权限。	write	cloudConnection *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:cloudConnections:get	授予查询云连接详情权限。	read	cloudConnection *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:cloudConnections:list	授予查询云连接列表权限。	list	cloudConnection *	-
cc:cloudConnections:tag	授予为云连接实例打标签权限。	tagging	cloudConnection *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cc:cloudConnections:unTag	授予为云连接实例删除标签权限。	tagging	cloudConnection *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cc:cloudConnections:listTags	授予查询为云连接资源的标签列表权限。	list	cloudConnection *	-
cc:networkInstances:create	授予创建网络实例权限。	write	networkInstance *	-
			cloudConnection *	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 • cc:VpcId • cc:VirtualGatewayId • cc:EnterpriseRouterId
cc:networkInstances:delete	授予删除网络实例权限。	write	networkInstance *	• cc:VpcId • cc:VirtualGatewayId • cc:EnterpriseRouterId
			cloudConnection *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:networkInstances:update	授予更新网络实例权限。	write	networkInstance *	• cc:VpcId • cc:VirtualGatewayId • cc:EnterpriseRouterId
			cloudConnection *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:networkInstances:get	授予查询网络实例详情权限。	read	networkInstance *	-
			cloudConnection *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:networkInstances:list	授予查询网络实例列表权限。	list	networkInstance *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
cc:bandwidthPackages:create	授予创建带宽包权限。	write	bandwidthPackage *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
cc:bandwidthPackages:delete	授予删除带宽包权限。	write	bandwidthPackage *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:bandwidthPackages:update	授予更新带宽包权限。	write	bandwidthPackage *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:bandwidthPackages:get	授予查询带宽包详情权限。	read	bandwidthPackage *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:bandwidthPackages:list	授予查询带宽包列表权限。	list	bandwidthPackage *	-
cc:bandwidthPackages:tag	授予为带宽包打标签权限。	tagging	bandwidthPackage *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cc:bandwidthPackages:unTag	授予为带宽包删除标签权限。	tagging	bandwidthPackage *	• g:EnterpriseProjectId • 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
cc:bandwidthPackages:listTags	授予查询带宽包资源的标签列表权限。	list	bandwidthPackage *	-
cc:bandwidthPackages:associate	授予关联带宽包权限。	write	bandwidthPackage *	g:ResourceTag/<tag-key>
			cloudConnection *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:bandwidthPackages:disassociate	授予解关联带宽包权限。	write	bandwidthPackage *	g:ResourceTag/<tag-key>
			cloudConnection *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:interRegionBandwidths:create	授予创建域间带宽权限。	write	interRegionBandwidth *	-
			cloudConnection *	g:ResourceTag/<tag-key>
			-	• g:EnterpriseProjectId • cc:BandwidthPackageId
cc:interRegionBandwidths:delete	授予删除域间带宽权限。	write	interRegionBandwidth *	cc:BandwidthPackageId
			cloudConnection *	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
cc:interRegionBandwidths:update	授予更新域间带宽权限。	write	interRegionBandwidth *	cc:BandwidthPackageId
			cloudConnection *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:interRegionBandwidths:get	授予查询域间带宽详情权限。	read	interRegionBandwidth *	-
			cloudConnection *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:interRegionBandwidths:list	授予查询域间带宽列表权限。	list	interRegionBandwidth *	-
cc:cloudConnectionRoutes:get	授予查询云连接路由详情权限。	read	-	-
cc:cloudConnectionRoutes:list	授予查询云连接路由列表权限。	list	-	-
cc:authorisation:create	授予创建虚拟私有云授权的权限。	write	-	-
cc:authorisation:delete	授予删除虚拟私有云授权的权限。	write	-	-
cc:authorisation:update	授予更新虚拟私有云授权基本信息的权限。	write	-	-
cc:authorisation:list	授予查询虚拟私有云授权列表权限。	list	-	-
cc:authorisation:listPermissions	授予查询被授权的虚拟私有云列表权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
cc:centralNetwork:create	授予创建中心网络权限。	write	centralNetwork *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys • cc:MultipleEnterpriseRouterIds
cc:centralNetwork:delete	授予删除中心网络权限。	write	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:centralNetwork:update	授予更新中心网络权限。	write	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cc:centralNetwork:get	授予查询中心网络详情权限。	read	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:centralNetwork:list	授予查询中心网络列表权限。	list	centralNetwork *	-
cc:centralNetwork:tag	授予为中心网络添加标签权限。	tagging	centralNetwork *	• g:EnterpriseProjectId • 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
cc:centralNetwork:unTag	授予删除中心网络标签权限。	tagging	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cc:centralNetwork:listTags	授予查询中心网络标签权限。	list	centralNetwork *	-
cc:centralNetwork:createPolicy	授予创建中心网络策略权限。	write	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	cc:MultipleEnterpriseRouterIds
cc:centralNetwork:applyPolicy	授予应用中心网络策略权限。	write	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:centralNetwork:deletePolicy	授予删除中心网络策略权限。	write	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:centralNetwork:listPolicies	授予查询中心网络策略列表权限。	list	centralNetwork *	-
cc:centralNetwork:listChangeSet	授予查询当前策略与被应用策略变化集权限。	list	centralNetwork *	-
cc:centralNetwork:listConnections	授予查询中心网络连接列表权限。	list	centralNetwork *	-
cc:centralNetwork:updateConnection	授予更新中心网络连接权限。	write	centralNetwork *	• 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
			-	cc:GlobalConnectionBandwidthId
cc:centralNetworkAttachment:createGdgw	授予创建中心网络GDGW附件权限。	write	centralNetworkAttachment *	-
			centralNetwork *	g:ResourceTag/<tag-key>
			-	• g:EnterpriseProjectId • cc:EnterpriseRouterId • cc:GlobalDcGatewayId
cc:centralNetworkAttachment:updateGdgw	授予更新中心网络GDGW附件权限。	write	centralNetworkAttachment *	• cc:GlobalDcGatewayId • cc:EnterpriseRouterId
			centralNetwork *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:centralNetworkAttachment:getGdgw	授予查询中心网络GDGW附件详情权限。	read	centralNetworkAttachment *	• cc:GlobalDcGatewayId • cc:EnterpriseRouterId
			centralNetwork *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:centralNetworkAttachment:listGdgws	授予查询中心网络GDGW附件列表权限。	list	centralNetworkAttachment *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			centralNetwork *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:centralNetworkAttachment:createErRouteTable	授予创建中心网络er-route-table附件权限。	write	centralNetworkAttachment *	-
			centralNetwork *	g:ResourceTag/<tag-key>
			-	• g:EnterpriseProjectId • cc:MultipleEnterpriseRouterIds
cc:centralNetworkAttachment:updateErRouteTable	授予更新中心网络er-route-table附件权限。	write	centralNetworkAttachment *	cc:MultipleEnterpriseRouterIds
			centralNetwork *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:centralNetworkAttachment:getErRouteTable	授予查询中心网络er-route-table附件详情权限。	read	centralNetworkAttachment *	cc:MultipleEnterpriseRouterIds
			centralNetwork *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:centralNetworkAttachment:listErRouteTables	授予查询中心网络er-route-table附件列表权限。	list	centralNetworkAttachment *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			centralNetwork *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:centralNetworkAttachment:delete	授予删除中心网络附件权限。	write	centralNetworkAttachment *	• cc:GlobalDcGatewayId • cc:EnterpriseRouterId • cc:MultipleEnterpriseRouterIds
			centralNetwork *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:centralNetworkAttachment:list	授予查询中心网络附件列表权限。	list	centralNetworkAttachment *	-
			centralNetwork *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId

CC的API通常对应着一个或多个授权项。表5-68展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-68 API 与授权项的关系

API	对应的授权项	依赖的授权项
POST /v3/{domain_id}/ccaas/cloud-connections	cc:cloudConnections:create	-
PUT /v3/{domain_id}/ccaas/cloud-connections/{id}	cc:cloudConnections:update	-

API	对应的授权项	依赖的授权项
DELETE /v3/{domain_id}/ccaas/cloud-connections/{id}	cc:cloudConnections:delete	-
GET /v3/{domain_id}/ccaas/cloud-connections/{id}	cc:cloudConnections:get	-
GET /v3/{domain_id}/ccaas/cloud-connections	cc:cloudConnections:list	-
POST /v3/{domain_id}/ccaas/cloud-connections/filter	cc:cloudConnections:list	-
POST /v3/{domain_id}/ccaas/cloud-connections/{id}/tag	cc:cloudConnections:tag	-
POST /v3/{domain_id}/ccaas/cloud-connections/{id}/untag	cc:cloudConnections:unTag	-
GET /v3/{domain_id}/ccaas/cloud-connections/tags	cc:cloudConnections:listTags	-
POST /v3/{domain_id}/ccaas/network-instances	cc:networkInstances:create	-
PUT /v3/{domain_id}/ccaas/network-instances/{id}	cc:networkInstances:update	-
DELETE /v3/{domain_id}/ccaas/network-instances/{id}	cc:networkInstances:delete	-
GET /v3/{domain_id}/ccaas/network-instances/{id}	cc:networkInstances:get	-

API	对应的授权项	依赖的授权项
GET /v3/{domain_id}/ccaas/network-instances	cc:networkInstances:list	-
POST /v3/{domain_id}/ccaas/bandwidth-packages	cc:bandwidthPackages:create	-
PUT /v3/{domain_id}/ccaas/bandwidth-packages/{id}	cc:bandwidthPackages:update	-
DELETE /v3/{domain_id}/ccaas/bandwidth-packages/{id}	cc:bandwidthPackages:delete	-
GET /v3/{domain_id}/ccaas/bandwidth-packages/{id}	cc:bandwidthPackages:get	-
GET /v3/{domain_id}/ccaas/bandwidth-packages	cc:bandwidthPackages:list	-
POST /v3/{domain_id}/ccaas/bandwidth-packages/filter	cc:bandwidthPackages:list	-
POST /v3/{domain_id}/ccaas/bandwidth-packages/{id}/tag	cc:bandwidthPackages:tag	-
POST /v3/{domain_id}/ccaas/bandwidth-packages/{id}/untag	cc:bandwidthPackages:unTag	-
GET /v3/{domain_id}/ccaas/bandwidth-packages/tags	cc:bandwidthPackages:listTags	-

API	对应的授权项	依赖的授权项
POST /v3/{domain_id}/ccaas/bandwidth-packages/{id}/associate	cc:bandwidthPackages:associate	-
POST /v3/{domain_id}/ccaas/bandwidth-packages/{id}/disassociate	cc:bandwidthPackages:disassociate	-
POST /v3/{domain_id}/ccaas/inter-region-bandwidths	cc:interRegionBandwidths:create	-
PUT /v3/{domain_id}/ccaas/inter-region-bandwidths/{id}	cc:interRegionBandwidths:update	-
DELETE /v3/{domain_id}/ccaas/inter-region-bandwidths/{id}	cc:interRegionBandwidths:delete	-
GET /v3/{domain_id}/ccaas/inter-region-bandwidths/{id}	cc:interRegionBandwidths:get	-
GET /v3/{domain_id}/ccaas/inter-region-bandwidths	cc:interRegionBandwidths:list	-
GET /v3/{domain_id}/ccaas/cloud-connection-routes/{id}	cc:cloudConnectionRoutes:get	-
GET /v3/{domain_id}/ccaas/cloud-connection-routes	cc:cloudConnectionRoutes:list	-
POST /v3/{domain_id}/ccaas/authorisations	cc:authorisation:create	-

API	对应的授权项	依赖的授权项
DELETE /v3/{domain_id}/ccaas/authorisations/{id}	cc:authorisation:delete	-
PUT /v3/{domain_id}/ccaas/authorisations/{id}	cc:authorisation:update	-
GET /v3/{domain_id}/ccaas/authorisations	cc:authorisation:list	-
GET /v3/{domain_id}/ccaas/permissions	cc:authorisation:listPermissions	-
GET /v3/{domain_id}/ccaas/quotas	cc:quota:list	-
GET /v3/{domain_id}/gcn/quotas	cc:quota:list	-
GET /v3/{domain_id}/ccaas/capabilities	cc:capability:list	-
GET /v3/{domain_id}/gcn/capabilities	cc:capability:list	-
POST /v3/{domain_id}/gcn/central-networks	cc:centralNetwork:create	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate

API	对应的授权项	依赖的授权项
DELETE /v3/{domain_id}/gcn/central-networks/{central_network_id}	cc:centralNetwork:delete	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
PUT /v3/{domain_id}/gcn/central-networks/{central_network_id}	cc:centralNetwork:update	-
GET /v3/{domain_id}/gcn/central-networks/{central_network_id}	cc:centralNetwork:get	-
GET /v3/{domain_id}/gcn/central-networks	cc:centralNetwork:list	-
POST /v3/{domain_id}/gcn/central-networks/filter	cc:centralNetwork:list	-
POST /v3/{domain_id}/gcn/central-networks/{central_network_id}/tag	cc:centralNetwork:tag	-
POST /v3/{domain_id}/gcn/central-networks/{central_network_id}/untag	cc:centralNetwork:unTag	-

API	对应的授权项	依赖的授权项
GET /v3/{domain_id}/gcn/central-networks/tags	cc:centralNetwork:listTags	-
POST /v3/{domain_id}/gcn/central-network/{central_network_id}/policies	cc:centralNetwork:createPolicy	• er:instances:get • er:routeTables:get
POST /v3/{domain_id}/gcn/central-network/{central_network_id}/policies/{policy_id}/apply	cc:centralNetwork:applyPolicy	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
DELETE /v3/{domain_id}/gcn/central-network/{central_network_id}/policies/{policy_id}	cc:centralNetwork:deletePolicy	-
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/policies	cc:centralNetwork:listPolicies	-
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/policies/{policy_id}/change-set	cc:centralNetwork:listChangeSet	-
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/connections	cc:centralNetwork:listConnections	-

API	对应的授权项	依赖的授权项
PUT /v3/{domain_id}/gcn/central-network/{central_network_id}/connections/{connection_id}	cc:centralNetwork:updateConnection	-
POST /v3/{domain_id}/gcn/central-network/{central_network_id}/gdgw-attachments	cc:centralNetworkAttachment:createGdgw	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
PUT /v3/{domain_id}/gcn/central-network/{central_network_id}/gdgw-attachments/{gdgw_attachment_id}	cc:centralNetworkAttachment:updateGdgw	-
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/gdgw-attachments/{gdgw_attachment_id}	cc:centralNetworkAttachment:getGdgw	-
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/gdgw-attachments	cc:centralNetworkAttachment:listGdgws	-

API	对应的授权项	依赖的授权项
POST /v3/{domain_id}/gcn/central-network/{central_network_id}/er-route-table-attachments	cc:centralNetworkAttachment:createErRouteTable	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
PUT /v3/{domain_id}/gcn/central-network/{central_network_id}/er-route-table-attachments/{er_route_table_attachment_id}	cc:centralNetworkAttachment:updateErRouteTable	-
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/er-route-table-attachments/{er_route_table_attachment_id}	cc:centralNetworkAttachment:getErRouteTable	-
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/er-route-table-attachments	cc:centralNetworkAttachment:listErRouteTables	-

API	对应的授权项	依赖的授权项
DELETE /v3/{domain_id}/gcn/central-network/{central_network_id}/attachments/{attachment_id}	cc:centralNetworkAttachment:delete	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/attachments	cc:centralNetworkAttachment:list	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-69**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。

CC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 5-69 CC 支持的资源类型

资源类型	URN
cloudConnection	cc::<account-id>:cloudConnection:<cloud-connection-id>
interRegionBandwidth	cc::<account-id>:interRegionBandwidth:<inter-region-bandwidth-id>
networkInstance	cc::<account-id>:networkInstance:<network-instance-id>
siteNetwork	cc::<account-id>:siteNetwork:<site-network-id>
bandwidthPackage	cc::<account-id>:bandwidthPackage:<bandwidth-package-id>
centralNetwork	cc::<account-id>:centralNetwork:<central-network-id>

资源类型	URN
centralNetworkAttachment	cc::<account-id>:centralNetworkAttachment:<central-network-attachment-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cc:）仅适用于对应服务的操作，详情请参见表5-70。
  - 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：条件键。

CC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 5-70 CC 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
cc:VpcId	string	单值	根据指定的虚拟私有云资源ID过滤访问。
cc:VirtualGatewayId	string	单值	根据指定的专线虚拟网络资源ID过滤访问。
cc:EnterpriseRouterId	string	单值	根据指定的企业路由器资源ID过滤访问。
cc:MultipleEnterpriseRouterIds	string	多值	根据指定的多个企业路由器资源ID过滤访问。
cc:BandwidthPackageId	string	单值	根据指定的带宽包资源ID过滤访问。
cc:GlobalConnectionBandwidthId	string	单值	根据指定的全域互联带宽资源ID过滤访问。
cc:GlobalDcGatewayId	string	单值	根据指定的全球接入网关资源ID过滤访问。

5.10.4 容器

5.10.4.1 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 5-71 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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
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>
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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5-72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
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

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}	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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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5-73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 5-73 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5-74。
  - 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 5-74 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。
cce:AssociatePublicIp	string	单值	根据创建ECS是否涉及自动创建EIP操作筛选访问权限。如果要限制集群绑定或解绑EIP操作权限，则需要使用cce:cluster:eipBinding这个action进行管控。
cce:VpcId	string	单值	按照集群创建所选择的VPC筛选访问权限。
cce:SubnetId	string	单值	按照集群/节点/节点池创建所选择的子网筛选访问权限。
cce:Subnets	array	单值	按照节点池创建/更新所选择的多子网筛选访问权限。
cce:KmsKeys	string	单值	按照节点/节点池创建所选择的磁盘加密KMS密钥筛选访问权限。

5.10.4.2 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 5-75 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:AllowPublicAccess
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:AllowPublicAccess
swr:repo:deleteRepoTag	授予共享版仓库删除镜像仓库中指定版本的镜像的权限。	Write	repo *	-
swr:repo:createRepoTag	授予共享版仓库创建镜像版本的权限。	Write	repo *	-
swr:repo:listRepoTags	授予共享版仓库查询镜像版本列表的权限。	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 *	-
			-	swr:TargetRegion

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:TargetRegion
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:repository:createImmutableRule	授予创建企业仓库镜像不可变规则的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteImmutableRule	授予删除企业仓库镜像不可变规则的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listImmutableRules	授予企业仓库获取镜像不可变规则列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateImmutableRule	授予企业仓库修改镜像不可变规则的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listArtifacts	授予查询制品列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getArtifact	授予查询制品详情的权限。	Read	repository *	• 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
swr:repository:deleteArtifact	授予删除制品的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listAccessories	授予查询制品附件列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getArtifactAddition	授予查询制品附加信息的权限。	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:getConfigurations	授予查询企业版实例配置的权限。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:updateConfigurations	授予更新企业版实例配置的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listResourceInstances	授予授予查询资源实例列表的权限。	List	instance *	-
			-	• g:TagKeys • g:RequestTag/<tag-key>
swr:instance:getResourceInstancesCount	授予授予查询资源实例数量的权限。	Read	instance *	-
			-	• g:TagKeys • g:RequestTag/<tag-key>
swr:instance:createResourceTags	授予批量创建资源标签的权限。	Tagging	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• 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
swr:instance:deleteResourceTags	授予批量删除资源标签的权限。	Tagging	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
swr:instance:getProjectTags	授予查询项目标签的权限。	Read	-	-
swr:instance:getResourceTags	授予查询资源标签的权限。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:create	授予创建企业版实例的权限。	Write	instance *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys • **swr:VpcId** • **swr:SubnetId** • **swr:EnableObsEncrypt**
swr:instance:list	授予查询企业版实例列表信息的权限。	List	instance *	-
swr:instance:get	授予查询企业版实例信息的权限。	Read	instance *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
swr:instance:delete	授予删除企业版实例的权限。	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
swr:instance:getAuditLogs	授予查询企业版实例审计日志的权限。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:getStatistics	授予查询企业版实例统计信息的权限。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listJobs	授予查询任务列表的权限。	List	instance *	-
swr:instance:getJobs	授予查询任务详情的权限。	Read	instance *	-
swr:instance:deleteJob	授予删除任务的权限。	Write	instance *	-
swr:repository:createNamespace	授予创建命名空间(组织)的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	**swr:EnablePublicNameSpace**
swr:repository:listNamespaces	授予查询命名空间(组织)列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getNamespace	授予查询命名空间(组织)详情的权限。	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateNamespace	授予修改命名空间(组织)的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	**swr:EnablePublicNameSpace**
swr:repository:deleteNamespace	授予删除命名空间(组织)的权限。	Write	repository *	• 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
swr:repository:listRepositories	授予获取制品仓库列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getRepository	授予获取制品仓库详情的权限。	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateRepository	授予修改制品仓库配置的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteRepository	授予删除制品仓库的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listTags	授予查询制品版本列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getTag	授予查询制品版本详情的权限。	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteTag	授予删除制品版本的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getTagAddition	授予查询制品版本附加信息的权限。	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:createRetentionPolicy	授予创建版本清理策略的权限。	Write	repository *	• 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
swr:repository:listRetentionPolicies	授予查询版本清理策略列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getRetentionPolicy	授予查询版本清理策略详情的权限。	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateRetentionPolicy	授予修改版本清理策略配置的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteRetentionPolicy	授予删除版本清理策略的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:executeRetentionPolicy	授予应用版本清理策略的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listRetentionPolicyExecutions	授予获取版本清理执行记录列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listRetentionPolicyExecTasks	授予获取版本清理任务列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listRetentionPolicyExecSubTasks	授予获取版本清理子任务列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:createWebhook	授予创建触发器的权限。	Write	repository *	• 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
swr:repository:listWebhooks	授予查询触发器列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getWebhook	授予查询触发器详情的权限。	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateWebhook	授予修改触发器配置的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteWebhook	授予删除触发器的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listWebhookJobs	授予获取触发器执行记录列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:createRegistry	授予创建目标仓库的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listRegistries	授予获取目标仓库列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:getRegistry	授予获取目标仓库详情的权限。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:updateRegistry	授予修改目标仓库配置的权限。	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
swr:instance:deleteRegistry	授予删除目标仓库的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:createReplicationPolicy	授予创建复制策略的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listReplicationPolicies	授予查询复制策略列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:getReplicationPolicy	授予查询复制策略详情的权限。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:updateReplicationPolicy	授予修改复制策略的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:deleteReplicationPolicy	授予删除复制策略的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:executeReplicationPolicy	授予应用复制策略的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:stopReplicationPolicyExecution	授予停止复制任务的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listReplicationPolicyExecutions	授予查询复制记录列表的权限。	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
swr:instance:listReplicationPolicyExecTasks	授予查询复制任务列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listReplicationPolicyExecSubTasks	授予查询复制子任务列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:createSignPolicy	授予创建签名策略的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listSignPolicies	授予查询签名策略列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getSignPolicy	授予查询签名策略详情的权限。	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateSignPolicy	授予修改签名策略的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteSignPolicy	授予删除签名策略的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:executeSignPolicy	授予执行签名策略的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listSignPolicyExecutions	授予查询签名执行记录列表的权限。	List	repository *	• 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
swr:repository:listSignPolicyExecTasks	授予查询签名任务列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listSignPolicyExecSubTasks	授予查询签名策略执行记录子任务列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:createScanPolicy	授予创建扫描策略的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listScanPolicies	授予查询扫描策略列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getScanPolicy	授予查询扫描策略详情的权限。	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateScanPolicy	授予修改扫描策略的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteScanPolicy	授予删除扫描策略的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:executeScanPolicy	授予执行扫描策略的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listScanPolicyExecutions	授予查询扫描执行记录列表的权限。	List	repository *	• 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
swr:repository:listScanPolicyExecTasks	授予查询扫描任务列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:createBlockPolicy	授予创建阻断策略的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listBlockPolicies	授予查询阻断策略列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getBlockPolicy	授予查询阻断策略详情的权限。	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateBlockPolicy	授予修改阻断策略配置的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteBlockPolicy	授予删除阻断策略的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listBlockPolicyRecords	授予查询阻断记录列表的权限。	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:updateEndpointPolicy	授予更新公网访问白名单配置的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:updateEndpointPolicyStatus	授予更新公网访问白名单配置状态的权限。	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
swr:instance:getEndpointPolicy	授予查询公网访问白名单配置的权限。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:createInternalEndpoint	授予创建内网访问的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• **swr:VpcId** • **swr:SubnetId**
swr:instance:getInternalEndpoint	授予获取内网访问的权限。	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:deleteInternalEndpoint	授予删除内网访问的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listInternalEndpoints	授予查询内网访问列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:uploadArtifact	授予上传制品的权限。	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:downloadArtifact	授予下载制品的权限。	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:createTempCredential	授予创建临时访问凭证的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:createLTCredential	授予创建长期访问凭证的权限。	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
swr:instance:updateLTCredential	授予启用/停用长期访问凭证的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listLTCredentials	授予查询长期访问凭证列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:deleteLTCredential	授予删除长期访问凭证的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:addDomainName	授予增加域名的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:deleteDomainName	授予删除域名的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:updateDomainName	授予更新域名的权限。	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listDomainNames	授予查询域名列表的权限。	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

SWR的API通常对应着一个或多个授权项。表5-76展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-76 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	-

API	对应的授权项	依赖的授权项
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	-
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	-
POST /v2/manage/namespaces/{namespace}/repos/{repository}/tags	swr:repo:createRepoTag	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/tags	swr:repo:listRepoTags	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
GET /v2/manage/overview	swr::getDomainOverview	-
GET /v2/manage/reports/{resource_type}/{frequency}	swr::getDomainResourceReports	-
POST /v2/manage/namespaces/{namespace}/access	swr:namespace:createNamespaceAccess	-
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	-

API	对应的授权项	依赖的授权项
PATCH /v2/manage/namespaces/{namespace}/repos/{repository}/access	swr:repo:updateRepoAccess	-

⚠ 注意

SWR的细粒度鉴权，会兼容SWR的本地授权和鉴权体系，如果本地鉴权通过，且IAM未显示配置deny策略，则会以本地鉴权结果为准。

SWR的如下action：swr::createLoginSecret，swr:namespace:listNamespaces，swr:repo:listRepos，swr::getDomainOverview，swr::getDomainResourceReports，swr:repo:listSharedRepos在本地鉴权中，默认为allow。因此如需限制用户调用，则需要在IAM配置显示deny策略。

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-77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 5-77 SWR 支持的资源类型

资源类型	URN
repo	swr:<region>:<account-id>:repo:<namespace-name>/<repo-name>
repository	swr:<region>:<account-id>:repository:<instance-name>/<repository-path>
instance	swr:<region>:<account-id>:instance:<instance-name>
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5-78。
  - 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 5-78 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。
swr:VpcId	string	单值	按照用户VPC ID进行权限控制。
swr:SubnetId	string	单值	按照用户Subnet ID进行权限控制。
swr:EnablePublicNameSpace	boolean	单值	限制企业仓库是否允许创公开组织。
swr:EnableObsEncrypt	boolean	单值	限制企业版实例是否必须使用加密桶。
swr:AllowPublicAccess	boolean	单值	对镜像是否可以公开进行权限控制。
swr:TargetRegion	string	单值	根据目标区域进行权限控制。

5.10.5 大数据

5.10.5.1 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。
  - 资源类型列中必须资源在表中用星号（*）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 5-79 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5-80展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-80 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 5-81 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5-82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。

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 5-82 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5-83**。
  - 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 5-83 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。

5.10.5.2 数据治理中心 DataArts Studio

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DataArts Studio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DataArts Studio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DataArts Studio的相关操作。

说明

由于当前接口限制，SCP指定资源类型时，由于部分操作不支持指定具体的workspace或instance资源，会导致权限配置不符合预期。如允许（allow）某个不支持指定资源的操作，但又为其指定了具体资源时，会导致所有资源操作均被拒绝；拒绝（deny）某个不支持指定资源的操作，但又为其指定了具体资源时，会导致所有资源操作均被允许。

因此，在SCP需要指定资源类型时，需要剔除这类操作，然后将这类操作独立为不指定资源或指定全局资源的SCP语句，使用多个SCP语句一起为用户赋权。不指定资源或指定全局资源的SCP语句，即JSON策略内容中不带Resource元素，或者Resource内容如下所示：

```
"Resource": [
    "DataArtsStudio:*:*:workspace:*",
    "DataArtsStudio:*:*:instance:*"
]
```

当前DataArts Studio不支持指定具体资源的操作汇总如下：

- 不支持指定workspace资源，仅支持指定instance资源：
  - DataArtsStudio:workspace:create
  - DataArtsStudio:workspace:list
- 不支持指定instance资源或workspace资源：
  - DataArtsStudio:instance:create
  - DataArtsStudio:instance:get
  - DataArtsStudio:instance:list
  - DataArtsStudio:instance:resize
  - DataArtsStudio:instance:getAgency
  - DataArtsStudio:instance:createAgency
  - DataArtsStudio:instance:uploadDriver
  - DataArtsStudio:instance:deleteDriver
  - DataArtsStudio:instance:listDrivers
  - DataArtsStudio:instance:listTags
  - DataArtsStudio:workspace:listTags

表 5-84 DataArts Studio 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	别名
DataArtsStudio:workspace:list	授予权限以列举所有工作空间。	List	workspace *	g:ResourceTag/<tag-key>	dgc:workspace:list
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:workspace:create	授予权限以创建工作空间。	Write	workspace *	-	-
			instance *	g:ResourceTag/<tag-key>	

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			-	• g:RequestTag/<tag-key> • g:TagKeys	
DataArtsStudio:workspace:get	授予权限以查询工作空间信息。	Read	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:workspace:frozen	授予权限以冻结工作空间。	Write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:workspace:unfrozen	授予权限以解除工作空间冻结。	Write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:workspace:update	授予权限以更新工作空间信息。	Write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:instance:list	授予权限以列举所有实例。	List	instance *	g:ResourceTag/<tag-key>	dgc:workspace:list
DataArtsStudio:instance:create	授予权限以创建实例。	Write	instance *	-	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
DataArtsStudio:instance:get	授予权限以查询实例。	Read	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:resize	授予权限以变更实例规格。	Write	instance *	g:ResourceTag/<tag-key>	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
DataArtsStudio:instance:listDrivers	授予权限以查询所有驱动文件。	List	-	-	-
DataArtsStudio:instance:uploadDriver	授予权限以上传驱动文件。	Write	-	-	-
DataArtsStudio:instance:deleteDriver	授予权限以删除驱动文件。	Write	-	-	-
DataArtsStudio:workspace:delete	授予权限以删除工作空间。	Write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:instance:getAgency	授予权限以查询云服务访问授权委托。	Read	-	-	-
DataArtsStudio:instance:createAgency	授予权限以创建云服务访问授权委托。	Write	-	-	-
DataArtsStudio:instance:delete	授予权限以删除实例。	Write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:migrateBusinessModel	授予权限以迁移实例商业模式。	Write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:operate	授予权限以操作实例上的资源。	Write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:workspace:operate	授予权限以操作工作空间上的资源。	Write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:instance:createRole	授予权限以创建自定义角色。	Write	instance *	g:ResourceTag/<tag-key>	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
DataArtsStudio:instance:listRoles	授予权限以查询自定义角色列表。	List	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:getRoleType	授予权限以查询自定义角色类型。	Read	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:getRole	授予权限以查询自定义角色。	Read	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:updateRole	授予权限以更新自定义角色。	Write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:deleteRole	授予权限以删除自定义角色。	Write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:tagResource	授予权限以增加实例标签。	Write	instance *	g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
DataArtsStudio:instance:unTagResource	授予权限以删除实例标签。	Write	instance *	g:ResourceTag/<tag-key>	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
DataArtsStudio:instance:listIncrementalPackages	授予权限以列举所有增量包。	List	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:workspace:createIncrementalPackage	授予权限以创建工作空间增量包。	Write	workspace *	• g:ResourceTag/<tag-key> • **DataArtsStudio:EnablePublicAccess**	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:workspace:tagResource	授予权限以增加工作空间标签。	Write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
DataArtsStudio:workspace:unTagResource	授予权限以删除工作空间标签。	Write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
			-	• g:RequestTag/<tag-key> • g:TagKeys	
DataArtsStudio:instance:createIncrementalPackage	授予权限以创建实例增量包。	Write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:listTags	授予权限以获取所有实例标签列表。	List	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:workspace:listTags	授予权限以获取所有工作空间标签列表。	List	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:instance:listTagsForResource	授予权限以获取某个实例标签列表。	List	instance *	g:ResourceTag/<tag-key>	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
DataArtsStudio:workspace:listTagsForResource	授予权限以获取某个工作空间标签列表。	List	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:workspace:updateDataServiceApiQuota	授予权限以更新工作空间数据服务API配额。	Write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:workspace:executeDataServiceInstanceAction	授予权限以执行数据服务集群操作命令。	Write	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	
DataArtsStudio:instance:configureDataSecurityAdministrator	授予权限以配置数据安全管理员。	Write	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:instance:listResourcesByTag	授予权限以根据标签筛选实例列表。	List	instance *	g:ResourceTag/<tag-key>	-
DataArtsStudio:workspace:listResourcesByTag	授予权限以根据标签筛选空间列表。	List	workspace *	g:ResourceTag/<tag-key>	-
			instance *	g:ResourceTag/<tag-key>	

DataArts Studio的API通常对应着一个或多个授权项。**表5-85**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-85 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}/workspaces/{instance_id}	DataArtsStudio:workspace:list	-
POST /v1/{project_id}/workspaces/{instance_id}	DataArtsStudio:workspace:create	-
GET /v1/{project_id}/workspaces/{instance_id}/{workspace_id}	DataArtsStudio:workspace:get	-
POST /v1/{project_id}/change-resource	DataArtsStudio:instance:resize	-
GET /v1/{project_id}/instances	DataArtsStudio:instance:list	-
POST /v1/{project_id}/instances/onekey-purchase	DataArtsStudio:instance:create	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-86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。

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

表 5-86 DataArts Studio 支持的资源类型

资源类型	URN
workspace	DataArtsStudio:<region>:<account-id>:workspace:<instance-id>/<workspace-id>
instance	DataArtsStudio:<region>:<account-id>:instance:<instance-id>

条件（Condition）

条件键概述

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DataArtsStudio:）仅适用于对应服务的操作，详情请参见**表5-87**。
  - 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。

DataArts Studio支持的服务级条件键

DataArts Studio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 5-87 DataArts Studio 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
DataArtsStudio:EnablePublicAccess	boolean	单值	是否开启公网访问。

5.10.5.3 数据仓库服务 GaussDB(DWS)

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GaussDB(DWS)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GaussDB(DWS)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GaussDB(DWS)的相关操作。

表 5-88 GaussDB(DWS)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
dws:cluster:list	授予集群列表查询权限。	list	-	-
dws:cluster:getDetail	授予集群详情查看权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:create	授予DWS集群创建权限。	write	-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dws:cluster:delete	授予DWS集群删除权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:scaleIn	授予DWS集群缩容权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listRing	授予获得合适的缩容环列表权限。	list	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
dws:cluster:restore	授予就地恢复集群权限。	write	cluster *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dws:cluster:scaleOut	授予集群扩容权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:resize	授予集群扩容和调整大小权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:expandDisk	授予DWS集群磁盘扩容权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:restart	授予DWS集群重启权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:resetPassword	授予DWS集群重置密码权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listAuditLog	授予查看审计日志列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:setMaintainceWindow	授予维护时间窗修改权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:switchover	授予集群主备恢复权限。	write	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
dws:cluster:cancelReadonly	授予集群解除只读权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:addCN	授予集群增加CN节点权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listCN	授予获取集群CN列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteCN	授予删除CN节点权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:redistribution	授予集群数据重分布权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createDataSource	授予创建MRS数据源权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateDataSource	授予更新MRS数据源权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteDataSource	授予删除MRS数据源权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:alarm:listDetail	授予查询告警详情列表权限。	list	-	-
dws:alarm:report	授予上报告警权限。	write	-	-
dws:event:createSpec	授予创建事件配置权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dws:event:deleteSpec	授予删除事件配置权限。	write	-	-
dws:event:report	授予上报事件权限。	write	-	-
dws:cluster:createConnection	授予创建DWS集群连接权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteConnection	授予删除DWS集群连接权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateConnection	授予更新DWS集群连接权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:bindEIP	授予公网IP绑定权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:unbindEIP	授予公网IP解绑权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listELB	授予获得弹性负载均衡列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:bindELB	授予绑定弹性负载均衡权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:unbindELB	授予解绑弹性负载均衡权限。	write	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
dws:cluster:createSnapshotPolicy	授予设置自动快照策略权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listSnapshotStatistics	授予查询快照空间容量权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listSnapshot	授予查看集群快照列表权限。	list	cluster	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getSnapshotDetail	授予查看集群快照详情权限。	list	cluster	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createSnapshot	授予使用API创建快照权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteSnapshotPolicy	授予删除快照策略权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listSnapshotPolicy	授予查询快照策略权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:copySnapshot	授予复制快照权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteSnapshot	授予删除快照权限。	write	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
dws:cluster:restoreSnapshot	授予恢复快照权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteDisasterRecovery	授予删除容灾权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createDisasterRecovery	授予创建备份容灾权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:restoreDisaster	授予容灾恢复权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws::listTagsForProject	授予查询该项目下的标签列表权限。	list	-	-
dws:cluster:listConfig	授予查看集群配置参数权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:service:listSpec	授予查看服务规格列表权限。	list	-	-
dws:cluster:listDataSource	授予查看集群数据源权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:service:listJobDetail	授予查看任务进度详情权限。	list	-	-
dws:service:listStatistics	授予查看当前可用资源数量权限。	list	-	-
dws:service:listQuotas	授予查看用户配额权限。	list	-	-
dws:cluster:updateConfig	授予更新集群配置参数权限。	write	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
dws:service:listAZ	授予查看服务可用区列表权限。	list	-	-
dws:service:listDssPools	授予查看专属存储池列表权限。	list	-	-
dws:service:listEps	授予查看eps列表权限。	list	-	-
dws:service:authorize	授予获取用户授权权限。	write	-	-
dws:service:checkAuthorize	授予检查用户授权权限。	read	-	-
dws::updateTag	授予更新标签权限。	tagging	cluster *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dws:cluster:getSnapshotPolicy	授予查看快照策略权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:bindOrUnbindELB	授予绑定或解绑弹性负载均衡权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:bindOrUnbindEIP	授予绑定或解绑弹性IP权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteNode	授予删除节点权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listConnection	授予查询DWS集群连接列表权限。	list	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
dws:cluster:checkConnection	授予检查DWS集群连接权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listDN	授予获取集群DN列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listBucket	授予获取桶列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listScaleInNode	授予获取缩容待删除节点列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listFlavorForResize	授予查询支持变更的规格列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listFlavorForRestore	授予查询支持恢复的规格列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws::countResourceByTag	授予使用标签查询集群权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateSnapshotPolicy	授予更新快照策略权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws::listResourceByTag	授予根据标签查询集群列表权限。	list	cluster *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
dws:cluster:assessRisk	授予评估调整大小风险权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:checkRestoreTable	授予恢复表检查权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:checkSupportFineGrainedBackup	授予检测集群是否支持细粒度备份权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:configureNetwork	授予配置集群网络权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:expandWithExistedNodes	授予集群从空闲节点扩容权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getAntiAffinity	授予查询反亲和性状态权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getCnCount	授予查询集群CN数量权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getCredential	授予获取集群JDBC连接凭证权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getDiskExpandScope	授予获取磁盘扩容范围权限。	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
dws:cluster:getEncryptInfo	授予查看集群加密信息权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listHistoryConfig	授予查询参数修改历史权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getHistoryConfigDetail	授予查询参数修改历史详情权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getInstanceDetail	授予实例详情查看权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getProcessTopo	授予查询集群节点进程拓扑权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getRedistribution	授予查询重分布详情权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getRestoreDatabase	授予获取用户恢复数据库权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getRoachConfig	授予获取roach参数配置权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getSnapshotEncryptInfo	授予查看快照加密信息权限。	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
dws:cluster:getSnapshotStorage	授予查询快照空间容量使用情况权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getTaskDetail	授予查询集群任务详情权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getVolumeInfo	授予查询磁盘信息权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listNode	授予查询节点列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listSchema	授予获取用户结构列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listTable	授予获取用户表列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listDatabase	授予获取用户数据库列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:recoverRedistribution	授予恢复重分布权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:resizeFlavor	授予执行规格变更权限。	write	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
dws:cluster:resizeRetry	授予调整大小重试权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:restoreTable	授予表恢复权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:retryELBSwitch	授予重试ELB切换任务权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listRingForScaleIn	授予获得缩容环列表权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:stopSnapshot	授予停止快照权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:suspendRedistribution	授予暂停重分布权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateInstanceAliasName	授予更新节点别名权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateRoachConfig	授予更新roach参数配置权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateScheduleConfig	授予更新调度配置权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:service:getClusterSum	授予查询集群数量权限。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dws:service:getResourceStatistics	授予查询资源统计权限。	read	-	-
dws:service:getStorageStatistics	授予查询存储统计信息权限。	read	-	-
dws:cluster:listDisasterRecovery	授予容灾列表查询操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:checkDisasterRecoveryName	授予容灾名称检查操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateDisasterRecoveryConfig	授予更新容灾配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:addOperationalTask	授予新增调度任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:bindManageIp	授予绑定管理面IP操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:checkAccessLts	授予检查LTS服务是否正常操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:checkLogicalClusterData	授予逻辑集群-检查集群有无业务数据操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:closeAccessLts	授予关闭云服务日志操作权限。	write	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
dws:cluster:createLogicalCluster	授予逻辑集群-创建逻辑集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createApplicationForDM	授予数据迁移-增加作业任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createClusterForDM	授予数据迁移-创建集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createConnectionForDM	授予数据迁移-增加指定连接信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createMappingForDM	授予数据迁移-增加指定映射信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteApplicationForDM	授予数据迁移-删除作业任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteClusterForDM	授予数据迁移-删除集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteConnectionForDM	授予数据迁移-删除指定连接信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteMappingForDM	授予数据迁移-删除指定映射信息操作权限。	write	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
dws:cluster:dialsConnectionForDM	授予数据迁移-连接信息探活操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getApplicationForDM	授予数据迁移-查询作业任务详情操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listApplicationConfigForDM	授予数据迁移-作业任务参数配置信息操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listApplicationForDM	授予数据迁移-查询集群内所有作业任务操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getClusterForDM	授予数据迁移-查询集群信息详情操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listClusterForDM	授予数据迁移-查询集群信息列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listConfigurationTemplateForDM	授予数据迁移-查询参数模板操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getConnectionForDM	授予数据迁移-查询连接信息详情操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listConnectionForDM	授予数据迁移-查询所有连接信息操作权限。	list	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
dws:cluster:listDependApplicationForDM	授予数据迁移-查询所有依赖作业任务操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getMappingForDM	授予数据迁移-查询映射信息详情操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listMappingForDM	授予数据迁移-查询所有映射信息操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listProductForDM	授予GDS-Kafka-查询产品信息操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateConnectionForDM	授予数据迁移-修改指定连接信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateMappingForDM	授予数据迁移-修改指定映射信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:startApplicationForDM	授予数据迁移-启动作业任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:stopApplicationForDM	授予数据迁移-停止作业任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteCrossRegionSnapshotPolicy	授予删除跨区域备份配置操作权限。	write	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
dws:cluster:deleteLogicalCluster	授予逻辑集群-删除逻辑集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteOperationalTask	授予调度器-删除调度任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:operateDisasterRecovery	授予容灾-容灾操作，启/停/切换等操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateLogicalCluster	授予逻辑集群-更新逻辑集群权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listAllCrossRegionSnapshotConfig	授予查询所有跨区域快照配置操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getDisasterRecoveryProject	授予容灾-查询可用project操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getDisasterRecoveryRegion	授予容灾-查询可用region操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getLastOperationalTask	授予调度器-查询上次构建任务操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getLogicalClusterRings	授予逻辑集群-查询集群环信息操作权限。	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
dws:cluster:getLogicalClusterVolume	授予逻辑集群-查询集群磁盘信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getOperationalTaskConfig	授予调度器-获取调度器运维任务公共配置操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getOperationalTaskDetail	授予调度器-获取运维任务详情列表操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getOperationalTaskStatus	授予调度器-获取调度器状态操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listSnapshotRegion	授予获取跨区域快照可用region操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getTargetAllCrossRegionSnapshotConfig	授予查询所有跨区域快照配置操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:initLogicalClusterSwitch	授予逻辑集群-切换逻辑集群开关操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listAccessLts	授予查询LTS列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listLogicalCluster	授予逻辑集群-查询逻辑集群列表操作权限。	list	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
dws:cluster:listLogicalClusterTask	授予逻辑集群-查询任务信息操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listOperationalTask	授予调度器-获取运维任务列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:openAccessLts	授予开启云服务日志操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:pauseOperationalTask	授予调度器-暂停调度任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getDisasterRecoveryDetail	授予容灾-查询容灾详情操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:refreshOperationalTask	授予调度器-远程刷新当前集群运维任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:restartLogicalCluster	授予逻辑集群-重启逻辑集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:resumeOperationalTask	授予调度器-恢复调度任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:setCrossRegionSnapshotPolicy	授予设置跨区域备份配置操作权限。	write	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
dws:cluster:startOperationalTask	授予调度器-打开调度器操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:stopOperationalTask	授予调度器-关闭调度器操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:switchLogicalCluster	授予逻辑集群-转换到逻辑集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:syncCrossRegionBackupClusterInfo	授予同步跨region备份集群信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:syncCrossRegionBackupConfig	授予同步跨区域快照配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:syncCrossRegionBackupInfo	授予同步跨region快照信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:syncLogicalCluster	授予逻辑集群-逻辑集群从后台同步操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateOperationalTaskConfig	授予调度器-修改调度器运维任务公共配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateOperationalTask	授予调度器-修改调度任务操作权限。	write	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
dws:cluster:addPlanForWLM	授予工作负载管理-添加工作负载计划操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:addPlanStageForWLM	授予工作负载管理-添加工作负载计划阶段操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:addQueueForWLM	授予工作负载管理-添加工作负载队列操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:addQueueUserForWLM	授予工作负载管理-添加工作负载队列的绑定用户操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deletePlanForWLM	授予工作负载管理-删除工作负载计划操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deletePlanStageForWLM	授予工作负载管理-删除工作负载计划阶段操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteQueueForWLM	授予工作负载管理-删除工作负载队列操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteQueueUserForWLM	授予工作负载管理-删除工作负载队列的绑定用户操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:exportPlanForWLM	授予工作负载管理-导出工作负载计划操作权限。	write	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
dws:cluster:getPlanDetailForWLM	授予工作负载管理-查询某个工作负载计划详细信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getPlanLogForWLM	授予工作负载管理-查看计划执行日志操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getPlanQueueForWLM	授予工作负载管理-查询某个队列是否在计划中操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getPlanStageForWLM	授予工作负载管理-查询工作负载计划阶段操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listQueueForWLM	授予工作负载管理-获得当前集群的工作负载队列的名称列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getQueueDetailForWLM	授予工作负载管理-获得工作负载队列信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getQueueRuleForWLM	授予工作负载管理-获得工作负载队列异常规则信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:importPlanForWLM	授予工作负载管理-导入工作负载计划操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listPlanQueueForWLM	授予工作负载管理-查询所有工作负载计划可用的队列信息操作权限。	list	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
dws:cluster:listPlanForWLM	授予工作负载管理-查询工作负载计划操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listQueueUserForWLM	授予工作负载管理-获得工作负载队列的绑定用户列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listUserForWLM	授予工作负载管理-获得集群中所有未绑定工作负载队列的用户列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getClusterDBInfoForWLM	授予工作负载管理-查询集群数据库信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listClusterPlanForWLM	授予工作负载管理-查询集群中所有工作负载计划操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getClusterSchemaInfoForWLM	授予工作负载管理-查询集群模式空间信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getClusterVersionForWLM	授予工作负载管理-获得当前集群后台数据库的版本操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getFunctionStatusForWLM	授予工作负载管理-获得工作负载功能开关状态操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:setFunctionStatusForWLM	授予工作负载管理-设置工作负载功能开关状态操作权限。	write	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
dws:cluster:startPlanForWLM	授予工作负载管理-启动工作负载计划操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:stopPlanForWLM	授予工作负载管理-停止工作负载计划操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:switchPlanStageForWLM	授予工作负载管理-切换工作负载阶段操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updatePlanStageForWLM	授予工作负载管理-修改工作负载计划阶段操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateQueueBaseForWLM	授予工作负载管理-更新工作负载队列基础信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateQueueResourceForWLM	授予工作负载管理-更新工作负载队列资源配置信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateQueueRuleForWLM	授予工作负载管理-更新工作负载队列异常规则信息操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateSchemaLimitForWLM	授予工作负载管理-更新模式空间限额操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getMonitorConfigForDMS	授予DMS-查询采集配置或存储配置额操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:listClusterOverview	授予DMS-获取集群概览操作权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dws:cluster:listClusterInstanceForDMS	授予DMS-获取集群实例列表操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getDDLExamineDetailForDMS	授予DMS-查询审核结果详细信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getClusterDnStreamForDMS	授予DMS-查询dn数据流监控信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listClusterAlarmRuleForDMS	授予DMS-查询租户侧告警规则列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getClusterInstanceForDMS	授予DMS-查询实例信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getHostNetMetricsForDMS	授予DMS-查询网络状态操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:getHistoryMetrics	授予DMS-查询历史监控数据操作权限。	read	-	-
dws:cluster:getMonitoringInfoForDMS	授予DMS-查询监控数据操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listAlarmRuleForDMS	授予DMS-租户侧根据告警id查询告警规则操作权限。	list	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
dws:cluster:updateCollectionItemForDMS	授予DMS-更新采集配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:doDDLExamineActionForDMS	授予DMS-手动触发审核操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:downloadDDLExamineDetailForDMS	授予DMS-DDL审核详情下载操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listInstanceDiskIOForDMS	授予DMS-查询磁盘IO操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:resetCollectionItemForDMS	授予DMS-重置采集配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getQueryRangeForDMS	授予DMS-查询时间句柄操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:getAlarmConfig	授予DMS-租户侧查询所有集群和告警配置信息操作权限。	read	-	-
dws:cluster:switchoverCollectionItemForDMS	授予DMS-切换采集开关操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:getOSMetrics	授予DMS-查询DWS硬件资源使用情况操作权限。	read	-	-
dws:cluster:listPerfDashboardForDMS	授予DMS-查询当前用户所有性能监控面板操作权限。	list	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
dws:cluster:disableCollectionItemForDMS	授予DMS-关闭采集开关操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:getAggregationOSMetrics	授予DMS-查询DWS集群硬件资源使用情况操作权限。	read	-	-
dws:cluster:terminateSessionForDMS	授予DMS-终止会话操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getPerfDashboardDetailForDMS	授予DMS-通过面板id获取面板信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:createAlarmRule	授予DMS-租户侧添加告警规则操作权限。	write	-	-
dws:cluster:enableCollectionItemForDMS	授予DMS-开启采集开关操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listInstanceNetworkMetricsForDMS	授予DMS-查询DWS集群节点各网卡流量操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createPerfDashboardForDMS	授予DMS-创建用户面板操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getMonitorMetricsForDMS	授予DMS-获取首页监控项操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createSQLProbeForDMS	授予DMS-新增SQL探针操作权限。	write	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
dws:cluster:listInstanceIOStatusForDMS	授予DMS-查询DWS集群各节点磁盘IO使用情况操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getMonitorMetricsByDimensionForDMS	授予DMS-按维度获取指标操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateStorageConfigForDMS	授予DMS-更新存储配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:updateAlarmRule	授予DMS-租户侧修改告警规则操作权限。	write	-	-
dws:cluster:getInstanceIOAggResultForDMS	授予DMS-查询DWS集群各节点磁盘IO汇聚使用情况操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updatePerfDashboardForDMS	授予DMS-修改用户面板操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getMonitorHistoryMetricsCost	授予DMS-查询队列历史消耗操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:deleteAlarmRule	授予DMS-租户侧删除规则操作权限。	write	-	-
dws:cluster:updateSQLProbeForDMS	授予DMS-修改SQL探针操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:startMonitorMetricsCollectionForDMS	授予DMS-开始采集操作权限。	write	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
dws:cluster:listInstanceStorageForDMS	授予DMS-查询DWS集群各节点文件系统使用情况操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deletePerfDashboardForDMS	授予DMS-删除用户监控面板操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getMonitorMetricsDetailForDMS	授予DMS-查询指标数据操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteSQLProbeForDMS	授予DMS-删除SQL探针操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:stopAlarmRule	授予DMS-租户侧停用规则操作权限。	write	-	-
dws:cluster:stopMonitorMetricsCollectionForDMS	授予DMS-停止采集操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listExceptionTableForDMS	授予DMS-查询表倾斜或脏页率信息操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getInstanceStorageAggForDMS	授予DMS-查询DWS集群各节点文件系统使用情况操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getWDRSnapShotForDMS	授予DMS-获取快照记录操作权限。	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
dws:cluster:getPerfMetricsDataForDMS	授予DMS-获取所有监控指标操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listQueryForDMS	授予DMS-获取当前所有的查询操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getInstanceIOMetricsForDMS	授予DMS-查询网卡IO数据操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getSQLProbeDetailForDMS	授予DMS-查询SQL探针详情操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:switchoverMonitorMetricStatusForDMS	授予DMS-切换采集开关操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:startAlarmRule	授予DMS-租户侧启用规则操作权限。	write	-	-
dws:monitor:getClusterStatus	授予DMS-查询DWS集群状态操作权限。	read	-	-
dws:cluster:getPerfMetricsDetailForDMS	授予DMS-通过pmid获取监控项操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listSlowInstanceForDMS	授予DMS-查询慢节点操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getDDLExamineConfigForDMS	授予DMS-查询采集配置操作权限。	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
dws:cluster:getMonitoringViewStatusForDMS	授予DMS-获取DMS视图状态操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:enableAlarm	授予DMS-租户侧集群启用告警功能操作权限。	write	-	-
dws:cluster:createWDRSnapShotForDMS	授予DMS-新增快照操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listExecuteStatusForDMS	授予DMS-查询DWS集群查询执行情况操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getSlowInstanceDetailForDMS	授予DMS-查询慢节点详情操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:enableSQLProbeForDMS	授予DMS-更新SQL探针启用状态操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getWDRConfigForDMS	授予DMS-查询集群WDR配置操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:disableAlarm	授予DMS-租户侧集群停用告警功能操作权限。	write	-	-
dws:cluster:getMonitoringViewForDMS	授予DMS-获取可用菜单操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getDatabaseUsageForDMS	授予DMS-查询DWS集群中数据库使用情况操作权限。	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
dws:cluster:listSQLProbeForDMS	授予DMS-分页查询SQL探针操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:getAlarmMetrics	授予DMS-租户侧查询告警指标操作权限。	read	-	-
dws:monitor:listMetricStatus	授予DMS-获取功能状态操作权限。	list	-	-
dws:cluster:listSessionStatusForDMS	授予DMS-查询DWS集群会话执行情况操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:downloadPerfHistoryForDMS	授予DMS-下载历史监控趋势操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:addPerfItemForDMS	授予DMS-添加监控项操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listClusterSessionForDMS	授予DMS-获取当前所有的会话操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getSQLDiagnosticsForDMS	授予DMS-查询SQL诊断详情操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateWDRSnapShotForDMS	授予DMS-更新集群WDR配置操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:clearAlarm	授予DMS-租户侧告警清除操作权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dws:cluster:executeSQLProbeForDMS	授予DMS-执行SQL探针操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listQueryStatusForDMS	授予DMS-获取查询的当前状态操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getWDRReportForDMS	授予DMS-获取报告记录操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listWLMQueueForDMS	授予DMS-查询当前的工作负载队列操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updatePerfItemForDMS	授予DMS-更新监控项操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getQueryCostForDMS	授予DMS-获取历史资源消耗操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createWDRReportForDMS	授予DMS-新增WDR报告操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:downloadWDRReportForDMS	授予DMS-WDR报告下载操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listDatabaseForDMS	授予DMS-查询当前集群所有数据库操作权限。	list	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
dws:cluster:listUserWLMQueueForDMS	授予DMS-查询用户工作负载队列操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deletePerfItemForDMS	授予DMS-删除监控项操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:getExceptionAlarmRule	授予DMS-查询异常告警规则操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getWDRHostForDMS	授予DMS-查询节点信息操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getHistoryPerfDataForDMS	授予DMS-查询历史监控数据操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteWDRReportForDMS	授予DMS-删除WDR报告操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getPerfDetailByDimensionForDMS	授予DMS-通过集群id，维度获取监控对象操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:downloadPerfHistoryByIdForDMS	授予DMS-下载历史监控趋势操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listWaitingWLMForDMS	授予DMS-获取当前等待的查询操作权限。	list	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
dws:cluster:getQueryPropertyForDMS	授予DMS-获取查询属性操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listBucketForDMS	授予DMS-获取OBS桶列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getHistoryQueryPropertyForDMS	授予DMS-获取历史查询属性操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listExceptionWLMForDMS	授予DMS-查询当前异常任务操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:terminateQueryForDMS	授予DMS-终止查询操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateTaskForDMS	授予DMS-更新任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:retryTaskForDMS	授予DMS-重试任务操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listTaskForDMS	授予DMS-任务查询操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getDatabaseOmUserStatus	授予获取运维用户状态操作权限。	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
dws:cluster:executeDatabaseOmUserAction	授予执行运维用户操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getClusterInstancesInfo	授予查询集群实例逻辑集群详情操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getMetadataSyncStatus	授予dataArts元数据同步开启状态查询操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:startMetadataSync	授予开启dataArts元数据同步操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:stopMetadataSync	授予关闭dataArts元数据同步操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updatePeriodCluster	授予更新包周期集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createPeriodCluster	授予创建包周期集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteConfigTemplate	授予删除配置模板操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getCountDown	授予获取倒计时信息操作权限。	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
dws:cluster:getObsHotStorage	授予查询存算分离集群OBS数据使用情况操作权限。	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listConfigTemplate	授予查询配置参数模板操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listDwsResource	授予获取集群实例资源列表操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listDiscountNode	授予查询折扣套餐包节点操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:changeToPeriod	授予按需转包周期操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:rotateKey	授予密钥轮转操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:operateCluster	授予集群操作，修复集群、解除只读等操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:doUpgrade	授予升级集群操作权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listUpgradePath	授予获取集群升级路径操作权限。	list	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
dws:cluster:listUpgradeRecord	授予获取集群升级记录操作权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listLogicalClusterPlans	授予查询定时增删计划权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createLogicalClusterPlan	授予添加定时增删计划权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteLogicalClusterPlan	授予删除定时增删计划权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listDatabaseUsers	授予查询所有数据库用户权限。	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:switchLogicalClusterPlan	授予启停定时增删计划权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateLogicalClusterPlan	授予编辑定时增删计划权限。	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

GaussDB(DWS)的API通常对应着一个或多个授权项。表5-89展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-89 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}/alarm-subs	dws:alarm:createSubscription	-

API	对应的授权项	依赖的授权项
DELETE /v2/{project_id}/alarm-subs/{alarm_sub_id}	dws:alarm:deleteSubscription	-
POST /v1.0/{project_id}/clusters/{cluster_id}/cns/batch-create	dws:cluster:addCN	-
PUT /v2/{project_id}/clusters/{cluster_id}/workload/queues	dws:cluster:addQueueForWLM	-
	dws:cluster:assessRisk	-
POST /v2/{project_id}/clusters/{cluster_id}/eips/{eip_id}	dws:cluster:bindEIP	-
	dws:cluster:bindOrUnbindEIP	
POST /v2/{project_id}/clusters/{cluster_id}/elbs/{elb_id}	dws:cluster:bindELB	-
	dws:cluster:bindOrUnbindELB	-
POST /v1.0/{project_id}/clusters/{cluster_id}/cancel-readonly	dws:cluster:cancelReadonly	-
GET /v2/{project_id}/disaster-recovery/check-name	dws:cluster:checkConnection	-
	dws:cluster:checkDisasterRecoveryName	-
POST /v1/{project_id}/clusters/{cluster_id}/check-instance-storage	dws:cluster:expandDisk	-
	dws:cluster:resize	-
	dws:cluster:checkRestoreTable	-
	dws:cluster:scaleIn	-

API	对应的授权项	依赖的授权项
	dws:cluster:checkSupportFineGrainedBackup	-
	dws:cluster:configureNetwork	-
POST /v1.0/{project_id}/snapshots/{snapshot_id}/linked-copy	dws:cluster:copySnapshot	-
POST /v1.0/{project_id}/clusters	dws:cluster:create	• ecs:cloudServerQuotas:get • ecs:cloudServerFlavors:get • bms:serverQuotas:get • bms:serverFlavors:get • vpc:subnets:get • vpc:vpcs:list • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:securityGroups:get • vpc:securityGroups:create • vpc:securityGroups:delete • vpc:securityGroupRules:create • vpc:securityGroupRules:delete • vpc:quotas:list • eip:publicIps:list • eip:publicIps:get • eip:publicIps:create • evs:quotas:get
POST /v2/{project_id}/clusters	dws:cluster:create	-
POST /v2/{project_id}/cluster-precheck	dws:cluster:create	-

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/clusters/{cluster_id}/dns	dws:cluster:createConnection	-
	dws:cluster:createDataSource	-
POST /v2/{project_id}/clusters/{cluster_id}/workload	dws:cluster:setFunctionStatusForWLM	-
POST /v1.0/{project_id}/snapshots	dws:cluster:createSnapshot	-
PUT /v2/{project_id}/clusters/{cluster_id}/snapshot-policies	dws:cluster:createSnapshotPolicy	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}	dws:cluster:delete	-
POST /v1.0/{project_id}/clusters/{cluster_id}/cns/batch-delete	dws:cluster:deleteCN	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/dns	dws:cluster:deleteConnection	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/ext-data-sources/{ext_data_source_id}	dws:cluster:deleteDataSource	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/clusters/{cluster_id}/nodes/delete	dws:cluster:deleteNode	-
DELETE /v1.0/{project_id}/snapshots/{snapshot_id}	dws:cluster:deleteSnapshot	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/snapshot-policies/{id}	dws:cluster:deleteSnapshotPolicy	-
DELETE /v2/{project_id}/clusters/{cluster_id}/workload/queues	dws:cluster:deleteQueueForWLM	-
POST /v1.0/{project_id}/clusters/{cluster_id}/expand-instance-storage	dws:cluster:expandDisk	-
	dws:cluster:expandWithExistedNodes	-
	dws:cluster:getAntiAffinity	-
	dws:cluster:getCnCount	-
	dws:cluster:listConfig	-
	dws:cluster:getCredential	-
GET /v1.0/{project_id}/clusters/{cluster_id}	dws:cluster:getDetail	-
GET /v2/{project_id}/disaster-recoveries	dws:cluster:getDisasterRecovery	-
	dws:cluster:getDiskExpandScope	-
	dws:cluster:getEncryptInfo	-
	dws:cluster:getHistoryConfigDetail	-
	dws:cluster:getInstanceDetail	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/disaster-recovery/{disaster_recovery_id}	dws:cluster:getDisasterRecovery	-
	dws:cluster:getInstanceDetail	-
	dws:cluster:getProcessTopo	-
	dws:cluster:getRedistribution	-
	dws::listResourceByTag	-
	dws::countResourceByTag	-
	dws:cluster:getRestoreDatabase	-
	dws:cluster:getRoachConfig	-
	dws:cluster:getSnapshotEncryptInfo	-
	dws:cluster:getSnapshotPolicy	-
	dws:cluster:getSnapshotStorage	-
	dws:cluster:getTaskDetail	-
	dws:cluster:getVolumeInfo	-
GET /v1.0/{project_id}/clusters	dws:cluster:list	-
GET /v1.0/{project_id}/clusters/{cluster_id}/audit-log-records	dws:cluster:listAuditLog	-
	dws:cluster:listBucket	-
GET /v1.0/{project_id}/clusters/{cluster_id}/cns	dws:cluster:listCN	-
GET /v1.0/{project_id}/clusters/{cluster_id}/configurations	dws:cluster:listConfig	-

API	对应的授权项	依赖的授权项
GET /v1.0/{project_id}/clusters/{cluster_id}/configurations/{configuration_id}	dws:cluster:listConfig	-
	dws:cluster:listConnection	-
	dws:cluster:listDatabase	-
GET /v1.0/{project_id}/clusters/{cluster_id}/ext-data-sources	dws:cluster:listDataSource	-
GET /v2/{project_id}/clusters/{cluster_id}/elbs	dws:cluster:listDN	-
	dws:cluster:listELB	-
	dws:cluster:listFlavorForResize	-
	dws:cluster:listFlavorForRestore	-
	dws:cluster:listHistoryConfig	-
	dws:cluster:listNode	-
	dws::listResourceByTag	-
	dws:cluster:listRing	-
GET /v1.0/{project_id}/clusters/{cluster_id}/shrink-numbers	dws:cluster:listRingForScaleIn	-
	dws:cluster:listSchema	-
	dws:cluster:listScaleInNode	-
GET /v1.0/{project_id}/clusters/{cluster_id}/snapshots	dws:cluster:listSnapshot	-
GET /v1.0/{project_id}/snapshots	dws:cluster:listSnapshot	-
GET /v1.0/{project_id}/snapshots/{snapshot_id}	dws:cluster:getSnapshotDetail	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/clusters/{cluster_id}/snapshot-policies	dws:cluster:listSnapshotPolicy	-
GET /v1.0/{project_id}/clusters/{cluster_id}/snapshots/statistics	dws:cluster:listSnapshotStatistics	-
	dws:cluster:listTable	-
GET /v2/{project_id}/clusters/{cluster_id}/workload	dws:cluster:getFunctionStatusForWLM	-
GET /v2/{project_id}/clusters/{cluster_id}/workload/queues	dws:cluster:listQueueForWLM	-
POST /v2/{project_id}/disaster-recovery/{disaster_recovery_id}/pause	dws:cluster:pauseDisasterRecovery	-
	dws:cluster:recoverRedistribution	-
POST /v2/{project_id}/clusters/{cluster_id}/redistribution	dws:cluster:redistribution	-
POST /v1.0/{project_id}/clusters/{cluster_id}/reset-password	dws:cluster:resetPassword	-
POST /v1.0/{project_id}/clusters/{cluster_id}/resize	dws:cluster:resize	-
	dws:cluster:resizeFlavor	-
	dws:cluster:resizeRetry	-

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/clusters/{cluster_id}/restart	dws:cluster:restart	-
POST /v2/{project_id}/disaster-recovery/{disaster_recovery_id}/recovery	dws:cluster:restore	-
	dws:cluster:restoreDisaster	-
POST /v1.0/{project_id}/snapshots/{snapshot_id}/actions	dws:cluster:restoreSnapshot	-
	dws:cluster:restoreTable	-
	dws:cluster:retryELBSwitch	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/maintenance-window	dws:cluster:scaleOut	-
	dws:cluster:setMaintainceWindow	-
POST /v1.0/{project_id}/clusters/{cluster_id}/cluster-shrink	dws:cluster:scaleIn	-
POST /v1/{project_id}/snapshots/{snapshot_id}/stop	dws:cluster:stopSnapshot	-
	dws:cluster:suspendRedistribution	-
POST /v1.0/{project_id}/clusters/{cluster_id}/switchover	dws:cluster:switchover	-
DELETE /v2/{project_id}/clusters/{cluster_id}/eips/{eip_id}	dws:cluster:unbindEIP	-

API	对应的授权项	依赖的授权项
DELETE /v2/{project_id}/clusters/{cluster_id}/elbs/{elb_id}	dws:cluster:unbindELB	-
PUT /v2/{project_id}/clusters/{cluster_id}/configurations/{configuration_id}	dws:cluster:updateConfig	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/dns	dws:cluster:updateConnection	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/ext-data-sources/{ext_data_source_id}	dws:cluster:updateDataSource	-
	dws:cluster:updateInstanceAliasName	-
	dws:cluster:updateRoachConfig	-
	dws:cluster:updateScheduleConfig	-
	dws:cluster:updateSnapshotPolicy	-
	dws::updateTag	-
POST /v2/{project_id}/event-subs	dws::updateTag	-
	dws:event:createSpec	-
	dws:event:createSubscription	-
DELETE /v2/{project_id}/event-subs/{event_sub_id}	dws:event:deleteSpec	-
	dws:event:deleteSubscription	-
GET /v2/{project_id}/event-subs	dws:event:listSubscription	-
	dws:event:report	-
PUT /v2/{project_id}/event-subs/{event_sub_id}	dws:event:updateSubscription	-
	dws:service:authorize	-
	dws:service:checkAuthorize	-

API	对应的授权项	依赖的授权项
	dws:service:getClusterSum	-
	dws:service:getResourceStatistics	-
	dws:service:getStorageStatistics	-
GET /v1.0/{project_id}/dss-pools	dws:service:listDssPools	-
	dws:service:listEps	-
GET /v2/{project_id}/node-types	dws:service:listSpec	-
GET /v1.0/{project_id}/statistics	dws:service:listStatistics	-
GET /v1.0/{project_id}/tags	dws::listTagsForProject	-
	dws:cluster:addOperationalTask	-
	dws:cluster:bindManageIp	-
	dws:cluster:checkAccessLts	-
	dws:cluster:checkDisasterRecoveryName	-
	dws:cluster:checkLogicalClusterData	-
	dws:cluster:closeAccessLts	-
	dws:cluster:createDisasterRecovery	-
POST /v2/{project_id}/clusters/{cluster_id}/logical-clusters	dws:cluster:createLogicalCluster	-
	dws:cluster:createApplicationForDM	-
	dws:cluster:createClusterForDM	-
	dws:cluster:createConnectionForDM	-
	dws:cluster:createMappingForDM	-
	dws:cluster:deleteApplicationForDM	-
	dws:cluster:deleteClusterForDM	-
	dws:cluster:deleteConnectionForDM	-

API	对应的授权项	依赖的授权项
	dws:cluster:deleteMappingForDM	-
	dws:cluster:dialsConnectionForDM	-
	dws:cluster:getApplicationForDM	-
	dws:cluster:listApplicationConfigForDM	-
	dws:cluster:listApplicationForDM	-
	dws:cluster:getClusterForDM	-
	dws:cluster:listClusterForDM	-
	dws:cluster:listConfigurationTemplateForDM	-
	dws:cluster:getConnectionForDM	-
	dws:cluster:listConnectionForDM	-
	dws:cluster:listDependApplicationForDM	-
	dws:cluster:getMappingForDM	-
	dws:cluster:listMappingForDM	-
	dws:cluster:listProductForDM	-
	dws:cluster:updateConnectionForDM	-
	dws:cluster:updateMappingForDM	-
	dws:cluster:startApplicationForDM	-
	dws:cluster:stopApplicationForDM	-
	dws:cluster:deleteCrossRegionSnapshotPolicy	-
	dws:cluster:deleteDisasterRecovery	-

API	对应的授权项	依赖的授权项
DELETE /v2/{project_id}/clusters/{cluster_id}/logical-clusters/{logical_cluster_id}	dws:cluster:deleteLogicalCluster	-
	dws:cluster:deleteOperationalTask	-
	dws:cluster:operateDisasterRecovery	-
PUT /v2/{project_id}/clusters/{cluster_id}/logical-clusters/{logical_cluster_id}	dws:cluster:updateLogicalCluster	-
	dws:cluster:listAllCrossRegionSnapshotConfig	-
	dws:cluster:getDisasterRecoveryProject	-
	dws:cluster:getDisasterRecoveryRegion	-
	dws:cluster:getLastOperationalTask	-
	dws:cluster:getLogicalClusterRings	-
	dws:cluster:getLogicalClusterVolume	-
	dws:cluster:getOperationalTaskConfig	-
	dws:cluster:getOperationalTaskDetail	-
	dws:cluster:getOperationalTaskStatus	-
	dws:cluster:listSnapshotRegion	-
	dws:cluster:getTargetAllCrossRegionSnapshotConfig	-
	dws:cluster:initLogicalClusterSwitch	-
	dws:cluster:listAccessLts	-
	dws:cluster:listDisasterRecovery	-
	dws:cluster:listLogicalCluster	-
	dws:cluster:listLogicalClusterTask	-
	dws:cluster:listOperationalTask	-

API	对应的授权项	依赖的授权项
	dws:cluster:openAccessLts	-
	dws:cluster:pauseOperationalTask	-
	dws:cluster:getDisasterRecoveryDetail	-
	dws:cluster:refreshOperationalTask	-
POST /v2/{project_id}/clusters/{cluster_id}/logical-clusters/{logical_cluster_id}/restart	dws:cluster:restartLogicalCluster	-
	dws:cluster:resumeOperationalTask	-
	dws:cluster:setCrossRegionSnapshotPolicy	-
	dws:cluster:startOperationalTask	-
	dws:cluster:stopOperationalTask	-
	dws:cluster:switchLogicalCluster	-
	dws:cluster:syncCrossRegionBackupClusterInfo	-
	dws:cluster:syncCrossRegionBackupConfig	-
	dws:cluster:syncCrossRegionBackupInfo	-
	dws:cluster:syncLogicalCluster	-
	dws:cluster:updateDisasterRecoveryConfig	-
	dws:cluster:updateOperationalTaskConfig	-
	dws:cluster:updateOperationalTask	-
	dws:cluster:addPlanForWLM	-
	dws:cluster:addPlanStageForWLM	-
	dws:cluster:addQueueForWLM	-
	dws:cluster:addQueueUserForWLM	-
	dws:cluster:deletePlanForWLM	-

API	对应的授权项	依赖的授权项
	dws:cluster:deletePlanStageForWLM	-
	dws:cluster:deleteQueueForWLM	-
	dws:cluster:deleteQueueUserForWLM	-
	dws:cluster:exportPlanForWLM	-
	dws:cluster:getPlanDetailForWLM	-
	dws:cluster:getPlanDetailForWLM	-
	dws:cluster:getPlanLogForWLM	-
	dws:cluster:getPlanQueueForWLM	-
	dws:cluster:getPlanStageForWLM	-
	dws:cluster:listQueueForWLM	-
	dws:cluster:getQueueDetailForWLM	-
	dws:cluster:getQueueRuleForWLM	-
	dws:cluster:importPlanForWLM	-
	dws:cluster:listPlanQueueForWLM	-
	dws:cluster:listPlanForWLM	-
	dws:cluster:listQueueUserForWLM	-
	dws:cluster:listUserForWLM	-
	dws:cluster:getClusterDBInfoForWLM	-
	dws:cluster:listClusterPlanForWLM	-
	dws:cluster:getClusterSchemaInfoForWLM	-
	dws:cluster:getClusterVersionForWLM	-
	dws:cluster:getFunctionStatusForWLM	-

API	对应的授权项	依赖的授权项
	dws:cluster:setFunctionStatusForWLM	-
	dws:cluster:startPlanForWLM	-
	dws:cluster:startPlanForWLM	-
	dws:cluster:stopPlanForWLM	-
	dws:cluster:stopPlanForWLM	-
	dws:cluster:switchPlanStageForWLM	-
	dws:cluster:switchPlanStageForWLM	-
	dws:cluster:updatePlanStageForWLM	-
	dws:cluster:updateQueueBaseForWLM	-
	dws:cluster:updateQueueResourceForWLM	-
	dws:cluster:updateQueueRuleForWLM	-
	dws:cluster:updateSchemaLimitForWLM	-
	dws:cluster:getMonitorConfigForDMS	-
	dws:monitor:listClusterOverview	-
	dws:cluster:listClusterInstanceForDMS	-
	dws:cluster:getDDLExamineDetailForDMS	-
	dws:cluster:getClusterDnStreamForDMS	-
	dws:cluster:listClusterAlarmRuleForDMS	-
	dws:cluster:getClusterInstanceForDMS	-
	dws:cluster:getDDLExamineDetailForDMS	-
	dws:cluster:getHostNetMetricsForDMS	-

API	对应的授权项	依赖的授权项
	dws:monitor:getHistoryMetrics	-
	dws:cluster:getMonitoringInfoForDMS	-
	dws:cluster:listAlarmRuleForDMS	-
	dws:cluster:updateCollectionItemForDMS	-
	dws:cluster:doDDLExamineActionForDMS	-
	dws:cluster:downloadDDLExamineDetailForDMS	-
	dws:cluster:listInstanceDiskIOForDMS	-
	dws:cluster:resetCollectionItemForDMS	-
	dws:monitor:listClusterOverview	-
	dws:monitor:listClusterOverview	-
	dws:cluster:getQueryRangeForDMS	-
	dws:monitor:getAlarmConfig	-
	dws:cluster:switchoverCollectionItemForDMS	-
	dws:monitor:listClusterOverview	-
	dws:monitor:listClusterOverview	-
	dws:monitor:getOSMetrics	-
	dws:cluster:listPerfDashboardForDMS	-
	dws:cluster:disableCollectionItemForDMS	-
	dws:monitor:listClusterOverview	-
	dws:monitor:getAggregationOSMetrics	-
	dws:cluster:terminateSessionForDMS	-
	dws:cluster:getPerfDashboardDetailForDMS	-

API	对应的授权项	依赖的授权项
	dws:monitor:createAlarmRule	-
	dws:cluster:enableCollectionItemForDMS	-
	dws:monitor:listClusterOverview	-
	dws:cluster:listInstanceNetworkMetricsForDMS	-
	dws:cluster:createPerfDashboardForDMS	-
	dws:cluster:getMonitorMetricsForDMS	-
	dws:monitor:listClusterOverview	-
	dws:cluster:createSQLProbeForDMS	-
	dws:cluster:listInstanceIOStatusForDMS	-
	dws:cluster:getMonitorMetricsByDimensionForDMS	-
	dws:cluster:updateStorageConfigForDMS	-
	dws:monitor:listClusterOverview	-
	dws:monitor:updateAlarmRule	-
	dws:cluster:getInstanceIOAggResultForDMS	-
	dws:cluster:updatePerfDashboardForDMS	-
	dws:cluster:getMonitorHistoryMetricsCost	-
	dws:monitor:deleteAlarmRule	-
	dws:cluster:updateSQLProbeForDMS	-
	dws:cluster:startMonitorMetricsCollectionForDMS	-
	dws:cluster:listInstanceStorageForDMS	-
	dws:cluster:deletePerfDashboardForDMS	-

API	对应的授权项	依赖的授权项
	dws:cluster:getMonitorMetricsDetailForDMS	-
	dws:cluster:deleteSQLProbeForDMS	-
	dws:monitor:stopAlarmRule	-
	dws:cluster:stopMonitorMetricsCollectionForDMS	-
	dws:cluster:listExceptionTableForDMS	-
	dws:cluster:getInstanceStorageAggForDMS	-
	dws:cluster:getWDRSnapShotForDMS	-
	dws:cluster:getPerfMetricsDataForDMS	-
	dws:cluster:listQueryForDMS	-
	dws:cluster:getInstanceIOMetricsForDMS	-
	dws:cluster:getSQLProbeDetailForDMS	-
	dws:cluster:switchoverMonitorMetricStatusForDMS	-
	dws:monitor:startAlarmRule	-
	dws:monitor:getClusterStatus	-
	dws:cluster:getPerfMetricsDetailForDMS	-
	dws:cluster:listSlowInstanceForDMS	-
	dws:cluster:getDDLExamineConfigForDMS	-
	dws:cluster:getMonitoringViewStatusForDMS	-
	dws:monitor:enableAlarm	-
	dws:cluster:createWDRSnapShotForDMS	-
	dws:cluster:listExecuteStatusForDMS	-

API	对应的授权项	依赖的授权项
	dws:cluster:listQueryForDMS	-
	dws:cluster:getSlowInstanceDetailForDMS	-
	dws:cluster:enableSQLProbeForDMS	-
	dws:cluster:getWDRConfigForDMS	-
	dws:monitor:disableAlarm	-
	dws:cluster:getMonitoringViewForDMS	-
	dws:cluster:createWDRSnapShotForDMS	-
	dws:cluster:getDatabaseUsageForDMS	-
	dws:cluster:listSQLProbeForDMS	-
	dws:monitor:getAlarmMetrics	-
	dws:monitor:listMetricStatus	-
	dws:cluster:listSessionStatusForDMS	-
	dws:cluster:downloadPerfHistoryForDMS	-
	dws:cluster:addPerfItemForDMS	-
	dws:cluster:listClusterSessionForDMS	-
	dws:cluster:getSQLDiagnosticsForDMS	-
	dws:cluster:updateWDRSnapShotForDMS	-
	dws:monitor:clearAlarm	-
	dws:cluster:executeSQLProbeForDMS	-
	dws:cluster:listQueryStatusForDMS	-
	dws:cluster:getWDRReportForDMS	-

API	对应的授权项	依赖的授权项
	dws:cluster:listWLMQueueForDMS	-
	dws:cluster:updatePerfItemForDMS	-
	dws:cluster:executeSQLProbeForDMS	-
	dws:cluster:getQueryCostForDMS	-
	dws:cluster:createWDRReportForDMS	-
	dws:cluster:downloadWDRReportForDMS	-
	dws:cluster:listDatabaseForDMS	-
	dws:cluster:listUserWLMQueueForDMS	-
	dws:cluster:deletePerfItemForDMS	-
	dws:cluster:createWDRReportForDMS	-
	dws:cluster:getQueryCostForDMS	-
	dws:monitor:getExceptionAlarmRule	-
	dws:cluster:getWDRHostForDMS	-
	dws:cluster:getHistoryPerfDataForDMS	-
	dws:cluster:deleteWDRReportForDMS	-
	dws:cluster:getQueryCostForDMS	-
	dws:cluster:getPerfDetailByDimensionForDMS	-
	dws:cluster:downloadPerfHistoryByIdForDMS	-
	dws:cluster:listWaitingWLMForDMS	-
	dws:cluster:downloadWDRReportForDMS	-
	dws:cluster:getQueryPropertyForDMS	-

API	对应的授权项	依赖的授权项
	dws:cluster:listBucketForDMS	-
	dws:cluster:getHistoryQueryPropertyForDMS	-
	dws:cluster:listExceptionWLMForDMS	-
	dws:cluster:addPerfItemForDMS	-
	dws:cluster:terminateQueryForDMS	-
	dws:cluster:updateTaskForDMS	-
	dws:cluster:retryTaskForDMS	-
	dws:cluster:listTaskForDMS	-
GET /v1/{project_id}/clusters/{cluster_id}/db-manager/om-user/status	dws:cluster:getDatabaseOmUserStatus	-
POST /v1/{project_id}/clusters/{cluster_id}/db-manager/om-user/action	dws:cluster:executeDatabaseOmUserAction	-
GET /v2/{project_id}/clusters/{cluster_id}/instances	dws:cluster:getClusterInstancesInfo	-
	dws:cluster:getMetadataSyncStatus	-
	dws:cluster:startMetadataSync	-
	dws:cluster:stopMetadataSync	-
	dws:cluster:updatePeriodCluster	-
	dws:cluster:createPeriodCluster	-
	dws:cluster:deleteConfigTemplate	-
	dws:cluster:getCountDown	-
	dws:cluster:getObsHotStorage	-
	dws:cluster:listConfigTemplate	-

API	对应的授权项	依赖的授权项
	dws:cluster:listDwsResource	-
	dws:cluster:listDiscountNode	-
	dws:cluster:changeToPeriod	-
	dws:cluster:rotateKey	-
	dws:cluster:operateCluster	-
	dws:cluster:setMaintainceWindow	-
	dws:cluster:doUpgrade	-
	dws:cluster:listUpgradePath	-
	dws:cluster:listUpgradeRecord	-
	dws:cluster:delete	-
GET /v1/{project_id}/clusters/{cluster_id}/db-manager/objects	dws:cluster:getDatabaseObjects	-
	dws:cluster:listLogicalClusterPlans	-
	dws:cluster:createLogicalClusterPlan	-
	dws:cluster:deleteLogicalClusterPlan	-
	dws:cluster:listDatabaseUsers	-
	dws:cluster:switchLogicalClusterPlan	-
	dws:cluster:updateLogicalClusterPlan	-
	dws:cluster:getAccessWhitelistStatus	-
POST /v1/{project_id}/clusters/{cluster_id}/access-whitelist	dws:cluster:addAccessWhitelist	-
	dws:cluster:getAccessWhitelist	-

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/clusters/{cluster_id}/access-whitelist/{whitelist_id}	dws:cluster:getAccessWhitelistDetail	-
	dws:cluster:setAccessWhitelistDetail	-
DELETE /v2/{project_id}/clusters/{cluster_id}	dws:cluster:delete	-

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。

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

表 5-90 GaussDB(DWS)支持的资源类型

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

条件（Condition）

GaussDB(DWS)服务不支持在SCP中的条件键中配置服务级的条件键。

GaussDB(DWS)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。

5.10.5.4 MapReduce 服务 MRS

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MapReduce服务（MRS）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MapReduce服务（MRS）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MapReduce服务（MRS）的相关操作。

表 5-91 MapReduce 服务（MRS）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
mrs:cluster:createCluster	授予权限以创建集群。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:RequestTag/<tag-key>,g:TagKeys,g:EnterpriseProjectId
mrs:cluster:deleteCluster	授予权限以删除集群。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:listHosts	授予权限以查询集群中的节点。	list	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:listFiles	授予权限以查询集群中的文件列表。	list	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
mrs:cluster:createJob	授予权限以在集群中执行作业。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:list	授予权限以查询集群列表。	list	-	g:RequestTag/<tag-key>,g:TagKeys,g:EnterpriseProjectId
mrs:cluster:listJobs	授予权限以查询集群的作业列表。	list	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:getJob	授予权限以查询集群的作业详情。	read	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:getCluster	授予权限以查询集群详情。	read	mrs:<region>:<account-id>:cluster:<cluster-id>	-
mrs:cluster:resizeNodes	授予权限以调整集群节点。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:updateClusterName	授予权限以重命名集群。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:listTags	授予权限以查询集群标签。	list	-	g:EnterpriseProjectId
mrs:cluster:updateTags	授予权限以增删集群标签。	tagging	-	g:RequestTag/<tag-key>,g:TagKeys,g:EnterpriseProjectId
mrs:cluster:listClustersByTag	授予权限以查询特定标签的集群列表。	list	-	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
mrs:cluster:stopJob	授予权限以停止集群作业。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:deleteJobs	授予权限以批量删除集群作业。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:stopSql	授予权限以取消sql执行。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:createSql	授予权限以提交sql执行。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:listPolicies	授予权限以获取集群内所有的弹性伸缩策略。	list	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:updatePolicies	授予权限以修改集群的弹性伸缩策略。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:getAgencyMapping	授予权限以获取用户代理信息。	read	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:updateAgencyMapping	授予权限以更新用户代理信息。	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:getSql	授予权限以获取sql执行结果。	read	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId

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。

MapReduce服务（MRS）定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-92 MapReduce 服务（MRS）支持的资源类型

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

条件（Condition）

MRS服务不支持在SCP中的条件键中配置服务级的条件键。

MRS服务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。

5.10.5.5 云搜索服务 CSS

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CSS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CSS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CSS的相关操作。

表 5-93 CSS 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
css:VPCEndpoint:updateWhitelist	授予权限更新已存在的终端节点白名单。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:log:updateBackupPolicy	授予权限日志备份修改或删除。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:setSnapshotPolicy	授予权限操作备份策略。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:getSnapshotPolicy	授予权限查询备份策略。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:restore	授予权限恢复快照。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:create	授予权限创建快照。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:publicIPAddress:associates	授予权限开启或关闭公网访问。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:publicIPAddress:setAccessControl	授予权限对白名单列表进行操作。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:tag:get	授予权限查询资源标签。	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
css:publicIPAddress:modifyBandwidth	授予权限修改带宽大小。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:VPCEndpoint:enableOrDisable	授予权限创建或删除VPCEP。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:log:getBasicConfigurations	授予权限日志基础配置查询。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:list	授予权限查看快照列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:log:list	授予权限查看日志。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:setSnapshotContiguration	授予权限设置快照基础配置。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:listFlavors	授予权限查询规格ID列表。	list	-	-
css:cluster:listDiskType	授予权限列举可用磁盘类型。	list	-	-
css:tag:list	授予权限查询项目标签。	list	cluster *	-
css:VPCEndpoint:manageConnection	授予权限操作终端节点的连接。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:log:listJob	授予权限查询作业列表。	list	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
css:cluster:downloadCert	授予权限获取证书内容。	read	-	-
css:cluster:get	授予权限查询集群详情。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:enableAtomaticSnapsot	授予权限设置快照自动备份的基础配置。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:delete	授予权限删除指定快照。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:IKThesaurus:get	授予权限查看自定义词库配置。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:restart	授予权限重启ElasticSearch集群。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:modifySecurityGroup	授予权限修改集群安全组。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:configurations:list	授予权限查询获取参数配置的任务操作列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:delete	授予权限删除集群。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:modifySpecifications	授予权限修改集群规格。	write	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
css:cluster:list	授予权限列举集群信息。	list	cluster *	-
css:cluster:scaleOut	授予权限扩容集群。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:IKThesaurus:load	授予权限加载自定义词库。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:configurations:modify	授予权限更新参数配置。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:configurations:get	授予权限列举参数配置列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:IKThesaurus:delete	授予权限删除词库。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:expand	授予权限扩容实例的数量和存储容量。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:disableSnapshotFuction	授予权限关闭集群快照功能。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:upgradeCluster	授予权限升级集群或节点替换。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:VPCEndpoint:listConnection	授予权限查询VPCEP的连接。	list	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
css:cluster:scaleIn	授予权限对集群缩容。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:log:setBasicConfigurations	授予权限日志基础配置设置。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:tag:addOrDelete	授予权限批量添加删除资源标签。	tagging	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
css:publicKibana:close	授予权限关闭公网访问。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:tag:edit	授予权限修改集群标签。	tagging	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
css:cluster:create	授予权限创建集群。	write	cluster *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
css:cluster:toPeriod	授予权限对集群转包周期。	write	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
css:cluster:modifyName	授予权限修改集群名称。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:log:backup	授予权限对日志备份。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:closeLogSetting	授予权限关闭日志功能。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:openLogSetting	授予权限开启日志功能。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:modifyPassword	授予权限修改集群密码。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:publicIPAddress:disassociates	授予权限解绑公网。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:publicKibana:open	授予权限绑定公网。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:tag:delete	授予权限删除标签。	tagging	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	g:TagKeys
css:cluster:shrinkNodes	授予权限指定节点缩容。	write	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
css:cluster:changeMode	授予权限修改安全模式。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:addIndependenceNodes	授予权限添加独立master,client。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:rollingReboot	授予权限滚动重启ElasticSearch集群。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:listActions	授予权限查询操作记录。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:uploadCerts	授予权限上传证书。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:deleteCerts	授予权限删除证书。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:listCerts	授予权限查询证书列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:getCertsDetail	授予权限查询证书详情。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:deleteConfTemplate	授予权限删除自定义模板。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:listConfigTemplate	授予权限查询模板列表。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
css:logstash:confStop	授予权限停止或热停止pipeline迁移数据。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:checkConnection	授予权限连通性测试。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:confDelete	授予权限删除配置文件。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:confStart	授予权限启动或热启动pipeline迁移数据。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:getConfDetail	授予权限用于查询配置文件内容。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:azmigrate	授予权限进行可用区切换。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:confUpdate	授予权限更新配置文件。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:listPipelines	授予权限查询pipeline列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:retryAction	授予权限重试该任务或终止该任务的影响。	write	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
css:logstash:listConfs	授予权限查询配置文件列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:configFavorites	授予权限添加到自定义模板。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:listUpgradeCluster	授予权限获取升级镜像id及升级详情。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:submitConf	授予权限创建配置文件。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:plugin:list	授予权限查询集群插件列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:plugin:getOperationRecords	授予权限查询插件的操作记录。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:plugin:delete	授予权限删除插件。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:plugin:installOrUninstall	授予权限安装或卸载插件。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:plugin:upload	授予权限上传插件。	write	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
css:plugin:getDefault	授予权限查询默认插件。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:getAgencies	授予权限获取代理。	read	-	-
css:cluster:modifyRoute	授予权限修改集群路由。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:getRoutes	授予权限获取集群路由。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:actionList	授予权限查询集群任务列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:createUserInfo	授予权限查创建用户信息。	write	cluster *	-
css:VPCEndpoint:modifyConnections	授予权限修改连接大小。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:queryNeedDeleteInstances	授予权限查询需要删除的节点。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:queryKey	授予权限获得密钥。	read	-	-
css:cluster:queryKeys	授予权限获得密钥列表。	list	-	-
css:cluster:getPubliczonePice	授予权限获取带宽价格。	read	cluster *	-
css:datastore:get	授予权限获取数据引擎。	read	cluster *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
css:datastore:list	授予权限获取数据引擎列表。	list	cluster *	-
css:cluster:getDiskUsage	授予权限获取集群存储容量状态。	read	cluster *	-
css:snapshot:showDetail	授予权限获得快照详情。	read	cluster *	-
css:cluster:getAvailableBuckets	授予权限获取可用OBS桶。	list	-	-
css:cluster:checkCssName	授予权限检查集群名称。	write	cluster *	-
css:snapshot:deleteAllFailedTask	授予权限删除所有的失败任务。	write	-	-
css:snapshot:deleteSingleFailedTask	授予权限删除指定失败任务。	write	-	-
css:snapshot:getAllFailedTask	授予权限查看备份失败任务。	list	-	-
css::createServiceAgency	授予权限创建委托。	write	-	-
css:cluster:createAiOps	授予权限创建检测任务。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:listAiOps	授予权限获取检测任务列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:deleteAiOps	授予权限删除检测任务。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:listSmnTopics	授予权限获取SMN主题列表。	list	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
css:cluster:listElbs	授予权限下获取当前集群可用的负载均衡器列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:elbSwitch	授予权限打开或关闭负载均衡功能。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:createElbListener	授予权限为当前集群创建监听器。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:updateElbListener	授予权限修改当前集群的监听器。	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:getElbDetail	授予权限查询当前集群使用的负载均衡器信息。	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:listElbCerts	授予权限获取负载均衡器证书列表。	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

CSS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
POST /v1.0/{project_id}/clusters	css:cluster:create	• ecs:cloudServerFlavors:get • evs:types:get • vpc:vpcs:list • vpc:securityGroups:list • vpc:securityGroups:get • vpc:subnets:list • vpc:subnets:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:ports:get • css:cluster:getAgencies • iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject • iam:agencies:pass

API	对应的授权项	依赖的授权项
POST /v2.0/{project_id}/clusters	css:cluster:create	• ecs:cloudServerFlavors:get • evs:types:get • vpc:vpcs:list • vpc:securityGroups:list • vpc:securityGroups:get • vpc:subnets:list • vpc:subnets:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:ports:get • css:cluster:getAgencies • iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject • iam:agencies:pass
POST /v1.0/{project_id}/clusters/{cluster_id}/sg/change	css:cluster:modifySecurityGroup	• vpc:securityGroups:list • vpc:ports:update
GET /v1.0/{project_id}/clusters	css:cluster:list	-
GET /v1.0/{project_id}/clusters/{cluster_id}	css:cluster:get	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}	css:cluster:delete	-
POST /v1.0/{project_id}/cluster/{cluster_id}/period	css:cluster:toPeriod	-
POST /v1.0/{project_id}/clusters/{cluster_id}/changename	css:cluster:modifyName	-

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/clusters/{cluster_id}/password/reset	css:cluster:modifyPassword	-
POST /v1.0/{project_id}/clusters/{cluster_id}/restart	css:cluster:restart	-
POST /v2.0/{project_id}/clusters/{cluster_id}/restart	css:cluster:restart	-
POST /v1.0/{project_id}/clusters/{cluster_id}/extend	css:cluster:scaleOut	• ecs:cloudServerFlavors:get • evs:types:get • vpc:vpcs:list • vpc:subnets:list • vpc:subnets:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:ports:get
POST /v1.0/{project_id}/clusters/{cluster_id}/role_extend	css:cluster:expand	• ecs:cloudServerFlavors:get • evs:types:get • vpc:vpcs:list • vpc:subnets:list • vpc:subnets:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:ports:get
POST /v1.0/{project_id}/clusters/{cluster_id}/flavor	css:cluster:modifySpecifications	ecs:cloudServerFlavors:get
GET /v1.0/{project_id}/es-flavors	css:cluster:listFlavors	ecs:cloudServerFlavors:get

API	对应的授权项	依赖的授权项
GET /v1.0/{project_id}/{resource_type}/tags	css:tag:list	-
GET /v1.0/{project_id}/{resource_type}/{cluster_id}/tags	css:tag:get	-
POST /v1.0/{project_id}/{resource_type}/{cluster_id}/tags	css:tag:edit	-
DELETE /v1.0/{project_id}/{resource_type}/{cluster_id}/tags/{key}	css:tag:delete	-
POST /v1.0/{project_id}/{resource_type}/{cluster_id}/tags/action	css:tag:addOrDelete	-
POST /v1.0/{project_id}/clusters/{cluster_id}/{types}/flavor	css:cluster:modifySpecifications	ecs:cloudServerFlavors:get
POST /v1.0/extend/{project_id}/clusters/{cluster_id}/role/shrink	css:cluster:scaleIn	• iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject
GET /v1.0/{project_id}/cer/download	css:cluster:downloadCert	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/instance/{instance_id}/replace	css:cluster:upgradeCluster	• iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/clusters/{cluster_id}/node/offline	css:cluster:shrinkNodes	• iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject
POST /v1.0/{project_id}/clusters/{cluster_id}/mode/change	css:cluster:changeMode	-
POST /v1.0/{project_id}/clusters/{cluster_id}/type/{type}/independent	css:cluster:addIndependenceNodes	• ecs:cloudServerFlavors:get • evs:types:get • vpc:vpcs:list • vpc:subnets:list • vpc:subnets:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:ports:get
POST /v1.0/{project_id}/clusters/{cluster_id}/inst-type/{inst_type}/image/upgrade	css:cluster:upgradeCluster	-
POST /v1.0/{project_id}/clusters/{cluster_id}/inst-type/{inst_type}/azmigrate	css:cluster:azmigrate	• iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject
GET /v1.0/{project_id}/clusters/{cluster_id}/upgrade/detail	css:cluster:listUpgradeCluster	-

API	对应的授权项	依赖的授权项
GET /v1.0/{project_id}/clusters/{cluster_id}/target/{upgrade_type}/images	css:cluster:listUpgradeCluster	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/upgrade/{action_id}/retry	css:cluster:retryAction	-
POST /v1.0/{project_id}/clusters/{cluster_id}/thesaurus	css:IKThesaurus:load	• obs:bucket:listAllMyBuckets • obs:bucket:getBucketLocation • obs:bucket:getBucketStoragePolicy • obs:object:getObject
GET /v1.0/{project_id}/clusters/{cluster_id}/thesaurus	css:IKThesaurus:get	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/thesaurus	css:IKThesaurus:delete	-
POST /v1.0/{project_id}/clusters/{cluster_id}/publickibana/open	css:publicKibana:open	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/publickibana/close	css:publicKibana:close	-

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/clusters/{cluster_id}/publickibana/bandwidth	css:publicIPAddress:modifyBandwidth	-
POST /v1.0/{project_id}/clusters/{cluster_id}/publickibana/whitelist/update	css:publicIPAddress:setAccessControl	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/publickibana/whitelist/close	css:publicIPAddress:setAccessControl	-
POST /v1.0/{project_id}/clusters/{cluster_id}/logs/open	css:cluster:openLogSetting	• iam:agencies:pass • obs:bucket:listAllMyBuckets • obs:bucket:getBucketLocation • obs:bucket:getBucketStoragePolicy • iam:agencies:listAgencies
PUT /v1.0/{project_id}/clusters/{cluster_id}/logs/close	css:cluster:closeLogSetting	-
GET /v1.0/{project_id}/clusters/{cluster_id}/logs/records	css:log:listJob	-
GET /v1.0/{project_id}/clusters/{cluster_id}/logs/settings	css:log:getBasicConfigurations	-

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/clusters/{cluster_id}/logs/settings	css:log:setBasicConfigurations	• obs:bucket:listAllMyBuckets • obs:bucket:getBucketLocation • obs:bucket:getBucketStoragePolicy • iam:agencies:listAgencies • iam:agencies:pass
POST /v1.0/{project_id}/clusters/{cluster_id}/logs/policy/update	css:log:updateBackupPolicy	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/logs/policy/close	css:log:updateBackupPolicy	-
POST /v1.0/{project_id}/clusters/{cluster_id}/logs/collect	css:log:backup	-
POST /v1.0/{project_id}/clusters/{cluster_id}/logs/search	css:log:list	-
POST /v1.0/{project_id}/clusters/{cluster_id}/public/open	css:publicIPAddress:associates	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/public/close	css:publicIPAddress:disassociates	-
POST /v1.0/{project_id}/clusters/{cluster_id}/public/bandwidth	css:publicIPAddress:modifyBandwidth	-

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/clusters/{cluster_id}/public/whitelist/update	css:publicIPAddress:setAccessControl	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/public/whitelist/close	css:publicIPAddress:setAccessControl	-
POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/auto_setting	css:snapshot:enableAtomaticSnapsot	• obs:bucket:createBucket • obs:bucket:headBucket • iam:agencies:listAgencies • iam:agencies:createAgency • iam:permissions:grantRoleToAgency
POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/setting	css:snapshot:setSnapshotContiguration	• obs:bucket:listAllMyBuckets • obs:bucket:getBucketLocation • obs:bucket:getBucketStoragePolicy • iam:agencies:listAgencies • iam:agencies:pass
POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot	css:snapshot:create	iam:agencies:pass
POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/{snapshot_id}/restore	css:snapshot:restore	-

API	对应的授权项	依赖的授权项
DELETE /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/{snapshot_id}	css:snapshot:delete	-
POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/policy	css:snapshot:setSnapshotPolicy	-
GET /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/policy	css:snapshot:getSnapshotPolicy	-
GET /v1.0/{project_id}/clusters/{cluster_id}/index_snapshots	css:snapshot:list	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/index_snapshots	css:snapshot:disableSnapshotFuction	-
POST /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/open	css:VPCEndpoint:enableOrDisable	• vpcep:endpoints:create • vpcep:endpoints:list • vpcep:endpoints:get • vpcep:endpoints:delete • vpcep:endpoints:update
PUT /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/close	css:VPCEndpoint:enableOrDisable	• vpcep::listQuotas • vpcep:endpoints:create • vpcep:endpoints:list • vpcep:endpoints:get • vpcep:endpoints:delete • vpcep:endpoints:update

API	对应的授权项	依赖的授权项
GET /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/connections	css:VPCEndpoint:listConnection	vpcep:endpoints:get
POST /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/connections	css:VPCEndpoint:manageConnection	-
POST /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/permissions	css:VPCEndpoint:updateWhitelist	-
POST /v1.0/{project_id}/clusters/{cluster_id}/ymls/update	css:configurations:modify	-
GET /v1.0/{project_id}/clusters/{cluster_id}/ymls/joblists	css:configurations:list	-
GET /v1.0/{project_id}/clusters/{cluster_id}/ymls/template	css:configurations:get	-
POST /v2.0/{project_id}/clusters/{cluster_id}/snapshots/policy/open	css:snapshot:setSnapshotPolicy	-
PUT /v2.0/{project_id}/clusters/{cluster_id}/snapshots/policy/close	css:snapshot:setSnapshotPolicy	-

API	对应的授权项	依赖的授权项
POST /v2.0/{project_id}/clusters/{cluster_id}/rolling_restart	css:cluster:rollingReboot	-
GET /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/listactions	css:logstash:listActions	-
DELETE /v1.0/{project_id}/lgsconf/deletetemplate	css:logstash:deleteConfTemplate	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/stop	css:logstash:confStop	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/hot-stop	css:logstash:confStop	-
POST /v1.0/{project_id}/clusters/{cluster_id}/checkconnection	css:logstash:checkConnection	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/delete	css:logstash:confDelete	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/start	css:logstash:confStart	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/hot-start	css:logstash:confStart	-

API	对应的授权项	依赖的授权项
GET /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/confdetail	css:logstash:getConfDetail	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/update	css:logstash:confUpdate	-
GET /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/listpipelines	css:logstash:listPipelines	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/submit	css:logstash:submitConf	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/favorite	css:logstash:configFavorites	-
GET /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/listconfs	css:logstash:listConfs	-
GET /v1.0/{project_id}/lgsconf/template	css:logstash:listConfigTemplate	-
POST /v1.0/{project_id}/clusters/{cluster_id}/certs/upload	css:cluster:uploadCerts	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/certs/{cert_id}/delete	css:cluster:deleteCerts	-

API	对应的授权项	依赖的授权项
GET /v1.0/{project_id}/clusters/{cluster_id}/certs	css:cluster:listCerts	-
GET /v1.0/{project_id}/clusters/{cluster_id}/certs/{cert_id}	css:cluster:getCertsDetail	-
POST /v1.0/{project_id}/clusters/{cluster_id}/route	css:cluster:modifyRoute	-
GET /v1.0/{project_id}/clusters/{cluster_id}/route	css:cluster:getRoutes	-
POST /v1.0/{project_id}/clusters/{cluster_id}/ai-ops	css:cluster:createAiOps	-
GET /v1.0/{project_id}/clusters/{cluster_id}/ai-ops	css:cluster:listAiOps	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/ai-ops/{aiops_id}	css:cluster:deleteAiOps	-
GET /v1.0/{project_id}/domains/{domain_id}/ai-ops/smn-topics	css:cluster:listSmnTopics	• css:cluster:getAgencies • iam:agencies:list • iam:agencies:listAgencies • iam:agencies:listAttachedPolicies • iam:agencies:pass
GET /v1.0/{project_id}/clusters/{cluster_id}/loadbalancers	css:cluster:listElbs	elb:loadbalancers:list

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/clusters/{cluster_id}/loadbalancers/es-switch	css:cluster:elbSwitch	• elb:loadbalancers:list • iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject • iam:agencies:pass
POST /v1.0/{project_id}/clusters/{cluster_id}/es-listeners	css:cluster:createElbListener	-
GET /v1.0/{project_id}/clusters/{cluster_id}/es-listeners	css:cluster:getElbDetail	-
GET /v1.0/{project_id}/clusters/{cluster_id}/elb/certificates	css:cluster:listElbCerts	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/es-listeners/{listener_id}	css:cluster:updateElbListener	-

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。

CSS定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-95 CSS 支持的资源类型

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

条件（Condition）

条件键概述

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css:）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。

CSS支持的服务级条件键

CSS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 5-96 CSS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
css:AssociatePublicIp	boolean	单值	是否允许实例开启公网访问。

条件键示例

- css:AssociatePublicIp

  示例：禁止创建带EIP的CSS集群

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "css:cluster:create"
      ],
      "Condition": {
        "Bool": {
          "css:AssociatePublicIp": [
            "true"
          ]
        }
      }
    }
  ]
}
```

  示例：禁止给CSS集群绑定EIP

```
{
 "Version": "5.0",
 "Statement": [
  {
   "Effect": "Deny",
   "Action": [
    "css:publicIPAddress:associates",
    "css:publicKibana:open"
   ]
  }
 ]
}
```

5.10.6 CDN 与智能边缘

5.10.6.1 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 5-97 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
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

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:configuration:queryDomainList	授予权限查询域名信息列表。	list	domain *	g:EnterpriseProjectId
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
cdn:configuration:queryReferConf	授予权限查询refer白名单配置。	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
cdn:configuration:batchModifyHttpsConf	授予权限批量修改域名证书配置。	write	domain *	g:EnterpriseProjectId
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5-98**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 /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5-99**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 5-99 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。

5.10.7 数据库

5.10.7.1 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 5-100 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5-101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 /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。

RDS定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-102 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5-103。
  - 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 5-103 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。

5.10.7.2 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 5-104 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5-105**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-105 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5-106**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 5-106 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5-107。
  - 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 5-107 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。

5.10.7.3 云数据库 GaussDB

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GaussDB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GaussDB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GaussDB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GaussDB的相关操作。

表 5-108 GaussDB 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
gaussdb:backup:createBackup	授予创建数据库实例手动备份的权限。	write	instance	-
gaussdb:backup:deleteBackup	授予删除备份的权限。	write	instance	-
gaussdb:backup:listAll	授予查询备份列表的权限。	list	instance	-
gaussdb:instance:updateBackupPolicy	授予设置备份策略的权限。	write	instance	gaussdb:BackupEnabled
gaussdb:param:applyParam	授予应用参数模板的权限。	write	instance	-
gaussdb:tag:create	授予添加资源标签的权限。	tagging	instance	-
gaussdb:instance:bindEIP	授予绑定弹性公网IP的权限。	write	instance	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
gaussdb:instance:check	授予校验实例相关信息的权限。	read	instance	-
gaussdb:instance:createInstance	授予创建数据库实例的权限。	write	instance	• gaussdb:BackupEnabled • gaussdb:Encrypted
gaussdb:instance:createDatabase	授予创建数据库的权限。	write	instance	-
gaussdb:instance:createDatabaseSchema	授予创建数据库Schema的权限。	write	instance	-
gaussdb:instance:createDatabaseUser	授予创建数据库用户的权限。	write	instance	-
gaussdb:instance:deleteInstance	授予删除数据库实例的权限。	write	instance	-
gaussdb:instance:get	授予查询实例详情的权限。	read	instance	-
gaussdb:instance:getBackupPolicy	授予查询自动备份策略的权限。	read	instance	-
gaussdb:instance:getBalanceStatus	授予查询实例主备平衡状态的权限。	read	instance	-
gaussdb:instance:getDiskUsage	授予查询磁盘使用率的权限。	read	instance	-
gaussdb:instance:getRecyclePolicy	授予查看实例回收备份策略的权限。	read	instance	-
gaussdb:instance:downloadSslCert	授予下载实例SSL证书的权限。	read	instance	-
gaussdb:instance:grantDatabasePrivilege	授予授权数据库账号的权限。	write	instance	-
gaussdb:instance:listAll	授予查询数据库实例列表的权限。	list	instance	-
gaussdb:instance:listPublicIps	授予查询实例已绑定EIP列表的权限。	list	instance	-
gaussdb:instance:listComponents	授予查询实例组件列表的权限。	list	instance	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
gaussdb:instance:listDatabases	授予查询数据库列表的权限。	list	instance	-
gaussdb:instance:listDatabaseUsers	授予查询数据库用户列表的权限。	list	instance	-
gaussdb:tag:listAll	授予查询资源标签列表的权限。	list	instance	-
gaussdb:quota:listAll	授予查询配额列表的权限。	list	instance	-
gaussdb:instance:listRecoverableTimes	授予查询备份可恢复时间段的权限。	list	instance	-
gaussdb:instance:listSchemas	授予查询数据库Schema列表的权限。	list	instance	-
gaussdb:instance:renameInstance	授予重置实例名称的权限。	write	instance	-
gaussdb:instance:resetPassword	授予重置数据库密码的权限。	write	instance	-
gaussdb:instance:resizeFlavor	授予变更实例规格的权限。	write	instance	-
gaussdb:instance:restartInstance	授予重启数据库实例的权限。	write	instance	-
gaussdb:instance:setRecyclePolicy	授予设置实例回收备份策略的权限。	write	instance	-
gaussdb:instance:switchShard	授予分片节点主备切换的权限。	write	instance	-
gaussdb:instance:extend	授予扩容相关操作的权限。	write	instance	-
gaussdb:param:update	授予修改参数组的权限。	write	instance	-
gaussdb:param:check	授予校验参数组的权限。	read	instance	-
gaussdb:param:copy	授予复制参数模板的权限。	write	instance	-
gaussdb:param:createParam	授予创建参数组的权限。	write	instance	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
gaussdb:param:deleteParam	授予删除参数组的权限。	write	instance	-
gaussdb:param:get	授予查询参数配置详情的权限。	read	instance	-
gaussdb:param:compare	授予比较两个参数模板之间差异的权限。	read	instance	-
gaussdb:param:listAll	授予查询参数组列表的权限。	list	instance	-
gaussdb:param:reset	授予重置参数模板的权限。	write	instance	-
gaussdb:quota:update	授予修改配额的权限。	write	instance	-
gaussdb:task:listAll	授予查询任务列表的权限。	list	instance	-
gaussdb:task:delete	授予删除任务记录的权限。	write	instance	-
gaussdb:task:get	授予查询任务详情的权限。	read	instance	-

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

表 5-109 实例管理

权限	API	对应的授权项	依赖的授权项
创建数据库实例	POST /v3/{project_id}/instances	gaussdb:instance:createInstance	-
删除数据库实例	DELETE /v3/{project_id}/instances/{instance_id}	gaussdb:instance:delete	-
查询数据库实例列表	GET /v3/{project_id}/instances	gaussdb:instance:listAll	-

权限	API	对应的授权项	依赖的授权项
重置数据库密码	POST /v3/{project_id}/instances/{instance_id}/password	gaussdb:instance:resetPassword	-
修改实例名称	PUT /v3/{project_id}/instances/{instance_id}/name	gaussdb:instance:rename	-
重启数据库实例	POST /v3/{project_id}/instances/{instance_id}/restart	gaussdb:instance:restart	-
分片节点主备切换	POST /v3/{project_id}/instances/{instance_id}/switch-shard	gaussdb:instance:switchShard	-
查询实例的组件列表	GET /v3/{project_id}/instances/{instance_id}/components	gaussdb:instance:listComponents	-
规格变更	PUT /v3/{project_id}/instance/{instance_id}/flavor	gaussdb:instance:resizeFlavor	-
查询实例主备平衡状态	GET /v3/{project_id}/instances/{instance_id}/balance	gaussdb:instance:getBalanceStatus	-
查询解决方案模板配置	GET /v3/{project_id}/deployment-form	gaussdb:instance:listAll	-
查询已绑定的EIP列表	GET /v3/{project_id}/instances/{instance_id}/public-ips?offset={offset}&limit={limit}	gaussdb:instance:listPublicIps	-

权限	API	对应的授权项	依赖的授权项
弱密码校验	POST /v3/{project_id}/weak-password-verification	gaussdb:instance:check	-
绑定/解绑弹性公网IP	POST /v3/{project_id}/instances/{instance_id}/nodes/{node_id}/public-ip	gaussdb:instance:bindPublicIp	-
查询实例SSL证书下载地址	GET /v3/{project_id}/instances/{instance_id}/ssl-cert/download-link	gaussdb:instance:downloadSslCert	-
查询租户的实例配额	GET /v3/{project_id}/project-quotas?type={type}	gaussdb:quota:listAll	-

表 5-110 参数配置

权限	API	对应的授权项	依赖的授权项
获取参数模板列表	GET /v3/{project_id}/configurations?offset={offset}&limit={limit}	gaussdb:param:listAll	-
获取指定实例的参数	GET /v3/{project_id}/instances/{instance_id}/configurations	gaussdb:instance:get	-
修改指定实例的参数	PUT /v3/{project_id}/instances/{instance_id}/configurations	gaussdb:param:update	-
创建参数模板	POST /v3/{project_id}/configurations	gaussdb:param:createParam	-
删除参数模板	DELETE /v3/{project_id}/configurations/{config_id}	gaussdb:param:delete	-

权限	API	对应的授权项	依赖的授权项
查询参数模板详情	GET /v3/{project_id}/configurations/{config_id}	gaussdb:param:get	-
复制参数模板	POST /v3/{project_id}/configurations/{config_id}/copy	gaussdb:param:copy	-
重置参数组	POST /v3/{project_id}/configurations/{config_id}/reset	gaussdb:param:reset	-
比较两个参数组模板之间的差异	POST /v3/{project_id}/configurations/comparison	gaussdb:param:compare	-
查询可应用实例列表	GET /v3/{project_id}/configurations/{config_id}/applicable-instances	gaussdb:instance:listAll	-
校验参数组名称是否存在	GET /v3/{project_id}/configurations/name-validation?name={name}	gaussdb:param:check	-
应用参数模板	PUT /v3/{project_id}/configurations/{config_id}/apply	gaussdb:param:apply	-
查询参数模板的应用记录	GET /v3/{project_id}/configurations/{config_id}/applied-histories	gaussdb:param:listAll	-
查询参数模板的修改历史	GET /v3/{project_id}/configurations/{config_id}/histories	gaussdb:param:listAll	-

表 5-111 备份管理

权限	API	对应的授权项	依赖的授权项
设置自动备份策略	PUT /v3/{project_id}/instances/{instance_id}/backups/policy	gaussdb:instance:updateBackupPolicy	-
查询自动备份策略	GET /v3/{project_id}/instances/{instance_id}/backups/policy	gaussdb:instance:getBackupPolicy	-
查询备份列表	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}	gaussdb:backup:listAll	-
创建手动备份	POST /v3/{project_id}/backups	gaussdb:backup:create	-
删除手动备份	DELETE /v3/{project_id}/backups/{backup_id}	gaussdb:backup:delete	-
查询可恢复时间段	GET /v3/{project_id}/instances/{instance_id}/restore-time?date={date}	gaussdb:instance:listRecoverableTimes	-
恢复到新实例	POST /v3/{project_id}/instances	gaussdb:instance:createInstance	-
查询可用于备份恢复的实例列表	GET /v3/{project_id}/restorable-instances	gaussdb:instance:listAll	-
根据时间点或者备份文件查询原实例信息	GET /v3/{project_id}/instance-snapshot?instance_id={instance_id}&backup_id={backup_id}&restore_time={restore_time}	gaussdb:instance:get	-

表 5-112 引擎版本和规格

权限	API	对应的授权项	依赖的授权项
查询数据库引擎的版本	GET /v3/{project_id}/datastore/versions	gaussdb:instance:listAll	-
查询数据库规格	GET /v3/{project_id}/flavors?limit={limit}&offset={offset}&ha_mode={ha_mode}&version={version}&spec_code={spec_code}	gaussdb:instance:listAll	-
查询引擎列表	GET /v3/{project_id}/datastores	gaussdb:instance:listAll	-
查询实例可变更规格	GET /v3/{project_id}/instances/{instance_id}/available-flavors	gaussdb:instance:listAll	-

表 5-113 管理数据库和用户

权限	API	对应的授权项	依赖的授权项
创建数据库	POST /v3/{project_id}/instances/{instance_id}/database	gaussdb:instance:createDatabase	-
创建数据库用户	POST /v3/{project_id}/instances/{instance_id}/db-user	gaussdb:instance:createDatabaseUser	-
创建数据库SCHEMA	POST /v3/{project_id}/instances/{instance_id}/schema	gaussdb:instance:createDatabaseSchema	-
授权数据库账号	POST /v3/{project_id}/instances/{instance_id}/db-privilege	gaussdb:instance:grantDatabasePrivilege	-

权限	API	对应的授权项	依赖的授权项
重置数据库账号密码	PUT /v3/{project_id}/instances/{instance_id}/db-user/password	gaussdb:instance:resetPassword	-
查询数据库列表	GET /v3/{project_id}/instances/{instance_id}/databases	gaussdb:instance:listDatabases	-
查询数据库用户列表	GET /v3/{project_id}/instances/{instance_id}/db-users	gaussdb:instance:listDatabaseUsers	-
查询数据库SCHEMA列表	GET /v3/{project_id}/instances/{instance_id}/schemas	gaussdb:instance:listSchemas	-

表 5-114 标签管理

权限	API	对应的授权项	依赖的授权项
查询实例标签	GET /v3/{project_id}/instances/{instance_id}/tags	gaussdb:tag:listAll	-
查询项目标签	GET /v3/{project_id}/tags	gaussdb:tag:listAll	-
查询预定义标签	GET /v3/{project_id}/predefined-tags	gaussdb:tag:listAll	-
添加实例标签	POST /v3/{project_id}/instances/{instance_id}/tags	gaussdb:tag:create	-

表 5-115 磁盘管理

权限	API	对应的授权项	依赖的授权项
查询实例存储空间使用信息	GET /v3/{project_id}/instances/{instance_id}/volume-usage	gaussdb:instance:getDiskUsage	-
查询数据库磁盘类型	GET /v3/{project_id}/storage-type?version={version}&ha_mode={ha_mode}	gaussdb:instance:listAll	-

表 5-116 配额管理

权限	API	对应的授权项	依赖的授权项
修改企业项目配额	PUT /v3/{project_id}/enterprise-projects/quotas	gaussdb:quota:update	-
查询企业项目配额组	GET /v3/{project_id}/enterprise-projects/quotas	gaussdb:quota:listAll	-

表 5-117 任务管理

权限	API	对应的授权项	依赖的授权项
获取任务信息	GET /v3/{project_id}/jobs?id={id}	gaussdb:task:get	-
查询任务列表	GET /v3/{project_id}/tasks	gaussdb:task:listAll	-
删除任务记录	DELETE /v3/{project_id}/jobs/{job_id}	gaussdb:task:delete	-

表 5-118 回收站

权限	API	对应的授权项	依赖的授权项
设置回收站策略	PUT /v3/{project_id}/recycle-policy	gaussdb:instance:setRecyclePolicy	-
查看回收站策略	GET /v3/{project_id}/recycle-policy	gaussdb:instance:getRecyclePolicy	-
查询回收站所有引擎实例列表	GET /v3/{project_id}/recycle-instances	gaussdb:instance:listAll	-

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。

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

表 5-119 GaussDB 支持的资源类型

资源类型	URN
instance	gaussdb:<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gaussdb:）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。

GaussDB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 5-120 GaussDB 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
gaussdb: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。限定词选择“默认”。
gaussdb: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。限定词选择“默认”。

5.10.7.4 数据复制服务 DRS

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DRS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。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

关于DRS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DRS的相关操作。

表 5-121 DRS 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
drs:backupMigrationJob:createJob	授予创建离线迁移任务的权限。	write	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys
drs:backupMigrationJob:deleteJob	授予删除离线迁移任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:backupMigrationJob:getJobDetail	授予查询离线迁移任务详细信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:backupMigrationJob:modifyOfflineTaskInfo	授予修改离线迁移任务信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:cloudDataGuardJob:getChartMonitor	授予查询报表图的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:cloudDataGuardJob:getDataGuardMonitor	授予查询容灾监控数据的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:cloudDataGuardJob:getLastDataDisplay	授予查询灾备最后数据的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:cloudDataGuardJob:getRpoAndRto	授予查询指定任务的RPO和RTO的权限。	list	job	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
drs:compareJob:createDataCompareJob	授予创建数据级表对比任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:createObjectCompareJob	授予创建对象级表对比任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:deleteDataCompareJob	授予取消数据级表对比任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getTopicInfo	授予查询已创建全部主题信息的权限。	list	-	-
drs:migrationJob:listAllSmnInfo	授予查询已录入全部信息的权限。	list	-	-
drs:configuration:getPublicIp	授予查询EIP列表或者Eip信息的权限。	list	-	-
drs:configuration:getVpcs	授予查询VPC列表的权限。	list	-	-
drs:configuration:listSubnets	授予查询子网列表的权限。	list	-	-
drs:configuration:getFeatures	授予查询特性白名单的权限。	list	-	-
drs:configuration:addTag	授予添加资源标签的权限。	tagging	-	-
drs:compareJob:exportAccountCompareResult	授予导出并下载用户比对任务比对结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:exportCompareReport	授予下载比对结果的权限。	list	job	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
drs:configuration:getInstancesTag	授予批量查询资源标签的权限。	list		
drs:compareJob:exportContentsCompareResult	授予导出内容比对任务比对结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getProjectTags	授予查询项目标签的权限。	list	-	-
drs:compareJob:exportLinesCompareResult	授予导出行比对任务比对结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:exportObjectsCompareResult	授予导出对象比对任务比对结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getAccountCompare	授予查询账户对比概览的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getAccountCompareDetail	授予查询账户对比详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getAccountCompareDetails	授予查询账户对比详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:subscriptionJob:exportJobs	授予导出订阅任务列表的权限。	list	-	-
drs:compareJob:getAccountDetails	授予查询行对比总览的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getCompareJobEstimatedTime	授予查询对比预估时间的权限。	list	job	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
drs:compareJob:getComparePolicy	授予查询对比策略的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:subscriptionJob:listJobs	授予查询订阅任务列表的权限。	list		
drs:compareJob:getContentCompare	授予查询内容对比总览的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getContentCompareDetail	授予查询内容对比详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getContentCompareDiff	授予查询内容对比差异的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getDataCompareDetail	授予查询行对比详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getDataCompareResult	授予查询数据级表对比任务结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getFlowObjectsCompare	授予查询动态对象级迁移对比概览的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getHealthCompareJobDetail	授予查询健康对比任务详情信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getLineCompare	授予查询行对比总览的权限。	list	job	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
drs:compareJob:getLineCompareDetail	授予查询行对比详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getObjectCompare	授予根据对比任务ID查询对象级迁移对比概览的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getObjectsCompareDetail	授予查询对象级对比详细信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getObjectsMigrateCompare	授予根据任务ID查询对象级迁移对比概览的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getObjectsMigrateCompareDetail	授予查询对象级迁移对比详细信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getTableCompareDetail	授予查询数据级表对比任务详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:listDataCompare	授予查询数据级表对比任务列表的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:listHealthCompareJobs	授予查询健康对比报告列表的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:modifyComparePolicy	授予修改对比策略的权限。	write	job	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
drs:compareJob:startJob	授予立即启动数据级表对比任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:stopJob	授予停止对比任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:addDataTransformationInfo	授予添加数据加工的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:batchModifyTag	授予批量添加修改资源标签的权限。	tagging	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys
drs:configuration:batchReplaceTags	授予批量重置资源标签的权限。	tagging	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys
drs:configuration:checkDataTransformationInfo	授予校验数据加工信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:deleteDataTransformationInfo	授予删除数据加工数据的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:deleteSmnInfo	授予删除已录入单个信息的权限。	write	job	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
drs:configuration:deleteSmnInfoForTopic	授予删除已录入单个主题信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:deleteTag	授予删除资源标签的权限。	tagging	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys
drs:configuration:downloadTemplate	授予导入对象信息前下载Excel模板的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getAddColumns	授予查询数据加工信息(多表归一加多个列)的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getAddColumnsFromDb	授予查询数据加工信息(多表归一加多个列)-任务启动后查询的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getFlavorInfo	授予查询引擎的规格信息的权限。	list	-	-
drs:backupMigrationJob:checkOfflineTaskName	授予校验离线迁移任务名称的权限。	write	-	-
drs:configuration:getColumnInfo	授予查询对象的列信息（列映射、列过滤）的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getDatabaseName	授予查询目标库名称的权限。	list	job	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
drs:configuration:getDatabaseParams	授予查询数据库参数的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:backupMigrationJob:exportJobList	授予导出离线迁移任务列表的权限。	list	-	-
drs:backupMigrationJob:getBackupFileDbList	授予查询备份文件数据库列表的权限。	list	-	-
drs:configuration:getDataTransformationData	授予查询数据加工数据的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:backupMigrationJob:getRedisInstList	授予查询Redis数据库实例列表的权限。	list	-	-
drs:backupMigrationJob:listBuckets	授予查询桶列表的权限。	list	-	-
drs:backupMigrationJob:listJobs	授予查询离线迁移任务列表的权限。	list	-	-
drs:backupMigrationJob:listObsObject	授予查询当前桶对象列表的权限。	list	-	-
drs:configuration:getDataTransformationInfo	授予查询数据加工信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:listFeature	授予查询支持特性列表的权限。	list	-	-
drs:configuration:listLinks	授予查询可用链路信息的权限。	list	-	-
drs:configuration:getEffectTime	授予查询指定任务数据库影响时间的权限。	list	job	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
drs:configuration:getESConfig	授予查询ElasticSearch的配置信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getInstanceTag	授予查询资源标签的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getSupportDataTransformationType	授予查询数据加工数据类型的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getTableInfo	授予查询表结构和表数据的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:importSmnInfo	授予录入收件方式与信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:listTopics	授予查询涉及到的kafka的topic信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:modifyDatabaseParams	授予修改数据库参数的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:modifyESConfig	授予修改ElasticSearch的配置信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:modifySmnInfo	授予修改收件方式与信息的权限。	write	job	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
drs:configuration:modifyTag	授予修改资源标签的权限。	tagging	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys
drs:configuration:modifyUserInfo	授予更新迁移用户信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:setMigrationTransSpeed	授予设置迁移速度的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getInstanceNum	授予查询任务数量的权限。	list	-	-
drs:configuration:getInstanceQuotas	授予查询配额的权限。	list	-	-
drs:configuration:getQuota	授予查询租户在DRS服务下的配额信息的权限。	list	-	-
drs:migrationJoAb:batchDeleteJobs	授予批量结束或删除任务的权限。	write	-	-
drs:configuration:updateDataTransformationInfo	授予更新数据加工信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:addSubscribeJob	授予创建包周期订购的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:associateSmnInfo	授予关联管控主题信息的权限。	write	job	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
drs:migrationJob:batchPauseJob	授予批量暂停任务的权限。	write	-	-
drs:migrationJob:batchPreCheckJob	授予批量预检查的权限。	write	-	-
drs:migrationJob:batchRetryJob	授予重试任务的权限。	write	-	-
drs:migrationJob:batchSetTransformation	授予加工同步对象的权限。	write	-	-
drs:migrationJob:batchStartJob	授予批量启动任务的权限。	write	-	-
drs:migrationJob:batchTestClusterConnection	授予批量测试连接（集群模式）的权限。	write	-	-
drs:migrationJob:batchTestConnection	授予批量测试连接的权限。	write	-	-
drs:migrationJob:downloadBatchCreateTemplate	授予下载批量创建任务模板的权限。	list	-	-
drs:migrationJob:importBatchCreateJobs	授予导入批量创建任务的权限。	write	-	-
drs:migrationJob:listAsyncJobDetail	授予查询租户指定ID批量异步任务详情的权限。	list	-	-
drs:migrationJob:listAsyncJobs	授予查询批量异步创建任务列表的权限。	list	-	-
drs:migrationJob:listJobInfo	授予根据任务ID批量查询任务详情的权限。	list	-	-
drs:migrationJob:listJobStatus	授予根据任务ID批量查询任务状态的权限。	list	-	-

授权项	描述	访问级别	资源类型（* 为必须）	条件键
drs:migrationJob:asyncBatchCreateJobByAsyncId	授予批量异步创建任务的权限。	write	job	drs:netType g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys
drs:migrationJob:getJobList	授予查询租户任务列表的权限。	list	-	-
drs:migrationJob:listPrecheckResult	授予查询批量任务的预检查结果的权限。	list	-	-
drs:migrationJob:selectDatabaseObject	授予选择需要迁移的数据库或者表的权限。	write	-	-
drs:configuration:listEPs	授予查询企业项目的权限。	list	-	-
drs:migrationJob:asyncBatchSaveJob	授予批量异步保存任务信息的权限。	write	job	drs:netType g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys
drs:migrationJob:asyncBatchUpdateJobByAsyncId	授予批量异步更新租户指定ID任务详情的权限。	write	job	drs:netType g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys
drs:migrationJob:batchCreateJob	授予批量同步创建任务的权限。	write	job	drs:netType g:EnterpriseProjectId 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
drs:migrationJob:changeFlavor	授予创建规格变更的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getCesJobs	授予查询迁移任务列表的权限。	list	-	-
drs:migrationJob:changeFlavorByNeed	授予按需页面进行node规格变更的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:createJob	授予创建对比任务的权限。	write	-	-
drs:migrationJob:checkInheritJob	授予判断任务能否继承的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:checkRestartPoint	授予检查跳跃续传位点的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:checkTableExist	授予查询表结构和表数据是否存在的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:copyJobAction	授予复制任务下发动作的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:createJob	授予创建在线迁移任务的权限。	write	job	drs:netType g:EnterpriseProjectId 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
drs:migrationJob:createJobs	授予创建任务的权限。	write	job	drs:netType g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys
drs:migrationJob:deleteColumnInfo	授予删除对象的列信息（列映射、列过滤）的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:deleteJob	授予删除在线迁移任务V1的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:downloadDbObjectTemplate	授予下载对象选择模板的权限。	read	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:endJob	授予结束在线迁移任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:exportAddedDeletedObjectsInfo	授予导出增删的对象信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getCompareResult	授予查询对比结果的权限。	list	-	-
drs:migrationJob:exportErrorInfo	授予导出错误信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:exportObjectsSentInfo	授予导出已经下发的对象信息的权限。	list	job	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
drs:migrationJob:getAccess	授予查询指定任务允许操作信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getAggregationTable	授予查询内存中多表映射信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getCesJob	授予查询迁移任务的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getDbObjectCollectionStatus	授予获取提交查询数据库对象信息的结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getDbObjects	授予查询数据库对象信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getDbObjectsCollectAsync	授予提交查询数据库对象信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getDbObjectTemplateProgress	授予查询对象选择导入进度的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getDbObjectTemplateResult	授予获取对象选择导入结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getFullJobDetails	授予查询全量同步的详情的权限。	list	job	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
drs:migrationJob:getImportExcelProcess	授予查询解析excel的进度的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getIncreComponentsDetails	授予查询增量组件的详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getJob	授予查询在线迁移任务详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getJobDetail	授予查询任务详情的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getJobMeteringPrice	授予查询任务价格信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getObjectHasColumn	授予查询有列信息（列映射、列过滤）的对象的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getObjectsCompareOverviewa	授予查询数据级流式对比的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getObjectSelectInfo	授予查询任务对象选择信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getOperationInfo	授予查询指定任务操作统计信息的权限。	list	job	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
drs:migrationJob:getProgress	授予查询指定任务迁移进度的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:listDatabaseParams	授予查询源库和目标库的数据库参数的权限。	list	-	-
drs:migrationJob:getSmnInfo	授予查询已录入单个信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getSmnInfoForTopic	授予查询已录入单个主题信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getSrcUsers	授予查询源库迁移用户列表的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getOpenStreamResult	授予查询开启流结果的权限。	list	-	-
drs:migrationJob:getSupportObject	授予查询任务是否支持对象选择/列映射等的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getSupportSearchObjectType	授予查询任务支持查询用户选择对象的类型的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getSwitchVipStatus	授予查询VIP倒换结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:batchDeleteJob	授予批量删除任务的权限。	write	-	-
drs:migrationJob:batchOperateJob	授予批量操作租户指定ID任务的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
drs:migrationJob:getTaskLog	授予获取迁移日志的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getTuningParams	授予查询调优参数的值的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:checkAction	授予校验任务名称的权限。	write	-	-
drs:migrationJob:getUpdateObjectSavingStatus	授予获取对象保存进度的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getUserSelectedObjectInfo	授予查询用户选择的同步映射关系的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:cloneJobs	授予克隆mysql同步任务的权限。	write	-	-
drs:migrationJob:getUserSetObjectInfo	授予查询已同步的对象信息的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:jobAction	授予执行任务特定的操作的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:jobUpdateAction	授予任务、抓取和回放的启停操作的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:exportJobs	授予导出在线迁移任务列表的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
drs:migrationJob:listJobs	授予查询租户任务列表的权限。	list	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys
drs:migrationJob:getBatchTaskLog	授予批量获取迁移日志的权限。	list	-	-
drs:migrationJob:getCountdown	授予查询云服务倒计时信息的权限。	list	-	-
drs:migrationJob:getDrsJobByRdsInstanceId	授予查询rds实例相关的迁移任务的权限。	list	-	-
drs:migrationJob:listJobs		list	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys
drs:migrationJob:listReplayFaultsJobs	授予查询回放故障列表的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:modifyColumnInfo	授予修改对象的列信息（列映射、列过滤）的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:modifyCommonSetting	授予更新任务配置的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:modifyConflictPolicy	授予更新同步任务忽略策略的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getJobs	授予查询在线迁移任务列表的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
drs:migrationJob:getNodeNumByDDMInstance	授予根据ddm sharding个数计算对应子任务数量的权限。	list	-	-
drs:migrationJob:modifyGroupAndStream	授予开启或者关闭对接LTS服务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getPrecheckResult	授予查询迁移任务预检查结果的权限。	list	-	-
drs:migrationJob:modifyIncreStartPosition	授予更新增量任务的启动位点的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getResourceInstances	授予查询资源实例以及关联资源信息的权限。	list	-	-
drs:migrationJob:modifyJob	授予修改在线迁移任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:modifySyncTypePolicy	授予更新同步类型策略的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getSubscribeNumber	授予查询包周期订购规格信息的权限。	list	-	-
drs:migrationJob:operateJobByJobId	授予操作租户指定ID任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:selectGroupAndStream	授予查询用户当前任务是否开启lts服务的权限。	list	job	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
drs:migrationJob:sendImportCheck	授予上传excel文件的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:switchVip	授予双VIP倒换的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:updateDDLPolicy	授予更新过滤DDL策略的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:listProgressInfo	授予根据任务ID批量查询迁移进度、增量时延信息的权限。	list	-	-
drs:migrationJob:updateJobInfo	授予更新租户指定ID任务详情的权限。	write	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys
drs:migrationJob:updateObjectInfo	授予更新数据库对象选择信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:updateTuningParams	授予修改调优参数的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:uploadDbObjectTemplate	授予对象选择导入数据的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:downloadReport	授予下载流量回放相关文件的权限。	list	job	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
drs:replayJob:exportAbnormalSqlData	授予下载流量回放异常SQL的权限。	list	job	drs:netType g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys
drs:migrationJob:resourceCheck	授予创建在线迁移任务资源检查的权限。	write	-	-
drs:migrationJob:skipPrecheck	授予跳过预检查的权限。	write	-	-
drs:replayJob:exportSlowSqlData	授予导出流量回放SQL的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:getAbnormalSqlData	授予查询流量回放异常量SQL的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:getAllSqlFile	授予查询流量回放全量SQL文件的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:getExecuteResultData	授予查询流量回放结果的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:getExportSlowSqlStatus	授予查询流量回放文件导出状态的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:getReplayErrorTemplate	授予查询异常sql模板的权限。	list	job	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
drs:replayJob:getReplayFile	授予查询流量回放文件的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:cloudDataGuardJob:getMonitoringData	授予根据任务ID查询容灾监控数据的权限。	list	-	-
drs:cloudDataGuardJob:batchSwitchover	授予批量主备倒换的权限。	write	-	-
drs:cloudDataGuardJob:listJobInfo	授予根据任务ID批量查询灾备初始化对象详情的权限。	list	-	-
drs:cloudDataGuardJob:listRpoAndRto	授予批量查询RPO和RTO的权限。	list	-	-
drs:cloudDataGuardJob:listStructProcess	授予根据任务ID批量查询灾备初始化进度的权限。	list	-	-
drs:migrationJob:batchSetSmn	授予批量设置告警信息的权限。	write	-	-
drs:migrationJob:batchSetSpeedLimit	授予批量设置任务限速的权限。	write	-	-
drs:migrationJob:batchUpdateDefinerMigrateSetting	授予批量设置Definer迁移是否迁移到到该用户下的权限。	write	-	-
drs:migrationJob:batchUpdateJobInfo	授予批量修改任务名称或描述，设置异常通知信息的权限。	write	-	-
drs:migrationJob:batchUpdateUserMigrate	授予批量设置需要迁移的用户和角色的权限。	write	-	-
drs:migrationJob:changeSrcOrTargetPwd	授予修改任务源或目标数据库密码的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
drs:migrationJob:setBatchSyncPolicy	授予批量设置同步策略的权限。	write	-	-
drs:replayJob:getReplayRecord	授予查询流量报告的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:getReplaySlowTemplate	授予查询慢sql模板的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:getSlowSqlData	授予查询流量回放慢SQL的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:listReplayData	授予查询流量回放统计列表的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:subscriptionJob:createJob	授予创建订阅任务的权限。	write	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys
drs:subscriptionJob:deleteJob	授予删除订阅任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:subscriptionJob:editJobInfo	授予编辑订阅任务信息的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:subscriptionJob:getJobDetail	授予查询订阅任务详情的权限。	list	job	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
drs:subscriptionJob:getSubscriptionRecord	授予查询详细的订阅内容的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:subscriptionJob:jobAction	授予订阅任务操作的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getUserGuideInfo	授予获取用户指引详情的权限。	list	-	-
drs:configuration:modifyUserGuideInfo	授予更新用户指引的权限。	write	-	-
drs:subscriptionJob:updateConsumeTime	授予修改消费时间点的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:subscriptionJob:updateJob	授予修改订阅任务的权限。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:cloudDataGuardJob:getRdsInstanceCount	授予查询指定DDM下面rds实例的数量的权限。	list	-	-
drs:configuration:getAvailableNodeType	授予查询可用的node规格的权限。	list	-	-
drs:configuration:getAvailableZoneWithoutSellOut	授予查询node规格未售罄的可用AZ的权限。	list	-	-
drs:configuration:listAvailableZoneStatus	授予查询AZ状态的权限。	list	-	-
drs:configuration:listAvailableZone	授予查询可用AZ的权限。	list	-	-
drs:migrationJob:listAvailableZone	授予查询规格未售罄的可用区的权限。	list	-	-
drs:configuration:listResourcesByTag	授予根据标签查询任务的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
drs::listDrivers	授予查询驱动列表的权限。	list	-	-
drs::uploadDriver	授予上传驱动的权限。	write	-	-
drs::deleteDriver	授予删除驱动的权限。	write	-	-
drs:migrationJob:syncDriver	授予同步驱动的权限。	write	-	-
drs:configuration:modifyConfigInfo	授予更新任务的参数信息。	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getJobParameters	授予查询任务的参数配置列表信息。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getJobParametersHistory	授予查询任务的参数配置修改历史。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:showReplayTimeScope	授予查询录制回放时间窗口的权限。	read	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:showReplayResults	授予查询录制回放结果数据的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:exportReport	授予导出录制回放报表文件的权限。	read	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:showReportExportStatus	授予查询录制回放报表导出状态的权限。	read	job	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
drs:replayJob:showReportFileObsUris	授予查询录制回放报表下载链接的权限。	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

DRS的API通常对应着一个或多个授权项。表5-122展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-122 API 与授权项的关系

API	对应的授权项	依赖的授权项
DELETE /v3/{project_id}/jobs/batch-jobs	drs:migrationJoAb:batchDeleteJobs	-
DELETE /v5/{project_id}/jdbc-drivers	drs::deleteDriver	-
DELETE /v5/{project_id}/jobs	drs:migrationJob:batchDeleteJob	-
DELETE /v5/{project_id}/jobs/{job_id}	drs:migrationJob:deleteJob	-
GET /v3/{project_id}/jobs/{job_id}/get-src-user	drs:migrationJob:getSrcUsers	-
GET /v3/{project_id}/node-type	drs:configuration:getAvailableNodeType	-
GET /v3/{project_id}/quotas	drs:configuration:getQuota	-
GET /v5.1/{project_id}/jobs/{job_id}/db-object	drs:migrationJob:getDbObjects	-
GET /v5/{project_id}/{resource_type}/{resource_id}/tags	drs:configuration:getInstanceTag	-
GET /v5/{project_id}/{resource_type}/tags	drs:configuration:getProjectTags	-
GET /v5/{project_id}/batch-async-jobs	drs:migrationJob:listAsyncJobs	-

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/batch-async-jobs/{async_job_id}	drs:migrationJob:listAsyncJobDetail	-
GET /v5/{project_id}/enterprise-projects	drs:configuration:listEPs	-
GET /v5/{project_id}/jdbc-drivers	drs::listDrivers	-
GET /v5/{project_id}/job/{job_id}/columns	drs:configuration:getColumnInfo	-
GET /v5/{project_id}/job/{job_id}/data-filtering/result	drs:configuration:getDataTransformationData	-
GET /v5/{project_id}/jobs	drs:migrationJob:getJobList	-
GET /v5/{project_id}/jobs/{job_id}	drs:migrationJob:getJobDetail	-
GET /v5/{project_id}/jobs/{job_id}/actions	drs:migrationJob:getAccess	-
GET /v5/{project_id}/jobs/{job_id}/compare-policy	drs:compareJob:getComparePolicy	-
GET /v5/{project_id}/jobs/{job_id}/configuration-histories	drs:configuration:getJobParametersHistory	-
GET /v5/{project_id}/jobs/{job_id}/configurations	drs:configuration:getJobParameters	-
GET /v5/{project_id}/jobs/{job_id}/data-processing-rules	drs:configuration:getDataTransformationInfo	-
GET /v5/{project_id}/jobs/{job_id}/data-processing-rules/result	drs:configuration:getDataTransformationInfo	-
GET /v5/{project_id}/jobs/{job_id}/db-object/template	drs:migrationJob:downloadDbObjectTemplate	-
GET /v5/{project_id}/jobs/{job_id}/db-object/template/progress	drs:migrationJob:getDbObjectTemplateProgress	-

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/jobs/{job_id}/db-object/template/result	drs:migrationJob:getDbObjectTemplateResult	-
GET /v5/{project_id}/jobs/{job_id}/db-objects	drs:migrationJob:getDbObjects	-
GET /v5/{project_id}/jobs/{job_id}/db-objects/collection-status	drs:migrationJob:getDbObjectCollectionStatus	-
GET /v5/{project_id}/jobs/{job_id}/db-objects/saving-status	drs:migrationJob:getUpdateObjectSavingStatus	-
GET /v5/{project_id}/jobs/{job_id}/db-position	drs:migrationJob:checkAction	-
GET /v5/{project_id}/jobs/{job_id}/dirty-data	drs:migrationJob:listReplayFaultsJobs	-
GET /v5/{project_id}/jobs/{job_id}/health-compare-jobs	drs:compareJob:listHealthCompareJobs	-
GET /v5/{project_id}/jobs/{job_id}/increment-components-detail	drs:migrationJob:getIncreComponentsDetails	-
GET /v5/{project_id}/jobs/{job_id}/metering	drs:migrationJob:getJobMeteringPrice	-
GET /v5/{project_id}/jobs/{job_id}/monitor-data	drs:cloudDataGuardJob:getDataGuardMonitor	-
GET /v5/{project_id}/jobs/{job_id}/object/support	drs:migrationJob:getSupportObject	-
GET /v5/{project_id}/jobs/{job_id}/progress-data/{type}	drs:migrationJob:getObjectsCompareOverviewa	-
GET /v5/{project_id}/jobs/{resource_type}/{job_id}/tags	drs:configuration:getInstanceTag	-
GET /v5/{project_id}/jobs/{resource_type}/tags	drs:configuration:getProjectTags	-

API	对应的授权项	依赖的授权项
GET /v5/{project_id}/jobs/template	drs:migrationJob:downloadBatchCreateTemplate	-
GET /v5/{project_id}/links	drs:configuration:listLinks	-
POST /v3/{project_id}/available-zone	drs:migrationJob:listAvailableZone	-
POST /v3/{project_id}/jobs	drs:migrationJob:listJobs	-
POST /v3/{project_id}/jobs/{job_id}/params	drs:configuration:modifyDatabaseParams	-
POST /v3/{project_id}/jobs/{type}/batch-struct-detail	drs:cloudDataGuardJob:listJobInfo	-
POST /v3/{project_id}/jobs/batch-connection	drs:migrationJob:batchTestConnection	-
POST /v3/{project_id}/jobs/batch-creation	drs:migrationJob:batchCreateJob	-
POST /v3/{project_id}/jobs/batch-detail	drs:migrationJob:listJobInfo	-
POST /v3/{project_id}/jobs/batch-get-params	drs:configuration:listDatabaseParams	-
POST /v3/{project_id}/jobs/batch-pause-task	drs:migrationJob:batchPauseJob	-
POST /v3/{project_id}/jobs/batch-precheck	drs:migrationJob:batchPreCheckJob	-
POST /v3/{project_id}/jobs/batch-precheck-result	drs:migrationJob:listPrecheckResult	-
POST /v3/{project_id}/jobs/batch-progress	drs:migrationJob:listProgressInfo	-
POST /v3/{project_id}/jobs/batch-replace-definer	drs:migrationJob:batchUpdateDefinerMigrateSetting	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/jobs/batch-retry-task	drs:migrationJob:batchRetryJob	-
POST /v3/{project_id}/jobs/batch-rpo-and-rto	drs:cloudDataGuardJob:listRpoAndRto	-
POST /v3/{project_id}/jobs/batch-set-smn	drs:migrationJob:batchSetSmn	-
POST /v3/{project_id}/jobs/batch-starting	drs:migrationJob:batchStartJob	-
POST /v3/{project_id}/jobs/batch-status	drs:migrationJob:listJobStatus	-
POST /v3/{project_id}/jobs/batch-struct-process	drs:cloudDataGuardJob:listStructProcess	-
POST /v3/{project_id}/jobs/batch-switchover	drs:cloudDataGuardJob:batchSwitchover	-
POST /v3/{project_id}/jobs/batch-sync-policy	drs:migrationJob:setBatchSyncPolicy	-
POST /v3/{project_id}/jobs/batch-transformation	drs:migrationJob:batchSetTransformation	-
POST /v3/{project_id}/jobs/cluster/batch-connection	drs:migrationJob:batchTestClusterConnection	-
POST /v3/{project_id}/jobs/create-compare-task	drs:compareJob:createJob	-
POST /v3/{project_id}/jobs/disaster-recovery-monitoring-data	drs:cloudDataGuardJob:getMonitoringData	-
POST /v3/{project_id}/jobs/query-compare-result	drs:compareJob:getCompareResult	-
POST /v5.1/{project_id}/jobs/{job_id}/db-objects/collect	drs:migrationJob:getDbObjectsCollectAsync	-
POST /v5/{project_id}/{resource_type}/{resource_id}/tags/create	drs:configuration:addTag	-

API	对应的授权项	依赖的授权项
POST /v5/{project_id}/{resource_type}/{resource_id}/tags/delete	drs:configuration:deleteTag	-
POST /v5/{project_id}/{resource_type}/resource-instances/count	drs:configuration:listResourcesByTag	-
POST /v5/{project_id}/{resource_type}/resource-instances/filter	drs:configuration:listResourcesByTag	-
POST /v5/{project_id}/batch-async-jobs/{async_job_id}/commit	drs:migrationJob:asyncBatchCreateJobByAsyncId	-
POST /v5/{project_id}/jdbc-driver	drs::uploadDriver	-
POST /v5/{project_id}/job/{job_id}/columns/collect	drs:configuration:getColumnInfo	-
POST /v5/{project_id}/job/{job_id}/data-filtering/check	drs:configuration:checkDataTransformationInfo	-
POST /v5/{project_id}/jobs	drs:migrationJob:createJobs	-
POST /v5/{project_id}/jobs/{job_id}/action	drs:migrationJob:operateJobByJobId	-
POST /v5/{project_id}/jobs/{job_id}/collect-db-position	drs:migrationJob:checkAction	-
POST /v5/{project_id}/jobs/{job_id}/db-object/template	drs:migrationJob:uploadDbObjectTemplate	-
POST /v5/{project_id}/jobs/{job_id}/db-objects/collect	drs:migrationJob:getDbObjectsCollectAsync	-
POST /v5/{project_id}/jobs/{job_id}/object-mappings	drs:migrationJob:getUserSelectedObjectInfo	-
POST /v5/{project_id}/jobs/{job_id}/operation-statistics/export	drs:migrationJob:getOperationInfo	-
POST /v5/{project_id}/jobs/{job_id}/stop	drs:migrationJob:deleteJob	-

API	对应的授权项	依赖的授权项
POST /v5/{project_id}/jobs/{resource_type}/{job_id}/tags/action	drs:configuration:batchReplaceTags	-
POST /v5/{project_id}/jobs/action	drs:migrationJob:batchOperateJob	-
POST /v5/{project_id}/jobs/batch-async-create	drs:migrationJob:asyncBatchSaveJob	-
POST /v5/{project_id}/jobs/batch-stop	drs:migrationJob:deleteJob	-
POST /v5/{project_id}/jobs/clone	drs:migrationJob:cloneJobs	-
POST /v5/{project_id}/jobs/name-validation	drs:migrationJob:checkAction	-
POST /v5/{project_id}/jobs/template	drs:migrationJob:importBatchCreateJobs	-
PUT /v3/{project_id}/job/{job_id}/tuning-params/modify-params	drs:migrationJob:updateTuningParams	-
PUT /v3/{project_id}/jobs/batch-limit-speed	drs:migrationJob:batchSetSpeedLimit	-
PUT /v3/{project_id}/jobs/batch-modification	drs:migrationJob:batchUpdateJobInfo	-
PUT /v3/{project_id}/jobs/batch-modify-pwd	drs:migrationJob:changeSrcOrTargetPwd	-
PUT /v3/{project_id}/jobs/batch-select-objects	drs:migrationJob:selectDatabaseObject	-
PUT /v3/{project_id}/jobs/batch-update-user	drs:migrationJob:batchUpdateUserMigrate	-
PUT /v5/{project_id}/batch-async-jobs/{async_job_id}	drs:migrationJob:asyncBatchUpdateJobByAsyncId	-
PUT /v5/{project_id}/jobs/{job_id}	drs:migrationJob:updateJobInfo	-

API	对应的授权项	依赖的授权项
PUT /v5/{project_id}/jobs/{job_id}/data-processing-rules	drs:configuration:addDataTransformationInfo	-
PUT /v5/{project_id}/jobs/{job_id}/modify-configuration	drs:configuration:modifyConfigInfo	-
PUT /v5/{project_id}/jobs/{job_id}/start-position	drs:migrationJob:modifyIncreStartPosition	-
PUT /v5/{project_id}/jobs/{job_id}/update-jdbc-driver	drs:migrationJob:syncDriver	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-123**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。

DRS定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-123 DRS 支持的资源类型

资源类型	URN
job	drs:<region>:<account-id>:job:<job-id>

条件（Condition）

DRS不支持在SCP中的条件键中配置服务级的条件键。DRS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 云数据库 TaurusDB

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）即为身份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身份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（-），则必须在身份策略语句的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TaurusDB定义的资源类型的详细信息请参见**资源类型（Resource）**。
- “条件键”列包括了可以在身份策略语句的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TaurusDB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TaurusDB的相关操作。

表 5-124 TaurusDB 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
gaussdbformysql:backup:modifyPolicy	授予设置自动备份策略的权限。	permission_management	-	-
gaussdbformysql:param:delete	授予删除参数组的权限。	permission_management	-	-
gaussdbformysql:instance:switchover	授予手动主备切换的权限。	permission_management	instance *	g:EnterpriseProjectId
gaussdbformysql:auditlog:list	授予实例获取审计日志列表的权限。	list	instance *	g:EnterpriseProjectId
gaussdbformysql:backup:create	授予创建手动备份权限。	write	-	-
gaussdbformysql:backup:delete	授予删除备份的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
gaussdbformysql:backup:getRestoreTime	授予获取实例可恢复时间点的权限。	read	instance *	g:EnterpriseProjectId
gaussdbformysql:backup:list	授予获取备份列表的权限。	list	-	-
gaussdbformysql:backup:listPolicy	授予获取备份策略的权限。	list	instance *	g:EnterpriseProjectId
gaussdbformysql:database:create	授予实例创建数据库的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:database:delete	授予实例删除数据库的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:database:list	授予实例查询数据库列表的权限。	list	instance *	g:EnterpriseProjectId
gaussdbformysql:database:modify	授予修改数据库相关信息的权限。	permission_management	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:getSecondLevelMonitoringConfig	授予查询秒级监控配置的权限。	read	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:addReadOnlyNodes	授予添加只读节点的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:create	授予创建实例的权限。	write	-	g:EnterpriseProjectId
gaussdbformysql:instance:delete	授予删除实例的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:deleteSqlFilterRules	授予删除Sql限流规则的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:get	授予获取实例详情的权限。	read	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:getDcc	授予获取专属资源池详情的权限。	read	-	-
gaussdbformysql:instance:getSqlFilterRule	授予获取SQL限流规则的权限。	read	instance *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
gaussdbformysql:instance:getSqlFilterStatus	授予获取SQL限流开关状态的权限。	read	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:list	授予获取实例列表的权限。	list	-	-
gaussdbformysql:proxy:list	授予获取数据库代理列表的权限。	list	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:listSpec	授予获取数据库代理规格列表的权限。	list	-	-
gaussdbformysql:instance:listDcc	授予获取专属资源列表的权限。	list	-	-
gaussdbformysql:instance:listEngine	授予查询引擎信息的权限。	list	-	-
gaussdbformysql:instance:listSpec	授予查询规格列表的权限。	list	-	-
gaussdbformysql:auditlog:operate	授予开启关闭审计日志的权限。	permission_management	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:bindPublicIp	授予实例绑定公网IP的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:deleteReadOnlyNodes	授予实例删除只读节点的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:modifyVip	授予实例修改读写内网地址的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:modifyMaintenanceWindow	授予修改实例运维时间窗的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:modifySecondLevelMonitorPolicy	授予修改实例秒级监控频率的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:modifyPassword	授予修改实例密码的权限。	write	instance *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
gaussdbformysql:instance:modifyPort	授予修改实例端口的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:modifySecurityGroup	授予修改实例安全组的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:modifySSL	授予修改SSL开关的权限。	permission_management	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:modifyStorageSize	授予实例磁盘扩缩容的权限。	permission_management	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:rename	授予修改实例名称的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:unbindPublicIp	授予实例解绑公网IP的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:upgrade	授予实例升级内核版本的权限。	permission_management	instance *	g:EnterpriseProjectId
gaussdbformysql:user:create	授予实例创建数据库用户的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:addNodes	授予数据库代理节点扩容的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:create	授予开启数据库代理的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:delete	授予关闭数据库代理的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:modifySpec	授予数据库代理规格变更的权限。	permission_management	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:modifyWeight	授予修改数据库代理权重的权限。	write	instance *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
gaussdbformysql:instance:modifySpec	授予变更实例规格的权限。	permission_management	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:restart	授予重启实例的权限。	permission_management	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:restoreInPlace	授予备份恢复到已有实例的权限。	permission_management	-	-
gaussdbformysql:instance:setSqlFilterRules	授予设置SQL限流规则的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:setSqlFilterStatus	授予开启/关闭SQL限流的权限。	permission_management	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:tableRestore	授予PITR库表级恢复的权限。	permission_management	instance *	g:EnterpriseProjectId
gaussdbformysql:tag:deal	授予添加/删除资源标签的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:log:getErrorLogs	授予获取错误日志的权限。	read	instance *	g:EnterpriseProjectId
gaussdbformysql:log:getSlowLogs	授予获取慢日志的权限。	read	instance *	g:EnterpriseProjectId
gaussdbformysql:param:apply	授予应用参数组的权限。	permission_management	-	-
gaussdbformysql:param:create	授予创建参数组的权限。	write	-	-
gaussdbformysql:param:get	授予获取参数组详情的权限。	read	-	-
gaussdbformysql:param:list	授予获取参数组列表的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
gaussdbformysql:param:update	授予修改参数组的权限。	write	-	-
gaussdbformysql:proxy:modifyConsistency	授予修改数据库代理会话一致性的权限。	permission_management	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:modifyTransactionSplit	授予开启/关闭数据库代理事务拆分的权限。	permission_management	instance *	g:EnterpriseProjectId
gaussdbformysql:quota:list	授予查询配额的权限。	read	-	-
gaussdbformysql:quota:modify	授予修改配额的权限。	write	-	-
gaussdbformysql:tag:list	授予查询标签列表的权限。	list	-	-
gaussdbformysql:task:delete	授予删除任务的权限。	write	-	-
gaussdbformysql:task:list	授予获取任务列表的权限。	list	-	-
gaussdbformysql:user:delete	授予删除数据库用户的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:user:grantPrivilege	授予修改数据库用户的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:user:list	授予查询数据库用户列表的权限。	list	instance *	g:EnterpriseProjectId
gaussdbformysql:user:modify	授予查询数据库用户备注的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:user:revokePrivilege	授予删除数据库用户权限的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:user:updatePassWord	授予修改数据库用户密码的权限。	write	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:switchConnectionPoolType	授予更改数据库代理连接池类型的权限。	permission_management	instance *	g:EnterpriseProjectId

TaurusDB的API通常对应着一个或多个授权项。表5-125展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-125 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}/datastores/{database_name}	gaussdbformysql:instance:listEngine	-
GET /v3/{project_id}/flavors/{database_name}	gaussdbformysql:instance:listSpec	-
POST /v3/{project_id}/instances	gaussdbformysql:instance:create	-
GET /v3.1/{project_id}/instances	gaussdbformysql:instance:list	-
POST /v3/{project_id}/instances/{instance_id}/restart	gaussdbformysql:instance:restart	-
DELETE /v3/{project_id}/instances/{instance_id}	gaussdbformysql:instance:delete	-
GET /v3.1/{project_id}/instances/{instance_id}	gaussdbformysql:instance:get	-
GET /v3.1/{project_id}/instances/details	gaussdbformysql:instance:get	-
POST /v3/{project_id}/instances/{instance_id}/nodes/enlarge	gaussdbformysql:instance:addReadOnlyNodes	-

API	对应的授权项	依赖的授权项
DELETE /v3/{project_id}/instances/{instance_id}/nodes/{node_id}	gaussdbformysql:instance:deleteReadOnlyNodes	-
POST /v3/{project_id}/instances/{instance_id}/volume/extend	gaussdbformysql:instance:modifyStorageSize	-
PUT /v3/{project_id}/instances/{instance_id}/backups/policy/update	gaussdbformysql:backup:modifyPolicy	-
PUT /v3/{project_id}/instances/{instance_id}/name	gaussdbformysql:instance:rename	-
POST /v3/{project_id}/instances/{instance_id}/password	gaussdbformysql:instance:modifyPassword	-
POST /v3/{project_id}/instances/{instance_id}/action	gaussdbformysql:instance:modifySpec	-
GET /v3/{project_id}/dedicated-resources	gaussdbformysql:instance:listDcc	-
GET /v3/{project_id}/dedicated-resource/{dedicated_resource_id}	gaussdbformysql:instance:getDcc	-
POST /v3/{project_id}/instances/{instance_id}/proxy	gaussdbformysql:proxy:create	-

API	对应的授权项	依赖的授权项
DELETE /v3/{project_id}/instances/{instance_id}/proxy	gaussdbformysql:proxy:delete	-
GET /v3/{project_id}/instances/{instance_id}/proxies	gaussdbformysql:proxy:list	-
GET /v3/{project_id}/instances/{instance_id}/proxy/flavors	gaussdbformysql:proxy:listSpec	-
POST /v3/{project_id}/instances/{instance_id}/proxy/enlarge	gaussdbformysql:proxy:addNodes	-
PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/flavor	gaussdbformysql:proxy:modifySpec	-
PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/weight	gaussdbformysql:proxy:modifyWeight	-
POST /v3/{project_id}/instances/{instance_id}/proxy/transaction-split	gaussdbformysql:proxy:modifyTransactionSplit	-
POST /v3.1/{project_id}/instances/{instance_id}/error-logs	gaussdbformysql:log:getErrorLogs	-
POST /v3.1/{project_id}/instances/{instance_id}/slow-logs	gaussdbformysql:log:getSlowLogs	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/project-quotas	gaussdbformysql:quota:list	-
GET /v3/{project_id}/quotas	gaussdbformysql:quota:list	-
POST /v3/{project_id}/quotas	gaussdbformysql:quota:modify	-
PUT /v3/{project_id}/quotas	gaussdbformysql:quota:modify	-
POST /v3/{project_id}/backups/create	gaussdbformysql:backup:create	-
GET /v3/{project_id}/backups	gaussdbformysql:backup:list	-
GET /v3/{project_id}/instances/{instance_id}/backups/policy	gaussdbformysql:backup:listPolicy	-
GET /v3/{project_id}/configurations	gaussdbformysql:param:list	-
POST /v3/{project_id}/configurations	gaussdbformysql:param:create	-
DELETE /v3/{project_id}/configurations/{configuration_id}	gaussdbformysql:param:delete	-
GET /v3/{project_id}/configurations/{configuration_id}	gaussdbformysql:param:get	-
PUT /v3/{project_id}/configurations/{configuration_id}	gaussdbformysql:param:update	-
PUT /v3/{project_id}/configurations/{configuration_id}/apply	gaussdbformysql:param:apply	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/instances/{instance_id}/tags	gaussdbformysql:tag:list	-
GET /v3/{project_id}/tags	gaussdbformysql:tag:list	-
POST /v3/{project_id}/instances/{instance_id}/tags/action	gaussdbformysql:tag:deal	-
PUT /v3/{project_id}/instances/{instance_id}/monitor-policy	gaussdbformysql:instance:modifySecondLevelMonitorPolicy	-
GET /v3/{project_id}/instances/{instance_id}/monitor-policy	gaussdbformysql:instance:getSecondLevelMonitoringConfig	-
POST /v3/{project_id}/instances/{instance_id}/nodes/{node_id}/restart	gaussdbformysql:instance:restart	-
POST /v3/{project_id}/instance/{instance_id}/audit-log/switch	gaussdbformysql:auditlog:operate	-
GET /v3/{project_id}/instance/{instance_id}/audit-log/switch-status	gaussdbformysql:auditlog:list	-
GET /v3/{project_id}/jobs	gaussdbformysql:task:list	-
POST /v3/{project_id}/instances/{instance_id}/db-users	gaussdbformysql:user:create	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/instances/{instance_id}/db-users	gaussdbformysql:user:list	-
DELETE /v3/{project_id}/instances/{instance_id}/db-users	gaussdbformysql:user:delete	-
PUT /v3/{project_id}/instances/{instance_id}/db-users/comment	gaussdbformysql:user:modify	-
PUT /v3/{project_id}/instances/{instance_id}/db-users/password	gaussdbformysql:user:updatePassWord	-
POST /v3/{project_id}/instances/{instance_id}/db-users/privilege	gaussdbformysql:user:grantPrivilege	-
DELETE /v3/{project_id}/instances/{instance_id}/db-users/privilege	gaussdbformysql:user:revokePrivilege	-
GET /v3/{project_id}/instances/{instance_id}/databases/charsets	gaussdbformysql:database:list	-
POST /v3/{project_id}/instances/{instance_id}/databases	gaussdbformysql:database:create	-
GET /v3/{project_id}/instances/{instance_id}/databases	gaussdbformysql:database:list	-

API	对应的授权项	依赖的授权项
DELETE /v3/{project_id}/instances/{instance_id}/databases	gaussdbformysql:database:delete	-
PUT /v3/{project_id}/instances/{instance_id}/databases/comment	gaussdbformysql:database:modify	-
POST /v3/{project_id}/instances/{instance_id}/sql-filter/switch	gaussdbformysql:instance:setSqlFilterStatus	-
GET /v3/{project_id}/instances/{instance_id}/sql-filter/switch	gaussdbformysql:instance:getSqlFilterStatus	-
PUT /v3/{project_id}/instances/{instance_id}/sql-filter/rules	gaussdbformysql:instance:setSqlFilterRules	-
GET /v3/{project_id}/instances/{instance_id}/sql-filter/rules	gaussdbformysql:instance:getSqlFilterRule	-
DELETE /v3/{project_id}/instances/{instance_id}/sql-filter/rules	gaussdbformysql:instance:deleteSqlFilterRules	-
PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/session-consistence	gaussdbformysql:proxy:modifyConsistency	-
GET /v3/{project_id}/immediate-jobs	gaussdbformysql:task:list	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/scheduled-jobs	gaussdbformysql:task:list	-
DELETE /v3/{project_id}/scheduled-jobs	gaussdbformysql:task:delete	-
DELETE /v3/{project_id}/jobs/{job_id}	gaussdbformysql:task:delete	-
POST /v3/{project_id}/instances/{instance_id}/db-upgrade	gaussdbformysql:instance:upgrade	-
PUT /v3/{project_id}/instances/{instance_id}/ssl-option	gaussdbformysql:instance:modifySSL	-
PUT /v3/{project_id}/instances/{instance_id}/public-ips/bind	gaussdbformysql:instance:bindPublicIp	-
PUT /v3/{project_id}/instances/{instance_id}/public-ips/unbind	gaussdbformysql:instance:unbindPublicIp	-
PUT /v3/{project_id}/instances/{instance_id}/switchover	gaussdbformysql:instance:switchover	-
PUT /v3/{project_id}/instances/{instance_id}/ops-window	gaussdbformysql:instance:modifyMaintenanceWindow	-
PUT /v3/{project_id}/instances/{instance_id}/security-group	gaussdbformysql:instance:modifySecurityGroup	-

API	对应的授权项	依赖的授权项
PUT /v3/{project_id}/instances/{instance_id}/internal-ip	gaussdbformysql:instance:modifyVip	-
PUT /v3/{project_id}/instances/{instance_id}/port	gaussdbformysql:instance:modifyPort	-
PUT /v3/{project_id}/instances/{instance_id}/alias	gaussdbformysql:instance:rename	-
DELETE /v3/{project_id}/backups/{backup_id}	gaussdbformysql:backup:delete	-
POST /v3.1/{project_id}/instances/{instance_id}/restore/tables	gaussdbformysql:instance:tableRestore	-
POST /v3/{project_id}/instances/restore	gaussdbformysql:instance:restoreInPlace	-
GET /v3/{project_id}/instances/{instance_id}/restore-time	gaussdbformysql:backup:getRestoreTime	-
PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/connection-pool-type	gaussdbformysql:proxy:switchConnectionPoolType	-

资源类型（Resource）

资源类型（Resource）表示身份策略所作用的资源。如**表5-126**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身份策略语句中指定该资源的URN，身份策略仅作用于此资源；如未指定，Resource默认为“*”，则身份策略将应用到所有资源。您也可以在身份策略中设置条件，从而指定资源类型。

TaurusDB定义了以下可以在自定义身份策略的Resource元素中使用的资源类型。

表 5-126 TaurusDB 支持的资源类型

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

条件（Condition）

TaurusDB服务不支持在SCP中的条件键中配置服务级的条件键。TaurusDB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。

5.10.8 安全与合规

5.10.8.1 DDoS 防护 AAD

5.10.8.1.1 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 5-127 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	-	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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: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5-128展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-128 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	-
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	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/antiddos	anti-ddos:ip:listDefenseStatuses	-
POST /v1/{project_id}/antiddos-ip/resource-instances/count	anti-ddos:ip:listDefenseStatuses	-
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	-

API	对应的授权项	依赖的授权项
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	-
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5-129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 5-129 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。

5.10.8.1.2 原生高级防护 CNAD

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CNAD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CNAD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CNAD的相关操作。

表 5-130 CNAD 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
cnad:schedule:update	授予更新调度规格的权限。	write	schedule *	-
cnad:schedule:list	授予查询调度规则列表的权限。	list	schedule *	-
cnad:schedule:get	授予查询调度规则的权限。	read	schedule *	-
cnad:schedule:delete	授予删除调度规则的权限。	write	schedule *	-
cnad:schedule:create	授予创建调度规则的权限。	write	schedule *	-
cnad:quota:update	授予修改配额的权限。	write	-	-
cnad:blockade:release	授予解封IP的权限。	write	-	-
cnad:blockade:list	授予查询封堵记录列表的权限。	list	-	-
cnad:blockade:get	授予查询封堵记录的权限。	read	-	-
cnad:alarmConfig:update	授予修改告警通知的权限。	write	-	-
cnad:alarmConfig:create	授予创建告警通知的权限。	write	-	-
cnad:alarmConfig:delete	授予删除告警通知的权限。	write	-	-
cnad:alarmConfig:get	授予查询告警通知的权限。	read	-	-
cnad:attackReport:list	授予查询攻击事件的权限。	list	-	-
cnad:attackReport:update	授予更新攻击事件配置的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
cnad:attackTop:list	授予查询Top10被攻击IP的权限。	list	-	-
cnad:attackTypeReport:list	授予查询攻击类型分布的权限。	list	-	-
cnad:bindPolicy:create	授予绑定防护策略到防护IP的权限。	write	-	-
cnad:blackWhiteIpList:create	授予创建IP黑白名单的权限。	write	-	-
cnad:blackWhiteIpList:delete	授予删除IP黑白名单的权限。	write	-	-
cnad:cleanCountReport:list	授予查询DDoS防护趋势的权限。	list	-	-
cnad:cleanKbpsReport:list	授予查询清洗流量峰值统计数据的权限。	list	-	-
cnad:cleanScaleDropList:list	授予查询清洗范围的权限。	list	-	-
cnad:countReport:get	授予查询统计数据的权限。	read	-	-
cnad:ipTag:put	授予更新防护IP标签的权限。	write	-	-
cnad:package:create	授予创建实例的权限。	write	package *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cnad:package:get	授予查询实例信息的权限。	read	package *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cnad:package:list	授予查询实例列表的权限。	list	package *	-
cnad:package:put	授予更新实例的权限。	write	package *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cnad:packageDropList:list	授予查询实例摘要列表的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
cnad:packetAttackReport:list	授予查询攻击数据包的权限。	list	-	-
cnad:policy:create	授予创建防护策略的权限。	write	policy *	g:EnterpriseProjectId
cnad:policy:delete	授予删除防护策略的权限。	write	policy *	g:EnterpriseProjectId
cnad:policy:get	授予查询单个防护策略详情的权限。	read	policy *	g:EnterpriseProjectId
cnad:policy:list	授予查询防护策略详情的权限。	list	policy *	-
cnad:policy:put	授予更新防护策略的权限。	write	policy *	g:EnterpriseProjectId
cnad:policyDropList:list	授予查询防护策略列表的权限。	list	-	-
cnad:protectedIp:create	授予绑定防护IP到实例的权限。	write	-	-
cnad:protectedIp:list	授予查询防护IP列表的权限。	list	-	-
cnad:protectedIpDropList:list	授予查询防护IP下拉列表的权限。	list	-	-
cnad:quota:get	授予查询配额的权限。	read	-	-
cnad:securityStatusReport:get	授予查询资产安全状态的权限。	read	-	-
cnad:trafficAttackReport:list	授予查询攻击流量的权限。	list	-	-
cnad:policy:unbind	授予移除防护IP的防护策略的权限。	write	-	-
cnad:weekStatisticsReport:get	授予查询每周安全统计数据的权限。	read	-	-

CNAD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/unblockservice/{domain_id}/unblock-quota-statistics	cnad:quota:get	-
POST /v1/unblockservice/{domain_id}/unblock	cnad:blockade:release	-
GET /v1/unblockservice/{domain_id}/unblock-record	cnad:blockade:list	-
GET /v1/unblockservice/{domain_id}/block-statistics	cnad:blockade:get	-
POST /v1/cnad/alarm-config	cnad:alarmConfig:update	-
DELETE /v1/cnad/alarm-config	cnad:alarmConfig:delete	-
GET /v1/cnad/alarm-config	cnad:alarmConfig:get	-
POST /v1/cnad/policies/{policy_id}/bind	cnad:bindPolicy:create	-
POST /v1/cnad/policies/{policy_id}/ip-list/add	cnad:blackWhiteIpList:create	-
POST /v1/cnad/policies/{policy_id}/ip-list/delete	cnad:blackWhiteIpList:delete	-
PUT /v1/cnad/protected-ips/tags	cnad:ipTag:put	-
GET /v1/cnad/packages	cnad:package:list	-
PUT /v1/cnad/packages/{package_id}/name	cnad:package:put	-

API	对应的授权项	依赖的授权项
POST /v1/cnad/policies	cnad:policy:create	-
DELETE /v1/cnad/policies/{policy_id}	cnad:policy:delete	-
GET /v1/cnad/policies/{policy_id}	cnad:policy:get	-
GET /v1/cnad/policies	cnad:policy:list	-
PUT /v1/cnad/policies/{policy_id}	cnad:policy:put	-
POST /v1/cnad/packages/{package_id}/protected-ips	cnad:protectedIp:create	-
GET /v1/cnad/protected-ips	cnad:protectedIp:list	-
GET /v1/cnad/packages/{package_id}/unbound-protected-ips	cnad:protectedIpDropList:list	-
POST /v1/cnad/policies/{policy_id}/unbind	cnad:policy:unbind	-

资源类型（Resource）

资源类型（Resource）表示SCP策略所作用的资源。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。

CNAD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 5-132 CNAD 支持的资源类型

资源类型	URN
policy	cnad::<account-id>:policy:<policy-id>
schedule	cnad::<account-id>:schedule:<schedule-id>
package	cnad::<account-id>:package:<package-id>

条件（Condition）

CNAD服务不支持在SCP策略中的条件键中配置服务级的条件键。

CNAD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。

5.10.8.1.3 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。

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 5-133 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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
aad:forwardingRule:delete	授予删除转发规则的权限。	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: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
aad:whiteBlackIpRule:list	授予查询防护黑白名单列表的权限。	list	whiteBlackIpRule *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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5-134**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-134 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	-
GET /v1/{project_id}/cad/instances/events	aad:dashboard:get	-
GET /v1/{project_id}/cad/ddosinfo/peak	aad:dashboard:get	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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5-135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 5-135 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。

5.10.8.2 数据加密服务 DEW

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DEW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DEW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DEW的相关操作。

表 5-136 KMS 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
kms:cmk:create	授予创建KMS密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
kms:cmk:list	授予查看用户所有KMS密钥信息的权限。	list	KeyId *	-
			-	g:EnterpriseProjectId
kms:cmk:enable	授予更改KMS密钥状态为已启用的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • 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
kms:cmk:disable	授予禁用KMS密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:get	授予查看KMS密钥的详细信息的权限。	read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:RequestAlias • kms:ResourceAliases
kms:cmk:createDataKey	授予使用KMS密钥生成数据密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext

授权项	描述	访问级别	资源类型（* 为必须）	条件键
kms:cmk:createDataKeyWithoutPlaintext	授予使用KMS密钥生成不包含明文版本数据密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext
kms:cmk:encryptDataKey	授予加密数据密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext
kms:cmk:decryptDataKey	授予解密数据密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • 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
			-	• kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext
kms:cmk:encryptData	授予使用指定的KMS密钥加密小数据的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:EncryptionAlgorithm • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext
kms:cmk:decryptData	授予使用指定的KMS密钥解密数据的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • 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
			-	• kms:EncryptionAlgorithm • kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext
kms::generateRandom	授予生成安全随机字符串的权限。	write	-	kms:RecipientAttestation
kms:cmk:sign	授予为生成数字签名的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:MessageType • kms:SigningAlgorithm • kms:RequestAlias • kms:ResourceAliases
kms:cmk:verify	授予使用指定的KMS密钥验证数字签名的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • 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
			-	• kms:MessageType • kms:SigningAlgorithm • kms:RequestAlias • kms:ResourceAliases
kms:cmk:generateMac	授予生成消息验证码的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:MessageType • kms:SigningAlgorithm • kms:RequestAlias • kms:ResourceAliases
kms:cmk:verifyMac	授予使用指定的KMS密钥验证消息验证码的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:MacAlgorithm • kms:RequestAlias • kms:ResourceAliases

授权项	描述	访问级别	资源类型（* 为必须）	条件键
kms:cmk:getPublicKey	授予查询KMS密钥公钥的权限。	read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:RequestAlias • kms:ResourceAliases
kms::getVersions	授予查询服务版本的权限。	read	-	-
kms::getVersion	授予查询服务密钥API版本的权限。	read	-	-
kms::getInstance	授予查询用户密钥实例个数的权限。	read	-	-
kms::getQuota	授予查询用户配额的权限。	read	-	-
kms:cmk:scheduleKeyDeletion	授予定时删除KMS密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	kms:ScheduleKeyDeletionPendingWindowInDays

授权项	描述	访问级别	资源类型（*为必须）	条件键
kms:cmk:cancelKeyDeletion	授予取消定时删除KMS密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:updateKeyAlias	授予更改密钥别名的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:updateKeyDescription	授予更改密钥描述的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:createGrant	授予给特定密钥创建授权的权限。	permission_management	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • 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
			-	• kms:GranteePrincipalType • kms:GrantOperations • kms:GranteePrincipal • kms:RetiringPrincipal
kms:cmk:listGrants	授予查询特定密钥已授权列表的权限。	list	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms::listRetirableGrants	授予查询密钥可退役授权列表的权限。	list	-	-
kms:cmk:retireGrant	授予给特定密钥退役授权的权限。	permission_management	KeyId *	g:ResourceTag/<tag-key>
kms:cmk:revokeGrant	授予给特定密钥撤销授权的权限。	permission_management	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • 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
kms:cmk:getMaterial	授予获取密钥导入参数的权限。	read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	kms:WrappingAlgorithm
kms:cmk:importMaterial	授予导入密钥材料的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	kms:ExpirationTime
kms:cmk:deleteMaterial	授予删除密钥材料的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • 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
kms:cmk:enableRotation	授予开启指定密钥轮换的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:updateRotation	授予更改指定密钥轮换周期的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:disableRotation	授予关闭密钥轮换的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:getRotation	授予查询指定密钥轮换状态的权限。	read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • 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
kms:cmk:createTag	授予给指定密钥添加标签的权限。	tagging	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
kms:cmk:createTags	授予给指定密钥批量添加或者删除密钥标签的权限。	tagging	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
kms:cmk:listKeysByTag	授予查询指定密钥实例的权限。	list	KeyId *	-
kms:cmk:deleteTag	授予删除指定密钥标签的权限。	tagging	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	g:TagKeys

授权项	描述	访问级别	资源类型（* 为必须）	条件键
kms:cmk:getTags	授予查询指定密钥标签的权限。	read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms::listAllTags	授予查询指定密钥项目标签的权限。	list	-	-
kms:cmk:replicate	授予复制KMS密钥的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:updatePrimaryRegion	授予更新主区域的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	kms:PrimaryRegion

授权项	描述	访问级别	资源类型（*为必须）	条件键
kms:alias:create	授予创建别名的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			alias *	-
kms:alias:delete	授予删除别名的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			alias *	-
kms:alias:list	授予查询别名列表的权限。	list	-	-
kms:alias:associate	授予关联别名的权限。	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			alias *	-

表 5-137 KPS 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
kps:SSHKeyPair:create	授予创建和导入SSH密钥对的权限。	write	SSHKeyPair *	• kps:KmsKeyId • kps:Algorithm
kps:SSHKeyPair:delete	授予删除SSH密钥对的权限。	write	SSHKeyPair *	-
kps:SSHKeyPair:get	授予查询SSH密钥对详细信息的权限。	read	SSHKeyPair *	-
kps:SSHKeyPair:list	授予查询SSH密钥对列表的权限。	list	SSHKeyPair *	-
kps:SSHKeyPair:update	授予更新SSH密钥对描述的权限。	write	SSHKeyPair *	-
kps:SSHKeyPair:bind	授予虚拟机绑定新SSH密钥对的权限。	write	SSHKeyPair *	-
kps::deleteFailedTask	授予删除失败任务的权限。	write	-	-
kps:SSHKeyPair:unbind	授予虚拟机解绑SSH密钥对的权限。	write	SSHKeyPair *	-
kps::getFailedTask	授予查询失败任务信息的权限。	list	-	-
kps::getTask	授予查询当前任务执行状态的权限。	list	-	-
kps::getRunningTask	授予查询正在处理的任务信息的权限。	list	-	-
kps:SSHKeyPair:importPrivateKey	授予导入私钥到密钥对的权限。	write	SSHKeyPair *	kps:KmsKeyId
kps:SSHKeyPair:exportPrivateKey	授予导出密钥对私钥的权限。	write	SSHKeyPair *	-
kps:SSHKeyPair:clearPrivateKey	授予清除密钥对私钥的权限。	write	SSHKeyPair *	-

表 5-138 CSMS 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
csms:secret:create	授予创建和恢复凭据的权限。	write	secretName *	• csms:Type • csms:KmsKeyId
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
csms:secret:delete	授予立即删除凭据的权限。	write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:update	授予更新凭据元数据信息的权限。	write	secretName *	• csms:Type • csms:KmsKeyId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:get	授予查询和下载凭据信息的权限。	read	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:list	授予查询当前用户在本项目下创建的所有凭据的权限。	list	secretName *	g:EnterpriseProjectId
csms:secret:createVersion	授予指定凭据中创建新凭据版本的权限。	write	secretName *	• csms:Type • 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
csms:secret:getVersion	授予查询指定凭据版本的信息和其明文凭据值的权限。	read	secretName*	• csms:Type • csms:VersionId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:listVersion	授予查询指定凭据下的版本列表信息的权限。	list	secretName*	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:createStage	授予创建凭据版本状态的权限。	write	secretName*	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:getStage	授予查询指定凭据版本状态标记的版本信息的权限。	read	secretName*	• csms:Type • csms:VersionStage • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:updateStage	授予更新凭据版本状态的权限。	write	secretName*	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:deleteStage	授予删除指定凭据版本状态的权限。	write	secretName*	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms::getSecretQuota	授予查询指定项目凭据配额的权限。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
csms:secret:scheduleDeletion	授予创建凭据定时删除任务的权限。	write	secretName*	• csms:Type • csms:RecoveryWindowInDays • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:restoreSecret	授予取消凭据定时删除任务的权限。	write	secretName*	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:rotate	授予轮转凭据的权限。	write	secretName*	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:getSecretsByTag	授予通过标签过滤，返回凭据列表的权限。	list	secretName*	-
csms:secret:batchCreateOrDeleteTags	授予批量添加或删除凭据标签的权限。	tagging	secretName*	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
csms:secret:createTag	授予添加凭据标签的权限。	tagging	secretName*	• csms:Type • g:EnterpriseProjectId • 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
csms:secret:deleteTag	授予删除凭据标签的权限。	tagging	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	g:TagKeys
csms:secret:listTags	授予查询凭据标签的权限。	list	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms::listProjectTags	授予查询用户在指定项目下的所有凭据标签集合的权限。	list	-	-
csms:secret:updateVersion	授予更新凭据版本有效期的权限。	write	secretName *	• csms:Type • csms:VersionId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms::createEvent	授予创建凭据事件的权限。	write	-	-
csms::listEvents	授予查询当前用户在本项目下创建的所有事件通知的权限。	list	-	-
csms::getEvent	授予查询指定事件通知信息的权限。	read	-	-
csms::updateEvent	授予更新指定事件通知的元数据信息的权限。	write	-	-
csms::deleteEvent	授予立即删除指定的事件通知的权限。	write	-	-
csms::listNotificationRecords	授予查询已触发事件通知记录的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
csms::listTasks	授予查询凭据轮转任务的权限。	List	-	-

表 5-139 DHSM 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
dhsm:hsm:get	授予查询密码机详细信息的权限。	read	DHSM	-
dhsm:hsm:getJobInfo	授予查询任务详细信息的权限。	read	DHSM	-
dhsm:cluster:getCsr	授予下载证书请求文件的权限。	read	DHSM	-
dhsm:cluster:getCert	授予查询集群证书的权限。	read	DHSM	-
dhsm::getPreCreatedInfo	授予查询加密机资源信息的权限。	read	DHSM	-
dhsm:hsm:delete	授予删除密码机详细信息的权限。	write	DHSM	-
dhsm:hsm:updateAlias	授予更新密码机信息的权限。	write	DHSM	-
dhsm:hsm:create	授予创建密码机的权限。	write	DHSM	-
dhsm:hsm:updateHsm	授予更新密码机信息的权限。	write	DHSM	-
dhsm:cluster:create	授予创建集群的权限。	write	DHSM	-
dhsm:cluster:update	授予更新集群的权限。	write	DHSM	-
dhsm:cluster:delete	授予删除集群的权限。	write	DHSM	-
dhsm:cluster:addVsm	授予批量添加密码机的权限。	write	DHSM	-
dhsm:cluster:updateCert	授予配置证书的权限。	write	DHSM	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dhsm:hsm:createInstallOrder	授予创建安装订单的权限。	write	DHSM	-
dhsm:hsm:createOrder	授予创建订单的权限。	write	DHSM	-
dhsm:hsm:inquiryResource	授予询价的权限。	read	DHSM	-
dhsm:hsm:list	授予查询密码机列表的权限。	list	DHSM	-
dhsm:cluster:list	授予查询集群的权限。	list	DHSM	-
dhsm:hsm:listHsmsByTag	授予查询加密机实例的权限。	list	DHSM	-
dhsm:hsm:getHsmTags	授予查询标签列表的权限。	list	DHSM	-
dhsm::listTags	授予查询hsm全部标签的权限。	list	DHSM	-
dhsm::listChargeSpecCode	授予查询规格编码的权限。	list	DHSM	-
dhsm:hsm:createTags	授予批量创建或者删除标签的权限。	tagging	DHSM	-
dhsm:hsm:createResourceTag	授予创建资源标签的权限。	tagging	DHSM	-
dhsm:hsm:deleteResourceTag	授予删除资源标签的权限。	tagging	DHSM	-

DEW的API通常对应着一个或多个授权项。**表 API与KMS操作项的关系**、**表 API与CSMS操作项的关系**、**表 API与KPS操作项的关系**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-140 API 与 KMS 授权项的关系

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/kms/create-key	kms:cmk:create	-
POST /v1.0/{project_id}/kms/list-keys	kms:cmk:list	-
POST /v1.0/{project_id}/kms/enable-key	kms:cmk:enable	-

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/kms/disable-key	kms:cmk:disable	-
POST /v1.0/{project_id}/kms/describe-key	kms:cmk:get	-
POST /v1.0/{project_id}/kms/create-datakey	kms:cmk:createDataKey	-
POST /v1.0/{project_id}/kms/create-datakey-without-plaintext	kms:cmk:createDataKeyWithoutPlaintext	-
POST /v1.0/{project_id}/kms/encrypt-datakey	kms:cmk:encryptDataKey	-
POST /v1.0/{project_id}/kms/decrypt-datakey	kms:cmk:decryptDataKey	-
POST /v1.0/{project_id}/kms/encrypt-data	kms:cmk:encryptData	-
POST /v1.0/{project_id}/kms/decrypt-data	kms:cmk:decryptData	-
POST /v1.0/{project_id}/kms/gen-random	kms::generateRandom	-
POST /v1.0/{project_id}/kms/sign	kms:cmk:sign	-
POST /v1.0/{project_id}/kms/verify	kms:cmk:verify	-
POST /v1.0/{project_id}/kms/get-publickey	kms:cmk:getPublicKey	-
GET /	kms::getVersions	-
GET /{version_id}	kms::getVersion	-
POST /v1.0/{project_id}/kms/schedule-key-deletion	kms:cmk:scheduleKeyDeletion	-
POST /v1.0/{project_id}/kms/cancel-key-deletion	kms:cmk:cancelKeyDeletion	-
GET /v1.0/{project_id}/kms/user-instances	kms::getInstance	-
GET /v1.0/{project_id}/kms/user-quotas	kms::getQuota	-
POST /v1.0/{project_id}/kms/update-key-alias	kms:cmk:updateKeyAlias	-

API	对应的授权项	依赖的授权项
POST /v1.0/{project_id}/kms/update-key-description	kms:cmk:updateKeyDescription	-
POST /v1.0/{project_id}/kms/create-grant	kms:cmk:createGrant	-
POST /v1.0/{project_id}/kms/list-grants	kms:cmk:listGrants	-
POST /v1.0/{project_id}/kms/list-retirable-grants	kms::listRetirableGrants	-
POST /v1.0/{project_id}/kms/retire-grant	kms:cmk:retireGrant	-
POST /v1.0/{project_id}/kms/revoke-grant	kms:cmk:revokeGrant	-
POST /v1.0/{project_id}/kms/get-parameters-for-import	kms:cmk:getMaterial	-
POST /v1.0/{project_id}/kms/import-key-material	kms:cmk:importMaterial	-
POST /v1.0/{project_id}/kms/delete-imported-key-material	kms:cmk:deleteMaterial	-
POST /v1.0/{project_id}/kms/enable-key-rotation	kms:cmk:enableRotation	-
POST /v1.0/{project_id}/kms/update-key-rotation-interval	kms:cmk:updateRotation	-
POST /v1.0/{project_id}/kms/disable-key-rotation	kms:cmk:disableRotation	-
POST /v1.0/{project_id}/kms/get-key-rotation-status	kms:cmk:getRotation	-
POST /v1.0/{project_id}/kms/{key_id}/tags	kms:cmk:createTag	-
POST /v1.0/{project_id}/kms/{key_id}/tags/action	kms:cmk:createTags	-
POST /v1.0/{project_id}/kms/{resource_instances}/action	kms:cmk:listKeysByTag	-
DELETE /v1.0/{project_id}/kms/{key_id}/tags/{key}	kms:cmk:deleteTag	-
GET /v1.0/{project_id}/kms/{key_id}/tags	kms:cmk:getTags	-

API	对应的授权项	依赖的授权项
GET /v1.0/{project_id}/kms/tags	kms::listAllTags	-
POST /v2/{project_id}/kms/keys/{key_id}/replicate	kms:cmk:replicate	-
PUT /v2/{project_id}/kms/keys/{key_id}/update-primary-region	kms:cmk:updatePrimaryRegion	-

表 5-141 API 与 CSMS 授权项的关系

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/secrets	csms:secret:create	kms:cmk:createDataKey
POST /v1/{project_id}/secrets/{secret_name}/backup	csms:secret:get	• kms:cmk:createDataKey • kms:cmk:decryptDataKey • kms:cmk:list
POST /v1/{project_id}/secrets/restore	csms:secret:create	kms:cmk:decryptDataKey
DELETE /v1/{project_id}/secrets/{secret_name}	csms:secret:delete	-
PUT /v1/{project_id}/secrets/{secret_name}	csms:secret:update	-
GET /v1/{project_id}/secrets/{secret_name}	csms:secret:get	-
GET /v1/{project_id}/secrets	csms:secret:list	-
POST /v1/{project_id}/secrets/{secret_name}/versions	csms:secret:createVersion	kms:cmk:createDataKey
GET /v1/{project_id}/secrets/{secret_name}/versions/{version_id}	csms:secret:getVersion	kms:cmk:decryptDataKey
GET /v1/{project_id}/secrets/{secret_name}/versions	csms:secret:listVersion	-
GET /v1/{project_id}/secrets/{secret_name}/stages/{stage_name}	csms:secret:getStage	-

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/secrets/{secret_name}/stages/{stage_name}	csms:secret:updateStage	-
DELETE /v1/{project_id}/secrets/{secret_name}/stages/{stage_name}	csms:secret:deleteStage	-
POST /v1/{project_id}/secrets/{secret_name}/scheduled-deleted-tasks/create	csms:secret:scheduleDeletion	-
POST /v1/{project_id}/secrets/{secret_name}/scheduled-deleted-tasks/cancel	csms:secret:restoreSecret	-
POST /v1/{project_id}/secrets/{secret_name}/rotate	csms:secret:rotate	• rds:password:update • kms:cmk:createGrant • kms:cmk:retireGrant
POST /v1/{project_id}/csms/{resource_instances}/action	csms:secret:getSecretsByTag	-
POST /v1/{project_id}/csms/{secret_id}/tags/action	csms:secret:batchCreateOrDeleteTags	-
POST /v1/{project_id}/csms/{secret_id}/tags	csms:secret:createTag	-
DELETE /v1/{project_id}/csms/{secret_id}/tags/{key}	csms:secret:deleteTag	-
GET /v1/{project_id}/csms/{secret_id}/tags	csms:secret:listTags	-
GET /v1/{project_id}/csms/tags	csms::listProjectTags	-
PUT /v1/{project_id}/secrets/{secret_name}/versions/{version_id}	csms:secret:updateVersion	-
POST /v1/{project_id}/csms/events	csms::createEvent	-
GET /v1/{project_id}/csms/events	csms::listEvents	-
GET /v1/{project_id}/csms/events/{event_name}	csms::getEvent	-
PUT /v1/{project_id}/csms/events/{event_name}	csms::updateEvent	-

API	对应的授权项	依赖的授权项
DELETE /v1/{project_id}/csms/events/{event_name}	csms::deleteEvent	-
GET /v1/{project_id}/csms/notification-records	csms::listNotificationRecords	-
GET /v1/{project_id}/csms/tasks	csms::listTasks	-

表 5-142 API 与 KPS 授权项的关系

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/keypairs	kps:SSHKeyPair:create	• kms:cmk:createDataKey • kms:cmk:list
DELETE /v3/{project_id}/keypairs/{keypair_name}	kps:SSHKeyPair:delete	-
GET /v3/{project_id}/keypairs/{keypair_name}	kps:SSHKeyPair:get	-
GET /v3/{project_id}/keypairs	kps:SSHKeyPair:list	-
PUT /v3/{project_id}/keypairs/{keypair_name}	kps:SSHKeyPair:update	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/keypairs/associate	kps:SSHKeyPair:bind	• ecs:cloudServers:createServers • ecs:cloudServers:deleteServers • ecs:cloudServers:showServer • ecs:cloudServers:attach • ecs:cloudServers:listServerBlockDevices • ecs:cloudServers:showServerBlockDevice • ecs:cloudServers:detachVolume • ecs:cloudServers:listServerInterfaces • ecs:cloudServers:listServersDetails • ecs:cloudServerFlavors:get • ecs:cloudServerQuotas:get • evs:types:get • evs:volumes:use • ims:images:get • vpc:subnets:list
DELETE /v3/{project_id}/failed-tasks	kps::deleteFailedTask	-
DELETE /v3/{project_id}/failed-tasks/{task_id}	kps::deleteFailedTask	-

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/keypairs/disassociate	kps:SSHKeyPair:unbind	• ecs:cloudServers:createServers • ecs:cloudServers:deleteServers • ecs:cloudServers:showServer • ecs:cloudServers:attach • ecs:cloudServers:listServerBlockDevices • ecs:cloudServers:showServerBlockDevice • ecs:cloudServers:detachVolume • ecs:cloudServers:listServerInterfaces • ecs:cloudServers:listServersDetails • ecs:cloudServerFlavors:get • ecs:cloudServerQuotas:get • evs:types:get • evs:volumes:use • ims:images:get • vpc:subnets:list
GET /v3/{project_id}/failed-tasks	kps::getFailedTask	-
GET /v3/{project_id}/tasks/{task_id}	kps::getTask	-
GET /v3/{project_id}/running-tasks	kps::getRunningTask	-
POST /v3/{project_id}/keypairs/private-key/import	kps:SSHKeyPair:importPrivateKey	• kms:cmk:createDataKey • kms:cmk:list
POST /v3/{project_id}/keypairs/private-key/export	kps:SSHKeyPair:exportPrivateKey	kms:cmk:decryptDataKey

API	对应的授权项	依赖的授权项
POST /v3/{project_id}/keypairs/batch-associate	kps:SSHKeyPair:bind	• ecs:cloudServers:createServers • ecs:cloudServers:deleteServers • ecs:cloudServers:showServer • ecs:cloudServers:attach • ecs:cloudServers:listServerBlockDevices • ecs:cloudServers:showServerBlockDevice • ecs:cloudServers:detachVolume • ecs:cloudServers:listServerInterfaces • ecs:cloudServers:listServersDetails • ecs:cloudServerFlavors:get • ecs:cloudServerQuotas:get • evs:types:get • evs:volumes:use • ims:images:get • vpc:subnets:list
DELETE /v3/{project_id}/keypairs/{keypair_name}/private-key	kps:SSHKeyPair:clearPrivateKey	-

表 5-143 API 与 DHSM 授权项的关系

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/dew/hsms/{hsm_id}	dhsm:hsm:get	-
GET /v1/{project_id}/dew/hsms/jobs/{job_id}	dhsm:hsm:getJobInfo	-
GET /v1/{project_id}/dew/clusters/{cluster_id}/csr	dhsm:cluster:getCsr	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/dew/clusters/{cluster_id}/cert	dhsm:cluster:getCert	-
GET /v1/{project_id}/dew/resources	dhsm::getPreCreatedInfo	-
DELETE /v1/{project_id}/dew/hsms/{hsm_id}	dhsm:hsm:delete	-
PUT /v1/{project_id}/dew/hsms/{hsm_id}	dhsm:hsm:updateAlias	-
POST /v1/{project_id}/dew/hsms	dhsm:hsm:create	-
PUT /v1/{project_id}/dew/hsms/{hsm_id}	dhsm:hsm:updateHsm	-
POST /v1/{project_id}/dew/clusters	dhsm:cluster:create	-
PUT /v1/{project_id}/dew/clusters/{cluster_id}	dhsm:cluster:update	-
DELETE /v1/{project_id}/dew/clusters/{cluster_id}	dhsm:cluster:delete	-
POST /v1/{project_id}/dew/clusters/{cluster_id}/vsms	dhsm:cluster:addVsm	-
POST /v1/{project_id}/dew/clusters/{cluster_id}/cert	dhsm:cluster:updateCert	-
POST /v1/{project_id}/dew/install-order	dhsm:hsm:createInstallOrder	-
POST /v1/{project_id}/dew/order	dhsm:hsm:createOrder	-
POST /v1/dew/inquiry/resource	dhsm:hsm:inquiryResource	-
GET /v1/{project_id}/dew/hsms	dhsm:hsm:list	-
GET /v1/{project_id}/dew/clusters	dhsm:cluster:list	-
POST /v1/{project_id}/hsm/{resource_instances}/action	dhsm:hsm:listHsmsByTag	-
GET /v1/{project_id}/hsm/{resource_id}/tags	dhsm:hsm:getHsmTags	-
GET /v1/{project_id}/hsm/tags	dhsm::listTags	-
GET /v1/dew/spec-codes	dhsm::listChargeSpecCode	-

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/hsm/{resource_id}/tags/action	dhsm:hsm:createTags	-
POST /v1/{project_id}/hsm/{resource_id}/tags	dhsm:hsm:createResourceTag	-
DELETE /v1/{project_id}/hsm/{resource_id}/tags/{key}	dhsm:hsm:deleteResourceTag	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表 DEW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中设置条件键，从而定义资源类型。

DEW定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-144 DEW 支持的资源类型

资源类型	URN
KeyId	kms:<region>:<account-id>:KeyId:<cmk-id>
alias	kms:<region>:<account-id>:alias:<alias-name>
secretName	csms:<region>:<account-id>:secretName:<secret-name>
dhsm	dhsm:<region>:<account-id>:hsm:<hsm-id>
cluster	dhsm:<region>:<account-id>:cluster:<cluster-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（前缀通常为服务缩写，如DEW:）仅适用于对应服务的操作，详情请参见**表 DEW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。

DEW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。

说明

KPS服务不支持在身份策略中的条件键中配置服务级的条件键。

表 5-145 DEW 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
kms:EncryptionAlgorithm	string	单值	根据请求中的加解密算法的值过滤对加解密操作的访问。
kms:GranteePrincipalType	string	单值	根据请求中的授权主体类型约束过滤对CreateGrant操作的访问。
kms:GrantOperations	string	多值	根据需要授权的操作过滤对CreateGrant操作的访问权限。
kms:GranteePrincipal	string	单值	根据授权中的被授权方主体过滤对CreateGrant操作的访问权限。
kms:KeyOrigin	string	单值	根据创建或使用操作KMS密钥的origin属性过滤对API操作的访问。
kms:KeySpec	string	单值	根据创建或使用操作KMS密钥的key_spec属性过滤对API操作的访问。
kms:KeyUsage	string	单值	根据创建或使用操作KMS密钥的key_usage属性过滤对API操作的访问。
kms:MessageType	string	单值	根据请求中的message_type参数的值过滤对签名和验证签名操作的访问。
kms:RetiringPrincipal	string	单值	根据授权中的retiring_principal筛选对CreateGrant操作的访问。
kms:SigningAlgorithm	string	单值	根据请求中的signing_algorithm过滤对签名和验证操作的访问。
kms:ExpirationTime	date	单值	根据请求中的expiration_time参数的值过滤对ImportKeyMaterial操作的访问。
kms:WrappingAlgorithm	string	单值	根据请求中的wrapping_algorithm参数的值过滤对CreateParametersForImport操作的访问。
kms:RecipientAttestation	string	单值	根据请求中证明文档的平台配置寄存器（PCR）值控制CreateDatakey、DecryptData、DecryptDatakey和CreateRandom操作的访问。

服务级条件键	类型	单值/多值	说明
kms:MacAlgorithm	string	单值	根据请求中的mac_algorithm过滤对生成/校验消息验证码操作的访问。
kms:RequestAlias	string	单值	根据请求中的key_id属性过滤对API操作的访问。
kms:ResourceAliases	string	多值	根据使用操作KMS密钥的alias属性过滤对API操作的访问。
kms:MultiRegionKeyType	string	单值	根据使用操作KMS密钥的多区域密钥类型属性过滤对API操作的访问。
kms:PrimaryRegion	string	单值	根据请求中的primary_region属性过滤对API操作的访问。
kms:EncryptionContext	string	单值	根据请求中的additional_authenticated_data属性过滤对API操作的访问。
kms:ScheduleKeyDeletionPendingWindowInDays	numeric	单值	根据请求中的pending_days属性过滤对API操作的访问。
csms:Type	string	单值	根据凭据的类型筛选访问权限。
csms:KmsKeyId	string	单值	根据KMS密钥ID筛选访问权限。
csms:VersionId	string	单值	根据凭据版本ID筛选访问权限。
csms:VersionStage	string	单值	根据凭据版本状态筛选访问权限。
csms:RecoveryWindowInDays	numeric	单值	根据凭据删除等待时间筛选访问权限。
kps:KmsKeyId	string	单值	根据请求中的kms密钥的ID过滤访问权限。
kps:Algorithm	string	单值	根据请求中的SSH密钥对密钥算法过滤访问权限。

5.10.8.3 企业主机安全 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 5-146 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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	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
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:listSwrlmageRepository	授予权限以查询swr镜像仓库镜像列表。	list	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
			-	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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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5-147展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-147 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
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

API	对应的授权项	依赖的授权项
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
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

API	对应的授权项	依赖的授权项
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
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

API	对应的授权项	依赖的授权项
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
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

API	对应的授权项	依赖的授权项
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
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

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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5-148**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 5-148 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。

5.10.8.4 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 5-149 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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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5-150**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-150 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5-151**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 5-151 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。

5.10.8.5 云防火墙 CFW

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 5-152 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:LogGroupId

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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:LogGroupId
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>

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
cfw:instance:deleteInstance	授予删除云防火墙实例的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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成员列表的权限。	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 *	-

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: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	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:listAccounts	授予查看多账号列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listOrganizationTree	授予查看组织树的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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:instance:listReportProfile	授予查看防火墙周报模板列表的权限。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:createReportProfile	授予创建防火墙周报模板的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateReportProfile	授予更新防火墙周报模板的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getReportProfile	授予查看防火墙周报模板的权限。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:deleteReportProfile	授予删除防火墙周报模板的权限。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

CFW的API通常对应着一个或多个授权项。**表5-153**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-153 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:instances:listVpcAttachments • 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	-
GET /v1/{project_id}/firewall/east-west	cfw:instance:getEw	• er:instances:listVpcAttachments • vpc:vpcs:list • nat:natGateways:list • er:instances:listVpcAttachments • er:instances:get
POST /v2/{project_id}/cfw-cfw/{fw_instance_id}/tags/create	cfw:instance:createTags	-

API	对应的授权项	依赖的授权项
DELETE /v2/{project_id}/cfw-cfw/{fw_instance_id}/tags/delete	cfw:instance:deleteTags	-
GET /v1/{project_id}/capture-task	cfw:instance:listCaptureTask	-
POST /v1/{project_id}/capture-task	cfw:instance:createCaptureTask	-
POST /v1/{project_id}/capture-task/stop	cfw:instance:stopCaptureTask	-
POST /v1/{project_id}/capture-task/batch-delete	cfw:instance:deleteCaptureTask	-
GET /v1/{project_id}/capture-task/capture-result	cfw:instance:getCaptureTaskResult	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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/{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	-
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5-154**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 5-154 CFW 支持的资源类型

资源类型	URN
blackWhiteList	cfw:<region>:<account-id>:blackWhiteList:<blackWhiteList-id>
acl	cfw:<region>:<account-id>:acl:<acl-id>
instance	cfw:<region>:<account-id>:instance:<fwInstance-id>
serviceGroup	cfw:<region>:<account-id>:serviceGroup:<serviceGroup-id>
domainGroup	cfw:<region>:<account-id>:domainGroup:<domainGroup-id>
ipGroup	cfw:<region>:<account-id>:ipGroup:<ipGroup-id>
eip	cfw:<region>:<account-id>:eip:<eip-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cfw:）仅适用于对应服务的操作，详情请参见**表5-155**。
  - 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。

CFW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 5-155 CFW 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
cfw:LogGroupId	string	单值	根据请求参数中指定的LTS日志组ID过滤访问。

5.10.8.6 数据安全中心 DSC

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DSC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DSC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DSC的相关操作。

表 5-156 DSC 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
dsc:asset:delete	授予权限以删除数据资产。	write	asset *	-
dsc:asset:list	授予权限以查询数据资产列表。	list	asset *	-
dsc:asset:create	授予权限以添加数据资产。	write	asset *	-
dsc:asset:update	授予权限以更新数据资产信息。	write	asset *	-
dsc:maskTask:operate	授予权限以操作脱敏任务（启动、停止、开启、关闭等）。	write	maskTask *	-
dsc:maskTask:listSubTasks	授予权限以查询脱敏任务的子任务列表。	list	maskTask *	-
dsc:common:operate	授予权限以操作DSC通用资源。	write	-	-
dsc:common:list	授予权限以查询DSC通用资源列表。	list	-	-
dsc:scanTask:create	授予权限以创建敏感数据扫描任务。	write	scanTask *	-
dsc:scanTask:list	授予权限以查询敏感数据扫描任务列表或子任务列表。	list	scanTask *	-
dsc:scanTask:getResults	授予权限以查询单个扫描任务的扫描结果。	read	scanTask *	-
dsc:scanRuleGroup:list	授予权限以查询扫描规则组列表。	list	-	-
dsc:scanRuleGroup:create	授予权限以创建扫描规则组。	write	-	-
dsc:scanRuleGroup:delete	授予权限以删除扫描规则组。	write	-	-
dsc:scanRule:list	授予权限以查询扫描规则列表。	list	scanRule *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dsc:scanRule:create	授予权限以创建扫描规则。	write	scanRule *	-
dsc:scanRule:update	授予权限以更新扫描规则。	write	scanRule *	-
dsc:scanRule:delete	授予权限以删除扫描规则。	write	scanRule *	-
dsc:watermark:embed	授予权限以对文档、图片或者数据库嵌入水印。	write	-	-
dsc:watermark:extract	授予权限以从文档、图片或者数据库中提取水印。	write	-	-

DSC的API通常对应着一个或多个授权项。表5-157展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-157 API 与授权项的关系

API	对应的授权项	依赖的授权项
DELETE/v1/{project_id}/sdg/asset/obs/bucket/{bucket_id}	dsc:asset:delete	obs:bucket:GetBucketLogging
		obs:bucket:PutBucketLogging
GET/v1/{project_id}/sdg/asset/obs/buckets	dsc:asset:list	obs:bucket:listAllMyBuckets
POST/v1/{project_id}/sdg/asset/obs/buckets	dsc:asset:create	obs:bucket:GetBucketStorage
		obs:bucket:listAllMyBuckets
PUT/v1/{project_id}/sdg/asset/{asset_id}/name	dsc:asset:update	-
POST/v1/{project_id}/period/order	dsc:common:operate	bss:renewal:update
		bss:order:update

API	对应的授权项	依赖的授权项
GET/v1/{project_id}/period/product/specification	dsc:common:list	-
POST/v1/{project_id}/sdg/server/mask/dbs/templates/{template_id}/operation	dsc:maskTask:operate	-
GET/v1/{project_id}/sdg/server/mask/dbs/templates/{template_id}/tasks	dsc:maskTask:listSubTasks	-
PUT/v1/{project_id}/sdg/smn/topic	dsc:common:operate	-
GET/v1/{project_id}/sdg/smn/topics	dsc:common:list	smn:topic:list
GET/v1/{project_id}/openapi/called-records	dsc:common:list	-
POST/v1/{project_id}/sdg/scan/job	dsc:scanTask:create	-
GET/v1/{project_id}/sdg/scan/jobs	dsc:scanTask:list	-
GET/v1/{project_id}/sdg/server/scan/groups	dsc:scanRuleGroup:list	-
POST/v1/{project_id}/sdg/server/scan/groups	dsc:scanRuleGroup:create	-
DELETE/v1/{project_id}/sdg/server/scan/groups/{group_id}	dsc:scanRuleGroup:delete	-
GET/v1/{project_id}/sdg/server/scan/rules	dsc:scanRule:list	-

API	对应的授权项	依赖的授权项
POST/v1/{project_id}/sdg/server/scan/rules	dsc:scanRule:create	-
PUT/v1/{project_id}/sdg/server/scan/rules	dsc:scanRule:update	-
DELETE/v1/{project_id}/sdg/server/scan/rules/{rule_id}	dsc:scanRule:delete	-
GET/v1/{project_id}/sdg/scan/job/{job_id}/results	dsc:scanTask:getResults	-
GET/v1/{project_id}/sdg/server/relation/jobs/{job_id}/dbs	dsc:common:list	-
GET/v1/{project_id}/sdg/server/relation/jobs/{job_id}/dbs/{db_id}/tables	dsc:common:list	-
GET/v1/{project_id}/sdg/server/relation/jobs/{job_id}/dbs/{table_id}/columns	dsc:common:list	-
GET/v1/{project_id}/sdg/server/relation/jobs/{job_id}/obs/buckets	dsc:common:list	-
GET/v1/{project_id}/sdg/server/relation/jobs/{job_id}/obs/{bucket_id}/files	dsc:common:list	-
POST/v1/{project_id}/data/mask	dsc:sensitiveData:mask	-

API	对应的授权项	依赖的授权项
POST/v1/{project_id}/doc-address/watermark/embed	dsc:watermark:embed	-
POST/v1/{project_id}/doc-address/watermark/extract	dsc:watermark:extract	-
POST/v1/{project_id}/image-address/watermark/embed	dsc:watermark:embed	-
POST/v1/{project_id}/image-address/watermark/extract	dsc:watermark:extract	-
POST/v1/{project_id}/image-address/watermark/extract-image	dsc:watermark:extract	-
POST/v1/{project_id}/image/watermark/embed	dsc:watermark:embed	-
POST/v1/{project_id}/image/watermark/extract	dsc:watermark:extract	-
POST/v1/{project_id}/image/watermark/extract-image	dsc:watermark:extract	-
POST/v1/{project_id}/sdg/database/watermark/embed	dsc:watermark:embed	-
POST/v1/{project_id}/sdg/database/watermark/extract	dsc:watermark:extract	-
POST/v1/{project_id}/sdg/doc/watermark/embed	dsc:watermark:embed	-

API	对应的授权项	依赖的授权项
POST/v1/{project_id}/sdg/doc/watermark/extract	dsc:watermark:extract	-
GET/v1/{project_id}/sdg/asset/{asset_type}/{asset_id}/detail	dsc:common:list	-

资源类型（Resource）

资源类型（Resource）表示SCP策略所作用的资源。如表5-158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。

DSC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 5-158 DSC 支持的资源类型

资源类型	URN
scanTask	dsc:<region>:<account-id>:scanTask:<task-id>
scanRule	dsc:<region>:<account-id>:scanRule:<rule-id>
scanTemplate	dsc:<region>:<account-id>:scanTemplate:<template-id>
maskTask	dsc:<region>:<account-id>:maskTask:<task-id>
asset	dsc:<region>:<account-id>:asset:<asset-id>

条件（Condition）

DSC服务不支持在SCP策略中的条件键中配置服务级的条件键。

DSC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。

5.10.8.7 私有证书管理 PCA

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 5-159 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
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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	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>
			-	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>

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
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 *	-
			-	• 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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	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 5-160 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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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 5-161 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 5-162 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。

5.10.8.8 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 5-163 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:DomainNames • scm:ValidationMethod • scm:KeyAlgorithm
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:DomainNames • scm:ValidationMethod
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:DomainNames
scm:cert:expandQuota	授予权限扩容证书配额。	write	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
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>
			-	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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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>
			-	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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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>
			-	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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	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>
			-	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 5-164 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	-

API	对应的授权项	依赖的授权项
DELETE /v3/scm/certificates/{certificate_id}	scm:cert:delete	-
POST /v3/scm/certificates/{certificate_id}/read	scm:cert:getApplicationInfo	-
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 5-165 SCM 支持的资源类型

资源类型	URN
cert	scm:<region>:<account-id>:cert:<cert-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scm:）仅适用于对应服务的操作，详情请参见表5-166。
  - 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。

SCM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 5-166 SCM 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
scm:DomainNames	string	多值	根据请求参数中的域名过滤访问。
scm:ValidationMethod	string	单值	根据请求参数中的验证方式过滤访问。
scm:KeyAlgorithm	string	单值	根据请求参数中的密钥算法过滤访问。

5.10.8.9 云堡垒机 CBH

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CBH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CBH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CBH的相关操作。

表 5-167 CBH 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	别名
cbh::listAvailableZones	授予查询服务可用区的权限。	List	-	-	-
cbh::getEcsQuota	授予查询ECS资源配额的权限。	Read	-	-	-
cbh::getQuota	授予查询堡垒机实例配额的权限。	Read	-	-	-
cbh::listSpecifications	授予查询堡垒机规格的权限。	List	-	-	-
cbh:instance:listInstances	授予查询堡垒机列表的权限。	List	instance *	-	-
cbh:instance:getInstanceStatus	授予查询堡垒机状态的权限。	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	别名
cbh:instance:startInstance	授予启动堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:stopInstance	授予关闭堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:rebootInstance	授予重启堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:upgradeInstance	授予升级堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:loginInstance	授予以IAM用户登录堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:resetInstancePassword	授予重置堡垒机密码的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:resetInstanceLoginMethod	授予重置堡垒机登录方式的权限。	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	别名
cbh:instance:deleteInstance	授予删除故障堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:alterInstance	授予变更堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:createInstance	授予创建堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:RequestTag/tag-key • g:TagKeys • cbh:VpcId • cbh:SubnetId • cbh:AllowBindPublicIp	-
cbh:instance:bindInstanceEip	授予为堡垒机绑定EIP的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:unbindInstanceEip	授予为堡垒机解绑EIP的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:updateInstanceSecurityGroup	授予更新堡垒机安全组的权限。	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	别名
cbh::operateAuthorization	授予创建或取消堡垒机服务委托授权的权限。	Write	-	-	-
cbh::getAuthorization	授予获取租户给堡垒机服务委托授权信息的权限。	Read	-	-	-
cbh::listTags	授予查询全部标签的权限。	List	-	-	-
cbh:instance:getInstanceTags	授予查询堡垒机实例资源的标签信息的权限。	Read	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:countInstancesByTag	授予统计符合标签条件的实例数量的权限。	List	instance *	-	-
cbh:instance:listInstancesByTag	授予使用标签过滤实例的权限。	List	-	-	-
cbh:instance:operateInstanceTags	授予操作堡垒机实例资源标签的权限。	Tagging	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key • g:RequestTag/tag-key • g:TagKeys	-
cbh:instance:getOmUrl	授予获取堡垒机内资产运维链接的权限。	Read	instance *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	cbh:instance:getOmUrl

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
cbh:instance:rollbackInstance	授予回滚堡垒机的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	cbh:instance:upgrade
cbh:instance:migrateInstanceTraffic	授予迁移堡垒机流量的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	cbh:instance:upgrade
cbh:instance:switchInstanceVpc	授予切换堡垒机实例虚拟私有云的权限。	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • cbh:VpcId • cbh:SubnetId	-

cbh的API通常对应着一个或多个操作项。表5-168展示了API与操作项的关系，以及该API需要依赖的操作项。

表 5-168 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}/cbs/available-zone	cbh::listAvailableZones	-
	cbh::getEcsQuota	ecs:cloudServerFlavors:get
	cbh::getQuota	-
GET /v2/{project_id}/cbs/instance/specification	cbh::listSpecifications	-
GET /v2/{project_id}/cbs/instance/list	cbh:instance:listInstances	eps:enterpriseProjects:list
	cbh:instance:getInstanceStatus	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/cbs/instance/start	cbh:instance:startInstance	-
POST /v2/{project_id}/cbs/instance/stop	cbh:instance:stopInstance	-
	cbh:instance:rebootInstance	-
POST /v2/{project_id}/cbs/instance/upgrade	cbh:instance:upgradeInstance	-
POST /v2/{project_id}/cbs/instance/login	cbh:instance:loginInstance	-
PUT /v2/{project_id}/cbs/instance/password	cbh:instance:resetInstancePassword	-
PUT /v2/{project_id}/cbs/instance/login-method	cbh:instance:resetInstanceLoginMethod	-
DELETE /v2/{project_id}/cbs/instance	cbh:instance:deleteInstance	-
	cbh:instance:alterInstance	evs:quotas:get
POST /v2/{project_id}/cbs/instance	cbh:instance:createInstance	• vpc:quotas:list • vpc:subnets:list • vpc:subnets:get • vpc:securityGroups:list • ecs:cloudServerFlavors:get
	cbh:instance:bindInstanceEip	-
	cbh:instance:unbindInstanceEip	-
PUT /v2/{project_id}/cbs/instance/{server_id}/security-groups	cbh:instance:updateInstanceSecurityGroup	vpc:ports:update
	cbh::operateAuthorization	-
GET /v2/{project_id}/cbs/agency/authorization	cbh::getAuthorization	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/cbs/instance/tags	cbh::listTags	-
GET /v2/{project_id}/cbs/instance/{resource_id}/tags	cbh:instance:getInstanceTags	-
POST /v2/{project_id}/cbs/instance/count	cbh:instance:countInstancesByTag	-
POST /v2/{project_id}/cbs/instance/filter	cbh:instance:listInstancesByTag	-
	cbh:instance:operateInstanceTags	-
POST /v2/{project_id}/cbs/instance/{server_id}/eip/bind	cbh:instance:bindInstanceEip	• eip:publicIps:list • eip:publicIps:update
POST /v2/{project_id}/cbs/instance/{server_id}/eip/unbind	cbh:instance:unbindInstanceEip	• eip:publicIps:update • eip:publicIps:list
GET /v2/{project_id}/cbs/instance/ecs-quota	cbh::getEcsQuota	ecs:cloudServerFlavors:get
GET /v2/{project_id}/cbs/instance/quota	cbh::getQuota	-
GET /v2/{project_id}/cbs/instance/{server_id}/status	cbh:instance:getInstanceStatus	-
POST /v2/{project_id}/cbs/instance/reboot	cbh:instance:rebootInstance	-
PUT /v2/{project_id}/cbs/instance	cbh:instance:alterInstance	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/cbs/agency/authorization	cbh::operateAuthorization	-
POST /v2/{project_id}/cbs/instance/{resource_id}/tags/action	cbh:instance:operateInstanceTags	-
GET /v2/{project_id}/cbs/instance/get-om-url	cbh:instance:getOmUrl	-
	cbh:instance:migrateInstanceTraffic	-
POST /v2/{project_id}/cbs/instance/rollback	cbh:instance:rollbackInstance	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-169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。

CBH定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-169 CBH 支持的资源类型

资源类型	URN
instance	cbh:<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cbh:）仅适用于对应服务的操作，详情请参见表5-170。
  - 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。

CBH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 5-170 CBH 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
cbh:VpcId	string	单值	根据堡垒机实例通信的VPCID开启过滤访问。
cbh:SubnetId	string	单值	根据堡垒机实例通信的子网ID开启过滤访问。
cbh:AllowBindPublicIp	boolean	单值	根据堡垒机实例是否可以绑定公网IP开启权限。

5.10.8.10 数据库安全服务 DBSS

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DBSS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DBSS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DBSS的相关操作。

表 5-171 dbss 支持的授权项

操作项	描述	访问级别	资源类型（*为必须）	条件键
dbss:auditInstance:listSqlInjectRules	授予权限以查询SQL注入规则。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listSqls	授予权限以获取审计结果信息。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:switchSqlInjectRule	授予权限以开启或关闭sql注入策略。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:addSqlInjectRule	授予权限以添加自定义sql注入规则。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:orderSqlInjectRule	授予权限以对sql规则优先级进行排序。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:createReporter	授予权限以立即生成报表。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listReporters	授予权限以查询报表信息。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:getRiskRuleDetail	授予权限以查询指定风险规则策略。	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listAlarmEmails	授予权限以查询告警邮件信息。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-

操作项	描述	访问级别	资源类型（*为必须）	条件键
dbss:auditInstance:downloadReporter	授予权限以下载报表。	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listAuditScopeRules	授予权限以查询审计范围策略列表。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:addSensitiveRule	授予权限以添加隐私数据保护规则。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:editSensitiveRule	授予权限以编辑隐私数据保护规则。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:deleteReporter	授予权限以删除报表。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listOperateLog	授予权限以查询用户操作日志信息。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listMonitorInfos	授予权限以查询审计实例监控信息。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listSessionInfo	授予权限以查询审计实例会话信息。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:switchBackup	授予权限以开启或关闭备份功能。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss::downloadLicense	授予权限以下载销售许可证。	read	-	-
dbss::deleteAuditInstanceJob	授予权限以删除审计实例创建失败的任务。	write	-	-

操作项	描述	访问级别	资源类型（*为必须）	条件键
dbss::listRdsDb	授予权限以查询RDS数据库。	list	-	-
dbss:auditInstance:instanceStart	授予权限以开启审计实例。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:reboot	授予权限以重启审计实例。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:stop	授予权限以关闭审计实例。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:upgrade	授予权限以升级审计实例。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss::queryUpgradeStatus	授予权限以查询审计实例升级状态。	list	-	-
dbss:auditInstance:updateSecurityGroup	授予权限以修改审计实例安全组。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:modifyAttribute	授予权限以修改审计实例审计属性。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:downloadAgent	授予权限以下载agent。	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:switchAgent	授予权限以开启或关闭Agent。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listAgents	授予权限以获取agent列表。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-

操作项	描述	访问级别	资源类型（*为必须）	条件键
dbss:auditInstance:deleteAgent	授予权限以删除agent。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:addAgent	授予权限以添加agent。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:previewReporter	授予权限以预览报表。	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:setAlarmConfig	授予权限以配置告警信息。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:configAlarmEmail	授予权限以配置告警邮件信息。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:getAlarmConfig	授予权限以查询告警配置信息。	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listRiskRules	授予权限以查询风险规则策略。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:exportInstancesDatabaseConfig	授予权限以导出数据库配置。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:createOnPeriod	授予权限以包年包月计费模式创建审计实例。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys

操作项	描述	访问级别	资源类型（*为必须）	条件键
dbss:auditInstance:editSqlInjectRule	授予权限以编辑自定义sql注入规则。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:deleteSqlInjectRule	授予权限以删除自定义sql注入规则。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:deleteSensitiveRule	授予权限以删除隐私数据保护规则。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:deleteAuditScopeRule	授予权限以删除审计范围规则。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:deleteRiskRule	授予权限以删除风险规则。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:deleteBackup	授予权限以删除本地备份信息。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listBackups	授予权限以查询备份信息。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:getBackupConfig	授予权限以获取备份配置信息。	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:editAuditScopeRule	授予权限以编辑审计范围规则。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:instanceList	授予权限以查询审计实例信息。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-

操作项	描述	访问级别	资源类型（*为必须）	条件键
dbss:auditInstance:createOnDemand	授予权限以按需模式创建审计实例。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
dbss::listCommonInfo	授予权限以查询公共信息。	list	-	-
dbss:auditInstance:listInstancesSummaryInfo	授予权限以查询所有审计实例总览信息。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss::getauditInstancesSummaryTaskStatus	授予权限以查询总览任务状态。	read	-	-
dbss::updateAuditInstancesSummaryInfo	授予权限以更新所有审计实例总览信息。	write	-	-
dbss:auditInstance:setReporterConfig	授予权限以更改报表的计划任务配置信息。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:getReporterConfig	授予权限以获取报表的计划任务配置信息。	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:addBareDatabase	授予权限以添加自建数据库。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listDatabases	授予权限以查询数据库列表。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-

操作项	描述	访问级别	资源类型（*为必须）	条件键
dbss:auditInstance:switchDatabase	授予权限以开启关闭数据库审计功能。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:deleteDatabase	授予权限以删除数据库。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:addAuditScopeRule	授予权限以添加审计范围规则。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:switchAuditScopeRule	授予权限以开启关闭审计范围规则。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:addRiskRule	授予权限以添加风险规则。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:switchRiskRule	授予权限以开启或关闭风险规则。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:editRiskRule	授予权限以编辑风险规则。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:setRiskRulePriority	授予权限以设置风险规则优先级。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listStatistics	授予权限以查询审计实例概览信息。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listSensitiveRules	授予权限以查询隐私数据脱敏规则。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-

操作项	描述	访问级别	资源类型（*为必须）	条件键
dbss:auditInstance:modifySensitiveRuleSaveResultSwitch	授予权限以开启关闭存储结果集开关。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:modifySensitiveRuleAnonymizeSwitch	授予权限以开启关闭隐私数据脱敏开关。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:switchSensitiveRule	授予权限以开启或关闭隐私数据保护规则。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listAlarmItems	授予权限以查询告警信息。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:markAlarm	授予权限以标记告警信息。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:deleteAlarm	授予权限以删除告警信息。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:restoreBackup	授予权限以恢复备份信息。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:retryBackup	授予权限以重试备份操作。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:getRiskBackupConfigInfo	授予权限以获取风险导出配置信息。	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:switchRiskBackup	授予权限以开启关闭风险导出功能。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-

操作项	描述	访问级别	资源类型（*为必须）	条件键
dbss:auditInstance:getRiskBackupBucketInfo	授予权限以获取风险导出obs桶信息。	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:setRiskBackupBucketInfo	授予权限以设置风险导出obs桶信息。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:addRdsDatabase	授予权限以添加RDS数据库。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss::getServerInfo	授予权限以获取DBSS服务信息。	read	-	-
dbss::getAuditInstanceJob	授予权限以查看审计实例任务创建信息。	read	-	-
dbss:auditInstance:listJobs	授予权限以列举审计实例任务创建信息。	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss::listObsBuckets	授予权限以查询obs桶列表。	list	-	-
dbss:auditInstance:instanceDelete	授予权限以删除审计实例。	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss::listResourcesByTag	授予权限以根据标签信息查询审计实例。	tagging	-	• g:RequestTag/<tag-key> • g:TagKeys
dbss::tagResource	授予权限以批量添加实例标签。	tagging	-	• g:RequestTag/<tag-key> • g:TagKeys

操作项	描述	访问级别	资源类型（*为必须）	条件键
dbss::unTagResource	授予权限以批量删除实例标签。	tagging	-	• g:RequestTag/<tag-key> • g:TagKeys
dbss::listTags	授予权限以查询项目下的所有标签。	tagging	-	-
dbss::listTagsForResource	授予权限以查询实例标签信息。	tagging	-	-

DBSS的API通常对应着一个或多个操作项。表5-172展示了API与操作项的关系，以及该API需要依赖的操作项。

表 5-172 API 与操作项的关系

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/{instance_id}/audit/rule/risk/switch	dbss:auditInstance:switchRiskRule	-
POST /v1/{project_id}/{instance_id}/audit/agent/switch	dbss:auditInstance:switchAgent	-
GET /v1/{project_id}/dbss/audit/quota	dbss::listCommonInfo	-
GET /v1/{project_id}/dbss/audit/specification	dbss::listCommonInfo	-
GET /v2/{project_id}/dbss/audit/availability-zone	dbss::listCommonInfo	-
POST /v1/{project_id}/{instance_id}/dbss/audit/operate-log	dbss:auditInstance:listOperateLog	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/dbss/audit/security-group	dbss:auditInstance:updateSecurityGroup	-
GET /v1/{project_id}/dbss/audit/instances	dbss:auditInstance:instanceList	-
GET /v1/{project_id}/dbss/audit/jobs/{resource_id}	dbss:auditInstance:listJobs	-
POST /v2/{project_id}/dbss/audit/charge/period/order	dbss:auditInstance:createOnPeriod	dbss::listCommonInfo
GET /v1/{project_id}/{instance_id}/dbss/audit/databases	dbss:auditInstance:listDatabases	-
POST /v1/{project_id}/{instance_id}/dbss/audit/databases/rds	dbss:auditInstance:addRdsDatabase	-
GET /v1/{project_id}/{resource_type}/tags	dbss::listTags	-
POST /v1/{project_id}/{resource_type}/resource-instances/filter	dbss::listResourcesByTag	-
POST /v1/{project_id}/{resource_type}/resource-instances/count	dbss::listResourcesByTag	-
POST /v1/{project_id}/{resource_type}/{resource_id}/tags/create	dbss::tagResource	-

API	对应的操作项	依赖的操作项
DELETE /v1/{project_id}/{resource_type}/{resource_id}/tags/delete	dbss::unTagResource	-
GET /v1/{project_id}/{instance_id}/dbss/audit/rule/scopes	dbss:auditInstance:listAuditScopeRules	-
POST /v1/{project_id}/{instance_id}/dbss/audit/rule/sql-injections	dbss:auditInstance:listSqlInjectRules	-
GET /v1/{project_id}/{instance_id}/dbss/audit/rule/risk	dbss:auditInstance:listRiskRules	-
GET /v1/{project_id}/{instance_id}/dbss/audit/rule/risk/{risk_id}	dbss:auditInstance:getRiskRuleDetail	-
GET /v1/{project_id}/{instance_id}/dbss/audit/sensitive/masks	dbss:auditInstance:listSensitiveRules	-

资源类型（Resource）

DBSS服务不支持在身份策略中的资源中指定资源进行权限控制。如需允许访问DBSS服务，请在身份策略的Resource元素中使用通配符号*，表示身份策略将应用到所有资源。

表 5-173 dbss 支持的资源类型

资源类型	URN	条件键
auditInstance	dbss:<region>:<account-id>:auditInstance:<instance-id>	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

条件（Condition）

DBSS服务不支持在身份策略中的条件键中配置服务级的条件键。DBSS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。

5.10.8.11 Web 应用防火墙 WAF

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Web应用防火墙（WAF）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Web应用防火墙（WAF）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WAF的相关操作。

表 5-174 waf 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
waf:host:list	授予查询防护域名列表的权限。	list	host *	-
			-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
waf:host:create	授予创建防护域名的权限。	write	host *	-
			policy	-
			certificate	-
			-	g:EnterpriseProjectId
waf:host:get	授予查询防护域名的权限。	read	host *	g:EnterpriseProjectId
waf:host:put	授予更新防护域名的权限。	write	host *	g:EnterpriseProjectId
			certificate	-
waf:host:delete	授予删除防护域名的权限。	write	host *	g:EnterpriseProjectId
waf:sourceIp:get	授予查询回源IP信息的权限。	read	-	-
waf:policy:list	授予查询防护策略列表的权限。	list	policy *	-
			-	g:EnterpriseProjectId
waf:policy:create	授予创建防护策略的权限。	write	policy *	-
			-	g:EnterpriseProjectId
waf:policy:get	授予查询防护策略的权限。	read	policy *	g:EnterpriseProjectId
waf:policy:put	授予更新防护策略的权限。	write	policy *	g:EnterpriseProjectId
			host	-
waf:policy:delete	授予删除防护策略的权限。	write	policy *	g:EnterpriseProjectId
waf:ccRule:list	授予查询cc规则列表的权限。	list	policy *	-
			-	g:EnterpriseProjectId
waf:ccRule:create	授予创建cc规则的权限。	write	policy *	-
			-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
waf:ccRule:get	授予查询cc规则的权限。	read	policy *	g:EnterpriseProjectId
waf:ccRule:put	授予更新cc规则的权限。	write	policy *	g:EnterpriseProjectId
waf:ccRule:delete	授予删除cc规则的权限。	write	policy *	g:EnterpriseProjectId
waf:preciseProtectionRule:list	授予查询精准防护规则列表的权限。	list	policy *	-
			-	g:EnterpriseProjectId
waf:preciseProtectionRule:create	授予创建精准防护规则的权限。	write	policy *	-
			-	g:EnterpriseProjectId
waf:preciseProtectionRule:get	授予查询精准防护规则的权限。	read	policy *	g:EnterpriseProjectId
waf:preciseProtectionRule:put	授予更新精准防护规则的权限。	write	policy *	g:EnterpriseProjectId
waf:preciseProtectionRule:delete	授予删除精准防护规则的权限。	write	policy *	g:EnterpriseProjectId
waf:whiteBlackIpRule:list	授予查询黑白名单规则列表的权限。	list	policy *	-
			-	g:EnterpriseProjectId
waf:whiteBlackIpRule:create	授予创建黑白名单规则的权限。	write	policy *	-
			-	g:EnterpriseProjectId
waf:whiteBlackIpRule:get	授予查询黑白名单规则的权限。	read	policy *	g:EnterpriseProjectId
waf:whiteBlackIpRule:put	授予更新黑白名单规则的权限。	write	policy *	g:EnterpriseProjectId
waf:whiteBlackIpRule:delete	授予删除黑白名单规则的权限。	write	policy *	g:EnterpriseProjectId
waf:privacyRule:list	授予查询隐私屏蔽规则列表的权限。	list	policy *	-
			-	g:EnterpriseProjectId
waf:privacyRule:create	授予创建隐私屏蔽规则的权限。	write	policy *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			-	g:EnterpriseProjectId
waf:privacyRule:get	授予查询隐私屏蔽规则的权限。	read	policy *	g:EnterpriseProjectId
waf:privacyRule:put	授予更新隐私屏蔽规则的权限。	write	policy *	g:EnterpriseProjectId
waf:privacyRule:delete	授予删除隐私屏蔽规则的权限。	write	policy *	g:EnterpriseProjectId
waf:falseAlarmMaskRule:list	授予查询误报屏蔽规则列表的权限。	list	policy *	-
			-	g:EnterpriseProjectId
waf:falseAlarmMaskRule:create	授予创建误报屏蔽规则的权限。	write	policy *	-
			-	g:EnterpriseProjectId
waf:falseAlarmMaskRule:get	授予查询误报屏蔽规则的权限。	read	policy *	g:EnterpriseProjectId
waf:falseAlarmMaskRule:put	授予更新误报屏蔽规则的权限。	write	policy *	g:EnterpriseProjectId
waf:falseAlarmMaskRule:delete	授予删除误报屏蔽规则的权限。	write	policy *	g:EnterpriseProjectId
waf:geoIpRule:list	授予查询地理位置封禁规则列表的权限。	list	policy *	-
			-	g:EnterpriseProjectId
waf:geoIpRule:create	授予创建地理位置封禁规则的权限。	write	policy *	-
			-	g:EnterpriseProjectId
waf:geoIpRule:get	授予查询地理位置封禁规则的权限。	read	policy *	g:EnterpriseProjectId
waf:geoIpRule:put	授予更新地理位置封禁规则的权限。	write	policy *	g:EnterpriseProjectId
waf:geoIpRule:delete	授予删除地理位置封禁规则的权限。	write	policy *	g:EnterpriseProjectId
waf:antiTamperRule:list	授予查询网页防篡改规则列表的权限。	list	policy *	-
			-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
waf:antiTamperRule:create	授予创建网页防篡改规则的权限。	write	policy *	-
			-	g:EnterpriseProjectId
waf:antiTamperRule:get	授予查询网页防篡改规则的权限。	read	policy *	g:EnterpriseProjectId
waf:antiTamperRule:put	授予更新网页防篡改规则的权限。	write	policy *	g:EnterpriseProjectId
waf:antiTamperRule:delete	授予删除网页防篡改规则的权限。	write	policy *	g:EnterpriseProjectId
waf:antiLeakageRule:list	授予查询反敏感信息泄漏规则列表的权限。	list	policy *	-
			-	g:EnterpriseProjectId
waf:antiLeakageRule:create	授予创建反敏感信息泄漏规则的权限。	write	policy *	-
			-	g:EnterpriseProjectId
waf:antiLeakageRule:get	授予查询反敏感信息泄漏规则的权限。	read	policy *	g:EnterpriseProjectId
waf:antiLeakageRule:put	授予更新反敏感信息泄漏规则的权限。	write	policy *	g:EnterpriseProjectId
waf:antiLeakageRule:delete	授予删除反敏感信息泄漏规则的权限。	write	policy *	g:EnterpriseProjectId
waf:anticrawlerRule:list	授予查询反爬虫规则列表的权限。	list	policy *	-
			-	g:EnterpriseProjectId
waf:anticrawlerRule:create	授予创建反爬虫规则的权限。	write	policy *	-
			-	g:EnterpriseProjectId
waf:anticrawlerRule:get	授予查询反爬虫规则的权限。	read	policy *	g:EnterpriseProjectId
waf:anticrawlerRule:put	授予更新反爬虫规则的权限。	write	policy *	g:EnterpriseProjectId
waf:anticrawlerRule:delete	授予删除反爬虫规则的权限。	write	policy *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
waf:punishmentRule:list	授予查询攻击惩罚规则列表的权限。	list	policy *	-
			-	g:EnterpriseProjectId
waf:punishmentRule:create	授予创建攻击惩罚规则的权限。	write	policy *	-
			-	g:EnterpriseProjectId
waf:punishmentRule:get	授予查询攻击惩罚规则的权限。	read	policy *	g:EnterpriseProjectId
waf:punishmentRule:put	授予更新攻击惩罚规则的权限。	write	policy *	g:EnterpriseProjectId
waf:punishmentRule:delete	授予删除攻击惩罚规则的权限。	write	policy *	g:EnterpriseProjectId
waf:valueList:list	授予查询引用表列表的权限。	list	-	g:EnterpriseProjectId
waf:valueList:create	授予创建引用表的权限。	write	-	g:EnterpriseProjectId
waf:valueList:get	授予查询引用表的权限。	read	-	g:EnterpriseProjectId
waf:valueList:put	授予更新引用表的权限。	write	-	g:EnterpriseProjectId
waf:valueList:delete	授予删除引用表的权限。	write	-	g:EnterpriseProjectId
waf:ipgroup:list	授予查询IP地址组列表的权限。	list	-	g:EnterpriseProjectId
waf:ipgroup:create	授予创建IP地址组的权限。	write	-	g:EnterpriseProjectId
waf:ipgroup:get	授予查询IP地址组的权限。	read	-	g:EnterpriseProjectId
waf:ipgroup:put	授予修改IP地址组的权限。	write	-	g:EnterpriseProjectId
waf:ipgroup:delete	授予删除IP地址组的权限。	write	-	g:EnterpriseProjectId
waf:certificate:list	授予查看证书列表的权限。	list	certificate *	-
			-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
waf:certificate:create	授予创建证书的权限。	write	certificate *	-
			-	g:EnterpriseProjectId
waf:certificate:get	授予查询证书的权限。	read	certificate *	g:EnterpriseProjectId
waf:certificate:put	授予修改WAF证书的权限。	write	certificate *	g:EnterpriseProjectId
waf:certificate:delete	授予删除证书的权限。	write	certificate *	g:EnterpriseProjectId
waf:certificate:apply	授予应用证书到域名的权限。	write	certificate *	g:EnterpriseProjectId
			host *	-
waf:premiumInstance:list	授予查询独享引擎实例列表的权限。	list	premiumInstance *	-
			-	g:EnterpriseProjectId
waf:premiumInstance:create	授予创建独享引擎实例的权限。	write	premiumInstance *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
waf:premiumInstance:get	授予查询独享引擎实例的权限。	read	premiumInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
waf:premiumInstance:put	授予更新独享引擎实例的权限。	write	premiumInstance *	• 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
waf:premiumInstance:delete	授予删除独享引擎实例的权限。	write	premiumInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
waf:event:get	授予查询防护事件的权限。	read	-	g:EnterpriseProjectId
waf:ltsConfig:get	授予查询对接云日志的配置的权限。	list	-	g:EnterpriseProjectId
waf:ltsConfig:put	授予更新对接云日志配置的权限。	write	-	g:EnterpriseProjectId
waf:postpaid:create	授予开通按需计费的权限。	write	-	g:EnterpriseProjectId
waf:postpaid:delete	授予关闭按需计费的权限。	write	-	g:EnterpriseProjectId
waf:prepaid:create	授予创建包周期订单的权限。	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
waf:subscription:get	授予查询云模式订购信息的权限。	read	-	-
waf:alert:get	授予查询告警通知的配置的权限。	list	-	-
waf:alert:put	授予更新告警通知配置的权限。	write	-	-
waf:consoleConfig:get	授予查询页面配置信息的权限。	read	-	-

WAF的API通常对应着一个或多个授权项。表5-175展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-175 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}/waf/instance	waf:host:create	-

API	对应的授权项	依赖的授权项
DELETE /v1/{project_id}/waf/instance/{instance_id}	waf:host:delete	-
GET /v1/{project_id}/waf/instance	waf:host:list	-
GET /v1/{project_id}/waf/instance/{instance_id}/route	waf:host:get	-
GET /v1/{project_id}/waf/instance/{instance_id}	waf:host:get	-
PATCH /v1/{project_id}/waf/instance/{instance_id}	waf:host:put	-
PUT /v1/{project_id}/waf/instance/{instance_id}/protect-status	waf:host:put	-
POST /v1/{project_id}/premium-waf/host	waf:host:create	-
DELETE /v1/{project_id}/premium-waf/host/{host_id}	waf:host:delete	-
GET /v1/{project_id}/premium-waf/host	waf:host:list	-
GET /v1/{project_id}/premium-waf/host/{host_id}	waf:host:get	-
PUT /v1/{project_id}/premium-waf/host/{host_id}	waf:host:put	-

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/premium-waf/host/{host_id}/protect-status	waf:host:put	-
POST /v1/{project_id}/waf/policy	waf:policy:create	-
DELETE /v1/{project_id}/waf/policy/{policy_id}	waf:policy:delete	-
GET /v1/{project_id}/waf/policy	waf:policy:list	-
GET /v1/{project_id}/waf/policy/{policy_id}	waf:policy:get	-
PATCH /v1/{project_id}/waf/policy/{policy_id}	waf:policy:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}	waf:policy:put	-
POST /v1/{project_id}/waf/policy/{policy_id}/cc	waf:ccRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/custom	waf:preciseProtectionRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/antitamper	waf:antiTamperRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}/refresh	waf:antiTamperRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/antileakage	waf:antiLeakageRule:create	-

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/waf/policy/{policy_id}/anticrawler	waf:anticrawlerRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/punishment	waf:punishmentRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/geoip	waf:geoIpRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/ignore	waf:falseAlarmMaskRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/privacy	waf:privacyRule:create	-
POST /v1/{project_id}/waf/valuelist	waf:valueList:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/whiteblackip	waf:whiteBlackIpRule:create	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}	waf:ccRule:delete	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}	waf:preciseProtectionRule:delete	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}	waf:antiTamperRule:delete	-

API	对应的授权项	依赖的授权项
DELETE /v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id}	waf:antiLeakageRule:delete	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/anticrawler/{rule_id}	waf:anticrawlerRule:delete	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/punishment/{rule_id}	waf:punishmentRule:delete	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}	waf:geoIpRule:delete	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}	waf:falseAlarmMaskRule:delete	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}	waf:privacyRule:delete	-
DELETE /v1/{project_id}/waf/valuelist/{valuelistid}	waf:valueList:delete	-
DELETE /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}	waf:whiteBlackIpRule:delete	-
GET /v1/{project_id}/waf/policy/{policy_id}/custom	waf:preciseProtectionRule:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/cc	waf:ccRule:list	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/waf/policy/{policy_id}/antitamper	waf:antiTamperRule:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/antileakage	waf:antiLeakageRule:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/anticrawler	waf:anticrawlerRule:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/punishment	waf:punishmentRule:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/geoip	waf:geoIpRule:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/ignore	waf:falseAlarmMaskRule:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/privacy	waf:privacyRule:list	-
GET /v1/{project_id}/waf/valuelist	waf:valueList:list	-
GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip	waf:whiteBlackIpRule:list	-
PUT /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}	waf:ccRule:put	-

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}	waf:preciseProtectionRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}	waf:geoIpRule:put	-
-	waf:antiTamperRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id}	waf:antiLeakageRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/anticrawler/{rule_id}	waf:anticrawlerRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/anticrawler	waf:anticrawlerRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/punishment/{rule_id}	waf:punishmentRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/{ruletype}/{rule_id}/status	waf:whiteBlackIpRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}	waf:privacyRule:put	-
PUT /v1/{project_id}/waf/valuelist/{valuelistid}	waf:valueList:put	-

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}	waf:whiteBlackIpRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}	waf:falseAlarmMaskRule:put	-
GET /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}	waf:ccRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}	waf:preciseProtectionRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}	waf:whiteBlackIpRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}	waf:privacyRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}	waf:falseAlarmMaskRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}	waf:geoIpRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}	waf:antiTamperRule:get	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id}	waf:antiLeakageRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/anticrawler/{rule_id}	waf:anticrawlerRule:get	-
GET /v1/{project_id}/waf/policy/{policy_id}/punishment/{rule_id}	waf:punishmentRule:get	-
GET /v1/{project_id}/waf/valuelist/{valuelistid}	waf:valueList:get	-
POST /v1/{project_id}/waf/ip-groups	waf:ipgroup:create	-
DELETE /v1/{project_id}/waf/ip-group/{id}	waf:ipgroup:delete	-
GET /v1/{project_id}/waf/ip-groups	waf:ipgroup:list	-
GET /v1/{project_id}/waf/ip-group/{id}	waf:ipgroup:get	-
PUT /v1/{project_id}/waf/ip-group/{id}	waf:ipgroup:put	-
POST /v1/{project_id}/waf/certificate/{certificate_id}/apply-to-hosts	waf:certificate:apply	-
POST /v1/{project_id}/waf/certificate	waf:certificate:create	-

API	对应的授权项	依赖的授权项
DELETE /v1/{project_id}/waf/certificate/{certificate_id}	waf:certificate:delete	-
GET /v1/{project_id}/waf/certificate	waf:certificate:list	-
GET /v1/{project_id}/waf/certificate/{certificate_id}	waf:certificate:get	-
PUT /v1/{project_id}/waf/certificate/{certificate_id}	waf:certificate:put	-
GET /v1/{project_id}/waf/event	waf:event:get	-
GET /v1/{project_id}/waf/event/{eventid}	waf:event:get	-
GET /v1/{project_id}/waf/overviews/bandwidth/timeline	waf:event:get	-
GET /v1/{project_id}/waf/overviews/classification	waf:event:get	-
GET /v1/{project_id}/waf/overviews/qps/timeline	waf:event:get	-
GET /v1/{project_id}/waf/overviews/request/timeline	waf:event:get	-
GET /v1/{project_id}/waf/overviews/statistics	waf:event:get	-
GET /v1/{project_id}/waf/overviews/abnormal	waf:event:get	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/waf/config/console	waf:consoleConfig:get	-
POST /v1/{project_id}/premium-waf/instance	waf:premiumInstance:create	-
DELETE /v1/{project_id}/premium-waf/instance/{instance_id}	waf:premiumInstance:delete	-
GET /v1/{project_id}/premium-waf/instance	waf:premiumInstance:list	-
PUT /v1/{project_id}/premium-waf/instance/{instance_id}	waf:premiumInstance:put	-
GET /v1/{project_id}/premium-waf/instance/{instance_id}	waf:premiumInstance:get	-
GET /v1/{project_id}/waf/config/lts	waf:ltsConfig:get	-
PUT /v1/{project_id}/waf/config/lts/{ltsconfig_id}	waf:ltsConfig:put	-
POST /v1/{project_id}/waf/subscription/batchalter/prepaid-cloud-waf	waf:prepaid:create	-
POST /v1/{project_id}/waf/subscription/purchase/prepaid-cloud-waf	waf:prepaid:create	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/waf/subscription	waf:subscription:get	-
POST /v1/{project_id}/waf/postpaid	waf:postpaid:create	-
DELETE /v1/{project_id}/waf/postpaid	waf:postpaid:delete	-
GET /v2/{project_id}/waf/alerts	waf:alert:get	-
PUT /v2/{project_id}/waf/alert/{alert_id}	waf:alert:put	-
GET /v1/{project_id}/waf/config/source-ip	waf:sourceIp:get	-
POST /v1/{project_id}/composite-waf/hosts/migration	waf:host:create	-
GET /v1/{project_id}/composite-waf/host	waf:host:list	-
GET /v1/{project_id}/composite-waf/host/{host_id}	waf:host:get	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-176**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。

WAF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 5-176 waf 支持的资源类型

资源类型	URN
policy	waf:<region>:<account-id>:policy:<policy-id>
host	waf:<region>:<account-id>:host:<host-id>
premiumInstance	waf:<region>:<account-id>:premiumInstance:<instance-id>
certificate	waf:<region>:<account-id>:certificate:<certificate-id>

条件（Condition）

WAF服务不支持在SCP中的条件键中配置服务级的条件键。WAF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 IoT 物联网

5.10.9.1 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 5-177 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
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

授权项	描述	访问级别	资源类型	条件键
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
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

授权项	描述	访问级别	资源类型	条件键
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 • iotda:HttpForwardingEnableSSL • iotda:HttpForwardingEnableAuthentication • iotda:DMSKafkaForwardingEnableAuthentication • iotda:DMSKafkaForwardingEnableSSL • iotda:MysqlForwardingEnableSSL • iotda:MRSKafkaForwardingEnableAuthentication • iotda:DMSRocketMQForwardingEnableSSL • iotda:MongoDBForwardingEnableSSL
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

授权项	描述	访问级别	资源类型	条件键
iotda:routingactions:modify	修改规则动作	write	app	• g:EnterpriseProjectId • iotda:HttpForwardingEnableSSL • iotda:HttpForwardingEnableAuthentication • iotda:DMSKafkaForwardingEnableAuthentication • iotda:DMSKafkaForwardingEnableSSL • iotda:MysqlForwardingEnableSSL • iotda:MRSKafkaForwardingEnableAuthentication • iotda:DMSRocketMQForwardingEnableSSL • iotda:MongoDBForwardingEnableSSL
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

授权项	描述	访问级别	资源类型	条件键
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
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

授权项	描述	访问级别	资源类型	条件键
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
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

授权项	描述	访问级别	资源类型	条件键
iotda:tunnel:create	创建设备隧道	write	-	• g:EnterpriseProjectId • iotda:DeviceGroupId
iotda:tunnel:delete	删除设备隧道	write	-	g:EnterpriseProjectId
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:instance:create	创建实例	write	-	• g:EnterpriseProjectId • g:TagKeys • g:RequestTag/<tag-key>
iotda:instance:update	修改实例	write	-	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • iotda:AllowPublicAccess • iotda:AllowPublicForwarding • iotda:DomainConfiguration
iotda:instance:query	查询实例详情	read	instance	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
iotda:instance:queryList	查询实例列表	read	-	-
iotda:instance:delete	删除实例	write	instance	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
iotda:instance:operateTag	操作实例标签	write	instance	• g:EnterpriseProjectId • g:TagKeys • g:RequestTag/<tag-key>

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 5-178 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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
POST /v5/iot/{project_id}/ota-upgrades/packages	iotda:otapackages:create	-
GET /v5/iot/{project_id}/ota-upgrades/packages	iotda:otapackages:queryList	-

API	对应的授权项	依赖的授权项
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	-
POST /v5/iot/{project_id}/iotda-instances	iotda:instance:create	-
PUT /v5/iot/{project_id}/iotda-instances/{instance_id}	iotda:instance:update	-
GET /v5/iot/{project_id}/iotda-instances/{instance_id}	iotda:instance:query	-
GET /v5/iot/{project_id}/iotda-instances	iotda:instance:queryList	-
DELETE /v5/iot/{project_id}/iotda-instances/{instance_id}	iotda:instance:delete	-
POST /v5/iot/{project_id}/iotda-instances/{instance_id}/bind-tags	iotda:instance:operateTag	-
POST /v5/iot/{project_id}/iotda-instances/{instance_id}/unbind-tags	iotda:instance:operateTag	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-179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 5-179 IoTDA 支持的资源类型

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

资源类型	URN
instance	iotda:<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IoTDA:）仅适用于对应服务的操作，详情请参见**表5-180**。
  - 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。

IoTDA云服务定义了以下可以在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 5-180 IoTDA 支持的条件键

服务级条件键	类型	单值/多值	说明
iotda:AllowPublicAccess	布尔型	单值	根据修改实例时设置的允许公网访问的配置过滤请求
iotda:AllowPublicForwarding	布尔型	单值	根据修改实例时设置的允许公网转发的配置过滤请求
iotda:DomainConfiguration	布尔型	单值	根据修改实例时是否配置接入域名过滤请求
iotda:DeviceGroupId	字符串	单值	根据创建隧道时设置的设备所属的群组过滤请求
iotda:HttpForwardingEnableSSL	布尔型	单值	根据创建/修改规则动作时设置的Http通道开启TLS协议的配置过滤请求
iotda:HttpForwardingEnableAuthentication	布尔型	单值	根据创建/修改规则动作时设置的Http通道启用Token认证的配置过滤请求

服务级条件键	类型	单值/多值	说明
iotda:DMSKafkaForwardingEnableAuthentication	布尔型	单值	根据创建/修改规则动作时设置的DMSKafka通道启用mechanism为SCRAM-SHA-512的配置过滤请求
iotda:DMSKafkaForwardingEnableSSL	布尔型	单值	根据创建/修改规则动作时设置的DMSKafka通道开启TLS协议的配置过滤请求
iotda:MysqlForwardingEnableSSL	布尔型	单值	根据创建/修改规则动作时设置的Mysql协议通道开启TLS协议的配置过滤请求
iotda:MRSKafkaForwardingEnableAuthentication	布尔型	单值	根据创建/修改规则动作时设置的MRSKafka通道启用Kerberos认证的配置过滤请求
iotda:DMSRocketMQForwardingEnableSSL	布尔型	单值	根据创建/修改规则动作时设置的RocketMQ通道开启TLS协议的配置过滤请求
iotda:MongoDBForwardingEnableSSL	布尔型	单值	根据创建/修改规则动作时设置的MongoDB通道开启TLS协议的配置过滤请求

5.10.10 应用中间件

5.10.10.1 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 5-181 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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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 *	-

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
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 *	-
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5-182**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-182 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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/instances/{instance_id}/configs	dcs:instance:modifyConfiguration	-
PUT /v2/{project_id}/instances/{instance_id}/async-configs	dcs:instance:modifyConfiguration	-
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	-

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

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/instances/{instance_id}/tags	dcs:tag:get	-
GET /v2/{project_id}/instances/{instance_id}/bigkey-tasks	dcs:instance:listBigKey	-
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	-

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/instances/{instance_id}/hotkey/autoscan	dcs:instance:updateHotKeyAutoScanConfig	-
GET /v2/{project_id}/instances/{instance_id}/hotkey/autoscan	dcs:instance:getHotKeyAutoScanConfig	-
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	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/instances/{instance_id}/redislog	dcs:redisLog:get	-
POST /v2/{project_id}/instances/{instance_id}/redislog	dcs:redisLog:get	-
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	-

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/instances/{instance_id}/accounts/{account_id}/role	dcs:aclaccount:modify	-
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	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/instances/{instance_id}/diagnosis	dcs:instance:createDiagnosisTask	-
GET /v2/{project_id}/instances/{instance_id}/diagnosis	dcs:instance:listDiagnosisTask	-
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	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/instances/{instance_id}/config-histories	dcs:instance:get	-
PUT /v2/{project_id}/instances/{instance_id}/bandwidth	dcs:instance:modify	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/instance/{instance_id}/groups/{group_id}/group-nodes-state	dcs:instance:get	-
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	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/migration-task/{task_id}/exchange-ip	dcs:migrationTask:modify	-
GET /v2/{project_id}/tasks	dcs:task:list	-
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5-183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 5-183 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5-184。
  - 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 5-184 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。

5.10.10.2 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 5-185 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
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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5-186展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-186 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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
PUT /v3/{project_id}/govern/governance/{kind}/{policy_id}	cse:policy:update	-
GET /v3/{project_id}/govern/governance/display	cse:policy:list	-
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 5-187 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。

5.10.10.3 API 网关 APIG

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apig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apig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apig的相关操作。

表 5-188 apig 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	别名
apig:acl:list	授予权限以查看ACL策略列表。	list	instance *	g:ResourceTag/<tag-key>	apig:acls:list
apig:acl:create	授予权限以创建ACL策略。	write	instance *	g:ResourceTag/<tag-key>	apig:acls:create

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:acl:batchDelete	授予权限以批量删除ACL策略。	write	instance *	g:ResourceTag/<tag-key>	apig:acls:delete
apig:acl:delete	授予权限以删除ACL策略。	write	instance *	g:ResourceTag/<tag-key>	apig:acls:delete
apig:acl:get	授予权限以查看ACL策略详情。	read	instance *	g:ResourceTag/<tag-key>	apig:acls:get
apig:acl:update	授予权限以修改ACL策略。	write	instance *	g:ResourceTag/<tag-key>	apig:acls:update
apig:api:bindAcl	授予权限以绑定API和ACL策略。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:bindAcls
apig:api:batchUnbindAcl	授予权限以批量解除API和ACL策略的绑定关系。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:unbindAcls
apig:api:unbindAcl	授予权限以解除API和ACL策略的绑定关系。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:unbindAcls
apig:api:listBoundAcl	授予权限以获取API绑定的ACL策略列表。	list	instance *	g:ResourceTag/<tag-key>	apig:apis:listBindedAcls
apig:acl:listBoundApi	授予权限以获取ACL策略绑定的API列表。	list	instance *	g:ResourceTag/<tag-key>	apig:acls:listBindedApis
apig:acl:listUnboundApi	授予权限以获取ACL策略未绑定的API列表。	list	instance *	g:ResourceTag/<tag-key>	apig:acls:listUnbindedApis
apig:api:bindRequestThrottling	授予权限以绑定API和流控策略。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:bindThrottles
apig:api:batchUnbindRequestThrottling	授予权限以批量解除API和流控策略的绑定关系。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:unbindThrottles

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:api:unbindRequestThrottling	授予权限以解除API和流控策略的绑定关系。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:unbindThrottles
apig:requestThrottling:listBoundApi	授予权限以获取流控策略绑定的API列表。	list	instance *	g:ResourceTag/<tag-key>	apig:throttles:listBindedApis
apig:api:listBoundRequestThrottling	授予权限以获取API绑定的流控策略列表。	list	instance *	g:ResourceTag/<tag-key>	apig:apis:listBindedThrottles
apig:requestThrottling:listUnboundApi	授予权限以获取流控策略未绑定的API列表。	list	instance *	g:ResourceTag/<tag-key>	apig:throttles:listUnbindedApis
apig:apiGroup:list	授予权限以获取API分组列表。	list	instance *	g:ResourceTag/<tag-key>	apig:groups:list
apig:apiGroup:create	授予权限以创建API分组。	write	instance *	g:ResourceTag/<tag-key>	apig:groups:create
apig:apiGroup:delete	授予权限以删除API分组。	write	instance *	g:ResourceTag/<tag-key>	apig:groups:delete
apig:apiGroup:get	授予权限以查询API分组详情。	read	instance *	g:ResourceTag/<tag-key>	apig:groups:get
apig:apiGroup:update	授予权限以修改API分组。	write	instance *	g:ResourceTag/<tag-key>	apig:groups:update
apig:apiGroup:checkApiGroupNameExistOrNot	授予权限以校验API分组名称是否存在。	read	instance *	g:ResourceTag/<tag-key>	apig:groups:get
apig:api:list	授予权限以获取API列表。	list	instance *	g:ResourceTag/<tag-key>	apig:apis:list
apig:api:create	授予权限以创建API。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:create
apig:api:delete	授予权限以删除API。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:delete

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:api:get	授予权限以查询API详情。	read	instance *	g:ResourceTag/<tag-key>	apig:apis:get
apig:api:update	授予权限以修改API。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:update
apig:api:onlineOrOffline	授予权限以发布或下线API。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:publish
apig:api:batchDelete	授予权限以批量删除API。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:delete
apig:api:checkApiPathOrApiNameExistOrNot	授予权限以校验API定义。	read	instance *	g:ResourceTag/<tag-key>	apig:apis:get
apig:api:debug	授予权限以调试API。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:debug
apig:api:batchOnlineOrOffline	授予权限以批量发布或下线API。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:publish
apig:api:listHistoryVersion	授予权限以查询API历史版本列表。	list	instance *	g:ResourceTag/<tag-key>	apig:apis:get
apig:api:switchVersion	授予权限以切换API版本。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:publish
apig:api:getRuntimeDefinition	授予权限以查询API运行时定义。	read	instance *	g:ResourceTag/<tag-key>	apig:apis:get
apig:api:deleteHistoryVersion	授予权限以根据版本编号下线API。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:offline
apig:api:getHistoryVersion	授予权限以获取版本详情。	read	instance *	g:ResourceTag/<tag-key>	apig:apis:get
apig:app:list	授予权限以获取APP列表。	list	instance *	g:ResourceTag/<tag-key>	apig:apps:list
apig:app:create	授予权限以创建APP。	write	instance *	g:ResourceTag/<tag-key>	apig:apps:create
apig:app:delete	授予权限以删除APP。	write	instance *	g:ResourceTag/<tag-key>	apig:apps:delete

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:app:get	授予权限以查看APP详情。	read	instance *	g:ResourceTag/<tag-key>	apig:apps:get
apig:app:update	授予权限以修改APP信息。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:update
apig:app:listAppCode	授予权限以查询APP Code列表。	list	instance *	g:ResourceTag/<tag-key>	apig:appCodes:list
apig:app:createAppCode	授予权限以创建APP Code。	write	instance *	g:ResourceTag/<tag-key>	apig:appCodes:create
apig:app:generateAppCode	授予权限以自动生成APP Code。	write	instance *	g:ResourceTag/<tag-key>	apig:appCodes:update
apig:app:deleteAppCode	授予权限以删除APP Code。	write	instance *	g:ResourceTag/<tag-key>	apig:appCodes:delete
apig:app:getAppCode	授予权限以获取APP Code详情。	read	instance *	g:ResourceTag/<tag-key>	apig:appCodes:get
apig:app:resetSecret	授予权限以重置APP的密钥。	write	instance *	g:ResourceTag/<tag-key>	apig:apps:update
apig:app:validate	授予权限以校验APP是否存在。	read	instance *	g:ResourceTag/<tag-key>	apig:apps:get
apig:app:getBoundQuota	授予权限以查询APP关联的凭据配额策略。	read	instance *	g:ResourceTag/<tag-key>	apig:apps:get
apig:app:bindApi	授予权限以绑定API和APP。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:grantAppAccess
apig:app:unbindApi	授予权限以解除API和APP的绑定关系。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:relieveAppAccess
apig:app:listBoundApi	授予权限以查看APP已绑定的API列表。	list	instance *	g:ResourceTag/<tag-key>	apig:apps:listBindedApis

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:api:listBoundApp	授予权限以查看API已绑定的APP列表。	list	instance *	g:ResourceTag/<tag-key>	apig:apis:listBindedApps
apig:app:listUnboundApi	授予权限以查看APP未绑定的API列表。	list	instance *	g:ResourceTag/<tag-key>	apig:apps:listUnbindedApis
apig:api:export	授予权限以导出API。	read	instance *	g:ResourceTag/<tag-key>	apig:apis:export
apig:api:import	授予权限以导入API。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:import
apig:asyncTask:get	授予权限以查看异步任务结果详情。	read	instance *	g:ResourceTag/<tag-key>	apig:apis:export
apig:certificate:list	授予权限以获取SSL证书列表。	list	instance	g:ResourceTag/<tag-key>	-
apig:certificate:create	授予权限以创建SSL证书。	write	instance	g:ResourceTag/<tag-key>	-
apig:certificate:delete	授予权限以删除SSL证书。	write	instance	g:ResourceTag/<tag-key>	-
apig:certificate:get	授予权限以获取SSL证书详情。	read	instance	g:ResourceTag/<tag-key>	-
apig:certificate:update	授予权限以修改SSL证书。	write	instance	g:ResourceTag/<tag-key>	-
apig:certificate:listBoundDomain	授予权限以获取SSL证书已绑定的域名列表。	list	instance	g:ResourceTag/<tag-key>	-
apig:certificate:batchBindDomain	授予权限以绑定域名到SSL证书。	write	instance	g:ResourceTag/<tag-key>	-
apig:certificate:batchUnbindDomain	授予权限以解绑SSL证书绑定的域名。	write	instance	g:ResourceTag/<tag-key>	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:apiGroup:batchBindCertificateToDomain	授予权限以绑定SSL证书到域名。	write	instance *	g:ResourceTag/<tag-key>	apig:domains:bindCertificate
apig:apiGroup:batchUnbindCertificateFromDomain	授予权限以解绑域名绑定的证书。	write	instance *	g:ResourceTag/<tag-key>	apig:domains:unbindCertificate
apig:loadBalanceChannel:list	授予权限以获取负载通道列表。	list	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:list
apig:loadBalanceChannel:create	授予权限以创建负载通道。	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:create
apig:loadBalanceChannel:delete	授予权限以删除负载通道。	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:delete
apig:loadBalanceChannel:get	授予权限以获取负载通道详情。	read	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:get
apig:loadBalanceChannel:update	授予权限以更新负载通道。	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:update
apig:loadBalanceChannel:updateHealthCheckConfig	授予权限以修改负载通道健康检查配置。	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:update
apig:loadBalanceChannel:listServerGroup	授予权限以查询负载通道后端服务器组列表。	list	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:get
apig:loadBalanceChannel:createServerGroup	授予权限以添加或更新VPC通道后端服务器组。	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:addOrUpdateMemberGroups
apig:loadBalanceChannel:deleteServerGroup	授予权限以删除VPC通道后端服务器组。	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:deleteMemberGroup

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:loadBalanceChannel:getServerGroup	授予权限以查看指定的VPC通道后端服务器组详情。	read	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:get
apig:loadBalanceChannel:updateServerGroup	授予权限以更新VPC通道后端服务器组。	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:updateMemberGroup
apig:loadBalanceChannel:listBackendServerAddress	授予权限以获取负载通道后端实例列表。	list	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:get
apig:loadBalanceChannel:createBackendServerAddress	授予权限以添加或更新负载通道后端实例。	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:addInstance
apig:loadBalanceChannel:updateBackendServerAddress	授予权限以更新负载通道后端实例。	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:addInstance
apig:loadBalanceChannel:deleteBackendServerAddress	授予权限以删除负载通道后端实例。	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:deleteInstance
apig:loadBalanceChannel:batchDisableBackendServerAddress	授予权限以批量修改后端服务器状态不可用。	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:batchDisableInstance
apig:loadBalanceChannel:batchEnableBackendServerAddress	授予权限以批量修改后端服务器状态可用。	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:batchEnableInstance
apig:instance:listTag	授予权限以获取标签列表。	list	instance *	g:ResourceTag/<tag-key>	apig:tags:list
apig:api:listUnboundPlugin	授予权限以获取API可绑定的插件列表。	list	instance *	g:ResourceTag/<tag-key>	apig:apis:listBindedPlugins

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:api:listBoundPlugin	授予权限以获取API已绑定的插件列表。	list	instance *	g:ResourceTag/<tag-key>	apig:apis:listBindedPlugins
apig:api:bindPlugin	授予权限以绑定插件到API。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:bindPlugins
apig:api:unbindPlugin	授予权限以解绑API绑定的插件。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:unbindPlugins
apig:plugin:list	授予权限以获取插件列表。	list	instance *	g:ResourceTag/<tag-key>	apig:plugins:list
apig:plugin:create	授予权限以创建插件。	write	instance *	g:ResourceTag/<tag-key>	apig:plugins:create
apig:plugin:delete	授予权限以删除插件。	write	instance *	g:ResourceTag/<tag-key>	apig:plugins:delete
apig:plugin:get	授予权限以获取插件详情。	read	instance *	g:ResourceTag/<tag-key>	apig:plugins:get
apig:plugin:update	授予权限以修改插件。	write	instance *	g:ResourceTag/<tag-key>	apig:plugins:update
apig:plugin:bindApi	授予权限以绑定API到插件。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:bindPlugins
apig:plugin:listUnbindApi	授予权限以获取插件可绑定的API列表。	list	instance *	g:ResourceTag/<tag-key>	apig:plugins:listUnbindedApis
apig:plugin:listBoundApi	授予权限以获取插件已绑定的API列表。	list	instance *	g:ResourceTag/<tag-key>	apig:plugins:listBindedApis
apig:plugin:unbindApi	授予权限以解绑插件绑定的API。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:unbindPlugins
apig:apiGroup:listGatewayResponse	授予权限以获取分组自定义响应列表。	list	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:list
apig:apiGroup:createGatewayResponse	授予权限以创建分组自定义响应。	write	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:create

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:apiGroup:deleteGatewayResponse	授予权限以删除分组自定义响应。	write	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:delete
apig:apiGroup:getGatewayResponse	授予权限以获取分组自定义响应详情。	read	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:get
apig:apiGroup:updateGatewayResponse	授予权限以修改分组自定义响应。	write	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:updat
apig:apiGroup:deleteGatewayResponseType	授予权限以删除分组指定错误类型的自定义响应配置。	write	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:update
apig:apiGroup:getGatewayResponseType	授予权限以获取分组下指定错误类型的自定义响应。	read	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:get
apig:apiGroup:updateGatewayResponseType	授予权限以修改分组下指定错误类型的自定义响应。	write	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:update
apig:instance:listApiOutline	授予权限以获取API概况。	list	instance *	g:ResourceTag/<tag-key>	apig:apis:get
apig:instance:listAppOutline	授予权限以获取APP概况。	list	instance *	g:ResourceTag/<tag-key>	apig:apps:get
apig:instance:listApiGroupOutline	授予权限以获取API分组概况。	list	instance *	g:ResourceTag/<tag-key>	apig:groups:get
apig:environmentVariable:list	授予权限以查询环境变量列表。	list	instance *	g:ResourceTag/<tag-key>	apig:variables:list
apig:environmentVariable:create	授予权限以新建环境变量。	write	instance *	g:ResourceTag/<tag-key>	apig:variables:create
apig:environmentVariable:delete	授予权限以删除环境变量。	write	instance *	g:ResourceTag/<tag-key>	apig:variables:delete

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:environmentVariable:get	授予权限以获取环境变量详情。	read	instance *	g:ResourceTag/<tag-key>	apig:variables:get
apig:environmentVariable:update	授予权限以修改环境变量。	write	instance *	g:ResourceTag/<tag-key>	apig:variables:update
apig:environment:list	授予权限以获取环境列表。	list	instance *	g:ResourceTag/<tag-key>	apig:envs:list
apig:environment:create	授予权限以创建环境。	write	instance *	g:ResourceTag/<tag-key>	apig:envs:create
apig:environment:delete	授予权限以删除环境。	write	instance *	g:ResourceTag/<tag-key>	apig:envs:delete
apig:environment:update	授予权限以修改环境。	write	instance *	g:ResourceTag/<tag-key>	apig:envs:update
apig:instance:listMetricData	授予权限以查询实例监控数据。	list	instance *	g:ResourceTag/<tag-key>	apig:metricData:get
apig:instance:listApiMonitoring	授予权限以查询最近一段时间API的统计信息。	list	instance *	g:ResourceTag/<tag-key>	apig:apis:get
apig:instance:listApiGroupMonitoring	授予权限以查询最近一小时内API分组的统计信息。	list	instance *	g:ResourceTag/<tag-key>	apig:groups:get
apig:requestThrottling:list	授予权限以获取流控策略列表。	list	instance *	g:ResourceTag/<tag-key>	apig:throttles:list
apig:requestThrottling:create	授予权限以创建流控策略。	write	instance *	g:ResourceTag/<tag-key>	apig:throttles:create
apig:requestThrottling:delete	授予权限以删除流控策略。	write	instance *	g:ResourceTag/<tag-key>	apig:throttles:delete
apig:requestThrottling:get	授予权限以获取流控策略详情。	read	instance *	g:ResourceTag/<tag-key>	apig:throttles:get

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:requestThrottling:update	授予权限以修改流控策略。	write	instance *	g:ResourceTag/<tag-key>	apig:throttles:update
apig:requestThrottling:batchDelete	授予权限以批量删除流控策略。	write	instance *	g:ResourceTag/<tag-key>	apig:throttles:delete
apig:api:bindSignatureKey	授予权限以绑定签名密钥和API。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:bindSigns
apig:api:unbindSignatureKey	授予权限以解除签名密钥和API的绑定关系。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:unbindSigns
apig:signatureKey:listBoundApi	授予权限以获取签名密钥绑定的API列表。	list	instance *	g:ResourceTag/<tag-key>	apig:signs:listBindedApis
apig:api:listBoundSignatureKey	授予权限以获取API绑定的签名密钥列表。	list	instance *	g:ResourceTag/<tag-key>	apig:apis:listBindedSigns
apig:signatureKey:listUnboundApi	授予权限以查询所有未绑定到该签名密钥上的API列表。	list	instance *	g:ResourceTag/<tag-key>	apig:signs:listUnbindedApis
apig:signatureKey:list	授予权限以获取签名密钥列表。	list	instance *	g:ResourceTag/<tag-key>	apig:signs:list
apig:signatureKey:create	授予权限以创建签名密钥。	write	instance *	g:ResourceTag/<tag-key>	apig:signs:create
apig:signatureKey:delete	授予权限以删除签名密钥。	write	instance *	g:ResourceTag/<tag-key>	apig:signs:delete
apig:signatureKey:update	授予权限以修改签名密钥。	write	instance *	g:ResourceTag/<tag-key>	apig:signs:update
apig:requestThrottling:listSpecial	授予权限以获取流控特殊设置列表。	list	instance *	g:ResourceTag/<tag-key>	apig:specialThrottles:get
apig:requestThrottling:createSpecial	授予权限以创建流控特殊设置。	write	instance *	g:ResourceTag/<tag-key>	apig:specialThrottles:create

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:requestThrottling:deleteSpecial	授予权限以删除流控特殊设置。	write	instance *	g:ResourceTag/<tag-key>	apig:specialThrottles:delete
apig:requestThrottling:updateSpecial	授予权限以修改某个流控策略下的某个特殊设置。	write	instance *	g:ResourceTag/<tag-key>	apig:specialThrottles:update
apig:instance:listSingleInstanceTag	授予权限以查询指定的实例标签列表。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instanceTags:list
apig:instance:batchCreateOrDeleteTag	授予权限以实现批量添加或删除实例标签的功能。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instanceTags:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
apig::listTag	授予权限以获取项目下所有实例标签。	list	-	-	apig:instanceTags:list
apig:instance:getNumByTags	授予权限以实现通过标签查询实例数量的功能。	read	instance *	-	-
			-	g:TagKeys	
apig:instance:listByTags	授予权限以实现通过标签查询实例列表的功能。	list	instance *	-	-
			-	g:TagKeys	
apig:instance:list	授予权限以获取专享版实例列表。	list	-	-	apig:instances:list

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:instance:create	授予权限以创建专享版实例。	write	-	• g:RequestTag/<tag-key> • g:TagKeys	apig:instances:create
apig:instance:delete	授予权限以删除专享版实例。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:delete
apig:instance:get	授予权限以查看专享版实例详情。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:get
apig:instance:update	授予权限以更新专享版实例。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:unbindEip	授予权限以解绑专享版实例的EIP。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:bindOrChangeEip	授予权限以添加或更换专享版实例的EIP。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:deleteOutboundEip	授予权限以关闭专享版实例的公网出口。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:instance:createOutboundEip	授予权限以开启专享版实例的公网出口。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:changeOutboundEipBandwidth	授予权限以修改专享版实例公网出口的带宽。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:getCreateProgress	授予权限以获取专享版实例的创建进度。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:deleteIngressEip	授予权限以关闭专享版实例的公网入口。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:createIngressEip	授予权限以开启专享版实例的公网入口。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:changeIngressEipBindwidth	授予权限以更新专享版实例的入公网带宽。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:resize	授予权限以创建按需专享版实例规格变更订单。	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	别名
apig:instance:getRestriction	授予权限以获取实例约束信息。	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:get
apig:instance:listParameter	授予权限以获取实例参数列表。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:features:list
apig:instance:updateParameter	授予权限以编辑实例参数。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:features:create
apig:instance:listFeature	授予权限以获取实例支持的特性列表。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:importMicroservice	授予权限以导入微服务到专享版实例。	write	instance *	g:ResourceTag/<tag-key>	apig:apis:import
apig:apiGroup:bindDomain	授予权限以绑定独立域名。	write	instance *	g:ResourceTag/<tag-key>	apig:domains:create
apig:apiGroup:unbindDomain	授予权限以解绑独立域名。	write	instance *	g:ResourceTag/<tag-key>	apig:domains:delete
apig:apiGroup:updateDomainConfig	授予权限以修改独立域名。	write	instance *	g:ResourceTag/<tag-key>	apig:domains:update
apig:apiGroup:createAndBindCertificateToDomain	授予权限以创建并绑定证书到独立域名。	write	instance *	g:ResourceTag/<tag-key>	apig:domains:bindCertificate

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:apiGroup:unbindAndDeleteCertificateFromDomain	授予权限以解绑并删除独立域名的证书。	write	instance *	g:ResourceTag/<tag-key>	apig:domains:unbindCertificate
apig:apiGroup:getCertificateOfDomain	授予权限以查看独立域名的证书。	read	instance *	g:ResourceTag/<tag-key>	apig:domains:getCertificate
apig:apiGroup:updateSLDomainSetting	授予权限以设置调试域名是否可以访问。	write	instance *	g:ResourceTag/<tag-key>	apig:domains:updateSLDomainSetting
apig:customAuthorizer:list	授予权限以获取自定义认证列表。	list	instance *	g:ResourceTag/<tag-key>	apig:authorizers:list
apig:customAuthorizer:create	授予权限以创建自定义认证。	write	instance *	g:ResourceTag/<tag-key>	apig:authorizers:create
apig:customAuthorizer:delete	授予权限以删除自定义认证。	write	instance *	g:ResourceTag/<tag-key>	apig:authorizers:delete
apig:customAuthorizer:get	授予权限以获取自定义认证详情。	read	instance *	g:ResourceTag/<tag-key>	apig:authorizers:get
apig:customAuthorizer:update	授予权限以修改自定义认证。	write	instance *	g:ResourceTag/<tag-key>	apig:authorizers:update
apig:instance:listVpcEndpoint	授予权限以获取实例终端节点列表。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:acceptOrRejectVpcEndpointConnection	授予权限以接受或拒绝终端节点连接。	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	别名
apig:instance:listVpcEndpointPermission	授予权限以获取实例终端节点服务的白名单列表。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:batchAddVpcEndpointPermission	授予权限以批量添加实例终端节点连接白名单。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:batchDeleteVpcEndpointPermission	授予权限以批量删除实例终端节点连接白名单。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:app:deleteAcl	授予权限以删除凭据的访问控制规则。	write	instance *	g:ResourceTag/<tag-key>	apig:apps:get
apig:app:getAcl	授予权限以获取凭据的访问控制规则。	read	instance *	g:ResourceTag/<tag-key>	apig:apps:get
apig:app:updateAcl	授予权限以设置凭据的访问控制规则。	write	instance *	g:ResourceTag/<tag-key>	apig:apps:get
apig:clientQuota:list	授予权限以获取凭据配额策略列表。	list	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:create	授予权限以创建凭据配额策略。	write	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:delete	授予权限以删除凭据配额策略。	write	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:get	授予权限以获取凭据配额策略详情。	read	instance *	g:ResourceTag/<tag-key>	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
apig:clientQuota:update	授予权限以修改凭据配额策略。	write	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:listBoundApp	授予权限以查询凭据配额策略已绑定的凭据列表。	list	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:bindApp	授予权限以绑定凭据配额和凭据。	write	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:unbindApp	授予权限以解除凭据配额和凭据的绑定关系。	write	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:listUnboundApp	授予权限以查询凭据配额可绑定的凭据列表。	list	instance *	g:ResourceTag/<tag-key>	-
apig:instance:listFeatureHistory	授予权限以查询特性的历史记录列表。	list	instance *	g:ResourceTag/<tag-key>	-
apig:instance:addCustomIngressPort	授予权限以新增实例自定义入方向端口。	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:listCustomIngressPort	授予权限以获取实例自定义入方向端口列表。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:deleteCustomIngressPort	授予权限以删除实例自定义入方向端口。	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	别名
apig:instance:listCustomIngressPortDomain	授予权限以获取实例自定义入方向端口绑定的域名信息列表。	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

apig的API通常对应着一个或多个授权项。表5-189展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-189 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /{project_id}/apigw/instances/{instance_id}/acls	apig:acl:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/acls	apig:acl:create	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/acls	apig:acl:batchDelete	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/acls/{acl_id}	apig:acl:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/acls/{acl_id}	apig:acl:get	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/acls/{acl_id}	apig:acl:update	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/acl-bindings	apig:api:bindAcl	• apig:instance:get • apig:api:get • apig:acl:get

API	对应的授权项	依赖的授权项
PUT /{project_id}/apigw/instances/{instance_id}/acl-bindings	apig:api:batchUnbindAcl	• apig:instance:get • apig:api:get • apig:acl:get
DELETE /{project_id}/apigw/instances/{instance_id}/acl-bindings/{acl_bindings_id}	apig:api:unbindAcl	• apig:instance:get • apig:api:get • apig:acl:get
GET /{project_id}/apigw/instances/{instance_id}/acl-bindings/binded-acls	apig:api:listBoundAcl	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/acl-bindings/binded-apis	apig:acl:listBoundApi	• apig:instance:get • apig:acl:get
GET /{project_id}/apigw/instances/{instance_id}/acl-bindings/unbinded-apis	apig:acl:listUnboundApi	• apig:instance:get • apig:acl:get
POST /{project_id}/apigw/instances/{instance_id}/throttle-bindings	apig:api:bindRequestThrottling	• apig:instance:get • apig:api:get • apig:requestThrottling:get
PUT /{project_id}/apigw/instances/{instance_id}/throttle-bindings	apig:api:batchUnbindRequestThrottling	• apig:instance:get • apig:api:get • apig:requestThrottling:get
DELETE /{project_id}/apigw/instances/{instance_id}/throttle-bindings/{throttle_binding_id}	apig:api:unbindRequestThrottling	• apig:instance:get • apig:api:get • apig:requestThrottling:get

API	对应的授权项	依赖的授权项
GET /{project_id}/apigw/instances/{instance_id}/throttle-bindings/binded-apis	apig:requestThrottling:listBoundApi	• apig:instance:get • apig:requestThrottling:get
GET /{project_id}/apigw/instances/{instance_id}/throttle-bindings/binded-throttles	apig:api:listBoundRequestThrottling	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/throttle-bindings/unbinded-apis	apig:requestThrottling:listUnboundApi	• apig:instance:get • apig:requestThrottling:get
GET /{project_id}/apigw/instances/{instance_id}/api-groups	apig:apiGroup:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups	apig:apiGroup:create	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}	apig:apiGroup:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}	apig:apiGroup:get	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}	apig:apiGroup:update	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups/check	apig:apiGroup:checkApiGroupNameExistOrNot	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/apis	apig:api:list	• apig:instance:get • apig:apiGroup:get

API	对应的授权项	依赖的授权项
POST /{project_id}/apigw/instances/{instance_id}/apis	apig:api:create	• apig:instance:get • apig:apiGroup:get • apig:loadBalanceChannel:get • apig:customAuthorizer:get • functiongraph:function:getFunctionConfig
DELETE /{project_id}/apigw/instances/{instance_id}/apis/{api_id}	apig:api:delete	• apig:instance:get • apig:apiGroup:get
GET /{project_id}/apigw/instances/{instance_id}/apis/{api_id}	apig:api:get	• apig:instance:get • apig:apiGroup:get
PUT /{project_id}/apigw/instances/{instance_id}/apis/{api_id}	apig:api:update	• apig:instance:get • apig:apiGroup:get • apig:loadBalanceChannel:get • apig:customAuthorizer:get • functiongraph:function:getFunctionConfig
POST /{project_id}/apigw/instances/{instance_id}/apis/action	apig:api:onlineOrOffline	• apig:instance:get • apig:apiGroup:get • apig:environment:list
-	apig:api:batchDelete	• apig:instance:get • apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/apis/check	apig:api:checkApiPathOrApiNameExistOrNot	• apig:instance:get • apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/apis/debug/{api_id}	apig:api:debug	• apig:instance:get • apig:apiGroup:get

API	对应的授权项	依赖的授权项
POST /{project_id}/apigw/instances/{instance_id}/apis/publish	apig:api:batchOnlineOrOffline	• apig:instance:get • apig:apiGroup:get • apig:environment:list
GET /{project_id}/apigw/instances/{instance_id}/apis/publish/{api_id}	apig:api:listHistoryVersion	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/apis/publish/{api_id}	apig:api:switchVersion	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/apis/runtime/{api_id}	apig:api:getRuntimeDefinition	• apig:instance:get • apig:environment:list
DELETE /{project_id}/apigw/instances/{instance_id}/apis/versions/{version_id}	apig:api:deleteHistoryVersion	• apig:instance:get • apig:apiGroup:get • apig:environment:list
GET /{project_id}/apigw/instances/{instance_id}/apis/versions/{version_id}	apig:api:getHistoryVersion	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/apps	apig:app:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/apps	apig:app:create	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/apps/{app_id}	apig:app:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}	apig:app:get	apig:instance:get

API	对应的授权项	依赖的授权项
PUT /{project_id}/apigw/instances/{instance_id}/apps/{app_id}	apig:app:update	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes	apig:app:listAppCode	• apig:instance:get • apig:app:get
POST /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes	apig:app:createAppCode	• apig:instance:get • apig:app:get
PUT /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes	apig:app:generateAppCode	• apig:instance:get • apig:app:get
DELETE /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes/{app_code_id}	apig:app:deleteAppCode	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes/{app_code_id}	apig:app:getAppCode	• apig:instance:get • apig:app:get
PUT /{project_id}/apigw/instances/{instance_id}/apps/secret/{app_id}	apig:app:resetSecret	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/apps/validation/{app_id}	apig:app:validate	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/bound-quota	apig:app:getBoundQuota	• apig:instance:get • apig:app:get
POST /{project_id}/apigw/instances/{instance_id}/app-auths	apig:app:bindApi	• apig:instance:get • apig:app:get • apig:api:get

API	对应的授权项	依赖的授权项
DELETE /{project_id}/apigw/instances/{instance_id}/app-auths/{app_auth_id}	apig:app:unbindApi	• apig:instance:get • apig:app:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/app-auths/binded-apis	apig:app:listBoundApi	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/app-auths/binded-apps	apig:api:listBoundApp	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/app-auths/unbinded-apis	apig:app:listUnboundApi	• apig:instance:get • apig:app:get
POST /{project_id}/apigw/instances/{instance_id}/openapi/export	apig:api:export	• apig:instance:get • apig:api:list • apig:api:get • apig:api:listBoundAcl • apig:acl:get • apig:api:listBoundRequestThrottling • apig:requestThrottling:get • apig:apiGroup:get • apig:apiGroup:getGatewayResponse • apig:environment:list • apig:api:listBoundPlugin • apig:plugin:get

API	对应的授权项	依赖的授权项
POST /{project_id}/apigw/instances/{instance_id}/openapi/async-export	apig:api:export	• apig:instance:get • apig:api:list • apig:api:get • apig:api:listBoundAcl • apig:acl:get • apig:api:listBoundRequestThrottling • apig:requestThrottling:get • apig:apiGroup:get • apig:apiGroup:getGatewayResponse • apig:environment:list • apig:api:listBoundPlugin • apig:plugin:get
POST /{project_id}/apigw/instances/{instance_id}/openapi/import	apig:api:import	• apig:instance:get • apig:api:get • apig:acl:get • apig:requestThrottling:get • apig:apiGroup:get • apig:apiGroup:getGatewayResponse • apig:environment:list • apig:plugin:get
POST /{project_id}/apigw/instances/{instance_id}/openapi/async-import	apig:api:import	• apig:instance:get • apig:api:get • apig:acl:get • apig:requestThrottling:get • apig:apiGroup:get • apig:apiGroup:getGatewayResponse • apig:environment:list • apig:plugin:get
GET /{project_id}/apigw/instances/{instance_id}/async-tasks/{task_id}	apig:asyncTask:get	apig:instance:get

API	对应的授权项	依赖的授权项
GET /{project_id}/apigw/certificates	apig:certificate:list	-
POST /{project_id}/apigw/certificates	apig:certificate:create	apig:instance:get
DELETE /{project_id}/apigw/certificates/{certificate_id}	apig:certificate:delete	-
GET /{project_id}/apigw/certificates/{certificate_id}	apig:certificate:get	-
PUT /{project_id}/apigw/certificates/{certificate_id}	apig:certificate:update	apig:instance:get
GET /{project_id}/apigw/certificates/{certificate_id}/attached-domains	apig:certificate:listBoundDomain	-
POST /{project_id}/apigw/certificates/{certificate_id}/domains/attach	apig:certificate:batchBindDomain	• apig:certificate:get • apig:apiGroup:get
POST /{project_id}/apigw/certificates/{certificate_id}/domains/detach	apig:certificate:batchUnbindDomain	• apig:certificate:get • apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificates/attach	apig:apiGroup:batchBindCertificateToDomain	• apig:instance:get • apig:apiGroup:get • apig:certificate:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificates/detach	apig:apiGroup:batchUnbindCertificateFromDomain	• apig:instance:get • apig:apiGroup:get • apig:certificate:get

API	对应的授权项	依赖的授权项
GET /{project_id}/apigw/instances/{instance_id}/vpc-channels	apig:loadBalanceChannel:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-channels	apig:loadBalanceChannel:create	• apig:instance:get • cce:cluster:getCluster • ecs:cloudServers:showServer • cce:cluster:generateClientCredential
DELETE /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}	apig:loadBalanceChannel:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}	apig:loadBalanceChannel:get	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}	apig:loadBalanceChannel:update	• apig:instance:get • cce:cluster:getCluster • ecs:cloudServers:showServer • cce:cluster:generateClientCredential
PUT /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/health-config	apig:loadBalanceChannel:updateHealthCheckConfig	• apig:instance:get • apig:loadBalanceChannel:get
GET /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups	apig:loadBalanceChannel:listServerGroup	• apig:instance:get • apig:loadBalanceChannel:get

API	对应的授权项	依赖的授权项
POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups	apig:loadBalanceChannel:createServerGroup	• apig:instance:get • apig:loadBalanceChannel:get
DELETE /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id}	apig:loadBalanceChannel:deleteServerGroup	• apig:instance:get • apig:loadBalanceChannel:get
GET /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id}	apig:loadBalanceChannel:getServerGroup	• apig:instance:get • apig:loadBalanceChannel:get
PUT /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id}	apig:loadBalanceChannel:updateServerGroup	• apig:instance:get • apig:loadBalanceChannel:get
GET /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members	apig:loadBalanceChannel:listBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members	apig:loadBalanceChannel:createBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get • ecs:cloudServers:showServer
PUT /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members	apig:loadBalanceChannel:updateBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get • ecs:cloudServers:showServer

API	对应的授权项	依赖的授权项
DELETE /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/{member_id}	apig:loadBalanceChannel:deleteBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/batch-disable	apig:loadBalanceChannel:batchDisableBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/batch-enable	apig:loadBalanceChannel:batchEnableBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get
GET /{project_id}/apigw/instances/{instance_id}/tags	apig:instance:listTag	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/apis/{api_id}/attachable-plugins	apig:api:listUnboundPlugin	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/apis/{api_id}/attached-plugins	apig:api:listBoundPlugin	• apig:instance:get • apig:api:get
POST /{project_id}/apigw/instances/{instance_id}/apis/{api_id}/plugins/attach	apig:api:bindPlugin	• apig:instance:get • apig:api:get • apig:plugin:get
PUT /{project_id}/apigw/instances/{instance_id}/apis/{api_id}/plugins/detach	apig:api:unbindPlugin	• apig:instance:get • apig:api:get • apig:plugin:get

API	对应的授权项	依赖的授权项
GET /{project_id}/apigw/instances/{instance_id}/plugins	apig:plugin:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/plugins	apig:plugin:create	• apig:instance:get • apig:loadBalanceChannel:get • functiongraph:function:getFunctionConfig
DELETE /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}	apig:plugin:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}	apig:plugin:get	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}	apig:plugin:update	• apig:instance:get • apig:loadBalanceChannel:get • functiongraph:function:getFunctionConfig
POST /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attach	apig:plugin:bindApi	• apig:instance:get • apig:api:get • apig:plugin:get
GET /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attachable-apis	apig:plugin:listUnbindApi	• apig:instance:get • apig:plugin:get
GET /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attached-apis	apig:plugin:listBoundApi	• apig:instance:get • apig:plugin:get
PUT /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/detach	apig:plugin:unbindApi	• apig:instance:get • apig:api:get • apig:plugin:get

API	对应的授权项	依赖的授权项
GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses	apig:apiGroup:listGatewayResponse	• apig:instance:get • apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses	apig:apiGroup:createGatewayResponse	• apig:instance:get • apig:apiGroup:get
DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}	apig:apiGroup:deleteGatewayResponse	• apig:instance:get • apig:apiGroup:get
GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}	apig:apiGroup:getGatewayResponse	• apig:instance:get • apig:apiGroup:get
PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}	apig:apiGroup:updateGatewayResponse	• apig:instance:get • apig:apiGroup:get
DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}/{response_type}	apig:apiGroup:deleteGatewayResponseType	• apig:instance:get • apig:apiGroup:get
GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}/{response_type}	apig:apiGroup:getGatewayResponseType	• apig:instance:get • apig:apiGroup:get

API	对应的授权项	依赖的授权项
PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}/{response_type}	apig:apiGroup:updateGatewayResponseType	• apig:instance:get • apig:apiGroup:get
GET /{project_id}/apigw/instances/{instance_id}/resources/outline/apis	apig:instance:listApiOutline	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/resources/outline/apps	apig:instance:listAppOutline	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/resources/outline/groups	apig:instance:listApiGroupOutline	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/env-variables	apig:environmentVariable:list	• apig:instance:get • apig:apiGroup:get • apig:environment:list
POST /{project_id}/apigw/instances/{instance_id}/env-variables	apig:environmentVariable:create	• apig:instance:get • apig:apiGroup:get • apig:environment:list
DELETE /{project_id}/apigw/instances/{instance_id}/env-variables/{env_variable_id}	apig:environmentVariable:delete	• apig:instance:get • apig:apiGroup:get • apig:environment:list
GET /{project_id}/apigw/instances/{instance_id}/env-variables/{env_variable_id}	apig:environmentVariable:get	• apig:instance:get • apig:apiGroup:get • apig:environment:list

API	对应的授权项	依赖的授权项
PUT /{project_id}/apigw/instances/{instance_id}/env-variables/{env_variable_id}	apig:environmentVariable:update	• apig:instance:get • apig:apiGroup:get • apig:environment:list
GET /{project_id}/apigw/instances/{instance_id}/envs	apig:environment:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/envs	apig:environment:create	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/envs/{env_id}	apig:environment:delete	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/envs/{env_id}	apig:environment:update	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/metric-data	apig:instance:listMetricData	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/statistics/api/latest	apig:instance:listApiMonitoring	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/statistics/group/latest	apig:instance:listApiGroupMonitoring	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/throttles	apig:requestThrottling:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/throttles	apig:requestThrottling:create	apig:instance:get

API	对应的授权项	依赖的授权项
DELETE /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}	apig:requestThrottling:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}	apig:requestThrottling:get	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}	apig:requestThrottling:update	apig:instance:get
-	apig:requestThrottling:batchDelete	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/sign-bindings	apig:api:bindSignatureKey	• apig:instance:get • apig:api:get • apig:signatureKey:list
DELETE /{project_id}/apigw/instances/{instance_id}/sign-bindings/{sign_bindings_id}	apig:api:unbindSignatureKey	• apig:instance:get • apig:api:get • apig:signatureKey:list
GET /{project_id}/apigw/instances/{instance_id}/sign-bindings/binded-apis	apig:signatureKey:listBoundApi	• apig:instance:get • apig:signatureKey:list
GET /{project_id}/apigw/instances/{instance_id}/sign-bindings/binded-signs	apig:api:listBoundSignatureKey	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/sign-bindings/unbinded-apis	apig:signatureKey:listUnboundApi	• apig:instance:get • apig:signatureKey:list

API	对应的授权项	依赖的授权项
GET /{project_id}/apigw/instances/{instance_id}/signs	apig:signatureKey:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/signs	apig:signatureKey:create	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/signs/{sign_id}	apig:signatureKey:delete	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/signs/{sign_id}	apig:signatureKey:update	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials	apig:requestThrottling:listSpecial	• apig:instance:get • apig:requestThrottling:get
POST /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials	apig:requestThrottling:createSpecial	• apig:instance:get • apig:requestThrottling:get
DELETE /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials/{strategy_id}	apig:requestThrottling:deleteSpecial	• apig:instance:get • apig:requestThrottling:get
PUT /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials/{strategy_id}	apig:requestThrottling:updateSpecial	• apig:instance:get • apig:requestThrottling:get

API	对应的授权项	依赖的授权项
GET /{project_id}/apigw/instances/{instance_id}/instance-tags	apig:instance:listSingleInstanceTag	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/instance-tags/action	apig:instance:batchCreateOrDeleteTag	apig:instance:get
GET /{project_id}/apigw/instance-tags	apig::listTag	apig:instance:get
POST /{project_id}/apigw/resource-instances/count	apig:instance:getNumByTags	-
POST /{project_id}/apigw/resource-instances/filter	apig:instance:listByTags	-
GET /{project_id}/apigw/instances	apig:instance:list	-
POST /{project_id}/apigw/instances	apig:instance:create	• vpc:securityGroups:get • vpc:ports:create • vpc:ports:update • eip:publicIps:get • eip:publicIps:update • eps:enterpriseProjects:list
DELETE /{project_id}/apigw/instances/{instance_id}	apig:instance:delete	• eip:publicIps:get • eip:publicIps:update • vpc:ports:delete
GET /{project_id}/apigw/instances/{instance_id}	apig:instance:get	-
PUT /{project_id}/apigw/instances/{instance_id}	apig:instance:update	• vpc:securityGroups:get • vpc:ports:update
DELETE /{project_id}/apigw/instances/{instance_id}/eip	apig:instance:unbindEip	• apig:instance:get • eip:publicIps:update
PUT /{project_id}/apigw/instances/{instance_id}/eip	apig:instance:bindOrChangeEip	• apig:instance:get • eip:publicIps:update

API	对应的授权项	依赖的授权项
DELETE /{project_id}/apigw/instances/{instance_id}/nat-eip	apig:instance:deleteOutboundEip	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/nat-eip	apig:instance:createOutboundEip	• apig:instance:get • vpc:ports:get
PUT /{project_id}/apigw/instances/{instance_id}/nat-eip	apig:instance:changeOutboundEipBandwidth	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/progress	apig:instance:getCreateProgress	-
DELETE /{project_id}/apigw/instances/{instance_id}/ingress-eip	apig:instance:deleteIngressEip	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/ingress-eip	apig:instance:createIngressEip	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/ingress-eip	apig:instance:changeIngressEipBindwidth	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/postpaid-resize	apig:instance:resize	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/restriction	apig:instance:getRestriction	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/features	apig:instance:listParameter	apig:instance:get

API	对应的授权项	依赖的授权项
POST /{project_id}/apigw/instances/{instance_id}/features	apig:instance:updateParameter	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/instance-features	apig:instance:listFeature	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/microservice/import	apig:instance:importMicroservice	• apig:instance:get • apig:api:create • apig:apiGroup:get • apig:apiGroup:create • apig:loadBalanceChannel:get • apig:loadBalanceChannel:create • cce:cluster:getCluster • cce:cluster:generateClientCredential
POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains	apig:apiGroup:bindDomain	• apig:instance:get • apig:apiGroup:get
DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}	apig:apiGroup:unbindDomain	• apig:instance:get • apig:apiGroup:get
PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}	apig:apiGroup:updateDomainConfig	• apig:instance:get • apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate	apig:apiGroup:createAndBindCertificateToDomain	• apig:instance:get • apig:apiGroup:get • apig:certificate:get

API	对应的授权项	依赖的授权项
DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate/{certificate_id}	apig:apiGroup:unbindAndDeleteCertificateFromDomain	• apig:instance:get • apig:apiGroup:get • apig:certificate:get
GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate/{certificate_id}	apig:apiGroup:getCertificateOfDomain	• apig:instance:get • apig:apiGroup:get • apig:certificate:get
PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/sl-domain-access-settings	apig:apiGroup:updateSLDomainSetting	• apig:instance:get • apig:apiGroup:get
GET /{project_id}/apigw/instances/{instance_id}/authorizers	apig:customAuthorizer:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/authorizers	apig:customAuthorizer:create	• apig:instance:get • functiongraph:function:getFunctionConfig
DELETE /{project_id}/apigw/instances/{instance_id}/authorizers/{authorizer_id}	apig:customAuthorizer:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/authorizers/{authorizer_id}	apig:customAuthorizer:get	apig:instance:get

API	对应的授权项	依赖的授权项
PUT /{project_id}/apigw/instances/{instance_id}/authorizers/{authorizer_id}	apig:customAuthorizer:update	• apig:instance:get • functiongraph:function:getFunctionConfig
GET /{project_id}/apigw/instances/{instance_id}/vpc-endpoint/connections	apig:instance:listVpcEndpoint	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-endpoint/connections/action	apig:instance:acceptOrRejectVpcEndpointConnection	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/vpc-endpoint/permissions	apig:instance:listVpcEndpointPermission	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-endpoint/permissions/batch-add	apig:instance:batchAddVpcEndpointPermission	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-endpoint/permissions/batch-delete	apig:instance:batchDeleteVpcEndpointPermission	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-acl	apig:app:deleteAcl	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-acl	apig:app:getAcl	• apig:instance:get • apig:app:get
PUT /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-acl	apig:app:updateAcl	• apig:instance:get • apig:app:get

API	对应的授权项	依赖的授权项
GET /{project_id}/apigw/instances/{instance_id}/app-quotas	apig:clientQuota:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/app-quotas	apig:clientQuota:create	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}	apig:clientQuota:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}	apig:clientQuota:get	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}	apig:clientQuota:update	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/bound-apps	apig:clientQuota:listBoundApp	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/binding-apps	apig:clientQuota:bindApp	• apig:instance:get • apig:clientQuota:get
DELETE /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/bound-apps/{app_id}	apig:clientQuota:unbindApp	• apig:instance:get • apig:app:get • apig:clientQuota:get

API	对应的授权项	依赖的授权项
GET /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/bindable-apps	apig:clientQuota:listUnboundApp	• apig:instance:get • apig:clientQuota:get
-	apig:instance:listFeatureHistory	• apig:instance:get • apig:instance:listFeature
POST /{project_id}/apigw/instances/{instance_id}/custom-ingress-ports	apig:instance:addCustomIngressPort	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/custom-ingress-ports	apig:instance:listCustomIngressPort	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/custom-ingress-ports/{ingress_port_id}	apig:instance:deleteCustomIngressPort	• apig:instance:get • apig:instance:listCustomIngressPort
GET /{project_id}/apigw/instances/{instance_id}/custom-ingress-ports/{ingress_port_id}/domains	apig:instance:listCustomIngressPortDomain	• apig:instance:get • apig:apiGroup:get • apig:instance:listCustomIngressPort

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-190**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。

apig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 5-190 apig 支持的资源类型

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

条件（Condition）

apig服务不支持在SCP中的条件键中配置服务级的条件键。apig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 开发与运维

5.10.11.1 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 5-191 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/<tag-key>
servicestage:app:createApplication	授予用户创建应用权限	write	app	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
servicestage:app:modifyApplication	授予用户更新应用权限	write	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • g:RequestTag/<tag-key> • g:TagKeys
servicestage:app:deleteApplication	授予用户删除应用权限	write	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
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/<tag-key> • g:EnterpriseProjectId
servicestage:app:deleteConfiguration	授予用户删除应用配置权限	write	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
servicestage:app:modifyConfiguration	授予用户更新应用配置权限	write	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
servicestage:app:getComponent	授予用户查看指定应用组件权限	read	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型	条件键
servicestage:app:createComponent	授予用户创建应用组件权限	write	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
servicestage:app:modifyComponent	授予用户更新应用组件权限	write	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
servicestage:app:deleteComponent	授予用户删除应用组件权限	write	app	• g:ResourceTag/<tag-key> • 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/<tag-key> • g:TagKeys
servicestage:environment:get	授予用户查看环境信息权限	read	environment	• g:ResourceTag/<tag-key> • 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/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
servicestage:environment:delete	授予用户删除环境权限	write	environment	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型	条件键
servicestage:environment:tag	授予TMS用户创建环境标签权限	tagging	environment	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
servicestage:app:tag	授予TMS用户创建应用标签权限	tagging	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • 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/<tag-key> • 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/<tag-key> • g:TagKeys
servicestage:environment:unTagResource	授予TMS用户删除环境资源标签权限	tagging	environment	• g:ResourceTag/<tag-key> • g:RequestTag/<tag-key> • 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/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
servicestage:environment:listTags	授予TMS用户查询环境资源标签列表权限	read	-	-

授权项	描述	访问级别	资源类型	条件键
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	-
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	-

授权项	描述	访问级别	资源类型	条件键
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	-
servicestage:environment:listTagsForResource	授予eps用户查询环境资源标签列表权限	read	environment	• g:ResourceTag/<tag-key> • 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/<tag-key> • g:EnterpriseProjectId

ServiceStage的API通常对应着一个或多个授权项。表5-192展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-192 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	-

API	对应的授权项	依赖的授权项
PATCH /v2/{project_id}/cas/environments/{environment_id}/resources	servicestage:environment:modify	-
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	-

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/cas/applications/{application_id}/components/{component_id}	servicestage:app:modifyComponent	-
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	-

API	对应的授权项	依赖的授权项
DELETE /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}	servicestage:app:deleteComponent	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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5-193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 5-193 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。

5.10.11.2 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 5-194 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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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。

5.10.11.3 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 5-195 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	-	-
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	-	-

操作项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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5-196展示了API与操作项的关系，以及该API需要依赖的操作项。

表 5-196 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	-

API	对应的操作项	依赖的操作项
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	-
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	-

API	对应的操作项	依赖的操作项
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	-
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	-

API	对应的操作项	依赖的操作项
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	-
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	-

API	对应的操作项	依赖的操作项
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	-
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。

5.10.11.4 性能测试 CodeArts PerfTest

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 PerfTest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 PerfTest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 PerfTest的相关操作。

表 5-197 CodeArts PerfTest 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
codeartsperftest:privateResourceGroup:update	授予权限修改私有资源组。	write	privateResourceGroup	-
codeartsperftest:privateResourceGroup:list	授予权限查看私有资源组列表。	list	privateResourceGroup	-
codeartsperftest:privateResourceGroup:get	授予权限查看私有资源组。	read	privateResourceGroup	-
codeartsperftest:privateResourceGroup:delete	授予权限删除私有资源组。	write	privateResourceGroup	-
codeartsperftest:privateResourceGroup:create	授予权限创建私有资源组。	write	privateResourceGroup	-
codeartsperftest:jmeter:updateJmeterTask	授予权限修改JMeter任务。	write	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:updateJmeterProject	授予权限修改JMeter工程。	write	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:listJmeterTask	授予权限查看JMeter任务列表。	list	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:listJmeterProject	授予权限查看JMeter工程列表。	list	jmeter	-
codeartsperftest:jmeter:getJmeterTask	授予权限查看JMeter任务。	read	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:getJmeterProject	授予权限查看JMeter工程。	get	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:executeJmeterTask	授予权限执行或停止JMeter任务。	write	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:deleteJmeterTask	授予权限删除JMeter任务。	write	jmeter	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
codeartsperftest:jmeter:deleteJmeterProject	授予权限删除JMeter工程。	write	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:createJmeterTask	授予权限创建JMeter任务。	write	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:createJmeterResource	授予权限创建JMeter变量、jar包等。	write	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:createJmeterProject	授予权限创建JMeter工程。	write	jmeter	-
codeartsperftest:cpts:updatePerfTestTask	授予权限修改PerfTest任务。	write	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:updatePerfTestProject	授予权限修改PerfTest工程、用例、目录等。	write	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:listPerfTestTask	授予权限查看PerfTest任务列表。	list	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:listPerfTestProject	授予权限查看PerfTest工程列表。	list	cpts	-
codeartsperftest:cpts:getPerfTestTask	授予权限查看PerfTest任务。	read	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:getPerfTestProject	授予权限查看PerfTest工程。	read	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:executePerfTestTask	授予权限执行或停止PerfTest任务。	write	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:deletePerfTestTask	授予权限删除PerfTest任务。	write	cpts	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
codeartsperftest:cpts:deletePerfTestProject	授予权限删除PerfTest工程、用例、目录等。	write	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:createPerfTestTask	授予权限创建PerfTest任务。	write	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:createPerfTestResource	授予权限创建PerfTest用例、目录、变量等。	write	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:createPerfTestProject	授予权限创建PerfTest工程。	write	cpts	-
codeartsperftest::uploadFile	授予权限上传文件。	write	-	-
codeartsperftest::updateSlaTemplate	授予权限更新SLA模板。	write	-	-
codeartsperftest::updateCronTask	授予权限修改定时压测任务。	write	-	g:ResourceTag/<tag-key>
codeartsperftest::orderPackage	授予权限订购套餐包。	write	-	-
codeartsperftest::listTag	授予权限查看标签列表。	list	-	-
codeartsperftest::listSlaTemplate	授予权限展示SLA模板集。	list	-	-
codeartsperftest::listPackage	授予权限查看已订购的套餐包。	list	-	-
codeartsperftest::listCronTask	授予权限查看定时压测任务列表。	list	-	-
codeartsperftest::getTag	授予权限查看工程对应的标签。	read	-	-
codeartsperftest::getSlaTemplate	授予权限查看SLA模板。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
codeartsperftest::getCronTask	授予权限查看定时压测任务。	read	-	g:ResourceTag/<tag-key>
codeartsperftest::deleteTag	授予权限删除工程对应的标签。	tagging	-	• g:ResourceTag/<tag-key> • g:TagKeys
codeartsperftest::deleteSlaTemplate	授予权限删除SLA模板。	write	-	-
codeartsperftest::deleteCronTask	授予权限删除定时压测任务。	write	-	g:ResourceTag/<tag-key>
codeartsperftest::createTag	授予权限创建工程对应的标签。	tagging	-	• g:ResourceTag/<tag-key> • g:RequestTag/<tag-key> • g:TagKeys
codeartsperftest::createSlaTemplate	授予权限创建SLA模板。	write	-	-
codeartsperftest::createCronTask	授予权限创建定时压测任务。	write	-	g:ResourceTag/<tag-key>

CodeArts PerfTest的API通常对应着一个或多个授权项。表5-198展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-198 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}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/monitors	codeartsperftest:jmeter:updateJmeterTask	-
GET /v1/{project_id}/jmeter/test-suites	codeartsperftest:jmeter:listJmeterProject	-
POST /v1/{project_id}/jmeter/test-suites	codeartsperftest:jmeter:createJmeterProject	-
POST /v2/{project_id}/stress/apps	codeartsperftest:cpts:createPerfTestResource	-

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/periodic_package	codeartsperftest::orderPackage	-
PUT /v2/{project_id}/stress/apps/batch	codeartsperftest:cpts:updatePerfTestProject	-
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/fields	codeartsperftest:jmeter:updateJmeterTask	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/transactions/{transaction_id}	codeartsperftest:jmeter:getJmeterTask	-
POST /v1/{project_id}/stress/agents/plugin-packages/init-multipart	codeartsperftest::uploadFile	-
GET /v1/{project_id}/all-plugin-func/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
PUT /v2/{project_id}/stress/agents/batch-delete	codeartsperftest:cpts:deletePerfTestProject	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/file-variables	codeartsperftest:jmeter:listJmeterProject	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/transactions/{transaction_id}/index/{index}/css-log	codeartsperftest:jmeter:getJmeterTask	-
POST /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/batch-update-status	codeartsperftest:jmeter:executeJmeterTask	-
GET /v2/{project_id}/stress/apps/{id}	codeartsperftest:cpts:getPerfTestProject	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/event	codeartsperftest:jmeter:getJmeterTask	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/third-jar-packages	codeartsperftest:jmeter:getJmeterProject	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}	codeartsperftest:jmeter:getJmeterProject	-
DELETE /v2/{project_id}/stress/apps/{id}	codeartsperftest:cpts:deletePerfTestProject	-
POST /v1/{project_id}/templates/file-upload/{template_id}	codeartsperftest::uploadFile	-
GET /v2/{project_id}/stress/apps	codeartsperftest:cpts:getPerfTestProject	-
DELETE /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}	codeartsperftest:jmeter:deleteJmeterProject	-
GET /v1/{project_id}/all-plugin-list/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}	codeartsperftest:jmeter:updateJmeterTask	-
GET /v1/{project_id}/all-plugin-req/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/file-variables/{file_variable_id}/export	codeartsperftest:jmeter:getJmeterProject	-
DELETE /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/third-jar-packages/{third_jar_id}	codeartsperftest:jmeter:deleteJmeterProject	-

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/monitors/{monitor_id}	codeartsperftest:cpts:updatePerfTestProject	-
DELETE /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}	codeartsperftest:jmeter:deleteJmeterTask	-
GET /v1/{project_id}/order-package	codeartsperftest::orderPackage	-
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/monitors/{jmeter_monitor_id}	codeartsperftest:jmeter:updateJmeterProject	-
POST /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans	codeartsperftest:jmeter:createJmeterTask	-
POST /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/debug	codeartsperftest:jmeter:executeJmeterTask	-
DELETE /v1/{project_id}/templates/file-delete/{template_id}	codeartsperftest:cpts:updatePerfTestProject	-
GET /v2/{project_id}/stress/apps/apm/business	codeartsperftest:cpts:getPerfTestProject	-
POST /v2/{project_id}/stress/apps/batch-delete	codeartsperftest:cpts:deletePerfTestProject	-
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/thread-groups	codeartsperftest:jmeter:updateJmeterTask	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/third-jar-packages/{third_jar_id}/export	codeartsperftest:jmeter:getJmeterProject	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/reports/log-outline	codeartsperftest:jmeter:getJmeterTask	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/stress/apps/apm/app-info/batch-get	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/stress/agents/plugin-packages	codeartsperftest:cpts:getPerfTestProject	-
POST /v1/{project_id}/plugin-json-upload/test-suites/{test_suite_id}	codeartsperftest::uploadFile	-
GET /v1/{project_id}/test-suites/{test_suite_id}/tasks/{task_id}/link-apps	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/variable-file-download/variables/{variable_id}	codeartsperftest:cpts:getPerfTestProject	-
POST /v1/{project_id}/cce-agencies	codeartsperftest:privateResourceGroup:create	-
POST /v1/{project_id}/saveuser	codeartsperftest::listPackage	-
DELETE /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/monitors/{jmeter_monitor_id}	codeartsperftest:jmeter:deleteJmeterProject	-
POST /v1/{project_id}/test-suites/jmeter-upload	codeartsperftest:jmeter:createJmeterProject	-
POST /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/third-jar-packages/init-multipart	codeartsperftest::uploadFile	-
POST /v1/{project_id}/cpts-agencies	codeartsperftest:privateResourceGroup:create	-
POST /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/file-variables	codeartsperftest::uploadFile	-
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}	codeartsperftest:jmeter:updateJmeterProject	-
POST /v1/{project_id}/monitors	codeartsperftest:cpts:createPerfTestResource	-

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/monitors	codeartsperftest:jmeter:createJmeterResource	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/export	codeartsperftest:jmeter:getJmeterTask	-
GET /v1/{project_id}/all-plugin-check/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
POST /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks	codeartsperftest:jmeter:executeJmeterTask	-
POST /v1/{project_id}/variable-file-upload/test-suites/{test_suite_id}	codeartsperftest::uploadFile	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/monitors	codeartsperftest:jmeter:listJmeterProject	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans	codeartsperftest:jmeter:listJmeterTask	-
POST /v1/{project_id}/templates/clone/{test_suite_id}	codeartsperftest:cpts:createPerfTestResource	-
PUT /v2/{project_id}/stress/apps/{id}	codeartsperftest:cpts:updatePerfTestProject	-
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/file-variables	codeartsperftest::uploadFile	-
PUT /v1/{project_id}/variable-file-upload/test-suites/{test_suite_id}	codeartsperftest::uploadFile	-
POST /v3/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/debug	codeartsperftest:jmeter:updateJmeterTask	-
DELETE /v2/{project_id}/stress/agents/{id}	codeartsperftest:cpts:deletePerfTestProject	-

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/stress/agents/plugin-packages/upload	codeartsperftest::uploadFile	-
DELETE /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/file-variables/{file_variable_id}	codeartsperftest:jmeter:deleteJmeterProject	-
POST /v1/{project_id}/stress/agents	codeartsperftest:cpts:getPerfTestProject	-
PUT /v1/{project_id}/stress/agents/{agent_id}	codeartsperftest:cpts:updatePerfTestProject	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/csv	codeartsperftest:cpts:getPerfTestTask	-
DELETE /v1/{project_id}/prg/{prg_id}/file/{prg_file_id}	codeartsperftest:privateResourceGroup:delete	-
GET /v1/{project_id}/search/{name}	codeartsperftest:cpts:getPerfTestProject	-
PUT /v2/{project_id}/test-cases/{case_id}/sla/{sla_id}	codeartsperftest:cpts:updatePerfTestProject	-
GET /v1/{project_id}/tasksinfos	codeartsperftest:cpts:listPerfTestTask	-
GET /v2/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/case-run-infos/{case_run_id}/detail/{detail_id}/chart	codeartsperftest:jmeter:getJmeterTask	-
GET /v1/{project_id}/services/ondemand_order	codeartsperftest::listPackage	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/sla/statistic	codeartsperftest:cpts:getPerfTestTask	-
GET /v1/{project_id}/{resource_type}/{resource_id}/tags	codeartsperftest::getTag	-
DELETE /v3/{project_id}/tasks/{task_id}	codeartsperftest:cpts:deletePerfTestTask	-

API	对应的授权项	依赖的授权项
POST /v1/{project_id}/services/ondemand_order	codeartsperftest::orderPackage	-
GET /v1/{project_id}/clusters/{cluster_id}	codeartsperftest:privateResourceGroup:get	-
GET /v2/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/case-run-infos/{case_run_id}/detail	codeartsperftest:jmeter:getJmeterTask	-
POST /v1/{project_id}/templates	codeartsperftest:cpts:createPerfTestResource	-
DELETE /v1/{project_id}/tasks/{task_id}	codeartsperftest:cpts:deletePerfTestTask	-
PUT /v1/{project_id}/task-cases/{case_id}/target/{target}	codeartsperftest:cpts:updatePerfTestProject	-
GET /v1/{project_id}/test-suites/count	codeartsperftest:cpts:listPerfTestProjectcodeartsperftest:jmeter:listJmeterProject(代码里判断具体用哪个)	-
GET /v2/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/cases	codeartsperftest:jmeter:getJmeterTask	-
PUT /v2/{project_id}/debug/tasks/{id}/stop	codeartsperftest:cpts:updatePerfTestProject	-
GET /v1/{project_id}/test-suites/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
PUT /v1/{project_id}/prgs/{prg_id}	codeartsperftest:privateResourceGroup:update	-
GET /v1/{project_id}/packages	codeartsperftest::listPackage	-
POST /v2/{project_id}/debug/tasks/batch-get	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/{resource_type}/tags	codeartsperftest::listTag	-
DELETE /v1/{project_id}/test-suites/{test_suite_id}	codeartsperftest:cpts:deletePerfTestProject	-

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/prgs/{prg_id}/ext	codeartsperftest:privateResourceGroup:update	-
POST /v1/{project_id}/{resource_type}/{resource_id}/tags/create	codeartsperftest::createTag	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/stages	codeartsperftest:cpts:getPerfTestTask	-
GET /v2/{project_id}/jmeter/test-suites/{jmeter_project_id}/monitors	codeartsperftest:jmeter:listJmeterProject	-
GET /v1/{project_id}/slas	codeartsperftest::listSlaTemplate	-
GET /v1/{project_id}/test-suites/upload/processes	codeartsperftest:cpts:getPerfTestProject	-
PUT /v1/{project_id}/templates/{template_id}	codeartsperftest:cpts:updatePerfTestProject	-
GET /v2/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/reports/details	codeartsperftest:jmeter:getJmeterTask	-
PUT /v1/{project_id}/test-suites/{test_suite_id}	codeartsperftest:cpts:updatePerfTestProject	-
GET /v2/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/reports/log-outline	codeartsperftest:jmeter:getJmeterTask	-
GET /v1/{project_id}/monitors-by-task/{task_id}	codeartsperftest:cpts:getPerfTestTask	-
DELETE /v1/{project_id}/{resource_type}/{resource_id}/tags/delete	codeartsperftest::deleteTag	-
POST /v1/{project_id}/domain-bindings-all/{test_suite_id}	codeartsperftest:cpts:createPerfTestResource	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/cron-task/execute-time	codeartsperftest::getCronTask	-
GET /v1/{project_id}/resources/nodes/scaling/{prg_id}	codeartsperftest:privateResourceGroup:get	-
GET /v2/{project_id}/task-run-infos/{task_run_id}/reports/details	codeartsperftest:cpts:getPerfTestTask	-
GET /v1/{project_id}/monitors-by-run-id/{run_id}	codeartsperftest:cpts:getPerfTestTask	-
PUT /v1/{project_id}/sla/{sla_id}	codeartsperftest::updateSlaTemplate	-
GET /v1/{project_id}/templates/{template_id}	codeartsperftest:cpts:getPerfTestProject	-
POST /v1/{project_id}/test-suites	codeartsperftest:cpts:createPerfTestProject	-
DELETE /v1/{project_id}/task-cases/{case_id}	codeartsperftest:cpts:deletePerfTestProject	-
DELETE /v2/{project_id}/debug/tasks/{id}	codeartsperftest:cpts:deletePerfTestProject	-
GET /v2/{project_id}/test-cases/{case_id}	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/variables/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
DELETE /v2/{project_id}/test-cases/{case_id}	codeartsperftest:cpts:deletePerfTestProject	-
POST /v2/{project_id}/test-cases/{case_id}/sla	codeartsperftest:cpts:createPerfTestResource	-
POST /v3/{project_id}/tasks	codeartsperftest:cpts:createPerfTestTask	-
PUT /v1/{project_id}/test-suites/{test_suite_id}/directory/{directory_id}	codeartsperftest:cpts:updatePerfTestProject	-
GET /v1/{project_id}/agencies/all	codeartsperftest:privateResourceGroup:get	-
GET /v1/{project_id}/tasks/history-run-list/{task_id}	codeartsperftest:cpts:listPerfTestTask	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/task-run-infos/{task_run_id}/details/export	codeartsperftest:cpts:getPerfTestTask	-
GET /v2/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/detail	codeartsperftest:cpts:getPerfTestTask	-
POST /v1/{project_id}/templates/swagger-import/{test_suite_id}/contract-id/{contract_id}/model-id/{model_id}	codeartsperftest:cpts:createPerfTestResource	-
PUT /v1/{project_id}/variables/{test_suite_id}	codeartsperftest:cpts:updatePerfTestProject	-
POST /v1/{project_id}/test-suites/{test_suit_id}/tasks/batch-update-task-status	codeartsperftest:cpts:executePerfTestTask	-
GET /v1/{project_id}/variables/{variable_type}/test-suites/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/cron-task	codeartsperftest::listCronTask	-
POST /v1/{project_id}/tasks	codeartsperftest:cpts:createPerfTestTask	-
GET /v1/{project_id}/test-suites	codeartsperftest:cpts:listPerfTestProject	-
POST /v1/{project_id}/prg/{prg_id}/upload	codeartsperftest::uploadFile	-
POST /v1/{project_id}/{resource_type}/resource-instances/count	codeartsperftest::listTag	-
POST /v1/{project_id}/test-suites/download	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/all-tasks/{test_suite_id}	codeartsperftest:cpts:listPerfTestTask	-
GET /v1/{project_id}/tasks/{task_id}	codeartsperftest:cpts:getPerfTestTask	-

API	对应的授权项	依赖的授权项
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/multi-third-jar-packages/{third_jar_id}	codeartsperftest::uploadFile	-
GET /v1/{project_id}/cron-task/{cron_task_id}	codeartsperftest::getCronTask	-
POST /v1/{project_id}/prgs	codeartsperftest:privateResourceGroup:create	-
GET /v2/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/details/export	codeartsperftest:jmeter:getJmeterTask	-
GET /v1/{project_id}/monitor-list/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/invite-features	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/prgs/{prg_id}	codeartsperftest:privateResourceGroup:get	-
POST /v1/{project_id}/packages	codeartsperftest::orderPackage	-
DELETE /v1/{project_id}/prgs/{prg_id}/ext/{ext_id}	codeartsperftest:privateResourceGroup:delete	-
GET /v1/{project_id}/tasks/history-run-info/{run_id}	codeartsperftest:cpts:getPerfTestTask	-
DELETE /v1/{project_id}/cron-task/{cron_task_id}	codeartsperftest::deleteCronTask	-
GET /v1/{project_id}/test-suites/{test_suite_id}/directory	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/event/sla	codeartsperftest:cpts:getPerfTestTask	-
POST /v2/{project_id}/test-cases/batch-delete	codeartsperftest:cpts:deletePerfTestProject	-
PUT /v1/{project_id}/monitors-by-task/{task_id}	codeartsperftest:cpts:updatePerfTestTask	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/pods-info/{exec_info_id}	codeartsperftest:cpts:getPerfTestTask	-
GET /v1/{project_id}/clusters	codeartsperftest:privateResourceGroup:list	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}	codeartsperftest:jmeter:getJmeterTask	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/reports	codeartsperftest:cpts:getPerfTestTask	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/index/{index}/debug-result	codeartsperftest:cpts:getPerfTestTask	-
PUT /v3/{project_id}/tasks/{task_id}	codeartsperftest:cpts:updatePerfTestTask	-
DELETE /v2/{project_id}/test-cases/{case_id}/sla/{sla_id}	codeartsperftest:cpts:deletePerfTestProject	-
POST /v1/{project_id}/templates/swagger-insert/{test_suite_id}	codeartsperftest:cpts:createPerfTestResource	-
DELETE /v1/{project_id}/prgs/{prg_id}/delete_forced	codeartsperftest:privateResourceGroup:delete	-
GET /v2/{project_id}/test-cases/{case_id}/slas	codeartsperftest:cpts:getPerfTestProject	-
PUT /v1/{project_id}/test-suites/{test_suite_id}/domain-binding/{domain_binding_id}	codeartsperftest:cpts:updatePerfTestProject	-
POST /v1/{project_id}/test-suites/{test_suite_id}/tasks/{task_id}	codeartsperftest:cpts:updatePerfTestTask	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/index/{index}/css-log	codeartsperftest:cpts:getPerfTestTask	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/test-suites/{test_suite_id}/cases/{case_id}/debug	codeartsperftest:cpts:updatePerfTestProject	-
POST /v1/{project_id}/cron-task	codeartsperftest::createCronTask	-
POST /v1/{project_id}/templates/upload/{template_id}	codeartsperftest:cpts:createPerfTestResource	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/icon-metrics	codeartsperftest:cpts:getPerfTestTask	-
GET /v2/{project_id}/debug/tasks	codeartsperftest:cpts:getPerfTestProject	-
GET /v2/{project_id}/task-run-infos/{task_run_id}/cases	codeartsperftest:cpts:getPerfTestTask	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/event	codeartsperftest:cpts:getPerfTestTask	-
PUT /v1/{project_id}/cron-task/{cron_task_id}	codeartsperftest::updateCronTask	-
GET /v2/{project_id}/monitor-list/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/test-suites/{test_suit_id}/tasks/{task_id}/test-cases	codeartsperftest:cpts:getPerfTestTask	-
DELETE /v1/{project_id}/test-suites/{test_suite_id}/directory/{directory_id}	codeartsperftest:cpts:deletePerfTestProject	-
POST /v1/{project_id}/prgs/{prg_id}/ext	codeartsperftest:privateResourceGroup:create	-
GET /v2/{project_id}/tasks/{task_id}	codeartsperftest:cpts:getPerfTestTask	-
PUT /v1/{project_id}/domain-bindings-all/{test_suite_id}	codeartsperftest:cpts:updatePerfTestProject	-
POST /v1/{project_id}/sla	codeartsperftest::createSlaTemplate	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/variables	codeartsperftest:jmeter:getJmeterTask	-
POST /v1/{project_id}/{resource_type}/resource-instances/filter	codeartsperftest::listTag	-
POST /v1/{project_id}/test-suites/{test_suite_id}/directory	codeartsperftest:cpts:createPerfTestResource	-
PUT /v1/{project_id}/cron-task/{cron_task_id}/status	codeartsperftest::updateCronTask	-
GET /v1/{project_id}/prgs	codeartsperftest:privateResourceGroup:list	-
GET /v2/{project_id}/task-run-infos/{task_run_id}/reports/log-outline	codeartsperftest:cpts:getPerfTestTask	-
DELETE /v1/{project_id}/sla/{sla_id}	codeartsperftest::deleteSlaTemplate	-
PUT /v1/{project_id}/tasks/{task_id}	codeartsperftest:cpts:updatePerfTestTask	-
GET /v1/{project_id}/sla/{sla_id}	codeartsperftest::getSlaTemplate	-
DELETE /v1/{project_id}/prgs/{prg_id}	codeartsperftest:privateResourceGroup:delete	-
GET /v1/{project_id}/domain-bindings-all/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
POST /v3/{project_id}/test-suites/{test_suite_id}/cases/{case_id}/debug	codeartsperftest:cpts:updatePerfTestProject	-
POST /v1/{project_id}/variable-file-upload/init-multipart	codeartsperftest::uploadFile	-
POST /v1/{project_id}/templates/swagger-upload/{test_suite_id}	codeartsperftest:cpts:createPerfTestResource	-
GET /v2/{project_id}/test-cases/{case_id}/rel-temp-tasks	codeartsperftest:cpts:getPerfTestTask	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/test-cases	codeartsperftest:cpts:createPerfTestResource	-
PUT /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/stages	codeartsperftest:cpts:updatePerfTestTask	-
PUT /v2/{project_id}/test-cases/{case_id}	codeartsperftest:cpts:updatePerfTestProject	-
POST /v2/{project_id}/test-cases/batch-run	codeartsperftest:cpts:executePerfTestTask	-
POST /v1/{project_id}/task-cases	codeartsperftest:cpts:createPerfTestResource	-
GET /v1/{project_id}/prg/{prg_id}/files	codeartsperftest:privateResourceGroup:get	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/history-tasks	codeartsperftest:jmeter:getJmeterTask	-
GET /v1/{project_id}/all-templates/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/prg/regions	codeartsperftest:privateResourceGroup:get	-
GET /v2/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/detail/{detail_id}/chart	codeartsperftest:cpts:getPerfTestTask	-
POST /v1/{project_id}/test-suites/{test_suite_id}/tasks/{task_id}/cases/{case_id}/debug	codeartsperftest:cpts:updatePerfTestProject	-
DELETE /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/multi-third-jar-packages	codeartsperftest::uploadFile	-
POST /v1/{project_id}/domain-binding/{domain_binding_id}	codeartsperftest:cpts:deletePerfTestProject	-

API	对应的授权项	依赖的授权项
DELETE /v1/{project_id}/test-suites/upload	codeartsperftest:cpts:createPerfTestProject&&codeartsperftest:cpts:createPerfTestResource	-
PUT /v1/{project_id}/monitors/{monitor_id}	codeartsperftest:cpts:deletePerfTestProject	-
DELETE /v1/{project_id}/prgs/{prg_id}/ratio	codeartsperftest:privateResourceGroup:update	-
DELETE /v1/{project_id}/templates/{template_id}	codeartsperftest:cpts:deletePerfTestProject	-
GET /v1/{project_id}/variables	codeartsperftest:cpts:deletePerfTestProject	-
POST /v1/{project_id}/prg/upload/{upload_id}/processes	codeartsperftest:privateResourceGroup:get	-
GET /v1/{project_id}/variables/{test_suite_id}	codeartsperftest:cpts:createPerfTestProject	-
POST /v1/{project_id}/test-suites/{test_suit_id}/tasks/{task_id}/cron-tasks	codeartsperftest:cpts:getPerfTestTask	-
POST /v1/{project_id}/column/check-name	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/cron-tasks	codeartsperftest:jmeter:getJmeterTask	-
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/update-report-name	codeartsperftest:jmeter:getJmeterTask	-
PUT /v1/{project_id}/task-run-infos/{task_run_id}/update-report-name	codeartsperftest:cpts:getPerfTestTask	-
POST /v1/test-suites/upload-java/json-file	codeartsperftest:cpts:createPerfTestProject codeartsperftest:cpts:createPerfTestResource	-
POST /v1/test-suites/upload-java/init-multipart	codeartsperftest::uploadFile	-

API	对应的授权项	依赖的授权项
POST /v1/test-suites/upload-java/test-suites/{test_suite_id}	codeartsperftest::uploadFile	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-199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。

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

表 5-199 CodeArts PerfTest 支持的资源类型

资源类型	URN
cpts	codeartsperftest:<region>:<account-id>:cpts:<test-suite-name>
jmeter	codeartsperftest:<region>:<account-id>:jmeter:<test-suite-name>
privateResourceGroup	codeartsperftest:<region>:<account-id>:privateResourceGroup:<resource-group-name>

条件（Condition）

CodeArts PerfTest不支持在SCP中的条件键中配置服务级的条件键。

CodeArts PerfTest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。

5.10.12 企业应用

5.10.12.1 云解析服务 DNS

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DNS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DNS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DNS的相关操作。

表 5-200 DNS 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
dns:zone:list	授予列出域名的权限。	list	zone *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dns:zone:create	授予创建域名的权限。	write	zone *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dns:zone:createBatchPublicZonesByName	授予根据Zone Name批量创建域名的权限。	write	zone *	-
			-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
dns:zone:get	授予获取域名的权限。	read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:update	授予更新域名的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:delete	授予删除域名的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:associaterouter	授予将内网域名与VPC关联的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:disassociaterouter	授予取消内网域名与VPC关联的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:setProxyPattern	授予设置内网域名递归解析代理的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:transfer	授予创建公网域名转移任务的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:list	授予列出记录集的权限。	list	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:create	授予创建记录集的权限。	write	zone *	• 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
			-	• dns:RecordSetNames • dns:RecordSetTypes
dns:recordset:get	授予获取记录集的权限。	read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:update	授予更新记录集的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• dns:RecordSetNames • dns:RecordSetTypes
dns:recordset:delete	授予删除记录集的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• dns:RecordSetNames • dns:RecordSetTypes
dns:zone:setStatus	授予设置域名状态的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:setStatus	授予设置记录集状态的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• dns:RecordSetNames • dns:RecordSetTypes
dns:ptr:list	授予列出PTR记录的权限。	list	ptr *	-

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
dns:ptr:get	授予获取单个PTR记录的权限。	read	ptr *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:ptr:create	授予创建PTR记录的权限。	write	ptr *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dns:ptr:update	授予更新PTR记录的权限。	write	ptr *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:ptr:delete	授予删除PTR记录的权限。	write	ptr *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:tag:get	授予查询域名标签的权限。	read	zone	-
dns:tag:get	授予查询域名标签的权限。	read	ptr	-
dns:tag:set	授予为域名设置标签的权限。	tagging	zone	g:ResourceTag/<tag-key>
dns:tag:set	授予为域名设置标签的权限。	tagging	ptr	g:ResourceTag/<tag-key>
dns:zone:createRetrieval	授予找回域名的权限。	write	-	-
dns:zone:getRetrieval	授予查询域名找回状态的权限。	read	-	-
dns:customLine:create	授予创建自定义线路的权限。	write	customLine *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dns:customLine:list	授予列出自定义线路的权限。	list	customLine *	-
dns:customLine:delete	授予删除自定义线路的权限。	write	customLine *	-
dns:customLine:update	授予更新自定义线路的权限。	write	customLine *	-
dns:nameserver:list	授予列出名称服务器的权限。	list	-	-
dns:nameserver:getZoneNameServer	授予查询公网域名的DNS服务器的权限。	read	-	-
dns:quota:list	授予列出租户配额的权限。	list	-	-
dns:recordset:getPrivateRecordSetImport	授予查询内网RecordSet导入任务的权限。	read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:getPrivateRecordSetImportTemplate	授予下载内网RecordSet导入模板的权限。	read	-	-
dns:recordset:createPrivateRecordSetImport	授予创建内网RecordSet导入任务的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:deletePrivateRecordSetImportTask	授予删除内网RecordSet导入任务的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:createPublicRecordSetImport	授予创建公网RecordSet导入任务的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:getPublicRecordSetImport	授予查询公网RecordSet导入任务的权限。	read	zone *	• 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
dns:recordset:getPublicRecordSetImportTemplate	授予下载公网RecordSet导入模板的权限。	read	-	-
dns:recordset:deletePublicRecordSetImportTask	授予删除公网RecordSet导入任务的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:getExport	授予导出zone的权限。	read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:lineGroup:create	授予创建线路分组的权限。	write	lineGroup *	-
dns:lineGroup:list	授予列出线路分组的权限。	list	lineGroup *	-
dns:lineGroup:get	授予查询单个线路分组的权限。	read	lineGroup *	-
dns:lineGroup:delete	授予删除线路分组的权限。	write	lineGroup *	-
dns:lineGroup:update	授予更新线路分组的权限。	write	lineGroup *	-
dns:endpoint:create	授予创建终端节点的权限。	write	endpoint *	-
dns:endpoint:list	授予列出终端节点的权限。	list	endpoint *	-
dns:endpoint:get	授予查询单个终端节点的权限。	read	endpoint *	-
dns:endpoint:update	授予更新终端节点的权限。	write	endpoint *	-
dns:endpoint:delete	授予删除终端节点的权限。	write	endpoint *	-
dns:endpoint:createIpaddress	授予为终端节点绑定ip地址的权限。	write	endpoint *	-
dns:endpoint:deleteIpaddress	授予为终端节点解绑ip地址的权限。	write	endpoint *	-
dns:endpoint:listIpaddresses	授予列出终端节点ip地址的权限。	list	endpoint *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dns:endpoint:listVpcs	授予列出终端节点关联的VPC的权限。	list	endpoint *	-
dns:resolverRule:create	授予创建解析规则的权限，定义如何将来自VPC的查询路由给目标VPC。	write	resolverRule *	-
dns:resolverRule:list	授予列出解析规则的权限。	list	resolverRule *	-
dns:resolverRule:get	授予查询单个解析规则的权限。	read	resolverRule *	-
dns:resolverRule:update	授予更新解析规则的权限。	write	resolverRule *	-
dns:resolverRule:delete	授予删除解析规则的权限。	write	resolverRule *	-
dns:resolverRule:associaterouter	授予在解析规则上关联VPC的权限。	write	resolverRule *	-
dns:resolverRule:disassociaterouter	授予在解析规则上解关联VPC的权限。	write	resolverRule *	-
dns:zone:enableDnssecConfig	授予在zone上打开dnssec的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:disableDnssecConfig	授予在zone上关闭dnssec的权限。	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:getDnssecConfig	授予在zone上查询dnssec的权限。	read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:listPublicZoneBatchOperationRecords	授予列出公网域名批量操作记录的权限。	list	-	-
dns:zone:getPublicZoneBatchOperationResult	授予下载公网域名批量操作失败结果的权限。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
dns:recordset:batchImportPublicRecordSet	授予批量导入公网RecordSet的权限。	write	-	-
dns:zone:createAuthorizeTxtRecord	授予授权域名的权限。	write	-	-
dns:zone:getAuthorizeTxtRecord	授予查询域名授权状态的权限。	read	-	-
dns:zone:getDomainDetection	授予查询公网域名解析诊断结果的权限。	read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

DNS的API通常对应着一个或多个授权项。表5-201展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-201 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v2/zones	dns:zone:list	-
POST /v2/zones	dns:zone:create	• dns:tag:set • dns:quota:list
GET /v2/zones/{zone_id}	dns:zone:get	-
PATCH /v2/zones/{zone_id}	dns:zone:update	-
DELETE /v2/zones/{zone_id}	dns:zone:delete	-
GET /v2/zones/{zone_id}/nameservers	dns:zone:get	-
GET /v2/zones	dns:zone:list	-
POST /v2/zones	dns:zone:create	• vpc:vpcs:get • dns:tag:set • dns:quota:list
GET /v2/zones/{zone_id}	dns:zone:get	-

API	对应的授权项	依赖的授权项
PATCH /v2/zones/{zone_id}	dns:zone:update	-
DELETE /v2/zones/{zone_id}	dns:zone:delete	-
GET /v2/zones/{zone_id}/nameservers	dns:zone:get	-
POST /v2/zones/{zone_id}/associaterouter	dns:zone:associaterouter	vpc:vpcs:get
POST /v2/zones/{zone_id}/disassociaterouter	dns:zone:disassociaterouter	vpc:vpcs:get
GET /v2/zones/{zone_id}/recordsets	dns:recordset:list	-
POST /v2/zones/{zone_id}/recordsets	dns:recordset:create	dns:quota:list
GET /v2/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:get	-
PUT /v2/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:update	-
DELETE /v2/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:delete	-
GET /v2/recordsets	dns:recordset:list	-
PUT /v2/zones/{zone_id}/statuses	dns:zone:setStatus	-
GET /v2.1/recordsets	dns:recordset:list	-
POST /v2.1/zones/{zone_id}/recordsets	dns:recordset:create	dns:quota:list
GET /v2.1/zones/{zone_id}/recordsets	dns:recordset:list	-

API	对应的授权项	依赖的授权项
GET /v2.1/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:get	-
PUT /v2.1/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:update	-
DELETE /v2.1/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:delete	-
PUT /v2.1/recordsets/{recordset_id}/statuses/set	dns:recordset:setStatus	-
POST /v2.1/zones/{zone_id}/recordsets/batch/lines	dns:recordset:create	dns:quota:list
PUT /v2.1/zones/{zone_id}/recordsets	dns:recordset:update	-
DELETE /v2.1/zones/{zone_id}/recordsets	dns:recordset:delete	-
GET /v2/reverse/floatingips	dns:ptr:list	-
GET /v2/reverse/floatingips/{region}:{floatingip_id}	dns:ptr:get	-
PATCH /v2/reverse/floatingips/{region}:{floatingip_id}	dns:ptr:create	• eip:publicIps:get • dns:tag:set • dns:quota:list
PATCH /v2/reverse/floatingips/{region}:{floatingip_id}	dns:ptr:update	-
PATCH /v2/reverse/floatingips/{region}:{floatingip_id}	dns:ptr:delete	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/{resource_type}/tags	dns:tag:get	-
GET /v2/{project_id}/{resource_type}/{resource_id}/tags	dns:tag:get	-
POST /v2/{project_id}/{resource_type}/{resource_id}/tags	dns:tag:set	-
DELETE /v2/{project_id}/{resource_type}/{resource_id}/tags/{key}	dns:tag:set	-
POST /v2/{project_id}/{resource_type}/{resource_id}/tags/action	dns:tag:set	-
POST /v2/{project_id}/{resource_type}/resource_instances/action	dns:tag:get	-
POST /v2.1/customlines	dns:customLine:create	dns:quota:list
GET /v2.1/customlines	dns:customLine:list	-
DELETE /v2.1/customlines/{line_id}	dns:customLine:delete	-
PUT /v2.1/customlines/{line_id}	dns:customLine:update	-
GET /v2/nameservers	dns:nameserver:list	-
GET /v2/quotamg/dns/quotas	dns:quota:list	-

API	对应的授权项	依赖的授权项
POST /v2.1/linegroups	dns:lineGroup:create	dns:quota:list
GET /v2.1/linegroups	dns:lineGroup:list	-
GET /v2.1/linegroups/{linegroup_id}	dns:lineGroup:get	-
PUT /v2.1/linegroups/{linegroup_id}	dns:lineGroup:update	-
DELETE /v2.1/linegroups/{linegroup_id}	dns:lineGroup:delete	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-202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。

DNS定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-202 DNS 支持的资源类型

资源类型	URN
resolverRule	dns:<region>:<account-id>:resolverRule:<resolver-rule-id>
lineGroup	dns::<account-id>:lineGroup:<line-group-id>
customLine	dns::<account-id>:customLine:<custom-line-id>
zone	dns::<account-id>:zone:<zone-id>
endpoint	dns:<region>:<account-id>:endpoint:<endpoint-id>
ptr	dns:<region>:<account-id>:ptr:<ptr-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dns:）仅适用于对应服务的操作，详情请参见表5-203。
  - 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。

DNS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 5-203 DNS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
dns:RecordSetNames	string	多值	根据指定的记录集名称过滤访问。记录集名称所有字母必须为小写形式，不得带有结尾圆点。
dns:RecordSetTypes	string	多值	根据指定的记录集类型过滤访问。取值范围：A、AAAA、MX、CNAME、TXT、NS、SRV、CAA。

5.10.12.2 云桌面 Workspace

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。

  关于云桌面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。

  关于云桌面Workspace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元素中指定以下云桌面Workspace的相关操作。

表 5-204 workspace 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
workspace:authConfigs:get	授予查询认证登录方式配置信息的权限。	read	-	-
workspace:authConfigs:update	授予更新认证策略配置信息的权限。	write	-	-
workspace:assistAuthConfigs:get	授予查询辅助认证的配置信息的权限。	read	-	-
workspace:assistAuthConfigs:update	授予更新辅助认证配置的权限。	write	-	-
workspace:jobs:retry	授予重试任务的权限。	write	-	-
workspace:quotas:get	授予查询租户配额的权限。	read	-	-
workspace:tenants:getRoles	授予查询租户角色的权限。	read	-	-
workspace:tenants:ListConfig	授予查询租户个性配置列表的权限。	list	-	-
workspace:tenants:updateConfig	授予修改租户个性配置的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:natMappings:getConfig	授予查询租户的NAT映射配置项的权限。	read	-	-
workspace:natMappings:updateConfig	授予修改租户的NAT映射配置项的权限。	write	-	-
workspace:tenants:get	授予查询云办公服务详情的权限。	read	-	-
workspace:tenants:open	授予开通云办公服务的权限。	write	-	workspace:AccessMode
workspace:tenants:delete	授予注销云办公服务的权限。	write	-	-
workspace:tenants:update	授予修改云办公服务属性的权限。	write	-	workspace:AccessMode
workspace:tenants:getLockStatus	授予查询云办公服务是否被锁定的权限。	read	-	-
workspace:tenants:unlock	授予解除云办公服务锁定状态的权限。	write	-	-
workspace:agencies:create	授予创建委托的权限。	write	-	-
workspace:agencies:get	授予查询委托的权限。	read	-	-
workspace:desktops:createAiAccelerateJob	授予创建渲染加速任务的权限。	write	-	-
workspace:desktops:getAiAccelerateJob	授予查询渲染加速任务的权限。	read	-	-
workspace:desktops:getSysPrepInfo	授予查询sysprep详情的权限。	read	desktop *	• 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
workspace:desktops:checkBatchChangeImage	授予校验批量切换镜像的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:tenants:listDesktopNamePolicies	授予查询桌面名称策略列表的权限。	list	-	-
workspace:tenants:createDesktopNamePolicy	授予创建桌面名称策略的权限。	write	-	-
workspace:tenants:updateDesktopNamePolicy	授予更新桌面名称策略的权限。	write	-	-
workspace:tenants:batchDeleteDesktopNamePolicies	授予批量删除桌面名称策略的权限。	write	-	-
workspace:desktopPools:create	授予创建桌面池的权限。	write	desktopPool *	-
			user	-
			userGroup	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktopPools:list	授予查询桌面池列表的权限。	list	desktopPool *	-
workspace:desktopPools:update	授予修改桌面池属性的权限。	write	desktopPool *	-
workspace:desktopPools:delete	授予删除桌面池的权限。	write	desktopPool *	-
workspace:desktopPools:get	授予查询桌面池详情的权限。	read	desktopPool *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:desktopPools:expand	授予扩容桌面池的权限。	write	desktopPool *	-
workspace:desktopPools:resize	授予桌面池变更规格的权限。	write	desktopPool *	-
workspace:desktopPools:rebuild	授予桌面池重建系统盘的权限。	write	desktopPool *	-
workspace:desktopPools:batchAddVolumes	授予桌面池批量添加磁盘的权限。	write	desktopPool *	-
workspace:desktopPools:batchDeleteVolumes	授予桌面池批量删除磁盘的权限。	write	desktopPool *	-
workspace:desktopPools:batchExpandVolumes	授予桌面池批量扩容磁盘的权限。	write	desktopPool *	-
workspace:desktopPools:operate	授予操作桌面池的权限。	write	desktopPool *	-
workspace:desktopPools:listUsers	授予查询桌面池授权的用户、用户组的权限。	list	desktopPool *	-
workspace:desktopPools:authorizeUsers	授予桌面池授权用户、用户组的权限。	write	desktopPool *	-
			user	-
			userGroup	-
workspace:desktopPools:listDesktops	授予查询桌面池桌面信息的权限。	list	desktopPool *	-
workspace:desktopPools:listScriptTasks	授予查询桌面池的脚本执行任务列表的权限。	list	desktopPool *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:desktopPools:executeScripts	授予桌面池批量执行脚本的权限。	write	desktopPool *	-
			script	-
workspace:desktopPools:sendNotifications	授予发送消息通知的权限。	write	desktopPool *	-
workspace:desktops:export	授予导出桌面列表的权限。	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:create	授予创建桌面的权限。	write	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • workspace:AssociatePublicIp • workspace:AccessMode
workspace:desktops:list	授予查询桌面列表的权限。	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:update	授予更新桌面信息的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:delete	授予删除桌面的权限。	write	desktop *	• 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
workspace:desktops:get	授予查询桌面详情的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDelete	授予批量删除桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:logoff	授予批量注销桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDetail	授予查询桌面详情列表的权限。	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:operate	授予操作桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:resize	授予变更规格的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getConnectStatus	授予查询桌面登录状态统计数据的权限。	read	-	-
workspace:desktops:ListStatus	授予查询桌面登录状态的权限。	list	-	-
workspace:desktops:rebuild	授予重建桌面的权限。	write	desktop *	• 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
workspace:desktops:getActions	授予查询桌面开关机信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createConsole	授予获取远程登录控制台地址的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:updateSids	授予更新桌面SID的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:rejoinDomain	授予重新加入AD域的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createImage	授予桌面转镜像的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDetach	授予批量解绑用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:detach	授予解绑用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:attach	授予分配用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getNetwork	授予查询桌面网络信息的权限。	read	desktop *	• 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
workspace:desktops:changeNetwork	授予切换桌面网络的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:exclusiveHosts:listDesktops	授予查询专享桌面详情列表的权限。	list	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:desktops:listAll	授予查询普通桌面和渲染桌面列表的权限。	list	desktop *	-
workspace:desktopAssociate:listDiscoverVmInfo	授予查询可纳管的虚拟机列表的权限。	list	-	-
workspace:desktopAssociate:startTask	授予启动纳管虚拟机任务的权限。	write	-	-
workspace:desktopAssociate:switchScanTask	授予开启纳管扫描任务的权限。	write	-	-
workspace:desktopAssociate:getScanTaskSwitch	授予查询纳管扫描任务开关的权限。	read	-	-
workspace:desktops:setMaintenanceMode	授予批量设置桌面管理员维护模式的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:prepAttachUsers	授予预批量分配用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchAttachUsers	授予批量分配用户的权限。	write	desktop *	• 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
workspace:desktops:changeUsername	授予在Windows AD场景下，修改与桌面关联的用户名的权限。	write	-	-
workspace:desktops:sendNotifications	授予发送消息通知的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:migrate	授予迁移桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listAgents	授予查询桌面安装agent列表的权限。	list	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchInstallAgents	授予批量为桌面安装agent的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listTags	授予查询桌面标签的权限。	list	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:tag	授予创建桌面标签的权限。	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:untag	授予删除桌面标签的权限。	tagging	desktop *	• 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
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:listProjectTags	授予查询项目标签的权限。	list	-	-
workspace:desktops:operateTags	授予批量添加删除标签的权限。	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:listByTags	授予使用标签过滤桌面的权限。	list	-	-
workspace:exclusiveHosts:create	授予创建专享主机的权限。	write	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:exclusiveHosts:list	授予查询专享主机列表的权限。	list	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:exclusiveHosts:check	授予校验是否能创建专享主机的权限。	write	-	-
workspace:exclusiveHosts:get	授予查询专享主机详情的权限。	read	exclusiveHost *	g:EnterpriseProjectId
workspace:exclusiveHosts:update	授予更新专享主机信息的权限。	write	exclusiveHost *	g:EnterpriseProjectId
workspace:exclusiveHosts:delete	授予删除专享主机的权限。	write	exclusiveHost *	g:EnterpriseProjectId
workspace:mkp:listImages	授予查询云市场镜像列表的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:mkp:listCommodityInfos	授予查询云市场商品信息的权限。	list	-	-
workspace:mkp:createOrder	授予创建云市场产品订单的权限。	write	-	-
workspace:mkp:listListProductReserve	授予查询云市场库存信息的权限。	list	-	-
workspace:mkp:listCommodityDetails	授予查询云市场商品详情的权限。	list	-	-
workspace:mkp:listRelationCommodityDetails	授予查询商品的关联商品的权限。	list	-	-
workspace:mkp:listCommodityAgreements	授予查询云市场商品协议的权限。	list	-	-
workspace:networks:listEips	授予查询EIP列表的权限。	list	-	-
workspace:networks:createEips	授予创建EIP的权限。	write	-	-
workspace:networks:bindEips	授予绑定EIP的权限。	write	-	-
workspace:networks:unbindEips	授予解绑EIP的权限。	write	-	-
workspace:networks:getEipQuota	授予查询EIP配额的权限。	read	-	-
workspace:networks:ListNatGateways	授予查询Nat网关列表的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:orders:create	授予包周期下单的权限。	write	-	• workspace:CreateOrderType • workspace:AssociatePublicIp • workspace:AccessMode
workspace:orders:change	授予创建变更订单的权限。	write	-	workspace:ChangeOrderType
workspace:orders:batchInquiry	授予批量询价的权限。	write	-	-
workspace:quotas:check	授予校验配额的权限。	write	-	-
workspace:renderDesktops:create	授予创建渲染桌面的权限。	write	-	-
workspace:renderDesktops:delete	授予删除渲染桌面的权限。	write	-	-
workspace:renderDesktops:list	授予查询渲染桌面列表的权限。	list	-	-
workspace:renderDesktops:action	授予操作渲染桌面的权限。	write	-	-
workspace:scheduledTasks:list	授予查询定时任务列表的权限。	list	scheduledTask *	-
workspace:scheduledTasks:create	授予创建定时任务的权限。	write	scheduledTask *	-
			desktop	-
			desktopPool	-
			server	-
			serverGroup	-
workspace:scheduledTasks:get	授予查询定时任务详情的权限。	read	scheduledTask *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:scheduledTasks:update	授予更新定时任务的权限。	write	scheduledTask *	-
			desktop	-
			desktopPool	-
			server	-
			serverGroup	-
workspace:scheduledTasks:delete	授予删除定时任务的权限。	write	scheduledTask *	-
workspace:scheduledTasks:getFuture	授予查询定时任务未来执行时间的权限。	read	-	-
workspace:scheduledTasks:batchDelete	授予批量删除定时任务的权限。	write	scheduledTask *	-
workspace:scheduledTasks:listRecords	授予查询定时任务执行记录的权限。	list	scheduledTask *	-
workspace:scheduledTasks:getRecord	授予查询定时任务执行记录详情的权限。	read	scheduledTask *	-
workspace:scheduledTasks:exportRecords	授予导出定时任务记录及执行详情的权限。	list	scheduledTask *	-
workspace:users:subscribeSharer	授予订阅协同资源的权限。	write	user *	-
workspace:desktops:addSubResources	授予购买桌面附属资源的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:deleteSubResources	授予删除桌面附属资源的权限。	write	desktop *	• 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
workspace:desktops:createSnapshots	授予创建桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getSnapshots	授予查询桌面快照的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:deleteSnapshots	授予删除桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:restoreBySnapshot	授予使用桌面快照恢复桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:statistics:listDesktopStatus	授予统计桌面状态的权限。	list	-	-
workspace:statistics:getUnused	授予查询在指定时间段未使用的桌面的权限。	read	-	-
workspace:statistics:getUsed	授予查询使用桌面的时长的权限。	read	-	-
workspace:bindingPolicies:export	授予导出终端与桌面绑定配置excel的权限。	list	-	-
workspace:bindingPolicies:getConfig	授予查询终端与桌面绑定的开关配置信息的权限。	read	-	-
workspace:bindingPolicies:createConfig	授予设置终端与桌面绑定的开关配置的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:bindingPolicies:get	授予查询终端与桌面绑定配置列表的权限。	read	-	-
workspace:bindingPolicies:add	授予增加终端与桌面绑定配置的权限。	write	-	-
workspace:bindingPolicies:update	授予修改终端与桌面绑定配置的权限。	write	-	-
workspace:bindingPolicies:delete	授予删除终端与桌面绑定配置的权限。	write	-	-
workspace:volumes:delete	授予删除桌面数据盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:batchAdd	授予增加桌面磁盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:batchExpand	授予扩容桌面磁盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:wdh:getType	授予查询云办公主机类型的权限。	read	wdh *	g:EnterpriseProjectId
workspace:wdh:get	授予查询云办公主机列表的权限。	read	wdh *	g:EnterpriseProjectId
workspace:desktops:getRemoteAssistance	授予查询远程协助信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createRemoteAssistance	授予创建远程协助的权限。	write	desktop *	• 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
workspace:desktops:cancelRemoteAssistance	授予取消远程协助的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:add	授予单个桌面增加磁盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:expand	授予扩容磁盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:listDssPoolsDetail	授予获取专属分布式存储池详情列表的权限。	list	-	-
workspace:common:listTimezones	授予查询时区配置的权限。	list	-	-
workspace:connections:securityExport	授予导出连接记录的权限。	list	-	-
workspace:images:list	授予查询支持的镜像列表的权限。	list	-	-
workspace:policyGroups:import	授予导入策略组的权限。	write	-	-
workspace:accessPolicies:create	授予创建接入策略的权限。	write	-	-
workspace:accessPolicies:get	授予查询接入策略的权限。	read	-	-
workspace:accessPolicies:delete	授予删除指定接入策略的权限。	write	-	-
workspace:accessPolicies:getTarget	授予查询指定接入策略的应用对象的权限。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:accessPolicies:updateTarget	授予更新指定接入策略的应用对象的权限。	write	-	-
workspace:products:listDesktopProducts	授予查询支持的产品套餐列表的权限。	list	-	-
workspace:products:listSharerProducts	授予查询协同套餐列表的权限。	list	-	-
workspace:products:listInternetProducts	授予查询上网套餐列表的权限。	list	-	-
workspace:availabilityZones:list	授予查询支持的可用分区列表的权限。	list	-	-
workspace:userGroups:export	授予导出用户组的权限。	list	userGroup *	-
workspace:users:export	授予导出用户的权限。	list	user *	-
workspace:users:import	授予导入用户的权限。	write	user *	-
workspace:userGroups:exportUsers	授予导出用户组用户的权限。	list	userGroup *	-
workspace:users:operate	授予操作用户（锁定、解锁和重置密码）的权限。	write	user *	-
workspace:users:randomPassword	授予给用户重置随机密码的权限。	write	user *	-
workspace:users:deleteOtps	授予解绑OTP设备的权限。	write	user *	-
workspace:users:resendEmail	授予重新发送邮件的权限。	write	user *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:connections:securityList	授予查询连接信息的权限。	list	-	-
workspace:connections:listOnlineUsers	授予查询登录人数的权限。	list	-	-
workspace:userGroups:list	授予查询用户组列表的权限。	list	userGroup *	-
workspace:userGroups:create	授予创建用户组的权限。	write	userGroup *	-
workspace:userGroups:batchDelete	授予批量删除用户组的权限。	write	userGroup *	-
workspace:userGroups:delete	授予删除桌面用户组的权限。	write	userGroup *	-
workspace:userGroups:update	授予修改用户组信息的权限。	write	userGroup *	-
workspace:userGroups:operate	授予操作用户组的权限。	write	userGroup *	-
			user *	-
workspace:userGroups:getUsers	授予查询用户组中的用户的权限。	list	userGroup *	-
workspace:jobs:listSubJobs	授予查询子任务列表的权限。	list	-	-
workspace:jobs:deleteSubJobRecords	授予删除子任务记录的权限。	write	-	-
workspace:ou:get	授予查询OU信息的权限。	list	-	-
workspace:ou:create	授予新增OU信息的权限。	write	-	-
workspace:ou:delete	授予删除OU信息的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:ou:update	授予更新OU信息的权限。	write	-	-
workspace:policyGroups:list	授予查询策略组列表的权限。	list	policyGroup *	-
workspace:policyGroups:create	授予新增策略组的权限。	write	policyGroup *	-
			desktop	-
			desktopPool	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:delete	授予删除策略组的权限。	write	policyGroup *	-
workspace:policyGroups:get	授予查询策略组的权限。	read	policyGroup *	-
workspace:policyGroups:update	授予修改策略组的权限。	write	policyGroup *	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:export	授予导出策略组的权限。	list	policyGroup *	-
workspace:policyGroups:listPolicies	授予查询策略组中的策略项的权限。	list	policyGroup *	-
workspace:policyGroups:updatePolicies	授予修改策略组中的策略项的权限。	write	policyGroup *	-
workspace:policyGroups:listTargets	授予查询策略组应用对象的权限。	list	policyGroup *	-
workspace:policyGroups:updateTargets	授予修改策略组应用对象的权限。	write	policyGroup *	-
			desktop	-
			desktopPool	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:listDetail	授予查询策略组详情列表的权限。	list	policyGroup *	-
workspace:policyGroups:getOriginalPolicies	授予查询初始策略项的权限。	read	policyGroup *	-
workspace:users:list	授予查询用户列表的权限。	list	user *	-
workspace:users:create	授予创建用户的权限。	write	user *	-
workspace:users:delete	授予删除指定用户的权限。	write	user *	-
workspace:users:get	授予查询用户详情信息的权限。	read	user *	-
workspace:users:update	授予修改用户信息的权限。	write	user *	-
workspace:users:batchDelete	授予批量删除用户的权限。	write	user *	-
workspace:users:resetPassword	授予重置用户密码的权限。	write	user *	-
workspace:users:checkResetPasswordToken	授予校验重置域用户密码Token的权限。	write	user *	-
workspace:users:getTemplate	授予用户模板下载的权限。	read	-	-
workspace:users:checkExist	授予校验用户是否存在的权限。	write	user *	-
workspace:users:listOtps	授予查询OTP设备的权限。	list	user *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:users:getImportTemplate	授予创建用户模板下载的权限。	read	-	-
workspace:users:batchCreate	授予批量创建用户的权限。	write	user *	-
workspace:products:listVolumeProducts	授予查询磁盘产品列表的权限。	list	-	-
workspace:tenants:listExportTasks	授予查询导出任务列表的权限。	list	-	-
workspace:tenants:deleteExportTasks	授予批量删除导出任务记录的权限。	write	-	-
workspace:tenants:exportData	授予下载导出的文件的权限。	read	-	-
workspace:statistics:listAlarm	授予查询告警列表的权限。	list	-	-
workspace:statistics:getAlarm	授予查询告警数的权限。	read	-	-
workspace:statistics:getGrowthRate	授予查询指标环比值的权限。	read	-	-
workspace:statistics:getMetric	授予查询指标的权限。	read	-	-
workspace:statistics:getMetricTrend	授予查询指标趋势的权限。	read	-	-
workspace:statistics:updateNotificationRules	授予更新指标的通知规则的权限。	write	-	-
workspace:statistics:deleteNotificationRules	授予删除指标的通知规则的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:statistics:createNotifyRules	授予新增指标的通知规则的权限。	write	-	-
workspace:statistics:listNotificationRules	授予查询指标的通知规则的权限。	list	-	-
workspace:statistics:listNotificationRecords	授予查询指标通知记录的权限。	list	-	-
workspace:statistics:listDesktopMetrics	授予查询桌面使用统计信息的权限。	list	-	-
workspace:statistics:exportDesktopMetrics	授予导出桌面使用统计信息的权限。	list	-	-
workspace:statistics:listUserMetrics	授予查询用户使用统计信息的权限。	list	-	-
workspace:statistics:exportUserMetrics	授予导出用户使用统计信息;的权限。	list	-	-
workspace:appcenter:createBucketCredential	授予生成OBS桶凭证信息信息的权限。	write	-	-
workspace:appcenter:createAndAuthorizeBucket	授予添加并授权默认OBS桶的权限。	write	-	-
workspace:appcenter:listApps	授予按照名称分页查询应用的权限。	list	-	-
workspace:appcenter:createApp	授予上传应用的权限。	write	-	-
workspace:appcenter:updateApp	授予修改应用的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:appcenter:deleteApp	授予删除应用的权限。	write	-	-
workspace:appcenter:installApp	授予自动安装应用的权限。	write	-	-
workspace:appcenter:listAppAuthorizations	授予查询应用授权信息的权限。	list	-	-
workspace:appcenter:batchUpdateAppAuthorizations	授予设置应用授权的权限。	write	-	-
workspace:appcenter:batchDeleteApps	授予批量删除应用的权限。	write	-	-
workspace:appcenter:batchDisableApps	授予批量设置应用不可见的权限。	write	-	-
workspace:appcenter:batchEnableApps	授予批量设置应用可见的权限。	write	-	-
workspace:appcenter:batchInstallApps	授予批量自动安装安装应用的权限。	write	-	-
workspace:appcenter:listAppCatalogs	授予查询应用分类信息的权限。	list	-	-
workspace:appcenter:listJobs	授予查询应用安装job信息的权限。	list	-	-
workspace:appcenter:batchDeleteJobs	授予批量删除job的权限。	write	-	-
workspace:appcenter:retryJobs	授予重试失败job的权限。	write	-	-
workspace:appcenter:createAppRule	授予创建应用规则的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:appcenter:listAppRule	授予查询应用规则的权限。	list	-	-
workspace:appcenter:updateAppRule	授予修改应用规则的权限。	write	-	-
workspace:appcenter:deleteAppRule	授予删除应用规则的权限。	write	-	-
workspace:appcenter:batchDeleteAppRules	授予批量删除应用规则的权限。	write	-	-
workspace:appcenter:enableRuleRestriction	授予启用规则管控的权限。	write	-	-
workspace:appcenter:disableRuleRestriction	授予禁用规则管控的权限。	write	-	-
workspace:appcenter:addRestrictedRule	授予增加管控规则的权限。	write	-	-
workspace:appcenter:listRestrictedRule	授予查询管控规则列表的权限。	list	-	-
workspace:appcenter:deleteRestrictedRule	授予批量删除管控规则列表的权限。	write	-	-
workspace:appcenter:updateTenantProfile	授予启禁用租户功能的权限。	write	-	-
workspace:appcenter:listTenantProfiles	授予查询租户功能状态的权限。	list	-	-
workspace:scripts:create	授予创建脚本的权限。	write	script *	-
workspace:scripts:list	授予查询脚本列表的权限。	list	script *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:scripts:get	授予查询脚本详情的权限。	read	script *	-
workspace:scripts:put	授予更新脚本的权限。	write	script *	-
workspace:scripts:delete	授予删除脚本的权限。	write	script *	-
workspace:scripts:execute	授予批量执行脚本或命令的权限。	write	script *	-
			desktop *	-
workspace:scripts:getRecordDetail	授予查询脚本或命令执行记录详情的权限。	read	script *	-
workspace:scripts:listRecords	授予查询脚本执行记录列表的权限。	list	script *	-
workspace:scripts:listTasks	授予查询脚本任务列表的权限。	list	script *	-
workspace:scripts:retry	授予重试脚本的权限。	write	script *	-
workspace:scripts:stop	授予停止脚本或命令执行任务的权限。	write	script *	-
workspace:scripts:download	授予下载脚本输出记录的权限。	write	script *	-
workspace:tenants:getShareSpaceConfig	授予查询协同配置的权限。	read	-	-
workspace:tenants:updateShareSpaceConfig	授予修改协同配置的权限。	write	-	-
workspace:authConfigs:getStatus	授予查询认证状态的权限。	read	-	-
workspace:privacystatements:sign	授予签署隐私声明的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:sites:get	授予查询站点信息的权限。	read	-	-
workspace:sites:add	授予新增站点的权限。	write	-	workspace:AccessMode
workspace:sites:delete	授予删除站点的权限。	write	-	-
workspace:sites:updateAccessMode	授予修改站点接入方式的权限。	write	-	workspace:AccessMode
workspace:sites:updateSubnets	授予修改站点业务子网的权限。	write	-	-
workspace:tenants:checkEnterpriseIds	授予检查企业ID是否已被使用的权限。	write	-	-
workspace:tenants:updateEnterpriseId	授予修改企业ID的权限。	write	-	-
workspace:bandwidth:create	授予开通云办公带宽的权限。	write	-	-
workspace:bandwidth:list	授予查询云办公带宽列表的权限。	list	-	-
workspace:bandwidth:update	授予修改云办公带宽的权限。	write	-	-
workspace:bandwidth:delete	授予取消云办公带宽的权限。	write	-	-
workspace:bandwidth:getControlConfig	授予查询云办公带宽的控制配置的权限。	read	-	-
workspace:bandwidth:updateControlConfig	授予修改云办公带宽的控制配置的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:bandwidth:createChangeOrder	授予创建云办公带宽变更订单的权限。	write	-	-
workspace:desktops:batchCreateSnapshots	授予批量创建桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDeleteSnapshots	授予批量删除桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchRestoreSnapshots	授予批量恢复桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listSnapshots	授予查询桌面快照列表的权限。	list	-	-
workspace:desktops:verifyDesktopName	授予校验桌面名称的权限。	write	-	-
workspace:networks:getAvailableIp	授予根据子网id查询该子网下可用的ip的权限。	read	-	-
workspace:desktops:getAdStatus	授予查询AD网络状态的权限。	read	-	-
workspace:networks:checkIpIfExist	授予检查IP是否存在的权限。	write	-	-
workspace:images:checkIfExist	授予检查镜像是否存在的权限。	write	-	-
workspace:wdh:listDesktops	授予查询云办公主机包含桌面信息的权限。	list	wdh *	-
			-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:wdh:update	授予更新云办公主机信息的权限。	write	wdh *	g:EnterpriseProjectId
workspace:bindingPolicies:getTemplate	授予下载终端与桌面绑定模板的权限。	read	-	-
workspace:bindingPolicies:import	授予批量导入终端与桌面绑定的权限。	write	-	-
workspace:statistics:getRunState	授予运行状态统计的权限。	read	-	-
workspace:statistics:getLoginState	授予登录状态统计的权限。	read	-	-
workspace:networks:getUsingSubnets	授予查询正在被使用的子网列表的权限。	read	-	-
workspace:networks:listPorts	授予查询端口列表的权限。	list	-	-
workspace:renderDesktops:createConsole	授予获取远程登录控制台地址的权限。	write	-	-
workspace:renderDesktops:resize	授予变更渲染桌面规格的权限。	write	-	-
workspace:exclusiveHosts:resizeLites	授予变更专享主机规格的权限。	write	exclusiveHost *	g:EnterpriseProjectId
workspace:desktops:getMonitor	授予查询桌面监控信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDetachInfo	授予查询桌面历史解绑用户信息的权限。	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:desktops:getSysprepVersion	授予查询sysprep版本信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:networks:createNat	授予开通NAT网关上网功能的权限。	write	-	-
workspace:networks:listNats	授予查询NAT网关上网功能的权限。	list	-	-
workspace:networks:listSubnets	授予查询子网列表的权限。	list	-	-
workspace:networks:listVpcs	授予查询查询vpc的权限。	list	-	-
workspace:policyGroups:createTemplate	授予创建策略模板的权限。	write	-	-
workspace:policyGroups:listTemplate	授予查询策略模板列表的权限。	list	-	-
workspace:policyGroups:updateTemplate	授予更新策略模板的权限。	write	-	-
workspace:networks:listSecurityGroups	授予查询安全组列表的权限。	list	-	-
workspace:availabilityZones:getSummary	授予查询可用分区列表概要的权限。	read	-	-
workspace:availabilityZones:get	授予查询可用分区详情的权限。	read	-	-
workspace:users:importUser	授予导入用户列表的权限。	write	user *	-
workspace:users:uploadTemplate	授予导入桌面用户列表的权限。	write	user *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:accessPolicies:update	授予更新指定接入策略的权限。	write	-	-
workspace:desktops:verifySource	授予校验桌面来源的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDesktopNetworks	授予批量查询桌面网络信息的权限。	list	desktop *	-
workspace:desktops:batchChangeNetwork	授予批量切换桌面网络的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:jobs:get	授予查询任务详情的权限。	read	-	-
workspace:accessPolicies:importIp	授予导入IP列表的权限。	write	-	-
workspace:accessPolicies:getIpImportTemplate	授予下载IP导入模板的权限。	read	-	-
workspace:sites:listEdgeSites	授予查询边缘站点的权限。	list	-	-
workspace:sites:checkEdgeSiteResources	授予校验边缘站点资源的权限。	write	-	-
workspace:ou:listAdOus	授予查询AD域下OU信息的权限。	list	-	-
workspace:ou:listOuUsers	授予查询OU下用户信息的权限。	list	-	-
workspace:ou:importUsersByOU	授予导入OU用户的权限。	write	-	-
workspace:appGroup:list	授予查询应用组的权限。	list	appGroup *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:appGroup:create	授予创建应用组的权限。	write	appGroup *	-
			serverGroup	-
workspace:appGroup:delete	授予应用组删除的权限。	write	appGroup *	-
workspace:appGroup:get	授予查询应用组详情的权限。	read	appGroup *	-
workspace:appGroup:update	授予修改应用组的权限。	write	appGroup *	-
			serverGroup	-
workspace:app:listPublishedApp	授予查询已发布应用的权限。	list	app *	-
			appGroup *	-
workspace:app:publish	授予发布应用的权限。	write	app *	-
			appGroup *	-
workspace:app:get	授予查询应用详细信息的权限。	read	app *	-
			appGroup *	-
workspace:app:update	授予修改应用信息的权限。	write	app *	-
			appGroup *	-
workspace:app:deleteIcon	授予删除自定义应用图标的权限。	write	app *	-
			appGroup *	-
workspace:app:uploadIcon	授予修改自定义应用图标的权限。	write	app *	-
			appGroup *	-
workspace:app:check	授予校验应用的权限。	write	app *	-
			appGroup *	-
workspace:app:batchDisable	授予批量禁用应用的权限。	write	app *	-
			appGroup *	-
workspace:app:batchEnable	授予批量启用应用的权限。	write	app *	-
			appGroup *	-
workspace:app:unpublish	授予批量取消应用发布的权限。	write	app *	-
			appGroup *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:appGroup:listPublishableApp	授予可发布应用列表的权限。	list	appGroup *	-
workspace:appGroup:batchDeleteAuthorization	授予移除应用组授权的权限。	write	appGroup *	-
			user	-
			userGroup	-
workspace:appGroup:disassociate	授予解除服务组关联的所有应用组的权限。	write	-	-
workspace:appGroup:listAuthorization	授予查询应用组授权记录的权限。	list	appGroup *	-
workspace:appGroup:addAuthorization	授予增加应用组授权的权限。	write	appGroup *	-
			user	-
			userGroup	-
workspace:appGroup:batchDelete	授予批量删除应用组的权限。	write	appGroup *	-
workspace:appGroup:check	授予校验应用组的权限。	write	-	-
workspace:serverGroup:list	授予查询服务器组列表的权限。	list	serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:serverGroup:create	授予创建服务器组的权限。	write	serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:serverGroup:delete	授予删除服务器组的权限。	write	serverGroup *	• 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
workspace:serverGroup:get	授予查询指定服务器组的权限。	read	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:update	授予修改服务器组的权限。	write	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:getServerState	授予查询指定服务器组内服务器状态的权限。	read	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:listDetail	授予查询租户服务器组基础信息列表的权限。	list	serverGroup *	-
workspace:serverGroup:getRestrict	授予指定租户服务器组限制查询的权限。	read	serverGroup *	-
workspace:serverGroup:validate	授予校验服务器组的权限。	write	serverGroup *	-
workspace:serverGroup:tagResource	授予服务器组添加标签的权限。	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:unTagResource	授予服务器组删除标签的权限。	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• 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
workspace:serverGroup:listTagsForResource	授予查询服务器组标签的权限。	list	serverGroup *	-
			-	g:EnterpriseProjectId
workspace:serverGroup:listTags	授予查询租户所有服务器上标签的权限。	list	serverGroup *	-
workspace:serverGroup:batchCreateTags	授予批量添加服务器组标签的权限。	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:batchDeleteTags	授予批量删除服务器组标签的权限。	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:server:list	授予查询服务器列表的权限。	list	server *	-
workspace:server:delete	授予删除服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:get	授予查询指定服务器的权限。	read	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:update	授予修改服务器的权限。	write	server *	• 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
workspace:server:changeImage	授予修改服务器的镜像的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:reinstall	授予重装服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:getVncUrl	授予获取VNC远程登录地址的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:accessAgent:list	授予查询租户的所有HDA最新版本的权限。	list	-	-
workspace:accessAgent:batchUpgrade	授予批量升级服务器HDA版本的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:accessAgent:listLatestVersion	授予查询租户的HDA最新版本的权限。	list	-	-
workspace:server:listAccessAgentDetails	授予查询服务器的HDA相关信息的权限。	list	server *	-
workspace:accessAgent:getUpgradeFlag	授予查询HDA升级提醒标识的权限。	read	-	-
workspace:accessAgent:updateUpgradeFlag	授予更新HDA升级通知标识的权限。	write	-	-
workspace:accessAgent:listUpgradeRecords	授予查询服务器的HDA升级跟踪记录的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:server:batchDelete	授予批量删除服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchChangeMaintainMode	授予标记服务器维护状态的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchReboot	授予重启服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchRejoinDomain	授予批量服务器重新加域的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchStart	授予启动服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchStop	授予关闭服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchUpdateTsvi	授予批量更新服务器虚拟会话IP配置的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:create	授予创建应用服务器的权限。	write	server *	-
			serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:server:batchMigrateHosts	授予迁移云办公主机下面的服务器到目标云办公主机的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			wdh *	-
workspace:server:getMetricData	授予查询云应用服务器监控信息的权限。	read	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:jobs:batchDeleteSubJobs	授予批量删除子任务的权限。	write	-	-
workspace:jobs:countSubJobs	授予子任务数量查询的权限。	list	-	-
workspace:appWarehouse:authorizeObs	授予获取上传至OBS桶的ak/sk的权限。	write	-	-
workspace:appWarehouse:batchDeleteApp	授予批量删除应用仓库中的指定应用的权限。	write	-	-
workspace:appWarehouse:ListWarehouseApps	授予查询租户应用仓库中的应用列表的权限。	list	-	-
workspace:appWarehouse:createApp	授予在应用仓库中新增应用的权限。	write	-	-
workspace:appWarehouse:deleteApp	授予删除应用仓库中的指定应用的权限。	write	-	-
workspace:appWarehouse:uploadAppIcon	授予在应用仓库中上传图标文件的权限。	write	-	-
workspace:appWarehouse:createBucketOrAcl	授予添加桶或者桶授权的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:images:listImageJobs	授予查询租户的任务列表的权限。	list	-	-
workspace:images:getImageJob	授予查询任务详情的权限。	read	-	-
workspace:imageServer:list	授予查询镜像实例列表的权限。	list	imageServer *	-
			-	g:EnterpriseProjectId
workspace:imageServer:create	授予创建镜像实例的权限。	write	imageServer *	-
			-	g:EnterpriseProjectId
workspace:imageServer:get	授予查询指定镜像实例的权限。	read	imageServer *	g:EnterpriseProjectId
workspace:imageServer:update	授予修改镜像实例的权限。	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:attachApp	授予分发软件信息至镜像实例的权限。	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:listLatestAttachedApp	授予查询最近一次分发软件信息列表的权限。	list	imageServer *	-
workspace:imageServer:recreate	授予构建云应用镜像的权限。	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:batchDelete	授予批量删除镜像实例的权限。	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:listImageSubJobs	授予子任务查询的权限。	list	-	-
workspace:imageServer:batchDeleteImageSubJobs	授予批量删除子任务的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:imageServer:countImageSubJobs	授予子任务数量查询的权限。	read	-	-
workspace:appGroup:listMailRecord	授予查询应用组授权邮件发送记录的权限。	list	-	-
workspace:appGroup:resendMail	授予重发应用组授权邮件（根据授权邮件记录）的权限。	write	-	-
workspace:storage:listPersistentStorage	授予查询WKS存储的权限。	list	storage *	-
workspace:storage:createPersistentStorage	授予创建WKS存储的权限。	write	storage *	-
workspace:storage:deletePersistentStorage	授予删除WKS存储的权限。	write	storage *	-
workspace:storage:updateUserFolderAssignment	授予创建个人存储目录的权限。	write	storage *	-
workspace:storage:updateShareFolderAssignment	授予修改共享目录成员的权限。	write	storage *	-
workspace:storage:createShareFolder	授予创建共享存储目录的权限。	write	storage *	-
workspace:storage:deleteStorageClaim	授予删除共享目录的权限。	write	storage *	-
workspace:storage:deleteUserStorageAttachment	授予删除个人存储目录的权限。	write	storage *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:storage:batchDeletePersistentStorage	授予批量删除WKS存储的权限。	write	storage *	-
workspace:storage:listStorageAssignment	授予查询个人存储目录的权限。	list	storage *	-
workspace:storage:listShareFolder	授予查询共享存储目录的权限。	list	storage *	-
workspace:policyGroups:deleteTemplate	授予删除策略模板的权限。	write	-	-
workspace:privacystatements:get	授予查询最新版本的隐私声明的权限。	read	-	-
workspace:scalingPolicy:delete	授予删除弹性伸缩策略的权限。	write	-	-
workspace:scalingPolicy:list	授予查询服务器组弹性伸缩策略的权限。	read	-	-
workspace:scalingPolicy:create	授予新增/修改弹性伸缩策略的权限。	write	-	-
workspace:session:listAppConnection	授予查询应用使用记录的权限。	write	-	-
workspace:session:logoffUserSession	授予用户会话注销的权限。	write	-	-
workspace:session:listUserConnection	授予查询用户登录记录的权限。	write	-	-
workspace:session:listSessionByUserName	授予根据用户名查询当前会话的权限。	list	-	-
workspace:storagePolicy:create	授予新增或更新存储目录访问权限自定义策略的权限。	write	storage *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:storagePolicy:list	授予查询存储目录访问权限策略的权限。	list	storage *	-
workspace:storage:listSfs3Storage	授予查询SFS3.0存储的权限。	list	storage *	-
workspace:baseResource:list	授予查询可用分区列表的权限。	list	-	-
workspace:tenants:listConfigInfo	授予查询企业系统配置的权限。	list	-	-
workspace:tenants:active	授予租户服务激活、初始化的权限。	write	-	-
workspace:tenants:listTenantProfile	授予查询租户信息的权限。	list	-	-
workspace:server:listServerMetricData	授予查询服务器的监控数据的权限。	list	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:session:listSessions	授予查询企业会话列表的权限。	list	-	-
workspace:appWarehouse:updateApp	授予更新应用仓库中的应用的权限。	write	-	-
workspace:server:batchChangeImage	授予批量切换服务器镜像的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchReinstall	授予批量重装服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:authConfigs:get	授予查询认证登录方式配置信息的权限。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:authConfigs:update	授予更新认证策略配置信息的权限。	write	-	-
workspace:assistAuthConfigs:get	授予查询辅助认证的配置信息的权限。	read	-	-
workspace:assistAuthConfigs:update	授予更新辅助认证配置的权限。	write	-	-
workspace:jobs:retry	授予重试任务的权限。	write	-	-
workspace:quotas:get	授予查询租户配额的权限。	read	-	-
workspace:tenants:getRoles	授予查询租户角色的权限。	read	-	-
workspace:tenants:ListConfig	授予查询租户个性配置列表的权限。	list	-	-
workspace:tenants:updateConfig	授予修改租户个性配置的权限。	write	-	-
workspace:natMappings:getConfig	授予查询租户的NAT映射配置项的权限。	read	-	-
workspace:natMappings:updateConfig	授予修改租户的NAT映射配置项的权限。	write	-	-
workspace:tenants:get	授予查询云办公服务详情的权限。	read	-	-
workspace:tenants:open	授予开通云办公服务的权限。	write	-	workspace:AccessMode
workspace:tenants:delete	授予注销云办公服务的权限。	write	-	-
workspace:tenants:update	授予修改云办公服务属性的权限。	write	-	workspace:AccessMode

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:tenants:getLockStatus	授予查询云办公服务是否被锁定的权限。	read	-	-
workspace:tenants:unlock	授予解除云办公服务锁定状态的权限。	write	-	-
workspace:agencies:create	授予创建委托的权限。	write	-	-
workspace:agencies:get	授予查询委托的权限。	read	-	-
workspace:desktops:commitAiAccelerateJob	授予创建渲染加速任务的权限。	write	-	-
workspace:desktops:getAiAccelerateJob	授予查询渲染加速任务的权限。	read	-	-
workspace:desktops:getSysPrepInfo	授予查询sysprep详情的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:checkBatchChangeImage	授予校验批量切换镜像的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:tenants:listDesktopNamePolicies	授予查询桌面名称策略列表的权限。	list	-	-
workspace:tenants:createDesktopNamePolicy	授予创建桌面名称策略的权限。	write	-	-
workspace:tenants:updateDesktopNamePolicy	授予更新桌面名称策略的权限。	write	-	-
workspace:tenants:batchDeleteDesktopNamePolicies	授予批量删除桌面名称策略的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:desktopPools:create	授予创建桌面池的权限。	write	desktopPool *	-
			user	-
			userGroup	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktopPools:list	授予查询桌面池列表的权限。	list	desktopPool *	-
workspace:desktopPools:update	授予修改桌面池属性的权限。	write	desktopPool *	-
workspace:desktopPools:delete	授予删除桌面池的权限。	write	desktopPool *	-
workspace:desktopPools:get	授予查询桌面池详情的权限。	read	desktopPool *	-
workspace:desktopPools:expand	授予扩容桌面池的权限。	write	desktopPool *	-
workspace:desktopPools:resize	授予桌面池变更规格的权限。	write	desktopPool *	-
workspace:desktopPools:rebuild	授予桌面池重建系统盘的权限。	write	desktopPool *	-
workspace:desktopPools:batchAddVolumes	授予桌面池批量添加磁盘的权限。	write	desktopPool *	-
workspace:desktopPools:batchDeleteVolumes	授予桌面池批量删除磁盘的权限。	write	desktopPool *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:desktopPools:batchExpandVolumes	授予桌面池批量扩容磁盘的权限。	write	desktopPool *	-
workspace:desktopPools:operate	授予操作桌面池的权限。	write	desktopPool *	-
workspace:desktopPools:listUsers	授予查询桌面池授权的用户、用户组的权限。	list	desktopPool *	-
workspace:desktopPools:authorizeUsers	授予桌面池授权用户、用户组的权限。	write	desktopPool *	-
			user	-
			userGroup	-
workspace:desktopPools:listDesktops	授予查询桌面池桌面信息的权限。	list	desktopPool *	-
workspace:desktopPools:listScriptTasks	授予查询桌面池的脚本执行任务列表的权限。	list	desktopPool *	-
workspace:desktopPools:executeScripts	授予桌面池批量执行脚本的权限。	write	desktopPool *	-
			script	-
workspace:desktopPools:sendNotifications	授予发送消息通知的权限。	write	desktopPool *	-
workspace:desktops:export	授予导出桌面列表的权限。	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:create	授予创建桌面的权限。	write	desktop *	-

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 • workspace:AssociatePublicIp • workspace:AccessMode
workspace:desktops:list	授予查询桌面列表的权限。	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:update	授予更新桌面信息的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:delete	授予删除桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:get	授予查询桌面详情的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDelete	授予批量删除桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:logoff	授予批量注销桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDetail	授予查询桌面详情列表的权限。	list	desktop *	-

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
workspace:desktops:operate	授予操作桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:resize	授予变更规格的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getConnectStatus	授予查询桌面登录状态统计数据的权限。	read	-	-
workspace:desktops:ListStatus	授予查询桌面登录状态的权限。	list	-	-
workspace:desktops:rebuild	授予重建桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getActions	授予查询桌面开关机信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createConsole	授予获取远程登录控制台地址的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:updateSids	授予更新桌面SID的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:rejoinDomain	授予重新加入AD域的权限。	write	desktop *	• 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
workspace:desktops:createImage	授予桌面转镜像的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDetach	授予批量解绑用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:detach	授予解绑用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:attach	授予分配用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getNetwork	授予查询桌面网络信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:changeNetwork	授予切换桌面网络的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:exclusiveHosts:listDesktops	授予查询专享桌面详情列表的权限。	list	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:desktops:listAll	授予查询普通桌面和渲染桌面列表的权限。	list	desktop *	-
workspace:desktopAssociate:listDiscoverVmInfo	授予查询可纳管的虚拟机列表的权限。	list	-	-
workspace:desktopAssociate:startTask	授予启动纳管虚拟机任务的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:desktopAssociate:switchScanTask	授予开启纳管扫描任务的权限。	write	-	-
workspace:desktopAssociate:getScanTaskSwitch	授予查询纳管扫描任务开关的权限。	read	-	-
workspace:desktops:setMaintenanceMode	授予批量设置桌面管理员维护模式的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:prepAttachUsers	授予预批量分配用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchAttachUsers	授予批量分配用户的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:changeUsername	授予在Windows AD场景下，修改与桌面关联的用户名的权限。	write	-	-
workspace:desktops:sendNotifications	授予发送消息通知的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:migrate	授予迁移桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listAgents	授予查询桌面安装agent列表的权限。	list	desktop *	• 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
workspace:desktops:batchInstallAgents	授予批量为桌面安装agent的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listTags	授予查询桌面标签的权限。	list	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:tag	授予创建桌面标签的权限。	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:untag	授予删除桌面标签的权限。	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:listProjectTags	授予查询项目标签的权限。	list	-	-
workspace:desktops:operateTags	授予批量添加删除标签的权限。	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:listByTags	授予使用标签过滤桌面的权限。	list	-	-
workspace:exclusiveHosts:create	授予创建专享主机的权限。	write	exclusiveHost *	-
			-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:exclusiveHosts:list	授予查询专享主机列表的权限。	list	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:exclusiveHosts:check	授予校验是否能创建专享主机的权限。	write	-	-
workspace:exclusiveHosts:get	授予查询专享主机详情的权限。	read	exclusiveHost *	g:EnterpriseProjectId
workspace:exclusiveHosts:update	授予更新专享主机信息的权限。	write	exclusiveHost *	g:EnterpriseProjectId
workspace:exclusiveHosts:delete	授予删除专享主机的权限。	write	exclusiveHost *	g:EnterpriseProjectId
workspace:mkp:listImages	授予查询云市场镜像列表的权限。	list	-	-
workspace:mkp:listCommodityInfos	授予查询云市场商品信息的权限。	list	-	-
workspace:mkp:createOrder	授予创建云市场产品订单的权限。	write	-	-
workspace:mkp:listListProductReserve	授予查询云市场库存信息的权限。	list	-	-
workspace:mkp:listCommodityDetails	授予查询云市场商品详情的权限。	list	-	-
workspace:mkp:listRelationCommodityDetails	授予查询商品的关联商品的权限。	list	-	-
workspace:mkp:listCommodityAgreements	授予查询云市场商品协议的权限。	list	-	-
workspace:networks:listEips	授予查询EIP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
workspace:networks:createEips	授予创建EIP的权限。	write	-	-
workspace:networks:bindEips	授予绑定EIP的权限。	write	-	-
workspace:networks:unbindEips	授予解绑EIP的权限。	write	-	-
workspace:networks:getEipQuota	授予查询EIP配额的权限。	read	-	-
workspace:networks:ListNatGateways	授予查询Nat网关列表的权限。	list	-	-
workspace:orders:create	授予包周期下单的权限。	write	-	• workspace:CreateOrderType • workspace:AssociatePublicIp • workspace:AccessMode
workspace:orders:change	授予创建变更订单的权限。	write	-	workspace:ChangeOrderType
workspace:orders:batchInquiry	授予批量询价的权限。	write	-	-
workspace:quotas:check	授予校验配额的权限。	write	-	-
workspace:renderDesktops:create	授予创建渲染桌面的权限。	write	-	-
workspace:renderDesktops:delete	授予删除渲染桌面的权限。	write	-	-
workspace:renderDesktops:list	授予查询渲染桌面列表的权限。	list	-	-
workspace:renderDesktops:action	授予操作渲染桌面的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:scheduledTasks:list	授予查询定时任务列表的权限。	list	scheduledTask *	-
workspace:scheduledTasks:create	授予创建定时任务的权限。	write	scheduledTask *	-
			desktop	-
			desktopPool	-
			server	-
			serverGroup	-
workspace:scheduledTasks:get	授予查询定时任务详情的权限。	read	scheduledTask *	-
workspace:scheduledTasks:update	授予更新定时任务的权限。	write	scheduledTask *	-
			desktop	-
			desktopPool	-
			server	-
			serverGroup	-
workspace:scheduledTasks:delete	授予删除定时任务的权限。	write	scheduledTask *	-
workspace:scheduledTasks:getFuture	授予查询定时任务未来执行时间的权限。	read	-	-
workspace:scheduledTasks:batchDelete	授予批量删除定时任务的权限。	write	scheduledTask *	-
workspace:scheduledTasks:listRecords	授予查询定时任务执行记录的权限。	list	scheduledTask *	-
workspace:scheduledTasks:getRecord	授予查询定时任务执行记录详情的权限。	read	scheduledTask *	-
workspace:scheduledTasks:exportRecords	授予导出定时任务记录及执行详情的权限。	list	scheduledTask *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:users:subscribeSharer	授予订阅协同资源的权限。	write	user *	-
workspace:desktops:addSubResources	授予购买桌面附属资源的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:deleteSubResources	授予删除桌面附属资源的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createSnapshots	授予创建桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getSnapshots	授予查询桌面快照的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:deleteSnapshots	授予删除桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:restoreBySnapshot	授予使用桌面快照恢复桌面的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:statistics:listDesktopStatus	授予统计桌面状态的权限。	list	-	-
workspace:statistics:getUnused	授予查询在指定时间段未使用的桌面的权限。	read	-	-
workspace:statistics:getUsed	授予查询使用桌面的时长的权限。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:bindingPolicies:export	授予导出终端与桌面绑定配置excel的权限。	list	-	-
workspace:bindingPolicies:getConfig	授予查询终端与桌面绑定的开关配置信息的权限。	read	-	-
workspace:bindingPolicies:createConfig	授予设置终端与桌面绑定的开关配置的权限。	write	-	-
workspace:bindingPolicies:get	授予查询终端与桌面绑定配置列表的权限。	read	-	-
workspace:bindingPolicies:add	授予增加终端与桌面绑定配置的权限。	write	-	-
workspace:bindingPolicies:update	授予修改终端与桌面绑定配置的权限。	write	-	-
workspace:bindingPolicies:delete	授予删除终端与桌面绑定配置的权限。	write	-	-
workspace:volumes:delete	授予删除桌面数据盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:batchAdd	授予增加桌面磁盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:batchExpand	授予扩容桌面磁盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:wdh:getType	授予查询云办公主机类型的权限。	read	wdh *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:wdh:get	授予查询云办公主机列表的权限。	read	wdh *	g:EnterpriseProjectId
workspace:desktops:getRemoteAssistance	授予查询远程协助信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createRemoteAssistance	授予创建远程协助的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:cancelRemoteAssistance	授予取消远程协助的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:add	授予单个桌面增加磁盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:expand	授予扩容磁盘的权限。	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:listDssPoolsDetail	授予获取专属分布式存储池详情列表的权限。	list	-	-
workspace:common:listTimezones	授予查询时区配置的权限。	list	-	-
workspace:connections:securityExport	授予导出连接记录的权限。	list	-	-
workspace:images:list	授予查询支持的镜像列表的权限。	list	-	-
workspace:policyGroups:import	授予导入策略组的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:accessPolicies:create	授予创建接入策略的权限。	write	-	-
workspace:accessPolicies:get	授予查询接入策略的权限。	read	-	-
workspace:accessPolicies:delete	授予删除指定接入策略的权限。	write	-	-
workspace:accessPolicies:getTarget	授予查询指定接入策略的应用对象的权限。	read	-	-
workspace:accessPolicies:updateTarget	授予更新指定接入策略的应用对象的权限。	write	-	-
workspace:products:listDesktopProducts	授予查询支持的产品套餐列表的权限。	list	-	-
workspace:products:listSharerProducts	授予查询协同套餐列表的权限。	list	-	-
workspace:products:listInternetProducts	授予查询上网套餐列表的权限。	list	-	-
workspace:availabilityZones:list	授予查询支持的可用分区列表的权限。	list	-	-
workspace:userGroups:export	授予导出用户组的权限。	list	userGroup *	-
workspace:users:export	授予导出用户的权限。	list	user *	-
workspace:users:import	授予导入用户的权限。	write	user *	-
workspace:userGroups:exportUsers	授予导出用户组用户的权限。	list	userGroup *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:users:operate	授予操作用户（锁定、解锁和重置密码）的权限。	write	user *	-
workspace:users:randomPassword	授予给用户重置随机密码的权限。	write	user *	-
workspace:users:deleteOtps	授予解绑OTP设备的权限。	write	user *	-
workspace:users:resendEmail	授予重新发送邮件的权限。	write	user *	-
workspace:connections:securityList	授予查询连接信息的权限。	list	-	-
workspace:connections:listOnlineUsers	授予查询登录人数的权限。	list	-	-
workspace:userGroups:list	授予查询用户组列表的权限。	list	userGroup *	-
workspace:userGroups:create	授予创建用户组的权限。	write	userGroup *	-
workspace:userGroups:batchDelete	授予批量删除用户组的权限。	write	userGroup *	-
workspace:userGroups:delete	授予删除桌面用户组的权限。	write	userGroup *	-
workspace:userGroups:update	授予修改用户组信息的权限。	write	userGroup *	-
workspace:userGroups:operate	授予操作用户组的权限。	write	userGroup *	-
			user *	-
workspace:userGroups:getUsers	授予查询用户组中的用户的权限。	list	userGroup *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:jobs:listSubJobs	授予查询子任务列表的权限。	list	-	-
workspace:jobs:deleteSubJobRecords	授予删除子任务记录的权限。	write	-	-
workspace:ou:get	授予查询OU信息的权限。	list	-	-
workspace:ou:create	授予新增OU信息的权限。	write	-	-
workspace:ou:delete	授予删除OU信息的权限。	write	-	-
workspace:ou:update	授予更新OU信息的权限。	write	-	-
workspace:policyGroups:list	授予查询策略组列表的权限。	list	policyGroup *	-
workspace:policyGroups:create	授予新增策略组的权限。	write	policyGroup *	-
			desktop	-
			desktopPool	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:delete	授予删除策略组的权限。	write	policyGroup *	-
workspace:policyGroups:get	授予查询策略组的权限。	read	policyGroup *	-
workspace:policyGroups:update	授予修改策略组的权限。	write	policyGroup *	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:export	授予导出策略组的权限。	list	policyGroup *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:policyGroups:listPolicies	授予查询策略组中的策略项的权限。	list	policyGroup *	-
workspace:policyGroups:updatePolicies	授予修改策略组中的策略项的权限。	write	policyGroup *	-
workspace:policyGroups:listTargets	授予查询策略组应用对象的权限。	list	policyGroup *	-
workspace:policyGroups:updateTargets	授予修改策略组应用对象的权限。	write	policyGroup *	-
			desktop	-
			desktopPool	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:listDetail	授予查询策略组详情列表的权限。	list	policyGroup *	-
workspace:policyGroups:getOriginalPolicies	授予查询初始策略项的权限。	read	policyGroup *	-
workspace:users:list	授予查询用户列表的权限。	list	user *	-
workspace:users:create	授予创建用户的权限。	write	user *	-
workspace:users:delete	授予删除指定用户的权限。	write	user *	-
workspace:users:get	授予查询用户详情信息的权限。	read	user *	-
workspace:users:update	授予修改用户信息的权限。	write	user *	-
workspace:users:batchDelete	授予批量删除用户的权限。	write	user *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:users:resetPassword	授予重置用户密码的权限。	write	user *	-
workspace:users:checkResetPasswordToken	授予校验重置域用户密码Token的权限。	write	user *	-
workspace:users:getTemplate	授予用户模板下载的权限。	read	-	-
workspace:users:checkExist	授予校验用户是否存在的权限。	write	user *	-
workspace:users:listOtps	授予查询OTP设备的权限。	list	user *	-
workspace:users:getImportTemplate	授予创建用户模板下载的权限。	read	-	-
workspace:users:batchCreate	授予批量创建用户的权限。	write	user *	-
workspace:products:listVolumeProducts	授予查询磁盘产品列表的权限。	list	-	-
workspace:tenants:listExportTasks	授予查询导出任务列表的权限。	list	-	-
workspace:tenants:deleteExportTasks	授予批量删除导出任务记录的权限。	write	-	-
workspace:tenants:exportData	授予下载导出的文件的权限。	read	-	-
workspace:statistics:listAlarm	授予查询告警列表的权限。	list	-	-
workspace:statistics:getAlarm	授予查询告警数的权限。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:statistics:getGrowthRate	授予查询指标环比值的权限。	read	-	-
workspace:statistics:getMetric	授予查询指标的权限。	read	-	-
workspace:statistics:getMetricTrend	授予查询指标趋势的权限。	read	-	-
workspace:statistics:updateNotificationRules	授予更新指标的通知规则的权限。	write	-	-
workspace:statistics:deleteNotificationRules	授予删除指标的通知规则的权限。	write	-	-
workspace:statistics:createNotifyRules	授予新增指标的通知规则的权限。	write	-	-
workspace:statistics:listNotificationRules	授予查询指标的通知规则的权限。	list	-	-
workspace:statistics:listNotificationRecords	授予查询指标通知记录的权限。	list	-	-
workspace:statistics:listDesktopMetrics	授予查询桌面使用统计信息的权限。	list	-	-
workspace:statistics:exportDesktopMetrics	授予导出桌面使用统计信息的权限。	list	-	-
workspace:statistics:listUserMetrics	授予查询用户使用统计信息的权限。	list	-	-
workspace:statistics:exportUserMetrics	授予导出用户使用统计信息;的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:appcenter:createBucketCredential	授予生成OBS桶凭证信息信息的权限。	write	-	-
workspace:appcenter:createAndAuthorizeBucket	授予添加并授权默认OBS桶的权限。	write	-	-
workspace:appcenter:listApps	授予按照名称分页查询应用的权限。	list	-	-
workspace:appcenter:createApp	授予上传应用的权限。	write	-	-
workspace:appcenter:updateApp	授予修改应用的权限。	write	-	-
workspace:appcenter:deleteApp	授予删除应用的权限。	write	-	-
workspace:appcenter:installApp	授予自动安装应用的权限。	write	-	-
workspace:appcenter:listAppAuthorizations	授予查询应用授权信息的权限。	list	-	-
workspace:appcenter:batchUpdateAppAuthorizations	授予设置应用授权的权限。	write	-	-
workspace:appcenter:batchDeleteApps	授予批量删除应用的权限。	write	-	-
workspace:appcenter:batchDisableApps	授予批量设置应用不可见的权限。	write	-	-
workspace:appcenter:batchEnableApps	授予批量设置应用可见的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:appcenter:batchInstallApps	授予批量自动安装安装应用的权限。	write	-	-
workspace:appcenter:listAppCatalogs	授予查询应用分类信息的权限。	list	-	-
workspace:appcenter:listJobs	授予查询应用安装job信息的权限。	list	-	-
workspace:appcenter:batchDeleteJobs	授予批量删除job的权限。	write	-	-
workspace:appcenter:retryJobs	授予重试失败job的权限。	write	-	-
workspace:appcenter:createAppRule	授予创建应用规则的权限。	write	-	-
workspace:appcenter:listAppRule	授予查询应用规则的权限。	list	-	-
workspace:appcenter:updateAppRule	授予修改应用规则的权限。	write	-	-
workspace:appcenter:deleteAppRule	授予删除应用规则的权限。	write	-	-
workspace:appcenter:batchDeleteAppRules	授予批量删除应用规则的权限。	write	-	-
workspace:appcenter:enableRuleRestriction	授予启用规则管控的权限。	write	-	-
workspace:appcenter:disableRuleRestriction	授予禁用规则管控的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:appcenter:addRestrictedRule	授予增加管控规则的权限。	write	-	-
workspace:appcenter:listRestrictedRule	授予查询管控规则列表的权限。	list	-	-
workspace:appcenter:deleteRestrictedRule	授予批量删除管控规则列表的权限。	write	-	-
workspace:appcenter:updateTenantProfile	授予禁用租户功能的权限。	write	-	-
workspace:appcenter:listTenantProfiles	授予查询租户功能状态的权限。	list	-	-
workspace:scripts:create	授予创建脚本的权限。	write	script *	-
workspace:scripts:list	授予查询脚本列表的权限。	list	script *	-
workspace:scripts:get	授予查询脚本详情的权限。	read	script *	-
workspace:scripts:put	授予更新脚本的权限。	write	script *	-
workspace:scripts:delete	授予删除脚本的权限。	write	script *	-
workspace:scripts:execute	授予批量执行脚本或命令的权限。	write	script *	-
			desktop *	-
workspace:scripts:getRecordDetail	授予查询脚本或命令执行记录详情的权限。	read	script *	-
workspace:scripts:listRecords	授予查询脚本执行记录列表的权限。	list	script *	-
workspace:scripts:listTasks	授予查询脚本任务列表的权限。	list	script *	-
workspace:scripts:retry	授予重试脚本的权限。	write	script *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:scripts:stop	授予停止脚本或命令执行任务的权限。	write	script *	-
workspace:scripts:download	授予下载脚本输出记录的权限。	write	script *	-
workspace:tenants:getShareSpaceConfig	授予查询协同配置的权限。	read	-	-
workspace:tenants:updateShareSpaceConfig	授予修改协同配置的权限。	write	-	-
workspace:authConfigs:getStatus	授予查询认证状态的权限。	read	-	-
workspace:privacystatements:sign	授予签署隐私声明的权限。	write	-	-
workspace:sites:get	授予查询站点信息的权限。	read	-	-
workspace:sites:add	授予新增站点的权限。	write	-	workspace:AccessMode
workspace:sites:delete	授予删除站点的权限。	write	-	-
workspace:sites:updateAccessMode	授予修改站点接入方式的权限。	write	-	workspace:AccessMode
workspace:sites:updateSubnets	授予修改站点业务子网的权限。	write	-	-
workspace:tenants:checkEnterpriseIds	授予检查企业ID是否已被使用的权限。	write	-	-
workspace:tenants:updateEnterpriseId	授予修改企业ID的权限。	write	-	-
workspace:bandwidth:create	授予开通云办公带宽的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:bandwidth:list	授予查询云办公带宽列表的权限。	list	-	-
workspace:bandwidth:update	授予修改云办公带宽的权限。	write	-	-
workspace:bandwidth:delete	授予取消云办公带宽的权限。	write	-	-
workspace:bandwidth:getControlConfig	授予查询云办公带宽的控制配置的权限。	read	-	-
workspace:bandwidth:updateControlConfig	授予修改云办公带宽的控制配置的权限。	write	-	-
workspace:bandwidth:createChangeOrder	授予创建云办公带宽变更订单的权限。	write	-	-
workspace:desktops:batchCreateSnapshots	授予批量创建桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDeleteSnapshots	授予批量删除桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchRestoreSnapshots	授予批量恢复桌面快照的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listSnapshots	授予查询桌面快照列表的权限。	list	-	-
workspace:desktops:verifyDesktopName	授予校验桌面名称的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:networks:getAvailableIp	授予根据子网id查询该子网下可用的ip的权限。	read	-	-
workspace:desktops:getAdStatus	授予查询AD网络状态的权限。	read	-	-
workspace:networks:checkIpIfExist	授予检查IP是否存在的权限。	write	-	-
workspace:images:checkIfExist	授予检查镜像是否存在的权限。	write	-	-
workspace:wdh:listDesktops	授予查询云办公主机包含桌面信息的权限。	list	wdh *	-
			-	g:EnterpriseProjectId
workspace:wdh:update	授予更新云办公主机信息的权限。	write	wdh *	g:EnterpriseProjectId
workspace:bindingPolicies:getTemplate	授予下载终端与桌面绑定模板的权限。	read	-	-
workspace:bindingPolicies:import	授予批量导入终端与桌面绑定的权限。	write	-	-
workspace:statistics:getRunState	授予运行状态统计的权限。	read	-	-
workspace:statistics:getLoginState	授予登录状态统计的权限。	read	-	-
workspace:networks:getUsingSubnets	授予查询正在被使用的子网列表的权限。	read	-	-
workspace:networks:listPorts	授予查询端口列表的权限。	list	-	-
workspace:renderDesktops:createConsole	授予获取远程登录控制台地址的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:renderDesktops:resize	授予变更渲染桌面规格的权限。	write	-	-
workspace:exclusiveHosts:resizeLites	授予变更专享主机规格的权限。	write	exclusiveHost *	g:EnterpriseProjectId
workspace:desktops:getMonitor	授予查询桌面监控信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDetachInfo	授予查询桌面历史解绑用户信息的权限。	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:getSysprepVersion	授予查询sysprep版本信息的权限。	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:networks:createNat	授予开通NAT网关上网功能的权限。	write	-	-
workspace:networks:listNats	授予查询NAT网关上网功能的权限。	list	-	-
workspace:networks:listSubnets	授予查询子网列表的权限。	list	-	-
workspace:networks:listVpcs	授予查询查询vpc的权限。	list	-	-
workspace:policyGroups:createTemplate	授予创建策略模板的权限。	write	-	-
workspace:policyGroups:listTemplate	授予查询策略模板列表的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:policyGroups:updateTemplate	授予更新策略模板的权限。	write	-	-
workspace:networks:listSecurityGroups	授予查询安全组列表的权限。	list	-	-
workspace:availabilityZones:getSummary	授予查询可用分区列表概要的权限。	read	-	-
workspace:availabilityZones:get	授予查询可用分区详情的权限。	read	-	-
workspace:users:importUser	授予导入用户列表的权限。	write	user *	-
workspace:users:uploadTemplate	授予导入桌面用户列表的权限。	write	user *	-
workspace:accessPolicies:update	授予更新指定接入策略的权限。	write	-	-
workspace:desktops:verifySource	授予校验桌面来源的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDesktopNetworks	授予批量查询桌面网络信息的权限。	list	desktop *	-
workspace:desktops:batchChangeNetwork	授予批量切换桌面网络的权限。	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:jobs:get	授予查询任务详情的权限。	read	-	-
workspace:accessPolicies:importIp	授予导入IP列表的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:accessPolicies:getIpImportTemplate	授予下载IP导入模板的权限。	read	-	-
workspace:sites:listEdgeSites	授予查询边缘站点的权限。	list	-	-
workspace:sites:checkEdgeSiteResources	授予校验边缘站点资源的权限。	write	-	-
workspace:ou:listAdOus	授予查询AD域下OU信息的权限。	list	-	-
workspace:ou:listOuUsers	授予查询OU下用户信息的权限。	list	-	-
workspace:ou:importUsersByOU	授予导入OU用户的权限。	write	-	-
workspace:appGroup:list	授予查询应用组的权限。	list	appGroup *	-
workspace:appGroup:create	授予创建应用组的权限。	write	appGroup *	-
			serverGroup	-
workspace:appGroup:delete	授予应用组删除的权限。	write	appGroup *	-
workspace:appGroup:get	授予查询应用组详情的权限。	read	appGroup *	-
workspace:appGroup:update	授予修改应用组的权限。	write	appGroup *	-
			serverGroup	-
workspace:app:listPublishedApp	授予查询已发布应用的权限。	list	app *	-
			appGroup *	-
workspace:app:publish	授予发布应用的权限。	write	app *	-
			appGroup *	-
workspace:app:get	授予查询应用详细信息的权限。	read	app *	-
			appGroup *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:app:update	授予修改应用信息的权限。	write	app *	-
			appGroup *	-
workspace:app:deleteIcon	授予删除自定义应用图标的权限。	write	app *	-
			appGroup *	-
workspace:app:uploadIcon	授予修改自定义应用图标的权限。	write	app *	-
			appGroup *	-
workspace:app:check	授予校验应用的权限。	write	app *	-
			appGroup *	-
workspace:app:batchDisable	授予批量禁用应用的权限。	write	app *	-
			appGroup *	-
workspace:app:batchEnable	授予批量启用应用的权限。	write	app *	-
			appGroup *	-
workspace:app:unpublish	授予批量取消应用发布的权限。	write	app *	-
			appGroup *	-
workspace:appGroup:listPublishableApp	授予可发布应用列表的权限。	list	appGroup *	-
workspace:appGroup:batchDeleteAuthorization	授予移除应用组授权的权限。	write	appGroup *	-
			user	-
			userGroup	-
workspace:appGroup:disassociate	授予解除服务组关联的所有应用组的权限。	write	-	-
workspace:appGroup:listAuthorization	授予查询应用组授权记录的权限。	list	appGroup *	-
workspace:appGroup:addAuthorization	授予增加应用组授权的权限。	write	appGroup *	-
			user	-
			userGroup	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:appGroup:batchDelete	授予批量删除应用组的权限。	write	appGroup *	-
workspace:appGroup:check	授予校验应用组的权限。	write	-	-
workspace:serverGroup:list	授予查询服务器组列表的权限。	list	serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:serverGroup:create	授予创建服务器组的权限。	write	serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:serverGroup:delete	授予删除服务器组的权限。	write	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:get	授予查询指定服务器组的权限。	read	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:update	授予修改服务器组的权限。	write	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:getServerState	授予查询指定服务器组内服务器状态的权限。	read	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:listDetail	授予查询租户服务器组基础信息列表的权限。	list	serverGroup *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:serverGroup:getRestrict	授予指定租户服务器组限制查询的权限。	read	serverGroup *	-
workspace:serverGroup:validate	授予校验服务器组的权限。	write	serverGroup *	-
workspace:serverGroup:tagResource	授予服务器组添加标签的权限。	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:unTagResource	授予服务器组删除标签的权限。	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:listTagsForResource	授予查询服务器组标签的权限。	list	serverGroup *	-
			-	g:EnterpriseProjectId
workspace:serverGroup:listTags	授予查询租户所有服务器上标签的权限。	list	serverGroup *	-
workspace:serverGroup:batchCreateTags	授予批量添加服务器组标签的权限。	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:batchDeleteTags	授予批量删除服务器组标签的权限。	tagging	serverGroup *	• 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
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:server:list	授予查询服务器列表的权限。	list	server *	-
workspace:server:delete	授予删除服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:get	授予查询指定服务器的权限。	read	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:update	授予修改服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:changeImage	授予修改服务器的镜像的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:reinstall	授予重装服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:getVncUrl	授予获取VNC远程登录地址的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:accessAgent:list	授予查询租户的所有HDA最新版本的权限。	list	-	-
workspace:accessAgent:batchUpgrade	授予批量升级服务器HDA版本的权限。	write	server *	• 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
workspace:accessAgent:listLatestVersion	授予查询租户的HDA最新版本的权限。	list	-	-
workspace:server:listAccessAgentDetails	授予查询服务器的HDA相关信息的权限。	list	server *	-
workspace:accessAgent:getUpgradeFlag	授予查询HDA升级提醒标识的权限。	read	-	-
workspace:accessAgent:updateUpgradeFlag	授予更新HDA升级通知标识的权限。	write	-	-
workspace:accessAgent:listUpgradeRecords	授予查询服务器的HDA升级跟踪记录的权限。	list	-	-
workspace:server:batchDelete	授予批量删除服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchChangeMaintainMode	授予标记服务器维护状态的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchReboot	授予重启服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchRejoinDomain	授予批量服务器重新加域的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchStart	授予启动服务器的权限。	write	server *	• 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
workspace:server:batchStop	授予关闭服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchUpdateTsvi	授予批量更新服务器虚拟会话IP配置的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:create	授予创建应用服务器的权限。	write	server *	-
			serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:server:batchMigrateHosts	授予迁移云办公主机下面的服务器到目标云办公主机的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			wdh *	-
workspace:server:getMetricData	授予查询云应用服务器监控信息的权限。	read	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:jobs:batchDeleteSubJobs	授予批量删除子任务的权限。	write	-	-
workspace:jobs:countSubJobs	授予子任务数量查询的权限。	list	-	-
workspace:appWarehouse:authorizeObs	授予获取上传至OBS桶的ak/sk的权限。	write	-	-
workspace:appWarehouse:batchDeleteApp	授予批量删除应用仓库中的指定应用的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:appWarehouse:ListWarehouseApps	授予查询租户应用仓库中的应用列表的权限。	list	-	-
workspace:appWarehouse:createApp	授予在应用仓库中新增应用的权限。	write	-	-
workspace:appWarehouse:deleteApp	授予删除应用仓库中的指定应用的权限。	write	-	-
workspace:appWarehouse:uploadAppIcon	授予在应用仓库中上传图标文件的权限。	write	-	-
workspace:appWarehouse:createBucketOrAcl	授予添加桶或者桶授权的权限。	write	-	-
workspace:images:listImageJobs	授予查询租户的任务列表的权限。	list	-	-
workspace:images:getImageJob	授予查询任务详情的权限。	read	-	-
workspace:imageServer:list	授予查询镜像实例列表的权限。	list	imageServer *	-
			-	g:EnterpriseProjectId
workspace:imageServer:create	授予创建镜像实例的权限。	write	imageServer *	-
			-	g:EnterpriseProjectId
workspace:imageServer:get	授予查询指定镜像实例的权限。	read	imageServer *	g:EnterpriseProjectId
workspace:imageServer:update	授予修改镜像实例的权限。	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:attachApp	授予分发软件信息至镜像实例的权限。	write	imageServer *	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:imageServer:listLatestAttachedApp	授予查询最近一次分发软件信息列表的权限。	list	imageServer *	-
workspace:imageServer:recreate	授予构建云应用镜像的权限。	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:batchDelete	授予批量删除镜像实例的权限。	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:listImageSubJobs	授予子任务查询的权限。	list	-	-
workspace:imageServer:batchDeleteImageSubJobs	授予批量删除子任务的权限。	write	-	-
workspace:imageServer:countImageSubJobs	授予子任务数量查询的权限。	read	-	-
workspace:appGroup:listMailRecord	授予查询应用组授权邮件发送记录的权限。	list	-	-
workspace:appGroup:resendMail	授予重发应用组授权邮件（根据授权邮件记录）的权限。	write	-	-
workspace:storage:listPersistentStorage	授予查询WKS存储的权限。	list	storage *	-
workspace:storage:createPersistentStorage	授予创建WKS存储的权限。	write	storage *	-
workspace:storage:deletePersistentStorage	授予删除WKS存储的权限。	write	storage *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:storage:updateUserFolderAssignment	授予创建个人存储目录的权限。	write	storage *	-
workspace:storage:updateShareFolderAssignment	授予修改共享目录成员的权限。	write	storage *	-
workspace:storage:createShareFolder	授予创建共享存储目录的权限。	write	storage *	-
workspace:storage:deleteStorageClaim	授予删除共享目录的权限。	write	storage *	-
workspace:storage:deleteUserStorageAttachment	授予删除个人存储目录的权限。	write	storage *	-
workspace:storage:batchDeletePersistentStorage	授予批量删除WKS存储的权限。	write	storage *	-
workspace:storage:listStorageAssignment	授予查询个人存储目录的权限。	list	storage *	-
workspace:storage:listShareFolder	授予查询共享存储目录的权限。	list	storage *	-
workspace:policyGroups:deleteTemplate	授予删除策略模板的权限。	write	-	-
workspace:privacystatements:get	授予查询最新版本的隐私声明的权限。	read	-	-
workspace:scalingPolicy:delete	授予删除弹性伸缩策略的权限。	write	-	-
workspace:scalingPolicy:list	授予查询服务器组弹性伸缩策略的权限。	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
workspace:scalingPolicy:create	授予新增/修改弹性伸缩策略的权限。	write	-	-
workspace:session:listAppConnection	授予查询应用使用记录的权限。	write	-	-
workspace:session:logoffUserSession	授予用户会话注销的权限。	write	-	-
workspace:session:listUserConnection	授予查询用户登录记录的权限。	write	-	-
workspace:session:listSessionByUserName	授予根据用户名查询当前会话的权限。	list	-	-
workspace:storagePolicy:create	授予新增或更新存储目录访问权限自定义策略的权限。	write	storage *	-
workspace:storagePolicy:list	授予查询存储目录访问权限策略的权限。	list	storage *	-
workspace:storage:listSfs3Storage	授予查询SFS3.0存储的权限。	list	storage *	-
workspace:baseResource:list	授予查询可用分区列表的权限。	list	-	-
workspace:tenants:listConfigInfo	授予查询企业系统配置的权限。	list	-	-
workspace:tenants:active	授予租户服务激活、初始化的权限。	write	-	-
workspace:tenants:listTenantProfile	授予查询租户信息的权限。	list	-	-
workspace:server:listServerMetricData	授予查询服务器的监控数据的权限。	list	server *	• 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
workspace:session:listSessions	授予查询企业会话列表的权限。	list	-	-
workspace:appWarehouse:updateApp	授予更新应用仓库中的应用的权限。	write	-	-
workspace:server:batchChangeImage	授予批量切换服务器镜像的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchReinstall	授予批量重装服务器的权限。	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:tenants:updateAccessAddressBackupConfig	授予修改云办公服务接入地址备份配置的权限	write	-	-
workspace:tenants:listAccessAddressBackupConfig	授予获取云办公服务接入地址备份配置的权限	list	-	-
workspace:desktops:listWithConnectStatus	授予查询桌面连接状态列表的权限	list	-	-
workspace:orders:createDesktopOrder	授予创建桌面订单的权限	write	-	-
workspace:products:listHourPackageProducts	授予查询可订购小时包套餐的权限	list	-	-

云桌面Workspace的API通常对应着一个或多个授权项。**表5-205**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-205 API 与操作项的关系

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/auth-config/method-config	workspace:authConfigs:get	-
PUT /v2/{project_id}/auth-config/method-config	workspace:authConfigs:update	-
GET /v2/{project_id}/assist-auth-config/method-config	workspace:assistAuthConfigs:get	-
PUT /v2/{project_id}/assist-auth-config/method-config	workspace:assistAuthConfigs:update	-
POST /v2/{project_id}/workspace-jobs/{job_id}/actions	workspace:jobs:retry	-
GET /v2/{project_id}/quotas	workspace:quotas:get	-
GET /v2/{project_id}/tenants/roles	workspace:tenants:getRoles	-
GET /v2/{project_id}/tenant-configs	workspace:tenants:ListConfig	-
PUT /v2/{project_id}/tenant-configs	workspace:tenants:updateConfig	-
GET /v2/{project_id}/nat-mapping-configs	workspace:natMappings:getConfig	-
PUT /v2/{project_id}/nat-mapping-configs	workspace:natMappings:updateConfig	-
GET /v2/{project_id}/workspaces	workspace:tenants:get	• vpc:vpcs:get • vpc:subnets:get • vpc:securityGroups:get

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/workspaces	workspace:tenants:open	• eip:bandwidths:create • eip:publicIps:create • elb:healthmonitors:create • elb:healthmonitors:show • elb:listeners:create • elb:listeners:update • elb:listeners:show • elb:listeners:list • elb:loadbalancers:create • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:list • elb:members:update • elb:pools:create • elb:pools:update • elb:pools:show • vpc:ports:create • vpc:ports:delete • vpc:securityGroupRules:create • vpc:securityGroupRules:delete • vpc:securityGroupRules:get • vpc:securityGroups:create • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:get

API	对应的操作项	依赖的操作项
DELETE /v2/{project_id}/workspaces	workspace:tenants:delete	• elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:delete • elb:listeners:show • elb:loadbalancers:delete • elb:loadbalancers:show • elb:members:delete • elb:members:list • elb:pools:delete • elb:pools:show • vpc:ports:delete • vpc:securityGroups:delete • vpcep:endpoints:delete • vpcep:endpoints:get • eip:publicIps:disassociateInstance • eip:bandwidths:delete • eip:publicIps:delete

API	对应的操作项	依赖的操作项
PUT /v2/{project_id}/workspaces	workspace:tenants:update	• eip:bandwidths:create • eip:bandwidths:delete • eip:publicIps:create • eip:publicIps:delete • eip:publicIps:disassociateInstance • elb:healthmonitors:create • elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:create • elb:listeners:delete • elb:listeners:update • elb:listeners:show • elb:loadbalancers:create • elb:loadbalancers:delete • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:delete • elb:members:list • elb:members:update • elb:pools:create • elb:pools:delete • elb:pools:update • elb:pools:show • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:delete • vpcep:endpoints:get
GET /v2/{project_id}/workspaces/lock-status	workspace:tenants:getLockStatus	-
PUT /v2/{project_id}/workspaces/lock-status	workspace:tenants:unlock	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/agencies	workspace:agencies:create	• iam:agencies:listV5 • iam:agencies:getV5 • iam:agencies:createServiceLinkedAgencyV5 • iam:roles:getRole • iam:roles:listRoles • iam:agencies:getAgency • iam:agencies:listAgencies • iam:agencies:createAgency • iam:permissions:listRolesForAgencyOnProject • iam:permissions:grantRoleToAgencyOnProject
GET /v2/{project_id}/agencies	workspace:agencies:get	• iam:agencies:listV5 • iam:agencies:getV5 • iam:agencies:getAgency • iam:agencies:listAgencies • iam:permissions:listRolesForAgencyOnProject
POST /v3/{project_id}/desktops/{desktop_id}/ai-accelerate-job	workspace:desktops:commitAiAccelerateJob	-
POST /v2/{project_id}/desktops/{desktop_id}/ai-accelerate-job	workspace:desktops:createAiAccelerateJob	-
GET /v2/{project_id}/ai-accelerate-job/{job_id}	workspace:desktops:getAiAccelerateJob	-
POST /v2/{project_id}/sysprep	workspace:desktops:getSysPrepInfo	-
POST /v2/{project_id}/verification/batch-change-image	workspace:desktops:checkBatchChangeImage	ims:images:list
GET /v2/{project_id}/desktop-name-policies	workspace:tenants:listDesktopNamePolicies	-
POST /v2/{project_id}/desktop-name-policies	workspace:tenants:createDesktopNamePolicy	-

API	对应的操作项	依赖的操作项
PUT /v2/{project_id}/desktop-name-policies/{policy_id}	workspace:tenants:updateDesktopNamePolicy	-
POST /v2/{project_id}/desktop-name-policies/batch-delete	workspace:tenants:batchDeleteDesktopNamePolicies	-
POST /v2/{project_id}/desktop-pools	workspace:desktopPools:create	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
GET /v2/{project_id}/desktop-pools	workspace:desktopPools:list	ims:images:list
PUT /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:update	-
DELETE /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:delete	-
GET /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:get	ims:images:list

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktop-pools/{pool_id}/expand	workspace:desktopPools:expand	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
POST /v2/{project_id}/desktop-pools/{pool_id}/resize	workspace:desktopPools:resize	• vpc:subnets:get • ims:images:list
POST /v2/{project_id}/desktop-pools/{pool_id}/rebuild	workspace:desktopPools:rebuild	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-add	workspace:desktopPools:batchAddVolumes	-
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-delete	workspace:desktopPools:batchDeleteVolumes	-
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-expand	workspace:desktopPools:batchExpandVolumes	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktop-pools/{pool_id}/action	workspace:desktopPools:operate	-
GET /v2/{project_id}/desktop-pools/{pool_id}/users	workspace:desktopPools:listUsers	-
POST /v2/{project_id}/desktop-pools/{pool_id}/users	workspace:desktopPools:authorizeUsers	ims:images:list
GET /v2/{project_id}/desktop-pools/{pool_id}/desktops	workspace:desktopPools:listDesktops	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktop-pools/script-execution-tasks/detail	workspace:desktopPools:listScriptTasks	-
POST /v2/{project_id}/desktop-pools/{pool_id}/script-executions	workspace:desktopPools:executeScripts	-
POST /v2/{project_id}/desktop-pools/{pool_id}/notifications	workspace:desktopPools:sendNotifications	-
GET /v3/{project_id}/desktops/export	workspace:desktops:export	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktops	workspace:desktops:create	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • eip:publicIps:get • eip:publicIps:list • eip:publicIps:create • eip:publicIps:associateInstance • eip:publicIps:delete • eip:publicIps:createTags • vpc:quotas:list • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
GET /v2/{project_id}/desktops	workspace:desktops:list	-
PUT /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:update	-
DELETE /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:delete	• vpc:ports:get • vpc:ports:delete
GET /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:get	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktops/batch-delete	workspace:desktops:batchDelete	• vpc:ports:get • vpc:ports:delete
POST /v2/{project_id}/desktops/logoff	workspace:desktops:logoff	-
GET /v2/{project_id}/desktops/detail	workspace:desktops:listDetail	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
POST /v2/{project_id}/desktops/action	workspace:desktops:operate	-
POST /v2/{project_id}/desktops/resize	workspace:desktops:resize	• vpc:subnets:get • ims:images:list
GET /v2/{project_id}/connections/status	workspace:desktops:getConnectStatus	-
GET /v2/{project_id}/desktops/status	workspace:desktops:ListStatus	-
POST /v2/{project_id}/desktops/rebuild	workspace:desktops:rebuild	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
GET /v2/{project_id}/desktops/{desktop_id}/actions	workspace:desktops:getActions	-
GET /v2/{project_id}/desktops/{desktop_id}/remote-consoles	workspace:desktops:createConsole	-
PUT /v2/{project_id}/desktops/sids	workspace:desktops:updateSids	-
POST /v2/{project_id}/desktops/{desktop_id}/rejoin-domain	workspace:desktops:rejoinDomain	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktops/desktop-to-image	workspace:desktops:createImage	• ims:quotas:get • ims:images:get • ims:images:list • ims:images:setTags • ims:images:setOrDeleteTags • ims:images:updateMemberStatus • ims:images:copyInRegion • ims:serverImages:create
POST /v2/{project_id}/desktops/batch-detach	workspace:desktops:batchDetach	vpc:ports:get
POST /v2/{project_id}/desktops/detach	workspace:desktops:detach	vpc:ports:get
POST /v2/{project_id}/desktops/attach	workspace:desktops:attach	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
GET /v2/{project_id}/desktops/{desktop_id}/networks	workspace:desktops:getNetwork	• vpc:vpcs:get • vpc:networks:get • vpc:subnets:get • vpc:ports:get • vpc:securityGroups:get • eip:publicIps:list

API	对应的操作项	依赖的操作项
PUT /v2/{project_id}/desktops/{desktop_id}/networks	workspace:desktops:changeNetwork	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:securityGroups:get • eip:publicIps:list • eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
GET /v2/{project_id}/exclusive-hosts/{host_id}/desktops	workspace:exclusiveHosts:listDesktops	-
GET /v2/{project_id}/all-desktops	workspace:desktops:listAll	-
GET /v2/{project_id}/desktop-associate/discover-vm/infos	workspace:desktopAssociate:listDiscoverVmInfo	-
POST /v2/{project_id}/desktop-associate/tasks	workspace:desktopAssociate:startTask	-
POST /v2/{project_id}/desktop-associate/discover-vm/switch	workspace:desktopAssociate:switchScanTask	-
GET /v2/{project_id}/desktop-associate/discover-vm/switch	workspace:desktopAssociate:getScanTaskSwitch	-
PUT /v2/{project_id}/desktops/maintenance-mode	workspace:desktops:setMaintenanceMode	-
POST /v2/{project_id}/desktops/pre-batch-attach	workspace:desktops:prepAttachUsers	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktops/batch-attach	workspace:desktops:batchAttachUsers	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
PUT /v2/{project_id}/desktops/change-username	workspace:desktops:changeUsername	-
POST /v2/{project_id}/desktops/notifications	workspace:desktops:sendNotifications	-
POST /v2/{project_id}/desktops/{desktop_id}/migrate	workspace:desktops:migrate	• vpc:networks:get • vpc:subnets:get • vpc:ports:create • vpc:ports:delete • vpc:ports:update • vpc:ports:get
GET /v2/{project_id}/desktops/agents	workspace:desktops:listAgents	-
POST /v2/{project_id}/desktops/agents	workspace:desktops:batchInstallAgents	-
GET /v2/{project_id}/desktops/{desktop_id}/tags	workspace:desktops:listTags	-
POST /v2/{project_id}/desktops/{desktop_id}/tags	workspace:desktops:tag	-
DELETE /v2/{project_id}/desktops/{desktop_id}/tags/{key}	workspace:desktops:untag	-
GET /v2/{project_id}/desktops/tags	workspace:desktops:listProjectTags	-
POST /v2/{project_id}/desktops/{desktop_id}/tags/action	workspace:desktops:operateTags	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktops/resource_instances/action	workspace:desktops:listByTags	-
POST /v2/{project_id}/desktops/batch-tags	workspace:desktops:tag	-
DELETE /v2/{project_id}/desktops/batch-tags	workspace:desktops:untag	-
POST /v2/{project_id}/exclusive-hosts	workspace:exclusiveHosts:create	• vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:subnets:get • vpc:vpcs:get
GET /v2/{project_id}/exclusive-hosts	workspace:exclusiveHosts:list	-
POST /v2/{project_id}/exclusive-hosts/check-limits	workspace:exclusiveHosts:check	-
GET /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:get	• nat:snatRules:list • eip:publicIps:list
PUT /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:update	-
DELETE /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:delete	-
GET /v2/{project_id}/market-images	workspace:mkp:listImages	ims:images:list
GET /v2/{project_id}/mkp/commodities/commodity-ids	workspace:mkp:listCommodityInfos	-
POST /v2/{project_id}/mkp/order	workspace:mkp:createOrder	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/mkp/product-reserve	workspace:mkp:listListProductReserve	-
GET /v2/{project_id}/mkp/commodities	workspace:mkp:listCommodityDetails	-
GET /v2/{project_id}/mkp/commodities/{commodity_id}/relation-commodities	workspace:mkp:listRelationCommodityDetails	-
GET /v2/{project_id}/mkp/commodities/agreements	workspace:mkp:listCommodityAgreements	-
GET /v2/{project_id}/eips	workspace:networks:listEips	• eip:publicIps:list • eip:bandwidths:list
POST /v2/{project_id}/eips	workspace:networks:createEips	• vpc:quotas:list • eip:publicIps:create • eip:publicIps:associateInstance
POST /v2/{project_id}/eips/binding	workspace:networks:bindEips	• eip:publicIps:associateInstance • eip:publicIps:get
POST /v2/{project_id}/eips/unbinding	workspace:networks:unbindEips	• eip:publicIps:list • eip:publicIps:disassociateInstance
GET /v2/{project_id}/eips/quotas	workspace:networks:getEipQuota	vpc:quotas:list
GET /v2/{project_id}/nat-gateways	workspace:networks:ListNatGateways	• vpc:subnets:get • vpc:vpcs:get • nat:snatRules:list • nat:natGateways:list

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/periodic/subscribe/order	workspace:orders:create	• ims:images:list • vpc:vpcs:get • vpc:networks:get • vpc:subnets:get • vpc:ports:get • bss:order:update
POST /v2/{project_id}/periodic/{desktop_id}/change/order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/periodic/change/batch-order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/periodic/inquiry/change-image	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/change/order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/desktop-pool/periodic/inquiry/add-volume	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/change-image	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/extend-volume	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/resize	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/periodic/inquiry/add-resources	workspace:orders:batchInquiry	ims:images:list
GET /v2/{project_id}/checkOrderLimits	workspace:quotas:check	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/render-desktops	workspace:renderDesktops:create	• ims:images:list • ims:images:share • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get
DELETE /v2/{project_id}/render-desktops	workspace:renderDesktops:delete	• vpc:ports:get • vpc:ports:delete
GET /v2/{project_id}/render-desktops	workspace:renderDesktops:list	-
POST /v2/{project_id}/render-desktops/action	workspace:renderDesktops:action	-
GET /v2/{project_id}/scheduled-tasks	workspace:scheduledTasks:list	-
POST /v2/{project_id}/scheduled-tasks	workspace:scheduledTasks:create	-
GET /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:get	-
PUT /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:update	-
DELETE /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:delete	-
POST /v2/{project_id}/scheduled-tasks/future-executions	workspace:scheduledTasks:getFuture	-
POST /v2/{project_id}/scheduled-tasks/batch-delete	workspace:scheduledTasks:batchDelete	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records	workspace:scheduledTasks:listRecords	-

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/scheduled-tasks/{task_id}/records/{record_id}	workspace:scheduledTasks:getRecord	-
POST /v2/{project_id}/scheduled-tasks/{task_id}/records/export	workspace:scheduledTasks:exportRecords	-
POST /v2/{project_id}/user/share-resources	workspace:users:subscribeSharer	-
POST /v2/{project_id}/desktop/sub-resources	workspace:desktops:addSubResources	-
POST /v2/{project_id}/desktop/delete-sub-resources	workspace:desktops:deleteSubResources	-
POST /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:createSnapshots	-
GET /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:getSnapshots	-
DELETE /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:deleteSnapshots	-
POST /v2/{project_id}/desktops/{desktop_id}/snapshots/restore	workspace:desktops:restoreBySnapshot	-
GET /v2/{project_id}/statistics	workspace:statistics:listDesktopStatus	-
GET /v2/{project_id}/desktops/statistics/unused	workspace:statistics:getUnused	-
POST /v2/{project_id}/desktops/statistics/used	workspace:statistics:getUsed	-
GET /v3/{project_id}/terminals/binding-desktops/template/export	workspace:bindingPolicies:export	-
GET /v2/{project_id}/terminals/binding-desktops/config	workspace:bindingPolicies:getConfig	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/terminals/binding-desktops/config	workspace:bindingPolicies:createConfig	-
GET /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:get	-
POST /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:add	-
PUT /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:update	-
POST /v2/{project_id}/terminals/binding-desktops/batch-delete	workspace:bindingPolicies:delete	-
POST /v2/{project_id}/desktops/{desktop_id}/volumes/batch-delete	workspace:volumes:delete	-
POST /v2/{project_id}/volumes	workspace:volumes:batchAdd	-
POST /v2/{project_id}/volumes/expand	workspace:volumes:batchExpand	-
GET /v2/{project_id}/hosts/types	workspace:wdh:getType	-
GET /v2/{project_id}/hosts	workspace:wdh:get	-
GET /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:getRemoteAssistance	-
POST /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:createRemoteAssistance	-
DELETE /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:cancelRemoteAssistance	-
POST /v2/{project_id}/desktops/{desktop_id}/volumes	workspace:volumes:add	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktops/{desktop_id}/volumes/{volume_id}/expand	workspace:volumes:expand	-
GET /v2/{project_id}/dss-pools/detail	workspace:volumes:listDssPoolsDetail	dss:pools:list
GET /v2/{project_id}/common/timezones	workspace:common:listTimezones	-
GET /v3/{project_id}/desktops/connections/export	workspace:connections:securityExport	-
GET /v2/{project_id}/images	workspace:images:list	ims:images:list
POST /v2/{project_id}/policy-groups/import	workspace:policyGroups:import	-
POST /v2/{project_id}/access-policy	workspace:accessPolicies:create	-
GET /v2/{project_id}/access-policy	workspace:accessPolicies:get	-
DELETE /v2/{project_id}/access-policy	workspace:accessPolicies:delete	-
GET /v2/{project_id}/access-policy/{access_policy_id}/objects	workspace:accessPolicies:getTarget	-
PUT /v2/{project_id}/access-policy/{access_policy_id}/objects	workspace:accessPolicies:updateTarget	-
GET /v2/{project_id}/products	workspace:products:listDesktopProducts	ecs:cloudServerFlavors:get
GET /v2/{project_id}/products/sharer	workspace:products:listSharerProducts	-
GET /v2/{project_id}/products/adninternet	workspace:products:listInternetProducts	-
GET /v2/{project_id}/availability-zones	workspace:availabilityZones:list	-
GET /v2/{project_id}/groups/export	workspace:userGroups:export	-

API	对应的操作项	依赖的操作项
POST /v3/{project_id}/users/export	workspace:users:export	-
POST /v2/{project_id}/users/import	workspace:users:import	-
GET /v3/{project_id}/groups/{group_id}/users/export	workspace:userGroups:exportUsers	-
GET /v2/{project_id}/groups/{group_id}/users/export	workspace:userGroups:exportUsers	-
POST /v2/{project_id}/users/{user_id}/actions	workspace:users:operate	-
GET /v2/{project_id}/users/{user_id}/random-password	workspace:users:randomPassword	-
DELETE /v2/{project_id}/users/{user_id}/otp-devices	workspace:users:deleteOtps	-
POST /v2/{project_id}/users/{user_id}/resend-email	workspace:users:resendEmail	-
GET /v2/{project_id}/connections/desktops	workspace:connections:securityList	-
GET /v2/{project_id}/connections/desktops/export	workspace:connections:securityExport	-
GET /v2/{project_id}/connections/online-users	workspace:connections:listOnlineUsers	-
GET /v2/{project_id}/desktops/connections	workspace:connections:securityList	-
GET /v2/{project_id}/desktops/connections/export	workspace:connections:securityExport	-
GET /v2/{project_id}/desktops/online-users	workspace:connections:listOnlineUsers	-
GET /v2/{project_id}/groups	workspace:userGroups:list	-
POST /v2/{project_id}/groups	workspace:userGroups:create	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/groups/batch-delete	workspace:userGroups:batchDelete	-
DELETE /v2/{project_id}/groups/{group_id}	workspace:userGroups:delete	-
PUT /v2/{project_id}/groups/{group_id}	workspace:userGroups:update	-
POST /v2/{project_id}/groups/{group_id}/actions	workspace:userGroups:operate	-
GET /v2/{project_id}/groups/{group_id}/users	workspace:userGroups:getUsers	-
GET /v2/{project_id}/workspace-sub-jobs	workspace:jobs:listSubJobs	-
POST /v2/{project_id}/workspace-sub-jobs/batch-delete	workspace:jobs:deleteSubJobRecords	-
GET /v2/{project_id}/ous	workspace:ou:get	-
POST /v2/{project_id}/ous	workspace:ou:create	-
DELETE /v2/{project_id}/ous/{ou_id}	workspace:ou:delete	-
PUT /v2/{project_id}/ous/{ou_id}	workspace:ou:update	-
GET /v2/{project_id}/policy-groups	workspace:policyGroups:list	-
POST /v2/{project_id}/policy-groups	workspace:policyGroups:create	-
DELETE /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:delete	-
GET /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:get	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:update	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/policy-groups/export	workspace:policyGroups:export	-
GET /v2/{project_id}/policy-groups/{policy_group_id}/policies	workspace:policyGroups:listPolicies	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}/policies	workspace:policyGroups:updatePolicies	-
GET /v2/{project_id}/policy-groups/{policy_group_id}/targets	workspace:policyGroups:listTargets	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}/targets	workspace:policyGroups:updateTargets	-
GET /v2/{project_id}/policy-groups/detail	workspace:policyGroups:listDetail	-
GET /v2/{project_id}/policy-groups/original-policies	workspace:policyGroups:getOriginalPolicies	-
GET /v2/{project_id}/users	workspace:users:list	-
POST /v2/{project_id}/users	workspace:users:create	-
DELETE /v2/{project_id}/users/{user_id}	workspace:users:delete	-
GET /v2/{project_id}/users/{user_id}	workspace:users:get	-
PUT /v2/{project_id}/users/{user_id}	workspace:users:update	-
POST /v2/{project_id}/users/batch-delete	workspace:users:batchDelete	-
POST /v2/{project_id}/users/password	workspace:users:resetPassword	-
POST /v2/{project_id}/users/password-token	workspace:users:checkResetPasswordToken	-

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/users/desktop-users/template	workspace:users:getTemplate	-
POST /v2/{project_id}/users/exist	workspace:users:checkExist	-
GET /v2/{project_id}/users/{user_id}/otp-devices	workspace:users:listOtps	-
GET /v2/{project_id}/users/template/download	workspace:users:getImportTemplate	-
POST /v2/{project_id}/users/export	workspace:users:export	-
POST /v2/{project_id}/users/batch-create	workspace:users:batchCreate	-
GET /v2/{project_id}/volume/products	workspace:products:listVolumeProducts	-
GET /v2/{project_id}/export-tasks	workspace:tenants:listExportTasks	-
POST /v2/{project_id}/export-tasks/batch-delete	workspace:tenants:deleteExportTasks	-
GET /v2/{project_id}/export-tasks/{task_id}/download	workspace:tenants:exportData	-
GET /v2/{project_id}/alarms	workspace:statistics:listAlarm	ces:alarmHistory:list
GET /v2/{project_id}/statistics/alarms	workspace:statistics:getAlarm	ces:alarmHistory:list
GET /v2/{project_id}/statistics/growth-rate	workspace:statistics:getGrowthRate	-
GET /v2/{project_id}/statistics/metrics	workspace:statistics:getMetric	-
GET /v2/{project_id}/statistics/metrics/trend	workspace:statistics:getMetricTrend	-
PUT /v2/{project_id}/statistics/notify-rules/{rule_id}	workspace:statistics:updateNotificationRules	smn:topic:get

API	对应的操作项	依赖的操作项
DELETE /v2/{project_id}/statistics/notify-rules/{rule_id}	workspace:statistics:deleteNotificationRules	-
POST /v2/{project_id}/statistics/notify-rules	workspace:statistics:createNotifyRules	smn:topic:get
GET /v2/{project_id}/statistics/notify-rules	workspace:statistics:listNotificationRules	-
GET /v2/{project_id}/statistics/notification-records	workspace:statistics:listNotificationRecords	-
GET /v2/{project_id}/statistics/metrics/desktops	workspace:statistics:listDesktopMetrics	-
GET /v2/{project_id}/statistics/metrics/desktops/export	workspace:statistics:exportDesktopMetrics	-
GET /v2/{project_id}/statistics/metrics/users	workspace:statistics:listUserMetrics	-
GET /v2/{project_id}/statistics/metrics/users/export	workspace:statistics:exportUserMetrics	-
GET /v3/{project_id}/statistics/metrics/desktops/export	workspace:statistics:exportDesktopMetrics	-
GET /v3/{project_id}/statistics/metrics/users/export	workspace:statistics:exportUserMetrics	-
POST /v1/{project_id}/app-center/buckets/actions/create-credential	workspace:appcenter:createBucketCredential	• obs:bucket:GetBucketAcl • obs:object:PutObject • obs:object:DeleteObject
POST /v1/{project_id}/app-center/buckets	workspace:appcenter:createAndAuthorizeBucket	• obs:bucket:HeadBucket • obs:bucket:PutBucketAcl • obs:bucket:PutReplicationConfiguration • obs:bucket:CreateBucket • obs:bucket:PutBucketCORS
GET /v1/{project_id}/app-center/apps	workspace:appcenter:listApps	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/app-center/apps	workspace:appcenter:createApp	-
PATCH /v1/{project_id}/app-center/apps/{app_id}	workspace:appcenter:updateApp	-
DELETE /v1/{project_id}/app-center/apps/{app_id}	workspace:appcenter:deleteApp	-
POST /v1/{project_id}/app-center/apps/{app_id}/actions/auto-install	workspace:appcenter:installApp	-
GET /v1/{project_id}/app-center/apps/{app_id}/authorizations	workspace:appcenter:listAppAuthorizations	-
POST /v1/{project_id}/app-center/apps/{app_id}/actions/assign-authorizations	workspace:appcenter:batchUpdateAppAuthorizations	-
POST /v1/{project_id}/app-center/apps/actions/batch-delete	workspace:appcenter:batchDeleteApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-disable	workspace:appcenter:batchDisableApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-enable	workspace:appcenter:batchEnableApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-assign-authorization	workspace:appcenter:batchUpdateAppAuthorizations	-
POST /v1/{project_id}/app-center/apps/actions/batch-auto-install	workspace:appcenter:batchInstallApps	-
GET /v1/{project_id}/app-center/app-catalogs	workspace:appcenter:listAppCatalogs	-
GET /v1/{project_id}/app-center/jobs	workspace:appcenter:listJobs	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/app-center/jobs/actions/batch-delete	workspace:appcenter:batchDeleteJobs	-
POST /v1/{project_id}/app-center/jobs/actions/retry	workspace:appcenter:retryJobs	-
POST /v1/{project_id}/app-center/app-rules	workspace:appcenter:createAppRule	-
GET /v1/{project_id}/app-center/app-rules	workspace:appcenter:listAppRule	-
PATCH /v1/{project_id}/app-center/app-rules/{rule_id}	workspace:appcenter:updateAppRule	-
DELETE /v1/{project_id}/app-center/app-rules/{rule_id}	workspace:appcenter:deleteAppRule	-
POST /v1/{project_id}/app-center/app-rules/batch-delete	workspace:appcenter:batchDeleteAppRules	-
POST /v1/{project_id}/app-center/app-rules/actions/enable-rule-restriction	workspace:appcenter:enableRuleRestriction	-
POST /v1/{project_id}/app-center/app-rules/actions/disable-rule-restriction	workspace:appcenter:disableRuleRestriction	-
POST /v1/{project_id}/app-center/app-restricted-rules	workspace:appcenter:addRestrictedRule	-
GET /v1/{project_id}/app-center/app-restricted-rules	workspace:appcenter:listRestrictedRule	-
POST /v1/{project_id}/app-center/app-restricted-rules/actions/batch-delete	workspace:appcenter:deleteRestrictedRule	-
PATCH /v1/{project_id}/app-center/profiles	workspace:appcenter:updateTenantProfile	-
GET /v1/{project_id}/app-center/profiles	workspace:appcenter:listTenantProfiles	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/scripts	workspace:scripts:create	-
GET /v2/{project_id}/scripts	workspace:scripts:list	-
GET /v2/{project_id}/scripts/{script_id}	workspace:scripts:get	-
PUT /v2/{project_id}/scripts/{script_id}	workspace:scripts:put	-
DELETE /v2/{project_id}/scripts/{script_id}	workspace:scripts:delete	-
POST /v2/{project_id}/script-executions	workspace:scripts:execute	-
GET /v2/{project_id}/script-execution-records/{record_id}	workspace:scripts:getRecordDetail	-
GET /v2/{project_id}/script-execution-records	workspace:scripts:listRecords	-
GET /v2/{project_id}/script-execution-tasks	workspace:scripts:listTasks	-
POST /v2/{project_id}/script-executions/retry	workspace:scripts:retry	-
POST /v2/{project_id}/script-executions/stop	workspace:scripts:stop	-
POST /v2/{project_id}/script-execution-records/{record_id}/download	workspace:scripts:download	-
GET /v2/{project_id}/share-space/configuration	workspace:tenants:getShareSpaceConfig	-
PUT /v2/{project_id}/share-space/configuration	workspace:tenants:updateShareSpaceConfig	-
GET /v2/{project_id}/auth-config/status	workspace:authConfigs:getStatus	-
POST /v2/{project_id}/privacystatement	workspace:privacystatements:sign	-

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/quotas/detail	workspace:quotas:get	-
GET /v2/{project_id}/sites	workspace:sites:get	-
POST /v2/{project_id}/sites	workspace:sites:add	• eip:bandwidths:create • eip:publicIps:create • elb:healthmonitors:create • elb:healthmonitors:show • elb:listeners:create • elb:listeners:update • elb:listeners:show • elb:listeners:list • elb:loadbalancers:create • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:list • elb:members:update • elb:pools:create • elb:pools:update • elb:pools:show • vpc:ports:create • vpc:ports:delete • vpc:securityGroupRules:create • vpc:securityGroupRules:delete • vpc:securityGroupRules:get • vpc:securityGroups:create • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:get

API	对应的操作项	依赖的操作项
DELETE /v2/{project_id}/sites/{site_id}	workspace:sites:delete	• elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:delete • elb:listeners:show • elb:loadbalancers:delete • elb:loadbalancers:show • elb:members:delete • elb:members:list • elb:pools:delete • elb:pools:show • vpc:ports:delete • vpc:securityGroups:delete • vpcep:endpoints:delete • vpcep:endpoints:get • eip:publicIps:disassociateInstance • eip:bandwidths:delete • eip:publicIps:delete

API	对应的操作项	依赖的操作项
PUT /v2/{project_id}/sites/{site_id}/access-mode	workspace:sites:updateAccessMode	• eip:bandwidths:create • eip:bandwidths:delete • eip:publicIps:create • eip:publicIps:delete • eip:publicIps:disassociateInstance • elb:healthmonitors:create • elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:create • elb:listeners:delete • elb:listeners:update • elb:listeners:show • elb:loadbalancers:create • elb:loadbalancers:delete • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:delete • elb:members:list • elb:members:update • elb:pools:create • elb:pools:delete • elb:pools:update • elb:pools:show • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:delete • vpcep:endpoints:get
PUT /v2/{project_id}/sites/{site_id}/subnet-ids	workspace:sites:updateSubnets	• vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get
GET /v2/{project_id}/tenants/lock-status	workspace:tenants:getLockStatus	-

API	对应的操作项	依赖的操作项
PUT /v2/{project_id}/tenants/lock-status	workspace:tenants:unlock	-
POST /v2/{project_id}/workspaces/enterprise-ids/check	workspace:tenants:checkEnterpriseIds	-
PUT /v2/{project_id}/workspaces/enterprise-id	workspace:tenants:updateEnterpriseId	-
POST /v2/{project_id}/bandwidths	workspace:bandwidth:create	-
GET /v2/{project_id}/bandwidths	workspace:bandwidth:list	-
POST /v2/{project_id}/bandwidths/{bandwidth_id}/update	workspace:bandwidth:update	-
DELETE /v2/{project_id}/bandwidths/{bandwidth_id}	workspace:bandwidth:delete	-
GET /v2/{project_id}/bandwidths/{bandwidth_id}/control-list	workspace:bandwidth:getControlConfig	-
PUT /v2/{project_id}/bandwidths/{bandwidth_id}/control-list	workspace:bandwidth:updateControlConfig	-
POST /v2/{project_id}/bandwidths/{bandwidth_id}/periodic/change/order	workspace:bandwidth:createChangeOrder	-
POST /v2/{project_id}/adns	workspace:bandwidth:create	-
GET /v2/{project_id}/adns	workspace:bandwidth:list	-
POST /v2/{project_id}/desktops-adn/batch-delete	workspace:bandwidth:delete	-
POST /v2/{project_id}/snapshots/batch-create	workspace:desktops:batchCreateSnapshots	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/snapshots/batch-delete	workspace:desktops:batchDeleteSnapshots	-
POST /v2/{project_id}/snapshots/batch-restore	workspace:desktops:batchRestoreSnapshots	-
GET /v2/{project_id}/snapshots	workspace:desktops:listSnapshots	-
POST /v2/{project_id}/verification/desktop-name	workspace:desktops:verifyDesktopName	-
GET /v2/{project_id}/subnets/{subnet_id}/available-ip	workspace:networks:getAvailableIp	-
GET /v2/{project_id}/ad/status	workspace:desktops:getAdStatus	-
GET /v2/{project_id}/ip-exist	workspace:networks:checkIpIfExist	-
POST /v2/{project_id}/desktops/check-images	workspace:images:checkIfExist	ims:images:list
GET /v2/{project_id}/hosts/{host_id}/servers	workspace:wdh:listDesktops	-
PUT /v2/{project_id}/hosts	workspace:wdh:update	-
GET /v2/{project_id}/terminals/binding-desktops/template	workspace:bindingPolicies:getTemplate	-
POST /v2/{project_id}/terminals/binding-desktops/template/import	workspace:bindingPolicies:import	-
GET /v2/{project_id}/terminals/binding-desktops/template/export	workspace:bindingPolicies:export	-
GET /v2/{project_id}/desktops/statistics/run-state	workspace:statistics:getRunState	-
GET /v2/{project_id}/desktops/statistics/login-state	workspace:statistics:getLoginState	-

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/subnets/using-subnets	workspace:networks:getUsingSubnets	-
GET /v2/{project_id}/ports	workspace:networks:listPorts	-
GET /v2/{project_id}/render-desktops/{desktop_id}/remote-consoles	workspace:renderDesktops:createConsole	-
PUT /v2/{project_id}/render-desktops/resize	workspace:renderDesktops:resize	-
POST /v2/{project_id}/exclusive-hosts/{host_id}/resize-lites	workspace:exclusiveHosts:resizeLites	-
GET /services/v2/{project_id}/desktops/{desktop_id}	workspace:desktops:get	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktop-monitor/{desktop_id}	workspace:desktops:getMonitor	ces:metricData:get
GET /v2/{project_id}/desktops/export	workspace:desktops:export	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktops/{desktop_id}/detach-info	workspace:desktops:listDetachInfo	-
GET /v2/{project_id}/desktops/{desktop_id}/sysprep	workspace:desktops:getSysprepVersion	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/internet	workspace:networks:createNat	• vpc:ports:delete • vpc:ports:get • vpc:networks:get • eip:publicIps:create • eip:publicIps:update • eip:publicIps:delete • nat:snatRules:list • nat:snatRules:create • nat:natGateways:list • nat:natGateways:create
GET /v2/{project_id}/internet	workspace:networks:listNats	• vpc:subnets:get • vpc:vpcs:get • nat:snatRules:list • nat:natGateways:list
POST /v2/{project_id}/quotas/check	workspace:quotas:check	-
GET /v2/{project_id}/subnets	workspace:networks:listSubnets	• vpc:subnets:list • vpc:subnets:get
GET /v2/{project_id}/vpcs	workspace:networks:listVpcs	vpc:vpcs:list
POST /v2/{project_id}/policy-groups/policy-template	workspace:policyGroups:createTemplate	-
GET /v1/{project_id}/policy-templates	workspace:policyGroups:listTemplate	-
PUT /v2/{project_id}/policy-groups/policy-template/{policy_group_id}	workspace:policyGroups:updateTemplate	-
GET /v2/{project_id}/security-groups	workspace:networks:listSecurityGroups	-
GET /v2/{project_id}/availability-zones/summary	workspace:availabilityZones:getSummary	-
GET /v2/{project_id}/availability-zones/detail	workspace:availabilityZones:get	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/users/desktop-users/action/import	workspace:users:importUser	-
POST /v2/{project_id}/users/template-upload	workspace:users:uploadTemplate	-
PUT /v2/{project_id}/access-policy/{access_policy_id}	workspace:accessPolicies:update	-
POST /v2/{project_id}/desktops/{desktop_id}/verify-source	workspace:desktops:verifySource	-
GET /v2/{project_id}/desktops/networks	workspace:desktops:listDesktopNetworks	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:securityGroups:get • eip:publicIps:list
POST /v2/{project_id}/desktops/networks/batch-change	workspace:desktops:batchChangeNetwork	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:securityGroups:get • eip:publicIps:list • eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
GET /v2/{project_id}/workspace-jobs/{job_id}	workspace:jobs:get	-
POST /v2/{project_id}/ip/import	workspace:accessPolicies:importIp	-
GET /v2/{project_id}/ip/template/download	workspace:accessPolicies:getIpImportTemplate	-

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/wks-edge-sites	workspace:sites:listEdgeSites	• ies:edgeSite:list • ies:edgeSite:getMetricData
POST /v2/{project_id}/check-edge-site-resources	workspace:sites:checkEdgeSiteResources	• ies:edgeSite:list • ies:edgeSite:getMetricData
GET /v2/{project_id}/ad-ous	workspace:ou:listAdOus	-
GET /v2/{project_id}/ou-users	workspace:ou:listOuUsers	-
POST /v2/{project_id}/ou-users/import	workspace:ou:importUsersByOU	-
GET /v1/{project_id}/app-groups	workspace:appGroup:list	-
POST /v1/{project_id}/app-groups	workspace:appGroup:create	-
DELETE /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:delete	-
GET /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:get	-
PATCH /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:update	-
GET /v1/{project_id}/app-groups/{app_group_id}/apps	workspace:app:listPublishedApp	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps	workspace:app:publish	-
GET /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}	workspace:app:get	-
PATCH /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}	workspace:app:update	-

API	对应的操作项	依赖的操作项
DELETE /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}/icon	workspace:app:deleteIcon	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}/icon	workspace:app:uploadIcon	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/check	workspace:app:check	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/disable	workspace:app:batchDisable	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/enable	workspace:app:batchEnable	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/batch-unpublish	workspace:app:unpublish	-
GET /v1/{project_id}/app-groups/{app_group_id}/publishable-app	workspace:appGroup:listPublishableApp	-
POST /v1/{project_id}/app-groups/actions/batch-delete-authorization	workspace:appGroup:batchDeleteAuthorization	-
POST /v1/{project_id}/app-groups/actions/disassociate-app-group	workspace:appGroup:disassociate	-
GET /v1/{project_id}/app-groups/actions/list-authorizations	workspace:appGroup:listAuthorization	-
POST /v1/{project_id}/app-groups/authorizations	workspace:appGroup:addAuthorization	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/app-groups/batch-delete	workspace:appGroup:batchDelete	-
POST /v1/{project_id}/app-groups/rules/validate	workspace:appGroup:check	-
GET /v1/{project_id}/app-server-groups	workspace:serverGroup:list	-
POST /v1/{project_id}/app-server-groups	workspace:serverGroup:create	• ims:images:list • vpc:ports:get • vpc:subnets:get
DELETE /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:delete	-
GET /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:get	-
PATCH /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:update	ims:images:list
GET /v1/{project_id}/app-server-groups/{server_group_id}/state	workspace:serverGroup:getServerState	-
GET /v1/{project_id}/app-server-groups/actions/list	workspace:serverGroup:listDetail	-
GET /v1/{project_id}/app-server-groups/resources/restrict	workspace:serverGroup:getRestrict	-
POST /v1/{project_id}/app-server-groups/rules/validate	workspace:serverGroup:validate	-
POST /v1/{project_id}/server-group/{server_group_id}/tags/create	workspace:serverGroup:tagResource	-

API	对应的操作项	依赖的操作项
DELETE /v1/{project_id}/server-group/{server_group_id}/tags/delete	workspace:serverGroup:unTagResource	-
GET /v1/{project_id}/server-group/{server_group_id}/tags	workspace:serverGroup:listTagsForResource	-
GET /v1/{project_id}/server-group/tags	workspace:serverGroup:listTags	-
POST /v1/{project_id}/server-group/tags/batch-create	workspace:serverGroup:batchCreateTags	-
DELETE /v1/{project_id}/server-group/tags/batch-delete	workspace:serverGroup:batchDeleteTags	-
GET /v1/{project_id}/app-servers	workspace:server:list	-
DELETE /v1/{project_id}/app-servers/{server_id}	workspace:server:delete	• iam:roles:listRoles • vpc:ports:delete • vpc:ports:get
GET /v1/{project_id}/app-servers/{server_id}	workspace:server:get	-
PATCH /v1/{project_id}/app-servers/{server_id}	workspace:server:update	-
POST /v1/{project_id}/app-servers/{server_id}/actions/change-image	workspace:server:changeImage	• ims:images:list • vpc:ports:get • vpc:subnets:get
POST /v1/{project_id}/app-servers/{server_id}/actions/reinstall	workspace:server:reinstall	• ims:images:list • vpc:ports:get • vpc:subnets:get
GET /v1/{project_id}/app-servers/{server_id}/actions/vnc	workspace:server:getVncUrl	-
GET /v1/{project_id}/app-servers/access-agent/latest-version	workspace:accessAgent:list	-

API	对应的操作项	依赖的操作项
PATCH /v1/{project_id}/app-servers/access-agent/actions/upgrade	workspace:accessAgent:batchUpgrade	-
GET /v1/{project_id}/app-servers/access-agent/latest-version	workspace:accessAgent:listLatestVersion	-
GET /v1/{project_id}/app-servers/access-agent/list	workspace:server:listAccessAgentDetails	-
GET /v1/{project_id}/app-servers/access-agent/upgrade-flag	workspace:accessAgent:getUpgradeFlag	-
PATCH /v1/{project_id}/app-servers/access-agent/upgrade-flag	workspace:accessAgent:updateUpgradeFlag	-
GET /v1/{project_id}/app-servers/access-agent/upgrade-record	workspace:accessAgent:listUpgradeRecords	-
POST /v1/{project_id}/app-servers/actions/batch-delete	workspace:server:batchDelete	• iam:roles:listRoles • vpc:ports:delete • vpc:ports:get
PATCH /v1/{project_id}/app-servers/actions/batch-maint	workspace:server:batchChangeMaintainMode	-
PATCH /v1/{project_id}/app-servers/actions/batch-reboot	workspace:server:batchReboot	-
PATCH /v1/{project_id}/app-servers/actions/batch-rejoin-domain	workspace:server:batchRejoinDomain	-
PATCH /v1/{project_id}/app-servers/actions/batch-start	workspace:server:batchStart	-
PATCH /v1/{project_id}/app-servers/actions/batch-stop	workspace:server:batchStop	-
PATCH /v1/{project_id}/app-servers/actions/batch-update-tsvi	workspace:server:batchUpdateTsvi	• vpc:subnets:get • vpc:ports:update

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/app-servers/actions/create	workspace:server:create	• ims:images:list • ims:images:updateMemberStatus • ims:images:share • ims:images:get • vpc:securityGroups:get • vpc:securityGroupRules:get • vpc:networks:get • vpc:subnets:get • vpc:ports:create • vpc:ports:get • vpc:ports:delete • vpc:vpcs:get • dss:pools:list
PATCH /v1/{project_id}/app-servers/hosts/batch-migrate	workspace:server:batchMigrateHosts	-
GET /v1/{project_id}/app-servers/metric-data/{server_id}	workspace:server:getMetricData	-
GET /v1/{project_id}/app-server-sub-jobs	workspace:jobs:listSubJobs	-
POST /v1/{project_id}/app-server-sub-jobs/actions/batch-delete	workspace:jobs:batchDeleteSubJobs	-
GET /v1/{project_id}/app-server-sub-jobs/actions/count	workspace:jobs:countSubJobs	-
POST /v1/{project_id}/app-warehouse/action/authorize	workspace:appWarehouse:authorizeObs	• obs:bucket:GetBucketAcl • obs:object:PutObject • obs:object:DeleteObject
POST /v1/{project_id}/app-warehouse/actions/batch-delete	workspace:appWarehouse:batchDeleteApp	• obs:bucket:HeadBucket • obs:object:DeleteObject
GET /v1/{project_id}/app-warehouse/apps	workspace:appWarehouse:ListWarehouseApps	-
POST /v1/{project_id}/app-warehouse/apps	workspace:appWarehouse:createApp	-

API	对应的操作项	依赖的操作项
DELETE /v1/{project_id}/app-warehouse/apps/{id}	workspace:appWarehouse:deleteApp	• obs:bucket:HeadBucket • obs:object:DeleteObject
POST /v1/{project_id}/app-warehouse/apps/icon	workspace:appWarehouse:uploadAppIcon	obs:object:PutObject
POST /v1/{project_id}/app-warehouse/bucket-and-acl/create	workspace:appWarehouse:createBucketOrAcl	• obs:bucket:GetBucketAcl • obs:bucket:HeadBucket • obs:bucket:PutBucketAcl • obs:bucket:PutReplicationConfiguration • obs:bucket:CreateBucket • obs:bucket:PutBucketCORS
GET /v1/{project_id}/check/quota	workspace:quotas:get	-
GET /v1/{project_id}/image-server-jobs	workspace:images:listImageJobs	-
GET /v1/{project_id}/image-server-jobs/{job_id}	workspace:images:getImageJob	-
GET /v1/{project_id}/image-servers	workspace:imageServer:list	-
POST /v1/{project_id}/image-servers	workspace:imageServer:create	• ims:images:list • vpc:ports:get • vpc:subnets:get
GET /v1/{project_id}/image-servers/{server_id}	workspace:imageServer:get	-
PATCH /v1/{project_id}/image-servers/{server_id}	workspace:imageServer:update	-
POST /v1/{project_id}/image-servers/{server_id}/actions/attach-app	workspace:imageServer:attachApp	-
GET /v1/{project_id}/image-servers/{server_id}/actions/latest-attached-app	workspace:imageServer:listLatestAttachedApp	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/image-servers/{server_id}/actions/recreate-image	workspace:imageServer:recreate	• vpc:ports:get • vpc:subnets:get • ims:quotas:get • ims:images:get • ims:images:list • ims:images:setTags • ims:images:setOrDeleteTags • ims:images:updateMemberStatus • ims:images:copyInRegion • ims:serverImages:create
PATCH /v1/{project_id}/image-servers/actions/batch-delete	workspace:imageServer:batchDelete	-
GET /v1/{project_id}/image-server-sub-jobs	workspace:imageServer:listImageSubJobs	-
PATCH /v1/{project_id}/image-server-sub-jobs/actions/batch-delete	workspace:imageServer:batchDeleteImageSubJobs	-
GET /v1/{project_id}/image-server-sub-jobs/actions/count	workspace:imageServer:countImageSubJobs	-
GET /v2/{project_id}/job/{job_id}	workspace:jobs:get	-
GET /v1/{project_id}/mails	workspace:appGroup:listMailRecord	-
POST /v1/{project_id}/mails/actions/send	workspace:appGroup:resendMail	-
POST /v1/{project_id}/mails/actions/send-by-authorization	workspace:appGroup:resendMail	-
GET /v1/{project_id}/persistent-storages	workspace:storage:listPersistentStorage	-
POST /v1/{project_id}/persistent-storages	workspace:storage:createPersistentStorage	• obs:bucket:HeadBucket • obs:bucket:PutBucketPolicy • obs:bucket:PutBucketAcl • obs:bucket:PutBucketCORS

API	对应的操作项	依赖的操作项
DELETE /v1/{project_id}/persistent-storages/{storage_id}	workspace:storage:deletePersistentStorage	• obs:object:GetObject • obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/assign-folder	workspace:storage:updateUserFolderAssignment	-
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/assign-share-folder	workspace:storage:updateShareFolderAssignment	-
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/create-share-folder	workspace:storage:createShareFolder	• obs:object:GetObject • obs:object:PutObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/delete-storage-claim	workspace:storage:deleteStorageClaim	obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/delete-user-attachment	workspace:storage:deleteUserStorageAttachment	obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/actions/batch-delete	workspace:storage:batchDeletePersistentStorage	-
GET /v1/{project_id}/persistent-storages/actions/list-attachments	workspace:storage:listStorageAssignment	-
GET /v1/{project_id}/persistent-storages/actions/list-share-folders	workspace:storage:listShareFolder	-
GET /v1/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:get	-
GET /v1/{project_id}/policy-groups/{policy_group_id}/policy	workspace:policyGroups:listPolicies	-
GET /v1/{project_id}/policy-groups/{policy_group_id}/target	workspace:policyGroups:listTargets	-

API	对应的操作项	依赖的操作项
GET /v1/{project_id}/policy-groups/show/detail	workspace:policyGroups:listDetail	-
GET /v1/{project_id}/policy-templates	workspace:policyGroups:listTemplate	-
DELETE /v1/{project_id}/policy-templates/{policy_template_id}	workspace:policyGroups:deleteTemplate	-
PATCH /v1/{project_id}/policy-templates/{policy_template_id}	workspace:policyGroups:updateTemplate	-
GET /v1/{project_id}/privacy-statement	workspace:privacystatements:get	-
DELETE /v1/{project_id}/scaling-policy	workspace:scalingPolicy:delete	-
GET /v1/{project_id}/scaling-policy	workspace:scalingPolicy:list	-
PUT /v1/{project_id}/scaling-policy	workspace:scalingPolicy:create	-
GET /v1/{project_id}/schedule-task/{task_id}/execute-history	workspace:scheduledTasks:list	-
POST /v1/{project_id}/schedule-task	workspace:scheduledTasks:create	-
GET /v1/{project_id}/schedule-task/{execute_history_id}/execute-detail	workspace:scheduledTasks:getRecord	-
DELETE /v1/{project_id}/schedule-task/{task_id}	workspace:scheduledTasks:delete	-
POST /v1/{project_id}/schedule-task/future-executions	workspace:scheduledTasks:get	-
PATCH /v1/{project_id}/schedule-task/{task_id}	workspace:scheduledTasks:update	-
GET /v1/{project_id}/schedule-task/{task_id}/execute-history	workspace:scheduledTasks:listRecords	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/schedule-task/actions/batch-delete	workspace:scheduledTasks:batchDelete	-
POST /v1/{project_id}/session/app-connection	workspace:session:listAppConnection	-
POST /v1/{project_id}/session/logoff	workspace:session:logoffUserSession	-
POST /v1/{project_id}/session/user-connection	workspace:session:listUserConnection	-
GET /v1/{project_id}/session/user-session-info	workspace:session:listSessionByUserName	-
PUT /v1/{project_id}/storages-policy/actions/create-statements	workspace:storagePolicy:create	-
GET /v1/{project_id}/storages-policy/actions/list-statements	workspace:storagePolicy:list	-
GET /v1/{project_id}/users	workspace:users:list	-
GET /v1/persistent-storages/actions/list-sfs-storages	workspace:storage:listSfs3Storage	• obs:bucket:ListBucket • obs:bucket:GetBucketStorage • obs:bucket:ListAllMyBuckets
GET /v1/{project_id}/product	workspace:baseResource:list	ecs:availabilityZones:list
POST /v1/{project_id}/bundles/batch-query-config-info	workspace:tenants:listConfigInfo	-
GET /v1/{project_id}/product	workspace:baseResource:list	-
GET /v1/{project_id}/volume-type	workspace:baseResource:list	-
POST /v1/{project_id}/tenant/action/active	workspace:tenants:active	-
GET /v1/{project_id}/tenant/profile	workspace:tenants:listTenantProfile	-

API	对应的操作项	依赖的操作项
GET /v1/{project_id}/volume-type	workspace:baseResource:list	-
GET /v1/{project_id}/app-servers/server-metric-data/{server_id}	workspace:server:listServerMetricData	-
GET /v1/{project_id}/session/list-sessions	workspace:session:listSessions	-
PATCH /v1/{project_id}/app-warehouse/apps/{id}	workspace:appWarehouse:updateApp	-
POST /v1/{project_id}/app-servers/actions/batch-change-image	workspace:server:batchChangeImage	• ims:images:list • vpc:ports:get • vpc:subnets:get
POST /v1/{project_id}/app-servers/actions/batch-reinstall	workspace:server:batchReinstall	• ims:images:list • vpc:ports:get • vpc:subnets:get
GET /v2/{project_id}/auth-config/method-config	workspace:authConfigs:get	-
PUT /v2/{project_id}/auth-config/method-config	workspace:authConfigs:update	-
GET /v2/{project_id}/assist-auth-config/method-config	workspace:assistAuthConfigs:get	-
PUT /v2/{project_id}/assist-auth-config/method-config	workspace:assistAuthConfigs:update	-
POST /v2/{project_id}/workspace-jobs/{job_id}/actions	workspace:jobs:retry	-
GET /v2/{project_id}/quotas	workspace:quotas:get	-
GET /v2/{project_id}/tenants/roles	workspace:tenants:getRoles	-
GET /v2/{project_id}/tenant-configs	workspace:tenants:ListConfig	-
PUT /v2/{project_id}/tenant-configs	workspace:tenants:updateConfig	-

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/nat-mapping-configs	workspace:natMappings:getConfig	-
PUT /v2/{project_id}/nat-mapping-configs	workspace:natMappings:updateConfig	-
GET /v2/{project_id}/workspaces	workspace:tenants:get	• vpc:vpcs:get • vpc:subnets:get • vpc:securityGroups:get
POST /v2/{project_id}/workspaces	workspace:tenants:open	• eip:bandwidths:create • eip:publicIps:create • elb:healthmonitors:create • elb:healthmonitors:show • elb:listeners:create • elb:listeners:update • elb:listeners:show • elb:listeners:list • elb:loadbalancers:create • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:list • elb:members:update • elb:pools:create • elb:pools:update • elb:pools:show • vpc:ports:create • vpc:ports:delete • vpc:securityGroupRules:create • vpc:securityGroupRules:delete • vpc:securityGroupRules:get • vpc:securityGroups:create • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:get

API	对应的操作项	依赖的操作项
DELETE /v2/{project_id}/workspaces	workspace:tenants:delete	• elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:delete • elb:listeners:show • elb:loadbalancers:delete • elb:loadbalancers:show • elb:members:delete • elb:members:list • elb:pools:delete • elb:pools:show • vpc:ports:delete • vpc:securityGroups:delete • vpcep:endpoints:delete • vpcep:endpoints:get • eip:publicIps:disassociateInstance • eip:bandwidths:delete • eip:publicIps:delete

API	对应的操作项	依赖的操作项
PUT /v2/{project_id}/workspaces	workspace:tenants:update	• eip:bandwidths:create • eip:bandwidths:delete • eip:publicIps:create • eip:publicIps:delete • eip:publicIps:disassociateInstance • elb:healthmonitors:create • elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:create • elb:listeners:delete • elb:listeners:update • elb:listeners:show • elb:loadbalancers:create • elb:loadbalancers:delete • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:delete • elb:members:list • elb:members:update • elb:pools:create • elb:pools:delete • elb:pools:update • elb:pools:show • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:delete • vpcep:endpoints:get
GET /v2/{project_id}/workspaces/lock-status	workspace:tenants:getLockStatus	-
PUT /v2/{project_id}/workspaces/lock-status	workspace:tenants:unlock	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/agencies	workspace:agencies:create	• iam:agencies:listV5 • iam:agencies:getV5 • iam:agencies:createServiceLinkedAgencyV5 • iam:roles:getRole • iam:roles:listRoles • iam:agencies:getAgency • iam:agencies:listAgencies • iam:agencies:createAgency • iam:permissions:listRolesForAgencyOnProject • iam:permissions:grantRoleToAgencyOnProject
GET /v2/{project_id}/agencies	workspace:agencies:get	• iam:agencies:listV5 • iam:agencies:getV5 • iam:agencies:getAgency • iam:agencies:listAgencies • iam:permissions:listRolesForAgencyOnProject
POST /v3/{project_id}/desktops/{desktop_id}/ai-accelerate-job	workspace:desktops:commitAiAccelerateJob	-
POST /v2/{project_id}/desktops/{desktop_id}/ai-accelerate-job	workspace:desktops:createAiAccelerateJob	-
GET /v2/{project_id}/ai-accelerate-job/{job_id}	workspace:desktops:getAiAccelerateJob	-
POST /v2/{project_id}/sysprep	workspace:desktops:getSysPrepInfo	-
POST /v2/{project_id}/verification/batch-change-image	workspace:desktops:checkBatchChangeImage	ims:images:list
GET /v2/{project_id}/desktop-name-policies	workspace:tenants:listDesktopNamePolicies	-
POST /v2/{project_id}/desktop-name-policies	workspace:tenants:createDesktopNamePolicy	-

API	对应的操作项	依赖的操作项
PUT /v2/{project_id}/desktop-name-policies/{policy_id}	workspace:tenants:updateDesktopNamePolicy	-
POST /v2/{project_id}/desktop-name-policies/batch-delete	workspace:tenants:batchDeleteDesktopNamePolicies	-
POST /v2/{project_id}/desktop-pools	workspace:desktopPools:create	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
GET /v2/{project_id}/desktop-pools	workspace:desktopPools:list	ims:images:list
PUT /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:update	-
DELETE /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:delete	-
GET /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:get	ims:images:list

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktop-pools/{pool_id}/expand	workspace:desktopPools:expand	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
POST /v2/{project_id}/desktop-pools/{pool_id}/resize	workspace:desktopPools:resize	• vpc:subnets:get • ims:images:list
POST /v2/{project_id}/desktop-pools/{pool_id}/rebuild	workspace:desktopPools:rebuild	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-add	workspace:desktopPools:batchAddVolumes	-
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-delete	workspace:desktopPools:batchDeleteVolumes	-
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-expand	workspace:desktopPools:batchExpandVolumes	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktop-pools/{pool_id}/action	workspace:desktopPools:operate	-
GET /v2/{project_id}/desktop-pools/{pool_id}/users	workspace:desktopPools:listUsers	-
POST /v2/{project_id}/desktop-pools/{pool_id}/users	workspace:desktopPools:authorizeUsers	ims:images:list
GET /v2/{project_id}/desktop-pools/{pool_id}/desktops	workspace:desktopPools:listDesktops	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktop-pools/script-execution-tasks/detail	workspace:desktopPools:listScriptTasks	-
POST /v2/{project_id}/desktop-pools/{pool_id}/script-executions	workspace:desktopPools:executeScripts	-
POST /v2/{project_id}/desktop-pools/{pool_id}/notifications	workspace:desktopPools:sendNotifications	-
GET /v3/{project_id}/desktops/export	workspace:desktops:export	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktops	workspace:desktops:create	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • eip:publicIps:get • eip:publicIps:list • eip:publicIps:create • eip:publicIps:associateInstance • eip:publicIps:delete • eip:publicIps:createTags • vpc:quotas:list • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
GET /v2/{project_id}/desktops	workspace:desktops:list	-
PUT /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:update	-
DELETE /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:delete	• vpc:ports:get • vpc:ports:delete
GET /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:get	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktops/batch-delete	workspace:desktops:batchDelete	• vpc:ports:get • vpc:ports:delete
POST /v2/{project_id}/desktops/logoff	workspace:desktops:logoff	-
GET /v2/{project_id}/desktops/detail	workspace:desktops:listDetail	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
POST /v2/{project_id}/desktops/action	workspace:desktops:operate	-
POST /v2/{project_id}/desktops/resize	workspace:desktops:resize	• vpc:subnets:get • ims:images:list
GET /v2/{project_id}/connections/status	workspace:desktops:getConnectStatus	-
GET /v2/{project_id}/desktops/status	workspace:desktops:ListStatus	-
POST /v2/{project_id}/desktops/rebuild	workspace:desktops:rebuild	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
GET /v2/{project_id}/desktops/{desktop_id}/actions	workspace:desktops:getActions	-
GET /v2/{project_id}/desktops/{desktop_id}/remote-consoles	workspace:desktops:createConsole	-
PUT /v2/{project_id}/desktops/sids	workspace:desktops:updateSids	-
POST /v2/{project_id}/desktops/{desktop_id}/rejoin-domain	workspace:desktops:rejoinDomain	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktops/desktop-to-image	workspace:desktops:createImage	• ims:quotas:get • ims:images:get • ims:images:list • ims:images:setTags • ims:images:setOrDeleteTags • ims:images:updateMemberStatus • ims:images:copyInRegion • ims:serverImages:create
POST /v2/{project_id}/desktops/batch-detach	workspace:desktops:batchDetach	vpc:ports:get
POST /v2/{project_id}/desktops/detach	workspace:desktops:detach	vpc:ports:get
POST /v2/{project_id}/desktops/attach	workspace:desktops:attach	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
GET /v2/{project_id}/desktops/{desktop_id}/networks	workspace:desktops:getNetwork	• vpc:vpcs:get • vpc:networks:get • vpc:subnets:get • vpc:ports:get • vpc:securityGroups:get • eip:publicIps:list

API	对应的操作项	依赖的操作项
PUT /v2/{project_id}/desktops/{desktop_id}/networks	workspace:desktops:changeNetwork	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:securityGroups:get • eip:publicIps:list • eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
GET /v2/{project_id}/exclusive-hosts/{host_id}/desktops	workspace:exclusiveHosts:listDesktops	-
GET /v2/{project_id}/all-desktops	workspace:desktops:listAll	-
GET /v2/{project_id}/desktop-associate/discover-vm/infos	workspace:desktopAssociate:listDiscoverVmInfo	-
POST /v2/{project_id}/desktop-associate/tasks	workspace:desktopAssociate:startTask	-
POST /v2/{project_id}/desktop-associate/discover-vm/switch	workspace:desktopAssociate:switchScanTask	-
GET /v2/{project_id}/desktop-associate/discover-vm/switch	workspace:desktopAssociate:getScanTaskSwitch	-
PUT /v2/{project_id}/desktops/maintenance-mode	workspace:desktops:setMaintenanceMode	-
POST /v2/{project_id}/desktops/pre-batch-attach	workspace:desktops:prepAttachUsers	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktops/batch-attach	workspace:desktops:batchAttachUsers	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
PUT /v2/{project_id}/desktops/change-username	workspace:desktops:changeUsername	-
POST /v2/{project_id}/desktops/notifications	workspace:desktops:sendNotifications	-
POST /v2/{project_id}/desktops/{desktop_id}/migrate	workspace:desktops:migrate	• vpc:networks:get • vpc:subnets:get • vpc:ports:create • vpc:ports:delete • vpc:ports:update • vpc:ports:get
GET /v2/{project_id}/desktops/agents	workspace:desktops:listAgents	-
POST /v2/{project_id}/desktops/agents	workspace:desktops:batchInstallAgents	-
GET /v2/{project_id}/desktops/{desktop_id}/tags	workspace:desktops:listTags	-
POST /v2/{project_id}/desktops/{desktop_id}/tags	workspace:desktops:tag	-
DELETE /v2/{project_id}/desktops/{desktop_id}/tags/{key}	workspace:desktops:untag	-
GET /v2/{project_id}/desktops/tags	workspace:desktops:listProjectTags	-
POST /v2/{project_id}/desktops/{desktop_id}/tags/action	workspace:desktops:operateTags	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktops/resource_instances/action	workspace:desktops:listByTags	-
POST /v2/{project_id}/desktops/batch-tags	workspace:desktops:tag	-
DELETE /v2/{project_id}/desktops/batch-tags	workspace:desktops:untag	-
POST /v2/{project_id}/exclusive-hosts	workspace:exclusiveHosts:create	• vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:subnets:get • vpc:vpcs:get
GET /v2/{project_id}/exclusive-hosts	workspace:exclusiveHosts:list	-
POST /v2/{project_id}/exclusive-hosts/check-limits	workspace:exclusiveHosts:check	-
GET /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:get	• nat:snatRules:list • eip:publicIps:list
PUT /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:update	-
DELETE /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:delete	-
GET /v2/{project_id}/market-images	workspace:mkp:listImages	ims:images:list
GET /v2/{project_id}/mkp/commodities/commodity-ids	workspace:mkp:listCommodityInfos	-
POST /v2/{project_id}/mkp/order	workspace:mkp:createOrder	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/mkp/product-reserve	workspace:mkp:listListProductReserve	-
GET /v2/{project_id}/mkp/commodities	workspace:mkp:listCommodityDetails	-
GET /v2/{project_id}/mkp/commodities/{commodity_id}/relation-commodities	workspace:mkp:listRelationCommodityDetails	-
GET /v2/{project_id}/mkp/commodities/agreements	workspace:mkp:listCommodityAgreements	-
GET /v2/{project_id}/eips	workspace:networks:listEips	• eip:publicIps:list • eip:bandwidths:list
POST /v2/{project_id}/eips	workspace:networks:createEips	• vpc:quotas:list • eip:publicIps:create • eip:publicIps:associateInstance
POST /v2/{project_id}/eips/binding	workspace:networks:bindEips	• eip:publicIps:associateInstance • eip:publicIps:get
POST /v2/{project_id}/eips/unbinding	workspace:networks:unbindEips	• eip:publicIps:list • eip:publicIps:disassociateInstance
GET /v2/{project_id}/eips/quotas	workspace:networks:getEipQuota	vpc:quotas:list
GET /v2/{project_id}/nat-gateways	workspace:networks:ListNatGateways	• vpc:subnets:get • vpc:vpcs:get • nat:snatRules:list • nat:natGateways:list

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/periodic/subscribe/order	workspace:orders:create	• ims:images:list • vpc:vpcs:get • vpc:networks:get • vpc:subnets:get • vpc:ports:get • bss:order:update
POST /v2/{project_id}/periodic/{desktop_id}/change/order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/periodic/change/batch-order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/periodic/inquiry/change-image	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/change/order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/desktop-pool/periodic/inquiry/add-volume	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/change-image	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/extend-volume	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/resize	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/periodic/inquiry/add-resources	workspace:orders:batchInquiry	ims:images:list
GET /v2/{project_id}/checkOrderLimits	workspace:quotas:check	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/render-desktops	workspace:renderDesktops:create	• ims:images:list • ims:images:share • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get
DELETE /v2/{project_id}/render-desktops	workspace:renderDesktops:delete	• vpc:ports:get • vpc:ports:delete
GET /v2/{project_id}/render-desktops	workspace:renderDesktops:list	-
POST /v2/{project_id}/render-desktops/action	workspace:renderDesktops:action	-
GET /v2/{project_id}/scheduled-tasks	workspace:scheduledTasks:list	-
POST /v2/{project_id}/scheduled-tasks	workspace:scheduledTasks:create	-
GET /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:get	-
PUT /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:update	-
DELETE /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:delete	-
POST /v2/{project_id}/scheduled-tasks/future-executions	workspace:scheduledTasks:getFuture	-
POST /v2/{project_id}/scheduled-tasks/batch-delete	workspace:scheduledTasks:batchDelete	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records	workspace:scheduledTasks:listRecords	-

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/scheduled-tasks/{task_id}/records/{record_id}	workspace:scheduledTasks:getRecord	-
POST /v2/{project_id}/scheduled-tasks/{task_id}/records/export	workspace:scheduledTasks:exportRecords	-
POST /v2/{project_id}/user/share-resources	workspace:users:subscribeSharer	-
POST /v2/{project_id}/desktop/sub-resources	workspace:desktops:addSubResources	-
POST /v2/{project_id}/desktop/delete-sub-resources	workspace:desktops:deleteSubResources	-
POST /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:createSnapshots	-
GET /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:getSnapshots	-
DELETE /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:deleteSnapshots	-
POST /v2/{project_id}/desktops/{desktop_id}/snapshots/restore	workspace:desktops:restoreBySnapshot	-
GET /v2/{project_id}/statistics	workspace:statistics:listDesktopStatus	-
GET /v2/{project_id}/desktops/statistics/unused	workspace:statistics:getUnused	-
POST /v2/{project_id}/desktops/statistics/used	workspace:statistics:getUsed	-
GET /v3/{project_id}/terminals/binding-desktops/template/export	workspace:bindingPolicies:export	-
GET /v2/{project_id}/terminals/binding-desktops/config	workspace:bindingPolicies:getConfig	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/terminals/binding-desktops/config	workspace:bindingPolicies:createConfig	-
GET /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:get	-
POST /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:add	-
PUT /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:update	-
POST /v2/{project_id}/terminals/binding-desktops/batch-delete	workspace:bindingPolicies:delete	-
POST /v2/{project_id}/desktops/{desktop_id}/volumes/batch-delete	workspace:volumes:delete	-
POST /v2/{project_id}/volumes	workspace:volumes:batchAdd	-
POST /v2/{project_id}/volumes/expand	workspace:volumes:batchExpand	-
GET /v2/{project_id}/hosts/types	workspace:wdh:getType	-
GET /v2/{project_id}/hosts	workspace:wdh:get	-
GET /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:getRemoteAssistance	-
POST /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:createRemoteAssistance	-
DELETE /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:cancelRemoteAssistance	-
POST /v2/{project_id}/desktops/{desktop_id}/volumes	workspace:volumes:add	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/desktops/{desktop_id}/volumes/{volume_id}/expand	workspace:volumes:expand	-
GET /v2/{project_id}/dss-pools/detail	workspace:volumes:listDssPoolsDetail	dss:pools:list
GET /v2/{project_id}/common/timezones	workspace:common:listTimezones	-
GET /v3/{project_id}/desktops/connections/export	workspace:connections:securityExport	-
GET /v2/{project_id}/images	workspace:images:list	ims:images:list
POST /v2/{project_id}/policy-groups/import	workspace:policyGroups:import	-
POST /v2/{project_id}/access-policy	workspace:accessPolicies:create	-
GET /v2/{project_id}/access-policy	workspace:accessPolicies:get	-
DELETE /v2/{project_id}/access-policy	workspace:accessPolicies:delete	-
GET /v2/{project_id}/access-policy/{access_policy_id}/objects	workspace:accessPolicies:getTarget	-
PUT /v2/{project_id}/access-policy/{access_policy_id}/objects	workspace:accessPolicies:updateTarget	-
GET /v2/{project_id}/products	workspace:products:listDesktopProducts	ecs:cloudServerFlavors:get
GET /v2/{project_id}/products/sharer	workspace:products:listSharerProducts	-
GET /v2/{project_id}/products/adninternet	workspace:products:listInternetProducts	-
GET /v2/{project_id}/availability-zones	workspace:availabilityZones:list	-
GET /v2/{project_id}/groups/export	workspace:userGroups:export	-

API	对应的操作项	依赖的操作项
POST /v3/{project_id}/users/export	workspace:users:export	-
POST /v2/{project_id}/users/import	workspace:users:import	-
GET /v3/{project_id}/groups/{group_id}/users/export	workspace:userGroups:exportUsers	-
GET /v2/{project_id}/groups/{group_id}/users/export	workspace:userGroups:exportUsers	-
POST /v2/{project_id}/users/{user_id}/actions	workspace:users:operate	-
GET /v2/{project_id}/users/{user_id}/random-password	workspace:users:randomPassword	-
DELETE /v2/{project_id}/users/{user_id}/otp-devices	workspace:users:deleteOtps	-
POST /v2/{project_id}/users/{user_id}/resend-email	workspace:users:resendEmail	-
GET /v2/{project_id}/connections/desktops	workspace:connections:securityList	-
GET /v2/{project_id}/connections/desktops/export	workspace:connections:securityExport	-
GET /v2/{project_id}/connections/online-users	workspace:connections:listOnlineUsers	-
GET /v2/{project_id}/desktops/connections	workspace:connections:securityList	-
GET /v2/{project_id}/desktops/connections/export	workspace:connections:securityExport	-
GET /v2/{project_id}/desktops/online-users	workspace:connections:listOnlineUsers	-
GET /v2/{project_id}/groups	workspace:userGroups:list	-
POST /v2/{project_id}/groups	workspace:userGroups:create	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/groups/batch-delete	workspace:userGroups:batchDelete	-
DELETE /v2/{project_id}/groups/{group_id}	workspace:userGroups:delete	-
PUT /v2/{project_id}/groups/{group_id}	workspace:userGroups:update	-
POST /v2/{project_id}/groups/{group_id}/actions	workspace:userGroups:operate	-
GET /v2/{project_id}/groups/{group_id}/users	workspace:userGroups:getUsers	-
GET /v2/{project_id}/workspace-sub-jobs	workspace:jobs:listSubJobs	-
POST /v2/{project_id}/workspace-sub-jobs/batch-delete	workspace:jobs:deleteSubJobRecords	-
GET /v2/{project_id}/ous	workspace:ou:get	-
POST /v2/{project_id}/ous	workspace:ou:create	-
DELETE /v2/{project_id}/ous/{ou_id}	workspace:ou:delete	-
PUT /v2/{project_id}/ous/{ou_id}	workspace:ou:update	-
GET /v2/{project_id}/policy-groups	workspace:policyGroups:list	-
POST /v2/{project_id}/policy-groups	workspace:policyGroups:create	-
DELETE /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:delete	-
GET /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:get	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:update	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/policy-groups/export	workspace:policyGroups:export	-
GET /v2/{project_id}/policy-groups/{policy_group_id}/policies	workspace:policyGroups:listPolicies	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}/policies	workspace:policyGroups:updatePolicies	-
GET /v2/{project_id}/policy-groups/{policy_group_id}/targets	workspace:policyGroups:listTargets	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}/targets	workspace:policyGroups:updateTargets	-
GET /v2/{project_id}/policy-groups/detail	workspace:policyGroups:listDetail	-
GET /v2/{project_id}/policy-groups/original-policies	workspace:policyGroups:getOriginalPolicies	-
GET /v2/{project_id}/users	workspace:users:list	-
POST /v2/{project_id}/users	workspace:users:create	-
DELETE /v2/{project_id}/users/{user_id}	workspace:users:delete	-
GET /v2/{project_id}/users/{user_id}	workspace:users:get	-
PUT /v2/{project_id}/users/{user_id}	workspace:users:update	-
POST /v2/{project_id}/users/batch-delete	workspace:users:batchDelete	-
POST /v2/{project_id}/users/password	workspace:users:resetPassword	-
POST /v2/{project_id}/users/password-token	workspace:users:checkResetPasswordToken	-

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/users/desktop-users/template	workspace:users:getTemplate	-
POST /v2/{project_id}/users/exist	workspace:users:checkExist	-
GET /v2/{project_id}/users/{user_id}/otp-devices	workspace:users:listOtps	-
GET /v2/{project_id}/users/template/download	workspace:users:getImportTemplate	-
POST /v2/{project_id}/users/export	workspace:users:export	-
POST /v2/{project_id}/users/batch-create	workspace:users:batchCreate	-
GET /v2/{project_id}/volume/products	workspace:products:listVolumeProducts	-
GET /v2/{project_id}/export-tasks	workspace:tenants:listExportTasks	-
POST /v2/{project_id}/export-tasks/batch-delete	workspace:tenants:deleteExportTasks	-
GET /v2/{project_id}/export-tasks/{task_id}/download	workspace:tenants:exportData	-
GET /v2/{project_id}/alarms	workspace:statistics:listAlarm	ces:alarmHistory:list
GET /v2/{project_id}/statistics/alarms	workspace:statistics:getAlarm	ces:alarmHistory:list
GET /v2/{project_id}/statistics/growth-rate	workspace:statistics:getGrowthRate	-
GET /v2/{project_id}/statistics/metrics	workspace:statistics:getMetric	-
GET /v2/{project_id}/statistics/metrics/trend	workspace:statistics:getMetricTrend	-
PUT /v2/{project_id}/statistics/notify-rules/{rule_id}	workspace:statistics:updateNotificationRules	smn:topic:get

API	对应的操作项	依赖的操作项
DELETE /v2/{project_id}/statistics/notify-rules/{rule_id}	workspace:statistics:deleteNotificationRules	-
POST /v2/{project_id}/statistics/notify-rules	workspace:statistics:createNotifyRules	smn:topic:get
GET /v2/{project_id}/statistics/notify-rules	workspace:statistics:listNotificationRules	-
GET /v2/{project_id}/statistics/notification-records	workspace:statistics:listNotificationRecords	-
GET /v2/{project_id}/statistics/metrics/desktops	workspace:statistics:listDesktopMetrics	-
GET /v2/{project_id}/statistics/metrics/desktops/export	workspace:statistics:exportDesktopMetrics	-
GET /v2/{project_id}/statistics/metrics/users	workspace:statistics:listUserMetrics	-
GET /v2/{project_id}/statistics/metrics/users/export	workspace:statistics:exportUserMetrics	-
GET /v3/{project_id}/statistics/metrics/desktops/export	workspace:statistics:exportDesktopMetrics	-
GET /v3/{project_id}/statistics/metrics/users/export	workspace:statistics:exportUserMetrics	-
POST /v1/{project_id}/app-center/buckets/actions/create-credential	workspace:appcenter:createBucketCredential	• obs:bucket:GetBucketAcl • obs:object:PutObject • obs:object:DeleteObject
POST /v1/{project_id}/app-center/buckets	workspace:appcenter:createAndAuthorizeBucket	• obs:bucket:HeadBucket • obs:bucket:PutBucketAcl • obs:bucket:PutReplicationConfiguration • obs:bucket:CreateBucket • obs:bucket:PutBucketCORS
GET /v1/{project_id}/app-center/apps	workspace:appcenter:listApps	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/app-center/apps	workspace:appcenter:createApp	-
PATCH /v1/{project_id}/app-center/apps/{app_id}	workspace:appcenter:updateApp	-
DELETE /v1/{project_id}/app-center/apps/{app_id}	workspace:appcenter:deleteApp	-
POST /v1/{project_id}/app-center/apps/{app_id}/actions/auto-install	workspace:appcenter:installApp	-
GET /v1/{project_id}/app-center/apps/{app_id}/authorizations	workspace:appcenter:listAppAuthorizations	-
POST /v1/{project_id}/app-center/apps/{app_id}/actions/assign-authorizations	workspace:appcenter:batchUpdateAppAuthorizations	-
POST /v1/{project_id}/app-center/apps/actions/batch-delete	workspace:appcenter:batchDeleteApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-disable	workspace:appcenter:batchDisableApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-enable	workspace:appcenter:batchEnableApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-assign-authorization	workspace:appcenter:batchUpdateAppAuthorizations	-
POST /v1/{project_id}/app-center/apps/actions/batch-auto-install	workspace:appcenter:batchInstallApps	-
GET /v1/{project_id}/app-center/app-catalogs	workspace:appcenter:listAppCatalogs	-
GET /v1/{project_id}/app-center/jobs	workspace:appcenter:listJobs	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/app-center/jobs/actions/batch-delete	workspace:appcenter:batchDeleteJobs	-
POST /v1/{project_id}/app-center/jobs/actions/retry	workspace:appcenter:retryJobs	-
POST /v1/{project_id}/app-center/app-rules	workspace:appcenter:createAppRule	-
GET /v1/{project_id}/app-center/app-rules	workspace:appcenter:listAppRule	-
PATCH /v1/{project_id}/app-center/app-rules/{rule_id}	workspace:appcenter:updateAppRule	-
DELETE /v1/{project_id}/app-center/app-rules/{rule_id}	workspace:appcenter:deleteAppRule	-
POST /v1/{project_id}/app-center/app-rules/batch-delete	workspace:appcenter:batchDeleteAppRules	-
POST /v1/{project_id}/app-center/app-rules/actions/enable-rule-restriction	workspace:appcenter:enableRuleRestriction	-
POST /v1/{project_id}/app-center/app-rules/actions/disable-rule-restriction	workspace:appcenter:disableRuleRestriction	-
POST /v1/{project_id}/app-center/app-restricted-rules	workspace:appcenter:addRestrictedRule	-
GET /v1/{project_id}/app-center/app-restricted-rules	workspace:appcenter:listRestrictedRule	-
POST /v1/{project_id}/app-center/app-restricted-rules/actions/batch-delete	workspace:appcenter:deleteRestrictedRule	-
PATCH /v1/{project_id}/app-center/profiles	workspace:appcenter:updateTenantProfile	-
GET /v1/{project_id}/app-center/profiles	workspace:appcenter:listTenantProfiles	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/scripts	workspace:scripts:create	-
GET /v2/{project_id}/scripts	workspace:scripts:list	-
GET /v2/{project_id}/scripts/{script_id}	workspace:scripts:get	-
PUT /v2/{project_id}/scripts/{script_id}	workspace:scripts:put	-
DELETE /v2/{project_id}/scripts/{script_id}	workspace:scripts:delete	-
POST /v2/{project_id}/script-executions	workspace:scripts:execute	-
GET /v2/{project_id}/script-execution-records/{record_id}	workspace:scripts:getRecordDetail	-
GET /v2/{project_id}/script-execution-records	workspace:scripts:listRecords	-
GET /v2/{project_id}/script-execution-tasks	workspace:scripts:listTasks	-
POST /v2/{project_id}/script-executions/retry	workspace:scripts:retry	-
POST /v2/{project_id}/script-executions/stop	workspace:scripts:stop	-
POST /v2/{project_id}/script-execution-records/{record_id}/download	workspace:scripts:download	-
GET /v2/{project_id}/share-space/configuration	workspace:tenants:getShareSpaceConfig	-
PUT /v2/{project_id}/share-space/configuration	workspace:tenants:updateShareSpaceConfig	-
GET /v2/{project_id}/auth-config/status	workspace:authConfigs:getStatus	-
POST /v2/{project_id}/privacystatement	workspace:privacystatements:sign	-

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/quotas/detail	workspace:quotas:get	-
GET /v2/{project_id}/sites	workspace:sites:get	-
POST /v2/{project_id}/sites	workspace:sites:add	• eip:bandwidths:create • eip:publicIps:create • elb:healthmonitors:create • elb:healthmonitors:show • elb:listeners:create • elb:listeners:update • elb:listeners:show • elb:listeners:list • elb:loadbalancers:create • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:list • elb:members:update • elb:pools:create • elb:pools:update • elb:pools:show • vpc:ports:create • vpc:ports:delete • vpc:securityGroupRules:create • vpc:securityGroupRules:delete • vpc:securityGroupRules:get • vpc:securityGroups:create • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:get

API	对应的操作项	依赖的操作项
DELETE /v2/{project_id}/sites/{site_id}	workspace:sites:delete	• elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:delete • elb:listeners:show • elb:loadbalancers:delete • elb:loadbalancers:show • elb:members:delete • elb:members:list • elb:pools:delete • elb:pools:show • vpc:ports:delete • vpc:securityGroups:delete • vpcep:endpoints:delete • vpcep:endpoints:get • eip:publicIps:disassociateInstance • eip:bandwidths:delete • eip:publicIps:delete

API	对应的操作项	依赖的操作项
PUT /v2/{project_id}/sites/{site_id}/access-mode	workspace:sites:updateAccessMode	• eip:bandwidths:create • eip:bandwidths:delete • eip:publicIps:create • eip:publicIps:delete • eip:publicIps:disassociateInstance • elb:healthmonitors:create • elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:create • elb:listeners:delete • elb:listeners:update • elb:listeners:show • elb:loadbalancers:create • elb:loadbalancers:delete • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:delete • elb:members:list • elb:members:update • elb:pools:create • elb:pools:delete • elb:pools:update • elb:pools:show • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:delete • vpcep:endpoints:get
PUT /v2/{project_id}/sites/{site_id}/subnet-ids	workspace:sites:updateSubnets	• vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get
GET /v2/{project_id}/tenants/lock-status	workspace:tenants:getLockStatus	-

API	对应的操作项	依赖的操作项
PUT /v2/{project_id}/tenants/lock-status	workspace:tenants:unlock	-
POST /v2/{project_id}/workspaces/enterprise-ids/check	workspace:tenants:checkEnterpriseIds	-
PUT /v2/{project_id}/workspaces/enterprise-id	workspace:tenants:updateEnterpriseId	-
POST /v2/{project_id}/bandwidths	workspace:bandwidth:create	-
GET /v2/{project_id}/bandwidths	workspace:bandwidth:list	-
POST /v2/{project_id}/bandwidths/{bandwidth_id}/update	workspace:bandwidth:update	-
DELETE /v2/{project_id}/bandwidths/{bandwidth_id}	workspace:bandwidth:delete	-
GET /v2/{project_id}/bandwidths/{bandwidth_id}/control-list	workspace:bandwidth:getControlConfig	-
PUT /v2/{project_id}/bandwidths/{bandwidth_id}/control-list	workspace:bandwidth:updateControlConfig	-
POST /v2/{project_id}/bandwidths/{bandwidth_id}/periodic/change/order	workspace:bandwidth:createChangeOrder	-
POST /v2/{project_id}/adns	workspace:bandwidth:create	-
GET /v2/{project_id}/adns	workspace:bandwidth:list	-
POST /v2/{project_id}/desktops-adn/batch-delete	workspace:bandwidth:delete	-
POST /v2/{project_id}/snapshots/batch-create	workspace:desktops:batchCreateSnapshots	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/snapshots/batch-delete	workspace:desktops:batchDeleteSnapshots	-
POST /v2/{project_id}/snapshots/batch-restore	workspace:desktops:batchRestoreSnapshots	-
GET /v2/{project_id}/snapshots	workspace:desktops:listSnapshots	-
POST /v2/{project_id}/verification/desktop-name	workspace:desktops:verifyDesktopName	-
GET /v2/{project_id}/subnets/{subnet_id}/available-ip	workspace:networks:getAvailableIp	-
GET /v2/{project_id}/ad/status	workspace:desktops:getAdStatus	-
GET /v2/{project_id}/ip-exist	workspace:networks:checkIpIfExist	-
POST /v2/{project_id}/desktops/check-images	workspace:images:checkIfExist	ims:images:list
GET /v2/{project_id}/hosts/{host_id}/servers	workspace:wdh:listDesktops	-
PUT /v2/{project_id}/hosts	workspace:wdh:update	-
GET /v2/{project_id}/terminals/binding-desktops/template	workspace:bindingPolicies:getTemplate	-
POST /v2/{project_id}/terminals/binding-desktops/template/import	workspace:bindingPolicies:import	-
GET /v2/{project_id}/terminals/binding-desktops/template/export	workspace:bindingPolicies:export	-
GET /v2/{project_id}/desktops/statistics/run-state	workspace:statistics:getRunState	-
GET /v2/{project_id}/desktops/statistics/login-state	workspace:statistics:getLoginState	-

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/subnets/using-subnets	workspace:networks:getUsingSubnets	-
GET /v2/{project_id}/ports	workspace:networks:listPorts	-
GET /v2/{project_id}/render-desktops/{desktop_id}/remote-consoles	workspace:renderDesktops:createConsole	-
PUT /v2/{project_id}/render-desktops/resize	workspace:renderDesktops:resize	-
POST /v2/{project_id}/exclusive-hosts/{host_id}/resize-lites	workspace:exclusiveHosts:resizeLites	-
GET /services/v2/{project_id}/desktops/{desktop_id}	workspace:desktops:get	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktop-monitor/{desktop_id}	workspace:desktops:getMonitor	ces:metricData:get
GET /v2/{project_id}/desktops/export	workspace:desktops:export	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktops/{desktop_id}/detach-info	workspace:desktops:listDetachInfo	-
GET /v2/{project_id}/desktops/{desktop_id}/sysprep	workspace:desktops:getSysprepVersion	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/internet	workspace:networks:createNat	• vpc:ports:delete • vpc:ports:get • vpc:networks:get • eip:publicIps:create • eip:publicIps:update • eip:publicIps:delete • nat:snatRules:list • nat:snatRules:create • nat:natGateways:list • nat:natGateways:create
GET /v2/{project_id}/internet	workspace:networks:listNats	• vpc:subnets:get • vpc:vpcs:get • nat:snatRules:list • nat:natGateways:list
POST /v2/{project_id}/quotas/check	workspace:quotas:check	-
GET /v2/{project_id}/subnets	workspace:networks:listSubnets	• vpc:subnets:list • vpc:subnets:get
GET /v2/{project_id}/vpcs	workspace:networks:listVpcs	vpc:vpcs:list
POST /v2/{project_id}/policy-groups/policy-template	workspace:policyGroups:createTemplate	-
GET /v1/{project_id}/policy-templates	workspace:policyGroups:listTemplate	-
PUT /v2/{project_id}/policy-groups/policy-template/{policy_group_id}	workspace:policyGroups:updateTemplate	-
GET /v2/{project_id}/security-groups	workspace:networks:listSecurityGroups	-
GET /v2/{project_id}/availability-zones/summary	workspace:availabilityZones:getSummary	-
GET /v2/{project_id}/availability-zones/detail	workspace:availabilityZones:get	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/users/desktop-users/action/import	workspace:users:importUser	-
POST /v2/{project_id}/users/template-upload	workspace:users:uploadTemplate	-
PUT /v2/{project_id}/access-policy/{access_policy_id}	workspace:accessPolicies:update	-
POST /v2/{project_id}/desktops/{desktop_id}/verify-source	workspace:desktops:verifySource	-
GET /v2/{project_id}/desktops/networks	workspace:desktops:listDesktopNetworks	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:securityGroups:get • eip:publicIps:list
POST /v2/{project_id}/desktops/networks/batch-change	workspace:desktops:batchChangeNetwork	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:securityGroups:get • eip:publicIps:list • eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
GET /v2/{project_id}/workspace-jobs/{job_id}	workspace:jobs:get	-
POST /v2/{project_id}/ip/import	workspace:accessPolicies:importIp	-
GET /v2/{project_id}/ip/template/download	workspace:accessPolicies:getIpImportTemplate	-

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/wks-edge-sites	workspace:sites:listEdgeSites	• ies:edgeSite:list • ies:edgeSite:getMetricData
POST /v2/{project_id}/check-edge-site-resources	workspace:sites:checkEdgeSiteResources	• ies:edgeSite:list • ies:edgeSite:getMetricData
GET /v2/{project_id}/ad-ous	workspace:ou:listAdOus	-
GET /v2/{project_id}/ou-users	workspace:ou:listOuUsers	-
POST /v2/{project_id}/ou-users/import	workspace:ou:importUsersByOU	-
GET /v1/{project_id}/app-groups	workspace:appGroup:list	-
POST /v1/{project_id}/app-groups	workspace:appGroup:create	-
DELETE /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:delete	-
GET /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:get	-
PATCH /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:update	-
GET /v1/{project_id}/app-groups/{app_group_id}/apps	workspace:app:listPublishedApp	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps	workspace:app:publish	-
GET /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}	workspace:app:get	-
PATCH /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}	workspace:app:update	-

API	对应的操作项	依赖的操作项
DELETE /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}/icon	workspace:app:deleteIcon	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}/icon	workspace:app:uploadIcon	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/check	workspace:app:check	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/disable	workspace:app:batchDisable	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/enable	workspace:app:batchEnable	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/batch-unpublish	workspace:app:unpublish	-
GET /v1/{project_id}/app-groups/{app_group_id}/publishable-app	workspace:appGroup:listPublishableApp	-
POST /v1/{project_id}/app-groups/actions/batch-delete-authorization	workspace:appGroup:batchDeleteAuthorization	-
POST /v1/{project_id}/app-groups/actions/disassociate-app-group	workspace:appGroup:disassociate	-
GET /v1/{project_id}/app-groups/actions/list-authorizations	workspace:appGroup:listAuthorization	-
POST /v1/{project_id}/app-groups/authorizations	workspace:appGroup:addAuthorization	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/app-groups/batch-delete	workspace:appGroup:batchDelete	-
POST /v1/{project_id}/app-groups/rules/validate	workspace:appGroup:check	-
GET /v1/{project_id}/app-server-groups	workspace:serverGroup:list	-
POST /v1/{project_id}/app-server-groups	workspace:serverGroup:create	• ims:images:list • vpc:ports:get • vpc:subnets:get
DELETE /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:delete	-
GET /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:get	-
PATCH /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:update	ims:images:list
GET /v1/{project_id}/app-server-groups/{server_group_id}/state	workspace:serverGroup:getServerState	-
GET /v1/{project_id}/app-server-groups/actions/list	workspace:serverGroup:listDetail	-
GET /v1/{project_id}/app-server-groups/resources/restrict	workspace:serverGroup:getRestrict	-
POST /v1/{project_id}/app-server-groups/rules/validate	workspace:serverGroup:validate	-
POST /v1/{project_id}/server-group/{server_group_id}/tags/create	workspace:serverGroup:tagResource	-

API	对应的操作项	依赖的操作项
DELETE /v1/{project_id}/server-group/{server_group_id}/tags/delete	workspace:serverGroup:unTagResource	-
GET /v1/{project_id}/server-group/{server_group_id}/tags	workspace:serverGroup:listTagsForResource	-
GET /v1/{project_id}/server-group/tags	workspace:serverGroup:listTags	-
POST /v1/{project_id}/server-group/tags/batch-create	workspace:serverGroup:batchCreateTags	-
DELETE /v1/{project_id}/server-group/tags/batch-delete	workspace:serverGroup:batchDeleteTags	-
GET /v1/{project_id}/app-servers	workspace:server:list	-
DELETE /v1/{project_id}/app-servers/{server_id}	workspace:server:delete	• iam:roles:listRoles • vpc:ports:delete • vpc:ports:get
GET /v1/{project_id}/app-servers/{server_id}	workspace:server:get	-
PATCH /v1/{project_id}/app-servers/{server_id}	workspace:server:update	-
POST /v1/{project_id}/app-servers/{server_id}/actions/change-image	workspace:server:changeImage	• ims:images:list • vpc:ports:get • vpc:subnets:get
POST /v1/{project_id}/app-servers/{server_id}/actions/reinstall	workspace:server:reinstall	• ims:images:list • vpc:ports:get • vpc:subnets:get
GET /v1/{project_id}/app-servers/{server_id}/actions/vnc	workspace:server:getVncUrl	-
GET /v1/{project_id}/app-servers/access-agent/upgrade-record	workspace:accessAgent:list	-

API	对应的操作项	依赖的操作项
PATCH /v1/{project_id}/app-servers/access-agent/actions/upgrade	workspace:accessAgent:batchUpgrade	-
GET /v1/{project_id}/app-servers/access-agent/latest-version	workspace:accessAgent:listLatestVersion	-
GET /v1/{project_id}/app-servers/access-agent/list	workspace:server:listAccessAgentDetails	-
GET /v1/{project_id}/app-servers/access-agent/upgrade-flag	workspace:accessAgent:getUpgradeFlag	-
PATCH /v1/{project_id}/app-servers/access-agent/upgrade-flag	workspace:accessAgent:updateUpgradeFlag	-
GET /v1/{project_id}/app-servers/access-agent/upgrade-record	workspace:accessAgent:listUpgradeRecords	-
POST /v1/{project_id}/app-servers/actions/batch-delete	workspace:server:batchDelete	• iam:roles:listRoles • vpc:ports:delete • vpc:ports:get
PATCH /v1/{project_id}/app-servers/actions/batch-maint	workspace:server:batchChangeMaintainMode	-
PATCH /v1/{project_id}/app-servers/actions/batch-reboot	workspace:server:batchReboot	-
PATCH /v1/{project_id}/app-servers/actions/batch-rejoin-domain	workspace:server:batchRejoinDomain	-
PATCH /v1/{project_id}/app-servers/actions/batch-start	workspace:server:batchStart	-
PATCH /v1/{project_id}/app-servers/actions/batch-stop	workspace:server:batchStop	-
PATCH /v1/{project_id}/app-servers/actions/batch-update-tsvi	workspace:server:batchUpdateTsvi	• vpc:subnets:get • vpc:ports:update

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/app-servers/actions/create	workspace:server:create	• ims:images:list • ims:images:updateMemberStatus • ims:images:share • ims:images:get • vpc:securityGroups:get • vpc:securityGroupRules:get • vpc:networks:get • vpc:subnets:get • vpc:ports:create • vpc:ports:get • vpc:ports:delete • vpc:vpcs:get • dss:pools:list
PATCH /v1/{project_id}/app-servers/hosts/batch-migrate	workspace:server:batchMigrateHosts	-
GET /v1/{project_id}/app-servers/metric-data/{server_id}	workspace:server:getMetricData	-
GET /v1/{project_id}/app-server-sub-jobs	workspace:jobs:listSubJobs	-
POST /v1/{project_id}/app-server-sub-jobs/actions/batch-delete	workspace:jobs:batchDeleteSubJobs	-
GET /v1/{project_id}/app-server-sub-jobs/actions/count	workspace:jobs:countSubJobs	-
POST /v1/{project_id}/app-warehouse/action/authorize	workspace:appWarehouse:authorizeObs	• obs:bucket:GetBucketAcl • obs:object:PutObject • obs:object:DeleteObject
POST /v1/{project_id}/app-warehouse/actions/batch-delete	workspace:appWarehouse:batchDeleteApp	• obs:bucket:HeadBucket • obs:object:DeleteObject
GET /v1/{project_id}/app-warehouse/apps	workspace:appWarehouse:ListWarehouseApps	-
POST /v1/{project_id}/app-warehouse/apps	workspace:appWarehouse:createApp	-

API	对应的操作项	依赖的操作项
DELETE /v1/{project_id}/app-warehouse/apps/{id}	workspace:appWarehouse:deleteApp	• obs:bucket:HeadBucket • obs:object:DeleteObject
POST /v1/{project_id}/app-warehouse/apps/icon	workspace:appWarehouse:uploadAppIcon	obs:object:PutObject
POST /v1/{project_id}/app-warehouse/bucket-and-acl/create	workspace:appWarehouse:createBucketOrAcl	• obs:bucket:GetBucketAcl • obs:bucket:HeadBucket • obs:bucket:PutBucketAcl • obs:bucket:PutReplicationConfiguration • obs:bucket:CreateBucket • obs:bucket:PutBucketCORS
GET /v1/{project_id}/check/quota	workspace:quotas:get	-
GET /v1/{project_id}/image-server-jobs	workspace:images:listImageJobs	-
GET /v1/{project_id}/image-server-jobs/{job_id}	workspace:images:getImageJob	-
GET /v1/{project_id}/image-servers	workspace:imageServer:list	-
POST /v1/{project_id}/image-servers	workspace:imageServer:create	• ims:images:list • vpc:ports:get • vpc:subnets:get
GET /v1/{project_id}/image-servers/{server_id}	workspace:imageServer:get	-
PATCH /v1/{project_id}/image-servers/{server_id}	workspace:imageServer:update	-
POST /v1/{project_id}/image-servers/{server_id}/actions/attach-app	workspace:imageServer:attachApp	-
GET /v1/{project_id}/image-servers/{server_id}/actions/latest-attached-app	workspace:imageServer:listLatestAttachedApp	-

API	对应的操作项	依赖的操作项
POST /v1/{project_id}/image-servers/{server_id}/actions/recreate-image	workspace:imageServer:recreate	• vpc:ports:get • vpc:subnets:get • ims:quotas:get • ims:images:get • ims:images:list • ims:images:setTags • ims:images:setOrDeleteTags • ims:images:updateMemberStatus • ims:images:copyInRegion • ims:serverImages:create
PATCH /v1/{project_id}/image-servers/actions/batch-delete	workspace:imageServer:batchDelete	-
GET /v1/{project_id}/image-server-sub-jobs	workspace:imageServer:listImageSubJobs	-
PATCH /v1/{project_id}/image-server-sub-jobs/actions/batch-delete	workspace:imageServer:batchDeleteImageSubJobs	-
GET /v1/{project_id}/image-server-sub-jobs/actions/count	workspace:imageServer:countImageSubJobs	-
GET /v2/{project_id}/job/{job_id}	workspace:jobs:get	-
GET /v1/{project_id}/mails	workspace:appGroup:listMailRecord	-
POST /v1/{project_id}/mails/actions/send	workspace:appGroup:resendMail	-
POST /v1/{project_id}/mails/actions/send	workspace:appGroup:resendMail	-
GET /v1/{project_id}/persistent-storages	workspace:storage:listPersistentStorage	-
POST /v1/{project_id}/persistent-storages	workspace:storage:createPersistentStorage	• obs:bucket:HeadBucket • obs:bucket:PutBucketPolicy • obs:bucket:PutBucketAcl • obs:bucket:PutBucketCORS

API	对应的操作项	依赖的操作项
DELETE /v1/{project_id}/persistent-storages/{storage_id}	workspace:storage:deletePersistentStorage	• obs:object:GetObject • obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/assign-folder	workspace:storage:updateUserFolderAssignment	-
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/assign-share-folder	workspace:storage:updateShareFolderAssignment	-
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/create-share-folder	workspace:storage:createShareFolder	• obs:object:GetObject • obs:object:PutObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/delete-storage-claim	workspace:storage:deleteStorageClaim	obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/delete-user-attachment	workspace:storage:deleteUserStorageAttachment	obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/actions/batch-delete	workspace:storage:batchDeletePersistentStorage	-
GET /v1/{project_id}/persistent-storages/actions/list-attachments	workspace:storage:listStorageAssignment	-
GET /v1/{project_id}/persistent-storages/actions/list-share-folders	workspace:storage:listShareFolder	-
GET /v1/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:get	-
GET /v2/{project_id}/policy-groups/{policy_group_id}/policies	workspace:policyGroups:listPolicies	-
GET /v1/{project_id}/policy-groups/{policy_group_id}/target	workspace:policyGroups:listTargets	-

API	对应的操作项	依赖的操作项
GET /v2/{project_id}/policy-groups/detail	workspace:policyGroups:listDetail	-
GET /v1/{project_id}/policy-templates	workspace:policyGroups:listTemplate	-
DELETE /v1/{project_id}/policy-templates/{policy_template_id}	workspace:policyGroups:deleteTemplate	-
PATCH /v1/{project_id}/policy-templates/{policy_template_id}	workspace:policyGroups:updateTemplate	-
GET /v1/{project_id}/privacy-statement	workspace:privacystatements:get	-
DELETE /v1/{project_id}/scaling-policy	workspace:scalingPolicy:delete	-
GET /v1/{project_id}/scaling-policy	workspace:scalingPolicy:list	-
PUT /v1/{project_id}/scaling-policy	workspace:scalingPolicy:create	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records	workspace:scheduledTasks:list	-
POST /v2/{project_id}/scheduled-tasks	workspace:scheduledTasks:create	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records/{record_id}	workspace:scheduledTasks:getRecord	-
DELETE /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:delete	-
POST /v2/{project_id}/scheduled-tasks/future-executions	workspace:scheduledTasks:get	-
PUT /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:update	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records	workspace:scheduledTasks:listRecords	-

API	对应的操作项	依赖的操作项
POST /v2/{project_id}/scheduled-tasks/batch-delete	workspace:scheduledTasks:batchDelete	-
POST /v1/{project_id}/session/app-connection	workspace:session:listAppConnection	-
POST /v1/{project_id}/session/logoff	workspace:session:logoffUserSession	-
POST /v1/{project_id}/session/user-connection	workspace:session:listUserConnection	-
GET /v1/{project_id}/session/user-session-info	workspace:session:listSessionByUserName	-
PUT /v1/{project_id}/storages-policy/actions/create-statements	workspace:storagePolicy:create	-
GET /v1/{project_id}/storages-policy/actions/list-statements	workspace:storagePolicy:list	-
GET /v2/{project_id}/users	workspace:users:list	-
GET /v1/persistent-storages/actions/list-sfs-storages	workspace:storage:listSfs3Storage	• obs:bucket:ListBucket • obs:bucket:GetBucketStorage • obs:bucket:ListAllMyBuckets
GET /v1/{project_id}/availability-zone	workspace:baseResource:list	ecs:availabilityZones:list
POST /v1/{project_id}/bundles/batch-query-config-info	workspace:tenants:listConfigInfo	-
GET /v1/{project_id}/product	workspace:baseResource:list	-
GET /v1/{project_id}/product	workspace:baseResource:list	-
POST /v1/{project_id}/tenant/action/active	workspace:tenants:active	-
GET /v1/{project_id}/tenant/profile	workspace:tenants:listTenantProfile	-

API	对应的操作项	依赖的操作项
GET /v1/{project_id}/volume-type	workspace:baseResource:list	-
GET /v1/{project_id}/app-servers/server-metric-data/{server_id}	workspace:server:listServerMetricData	-
GET /v1/{project_id}/session/list-sessions	workspace:session:listSessions	-
PATCH /v1/{project_id}/app-warehouse/apps/{id}	workspace:appWarehouse:updateApp	-
POST /v1/{project_id}/app-servers/actions/batch-change-image	workspace:server:batchChangeImage	• ims:images:list • vpc:ports:get • vpc:subnets:get
POST /v1/{project_id}/app-servers/actions/batch-reinstall	workspace:server:batchReinstall	• ims:images:list • vpc:ports:get • vpc:subnets:get

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-206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。

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

表 5-206 云桌面支持的资源类型

资源类型	描述	URN
desktop	桌面	workspace:<region>:<account-id>:desktop:<desktop-id>
desktopPool	桌面池	workspace:<region>:<account-id>:desktopPool:<pool-id>
wdh	云办公主机	workspace:<region>:<account-id>:wdh:<wdh-id>
exclusiveHost	专享主机	workspace:<region>:<account-id>:exclusiveHost:<host-id>
user	用户	workspace:<region>:<account-id>:user:<user-id>

资源类型	描述	URN
userGroup	用户组	workspace:<region>:<account-id>:userGroup:<group-id>
policyGroup	策略组	workspace:<region>:<account-id>:policyGroup:<policy-group-id>
script	脚本	workspace:<region>:<account-id>:script:<script-id>
scheduledTask	定时任务	workspace:<region>:<account-id>:scheduledTask:<task-id>
server	应用服务器	workspace:<region>:<account-id>:server:<server-id>
serverGroup	应用服务器组	workspace:<region>:<account-id>:serverGroup:<server-group-id>
app	应用	workspace:<region>:<account-id>:app:<app-id>
appGroup	应用组	workspace:<region>:<account-id>:appGroup:<app-group-id>
imageServer	应用镜像服务器	workspace:<region>:<account-id>:imageServer:<image-server-id>
storage	存储	workspace:<region>:<account-id>:storage:<storage-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workspace:）仅适用于对应服务的操作，详情请参见**表5-207**。
  - 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。

云桌面定义了以下可以在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 5-207 云桌面支持的服务级条件键

服务级条件键	类型	单值/多值	说明
workspace:AccessMode	string	多值	根据请求参数中指定的接入方式过滤访问，有效的条件值应为INTERNET、DEDICATED、BOTH。
workspace:CreateOrderType	string	FALSE	根据请求参数中指定的创建订单类型过滤访问，有效的条件值应为createDesktops、addVolumes、createDehHosts、rebuildDesktops、createDesktopPool、expandDesktopPool、applyDesktopsInternet、createExclusiveHosts、subscribeUserSharer、createApps。
workspace:ChangeOrderType	string	FALSE	根据请求参数中指定的变更订单类型过滤访问，有效的条件值应为resizeDesktops、expandVolumes、meteredToPeriod、ADD_VOLUME、EXTEND_VOLUME、RESIZE、CHANGE_IMAGE、ADD_SUB_RESOURCES、DELETE_SUB_RESOURCES。
workspace:AssociatePublicIp	boolean	FALSE	按照关联eip开关值筛选桌面绑定eip的权限。

5.10.13 管理与监管

5.10.13.1 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 5-208 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

授权项	描述	访问级别	资源类型（*为必须）	条件键
smn:topic:updateTopic	授予更新主题信息的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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>
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
smn:tag:delete	授予删除主题标签的权限。	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• 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:topic:createNotifyPolicy	授予创建通知策略的权限。	write	topic *	-
smn:topic:updateNotifyPolicy	授予修改通知策略的权限。	write	topic *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
smn:topic:getNotifyPolicy	授予查询通知策略的权限。	read	topic *	-
smn:topic:deleteNotifyPolicy	授予删除通知策略的权限。	write	topic *	-

SMN的API通常对应着一个或多个授权项。表5-209展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-209 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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/notifications/topics/{topic_urn}/subscriptions/from-subscription-users	smn:topic:subscribe	-
POST /v2/{project_id}/notifications/topics/{topic_urn}/notify-policy	smn:topic:createNotifyPolicy	smn:topic:listSubscriptionsByTopic
PUT /v2/{project_id}/notifications/topics/{topic_urn}/notify-policy/{notify_policy_id}	smn:topic:updateNotifyPolicy	smn:topic:listSubscriptionsByTopic
GET /v2/{project_id}/notifications/topics/{topic_urn}/notify-policy	smn:topic:getNotifyPolicy	-
DELETE /v2/{project_id}/notifications/topics/{topic_urn}/notify-policy/{notify_policy_id}	smn:topic:deleteNotifyPolicy	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-210**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 5-210 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5-211**。
  - 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 5-211 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。

5.10.13.2 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 5-212 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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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5-213展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-213 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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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

API	对应的授权项	依赖的授权项
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
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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SCP所作用的资源。如表5-214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 5-214 LTS 支持的资源类型

资源类型	URN
logStream	lts:<region>:<account-id>:logStream:<group_id>/<stream_id>

资源类型	URN
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。

5.10.13.3 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 5-215 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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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>
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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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**
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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>
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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
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5-216**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-216 API 与操作项的关系

API	对应的操作项	依赖的操作项
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	-

API	对应的操作项	依赖的操作项
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	-
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	-

API	对应的操作项	依赖的操作项
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	-
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	-

API	对应的操作项	依赖的操作项
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	-
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	-

API	对应的操作项	依赖的操作项
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	-
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	-

API	对应的操作项	依赖的操作项
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	-
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	-
GET /v3/roles	iam:roles:list	-
GET /v3/roles/{role_id}	iam:roles:get	-
GET /v3.0/OS-PERMISSION/role-assignments	iam::listRoleAssignments	-

API	对应的操作项	依赖的操作项
GET /v3/domains/{domain_id}/groups/{group_id}/roles	iam:groups:listRolesOnDomain	-
GET /v3/projects/{project_id}/groups/{group_id}/roles	iam:groups:listRolesOnProject	-
PUT /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}	iam:groups:grantRoleOnDomain	-
PUT /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:groups:grantRoleOnProject	-
HEAD /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}	iam:groups:checkRoleOnDomain	-
HEAD /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:groups:checkRoleOnProject	-
GET /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/inherited_to_projects	iam:groups:listRoles	-
HEAD /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects	iam:groups:checkRole	-
DELETE /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects	iam:groups:revokeRole	-
DELETE /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}	iam:groups:revokeRoleOnDomain	-

API	对应的操作项	依赖的操作项
DELETE /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:groups:revokeRoleOnProject	-
PUT /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects	iam:groups:grantRole	-
GET /v3.0/OS-ROLE/roles	iam:roles:list	-
GET /v3.0/OS-ROLE/roles/{role_id}	iam:roles:get	-
POST /v3.0/OS-ROLE/roles	iam:roles:create	-
POST /v3.0/OS-ROLE/roles	iam:roles:create	-
PATCH /v3.0/OS-ROLE/roles/{role_id}	iam:roles:update	-
PATCH /v3.0/OS-ROLE/roles/{role_id}	iam:roles:update	-
DELETE /v3.0/OS-ROLE/roles/{role_id}	iam:roles:delete	-
GET /v3.0/OS-AGENCY/agencies	iam:agencies:list	-
GET /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:get	-
POST /v3.0/OS-AGENCY/agencies	iam:agencies:create	-
PUT /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:update	-
DELETE /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:delete	-
GET /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles	iam:agencies:listRolesOnDomain	-

API	对应的操作项	依赖的操作项
GET /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles	iam:agencies:listRolesOnProject	-
PUT /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:grantRoleOnDomain	-
PUT /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:grantRoleOnProject	-
HEAD /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:checkRoleOnDomain	-
HEAD /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:checkRoleOnProject	-
DELETE /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:revokeRoleOnDomain	-
DELETE /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:revokeRoleOnProject	-
GET /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/inherited_to_projects	iam:agencies:listRoles	-
PUT /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:agencies:grantRole	-

API	对应的操作项	依赖的操作项
HEAD /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:agencies:checkRole	-
DELETE /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:agencies:revokeRole	-
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups	iam::listGroupsAssignedEnterpriseProject	-
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles	iam:groups:listRolesOnEnterpriseProject	-
PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}	iam:groups:grantRoleOnEnterpriseProject	-
DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}	iam:groups:revokeRoleOnEnterpriseProject	-
GET /v3.0/OS-PERMISSION/groups/{group_id}/enterprise-projects	iam:groups:listAssignedEnterpriseProjects	-
GET /v3.0/OS-PERMISSION/users/{user_id}/enterprise-projects	iam:users:listAssignedEnterpriseProjects	-

API	对应的操作项	依赖的操作项
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users	iam::listUsersAssignedEnterpriseProject	-
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles	iam:users:listRolesOnEnterpriseProject	-
PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}	iam:users:grantRoleOnEnterpriseProject	-
DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}	iam:users:revokeRoleOnEnterpriseProject	-
PUT /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments	iam:agencies:grantRoleOnEnterpriseProject	-
DELETE /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments	iam:agencies:revokeRoleOnEnterpriseProject	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如**表5-217**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 5-217 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5-218。
  - 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 5-218 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。

5.10.13.4 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 5-219 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	别名
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	别名
			-	• 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	

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
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5-220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 5-220 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）

条件键概述

条件（Condition）是身份策略生效的特定条件，包括条件键和运算符。

- 条件键表示身份策略语句的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5-221。
  - 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，身份策略才能生效。支持的运算符请参见：运算符。

STS支持的服务级条件键

STS定义了以下可以在自定义身份策略的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身份策略语句应用的条件。

表 5-221 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	按您代入另一个账号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。
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。

5.10.13.5 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 5-222 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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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5-223展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-223 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	-

API	对应的授权项	依赖的授权项
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
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

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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 5-224 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。

5.10.13.6 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 5-225 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

授权项	描述	访问级别	资源类型（* 为必须）	条件键
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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 *	-

授权项	描述	访问级别	资源类型（* 为必须）	条件键
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 *	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（* 为必须）	条件键
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5-226展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-226 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

API	对应的授权项	依赖的授权项
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
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

API	对应的授权项	依赖的授权项
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
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

API	对应的授权项	依赖的授权项
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
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5-227**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 5-227 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。

5.10.13.7 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 5-228 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	-	-
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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	-	-
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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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
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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
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>
			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>

授权项	描述	访问级别	资源类型（*为必须）	条件键
			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	-	-
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5-229展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-229 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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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	-

API	对应的授权项	依赖的授权项
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	-
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5-230**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 5-230 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>
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5-231**。
  - 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 5-231 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。

5.10.13.8 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 5-232 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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
ram:permissions:get	授予获取RAM权限内容的权限。	read	permission *	-
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5-233**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-233 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5-234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 5-234 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5-235。

  - 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 5-235 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。

5.10.13.9 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 5-236 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5-237展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-237 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5-238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 5-238 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。

5.10.13.10 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 5-239 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5-240展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-240 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。

5.10.13.11 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 5-241 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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
rms:organizationConformancePacks:delete	授予权限删除组织合规规则包。	write	organizationConformancePacks *	-
rms:organizationConformancePacks:update	授予权限更新组织合规规则包。	write	organizationConformancePacks *	-
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:update	授予权限更新合规规则包。	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	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
rms:policyAssignments:create	授予权限创建新的合规规则以评估您的资源。	write	-	• g:TagKeys • g:RequestTag/<tag-key>
rms:policyAssignments:update	授予权限更新已存在的合规规则以评估您的资源。	write	policyAssignments *	g:ResourceTag/<tag-key>
			-	• g:TagKeys • g:RequestTag/<tag-key>
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 *	g:ResourceTag/<tag-key>
rms:policyAssignments:get	授予权限查看已存在的合规规则详情。	read	policyAssignments *	g:ResourceTag/<tag-key>
rms:organizationPolicyAssignments:put	授予权限对整个组织创建或更新合规规则以评估您的资源。	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	policyAssignments	g:ResourceTag/<tag-key>
rms:policyStates:runEvaluation	授予权限运行指定的合规规则以评估您的资源。	write	policyAssignments	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
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 *	-
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

授权项	描述	访问级别	资源类型（*为必须）	条件键
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:TrackerBucketName • rms:TrackerBucketPathPrefix
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	-	-
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>

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
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
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
rms:policyAssignmentsRemediation:putRemediationConfiguration	授予权限创建合规修正配置。	write	policyAssignmentsRemediation*	-
rms:policyAssignmentsRemediation:deleteRemediationConfiguration	授予权限删除合规修正配置。	write	policyAssignmentsRemediation*	-
rms:policyAssignmentsRemediation:getRemediationConfiguration	授予权限查看合规修正配置。	read	policyAssignmentsRemediation*	-
rms:policyAssignmentsRemediation:runRemediation	授予权限执行合规修正配置。	write	policyAssignmentsRemediation*	-
rms:policyAssignmentsRemediation:listRemediationExecutionStatuses	授予权限查看合规修正执行状态。	list	policyAssignmentsRemediation*	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
rms:policyAssignmentsRemediation:createRemediationExceptions	授予权限创建合规修正例外。	write	policyAssignmentsRemediation*	-
rms:policyAssignmentsRemediation:deleteRemediationExceptions	授予权限删除合规修正例外。	write	policyAssignmentsRemediation*	-
rms:policyAssignmentsRemediation:listRemediationExceptions	授予权限查看合规修正例外。	list	policyAssignmentsRemediation*	-

Config的API通常对应着一个或多个授权项。表5-242展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-242 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

API	对应的授权项	依赖的授权项
GET /v1/resource-manager/organizations/{organization_id}/conformance-packs	rms:organizationConformancePacks:list	organizations:organizations:get
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	-

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	rms:conformancePacks:get	-
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	-

API	对应的授权项	依赖的授权项
GET /v1/resource-manager/domains/{domain_id}/stored-queries	rms:storedQueries:list	-
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	-
PUT /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-configuration	rms:policyAssignmentsRemediation:putRemediationConfiguration	• iam:agencies:pass • iam:agencies:createServiceLinkedAgencyV5

API	对应的授权项	依赖的授权项
DELETE /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-configuration	rms:policyAssignmentsRemediation:deleteRemediationConfiguration	-
GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-configuration	rms:policyAssignmentsRemediation:getRemediationConfiguration	-
POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-execution	rms:policyAssignmentsRemediation:runRemediation	• functiongraph:function:invokeAsync • functiongraph:function:getFunctionConfig • rf:stack:create • rf:stack:delete • rf:stack:getTemplate • rf:stack:getMetadata • rf:privateTemplate:showMetadata
GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-execution-statuses	rms:policyAssignmentsRemediation:listRemediationExecutionStatuses	-
POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-execution-statuses/summary	rms:policyAssignmentsRemediation:listRemediationExecutionStatuses	-

API	对应的授权项	依赖的授权项
POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-exception/create	rms:policyAssignmentsRemediation:createRemediationExceptions	-
POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-exception/delete	rms:policyAssignmentsRemediation:deleteRemediationExceptions	-
GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-exception	rms:policyAssignmentsRemediation:listRemediationExceptions	-

资源类型（Resource）

资源类型（Resource）表示SCP所作用的资源。如表5-243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 5-243 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>

资源类型	URN
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>
policyAssignmentsRemediation	rms::<account-id>:policyAssignmentsRemediation:<policy-assignment-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5-244**。
  - 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 5-244 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:AuthorizedAccountOrg...	string	单值	根据指定的资源聚合授权账号的Organizations Path 过滤访问。
rms:TrackerBucketName	string	单值	根据指定的转储目标桶名称进行过滤访问。
rms:TrackerBucketPathPre...	string	单值	根据指定的转储目标桶桶前缀进行过滤访问。

条件键示例

- rms:AuthorizedAccountOrgPath

  示例：禁止组织内账号给组织外的账号进行聚合授权。

```
{
  "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】
          ]
        }
      }
    }
  ]
}
```

- rms:TrackerBucketName

  示例：禁止资源记录器转储到非预期的OBS桶。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "rms:trackerConfig:put"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotMatch": {
          "rms:TrackerBucketName": [
            "BucketName"
          ]
        }
      }
    }
  ]
}
```

- rms:TrackerBucketPathPrefix

  示例：禁止资源记录器转储到非预期的OBS路径下。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "rms:trackerConfig:put"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotMatch": {
          "rms:TrackerBucketPathPrefix": [
```



```
        "BucketFolder"
      ]
    }
   }
  }
 ]
}
```

5.10.13.12 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 5-245 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 *	-

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
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 *	-
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 *	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
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:analyzer:createResourceConfigurations	授予创建资源配置的权限。	Write	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:listResourceConfigurations	授予查询资源配置列表的权限。	List	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:deleteResourceConfigurations	授予删除资源配置的权限。	Write	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer::validatePolicy	授予验证策略的权限。	Read	-	-
AccessAnalyzer::checkNoNewAccess	授予检查更新后的策略是否有新的访问权限。	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 5-246 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。

5.10.13.13 云审计服务 CTS

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 5-247 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	-
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5-248展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-248 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	-
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	-

API	对应的授权项	依赖的授权项
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
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	-

API	对应的授权项	依赖的授权项
GET /v3/{project_id}/quotas	cts:quota:get	-
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

API	对应的授权项	依赖的授权项
PUT /v3/{project_id}/notifications	cts:notification:update	• smn:topic:listTopic • iam:users:listUsers • iam:groups:listGroups
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5-249**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 5-249 cts 支持的资源类型

资源类型	URN
tracker	cts:<region>:<account-id>:tracker:<tracker-id>
notification	cts:<region>:<account-id>:notification:<notification-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cts:）仅适用于对应服务的操作，详情请参见**表5-250**。
  - 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。

CTS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 5-250 CTS 支持的服务级条件键

服务级条件键	类型	单值/多值	说明
cts:TargetType	string	单值	按照数据转储类型筛选访问权限。
cts:TargetAccountId	string	单值	按照obs桶所属用户的DomainID（账号ID）筛选访问权限。
cts:TargetOrgId	string	单值	按照obs桶所属组织筛选访问权限。
cts:TargetOrgPath	string	单值	按照obs桶所属组织OU路径筛选访问权限。

5.10.13.14 资源治理中心 RGC

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RGC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RGC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RGC的相关操作。

表 5-251 RGC 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	别名
rgc:control:list	授予列出控制策略的权限。	List	-	-	-
rgc:controlViolation:list	授予列出不合规信息的权限。	List	-	-	-
rgc:control:get	授予获取控制策略详细信息的权限。	Read	-	-	-
rgc:control:enable	授予开启控制策略的权限。	Write	-	-	-
rgc:control:disable	授予关闭控制策略的权限。	Write	-	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rgc:controlOperate:get	授予获取控制策略操作状态的权限。	Read	-	-	-
rgc:enabledControl:list	授予列出开启的控制策略的权限。	List	-	-	-
rgc:controlsForOrganizationalUnit:list	授予列出某个注册组织单元下开启的控制策略的权限。	List	-	-	-
rgc:controlsForAccount:list	授予列出某个纳管账号开启的控制策略的权限。	List	-	-	-
rgc:complianceStatusForAccount:get	授予获取组织里某个纳管账号的资源合规状态的权限。	Read	-	-	-
rgc:complianceStatusForOrganizationalUnit:get	授予获取组织里某个注册组织单元下所有纳管账号的资源合规状态的权限。	Read	-	-	-
rgc:controlsForOrganizationalUnit:get	授予获取某个组织单元开启的控制策略的权限。	Read	-	-	-
rgc:controlsForAccount:get	授予获取某个账号开启的控制策略的权限。	Read	-	-	-
rgc:configRuleCompliance:list	授予列出纳管账号的Config规则合规性信息的权限。	List	-	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rgc:externalConfigRuleCompliance:list	授予列出纳管账号的外部Config规则合规性信息的权限。	List	-	-	-
rgc:driftDetail:list	授予列出漂移信息的权限。	List	-	-	-
rgc:managedOrganizationalUnit:register	授予注册组织单元的权限。	Write	-	-	-
rgc:managedOrganizationalUnit:reRegister	授予重新注册组织单元的权限。	Write	-	-	-
rgc:managedOrganizationalUnit:deRegister	授予取消注册组织单元的权限。	Write	-	-	-
rgc:operation:get	授予获取注册过程信息的权限。	Read	-	-	-
rgc:managedOrganizationalUnit:delete	授予删除注册组织单元的权限。	Write	-	-	-
rgc:managedOrganizationalUnit:get	授予获取已注册组织单元的权限。	Read	-	-	-
rgc:managedOrganizationalUnit:create	授予创建组织单元的权限。	Write	-	-	-
rgc:managedOrganizationalUnit:list	授予列举控制策略生效的注册组织单元信息的权限。	List	-	-	-
rgc:managedAccount:enroll	授予纳管账号的权限。	Write	-	-	-
rgc:managedAccount:unEnroll	授予取消纳管账号的权限。	Write	-	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rgc:managedAccount:update	授予更新纳管账号的权限。	Write	-	-	-
rgc:managedAccount:get	授予获取纳管账号的权限。	Read	-	-	-
rgc:managedAccountsForParent:list	授予列出注册组织单元下所有纳管账号信息的权限。	List	-	-	-
rgc:managedAccount:create	授予创建账号的权限。	Write	-	-	-
rgc:managedAccount:list	授予列出控制策略生效的纳管账号信息的权限。	List	-	-	-
rgc:managedCoreAccount:get	授予获取核心纳管账号的权限。	Read	-	-	-
rgc:homeRegion:get	授予查询主区域的权限。	Read	-	-	-
rgc:preLaunch:check	授予设置Landing Zone前检查的权限。	Write	-	-	-
rgc:landingZone:setup	授予设置Landing Zone的权限。	Write	-	-	-
rgc:landingZone:delete	授予删除Landing Zone的权限。	Write	-	-	-
rgc:landingZoneStatus:get	授予获取查询Landing Zone设置状态的权限。	Read	-	-	-
rgc:availableUpdate:get	授予获取Landing Zone可更新状态的权限。	Read	-	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键	别名
rgc:landingZoneConfiguration:get	授予获取Landing Zone配置信息的权限。	Read	-	-	-
rgc:landingZoneIdentityCenter:get	授予获取当前客户的Identity Center用户信息的权限。	Read	-	-	-
rgc:operation:list	授予获取注册组织单元或纳管账号的当前操作状态的权限。	List	-	-	-
rgc:templateDeployParam:get	授予获取模板部署参数的权限。	Read	-	-	-
rgc:template:create	授予创建模板的权限。	Write	-	-	-
rgc:template:delete	授予删除模板的权限。	Write	-	-	-
rgc:predefinedTemplate:list	授予列出预置模板的权限。	List	-	-	-
rgc:managedAccountTemplate:get	授予获取纳管账号模板详情的权限。	Read	-	-	-

RGC的API通常对应着一个或多个授权项。表5-252展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-252 API 与操作项的关系

API	对应的操作项	依赖的操作项
POST /v1/governance/control/enable	rgc:control:enable	-
POST /v1/governance/control/disable	rgc:control:disable	-

API	对应的操作项	依赖的操作项
GET /v1/governance/operated-controls/{control_operate_request_id}	rgc:controlOperate:get	-
GET /v1/governance/managed-organizational-unit/{managed_organizational_unit_id}/controls	rgc:controlsForOrganizationalUnit:list	-

资源类型（Resource）

RGC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RGC服务，请在SCP的Resource元素中使用通配符号*，表示策略将应用到所有资源。

条件（Condition）

RGC服务不支持在SCP中的条件键中配置服务级的条件键。

RGC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。

5.10.13.15 应用运维管理 AOM

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AOM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AOM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AOM的相关操作。

表 5-253 AOM 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
aom:metric:delete	授予权限以删除监控配置信息。	write	-	-
aom:icmgr:get	授予权限以获取采集组件版本信息。	read	-	-
aom:agency:get	授予权限以查询委托权限。	read	-	-
aom:icmgr:list	授予权限以获取采集组件版本信息。	list	-	-
aom:metric:list	授予权限以查询指标项。	list	-	-
aom:metric:put	授予权限以上报指标。	write	-	-
aom:discoveryRule:set	授予权限以创建或者更新服务发现规则列表。	write	-	-
aom:discoveryRule:delete	授予权限以删除服务发现规则列表。	write	-	-
aom:discoveryRule:list	授予权限以查询服务发现规则列表。	list	-	-
aom:alarmRule:create	授予权限以创建告警规则。	write	alarmRule *	g:ResourceTag/<tag-key>
			-	• g:TagKeys • g:RequestTag/<tag-key>
aom:alarmRule:list	授予权限以查询告警规则列表。	list	-	-
aom:alarmRule:update	授予权限以更新告警规则。	write	-	-
aom:alarmRule:delete	授予权限以删除告警规则。	write	alarmRule *	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
aom:alarm:put	授予权限以上报告警和事件。	write	-	-
aom:alarm:list	授予权限以查询告警和事件。	list	-	-
aom:alarmRule:get	授予权限以查询告警规则。	read	-	-
aom:event2AlarmRule:list	授予权限以查询事件类告警规则列表。	list	-	-
aom:event2AlarmRule:create	授予权限以创建事件类告警规则。	write	-	-
aom:event2AlarmRule:update	授予权限以更新事件类告警规则。	write	-	-
aom:event2AlarmRule:delete	授予权限以删除事件类告警规则。	write	-	-
aom:muteRule:create	授予权限以创建静默规则。	write	-	-
aom:muteRule:list	授予权限以查询静默规则列表。	list	-	-
aom:muteRule:update	授予权限以更新静默规则。	write	-	-
aom:muteRule:delete	授予权限以删除静默规则。	write	-	-
aom:actionRule:get	授予权限以查询行动规则。	read	-	-
aom:actionRule:list	授予权限以查询行动规则列表。	list	-	-
aom:actionRule:create	授予权限以创建行动规则。	write	-	-
aom:actionRule:update	授予权限以修改行动规则。	write	-	-
aom:actionRule:delete	授予权限以删除行动规则。	write	-	-

AOM的API通常对应着一个或多个授权项。**表5-254**展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-254 API 与授权项的关系

API	对应的授权项	依赖的授权项
DELETE /v1/{project_id}/aom/prometheus	aom:metric:delete	-
GET /v1/{project_id}/aom/prometheus	aom:metric:list	-
POST /v1/{project_id}/aom/prometheus	aom:metric:put	-
POST /v1/{project_id}/{prometheus_instance}/aom/api/v1/rules	aom:metric:put	-
GET /v1/{project_id}/access-code	aom:icmgr:get	-
GET /v1/{project_id}/aom/auth/grant	aom:agency:get	-
GET /v1/{project_id}/{cluster_id}/{namespace}/agents	aom:icmgr:list	-
POST /v2/{project_id}/series	aom:metric:list	-
POST /v2/{project_id}/samples	aom:metric:list	-
GET /v1/{project_id}/aom/api/v1/query_range	aom:metric:list	-
POST /v1/{project_id}/aom/api/v1/query_range	aom:metric:list	-
GET /v1/{project_id}/aom/api/v1/query	aom:metric:list	-
POST /v1/{project_id}/aom/api/v1/query	aom:metric:list	-

API	对应的授权项	依赖的授权项
GET /v1/{project_id}/aom/api/v1/label/{label_name}/values	aom:metric:list	-
GET /v1/{project_id}/aom/api/v1/labels	aom:metric:list	-
POST /v1/{project_id}/aom/api/v1/labels	aom:metric:list	-
GET /v1/{project_id}/aom/api/v1/metadata	aom:metric:list	-
POST /v1/{project_id}/ams/metrics	aom:metric:list	-
POST /v1/{project_id}/ams/metricdata	aom:metric:list	-
POST /v1/{project_id}/ams/report/metricdata	aom:metric:put	-
PUT /v1/{project_id}/inv/servicediscoveryrules	aom:discoveryRule:set	-
DELETE /v1/{project_id}/inv/servicediscoveryrules	aom:discoveryRule:delete	-
GET /v1/{project_id}/inv/servicediscoveryrules	aom:discoveryRule:list	-
POST /v2/{project_id}/alarm-rules	aom:alarmRule:create	-
GET /v2/{project_id}/alarm-rules	aom:alarmRule:list	-

API	对应的授权项	依赖的授权项
PUT /v2/{project_id}/alarm-rules	aom:alarmRule:update	-
DELETE /v2/{project_id}/alarm-rules/{alarm_rule_id}	aom:alarmRule:delete	-
GET /v2/{project_id}/alarm-rules/{alarm_rule_id}	aom:alarmRule:get	-
POST /v2/{project_id}/alarm-rules/delete	aom:alarmRule:delete	-
POST /v2/{project_id}/events	aom:alarm:list	-
POST /v2/{project_id}/events/statistic	aom:alarm:list	-
PUT /v2/{project_id}/push/events	aom:alarm:put	-
GET /v2/{project_id}/alarm-notified-histories	aom:alarm:list	-
GET /v2/{project_id}/event2alarm-rule	aom:event2AlarmRule:list	-
POST /v2/{project_id}/event2alarm-rule	aom:event2AlarmRule:create	-
PUT /v2/{project_id}/event2alarm-rule	aom:event2AlarmRule:update	-
DELETE /v2/{project_id}/event2alarm-rule	aom:event2AlarmRule:delete	-
POST /v2/{project_id}/alert/action-rules	aom:actionRule:create	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/alert/action-rules	aom:actionRule:list	-
PUT /v2/{project_id}/alert/action-rules	aom:actionRule:update	-
DELETE /v2/{project_id}/alert/action-rules	aom:actionRule:delete	-
GET /v2/{project_id}/alert/action-rules/{rule_name}	aom:actionRule:get	-
POST /v2/{project_id}/alert/mute-rules	aom:muteRule:create	-
DELETE /v2/{project_id}/alert/mute-rules	aom:muteRule:delete	-
PUT /v2/{project_id}/alert/mute-rules	aom:muteRule:update	-
GET /v2/{project_id}/alert/mute-rules	aom:muteRule:list	-
POST /v4/{project_id}/alarm-rules	aom:alarmRule:create	-
GET /v4/{project_id}/alarm-rules	aom:alarmRule:list	-
DELETE /v4/{project_id}/alarm-rules	aom:alarmRule:delete **说明** 该授权项的资源类型“alarmRule”仅对DELETE /v4/{project_id}/alarm-rules接口适用。	-

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。

AOM服务定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-255 AOM 服务支持的资源类型

资源类型	URN
alarmRule	aom:<region>:<account-id>:alarmRule:<alarm_rule_id>

条件（Condition）

AOM服务不支持在SCP中的条件键中配置服务级的条件键。

AOM服务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。

5.10.13.16 云监控服务 CES

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CES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CES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CES相关操作。

表 5-256 CES 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
ces:widgets:put	授予批量更新视图的权限。	write	dashboard	-
ces:widgets:create	授予创建视图的权限。	write	dashboard	-
ces:widgets:put	授予更新指定视图的权限。	write	dashboard	-
ces:widgets:delete	授予删除指定视图的权限。	write	dashboard	-
ces:dashboards:create	授予创建dashboard的权限。	write	dashboard	g:EnterpriseProjectId
ces:dashboards:list	授予批量查询dashboard列表的权限。	list	dashboard	g:EnterpriseProjectId
ces:dashboards:put	授予更新指定dashboard的权限。	write	dashboard	g:EnterpriseProjectId
ces:widgets:list	授予批量查询指定dashboard的视图列表权限。	list	dashboard	-
ces:widgets:create	授予创建指定dashboard的视图权限。	write	dashboard	-
ces:dashboards:delete	授予批量删除dashboard的权限	write	dashboard	g:EnterpriseProjectId
ces:widgets:get	授予查询指定视图的权限。	read	dashboard	-
ces:dashboards:delete	授予删除指定dashboard的权限。	write	dashboard	g:EnterpriseProjectId
ces:metrics:list	授予查询指标列表的权限。	list	-	-
ces:metricData:get	授予查询单条指标数据的权限。	read	-	-
ces:metricData:create	授予上报指标数据的权限。	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
ces:namespacesDimensions:listAgentDimensions	授予查询指定实例下agent维度指标信息的权限。	list	-	-
ces:namespacesDimensions:list	授予批量查询指定指标维度的权限。	list	-	-
ces:metaData:get	授予批量查询维度元数据的权限。	read	-	-
ces:metricData:list	授予批量查询指标数据的权限。	list	-	-
ces:namespacesDimensions:list	授予查询指标TopN维度的权限。	list	-	-
ces:alarms:list	授予查询告警规则列表的权限。	list	alarm	g:EnterpriseProjectId
ces:alarms:create	授予创建告警规则的权限。	write	alarm	g:EnterpriseProjectId
ces:alarms:put	授予更新告警规则的权限。	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ces:alarms:get	授予查询指定告警规则的权限。	read	alarm	g:EnterpriseProjectId
ces:alarms:putAction	授予启停告警规则的权限。	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ces:alarms:delete	授予批量删除告警规则的权限。	write	alarm	• 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
ces:alarms:listOneClickAlarms	授予查询一键告警列表的权限。	list	alarm	g:EnterpriseProjectId
ces:alarms:putOneClickAlarms	授予修改一键告警状态的权限。	write	alarm	g:EnterpriseProjectId
ces:alarms:list	授予查询告警规则列表的权限。	list	alarm	g:EnterpriseProjectId
ces:alarms:create	授予创建告警规则的权限。	write	alarm	g:EnterpriseProjectId
ces:alarms:putAlarmNotifications	授予修改告警通知信息的权限。	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ces:alarms:getPolicies	授予查询指定告警规则的策略列表权限。	read	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ces:alarms:updatePolicies	授予更新指定告警规则的策略列表权限。	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ces:alarms:getResources	授予查询指定告警规则的资源列表权限。	read	alarm	• 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
ces:alarms:addResources	授予为指定告警规则批量增加资源的权限。	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ces:alarms:deleteResources	授予为指定告警规则批量删除资源的权限。	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ces:alarms:putNotificationMaskRules	授予修改告警通知屏蔽规则的权限。	write	alarm	g:EnterpriseProjectId
ces:alarms:listNotificationMaskResources	授予查询告警通知屏蔽资源列表的权限。	list	alarm	g:EnterpriseProjectId
ces:alarms:deleteNotificationMaskRules	授予批量删除告警通知屏蔽规则的权限。	write	alarm	g:EnterpriseProjectId
ces:alarms:listNotificationMaskRules	授予查询告警通知屏蔽列表的权限。	list	alarm	g:EnterpriseProjectId
ces:alarms:createOneClickAlarms	授予创建一键告警的权限。	write	alarm	g:EnterpriseProjectId
ces:alarms:putOneClickAlarmPolicies	授予批量启停一键告警策略权限。	write	alarm	g:EnterpriseProjectId
ces:alarms:putOneClickAlarmNotifications	授予批量修改一键告警通知规则的权限。	write	alarm	g:EnterpriseProjectId
ces:alarms:deleteOneClickAlarms	授予批量删除一键告警的权限。	write	alarm	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
ces:alarms:list	授予查询告警列表的权限。	list	alarm	g:EnterpriseProjectId
ces:alarmHistory:list	授予查询告警记录列表的权限。	list	alarm	g:EnterpriseProjectId
ces:customAlarmTemplates:create	授予创建自定义告警模板的权限。	write	alarm	g:EnterpriseProjectId
ces:customAlarmTemplates:delete	授予删除指定自定义告警模板的权限。	write	alarm	g:EnterpriseProjectId
ces:customAlarmTemplates:list	授予查询自定义告警模板列表的权限。	list	alarm	g:EnterpriseProjectId
ces:customAlarmTemplates:listAssociatedAlarms	授予查询指定自定义告警模板关联的告警规则列表的权限。	read	alarm	g:EnterpriseProjectId
ces:customAlarmTemplates:put	授予更新指定自定义告警模板的权限。	write	alarm	g:EnterpriseProjectId
ces:quotas:get	授予查询配额的权限。	read	-	-
ces:quotas:get	授予批量查询配额的权限。	read	-	-
ces:events:get	授予查询指定事件详情的权限。	read	-	-
ces:events:list	授予查询事件列表的权限。	list	-	-
ces:agent:listTaskInvocations	授予批量查询指定服务器的agent任务的权限。	list	-	-
ces:agent:createAgentInvocations	授予批量创建agent任务的权限。	write	-	-
ces:events:post	授予上报事件的权限。	write	-	-
ces:resourceGroups:addResources	授予为指定资源分组批量添加关联资源的权限。	write	-	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
ces:resourceGroups:create	授予创建资源分组的权限。	write	-	g:EnterpriseProjectId
ces:resourceGroups:delete	授予删除指定资源分组的权限。	write	-	g:EnterpriseProjectId
ces:resourceGroups:deleteResources	授予为指定资源分组批量删除关联资源的权限。	write	-	g:EnterpriseProjectId
ces:resourceGroups:get	授予查询指定资源分组的权限。	read	-	g:EnterpriseProjectId
ces:resourceGroups:getServiceResources	授予查询指定资源分组指定服务类别指定维度的资源的权限。	read	-	g:EnterpriseProjectId
ces:resourceGroups:put	授予更新指定资源分组的权限。	write	-	g:EnterpriseProjectId
ces:tags:list	授予批量查询CES标签列表的权限。	list	-	-
ces:eventData:get	授予查询主机配置的权限。	list	-	-
ces:resourceGroups:list	授予查询所有资源分组的权限。	list	-	g:EnterpriseProjectId
ces:resourceGroups:get	授予查询指定资源分组的权限。	read	-	g:EnterpriseProjectId
ces:customAlarmTemplates:list	授予查询自定义告警模板列表的权限。	list	alarm	g:EnterpriseProjectId
ces:customAlarmTemplates:get	授予查询指定自定义告警模板的权限。	read	alarm	g:EnterpriseProjectId
ces:alarms:create	授予创建告警规则的权限。	write	alarm	g:EnterpriseProjectId
ces:dashboards:put	授予更新云服务看板的权限	write	dashboard	-
ces:namespacesDimensions:list	授予查询指标TopN维度的权限。	list	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
ces:namespacesDimensions:list	授予批量查询指定指标维度的权限。	list	-	-

CES的API通常对应着一个或多个授权项。表5-257展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-257 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}/dashboards	ces:dashboards:create	-
GET /v2/{project_id}/dashboards	ces:dashboards:list	-
PUT /v2/{project_id}/dashboards/{dashboard_id}	ces:dashboards:put	-
GET /v2/{project_id}/dashboards/{dashboard_id}/widgets	ces:widgets:list	-
POST /v2/{project_id}/dashboards/{dashboard_id}/widgets	ces:widgets:create	-
POST /v2/{project_id}/dashboards/batch-delete	ces:dashboards:delete	-
GET /v2/{project_id}/widgets/{widget_id}	ces:widgets:get	-
DELETE /v2/{project_id}/widgets/{widget_id}	ces:widgets:delete	-
POST /v2/{project_id}/widgets/batch-update	ces:widgets:put	-
GET /V1.0/{project_id}/metrics	ces:metrics:list	-
GET /V1.0/{project_id}/metric-data	ces:metricData:get	ces:metricData:list
POST /V1.0/{project_id}/metric-data	ces:metricData:create	-
POST /V1.0/{project_id}/batch-query-metric-data	ces:metricData:list	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/instances/{instance_id}/agent-dimensions	ces:namespacesDimensions:listAgentDimensions	ces:namespacesDimensions:list
GET /V1.0/{project_id}/alarms	ces:alarms:list	-
POST /V1.0/{project_id}/alarms	ces:alarms:create	-
PUT /V1.0/{project_id}/alarms/{alarm_id}	ces:alarms:put	ces:alarmsonoff:put
DELETE /V1.0/{project_id}/alarms/{alarm_id}	ces:alarms:delete	-
GET /V1.0/{project_id}/alarms/{alarm_id}	ces:alarms:get	ces:alarms:list
PUT /V1.0/{project_id}/alarms/{alarm_id}/action	ces:alarms:putAction	ces:alarms:put
GET /v2/{project_id}/alarms	ces:alarms:list	-
POST /v2/{project_id}/alarms	ces:alarms:create	-
PUT /v2/{project_id}/alarms/{alarm_id}/notifications	ces:alarms:putAlarmNotifications	ces:alarms:put
GET /v2/{project_id}/alarms/{alarm_id}/policies	ces:alarms:getPolicies	ces:alarms:get
PUT /v2/{project_id}/alarms/{alarm_id}/policies	ces:alarms:updatePolicies	ces:alarms:put
GET /v2/{project_id}/alarms/{alarm_id}/resources	ces:alarms:getResources	-
POST /v2/{project_id}/alarms/{alarm_id}/resources/batch-create	ces:alarms:addResources	ces:alarms:put
POST /v2/{project_id}/alarms/{alarm_id}/resources/batch-delete	ces:alarms:delete	ces:alarms:put
POST /v2/{project_id}/alarms/action	ces:alarms:putAction	ces:alarms:put
PUT /v2/{project_id}/notification-masks	ces:alarms:putNotificationMaskRules	ces:notificationMasks:update
PUT /v2/{project_id}/notification-masks/{notification_mask_id}	ces:alarms:putNotificationMaskRules	ces:notificationMasks:update

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/notification-masks/{notification_mask_id}/resources	ces:alarms:listNotificationMaskResources	ces:notificationMasks:list
POST /v2/{project_id}/notification-masks/batch-delete	ces:alarms:deleteNotificationMaskRules	ces:notificationMasks:delete
POST /v2/{project_id}/notification-masks/batch-query	ces:alarms:listNotificationMaskRules	ces:notificationMasks:list
POST /v2/{project_id}/notification-masks/batch-update	ces:alarms:putNotificationMaskRules	ces:notificationMasks:update
GET /v2/{project_id}/one-click-alarms	ces:alarms:listOneClickAlarms	ces:oneClickAlarms:list
POST /v2/{project_id}/one-click-alarms	ces:alarms:createOneClickAlarms	ces:oneClickAlarms:post
PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarm-rules/action	ces:alarms:putOneClickAlarms	ces:oneClickAlarms:put
GET /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarms	ces:alarms:listOneClickAlarms	ces:oneClickAlarms:list
PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarms/{alarm_id}/policies/action	ces:alarms:putOneClickAlarmPolicies	ces:oneClickAlarms:put
PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/notifications	ces:alarms:putOneClickAlarmNotifications	ces:oneClickAlarms:updateNotifications
POST /v2/{project_id}/one-click-alarms/batch-delete	ces:alarms:deleteOneClickAlarms	ces:oneClickAlarms:delete
POST /v2/{project_id}/alarms/batch-delete	ces:alarms:deleteResources	ces:alarms:put
GET /V1.0/{project_id}/alarm-histories	ces:alarmHistory:list	-
GET /v2/{project_id}/alarm-histories	ces:alarmHistory:list	-
POST /V1.0/{project_id}/alarm-template	ces:customAlarmTemplates:create	-
POST /v2/{project_id}/alarm-templates	ces:customAlarmTemplates:create	-

API	对应的授权项	依赖的授权项
DELETE /V1.0/{project_id}/alarm-template/{template_id}	ces:customAlarmTemplates:delete	-
POST /v2/{project_id}/alarm-templates/batch-delete	ces:customAlarmTemplates:delete	-
GET /v2/{project_id}/alarm-templates/{template_id}	ces:customAlarmTemplates:get	ces:customAlarmTemplates:list
GET /V1.0/{project_id}/alarm-template	ces:customAlarmTemplates:list	-
GET /v2/{project_id}/alarm-templates	ces:customAlarmTemplates:list	-
GET /v2/{project_id}/alarm-templates/{template_id}/association-alarms	ces:customAlarmTemplates:listAssociatedAlarms	ces:customAlarmTemplates:list
PUT /V1.0/{project_id}/alarm-template/{template_id}	ces:customAlarmTemplates:put	-
PUT /v2/{project_id}/alarm-templates/{template_id}	ces:customAlarmTemplates:put	-
GET /V1.0/{project_id}/quotas	ces:quotas:get	-
GET /V1.0/{project_id}/event/{event_name}	ces:events:get	-
GET /V1.0/{project_id}/events	ces:events:list	-
GET /v3/{project_id}/agent-invocations	ces:agent:listTaskInvocations	ces:taskInvocation:get
POST /v3/{project_id}/agent-invocations/batch-create	ces:agent:createAgentInvocations	ces:taskInvocation:post
POST /V1.0/{project_id}/events	ces:events:post	-
POST /v2/{project_id}/resource-groups/{group_id}/resources/batch-create	ces:resourceGroups:addResources	ces:resourceGroups:put
POST /V1.0/{project_id}/resource-groups	ces:resourceGroups:create	-
POST /v2/{project_id}/resource-groups	ces:resourceGroups:create	-
DELETE /V1.0/{project_id}/resource-groups/{group_id}	ces:resourceGroups:delete	-
POST /v2/{project_id}/resource-groups/batch-delete	ces:resourceGroups:delete	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/resource-groups/{group_id}/resources/batch-delete	ces:resourceGroups:deleteResources	ces:resourceGroups:put
GET /V1.0/{project_id}/resource-groups/{group_id}	ces:resourceGroups:get	-
GET /v2/{project_id}/resource-groups/{group_id}	ces:resourceGroups:get	-
GET /v2/{project_id}/resource-groups/{group_id}/services/{service}/resources	ces:resourceGroups:getServiceResources	ces:resourceGroups:get
GET /V1.0/{project_id}/resource-groups	ces:resourceGroups:list	ces:resourceGroups:get
GET /v2/{project_id}/resource-groups	ces:resourceGroups:list	ces:resourceGroups:get
PUT /V1.0/{project_id}/resource-groups/{group_id}	ces:resourceGroups:put	-
PUT /v2/{project_id}/resource-groups/{group_id}	ces:resourceGroups:put	-
GET /v2/{project_id}/{resource_type}/tags	ces:tags:list	-
GET /V1.0/{project_id}/event-data	ces:eventData:get	ces:sapEventData:list
POST /v3/{project_id}/agent-status/batch-query	ces:agent:listStatuses	-

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。

CES定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-258 CES 支持的资源类型

资源类型	URN
alarm	ces:<region>:<account-id>:alarm:<alarm-id>
dashboard	ces:<region>:<account-id>:dashboard:<dashboard-id>

条件（Condition）

CES服务不支持在SCP中的条件键中配置服务级的条件键。

CES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。

5.10.13.17 IAM 身份代理

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IAM身份代理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IAM身份代理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IAM身份代理的相关操作。

表 5-259 IAM 身份代理支持的授权项

授权项	描述	访问级别	资源类型（*为必须）	条件键
AgenciesAnywhere:trustAnchor:create	授予创建信任锚的权限。	Write	-	• g:TagKeys • g:RequestTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
AgenciesAnywhere:trustAnchor:enable	授予启用信任锚的权限。	Write	trustAnchor *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:trustAnchor:disable	授予禁用信任锚的权限。	Write	trustAnchor *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:trustAnchor:update	授予修改信任锚的权限。	Write	trustAnchor *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:trustAnchor:get	授予查询信任锚详情的权限。	Read	trustAnchor *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:trustAnchor:list	授予列举信任锚的权限。	List	-	-
AgenciesAnywhere:trustAnchor:delete	授予删除信任锚的权限。	Write	trustAnchor *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:trustAnchor:putNotificationSettings	授予设置信任锚点的通知设置的权限。	Write	trustAnchor *	g:ResourceTag/<tag-key>
AgenciesAnywhere:trustAnchor:resetNotificationSettings	授予重置信任锚点的通知设置的权限。	Write	trustAnchor *	g:ResourceTag/<tag-key>
AgenciesAnywhere:profile:create	授予创建配置的权限。	Write	-	• g:TagKeys • g:RequestTag/<tag-key>
AgenciesAnywhere:profile:enable	授予启用配置的权限。	Write	profile *	-
			-	g:ResourceTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
AgenciesAnywhere:profile:disable	授予禁用配置的权限。	Write	profile *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:profile:update	授予修改配置的权限。	Write	profile *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:profile:get	授予查询配置详情的权限。	Read	profile *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:profile:list	授予列举配置的权限。	List	-	-
AgenciesAnywhere:profile:delete	授予删除配置的权限。	Write	profile *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere::listResourcesByTag	授予根据标签查询资源列表或资源数量的权限。	List	-	• g:TagKeys • g:RequestTag/<tag-key>
AgenciesAnywhere::tagResource	授予标记指定资源的权限。	Tagging	trustAnchor	g:ResourceTag/<tag-key>
			profile	g:ResourceTag/<tag-key>
			crl	g:ResourceTag/<tag-key>
			-	• g:TagKeys • g:RequestTag/<tag-key>
AgenciesAnywhere::unTagResource	授予取消标记指定资源的权限。	Tagging	trustAnchor	g:ResourceTag/<tag-key>
			profile	g:ResourceTag/<tag-key>
			crl	g:ResourceTag/<tag-key>
			-	• g:TagKeys • g:RequestTag/<tag-key>

授权项	描述	访问级别	资源类型（*为必须）	条件键
AgenciesAnywhere::listTagsForResource	授予查询指定资源标签的权限。	List	profile	g:ResourceTag/<tag-key>
			crl	g:ResourceTag/<tag-key>
			trustAnchor	g:ResourceTag/<tag-key>
AgenciesAnywhere::listTags	授予查询资源标签的权限。	List	-	-
AgenciesAnywhere:crl:import	授予导入证书吊销列表的权限。	Write	-	• g:TagKeys • g:RequestTag/<tag-key>
AgenciesAnywhere:crl:enable	授予启用证书吊销列表的权限。	Write	crl *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:crl:disable	授予禁用证书吊销列表的权限。	Write	crl *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:crl:update	授予更新证书吊销列表的权限。	Write	crl *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:crl:get	授予查询证书吊销列表的权限。	Read	crl *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:crl:list	授予获取证书吊销列表表单的权限。	List	-	-
AgenciesAnywhere:crl:listForTrustAnchor	授予查询指定信任锚的证书吊销列表的权限。	List	trustAnchor *	g:ResourceTag/<tag-key>
AgenciesAnywhere:crl:delete	授予删除证书吊销列表的权限。	Write	crl *	-
			-	g:ResourceTag/<tag-key>

资源类型（Resource）

资源类型（Resource）表示策略所作用的资源。如**表5-260**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身份代理定义了以下可以在策略的Resource元素中使用的资源类型。

表 5-260 IAM 身份代理支持的资源类型

资源类型	URN
profile	AgenciesAnywhere::<account-id>:profile:<profile-id>
crl	AgenciesAnywhere::<account-id>:crl:<crl-id>
trustAnchor	AgenciesAnywhere::<account-id>:trustAnchor:<trust-anchor-id>

条件（Condition）

IAM身份代理服务不支持在策略中的条件键中配置服务级的条件键。IAM身份代理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。

5.10.14 用户服务

5.10.14.1 费用中心

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。
- **“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。
- 如果此列条件键没有值（-），表示此操作不支持指定条件键。

您可以在SCP语句的Action元素中指定以下费用中心的相关操作。

表 5-261 支持的授权项

授权项	功能说明	访问级别	资源类型	条件键
billing:balance:update	提现，充值/还款，余额预警	write	-	-
billing:balance:view	查看收支明细，付款历史记录，消费配额，调账记录，欠费查询	list	-	g:EnterpriseProjectId
billing:bill:update	账单设置	write	-	-
billing:bill:view	查看账单、本月消费、消费走势	list	-	g:EnterpriseProjectId
billing:resourcePackages:view	查看资源包，剩余量汇总，使用明细查询/导出	list	-	-
billing:resourcePackages:update	资源包剩余量预警设置	write	-	-
billing:billDetail:update	账单明细设置	write	-	g:EnterpriseProjectId
billing:billDetail:view	查看账单明细	read	-	g:EnterpriseProjectId
billing:contract:update	查看线下合同	write	-	-
billing:coupon:view	查看优惠券，激活代金券	read	-	-
billing:contract:viewDiscount	查看商务折扣	read	-	-
billing:invoice:manage	发票管理	write	-	-
billing:invoice:view	查看开票记录，发票详情	read	-	-
billing:invoice:export	导出发票信息，下载发票	read	-	-
billing:order:pay	支付订单	write	-	g:EnterpriseProjectId

授权项	功能说明	访问级别	资源类型	条件键
billing:order:view	查看订单信息、查看按需套餐包	list	-	g:EnterpriseProjectId
billing:subscription:renew	续费、设置自动续费、设置到期策略、按需转包年/包月	write	-	g:EnterpriseProjectId
billing:subscription:view	查看续费管理信息，查询可按需转包年/包月资源列表	list	-	g:EnterpriseProjectId
billing:subscription:unsubscribe	查看可退订资源，退订资源	write	-	g:EnterpriseProjectId
billing:bill:export	导出账单概览	read	-	g:EnterpriseProjectId
billing:billDetail:export	导出账单明细	read	-	g:EnterpriseProjectId
billing:balance:export	导出收支明细、付款记录	read	-	-
billing:consumption:view	查看企业项目消耗分析	read	-	-
billing::activeEPFinance	开通企业项目功能	write	-	-
billing::activeEPFundQuota	开通/关闭企业项目资金配额功能	write	-	-
billing::viewEPFundQuota	查询企业项目资金配额	read	-	-
billing::updateEPFundQuota	修改企业项目资金配额	write	-	-
billing::listEPFundQuotaHistory	查询企业项目资金配额调整记录	read	-	-
billing::updateEPGroup	修改企业项目群	write	-	-
billing::viewEPGroup	查看企业项目群	read	-	-

资源类型（Resource）

费用中心不支持在SCP中的资源中指定资源进行权限控制。如需允许访问费用中心，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）

费用中心不支持在SCP中的条件键中配置服务级的条件键。费用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。

5.10.14.2 成本中心

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。成本中心仅支持对所有资源有效，通配符号*表示所有。
  - 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。
- **“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。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

您可以在SCP语句的Action元素中指定以下成本中心的相关操作。

表 5-262 支持的授权项

操作项	描述	访问级别	资源类型	条件键
costCenter:costAnalysis:listCosts	授予查看成本分析的权限。	read	-	-
costCenter:costAnalysis:configReport	授予设置成本报告，新建、修改、删除自定义成本报告的权限。	write	-	-

操作项	描述	访问级别	资源类型	条件键
costCenter:costAnalysis:listReports	授予查看成本报告列表的权限。	read	-	-
costCenter:costDetail:listCostDetails	授予查询成本明细的权限。	read	-	-
costCenter:budget:configBudget	授予设置预算，包括新建、修改、删除预算的权限。	write	-	-
costCenter:budget:viewBudget	授予查看预算信息，包括查看预算列表、查看预算详情的权限。	read	-	-
costCenter:budget:deleteBudgetReport	授予删除预算报告的权限。	write	-	-
costCenter:budget:configBudgetReport	授予新增、修改预算报告的权限。	write	-	-
costCenter:budget:viewBudgetReport	授予查看预算报告，包括预算报告列表和详情的权限。	read	-	-
costCenter:costAnomalyDetection:deleteMonitor	授予删除监视器的权限。	write	-	-
costCenter:costAnomalyDetection:configMonitor	授予新增、编辑监控器的权限。	write	-	-
costCenter:costAnomalyDetection:viewMonitor	授予查看监视器列表和异常成本记录的权限。	read	-	-
costCenter:costAnomalyDetection:configMonitorAlert	授予设置异常成本监控提醒的权限。	write	-	-
costCenter:costAnomalyDetection:viewMonitorAlert	授予查看异常成本监控提醒的权限。	read	-	-

操作项	描述	访问级别	资源类型	条件键
costCenter:costAnomalyDetection:provideFeedback	授予提供异常成本评估的权限。	read	-	-
costCenter:recommendation:viewRecommendationSummary	授予查看成本建议概览的权限。	read	-	-
costCenter:recommendation:viewRecommendationSubscription	授予查询成本建议订阅的权限。	read	-	-
costCenter:recommendation:configRecommendationSubscription	授予设置/删除成本建议订阅的权限。	write	-	-
costCenter:recommendation:viewYearlyMonthlyRecommendation	授予查看按需转包年包月成本优化评估的权限。	read	-	-
costCenter:recommendation:viewResourcePkgRecommendation	授予查看资源包购买建议的权限。	read	-	-
costCenter:recommendation:viewResourceOptimizeRecommendation	授予查看空闲资源优化建议的权限。	read	-	-
costCenter:recommendation:configPreference	授予设置空闲资源规则的权限。	write	-	-
costCenter:costTag:updateStatus	授予激活/取消激活成本标签的权限。	write	-	-
costCenter:costTag:listCostTags	授予查看成本标签的权限。	read	-	-

操作项	描述	访问级别	资源类型	条件键
costCenter:costCategory:deleteCostCategory	授予删除成本单元的权限。	write	-	-
costCenter:costCategory:configCostCategory	授予设置成本单元，包括新建、编辑成本单元的权限。	write	-	-
costCenter:costCategory:viewCostCategory	授予查看成本单元，包括成本单元列表和详情的权限。	read	-	-
costCenter:resourcePackage:viewResourcePkgAnalysis	授予查看资源包使用率/覆盖率分析的权限。	read	-	-
costCenter:savingsPlans:viewSavingsPlansAnalysis	授予查看节省计划使用率/覆盖率分析的权限。	read	-	-
costCenter:reserveInstance:viewRIAnalysis	授予查看预留实例使用率/覆盖率分析的权限。	read	-	-
costCenter:savingsPlans:viewSavingsPlans	授予查看节省计划实例的权限。	read	-	-
costCenter:recommendation:viewSavingsPlansRecommendation	授予查看节省计划购买建议的权限。	read	-	-
costCenter::updateCostConfig	授予开启成本特性的权限。	write	-	-
costCenter:preference:delete	授予关闭成本特性的权限。	write	-	-
costCenter:costdetailreport:viewReportTask	授予查看成本明细OBS导出任务列表的权限。	read	-	-
costCenter:costdetailreport:configReportTask	授予创建/修改/删除成本明细OBS导出任务的权限。	write	-	-
costCenter:helper:listCostAllocations	授予查看成本分配占比统计的权限。	list	-	-

操作项	描述	访问级别	资源类型	条件键
costCenter:helper:viewCostRating	授予查看成熟度评分的权限。	read	-	-

资源类型（Resource）

成本中心不支持在SCP中的资源中指定资源进行权限控制。如需允许访问成本中心，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）

成本中心不支持在SCP中的条件键中配置服务级的条件键。成本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。

5.10.14.3 账号中心

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。账号中心仅支持对所有资源有效，通配符号*表示所有。
  - 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。
- **“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。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

您可以在SCP语句的Action元素中指定以下账号中心的相关操作。

表 5-263 支持的授权项

授权项	功能说明	访问级别	资源类型	条件键
account:accountInfo:update	更新账号信息，包括实名认证、基本信息、首选项等。	write	-	-
account:cps:view	云推官查看奖励推广计划推广数据。	read	-	-
account:cps:update	加入奖励推广计划。	write	-	-
account:privilege:view	查看我的特权、实物奖品。	read	-	-
account::close	关闭华为云业务、注销华为云业务、恢复华为云业务。	write	-	-

资源类型（Resource）

账号中心不支持在SCP中的资源中指定资源进行权限控制。如需允许访问账号中心，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）

账号中心不支持在SCP中的条件键中配置服务级的条件键。账号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。

5.10.14.4 企业中心

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。企业中心仅支持对所有资源有效，通配符号*表示所有。
  - 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。
- **“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。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

您可以在SCP语句的Action元素中指定以下企业中心的相关操作。

表 5-264 支持的授权项

授权项	功能说明	访问级别	资源类型	条件键
businessUnitCenter:bill:update	企业中心子账号账单操作	write	-	-
businessUnitCenter:bill:view	企业中心子账号账单查看	read	-	-
businessUnitCenter:billDetail:update	企业中心子账号账单明细操作	write	-	-
businessUnitCenter:billDetail:view	企业中心子账号账单明细查看	read	-	-
businessUnitCenter:businesUnitFinance:update	修改企业组织财务信息	write	-	-
businessUnitCenter:businesUnitFinance:view	查看企业组织财务信息	read	-	-
businessUnitCenter:businesUnit:update	修改企业组织与子账号	write	-	-
businessUnitCenter:businesUnit:view	查看企业组织与子账号	read	-	-
businessUnitCenter:businesUnitBudget:update	操作企业组织预算	write	-	-
businessUnitCenter:businesUnitBudget:view	查看企业组织预算	read	-	-
businessUnitCenter:businesUnitPolicy:update	修改企业组织控制策略	write	-	-
businessUnitCenter::active	开通与关闭企业中心功能	write	-	-

资源类型（Resource）

企业中心不支持在SCP中的资源中指定资源进行权限控制。如需允许访问企业中心，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）

企业中心不支持在SCP中的条件键中配置服务级的条件键。企业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。

5.10.14.5 消息中心

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。消息中心仅支持对所有资源有效，通配符号*表示所有。
- **“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。
  - 如果此列条件键没有值（-），表示此操作不支持指定条件键。

您可以在SCP语句的Action元素中指定以下消息中心的相关操作。

表 5-265 支持的授权项

授权项	功能说明	访问级别	资源类型	条件键
messageCenter:financeMsg:view	• 可查看和操作财务分类消息。 • 可查看**消息接收配置**和**语音接收配置**信息。	read	*	-
messageCenter:financeMsg:subscribe	• 可查看**消息接收配置**和**语音接收配置**信息。 • 可修改财务分类相关的消息接收方式。	write	*	-

授权项	功能说明	访问级别	资源类型	条件键
messageCenter:financeMsg:delete	• 可查看**消息接收配置**和**语音接收配置**信息。	read	*	-
messageCenter:filingMsg:view	• 可查看和操作备案分类消息。 • 可查看**消息接收配置**和**语音接收配置**信息。	read	*	-
messageCenter:filingMsg:subscribe	• 可查看**消息接收配置**和**语音接收配置**信息。 • 可修改备案分类相关的消息接收方式。	write	*	-
messageCenter:filingMsg:delete	• 可查看**消息接收配置**和**语音接收配置**信息。	read	*	-
messageCenter:contractMsg:view	• 可查看和操作合同分类消息。 • 可查看**消息接收配置**和**语音接收配置**信息。	read	*	-
messageCenter:contractMsg:subscribe	• 可查看**消息接收配置**和**语音接收配置**信息。 • 可修改合同分类相关的消息接收方式。	write	*	-
messageCenter:contractMsg:delete	• 可查看**消息接收配置**和**语音接收配置**信息。	read	*	-
messageCenter:campaignsMsg:view	• 可查看和操作活动分类消息。 • 可查看**消息接收配置**和**语音接收配置**信息。	read	*	-
messageCenter:campaignsMsg:subscribe	• 可查看**消息接收配置**和**语音接收配置**信息。 • 可修改活动分类相关的消息接收方式。	write	*	-
messageCenter:campaignsMsg:delete	• 可查看**消息接收配置**和**语音接收配置**信息。	read	*	-
messageCenter:productMsg:view	• 可查看和操作产品分类消息。 • 可查看**消息接收配置**和**语音接收配置**信息。	read	*	-
messageCenter:productMsg:subscribe	• 可查看**消息接收配置**和**语音接收配置**。 • 可修改产品分类相关的消息接收方式。	write	*	-
messageCenter:productMsg:delete	• 可查看**消息接收配置**和**语音接收配置**信息。	read	*	-

授权项	功能说明	访问级别	资源类型	条件键
messageCenter:omMsg:view	• 可查看和操作运维分类消息。 • 可查看**消息接收配置**和**语音接收配置**信息。	read	*	-
messageCenter:omMsg:subscribe	• 可查看**消息接收配置**和**语音接收配置**信息。 • 可修改运维分类相关的消息接收方式。	write	*	-
messageCenter:omMsg:delete	• 可查看**消息接收配置**和**语音接收配置**信息。	read	*	-
messageCenter:securityMsg:view	• 可查看和操作安全分类消息。 • 可查看**消息接收配置**和**语音接收配置**信息。	read	*	-
messageCenter:securityMsg:subscribe	• 可查看**消息接收配置**和**语音接收配置**信息。 • 可修改安全分类相关的消息接收方式。	write	*	-
messageCenter:securityMsg:delete	• 可查看**消息接收配置**和**语音接收配置**信息。	read	*	-
messageCenter:recipient:view	• 可查看**消息接收配置**、和**接收人管理**下相关信息。	read	*	-
messageCenter:recipient:update	• 可查看**消息接收配置和**信息。**接收人管理**界面可新增接收人。（与messageCenter:recipient:view搭配使用）	write	*	-

资源类型（Resource）

消息中心不支持在SCP中的资源中指定资源进行权限控制。如需允许访问消息中心，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）

消息中心不支持在SCP中的条件键中配置服务级的条件键。消息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。

5.10.14.6 客户运营能力

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BSS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BSS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BSS的相关操作。

表 5-266 BSS 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
billing:contract:viewDiscount	授予查看商务折扣的权限	read	-	-
billing:balance:view	授予查看收支明细，付款历史记录，消费配额，调账记录，欠费查询的权限	list	-	-
billing:coupon:view	授予查看优惠券、储值卡、激活代金券的权限	read	-	-
billing:order:view	授予查看订单信息、查看按需套餐包的权限	list	-	-
billing:order:pay	授予支付订单的权限	write	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
billing:subscription:renew	授予续费、设置自动续费、设置到期策略、按需转包年/包月的权限	write	-	-
billing:subscription:unsubscribe	授予查看可退订资源，退订资源，取消发货，硬件退换货的权限	write	-	-
billing:resourcePackages:view	授予查看资源包，剩余量汇总，使用明细查询/导出的权限	list	-	-
billing:billDetail:view	授予查看账单明细的权限	read	-	-
billing:bill:view	授予查看账单、本月消费、近7天扣费资源，消费走势的权限	list	-	-
costCenter:costAnalysis:listCosts	授予查看成本分析的权限	read	-	-
Billing::activeEPFinance	授予开通企业项目功能的权限	write	-	-
businessUnitCenter:businessUnit:view	授予查看组织与账号的权限	read	-	-
billing:invoice:update	授予发票管理，提供索取发票、管理发票抬头和收件地址的权限。	write	-	-

BSS 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 5-267 API 与授权项的关系（当前 API 均无需要依赖的授权项）

场景	子场景	接口名称	接口URL	授权项	授权项描述
管理产品	查询商品价格	查询按需产品价格	POST /v2/bills/ratings/on-demand-resources	billing:contract:viewDiscount	查看折扣、价格信息。

场景	子场景	接口名称	接口URL	授权项	授权项描述
		查询包年/包月产品价格	POST /v2/bills/ratings/period-resources/subscribe-rate	billing:contract:viewDiscount	查看折扣、价格信息
		查询包年/包月资源的续订金额	POST /v2/bills/ratings/period-resources/renew-rate	billing:contract:viewDiscount	查看折扣、价格信息。
管理账户	管理账户	查询账户余额	GET /v2/accounts/customer-accounts/balances	billing:balance:view	查看账户信息。
管理交易	管理优惠券	查询优惠券列表	GET /v2/promotions/benefits/coupons	billing:coupon:view	查看优惠券、现金券、代金券。
	管理包年/包月订单	查询订单列表	GET /v2/orders/customer-orders	billing:order:view	查看订单信息。
		查询订单详情	GET /v2/orders/customer-orders/details/{order_id}	billing:order:view	查看订单信息。
		支付包年/包月产品订单	POST /v2/orders/customer-orders/pay	billing:order:pay	订单支付。
		查询订单可用折扣	GET /v2/orders/customer-orders/order-discounts	billing:contract:viewDiscount	查看折扣、价格信息。

场景	子场景	接口名称	接口URL	授权项	授权项描述
		支付包年/包月产品订单	POST /v3/orders/customer-orders/pay	billing:order:pay	订单支付。
		查询退款订单的金额详情	GET /v2/orders/customer-orders/refund-orders	billing:order:view	查看订单信息。
	管理包年/包月资源	查询客户包年/包月资源列表	POST /v2/orders/suscriptions/resources/query	• billing:subscription:view • billing:order:view（待下线）	查看订单信息。
		续订包年/包月资源	POST /v2/orders/subscriptions/resources/renew	billing:subscription:renew	下单、取消订单、修改收货地址。
		退订包年/包月资源	POST /v2/orders/subscriptions/resources/unsubscribe	billing:subscription:unsubscribe	下单、取消订单、修改收货地址。**云服务粒度退订鉴权常见问题.**
		设置包年/包月资源自动续费	POST /v2/orders/subscriptions/resources/autorenew/**	billing:subscription:renew	下单、取消订单、修改收货地址。
		取消包年/包月资源自动续费	DELETE /v2/orders/subscriptions/resources/autorenew/{resource_id}	billing:subscription:renew	下单、取消订单、修改收货地址。

场景	子场景	接口名称	接口URL	授权项	授权项描述
		设置或取消包年/包月资源到期转按需	POST /v2/orders/subscriptions/resources/to-on-demand	billing:subscription:renew	下单、取消订单、修改收货地址。
	管理资源包	查询资源包列表	POST /v3/payments/free-resources/query	billing:resourcePackages:view	查看账单、月度成本、用量明细、成本管理、收支以及总览页面的费用走势。
		查询资源包使用明细	GET /v2/bills/customer-bills/free-resources-usage-records	• billing:resourcePackages:view • billing:billDetail:view（待下线）	查看消费明细、资源消费、账单分析、付款历史记录。
		查询资源包使用量	POST /v2/payments/free-resources/usages/details/query	billing:resourcePackages:view	查看账单、月度成本、用量明细、成本管理、收支以及总览页面的费用走势。
管理账单	管理账单	查询资源详单	POST /v2/bills/customer-bills/res-records/query	billing:billDetail:view	查看消费明细、资源消费、账单分析、付款历史记录。
		查询汇总账单	GET /v2/bills/customer-bills/monthly-sum	billing:bill:view	查看账单、月度成本、用量明细、成本管理、收支以及总览页面的费用走势。

场景	子场景	接口名称	接口URL	授权项	授权项描述
		查询资源消费记录	GET /v2/bills/customer-bills/res-fee-records	• billing:billDetail:view • billing:bill:view（待下线）	查看账单、月度成本、用量明细、成本管理、收支以及总览页面的费用走势。
管理成本	管理成本	查询成本数据	POST /v4/costs/cost-analysed-bills/query	costCenter:costAnalysis:listCosts	查看成本分析。
管理企业	管理企业项目	开通客户企业项目权限	POST /v2/enterprises/enterprise-projects/authority	Billing::activeEPFinance	开通企业项目功能。
	管理企业多账号	查询企业子账号列表	GET /v2/enterprises/multi-accounts/sub-customers	businessUnitCenter:businessUnit:view	企业中心组织与账号查看权限。
管理发票	管理发票	查询发票列表	GET /v1.0/{domain_id}/payments/intl-invoices	billing:invoice:manage	申请发票、查看信息。

资源类型（Resource）

BSS 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**BSS**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）

BSS服务不支持在SCP中的条件键中配置服务级的条件键。BSS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。

5.10.15 迁移

5.10.15.1 对象存储迁移服务 OMS

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OMS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OMS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OMS的相关操作。

表 5-268 OMS 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
oms:task:list	授予查询任务列表权限	list	task	-
oms:task:create	授予创建任务权限	write	task	-
oms:task:get	授予查询指定任务权限	read	task	-
oms:task:delete	授予删除任务权限	write	task	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
oms:task:update	授予更新指定任务权限	write	task	-
oms:synctask:list	授予查询同步任务列表权限	list	synctask	-
oms:synctask:create	授予创建同步任务权限	write	synctask	-
oms:synctask:get	授予查询指定同步任务权限	read	synctask	-
oms:synctask:delete	授予删除指定同步任务权限	write	synctask	-
oms:synctask:statistics	授予查询指定同步任务统计信息权限	read	synctask	-
oms:synctask:update	授予更新指定同步任务权限	write	synctask	-
oms:synctask:createEvent	授予创建指定同步任务事件权限	write	synctask	-
oms:taskgroup:create	授予创建任务组权限	write	taskgroup	-
oms:taskgroup:list	授予查询任务组列表权限	list	taskgroup	-
oms:taskgroup:get	授予查询指定任务组信息权限	read	taskgroup	-
oms:taskgroup:delete	授予删除指定任务组权限	write	taskgroup	-
oms:taskgroup:update	授予更新指定任务组权限	write	taskgroup	-
oms::listObjects	授予查询桶的对象列表权限	list	-	-
oms::checkCdnInfo	授予检查桶的CDN连通性权限	read	-	-
oms::listBuckets	授予查询桶列表权限	list	-	-
oms::listBucketRegions	授予查询桶区域列表的权限	list	-	-
oms::checkBucketPrefix	授予检查桶对象前缀的权限	read	-	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
oms::listCloudRegions	授权查询源端厂商支持区域列表的权限	list	-	-
oms::listCloudTypes	授予查询支持云厂商列表的权限	list	-	-

OMS的API通常对应着一个或多个授权项。表5-269展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-269 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}/tasks	oms:task:list	-
POST /v2/{project_id}/tasks	oms:task:create	-
GET /v2/{project_id}/tasks/{task_id}	oms:task:get	-
DELETE /v2/{project_id}/tasks/{task_id}	oms:task:delete	-
POST /v2/{project_id}/tasks/{task_id}/stop	oms:task:update	-
POST /v2/{project_id}/tasks/{task_id}/start	oms:task:update	-
PUT /v2/{project_id}/tasks/{task_id}/bandwidth-policy	oms:task:update	-
PUT /v2/{project_id}/tasks/{task_id}/access-keys	oms:task:update	-
GET /v2/{project_id}/sync-tasks	oms:synctask:list	-
POST /v2/{project_id}/sync-tasks	oms:synctask:create	-
GET /v2/{project_id}/sync-tasks/{sync_task_id}	oms:synctask:get	-
DELETE /v2/{project_id}/sync-tasks/{sync_task_id}	oms:synctask:delete	-
GET /v2/{project_id}/sync-tasks/{sync_task_id}/statistics	oms:synctask:statistics	-

API	对应的授权项	依赖的授权项
POST /v2/{project_id}/sync-tasks/{sync_task_id}/stop	oms:synctask:update	-
POST /v2/{project_id}/sync-tasks/{sync_task_id}/start	oms:synctask:update	-
POST /v2/{project_id}/sync-tasks/{sync_task_id}/events	oms:synctask:createEvent	-
POST /v2/{project_id}/taskgroups	oms:taskgroup:create	-
GET /v2/{project_id}/taskgroups	oms:taskgroup:list	-
GET /v2/{project_id}/taskgroups/{group_id}	oms:taskgroup:get	-
DELETE /v2/{project_id}/taskgroups/{group_id}	oms:taskgroup:delete	-
PUT /v2/{project_id}/taskgroups/{group_id}/stop	oms:taskgroup:update	-
PUT /v2/{project_id}/taskgroups/{group_id}/start	oms:taskgroup:update	-
PUT /v2/{project_id}/taskgroups/{group_id}/retry	oms:taskgroup:update	-
PUT /v2/{project_id}/taskgroups/{group_id}/update	oms:taskgroup:update	-
POST /v2/{project_id}/objectstorage/buckets/objects	oms::listObjects	-
POST /v2/{project_id}/objectstorage/buckets/cdn-info	oms::checkCdnInfo	-
POST /v2/{project_id}/objectstorage/buckets	oms::listBuckets	-
POST /v2/{project_id}/objectstorage/buckets/regions	oms::listBucketRegions	-
POST /v2/{project_id}/objectstorage/buckets/prefix	oms::checkBucketPrefix	-
GET /v2/{project_id}/objectstorage/data-center	oms::listCloudRegions	-

API	对应的授权项	依赖的授权项
GET /v2/{project_id}/objectstorage/cloud-type	oms::listCloudTypes	-

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。

OMS定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-270 OMS 支持的资源类型

资源类型	URN
Task	oms:<region>:<account-id>:task:*
	oms:<region>:<account-id>:task:<task-id>
SyncTask	oms:<region>:<account-id>:synctask:*
	oms:<region>:<account-id>:synctask:<synctask-id>
TaskGroup	oms:<region>:<account-id>:taskgroup:*
	oms:<region>:<account-id>:taskgroup:*

须知

同步任务API当前仅支持华南-广州-友好、华北-北京四、华东-上海一区域。

条件（Condition）

OMS服务不支持在SCP中的条件键中配置服务级的条件键。

OMS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。

5.10.15.2 主机迁移服务 SMS

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SMS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SMS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SMS的相关操作。

表 5-271 SMS 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
sms:template:list	授予查询模板列表权限	list	template	-
sms:template:create	授予新增模板信息权限	write	template	-
sms:template:batchDelete	授予批量删除指定ID的模板权限	write	template	-
sms:template:get	授予查询指定ID模板信息权限	read	template	-
sms:template:update	授予修改模板信息权限	write	template	-
sms:template:getTargetPassword	授予查询指定ID的模板中的目的端服务器的密码权限	read	template	-
sms:template:delete	授予删除指定ID的模板权限	write	template	-
sms:server:listErrors	授予查询待迁移源端的所有错误权限	list	server	-

授权项	描述	访问级别	资源类型（*为必须）	条件键
sms:server:list	授予查询源端服务器列表权限	list	server	g:EnterpriseProjectId
sms:server:register	授予上报源端服务器基本信息权限	write	server	g:EnterpriseProjectId
sms:server:batchDelete	授予批量删除源端服务器信息权限	write	server	g:EnterpriseProjectId
sms:server:get	授予查询指定ID的源端服务器权限	read	server	g:EnterpriseProjectId
sms:server:update	授予修改指定ID的源端服务器名称权限	write	server	g:EnterpriseProjectId
sms:server:delete	授予删除指定ID的源端服务器信息权限	write	server	g:EnterpriseProjectId
sms:server:updateDiskInfo	授予更新磁盘信息权限	write	server	g:EnterpriseProjectId
sms:server:overview	获取服务器总览权限	read	server	-
sms:server:updateState	授予更新任务对应源端复制状态权限	write	server	g:EnterpriseProjectId
sms:server:listTask	授予查询迁移任务列表权限	list	server	g:EnterpriseProjectId
sms:server:createTask	授予创建迁移任务权限	write	server	g:EnterpriseProjectId
sms:server:batchDeleteTask	授予批量删除迁移任务权限	write	server	g:EnterpriseProjectId
sms:server:getTask	授予查询指定ID的迁移任务权限	read	server	g:EnterpriseProjectId
sms:server:updateTask	授予更新指定ID的迁移任务权限	write	server	g:EnterpriseProjectId
sms:server:deleteTask	授予删除指定ID的迁移任务权限	write	server	g:EnterpriseProjectId
sms:server:manageTask	授予管理迁移任务权限	write	server	g:EnterpriseProjectId
sms:server:updateTaskProgress	授予上报数据迁移进度和速率权限	write	server	g:EnterpriseProjectId
sms:server:unlock	授予解锁指定任务的目的端服务器权限	write	server	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
sms:server:collectLog	授予上传迁移任务的日志权限	write	server	g:EnterpriseProjectId
sms:server:getTaskPassphrase	授予查询指定任务ID的安全传输通道的证书passphrase权限	read	server	g:EnterpriseProjectId
sms:server:checkNetwork	授予检查网卡安全组端口是否符合要求权限	read	server	-
sms:server:getTaskSpeedLimit	授予查询任务限速规则权限	read	server	g:EnterpriseProjectId
sms:server:updateTaskSpeedLimit	授予设置迁移限速规则权限	write	server	g:EnterpriseProjectId
sms:server:getCommand	授予获取服务端命令权限	read	server	g:EnterpriseProjectId
sms:server:updateCommandResult	授予上报服务端命令执行结果权限	write	server	g:EnterpriseProjectId
sms:server:getCert	授予获取SSL证书和私钥权限	read	server	g:EnterpriseProjectId
sms:migproject:list	授予获取项目列表权限	list	migproject	-
sms:migproject:create	授予新建迁移项目权限	write	migproject	-
sms:migproject:get	授予查询指定ID迁移项目详情权限	read	migproject	-
sms:migproject:update	授予更新迁移项目信息权限	write	migproject	-
sms:migproject:delete	授予删除迁移项目权限	write	migproject	-
sms:migproject:update	授予更新默认迁移项目权限	write	migproject	-
sms::getConfig	授予获取Agent配置信息权限	read	-	-
sms:server:updateNetworkCheckInfo	授予更新网络检测相关的信息权限	write	task	g:EnterpriseProjectId

授权项	描述	访问级别	资源类型（*为必须）	条件键
sms:server:getTaskConfig	授予查询任务配置权限	read	task	g:EnterpriseProjectId
sms:server:updateTaskConfig	授予更新任务配置权限	write	task	g:EnterpriseProjectId

SMS的API通常对应着一个或多个授权项。表5-272展示了API与授权项的关系，以及该API需要依赖的授权项。

表 5-272 API 与授权项的关系

API	对应的授权项	依赖的授权项
GET /v3/vm/templates	sms:template:list	-
POST /v3/vm/templates	sms:template:create	-
POST /v3/vm/templates/delete	sms:template:batchDelete	-
GET /v3/vm/templates/{id}	sms:template:get	-
PUT /v3/vm/templates/{id}	sms:template:update	-
GET /v3/vm/templates/{id}/target-password	sms:template:getTargetPassword	-
DELETE /v3/vm/templates/{id}	sms:template:delete	-
GET /v3/errors	sms:server:listErrors	-
GET /v3/sources	sms:server:list	-
POST /v3/sources	sms:server:register	-

API	对应的授权项	依赖的授权项
POST /v3/sources/delete	sms:server:batchDelete	• ecs:cloudServers:showServer • ecs:cloudServers:attach • evs:volumes:use • ecs:cloudServers:stop • ecs:cloudServers:start • ecs:cloudServers:detachVolume • evs:volumes:delete • evs:snapshots:delete • evs:volumes:get
GET /v3/sources/{source_id}	sms:server:get	-
PUT /v3/sources/{source_id}	sms:server:update	-
DELETE /v3/sources/{source_id}	sms:server:delete	• ecs:cloudServers:showServer • ecs:cloudServers:attach • evs:volumes:use • ecs:cloudServers:stop • ecs:cloudServers:start • ecs:cloudServers:detachVolume • evs:volumes:delete • evs:snapshots:delete • evs:volumes:get
PUT /v3/sources/{source_id}/diskinfo	sms:server:updateDiskInfo	-
GET /v3/sources/overview	sms:server:overview	-
PUT /v3/sources/{source_id}/changestate	sms:server:updateState	-
GET /v3/tasks	sms:server:listTask	-
POST /v3/tasks	sms:server:createTask	-

API	对应的授权项	依赖的授权项
POST /v3/tasks/delete	sms:server:batchDeleteTask	• ecs:cloudServers:showServer • ecs:cloudServers:attach • evs:volumes:use • ecs:cloudServers:stop • ecs:cloudServers:start • ecs:cloudServers:detachVolume • evs:volumes:delete • evs:snapshots:delete • evs:volumes:get
GET /v3/tasks/{task_id}	sms:server:getTask	-
PUT /v3/tasks/{task_id}	sms:server:updateTask	-
DELETE /v3/tasks/{task_id}	sms:server:deleteTask	• ecs:cloudServers:showServer • ecs:cloudServers:attach • evs:volumes:use • ecs:cloudServers:stop • ecs:cloudServers:start • ecs:cloudServers:detachVolume • evs:volumes:delete • evs:snapshots:delete • evs:volumes:get
POST /v3/tasks/{task_id}/action	sms:server:manageTask	-
PUT /v3/tasks/{task_id}/progress	sms:server:updateTaskProgress	-
POST /v3/tasks/{task_id}/unlock	sms:server:unlock	-
POST /v3/tasks/{task_id}/log	sms:server:collectLog	-
GET /v3/tasks/{task_id}/passphrase	sms:server:getTaskPassphrase	-

API	对应的授权项	依赖的授权项
GET /v3/tasks/{t_project_id}/networkacl/{t_network_id}/check	sms:server:checkNetwork	-
GET /v3/tasks/{task_id}/speed-limit	sms:server:getTaskSpeedLimit	-
POST /v3/tasks/{task_id}/speed-limit	sms:server:updateTaskSpeedLimit	-
GET /v3/sources/{server_id}/command	sms:server:getCommand	-
POST /v3/sources/{server_id}/command_result	sms:server:updateCommandResult	-
GET /v3/tasks/{task_id}/certkey	sms:server:getCert	-
GET /v3/migprojects	sms:migproject:list	-
POST /v3/migprojects	sms:migproject:create	-
GET /v3/migprojects/{mig_project_id}	sms:migproject:get	-
PUT /v3/migprojects/{mig_project_id}	sms:migproject:update	-
DELETE /v3/migprojects/{mig_project_id}	sms:migproject:delete	-
PUT /v3/migprojects/{mig_project_id}/default	sms:migproject:update	-
GET /v3/config	sms::getConfig	-
POST /v3/{task_id}/update-network-check-info	sms:server:updateNetworkCheckInfo	-
POST /v3/tasks/{task_id}/configuration-setting	sms:server:updateTaskConfig	-

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。

SMS定义了以下可以在SCP的Resource元素中使用的资源类型。

表 5-273 SMS 支持的资源类型

资源类型	URN
server	sms::<account-id>:server:*
	sms::<account-id>:server:<server-id>
Task	sms::<account-id>:task:*
	sms::<account-id>:task:<task-id>
template	sms::<account-id>:template:*
	sms::<account-id>:template:<template-id>
migproject	sms::<account-id>:migproject:*
	sms::<account-id>:migproject:<migproject-id>

条件（Condition）

SMS服务不支持在SCP中的条件键中配置服务级的条件键。

SMS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。如未指定任何服务和资源类型，则此标签策略不会对任何资源生效。
- 通配符：可以在标签值和强制执行字段中使用通配符 "*"，不过必须遵循以下约束：
  - 每个标签值仅使用一个通配符。例如，允许使用 *@example.com，但不允许使用 *@*.com。
  - 对于强制执行，可以用“<service>:*”对该服务的所有资源启用强制执行。但是不能使用通配符指定所有服务或指定所有服务的某个资源。

继承运算符

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

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

- **值设置运算符**

  您可以使用以下值设置运算符来控制策略与其父策略交互的方式：

表 6-1 值设置运算符

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

- **子控制运算符**

  默认情况下，允许所有运算符 (@@all)。

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

6.3 启用和禁用标签策略

只有组织管理账号才可以启用或禁用标签策略，委托管理员无法执行此操作。

启用标签策略

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

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入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 6-1 启用标签策略

步骤3 在弹窗中勾选确认框，然后单击“确定”，完成标签策略功能启用。

----结束

禁用标签策略

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

⚠ 注意

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

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入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 6-2 禁用标签策略

步骤3 在弹窗中单击“确定”，完成标签策略禁用。

----结束

6.4 创建标签策略

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

只有组织管理员才可以创建标签策略，委托管理员无法执行此操作。

操作步骤

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入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 6-3 进入标签策略管理页

步骤3 单击“创建”，进入创建标签策略页面。

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

（可选）输入策略描述。

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

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

  a. 输入标签策略定义的标签的键。

  b. 指定标签键的大小写形式。

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

  c. 指定标签键的允许值。

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

  图 6-4 添加标签键的允许值

  d. 指定执行标签策略检查的资源类型。

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

  说明

  如未指定任何服务和资源类型，则此标签策略不会对任何资源生效。

图 6-5 指定策略生效的资源类型

e. 单击“添加标签键”，可在策略内容中添加多个标签键用于标签策略检查。

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

图 6-6 使用 JSON 编辑策略

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

图 6-7 添加标签

步骤7 单击右下角的“保存”后，如跳转到标签策略列表，则标签策略创建成功。

----结束

6.5 查看有效的标签策略

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

有效标签策略生效的逻辑规则如下：

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

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

本章为您介绍如何在控制台上查看绑定在组织的根、OU和账号上的有效标签策略。

操作步骤

步骤1 进入华为云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 展开“标签策略”列表，单击列表上方的“查看有效标签策略”，在JSON视图查看有效标签策略内容。

图 6-8 查看有效标签策略

----结束

6.6 修改和删除标签策略

本章为您介绍如何修改和删除已创建的标签策略。

只有组织管理员才可以修改或删除标签策略，委托管理员无法执行此操作。

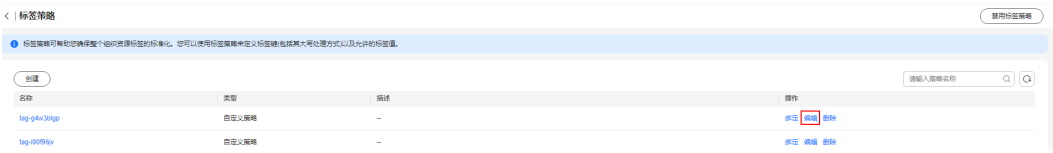
修改标签策略

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入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。

图 6-9 编辑标签策略



步骤4 可根据需要修改“策略名称”和“策略描述”。

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

步骤6 单击右下角“保存”后，如跳转到标签策略列表，则标签策略修改成功。

----结束

删除标签策略

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

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入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 在弹窗中单击“确定”，完成标签策略删除。

图 6-10 删除标签策略

----结束

6.7 绑定和解绑标签策略

管理账号可以为根、OU和账号绑定和解绑标签策略。

约束与限制

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

绑定标签策略

方式一：

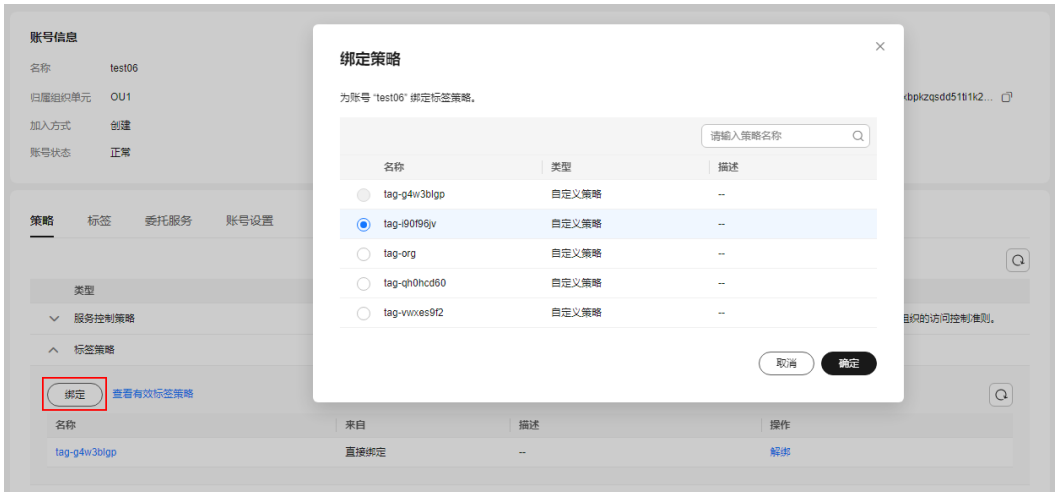
步骤1 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。

步骤2 选中要绑定标签策略的OU或者账号。

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

步骤4 在弹窗中选择要添加的策略后，单击“确定”，完成策略绑定。

图 6-11 绑定标签策略



----结束

方式二：

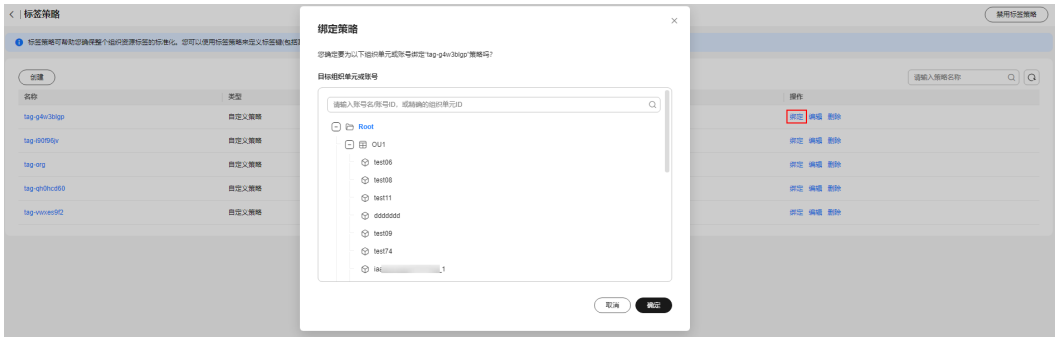
步骤1 在Organizations控制台，进入策略管理页。

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。

步骤4 单击“确定”，完成策略绑定。

图 6-12 绑定标签策略



----结束

解绑标签策略

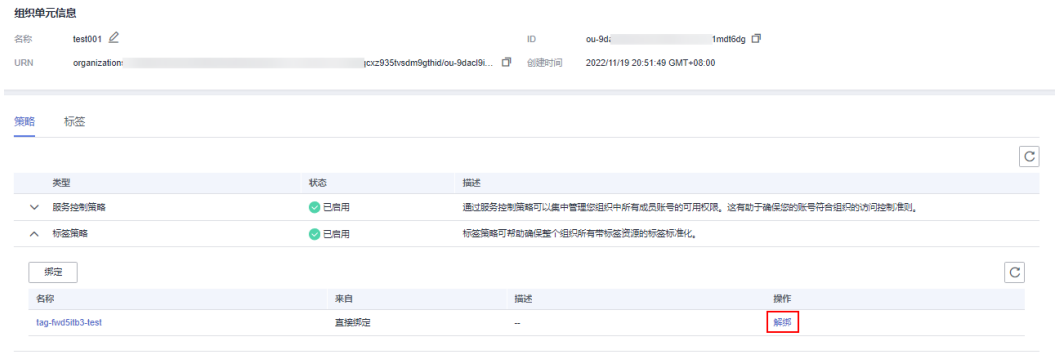
方式一：

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

步骤2 选中要解绑标签策略的OU或者账号。

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

图 6-13 解绑标签策略



步骤4 在弹窗中单击“解绑”，完成策略解绑。

----结束

方式二：

步骤1 在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”。

步骤5 单击“确定”，完成策略解绑。

图 6-14 解绑标签策略

----结束

6.8 支持标签策略的云服务

当前支持使用标签策略的云服务和资源类型如下表所示：

表 6-2 支持标签策略的云服务和资源类型

服务名称	资源类型
DDoS原生基础防护服务（Anti-DDoS）	公网IP（ip）
DDoS防护服务（AAD）	实例（instance）
应用运维管理（AOM）	告警规则（alarmRule）
API网关（APIG）	实例（instance）

服务名称	资源类型
弹性伸缩（AS）	弹性伸缩组（scalingGroup）
裸金属服务器（BMS）	实例（instance）
云堡垒机（CBH）	实例（instance）
云备份（CBR）	存储库（vault）
云连接（CC）	• 带宽包（bandwidthPackage） • 中心网络（centralNetwork） • 云连接（cloudConnection）
云容器引擎（CCE）	集群（cluster）
云容器实例 CCI	命名空间（namespace）
内容分发网络（CDN）	域名（domain）
云监控服务（CES）	告警规则（alarm）
云防火墙（CFW）	实例（instance）
DDoS原生高级防护（CNAD）	防护包（package）
微服务引擎（CSE）	引擎（engine）
云凭据管理服务（CSMS）	凭据（secret）
云搜索服务（CSS）	• 集群（cluster） • 日志流（logstream） • 存储库（repository）
云审计服务（CTS）	追踪器（tracker）
数据治理中心（DataArts Studio）	• 实例（instance） • 工作空间（workspace）
数据库安全服务（DBSS）	审计实例（auditInstance）
云专线（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）

服务名称	资源类型
数据湖探索（DLI）	• 数据库（database） • 增强型跨源连接（edsconnection） • 弹性资源池（elasticresourcepool） • 作业（jobs） • 队列（queue） • 资源（resource）
分布式消息服务（DMS）	• Kafka实例（kafka） • RabbitMQ实例（rabbitmq） • RocketMQ实例（rocketmq）
云解析服务（DNS）	• 反向解析记录（ptr） • 域名（zone）
数据复制服务（DRS）	任务（job）
数据仓库服务（DWS）	集群（cluster）
弹性云服务器（ECS）	实例（instance）
弹性负载均衡（ELB）	• 监听器（listener） • 负载均衡器（loadbalancer）
企业路由器（ER）	• 连接（attachments） • 实例（instances） • 路由表（routeTables）
云硬盘（EVS）	磁盘（volume）
函数工作流（FunctionGraph）	函数（function）
全球加速（GA）	• 加速器实例（accelerator） • 监听器（listener）
云数据库 GaussDB	实例（instance）
云数据库 GaussDB(for MySQL)	实例（instance）
云数据库 GeminiDB（原 云数据库 GaussDB for NoSQL）	实例（instance）
统一身份认证服务（IAM）	• 委托（agency） • 用户（user）
镜像服务（IMS）	镜像（image）
设备接入 IoTDA	实例（instance）
密钥管理服务（KMS）	用户主密钥（cmk）

服务名称	资源类型
云日志服务（LTS）	• 日志接入（accessConfig） • 主机组（hostGroup） • 日志组（logGroup） • 日志流（logStream）
AI开发平台 ModelArts	• Notebook实例（notebook） • 资源池（pool） • 服务（service） • 训练作业（trainJob）
MapReduce服务（MRS）	集群（cluster）
NAT网关（NAT）	• 公网NAT网关（gateway） • 私网NAT网关（privateGateway） • 中转IP（privateTransitIp） • 中转子网（transitSubnet）
组织（Organizations）	• 账号（account） • 组织单元（ou） • 策略（policy） • 根（root）
私有证书管理服务（PCA）	私有CA（ca）
资源访问管理（RAM）	资源共享实例（resourceShare）
云数据库（RDS）	实例 (instances)
配置审计（Config）（原 资源管理服务 RMS）	合规规则（policyAssignments）
SSL证书管理服务（SCM）	证书（cert）
安全云脑（SecMaster）	工作空间（workspace）
应用管理与运维平台（ServiceStage）	• 应用（app） • 环境（environment）
高性能弹性文件服务（SFS Turbo）	SFS Turbo（shares）
消息通知服务（SMN）	主题（topic）
虚拟私有云（VPC）	• 弹性公网IP（publicip） • 子网（subnet） • 虚拟私有云（vpc）
VPC终端节点（VPCEP）	• 终端节点服务（endpointServices） • 终端节点（endpoints）

服务名称	资源类型
虚拟专用网络（VPN）	• 对端网关（customerGateways） • VPN连接（vpnConnections） • VPN网关（vpnGateways）
Web应用防火墙（WAF）	高级实例（premiumlnstance）

6.9 支持标签策略的区域

当前支持使用标签策略的区域如下表所示：

表 6-3 支持标签策略的区域

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

7 可信服务管理

7.1 可信服务概述

什么是可信服务

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

什么是委托管理员

委托管理员账号是一个组织中有特殊权限的成员账号。管理账号可指定某个成员账号为某个可信服务的委托管理员账号。成为委托管理员账号后，该成员账号下的用户可以使用对应可信服务的组织级管理能力。例如，某一个成员账号成为CTS云服务的委托管理员后，可以查看所有成员账号的云审计日志。

服务关联委托

Organizations使用IAM服务的委托信任功能，使可信服务能够在您组织的成员账号中代表您执行任务。当您启用某个服务为可信服务时，该服务可以请求Organizations在其成员账号中创建服务关联委托，可信服务按需异步执行此操作。此服务关联委托具有预定义的IAM权限，允许可信服务在成员账号中拥有执行可信服务文档中所述任务的权限，相当于云服务能力在多账号组织场景下的拓展。当前支持的可信服务及其功能简介请参见：**已对接组织的可信服务**。

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

说明

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

7.2 启用和禁用可信服务

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

启用可信服务

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入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”。

步骤3 在弹窗中单击“确定”，完成可信服务启用。

图 7-1 启用可信服务

----结束

禁用可信服务

登录到组织的管理账号时，您可以禁用可信服务，步骤如下。

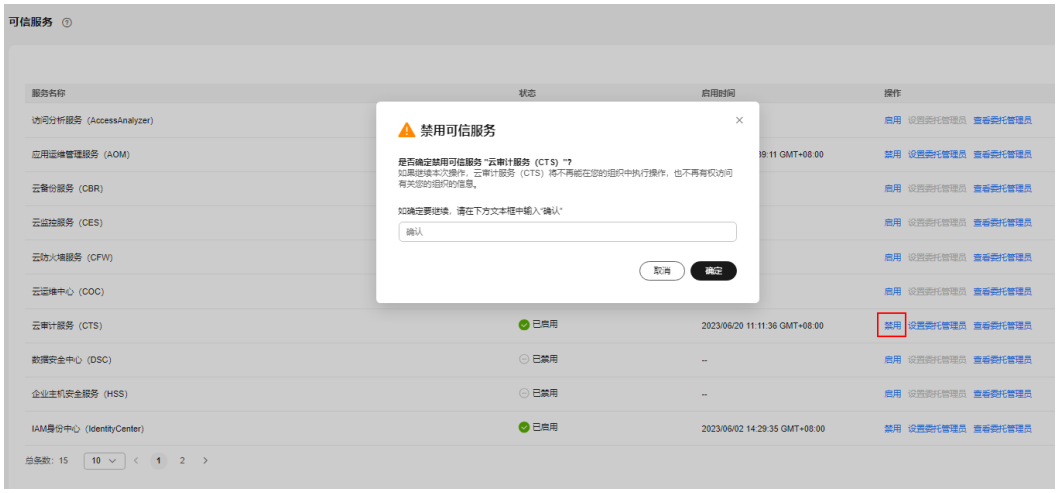
步骤1 以组织管理员或管理账号的身份登录管理控制台，进入Organizations控制台。

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 在弹窗中输入“确认”，然后单击“确定”，完成可信服务禁用。

图 7-3 禁用可信服务



----结束

7.3 已对接组织的可信服务

以组织管理员或管理账号的身份登录华为云，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账号状态为“正常”的成员账号中。	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
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

服务名称	功能简介	是否支持委托管理员	相关文档
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
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

服务名称	功能简介	是否支持委托管理员	相关文档
IAM身份中心（IdentityCenter）	IAM身份中心为用户提供基于组织的多账号统一身份管理与访问控制。可以统一管理企业中使用华为云的用户，一次性配置企业的身份管理系统与华为云的单点登录，以及所有用户对组织下账号状态为“正常”的账号的访问权限。	是	什么是IAM身份中心
云日志服务（LTS）	云日志服务联合组织服务推出多账号日志汇聚中心，组织管理员或LTS服务的委托管理员可以在LTS将组织下指定账号的日志流复制到自己的账号中，实现多账号日志的集中存储和分析，满足安全合规、集中分析等不同场景下的诉求。	是	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
访问分析（AccessAnalyzer）	访问分析提供组织级的访问分析功能，组织管理员或委托管理员可以在组织内创建和管理访问分析器，用于识别组织内与外部共享的资源等。	是	暂无

服务名称	功能简介	是否支持委托管理员	相关文档
云运维中心（COC）	云运维中心基于组织的跨账号能力，支持组织管理员或服务委托管理员在云运维中心查看其组织内成员的运维态势和资源情况，并支持对资源进行跨账号的作业任务执行。	是	暂无

7.4 添加、查看和取消委托管理员

须知

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

添加委托管理员

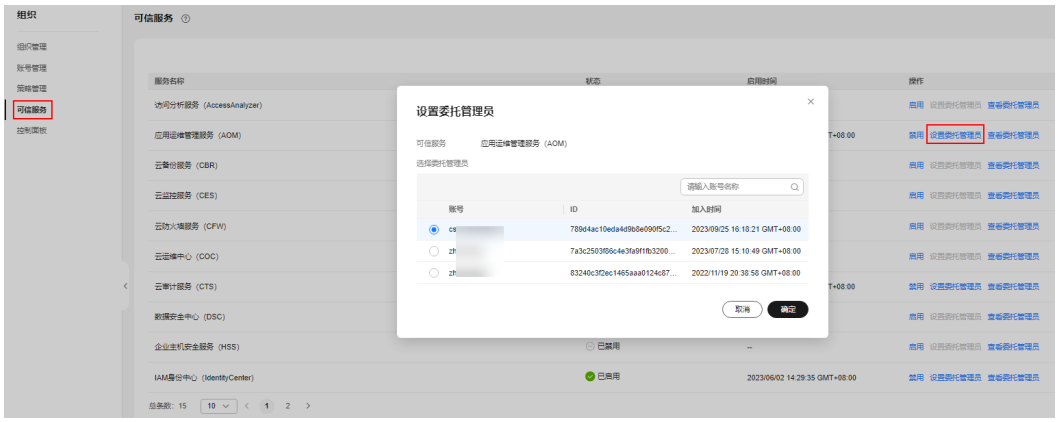
关闭中状态的账号无法设置为委托管理员。

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入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”。

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

图 7-4 设置委托管理员



----结束

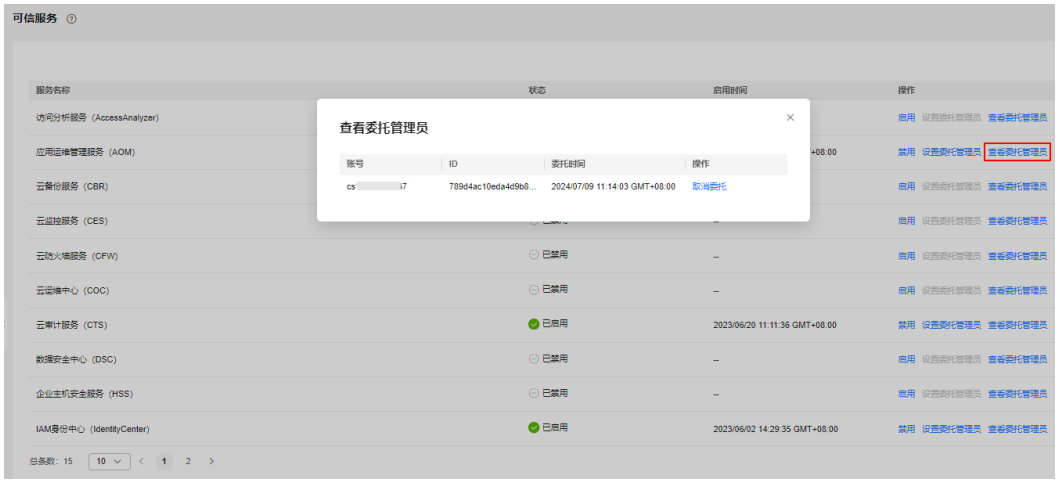
查看委托管理员

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入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 系统将弹窗展示该云服务的委托管理员信息。

图 7-5 查看委托管理员



----结束

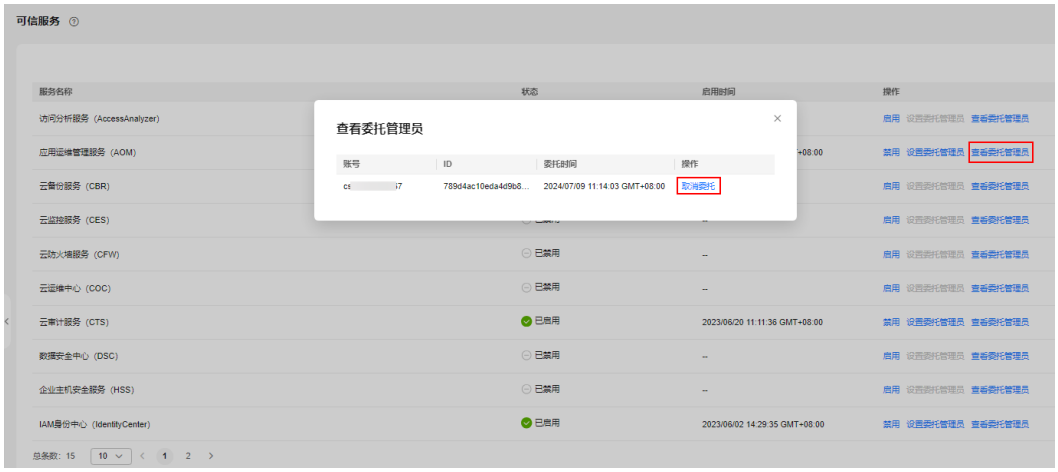
取消委托管理员

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入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 7-6 取消委托管理员



步骤4 在弹窗中单击“确定”，完成取消委托管理员操作。

----结束

8 标签管理

8.1 标签概述

标签简介

标签用于标识云资源，可通过标签实现对云资源的分类和搜索。您可以向以下组织资源添加标签：

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

您可以在以下时间添加标签：

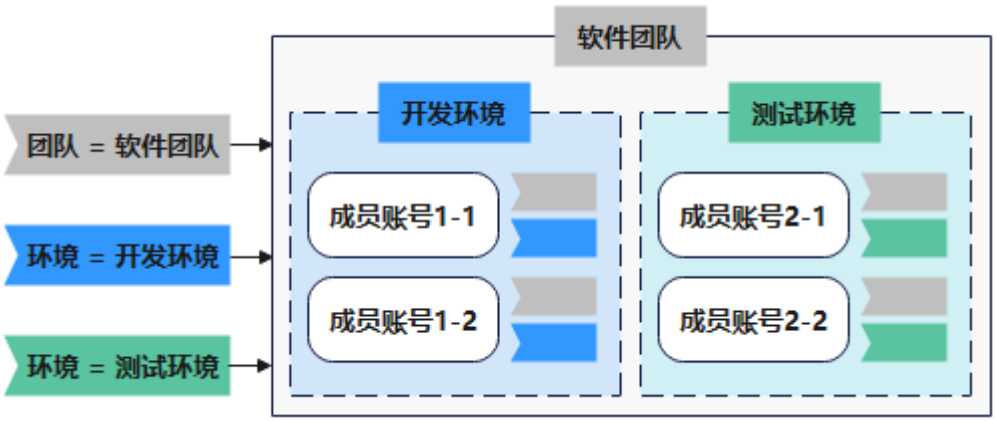
- 在创建OU、账号、SCP和标签策略时，可以添加标签。
- 根、OU、账号、SCP和标签策略创建完成后，可以在各自的详情页面添加、修改、查看、删除标签。

标签的基本知识

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

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

图 8-1 标签示例



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

标签的使用约束

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

  “标签键”：

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

  “标签值”：

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

本章将为您介绍如下内容：

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

8.2 添加标签

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”。

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

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

图 8-2 添加标签

----结束

8.2.2 添加策略标签

操作场景

本章节指导用户为SCP自定义策略和标签策略添加标签。

操作步骤

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

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入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。

步骤4 选择“标签”页签，单击“添加”。

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

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

图 8-3 添加标签

----结束

8.3 修改标签

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。

图 8-4 修改标签

----结束

8.3.2 修改策略标签

操作场景

本章节指导用户修改SCP自定义策略和标签策略的标签。

操作步骤

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

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

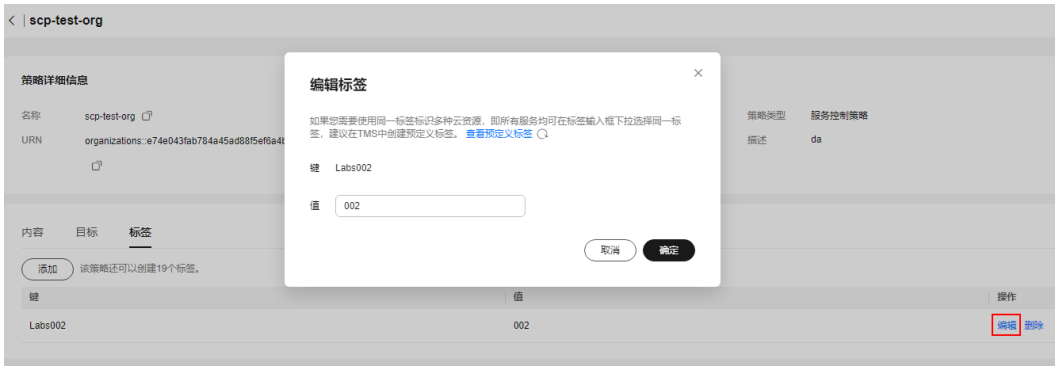
步骤2 进入策略管理页，单击服务控制策略，进入SCP管理页。

步骤3 在列表中单击自定义策略的名称，进入策略详情页。

步骤4 选择标签页签，单击要修改标签操作列的“编辑”。

步骤5 在弹窗中输入修改后标签值， 单击“确定”，完成标签修改。

图 8-5 修改标签



----结束

8.4 查看标签

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，可查看此组织单元已添加的全部标签信息。

----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管理控制台，进入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。

步骤4 选择“标签”页签，可查看此SCP已添加的全部标签信息。

----结束

8.5 删除标签

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。

图 8-6 删除标签

----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管理控制台，进入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。

步骤4 选择“标签”页签，单击要修改标签操作列的“删除”。

步骤5 在弹窗中单击“确定”，完成标签删除。

图 8-7 删除标签

----结束

9 使用 CTS 审计组织操作事件

9.1 支持审计的关键操作

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

表 9-1 云审计支持的 Organizations 操作列表

操作名称	资源类型	事件名称
创建组织	Organization	createOrganization
关闭组织	Organization	celeteOrganization
退出组织	Organization	leaveOrganization
创建组织单元	OrganizationUnit	createOrganizationalUnit
修改组织单元	OrganizationUnit	updateOrganizationalUnit
删除组织单元	OrganizationUnit	deleteOrganizationalUnit
邀请账号	Account	inviteAccount
创建账号	Account	createAccount
关闭账号	Account	closeAccount
更新账号	Account	updateAccount
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

操作名称	资源类型	事件名称
启用可信服务	TrustedService	enableTrustedService
禁用可信服务	TrustedService	disableTrustedService
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	• Account • OrganizationUnit • Policy • Root • Tag	tagResource
删除标签	• Account • OrganizationUnit • Policy • Root • Tag	untagResource

9.2 在 CTS 事件列表查看云审计事件

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)或云日志服务(LTS)，才可在OBS桶或LTS日志组里面查看历史事件信息。否则，您将无法追溯7天以前的操作记录。
- 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。
- 云审计控制台对用户的操作事件日志保留7天，过期自动删除，不支持人工删除。

在新版事件列表查看审计事件

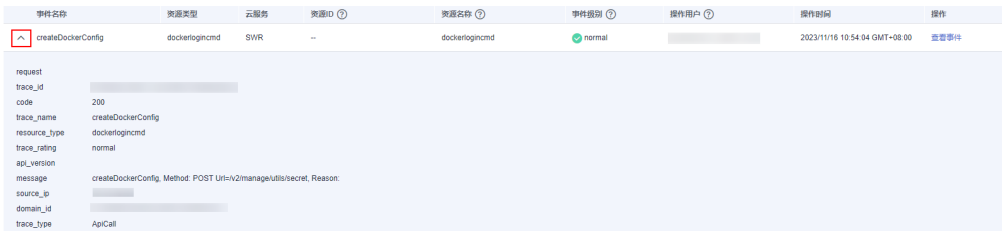
1. 登录管理控制台。
2. 单击左上角 ☰，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
   - 事件名称：输入事件的名称。
   - 事件ID：输入事件ID。
   - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
   - 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
   - 云服务：在下拉框中选择对应的云服务名称。
   - 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。
   - 企业项目ID：输入企业项目ID。
   - 访问密钥ID：输入访问密钥ID（包含临时访问凭证和永久访问密钥）。
   - 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7天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。

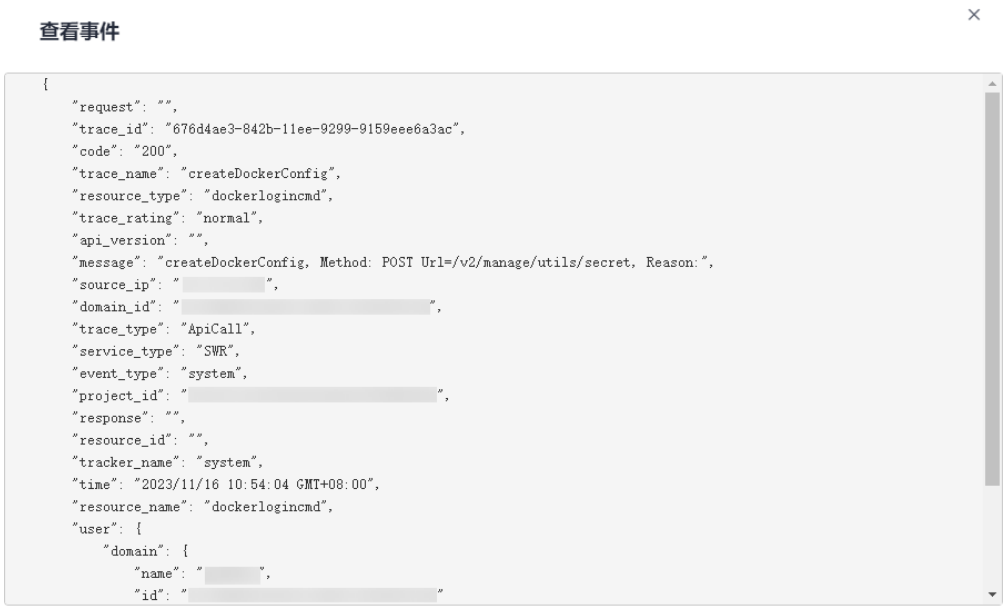
6. 关于事件结构的关键字段详解，请参见事件结构和事件样例。
7. （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

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、云服务、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1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。
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”。