组织

抽屉式帮助

文档版本	01
发布日期	2025-09-18

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 创建策略.....1
1.1 策略语法说明.....1
2 创建 SCP.....5

1 创建策略

1.1 策略语法说明

策略简介

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。

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**

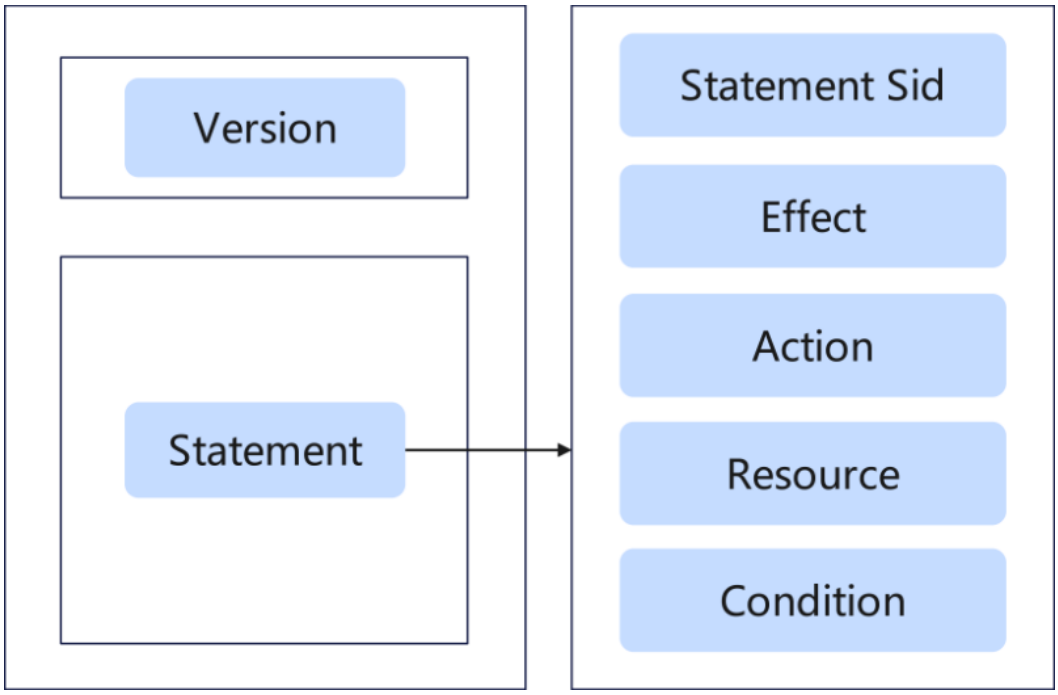
华为云服务在组织预置了常用SCP，称为系统策略。组织管理员给组织单元或账号绑定SCP时，可以直接使用这些策略。系统策略只能使用，不能修改。现有的SCP系统策略请参见：**SCP系统策略列表**。

- **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。

策略语法结构

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。



策略语法示例

下面以RAM的自定义策略为例，说明策略的语法。

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

策略参数

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 1-1 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。	• Deny：不允许执行。
	Action：授权项	Deny时可选	操作权限。	格式为“服务名:资源类型:操作”。 例如“vpc:subnets:list”：表示查看VPC子网列表权限，其中vpc为服务名，subnets为资源类型，list为操作。
	Condition：条件	Deny时可选。	使策略生效的特定条件，包括**条件键**和**运算符**。	格式为“条件运算符:{条件键：[条件值1,条件值2]}”。 如果您设置多个条件，同时满足所有条件时，该策略才生效。 示例: "StringEndWithIfExists":{"g:UserName":["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。	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
- NotAction

2 创建 SCP

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

约束与限制

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

操作步骤

步骤1 以组织管理员或管理账号的身份登录管理控制台，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。

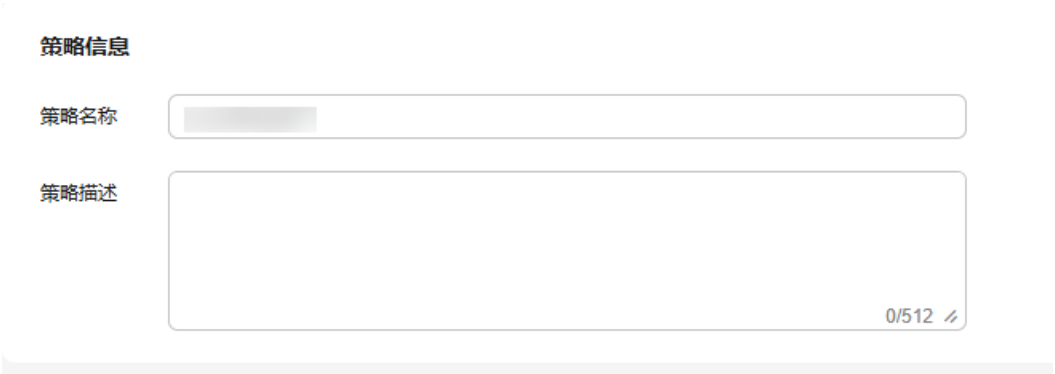
图 2-1 进入 SCP 管理页

步骤3 选择“正式运行模式”或“试运行模式”的策略，单击“创建”，进入SCP创建页面。

图 2-2 创建 SCP

步骤4 输入策略名称。新创建的策略名称不能与已有策略名称重复。

（可选）输入策略描述。



步骤5 在策略内容左侧可以直接编写JSON格式的策略内容。

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

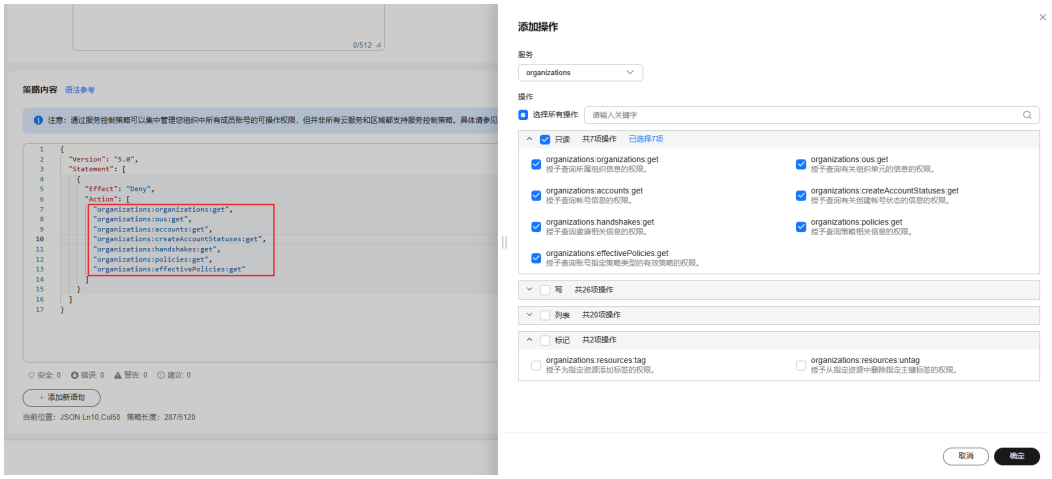
说明

自定义策略版本号（Version）固定为5.0，不可修改。

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

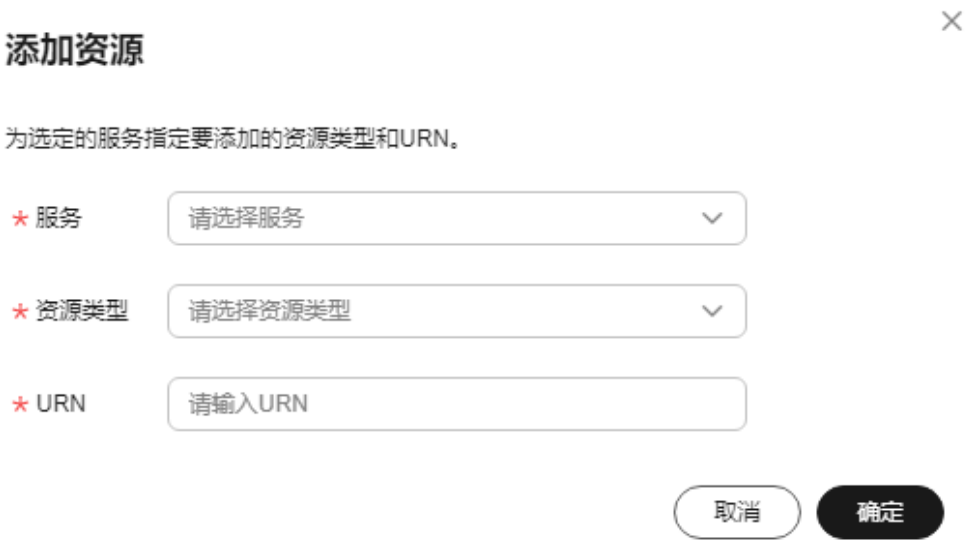
- 添加操作：单击 ⊕ 号，选择或搜索要添加的服务及相应操作项，添加成功的操作项会自动显示在策略内容左侧的Action元素下。如**图2-3**所示。

图 2-3 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2-4所示。

图 2-4 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2-5所示。

图 2-5 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 2-6 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 2-7 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。

说明

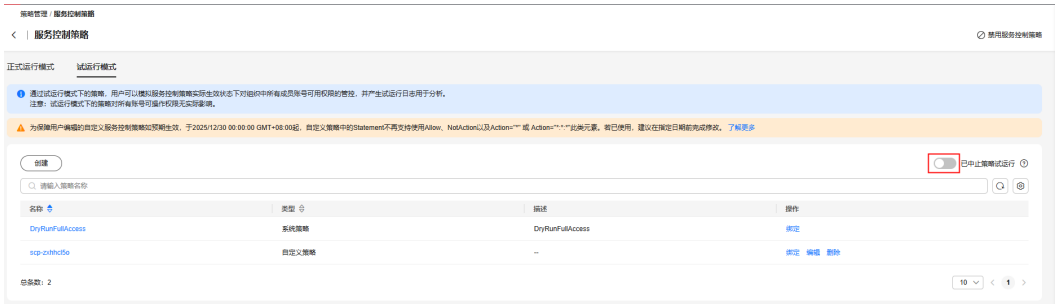
- 在试运行模式下，通过实施策略可以模拟服务控制策略实际生效时对组织内所有成员账户可用权限的管控，并生成试运行日志以供分析。
- 试运行模式下的策略对所有账号可操作权限无实际影响。

----结束

开启策略试运行

步骤1 进入策略管理页，单击“服务控制策略”，进入SCP管理页。

步骤2 在“试运行模式”的策略页签中，单击“已中止策略试运行”按钮。



步骤3 配置资源转储。

选择OBS桶，将策略试运行日志存储至您指定的对象存储服务OBS桶中。

- **配置当前账号下OBS桶：**

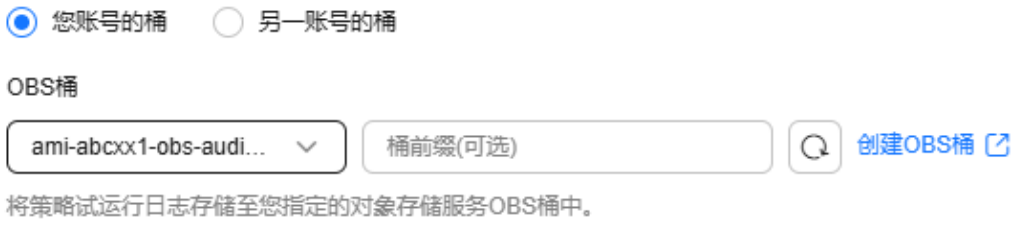
  选择“您账号的桶”，然后在下拉列表中选择您账号下的OBS桶，用于将策略试运行日志存储至您指定的对象存储服务OBS桶中。如果您需要将策略试运行日志存储在OBS桶内的某个文件夹下，则在选择OBS桶后，还需输入“桶前缀”，该前缀指OBS桶内某个文件夹的名称。如您的账号下无OBS桶，则需先创建OBS桶，详见**创建桶**。

- **配置其他账号下OBS桶：**

  选择“另一账号的桶”，并输入区域ID和桶名称，如果您需要将策略试运行日志存储在OBS桶内的某个文件夹下，则还需输入“桶前缀”，该前缀指OBS桶内某个文件夹的名称。需先使用其他账号对当前账号授予相关OBS桶的权限，具体操作请参见**跨账号授权**。

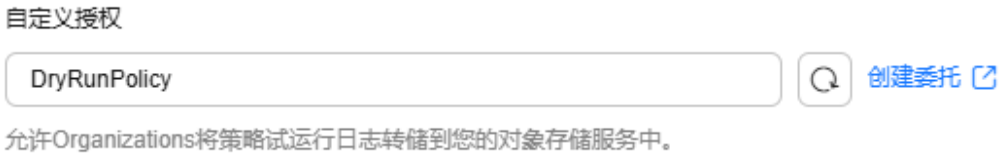
说明

开启策略试运行时，如果指定了当前账号或其他账号下的OBS桶，Organizations会向目标OBS桶中写入一个名为OrganizationsWritabilityCheckFile的空文件，此文件仅用于验证是否能够成功写入OBS桶。



步骤4 进行自定义授权。

创建Organizations云服务委托：您可自行在统一身份认证服务（IAM）中创建委托，并进行自定义授权，授权对象为云服务Organizations，但必须包含可以让策略试运行正常工作的权限（至少包含对象存储服务（OBS）的查询桶区域位置信息和上传对象的权限）。创建委托详见**委托其他云服务管理资源**。




```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "obs:bucket:getBucketLocation",
        "obs:object:putObject"
      ]
    }
  ]
}
```

策略试运行日志转储至OBS加密桶授权配置：

- 使用SSE-OBS方式加密的OBS桶

  如果您需要将策略试运行日志存储于使用SSE-OBS方式加密的OBS桶，无需其他操作，只需选择对应OBS桶进行存储即可。

- 使用SSE-KMS默认密钥方式加密的OBS桶

  如果您需要将策略试运行日志存储于使用SSE-KMS默认密钥方式加密的OBS桶，则需要在Organizations的委托中新增KMS的管理员权限（KMS Administrator）。

- 使用SSE-KMS自定义密钥方式加密的OBS桶

  如果您需要将策略试运行日志存储于使用SSE-KMS自定义密钥方式加密的OBS桶，则需要在Organizations的委托中新增KMS的管理员权限（KMS Administrator）。

  另外，如果您选择将策略试运行日志存储至其他账号的使用SSE-KMS自定义密钥方式加密的OBS桶，则除了需要在Organizations的委托中新增KMS的管理员权限（KMS Administrator），还需要在所选的OBS桶加密采用的自定义KMS密钥中设置密钥的跨账号权限。详情请参见**为自定义密钥创建授权**。

步骤5 配置完成后，单击“确定”，策略试运行配置成功。

----结束

更新策略试运行

步骤1 进入策略管理页，单击“服务控制策略”，进入SCP管理页。

步骤2 在“试运行模式”的策略页签中，单击“更新”按钮。

步骤3 在弹出的更新策略试运行配置窗口中，输入OBS桶和自定义授权等信息，单击“确定”，完成策略试运行更新，详情请参见**配置OBS桶**和**自定义授权**。

说明

若管理员更新了策略试运行配置中OBS桶信息或委托信息，最大生效时间为15分钟。

----结束

关闭策略试运行

步骤1 进入策略管理页，单击“服务控制策略”，进入SCP管理页。

步骤2 在“试运行模式”的策略页签中，单击“已启用策略试运行”按钮。

步骤3 在弹出的关闭策略试运行窗口中，输入文字“确认”，单击“确定”，策略试运行关闭成功。

说明

策略试运行关闭后，试运行的“更新”功能随即停止，此时试运行模式中的策略不再生成试运行日志。

----结束

跨账号授权

跨账号授予OBS桶存储策略试运行日志的权限

1. 用授权账号登录管理控制台，进入OBS管理控制台。
2. 参考**自定义创建桶策略（JSON视图）**对待授权账号授予相关OBS桶的权限。

   桶策略的示例如下，配置该桶策略，将允许被授权账号的策略试运行将转储文件存放至本OBS桶的指定路径内，以下参数需要您根据实际使用场景手动替换：

   - ${account_id}：需要被授权的账号的账号ID（domain_id）；
   - ${agency_name}：被授权的委托名称；
   - ${bucket_name}：用于存储文件的OBS桶的桶名；
   - ${folder_name}：用于存储文件的OBS桶内文件夹的名称。如果您未设置OBS桶内文件夹，则需删除“/${folder_name}”。

```
{
  "Statement": [
    {
      "Sid": "org-bucket-policy",
      "Effect": "Allow",
      "Principal": {
        "ID": [
          "domain/${account_id}:agency/${agency_name}"
        ]
      },
      "Action": [
        "PutObject",
        "GetBucketLocation"
      ]
    }
  ]
}
```