物联使能

子账号权限控制

腾讯云

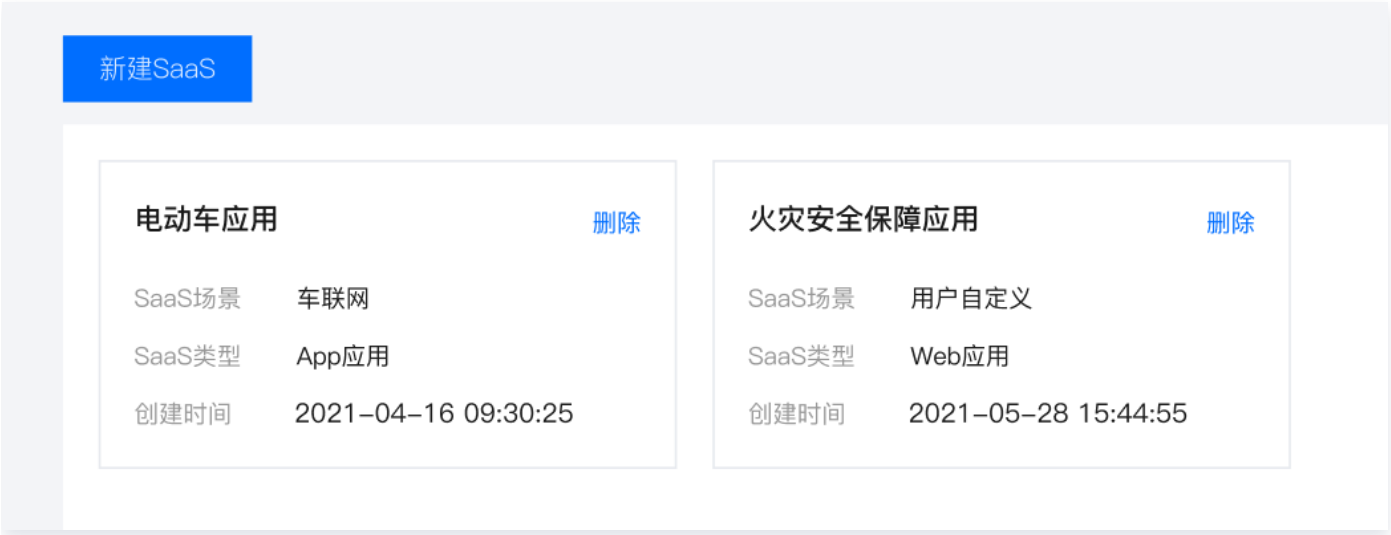
子账号权限控制

最近更新时间：2023-07-19 17:34:51

本文主要介绍如何授予子账号 SaaS 服务级访问控制权限。

操作场景

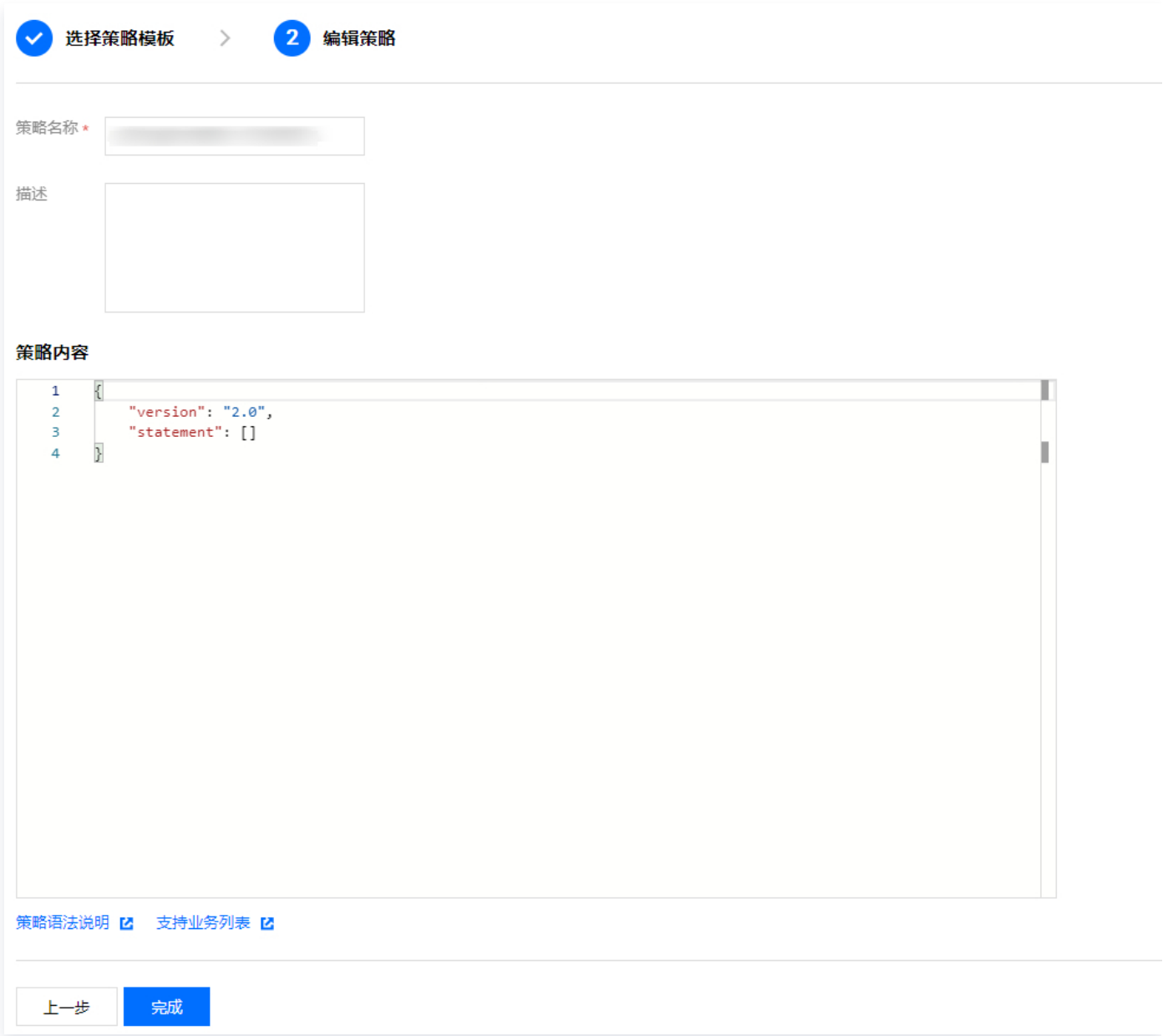
SaaS 服务级访问控制权限可以让子账号对自己创建的 SaaS 或主账号为其创建的 SaaS 拥有访问控制能力。
主账号已创建了一个或多个项目，并在某个项目下建立了若干 SaaS 服务。例如某项目下有2个 SaaS 服务，分配给2个不同的合作商，如下图所示：



操作步骤

创建策略

1. 使用腾讯云主账号登录 访问管理控制台，选择左侧菜单栏**策略**。
2. 进入策略页面，单击**新建自定义策略**。
3. 选择**按策略语法创建**。
4. 选择模板类型，勾选**空白模板**，单击**下一步**。
5. 填写自定义策略名称，并按照策略模板编辑策略内容。



策略内容

分配子账号所有权限，示例代码如下：

```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
        "*"
      ],
      "resource": [
        "qcs::iotcloud:gz:uin/your_uid:*",
        "qcs::iotexplorer:gz:uin/your_uid:project/your_project_id",
        "qcs::iotexplorer:gz:uin/your_uid:project/your_project_id/",
```

```
"qcs::iotexplorer:gz:uin/your_uid:project/your_project_id/service/your_ServiceAppID"
        ],
        "effect": "allow"
      }
   ]
}
```

策略说明如下：

- resource 对应的就是项目和 SaaS 。如果要把主账号某个项目 ID 的某个 SaaS ID 授权给某个子用户，则需要在 resource 部分增加下面3条。红色标注为需替换部分：`your_uid` 为用户账号 ID， `your_project_id` 为控制台项目 ID， `your_ServiceAppID` 为项目内 SaaS 服务 ID。

```
"qcs::iotexplorer:gz:uin/your_uid:project/your_project_id",
"qcs::iotexplorer:gz:uin/your_uid:project/your_project_id/",
"qcs::iotexplorer:gz:uin/your_uid:project/your_project_id/service/your_ServiceAppID"
```

- action： `*` 号表示所有操作。
- effect：allow 表示允许， deny 表示不允许。
- 项目策略语法使用说明，详情请参见 策略语法说明 。
  在 aciton 里面填 `*` （所有操作）将会放大操作权限，建议可指定 action，即将 SaaS 服务相关的 API 填在 action 中，示例代码如下所示：

```
{
    "version" :  "2.0" ,
    "statement" :  [ {
      "action" :  [
          "iotexplorer:GetProjectList" ,
          "iotexplorer:DescribeProject" ,
          "iotexplorer:CreateServceAppliation" ,
          "iotexplorer:DescribeServceAppliation" ,
          "iotexplorer:ModifyServceAppliation" ,
          "iotexplorer:GetServceAppliationList" ,
          "iotexplorer:DeleteServiceApplication"
      ] ,
      "resource" :  [
          "qcs::iotcloud:gz:uin/your_uid:*" ,
          "qcs::iotexplorer:gz:uin/your_uid:project/your_project_id" ,
          "qcs::iotexplorer:gz:uin/your_uid:project/your_project_id/" ,
```

```
"qcs::iotexplorer:gz:uin/your_uid:project/your_project_id/service/your_ServiceAppID"
      ] ,
      "effect" :  "allow"
    } ]
}
```

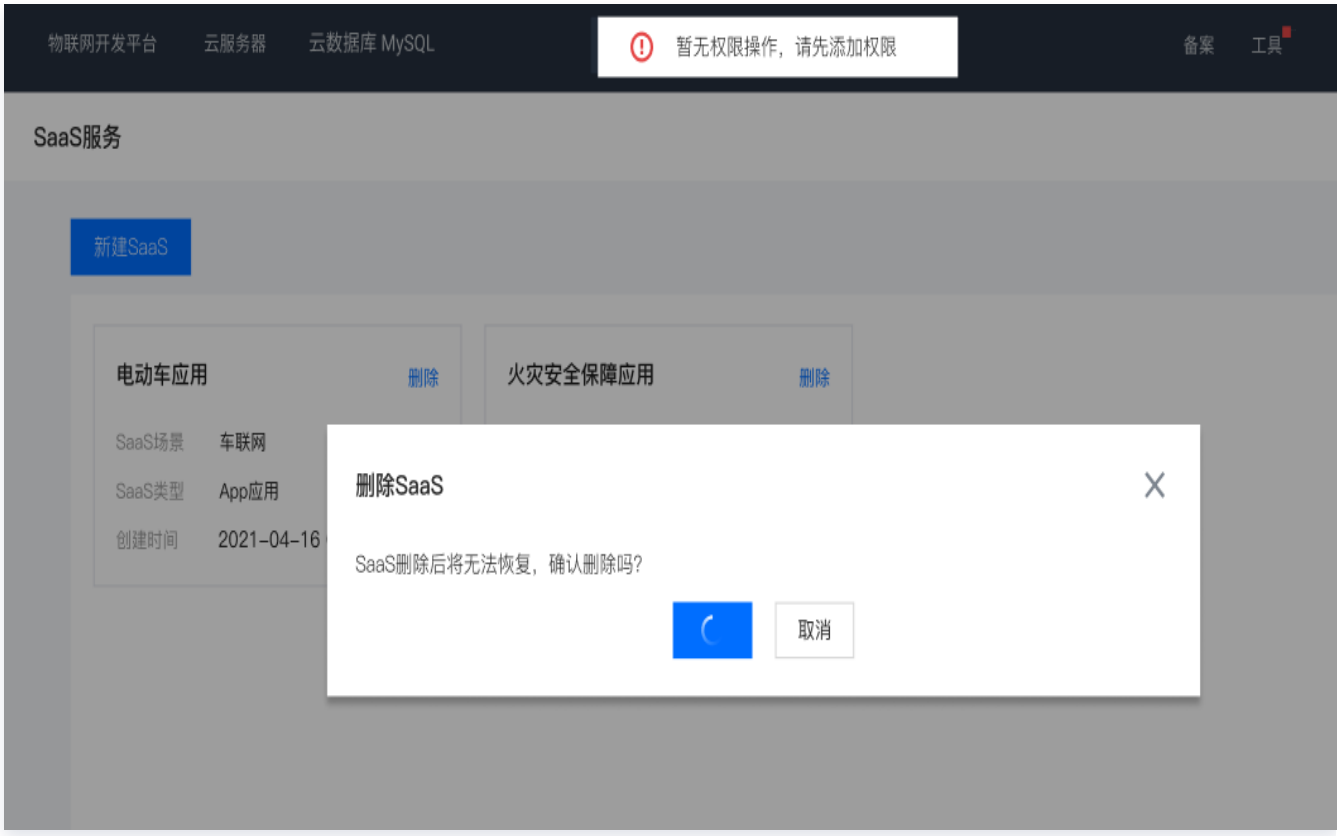
- 禁用子账号部分权限（此处示例禁用子账号删除 SaaS 权限）。

```
{
  "version": "2.0",
  "statement": [{
        "action": [
          "*"
        ],
        "resource": [
          "qcs::iotcloud:gz:uin/your_uid:*",
          "qcs::iotexplorer:gz:uin/your_uid:project/your_project_id",
          "qcs::iotexplorer:gz:uin/your_uid:project/your_project_id/",

"qcs::iotexplorer:gz:uin/your_uid:project/your_project_id/service/your_ServiceAppID"
        ],
        "effect": "allow"
      },
      {
        "action": [
          "iotexplorer:DeleteServiceApplication"
        ],
        "resource": [
          "qcs::iotcloud:gz:uin/your_uid:*",
          "qcs::iotexplorer:gz:uin/your_uid:project/your_project_id",
          "qcs::iotexplorer:gz:uin/your_uid:project/your_project_id/",

"qcs::iotexplorer:gz:uin/your_uid:project/your_project_id/service/your_ServiceAppID"
        ],
        "effect": "deny"
      }
  ]
}
```

- action：输入相关的接口名称，例如 `DeleteServiceApplication`（删除 SaaS 服务）。
  - effect：allow 表示允许， deny 表示不允许。
    当子账号登录 物联网开发平台，单击项目进入项目详情页面，单击**物联使能** > **SaaS服务**进入 SaaS 服务列表页。进行删除 SaaS 服务操作时，会弹出窗口提示暂无权限。



在禁用子账号部分操作权限时，也可在指定 Action 时不填写对应的服务 API，如不填写删除 SaaS 服务 `DeleteServiceApplication`，即不用再单独添加 Deny。示例代码如下所示：

```
{
  "version": "2.0",
  "statement": [{
    "action": [
      "iotexplorer:GetProjectList",
      "iotexplorer:DescribeProject",
      "iotexplorer:CreateServceAppliation",
      "iotexplorer:DescribeServceAppliation",
      "iotexplorer:ModifyServceAppliation",
      "iotexplorer:GetServceAppliationList"
    ],
    "resource": [
      "qcs::iotcloud:gz:uin/your_uid:*",
      "qcs::iotexplorer:gz:uin/your_uid:project/your_project_id",
      "qcs::iotexplorer:gz:uin/your_uid:project/your_project_id/",

"qcs::iotexplorer:gz:uin/your_uid:project/your_project_id/service/your_ServiceAppID"
    ],
    "effect": "allow"
  }]
}
```

关联策略

1. 自定义策略创建完毕后，进入**用户** > **用户列表**页面，选择想要赋予权限的子账号。
2. 单击用户类型为“子用户”的**用户名称**进入用户详情页，在“权限”栏中，单击**关联策略**。

3. 选择**从策略列表中选取策略关联**，搜索并勾选刚才创建的策略名称，单击**下一步** > **确定**，即可完成授予策略中定义的权限。