混沌演练平台

权限管理指南

腾讯云

文档目录

权限管理指南

概述

最近更新时间：2023-09-19 19:33:51

如果您在腾讯云中使用到了混沌演练平台（Chaos Fault Generator，CFG），且该服务虽然由不同的人管理，但都统一使用您的云账号密钥，将存在以下问题：

- 您的密钥由多人共享，泄密风险高。
- 您无法限制其他人的访问权限，其他人误操作易造成安全风险。

为解决以上问题，您可以通过使用子账号来实现不同的人管理不同的业务。默认情况下，子账号没有使用 CFG 的权限，我们需要创建策略来允许子账号拥有他们所需要的权限。

简介

访问管理（Cloud Access Management，CAM）是腾讯云提供的一套 Web 服务，它主要用于帮助客户安全管理腾讯云账户下的资源的访问权限。通过 CAM，您可以创建、管理和销毁用户（组），并通过身份管理和策略管理控制哪些人可以使用哪些腾讯云资源。
当您使用 CAM 时，可以将策略与一个用户或一组用户关联起来，策略能够授权或者拒绝用户使用指定资源完成指定任务。有关 CAM 策略的更多相关基本信息，请参见 策略语法 。有关 CAM 策略的更多相关使用信息，请参见 策略 。
若您无需对子账号进行 CAM 相关资源的访问管理，您可以跳过此章节。跳过这些部分不会影响您对文档中其余部分的理解和使用。

入门

CAM 策略必须授权使用一个或多个 CFG 操作或者必须拒绝使用一个或多个 CFG 操作。同时还必须指定可以用于操作的资源（可以是全部资源，某些操作也可以是部分资源），策略还可以包含操作资源所设置的条件。
CFG 部分 API 操作不支持资源级权限，意味着，对于该类 API 操作，您无法在使用该类操作的时候指定某个具体的资源来使用，而必须指定全部资源来使用。

授权策略语法

最近更新时间：2023-09-19 19:33:51

策略语法

CAM 策略：

```
{
    "version":"2.0",
    "statement":
    [
      {
        "effect":"effect",
        "action":["action"],
        "resource":["resource"],
      }
    ]
}
```

- **版本 version**：必填项，目前仅允许值为"2.0"。
- **语句 statement**：用来描述一条或多条权限的详细信息。该元素包括 effect、action、resource、condition 等多个其他元素的权限或权限集合。一条策略有且仅有一个 statement 元素。
- **影响 effect**：必填项，描述声明产生的结果是“允许”还是“显式拒绝”，包括 allow（允许）和 deny（显式拒绝）两种情况。
- **操作 action**：必填项，用来描述允许或拒绝的操作。操作可以是 API（以 cfg: 前缀描述）。
- **资源 resource**：必填项，描述授权的具体数据。资源是用六段式描述，每款产品的资源定义详情会有所区别。

混沌演练平台的操作

在混沌演练平台策略语句中，您可以从支持混沌演练平台的任何服务中指定任意的 API 操作。对于混沌演练平台，请使用以 cfg: 为前缀的 API。例如：cfg:CreateTask 或者 cfg:CreateTemplate 。
如果您要在单个语句中指定多个操作时，请使用逗号将它们隔开，如下所示：

```
"action":["cfg:action1","cfg:action2"]
```

您也可以使用通配符指定多项操作。例如：您可以指定名字以单词" Describe "开头的所有操作，如下所示：

```
"action":["cfg:Describe*"]
```

如果您要指定云数据库中所有操作，请使用 * 通配符，如下所示：

```
"action": ["cfg:*"]
```

混沌演练平台的资源

每个 CAM 策略语句都有适用于自己的资源。资源的一般形式如下：

```
qcs:project_id:service_type:region:account:resource
```

- **project_id**：描述项目信息，仅为了兼容 CAM 早期逻辑，无需填写。
- **service_type**：产品简称，如 cfg。
- **region**：地域信息，如 ap-guangzhou。
- **account**：资源拥有者的主账号信息，如 uin/653339763。
- **resource**：各产品的具体资源详情，如 instanceId/instance_id1 或者 instanceId/*。

例如：您可以使用特定任务ID（1）在语句中指定它，如下所示：

```
"resource":[ "qcs::cfg:ap-guangzhou:uin/11111:taskid/1"]
```

您还可以使用 * 通配符指定属于特定账户的所有实例，如下所示：

```
"resource":[ "qcs::cfg:ap-guangzhou:uin/11111:taskid/*"]
```

您要指定所有资源，或者如果特定 API 操作不支持资源级权限，请在 resource 元素中使用 * 通配符，如下所示：

```
"resource": ["*"]
```

如果您想要在一条指令中同时指定多个资源，请使用逗号将它们隔开，如下所示为指定两个资源的例子：

```
"resource":["resource1","resource2"]
```

下表描述了混沌演练平台能够使用的资源和对应的资源描述方法。其中，$ 为前缀的单词均为代称，region 指地域，account 指账户 ID。

资源	授权策略中的资源描述方法
演练任务	qcs::cfg:$region:$account:taskid/$TaskId
经验库	qcs::cfg::$account:templateid/$TemplateId
自定义动作	qcs::cfg::$account:actionid/$ActionId

可授权资源类型

最近更新时间：2022-01-06 11:05:20

资源级权限指能够指定用户对哪些资源具有执行操作的能力。
混沌演练平台部分支持资源级权限，即表示针对支持资源级权限的混沌演练平台操作，您可以控制何时允许用户执行操作或是允许用户使用特定资源。
访问管理 CAM 中可授权的资源类型如下：

资源类型	授权策略中的资源描述方法
混沌演练平台演练任务相关	qcs::cfg:$region:$account:taskid/* qcs::cfg:$region:$account:taskid/$TaskId
混沌演练平台经验库相关	qcs::cfg::$account:template/* qcs::cfg::$account:template/$TemplateId
混沌演练平台自定义动作相关	qcs::cfg::$account:actionid/* qcs::cfg::$account:actionid/$ActionId

下表将介绍当前支持资源级权限的混沌演练平台 API 操作，以及每个操作支持的资源和条件密钥。指定资源路径时，您可以在路径中使用 * 通配符。

支持资源级授权的 API 列表

演练任务相关

API 操作	资源路径
DeleteTask	qcs::cfg:$region:$account:taskid/* qcs::cfg:$region:$account:taskid/$TaskId
DescribeTask	qcs::cfg:$region:$account:taskid/* qcs::cfg:$region:$account:taskid/$TaskId
DescribeTaskExecuteLogs	qcs::cfg:$region:$account:taskid/* qcs::cfg:$region:$account:taskid/$TaskId
DescribeTaskList	qcs::cfg:$region:$account:taskid/* qcs::cfg:$region:$account:taskid/$TaskId
DescribeTaskStatistics	qcs::cfg:$region:$account:taskid/* qcs::cfg:$region:$account:taskid/$TaskId
DescribeTaskStatisticsOperateCondition	qcs::cfg:$region:$account:taskid/* qcs::cfg:$region:$account:taskid/$TaskId
EditTask	qcs::cfg:$region:$account:taskid/* qcs::cfg:$region:$account:taskid/$TaskId
ExecuteTask	qcs::cfg:$region:$account:taskid/* qcs::cfg:$region:$account:taskid/$TaskId
ExecuteTaskInstance	qcs::cfg:$region:$account:taskid/* qcs::cfg:$region:$account:taskid/$TaskId
ModifyTaskResult	qcs::cfg:$region:$account:taskid/* qcs::cfg:$region:$account:taskid/$TaskId
ModifyTaskStatus	qcs::cfg:$region:$account:taskid/* qcs::cfg:$region:$account:taskid/$TaskId

经验库相关

API 操作	资源路径
DeleteTemplate	qcs::cfg::$account:template/* qcs::cfg::$account:template/$TemplateId
DescribeTemplate	qcs::cfg::$account:template/* qcs::cfg::$account:template/$TemplateId
DescribeTemplateList	qcs::cfg::$account:template/* qcs::cfg::$account:template/$TemplateId
EditTemplate	qcs::cfg::$account:template/* qcs::cfg::$account:template/$TemplateId
ModifyTemplateIsUsed	qcs::cfg::$account:template/* qcs::cfg::$account:template/$TemplateId

动作库相关

API 操作	资源路径
DescribeActionLibraryList	qcs::cfg::$account:actionid/* qcs::cfg::$account:actionid/$ActionId
DeleteCustomAction	qcs::cfg::$account:actionid/* qcs::cfg::$account:actionid/$ActionId
UpdateCustomAction	qcs::cfg::$account:actionid/* qcs::cfg::$account:actionid/$ActionId
DescribeCustomAction	qcs::cfg::$account:actionid/* qcs::cfg::$account:actionid/$ActionId

不支持资源级授权的 API 列表

针对不支持资源级权限的混沌演练平台 API 操作，您仍可以向用户授予使用该操作的权限，但策略语句的资源元素必须指定为 *。

API 操作	API 描述
CreateTask	创建演练任务
CreateTemplate	创建经验库
CreateCustomAction	创建自定义动作
DescribeActionFieldConfigList	获取动作栏位配置参数列表
DescribeActionLibraryList	获取动作库列表
DescribeCamIdentity	获取用户 CAM 服务授权信息
DescribeNoticeId	获取用户通知模板 ID
DescribeObjectMetrics	获取对象类型的监控指标信息
DescribeObjectTypeList	查询对象类型列表
DescribeRegionList	查询地域列表

服务授权与角色权限

最近更新时间：2021-10-27 11:22:23

在使用腾讯云混沌演练工程（Chaotic Fault Generator，CFG）的过程中，为了能够使用相关云资源，会遇到多种需要进行服务授权的场景。每种场景通常对应不同的角色所包含的预设策略，其中主要涉及到 CFG_QCSLinkedRoleInChaos 角色。本文档接下来将展示授权策略的详情、授权场景及授权步骤。

角色权限（CFG_QCSLinkedRoleInChaos）

开通混沌演练平台服务后，腾讯云会授予您的账户 CFG_QCSLinkedRoleInChaos 角色的权限。该服务角色默认关联多个预设策略，为获取相关权限，需在特定的授权场景下执行对应的预设策略授权操作。操作完成之后，对应策略会出现在该角色的已授权策略列表中。CFG_QCSLinkedRoleInChaos 角色关联的预设策略包含混沌演练平台服务对云资源的访问权限。

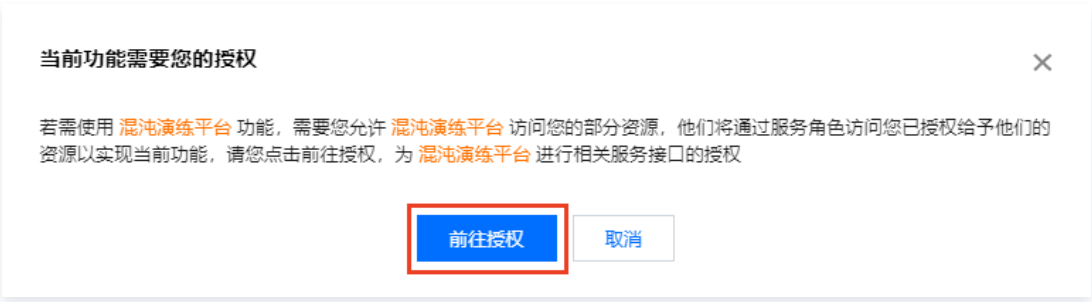
预设策略（QcloudAccessForCFGLinkedRoleInChaos）

授权场景

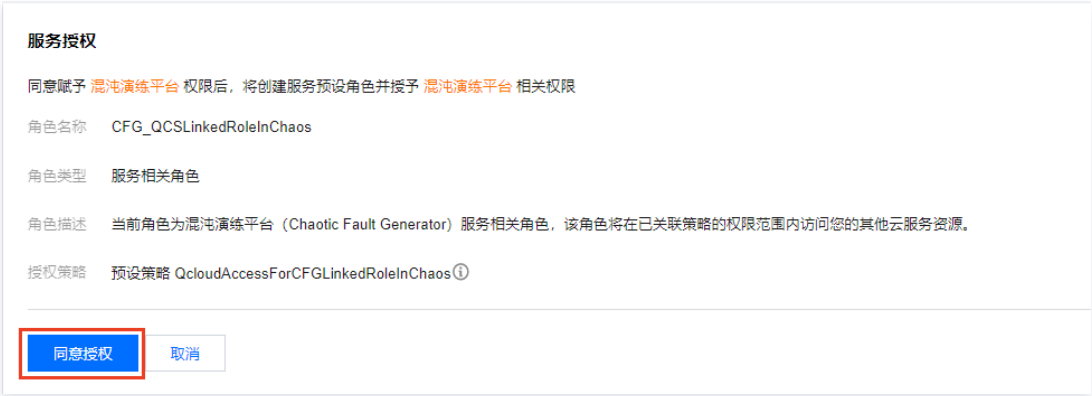
当您已注册并登录腾讯云账号后，首次登录 混沌演练平台控制台 时，需前往**访问管理**页面对当前账号授予腾讯云混沌演练平台服务操作云服务器（CVM）、负载均衡 (CLB)、腾讯云自动化助手(TAT)、弹性缓存 Redis(Redis)、 云数据库MySQL(CDB)、云监控(Monitor)、私有网络(VPC)等云资源的权限。

授权步骤

1. 登录 混沌演练平台控制台，选择左侧导航栏中的**演练管理**，弹出**服务授权**窗口。
2. 单击**前往授权**，进入**角色管理**页面。



3. 单击**同意授权**，完成身份验证后即可成功授权。



权限内容

负载均衡（CLB）

权限名称	权限说明
clb:DescribeTargets	查询应用型负载均衡云服务器列表
clb:BatchModifyTargetWeight	批量修改监听器绑定的后端机器的转发权重
clb:DescribeLoadBalancers	获取负载均衡实例列表
clb:SetLoadBalancerSecurityGroups	LB 绑定安全组

腾讯云自动化助手(TAT)

权限名称	权限说明
tat:DescribeAutomationAgentStatus	查询客户端状态
tat:DescribeCommands	查询命令
tat:InvokeCommand	触发命令
tat:DescribeInvocations	查询执行结果
tat:RunCommand	运行临时命令
tat:DescribeInvocationTasks	查询执行任务

弹性缓存Redis(Redis)

权限名称	权限说明
redis:DescribeInstances	展示实例内容
redis:KillMasterGroup	模拟故障

云数据库MySQL(CDB)

权限名称	权限说明
cdb:DescribeDBInstances	查询实例列表
cdb:SwitchDBInstanceMasterSlave	支持用户主动切换实例主从角色
cdb:DescribeTasks	查询云数据库实例的任务列表
cdb:ModifyInstanceParam	修改实例参数
cdb:DescribeInstanceParams	查询实例的可设置参数列表
cdb:DescribeInstanceParamRecords	查询实例的参数修改历史

云服务器（CVM）

权限名称	权限说明
cvm:DescribeInstances	查询云主机 V3
cvm:RebootInstances	重启云主机 V3
cvm:StopInstances	关闭云主机 V3
cvm:StartInstances	启动云主机 V3
cvm:CreateSecurityGroup	创建安全组
cvm:DeleteSecurityGroup	删除安全组

云监控（monitor）

权限名称	权限说明
monitor:CreateAlarmNotice	创建告警通知
monitor:DescribeAlarmHistories	告警2.0查询告警历史
monitor:DescribeAlarmPolicies	告警2.0策略列表

monitor:DescribeBaseMetrics	拉取监控指标列表
monitor:GetMonitorData	拉取监控数据

私有网络（VPC）

权限名称	权限说明
vpc:ResetNatGatewayConnection	调整 NAT 网关并发连接上限 V3
vpc:DescribeNatGateways	查询 NAT 网关 V3
vpc:ModifyNatGatewayAttribute	修改 NAT 网关的属性 V3

子用户与授权

最近更新时间：2022-01-06 11:05:30

> **注意**
> 主账户需要在 角色 页面查看是否具有 QcloudAccessForCFGLinkedRoleInChaos ，如果没有，请按照 服务授权与角色权限 中的**预设策略**操作完成授权，否则子用户无法正常使用 CFG 控制台和通过 CFG 调用其他云上资源。

创建子用户并授予 CFG 的所有操作权限

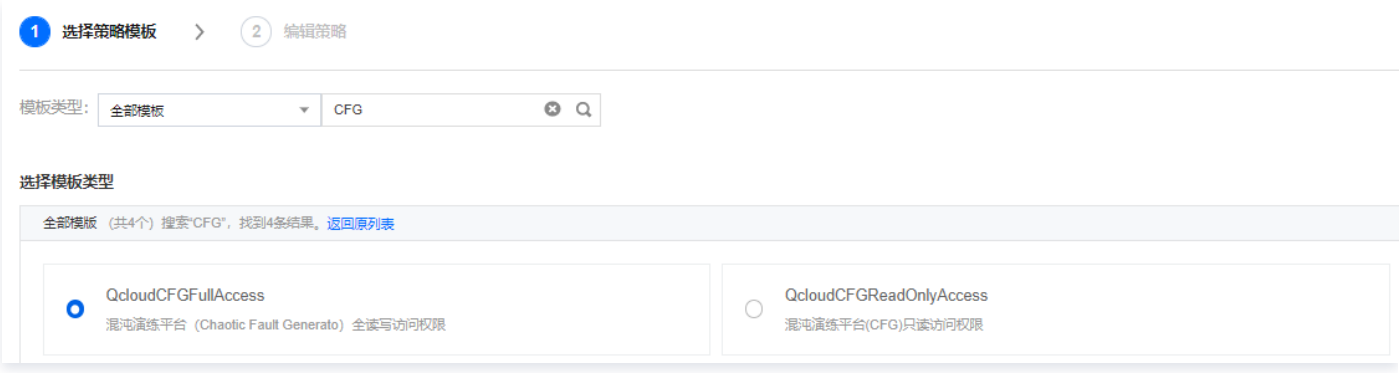
步骤1：使用主账号创建子用户

1. 登录 访问管理控制台，选择左侧导航栏中的**用户 > 用户列表**。
2. 在“用户列表”页面，选择**新建用户 > 自定义创建**，进入“新建子用户”页面。
3. 在“选择类型”步骤中，选择**可访问资源并接收消息**后单击**下一步**。
4. 在“填写用户信息”步骤中，您可批量创建子用户，设置访问方式和设置控制台密码等，请按需进行设置后单击**下一步**。
5. 在“设置用户权限”页面，按需选择不同的方式为当前新建的子用户设定权限，单击**下一步**保存设定，后续您可以更改相关权限设定。权限的三种设置方式：
   - 将子用户添加到现有用户组或新建用户组。
   - 复制现有用户权限。
   - 从策略列表中授权。
6. 在“审阅信息和权限”页面，确认信息无误之后单击**完成**，完成自定义创建子用户操作。

> **说明**
> 相关文档请参见 创建子用户 。

步骤2：创建自定义策略

1. 登录 访问管理控制台，选择左侧导航栏中的 策略 。
2. 在“策略”管理页面，选择**新建自定义策略 > 按策略语法创建**，进入创建页面。
3. 模板类型选择 CFG，并选择 **QcloudCFGFullAccess**，单击**下一步**。



4. 参考以下的授权语法，实现的效果是允许子账号操作 CFG 的全部功能和允许使用 CFG 角色操作相应资源。具体可以参考 CFG 角色说明 。

```
{
 "version": "2.0",
 "statement": [
    {
       "action": "cfg:*",
       "resource": "*",
       "effect": "allow"
    },
    {
       "effect": "allow",
       "action": "cam:PassRole",
       "resource": "qcs::cam::uin/${OwnerUin}:role/tencentcloudServiceRoleName/CFG_QCSLinkedRoleInChaos"
```

```
    }
  ]
}
```

步骤3：把策略关联到用户/用户组

1. 在“策略”管理页面，单击新建策略右侧的**关联用户/组**，弹出关联提示框。
2. 选择需要关联的用户，单击**确定**完成关联操作。您还可以切换用户或用户组，进行选择。

步骤4：为子用户添加 CAM 只读权限

1. 登录 访问管理控制台，选择左侧导航栏中的**用户** > 用户列表 。
2. 在“用户列表”页面，选择需要设置权限的子用户，进入**用户详情**页面。
3. 在“用户详情”页面，单击**关联策略**，进入**添加策略**页面。
4. 在“设置用户权限”步骤中，选择**从策略列表中选取策略关联**，勾选 QcloudCamReadOnlyAccess，单击**下一步**。
5. 在“审阅用户权限”步骤中，单击**确定**，完成子用户“用户与权限（CAM）只读访问权限”的授权。完成上述操作后，CFG 才能通过子用户获取到主账户已有的权限，完成鉴权流程。

步骤5：为子用户授权 CAM

以上设置完成后，用户可以登录子账号查看权限。
登录 访问管理控制台，选择左侧的导航栏中的 概览 进入概览页面，即可查看子用户登录地址。

创建子用户并授予 CFG 的部分操作权限

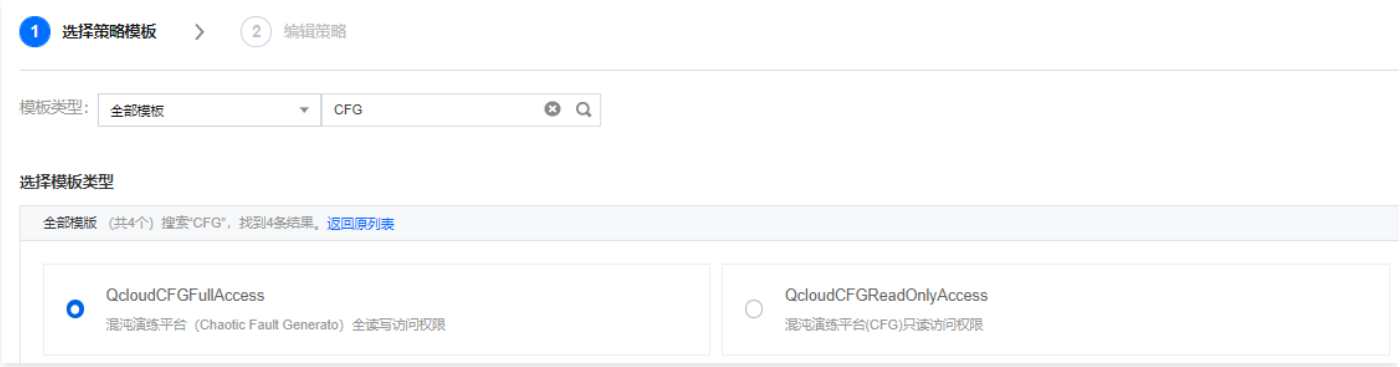
步骤1：使用主账号创建子用户

1. 登录 访问管理控制台，选择左侧导航栏中的**用户 > 用户列表**。
2. 在“用户列表”页面，选择**新建用户 > 自定义创建**，进入“新建子用户”页面。
3. 在“选择类型”步骤中，选择**可访问资源并接收消息**后，单击**下一步**。
4. 在“填写用户信息”步骤中，您可批量创建子用户，设置访问方式和设置控制台密码等，请按需进行设置后单击**下一步**。
5. 在“设置用户权限”页面，按需选择不同的方式为当前新建的子用户设定权限，单击**下一步**保存设定，后续您可以更改相关权限设定。权限的三种设置方式：
   - 将子用户添加到现有用户组或新建用户组。
   - 复制现有用户权限。
   - 从策略列表中授权。
6. 在“审阅信息和权限”页面，确认信息无误之后单击**完成**，完成自定义创建子用户操作。

> **说明**
> 相关文档请参见 创建子用户 。

步骤2：创建自定义策略

1. 登录 访问管理控制台，选择左侧导航栏中的 策略 。
2. 在“策略”管理页面，选择**新建自定义策略 > 按策略语法创建**，进入创建页面。
3. 模板类型选择 CFG，并选择 QcloudCFGFullAccess ，单击**下一步**。



4. 参考以下的授权语法，实现的效果是允许子账号操作 CFG 的全部功能和允许使用 CFG 角色操作相应资源。具体可以参考 CFG 角色说明

```
{
 "version": "2.0",
 "statement": [
    {
       "action": "cfg:*",
       "resource": "*",
       "effect": "allow"
    },
    {
       "effect": "allow",
       "action": "cam:PassRole",
       "resource": "qcs::cam::uin/${OwnerUin}:role/tencentcloudServiceRoleName/CFG_QCSLinkedRoleInChaos"
    }
 ]
}
```

> **注意**
> resource 中的资源描述，需要替换成主账号的 ID。

步骤3：把策略关联到用户/用户组

1. 在“策略”管理页面，单击新建策略右侧的**关联用户/组**，弹出关联提示框。
2. 选择需要关联的用户，单击**确定**完成关联操作。您还可以切换用户或用户组，进行选择。

步骤4：为子用户添加 CAM 只读权限

1. 登录 访问管理控制台，选择左侧导航栏中的**用户** > 用户列表 。
2. 在“用户列表”页面，选择需要设置权限的子用户，进入**用户详情**页面。
3. 在“用户详情”页面，单击**关联策略**，进入**添加策略**页面。
4. 在“设置用户权限”步骤中，选择**从策略列表中选取策略关联**，勾选 QcloudCamReadOnlyAccess，单击**下一步**。
5. 在“审阅用户权限”步骤中，单击**确定**，完成子用户“用户与权限（CAM）只读访问权限”的授权。完成上述操作后， CFG 才能通过子用户获取到主账户已有的权限，完成鉴权流程。

步骤5：完成

以上设置完成后，用户可以登录子账号查看权限。在左侧的导航栏中单击 概览 进入概览页面，可以查看子用户登录地址。

> **说明**
> 策略生效后，当前子账号可以看到所有的函数名，但是只能对 resource 中的函数进行操作和查看。

示例

> **说明**
> 以下示例仅为展示 CAM 用法，一个 CFG 混沌演练任务完成流程。在使用时，请将 OwnerUin 替换成主账号的 UIN。

```
{
  "version": "2.0",
  "statement": [
    {
       "action": "cfg:*",
       "resource": "*",
       "effect": "allow"
    },
    {
       "effect": "allow",
       "action": "cam:PassRole",
```

```
        "resource": "qcs::cam::uin/${OwnerUin}:role/tencentcloudServiceRoleName/CFG_QCSLinkedRoleInChaos"
      },
      {
        "action": [
          "tag:DescribeTagKeys",
          "tag:DescribeTagValues",
          "tag:DescribeResourceTagsByResourceIds",
          "tag:AttachResourcesTag",
          "tag:ModifyResourcesTagValue",
          "tag:DetachResourcesTag"
        ],
        "resource": "*",
        "effect": "allow"
      },
      {
        "action": [
          "monitor:DescribeAlarmPolicies"
        ],
        "resource": "*",
        "effect": "allow"
      }
    ]
}
```