组织

常见问题

文档版本	01
发布日期	2024-03-14

华为技术有限公司

商标声明


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

注意

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

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

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 IAM 与 Organizations 权限访问控制的区别

1. 作用对象的不同，IAM可以对账号下的IAM用户、IAM用户组、IAM委托进行授权。组织服务则是对根组织单元、组织单元和成员账号进行权限控制。
2. 权限控制范围有所区别且有所关联，如果账号已经加入Organizations服务成为成员账号，组织管理员将SCP绑定到组织单元或者成员账号时，则账号下的IAM用户、用户组、委托均会受到SCP和IAM策略的权限控制影响。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。
3. 作用效果不同。SCP是指定了组织中成员账号的权限边界，限制账号内用户的操作。IAM策略则是直接对IAM用户、IAM用户组、IAM委托进行授权。

2 SCP 常见问题

Organizations的服务控制策略（SCP）与IAM策略的语法类似，并使用相同的JSON格式语法，详细信息请参见**SCP语法介绍**。

创建SCP时的常见策略语法问题如下：

- **多个策略对象**
- **多个Statement元素**
- **策略长度超出限制**

多个策略对象

一个SCP必须包含一个并且只能包含一个JSON对象，通过在两旁放置的大括号“{ }”来表示对象。虽然您可以插入额外的大括号“{ }”在JSON对象中嵌套其他对象，但是一个策略只能包含一个最外层的“{ }”括号对。以下为错误示例，因为它包含了两个JSON对象（两个最外层“{ }”括号对）：

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:*:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
{
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "vpc:*:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```


但是，您可以通过使用正确的策略语法来实现上面示例的意图，将两个数据块合并到单个Statement元素中，而不是包含两个完整的策略对象（每个都有自己的Statement元素）。Statement元素将两个对象组成的数组作为其值，示例如下：

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:*:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Deny",
      "Action": [
        "vpc:*:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

如上示例无法进一步压缩到带一个元素的Statement中，因为两个元素具有不同的作用（Effect）。通常情况下，您只能在每个语句中的Effect和Resource元素相同时组合语句。

多个 Statement 元素

如下示例中的错误看起来可能是上一节中错误的变体，但是从语法上来看，它是一种不同类型的错误。如下示例中只有一个策略对象，如最外层的“{ }”括号对所表示，但是该策略对象中包含两个Statement元素。

一个SCP只能只包含一个Statement元素，Statement元素的值必须是对象，以“{ }”括号表示，其中包含一个Effect元素、一个Action元素、一个Resource元素和一个可选的Condition元素。如下示例中的策略对象包含了两个Statement元素，因此是错误的。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:*:*"
      ],
      "Resource": [
        "*"
      ]
    },
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "vpc:*:*"
      ],
      "Resource": [
        "*"
      ]
    }
```

```
 ]
}
```

Statement元素的值必须是对象，但值对象可以是多个值对象组成的数组，因此可以通过将两个Statement元素合并为一个具有对象数组的元素来解决此问题，例如下方示例中，Statement元素的值是对象数组，数组中包含两个对象，每个对象都是Statement元素的正确值，数组中的每个对象之间用逗号隔开。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:*:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Deny",
      "Action": [
        "vpc:*:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

策略长度超出限制

SCP内容的最大长度为5120个字符，包括所有字符和空格。如需缩减SCP的大小，您可以删除引号之外的所有空白字符（如空格和换行符）。