访问管理

最佳实践

产品文档

腾讯云

文档目录

最佳实践
安全最佳实践

最近更新时间：2024-01-23 17:59:15

基本指导原则

1.开启 MFA 保护

为增强账号安全性，建议您为所有账号绑定 MFA；为主账号及子账号都开启登录保护和敏感操作保护。对于支持邮箱登录的强烈推荐进行 MFA 二次验证。开启 MFA 后，账号登录及敏感操作需进行二次校验。相关设置请参考：为协作者设置安全保护、为子用户设置安全保护。

2.使用子账号访问腾讯云

请尽量不要使用主账号的身份凭证访问腾讯云，更不要将身份凭证共享给他人。一般情况下，应该为所有访问腾讯云的用户创建子账号，同时授权该子账号相应的管理权限。相关设置请参考：用户类型。

3.使用组给子账号分配权限

按照工作职责定义好组，并给组分配相应的管理权限。然后把用户分配到对应的组里。这样，当您修改组的权限时，组里相关用户的权限随即发生变更。另外，当组织架构发生调整时，只需要更新用户和组的关系即可。相关设置请参考：用户组。

4.最小权限原则

最小权限原则是一项标准的安全原则。即仅授予执行任务所需的最小权限，不要授予更多无关权限。例如，一个用户仅是 CDN 服务的使用者，那么不需要将其他服务的资源访问权限（如 COS 读写权限）授予给该用户。

5.分子账号管理用户、权限和资源

建议同一个子账号不同时管理用户、权限和资源。应该让部分子账户管理用户，部分子账号管理权限，部分子账号管理其他云资源。

6.定期轮转身份凭证

建议您或 CAM 用户要定期轮换登录密码或云 API 密钥。这样可以让身份凭证泄漏情况下的影响时间受限。
主账号密码设置请参考：账号密码。
子用户密码设置请参考：子用户重置密码。

7.删除不需要的证书和权限

删除用户不需要的证书以及用户不再需要的权限。尽量减少访问凭证泄漏后带来的安全风险。

8.使用策略条件来增强安全性

尽可能的为策略定义更精细化的条件，约束策略生效的场景，强化安全性。如约束用户必须在指定的时间，指定的服务器上执行某些操作等。
相关设置请参考：元素参考 condition。

多身份人员权限管理

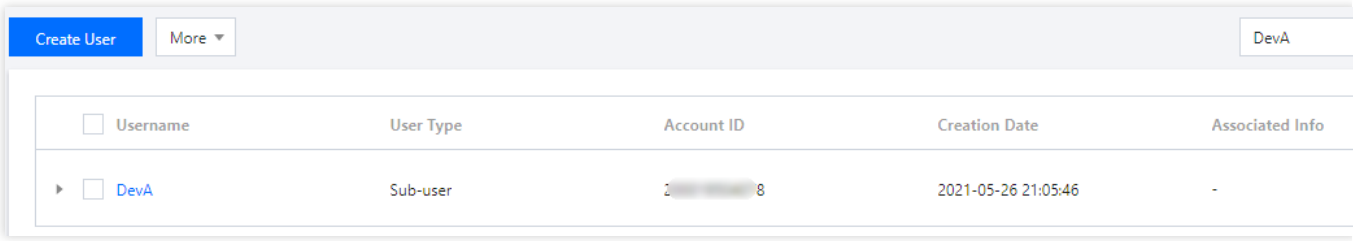
最近更新时间：2024-01-23 17:59:15

操作背景

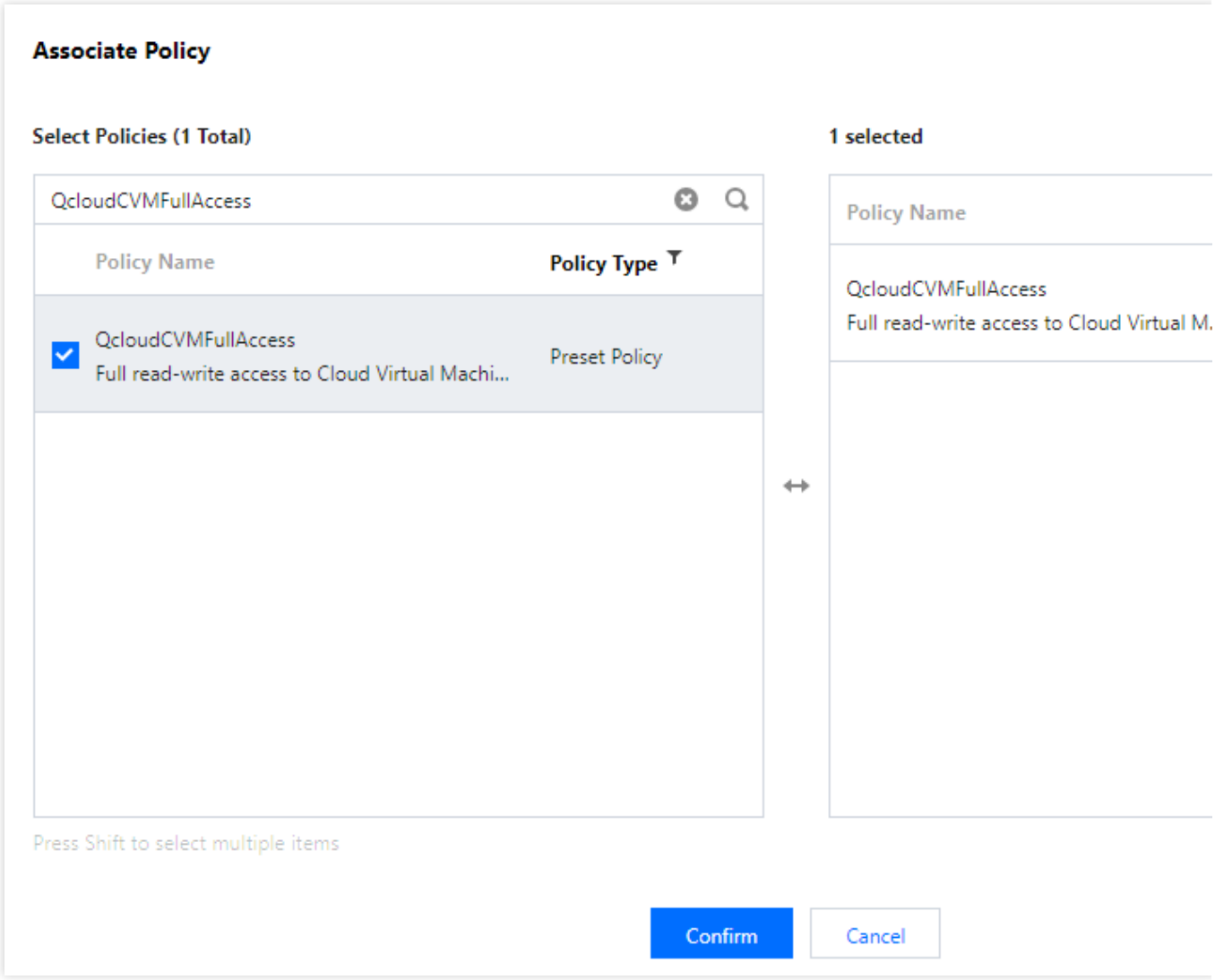
当您的企业涉及不同身份管理人员时，通过 CAM 进行权限划分，对不同身份的人员授予不同的权限，方便管理和控制。本文档以一个典型案例让您轻松了解如何实现子账号不同身份的管理权限。
假设存在以下条件：
企业帐号 CompanyExample 下有两个运维人员 DevA、DevB。
运维人员 DevA 为公司服务器运维人员，企业帐号 CompanyExample 该运维人员拥有云服务器（CVM）的全部操作权限。
运维人员 DevB 为公司云数据库 MySQL 运维人员，企业帐号 CompanyExample 该运维人员拥有云数据库 MySQL 的全部操作权限。

操作步骤

1. 使用企业账号 CompanyExample 登录 访问管理控制台。
2. 通过 自定义创建子用户 创建用户名分别为 DevA、DevB 的两个子账号。
3. 在 用户列表 页面搜索找到刚才已创建的子账号 DevA，单击右侧操作列下的**授权**，如下图：



4. 在弹出的关联策略窗口，搜索勾选 QcloudCVMFullAccess，单击**确定**，如下图：



5. 参考步骤2和3，为子账号 DevB 关联 QcloudCDBFullAccess 权限。

6. 授权成功后，子账号 DevA 则拥有云服务器（CVM）的全部操作权限，子账号 DevB 则拥有云数据库 MySQL 的全部操作权限。

说明：

如需将 CAM 用户配置为其他角色，可按照以上流程操作，只需参考步骤2和3搜索并勾选相应的权限策略名。具体权限可参考 系统权限。

系统权限

负责人	策略名称	策略说明
管理员	AdministratorAccess	该策略允许您管理账户内所有用户及其权限、财务相关的信息、云服务资产。
财务管理	QCloudFinanceFullAccess	该策略允许您管理账户内财务相关的内容，例如：付款、开

员		票。
数据库管理员	QcloudCynosDBFullAccess	云原生数据库 TDSQL-C 全读写访问权限
	QcloudMariaDBFullAccess	云数据库 MariaDB 全读写访问权限
	QcloudSQLServerFullAccess	云数据库 SQL Server 全读写访问权限
	QcloudCDWPGFullAccess	云数据仓库 PostgreSQL（CDWPG）全读写访问权限
网络管理员	QcloudCLBFullAccess	负载均衡（CLB）全读写访问权限
	QcloudVPCFullAccess	私有网络（VPC）全读写访问权限
	QcloudDCFullAccess	专线接入（DC）全读写访问权限
监控管理员	QcloudMonitorFullAccess	云监控（MONITOR）全读写访问权限，包括查看用户组的权限
	QcloudCATFullAccess	云拨测（CAT）全读写访问权限

授予标签下部分操作权限

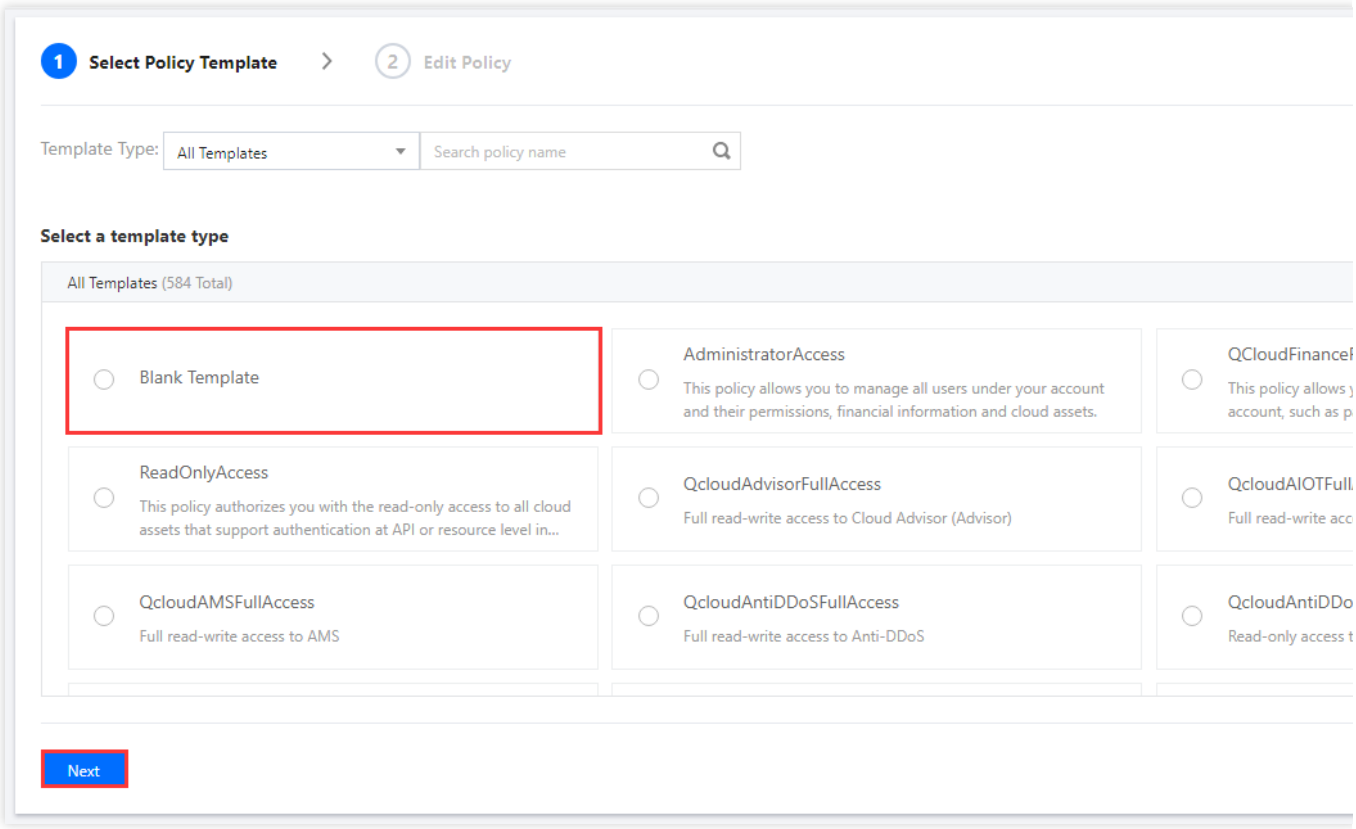
最近更新时间：2024-01-23 17:59:15

操作场景

若您的公司购买了多种腾讯云资源，资源均通过标签分组管理，希望能够授予不同团队员工按标签授予需要业务的部分接口操作权限。 本文档以一个典型案例让您轻松了解如何实现子账号拥有标签下资源的部分操作权限。
假设存在以下条件：
企业账号 CompanyExample 下有个子账号 DevA。
企业账号 CompanyExample 下有个为 test1&test1 的标签键值对。
企业账号 CompanyExample 希望给子账号 DevA 授予标签 test1&test1 下 CVM 资源的重启操作权限（cvm:RebootInstances ）。

操作步骤

1. 使用企业账号 CompanyExample 登录 访问管理控制台。
2. 在**策略**页面，单击**新建自定义策略** > 按策略语法创建。
3. 在选择模块类型下选择空白模板，单击**下一步**，进入编辑策略页面。

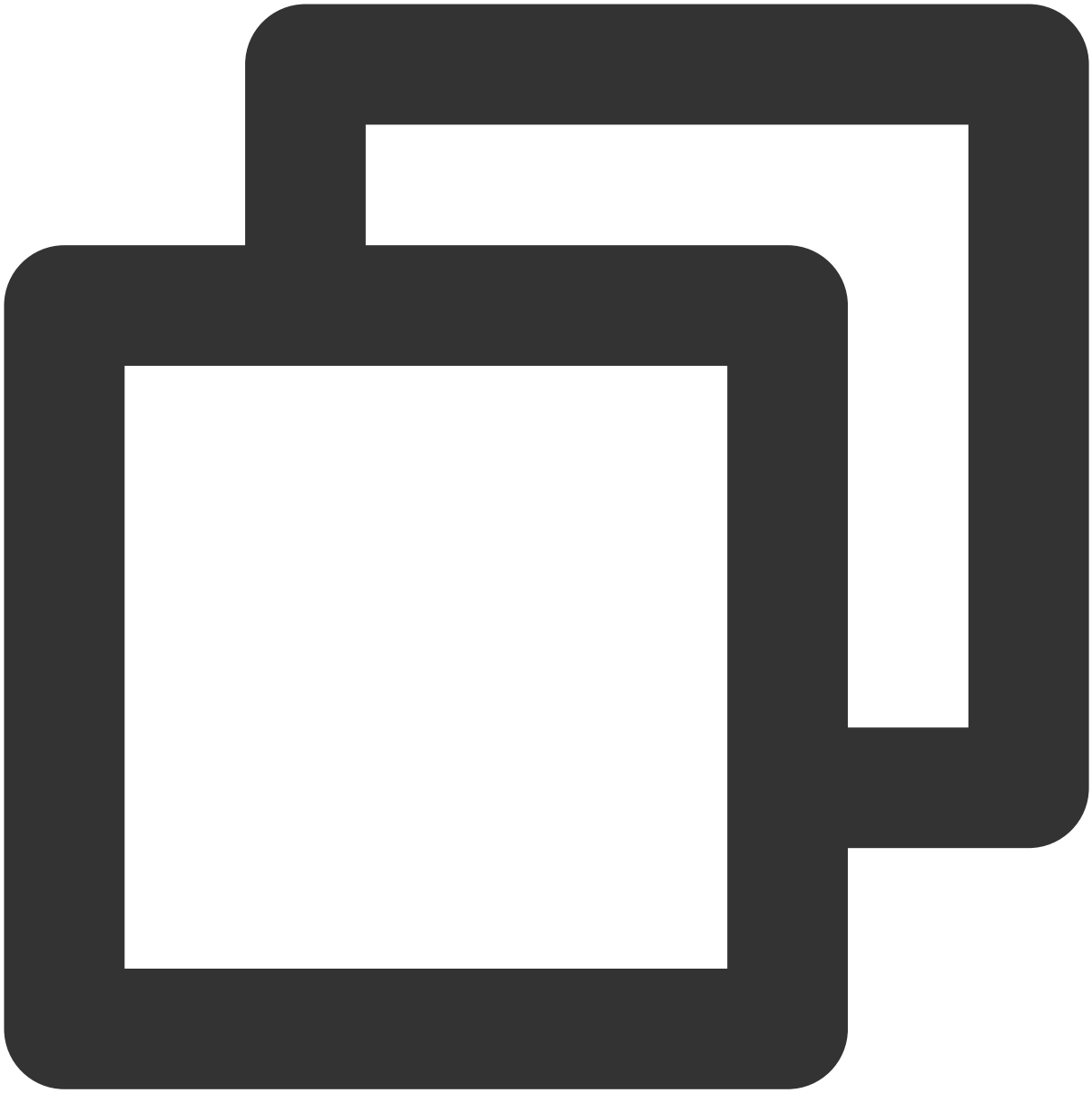


4. 进入编辑策略页面，填写如下表单：

策略名称：默认为 `policygen-当前日期` ，推荐您自行定义一个不重复且有意义的策略名称，例如 cvm-RebootInstances。

描述：可选，自行编写。

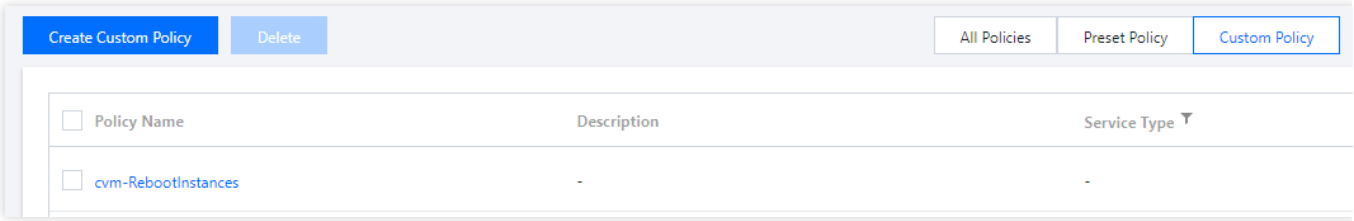
策略内容：复制以下内容并填写。其中， `cvm:RebootInstances` 为需要授权操作的接口名称， `test1&test1` 为需要授权操作的标签键及标签值。



```
{
"version": "2.0",
"statement": [
    {
        "effect": "allow",
        "action": [
            "cvm:RebootInstances"
        ],
        "resource": "*",
        "condition": {
            "for_any_value:string_equal": {
```

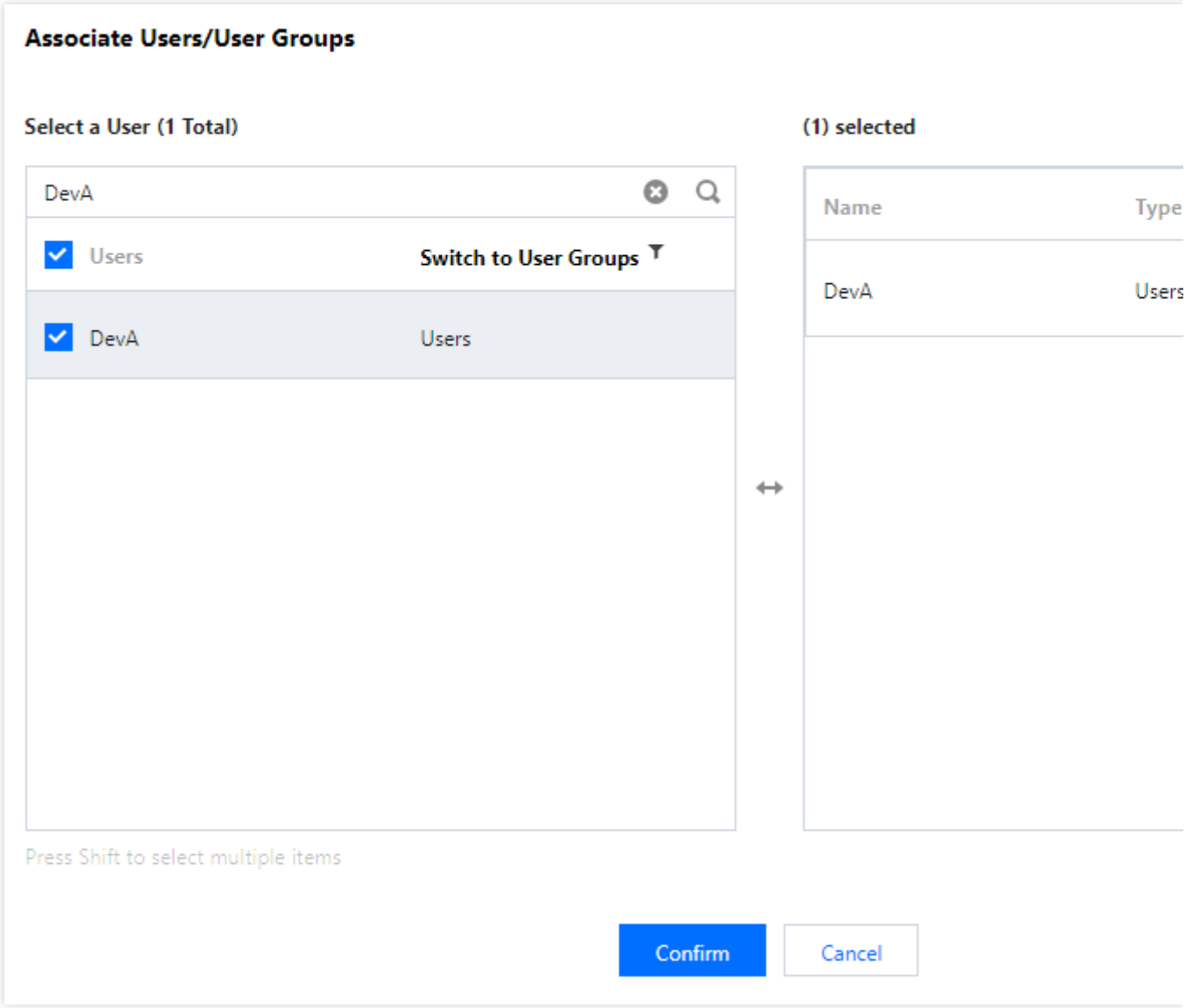
```
                "qcs:tag": [
                    "test1&test1"
                ]
            }
        }
    }
]
}
```

5. 单击**完成**，完成策略的创建。新建的策略将显示在策略列表页。
6. 在 策略列表 中搜索找到刚才已创建的策略，单击右侧操作列下的**关联用户/组**。



7. 在弹出的关联用户/用户组窗口中，搜索勾选子账号 DevA，单击**确定**完成授权操作。

子账号 DevA 将拥有标签 test1&test1 下 CVM 资源的重启操作权限。



关联文档

如果您想了解如何将资源和标签建立关联关系，请参阅 管理标签。
如果您想了解如何授予标签下资源的所有操作权限，请参阅 授权不同子账号拥有独立的云资源管理权限。

支持员工间资源隔离访问

概述

最近更新时间：2024-01-23 17:59:15

当一个主账号下有多个业务时，每个业务都有自己的资源，企业管理者会希望员工在使用CAM子账号登录时，不同业务的员工可以看到和操作的资源不同。
针对该场景，您可以通过访问管理（CAM）的两种权限设置方式（按照资源 ID 授权、按照标签授权）来实现资源的隔离访问。

场景说明

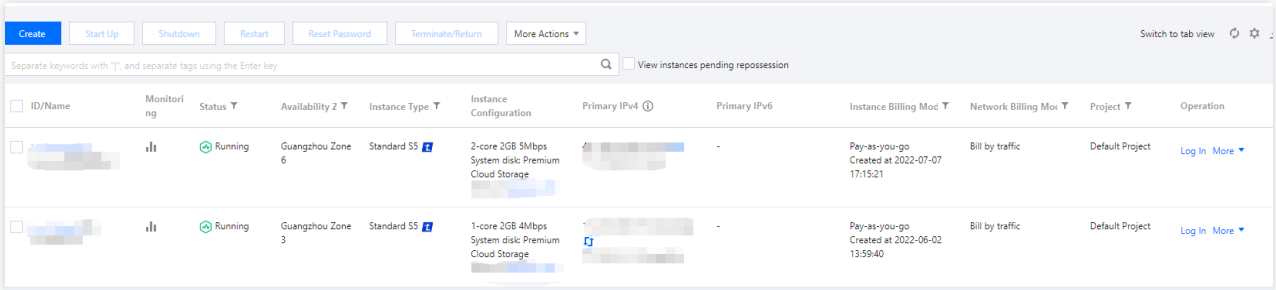
以云服务器（CVM）产品为例，假设在云上有两台云服务器，对应的信息如下：

资源 ID	镜像 ID	所属标签	所属项目
ins-duglsqg0	img-eb30mz89	game:webpage	webpage
ins-ijp192hy	img-eb30mz89	game:app	app

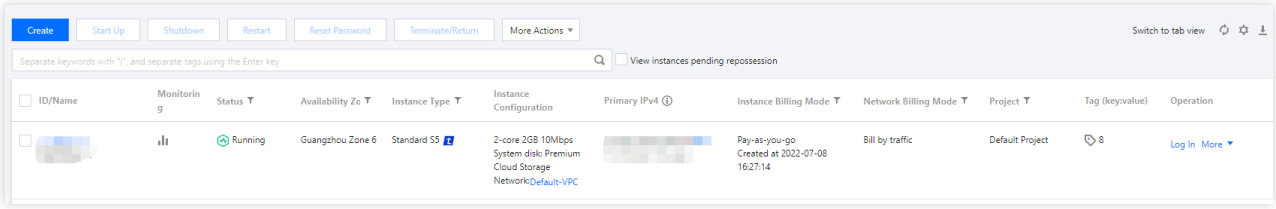
为员工创建 CAM 子用户 cvmtest01，通过上述两种权限设置方式实现 cvmtest01 只能查看和访问 ins-duglsqg0。

预期结果

使用管理员账号查看 CVM 广州区域列表效果：



使用 cvmtest01 查看 CVM 广州区域列表效果：



实现方式

方式一：按照资源 ID 授权

方式二：按照标签授权

按照资源 ID 授权

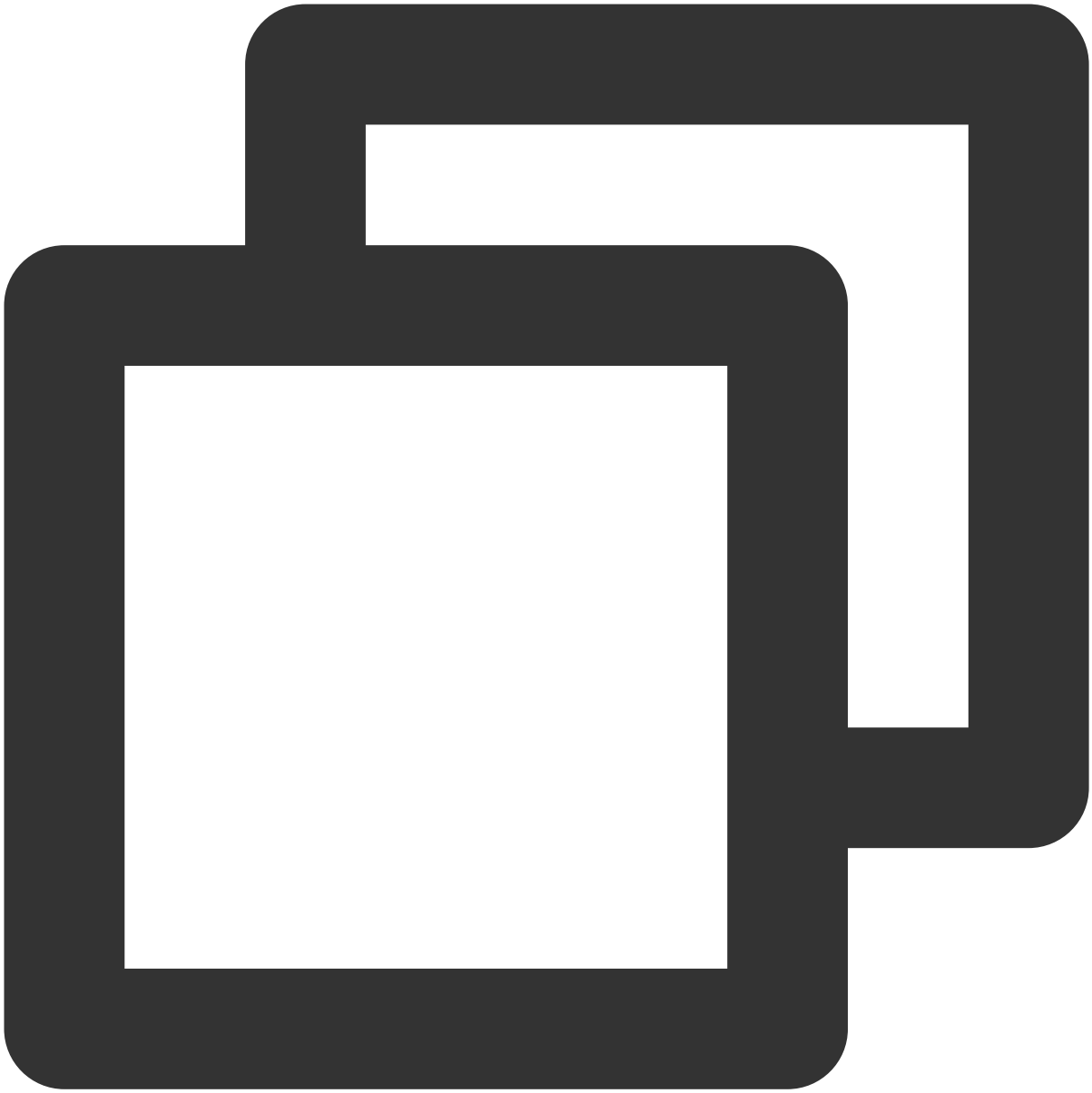
最近更新时间：2024-01-23 17:59:15

操作场景

该任务指导您按照资源 ID 授权，实现子用户 cvmtest01 只能管理 ins-duglsqg0。
查看详细操作场景 >>

策略内容

按照资源 ID 授权，最终实现上述预期结果时，对应的策略内容如下：



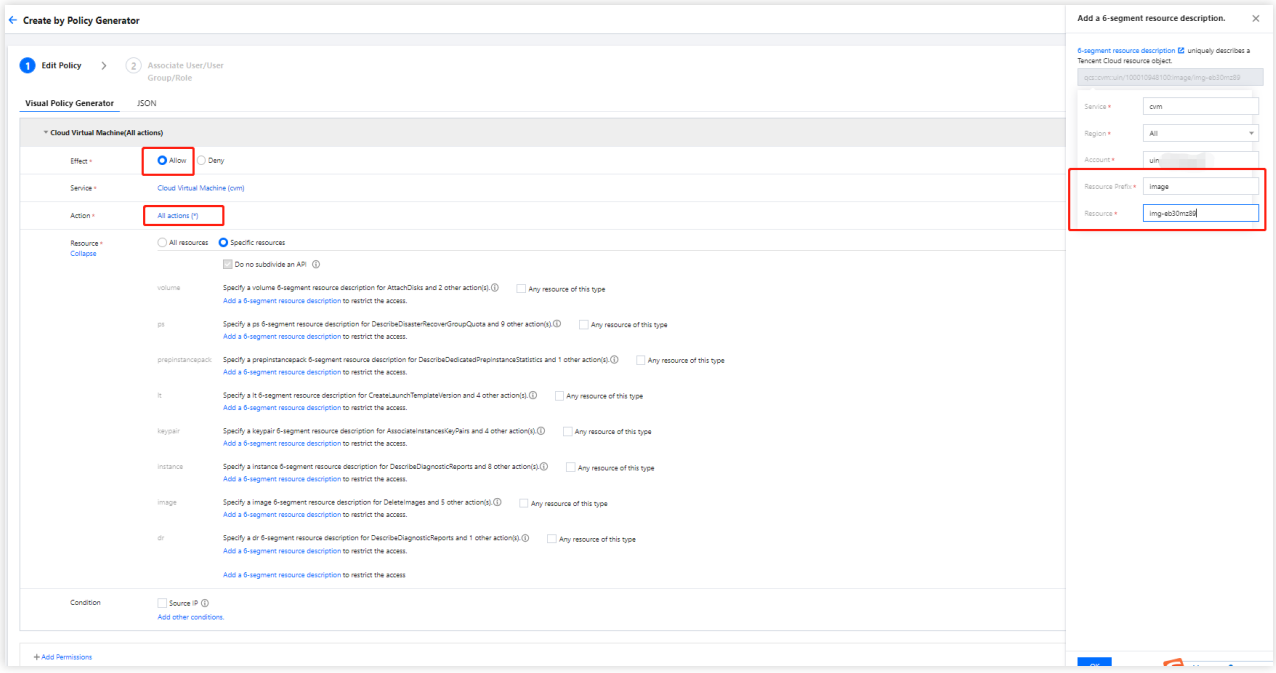
```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "cvm:*"
            ],
            "resource": [
                "qcs::cvm::uin/12345678:instance/ins-duglsqg0",//12345678为主账号UIN
                "qcs::cvm::uin/12345678:image/img-eb30mz89"
```

```
            ]
        },
        {
            "effect": "allow",
            "action": [
                "vpc:DescribeVpcEx",
                "vpc:DescribeNetworkInterfaces",
                "cvm:DescribeCbsStorages"
            ],
            "resource": [
                "*"
            ]
        }
    ]
}
```

操作步骤

步骤1：使用管理员账号创建策略并授权

1. 使用管理员账号登录访问管理控制台，在 策略 页面，按照策略生成器创建自定义策略（参考 创建自定义策略 - 按策略生成器创建）。



效果：允许

服务：云服务器cvm

操作：全部操作

资源：特定资源 - 添加自定义资源六段式

分别填写：资源前缀：instance 和资源 ID：ins-duglsqg0，以及资源前缀：image 和资源 ID：img-eb30mz89

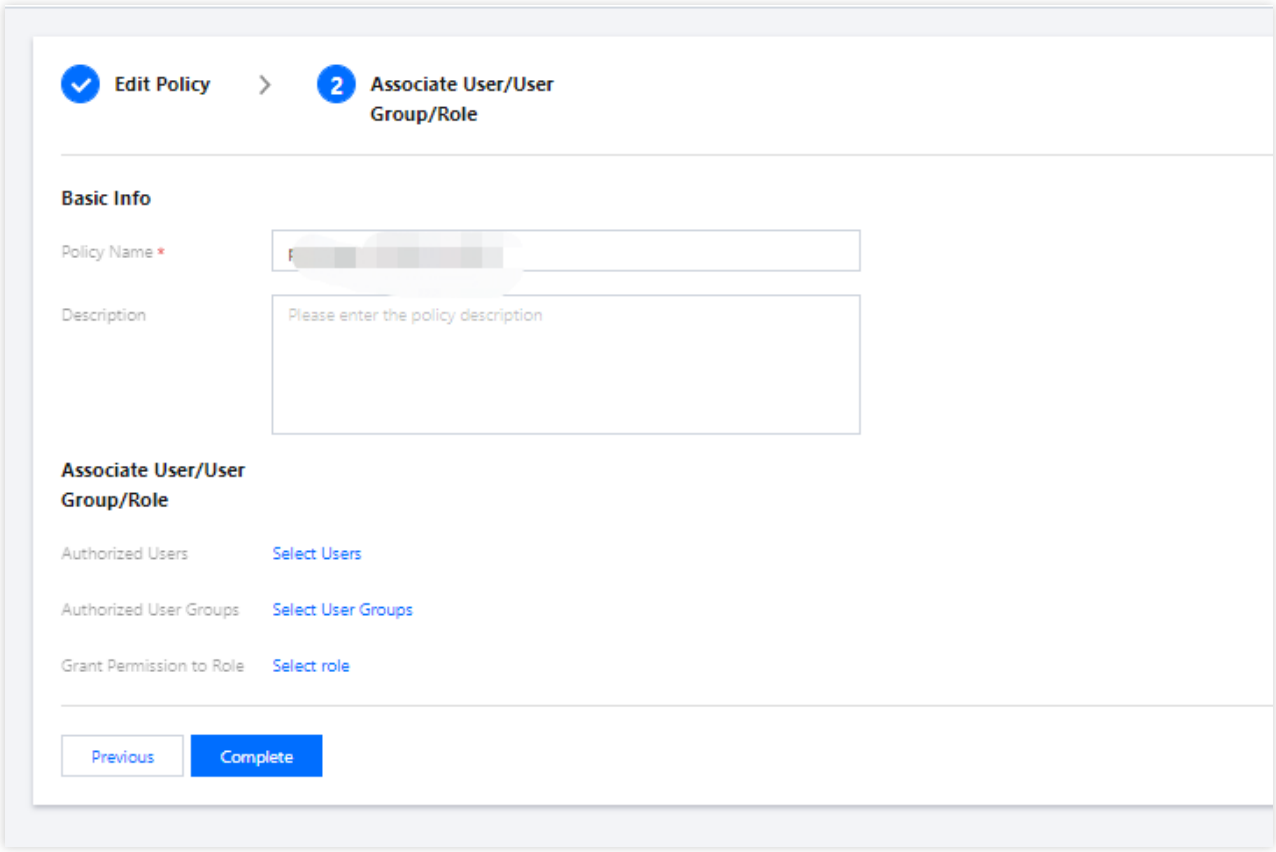
说明：

如何确定资源的前缀：在云服务器支持 CAM 的接口中有云服务器对应的资源六段式。

云服务器产品页面除了调用 CVM 相关接口外，还会使用 VPC 等接口，这时我们可以先跳过，继续生成策略，在实际操作的时候按照 CAM 的提示添加相关接口。

2. 单击**下一步**，指定策略的名称为 cvm-test01，并将策略授予子账号 cvmtest01。

3. 单击**完成**，完成授权。



步骤2：使用子账号登录验证权限

1. 使用子用户登录 云服务器控制台，进入实例列表页面。此时 CVM 页面会提示缺少 VPC 产品 DescribeVpcEx 以及对应资源的权限。

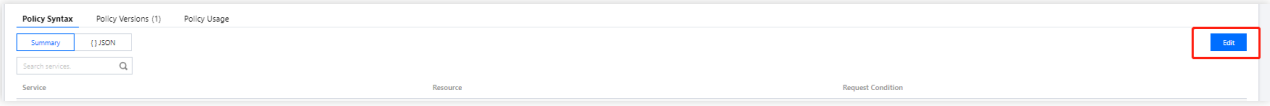
2. 根据页面提示内容，联系管理员账号在策略中添加对应授权。

步骤3：使用管理员账号调整策略内容

1. 使用主账号在VPC 支持 CAM 的接口清单中，找到 DescribeVpcEx 确定接口为操作级的接口。

2. 在访问管理控制台的 策略 页面，找到策略 cvm-test01，单击策略名进入策略详情。

3. 在策略语法中单击**编辑**，按照操作级接口的授权书写形式在策略详情中添加接口授权。



添加之前：

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "cvm:*"
            ],
            "resource": [
                "qcs::cvm::uin/[redacted]:instance/ins-duglsqg0",
                "qcs::cvm::uin/[redacted]:image/img-eb30mz89"
            ]
        }
    ]
}
```

添加之后：

```
        {
            "effect": "allow",
            "action": [
                "cvm:*"
            ],
            "resource": [
                "qcs::cvm::uin/[redacted]:instance/ins-duglsqg0",
                "qcs::cvm::uin/[redacted]:image/img-eb30mz89"
            ]
        },
        {
            "effect": "allow",
            "action": [
                "vpc:DescribeVpcEx"
            ],
            "resource": [
                "*"
            ]
        }

    ]
}
```

4. 添加之后重复 步骤2，使用子账号 cvmtest01 再次验证，发现仍有异常，缺少 VPC 下 DescribeNetworkInterfaces 以及对应资源的访问权限，查看私有网络支持 CAM 的接口确定 DescribeNetworkInterfaces 为操作级的接口。

5. 按照 步骤3 继续调整策略内容，直至系统没有报错。

最终策略的内容如下：

```
{
    "statement": [
        {
            "effect": "allow",
            "action": [
                "cvm:*"
            ],
            "resource": [
                "qcs::cvm::uin/[redacted]:instance/ins-duglsqg0",
                "qcs::cvm::uin/[redacted]:image/img-eb30mz89"
            ]
        },
        {
            "effect": "allow",
            "action": [
                "vpc:DescribeVpcEx",
                "vpc:DescribeNetworkInterfaces",
                "cvm:DescribeCbsStorages"
            ],
            "resource": [
                "*"
            ]
        }
    ]
}
```

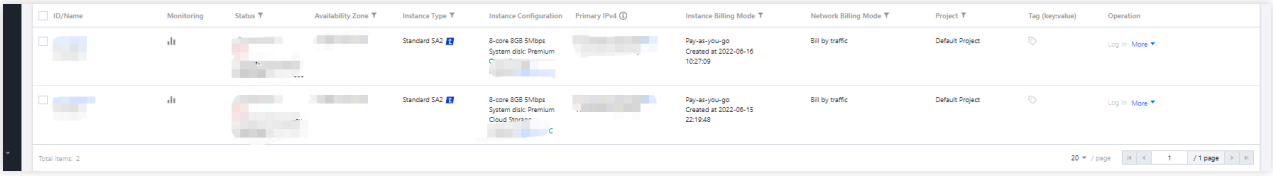
说明：

在书写 CAM 策略时，在需要操作具体资源时，资源级的接口授权需要和操作级分开书写，多个操作级接口可以书写在一起。

步骤4：验证结果

使用子用户 cvmtest01 再次验证，达到预期效果。

至此，子用户 cvmtest01 可以对实例进行开关机、重启、更名、重置密码等操作。



按照标签授权

最近更新时间：2024-01-23 17:59:15

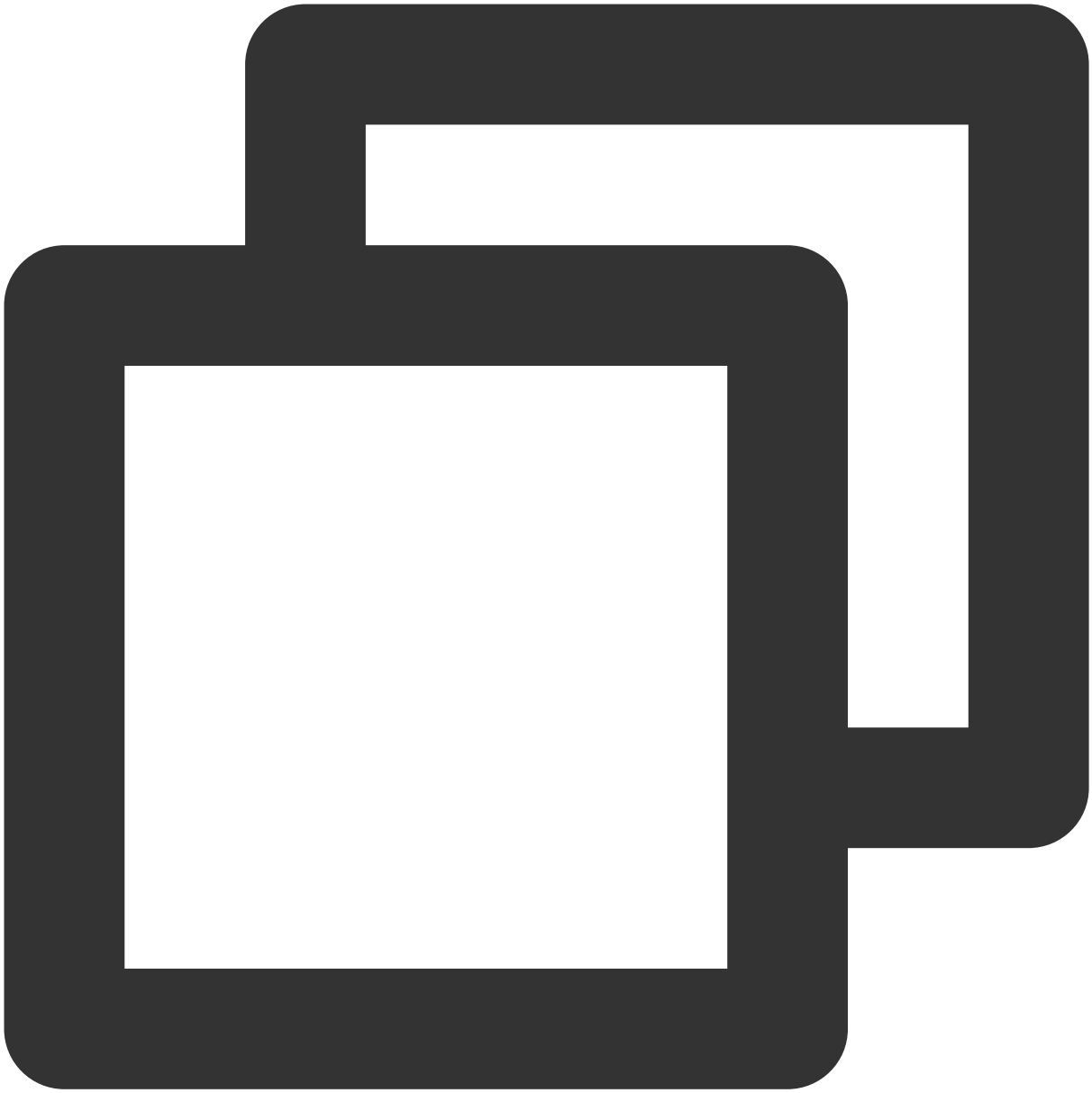
操作场景

该任务指导您按照标签授权，实现子用户 cvmtest01 只能管理 ins-duglsqg0 的资源级接口权限。

查看详细操作场景 >>

策略内容

按照标签授权，最终实现上述预期结果时，对应的策略内容如下：



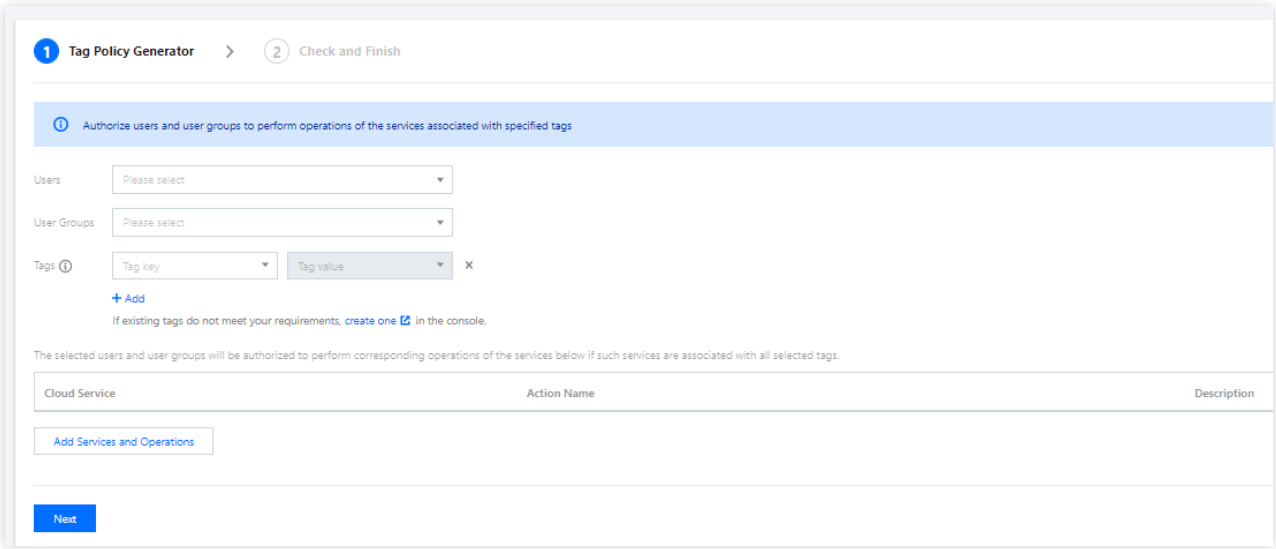
```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "cvm:*",
                "vpc:DescribeVpcEx",
                "vpc:DescribeNetworkInterfaces"
            ],
            "resource": "*",
```

```
            "condition": {
                "for_any_value:string_equal": {
                    "qcs:resource_tag": [
                        "game&webpage"
                    ]
                }
            }
        }
    ]
}
```

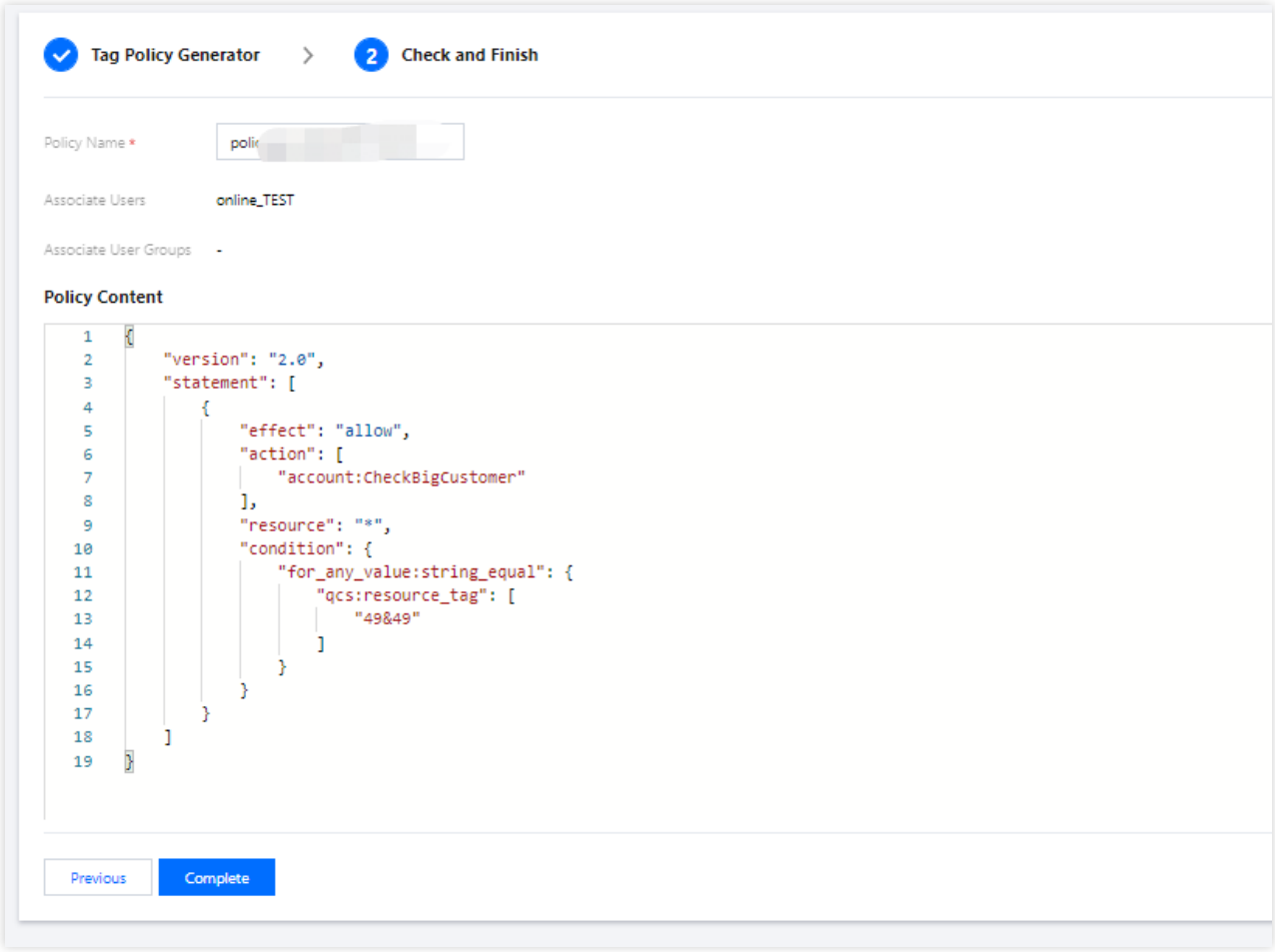
操作步骤

步骤1：创建策略并授权

1. 使用管理员账号登录访问管理控制台，在 策略 页面，按照标签创建自定义策略（参考 创建自定义策略 - 按标签授权）。



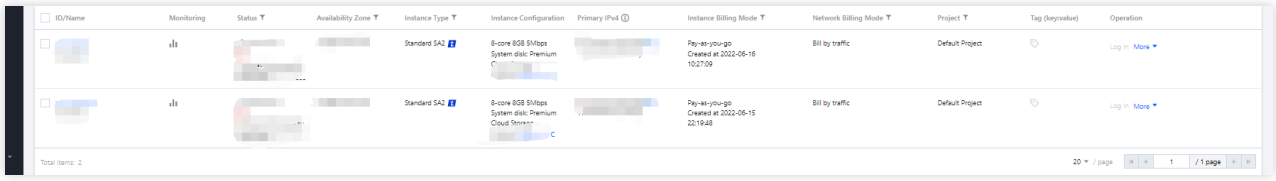
授予用户：cvmtest01
绑定标签：game：webpage
操作权限：云服务器的全部操作权限和 VPC 的 DescribeVpcEx 和 DescribeNetworkInterfaces（说明：无法确定涉及的其他接口时，可以参考 按照资源 ID 授权-步骤3进行验证添加）
2. 单击**下一步**，填写策略名称。
3. 单击**保存**，完成授权。



步骤2：验证结果

使用子用户 cvmtest01 登录 云服务器控制台，访问实例列表页面，达到预期效果。

至此，子用户 cvmtest01 可以对实例进行开关机、重启、更名、重置密码等操作。



企业多账号权限管理

概述

最近更新时间：2024-01-23 17:59:15

很多企业在腾讯云上会有多个主账号，账号越多，账号和权限的管理就会越复杂。这时企业管理者希望能够跨账号管理资源权限，减少管理的复杂度。员工如果需要访问多个主账号，希望能够减少 CAM 子账号的数量和登录次数。针对上述场景，腾讯云提供集团账号、角色和协作者三种方式进行跨账号的访问和管理。三种方式的对比如下，您可以根据实际场景选择适合自己企业的方式：

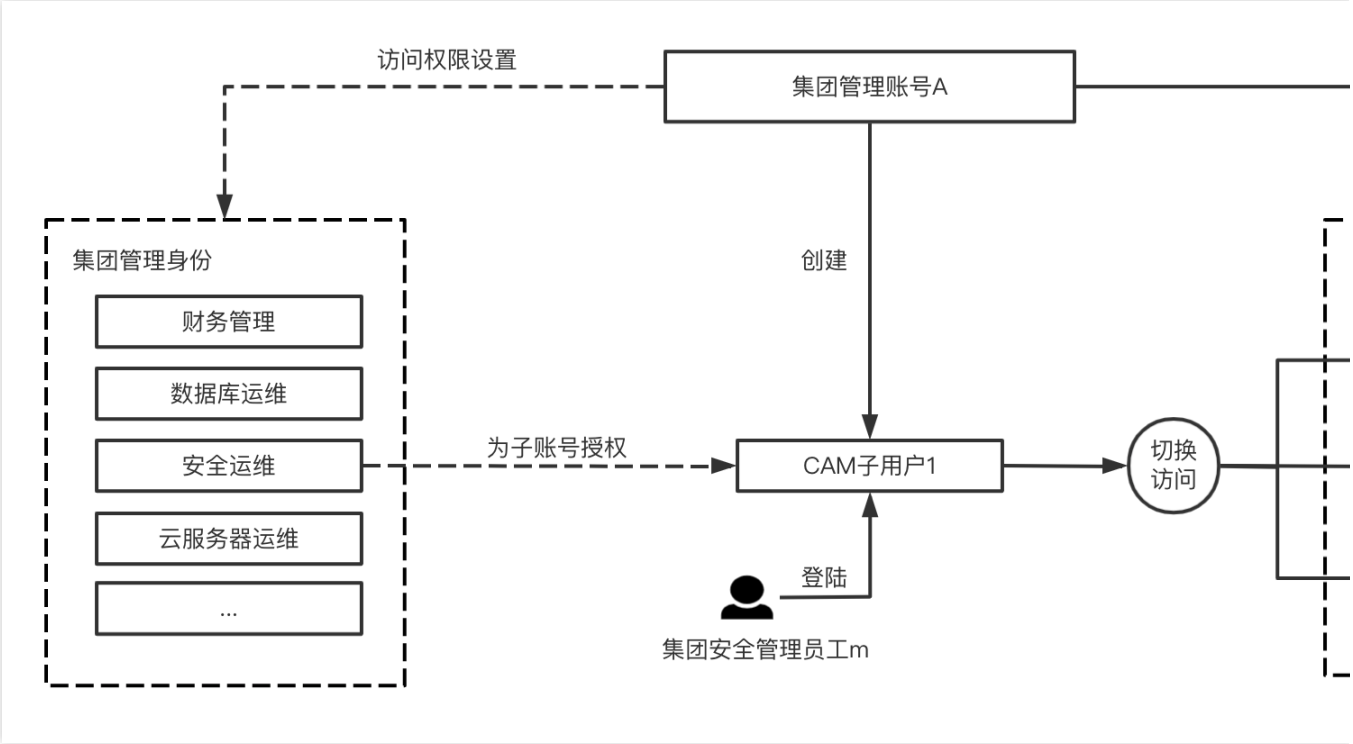
管理方式	特性说明
集团账号	图形化界面操作简易，只支持同一个集团内的企业实名账号使用
角色	需要在每个被管理主账号下创建角色，操作流程相对较长
协作者	只支持主账号作为协作对象

集团账号

最近更新时间：2024-01-23 17:59:15

集团账号简介

集团账号管理是腾讯云上面向集团客户的多账号管理产品，支持集团管理员统一管理集团及旗下子公司的腾讯云主账号，提供账号、财务、安全等的管理能力，更多说明请参见 集团账号管理文档。
在集团账号管理中，管理账号可以为 CAM 子账号同时授予多个创建的成员账号的管理权限，授权后，该 CAM 子账号支持只登录一次，就可以选择成员，访问管理多个成员账号。



操作场景

假设某集团在腾讯云有账号 A 和账号B，选择账号 A 作为管理账号开通按账号管理产品，集团内有子公司1和子公司2，分别有账号 C 和账号 D。集团内有安全管理员工 m，希望能够同时运维管理集团及其子公司的账号。
这时集团管理账号可以为员工 m 创建 CAM 子用户1，并授予账号 B、C、D 的安全运维权限，则员工通过 CAM 子用户1登录腾讯云控制台后，可以选择不同的成员账号进行切换执行安全运维的相关操作，无需在每个账号下分别为员工创建 CAM 子用户。

操作步骤

添加授权

1. 管理员账号登录集团账号控制台，进入 成员登录权限设置 页面。
2. 设置管理所有成员的权限模型，如网络运维、安全运维、云服务器运维、财务管理员等。
详细操作请参见 创建成员登录权限。
3. 在 成员账号管理 中，单击**添加成员**，选择**新建成**员，并选择需要管理的权限。
详细操作请参见 添加组织成员。
4. 成员创建成功后，通过**成员账号管理**列表 > **登录账号**，为子用户授予登录成员的权限。
详细操作请参见 授权登录成员账号。

使用子用户登录

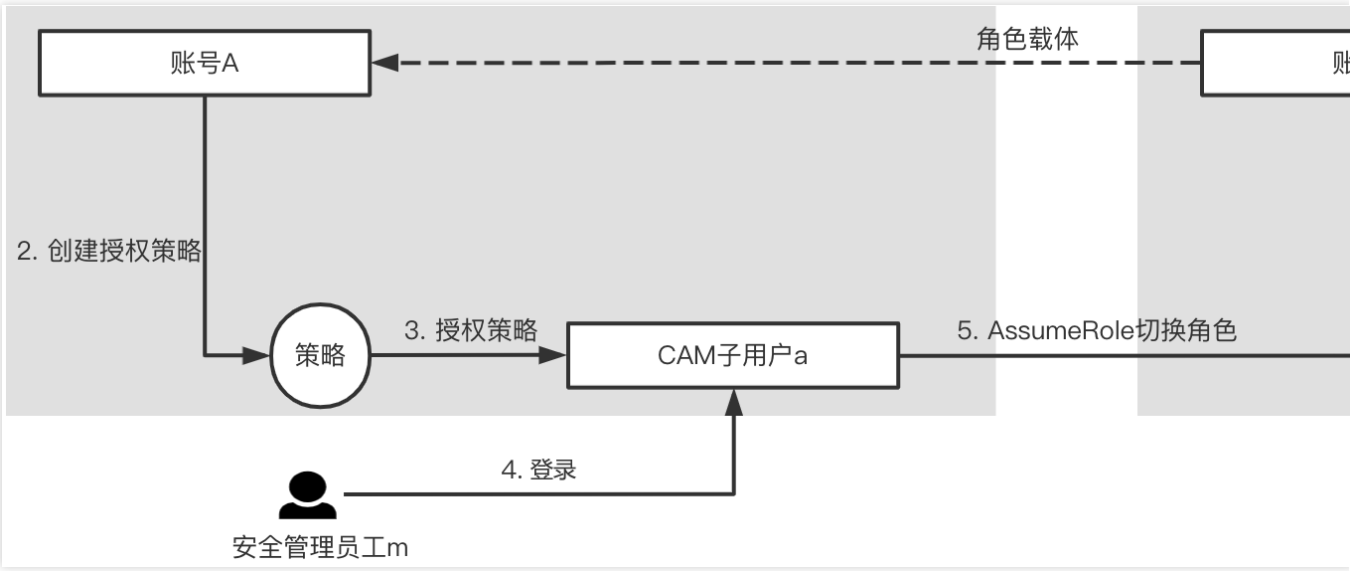
使用 CAM 子用户登录**集团账号管理控制台** > 成员账号管理，选择需要管理的成员和访问权限，单击操作列的**登录账号**，即可使用子用户登录成员控制台并进行管理操作。

角色

最近更新时间：2024-01-23 17:59:15

角色简介

角色是 CAM 的一种虚拟用户，可以被授予权限策略，拥有所属主账号的相应权限，详细说明请参见 角色概述。
在创建角色时，可以选择以腾讯云主账号作为角色载体、创建角色，并为角色绑定授权策略。 作为载体的主账号可以通过创建权限策略，将扮演角色的权限授予其 CAM 子账号，之后 CAM 子账号可以在腾讯云控制台通过切换角色登录到对应的主账号控制台执行授权范围内的操作，也可以通过云 API 发起跨账号请求。



操作场景

假设企业内有账号 A 和账号 B 两个主账号，企业安全管理员工 m 在账号 A 下有 CAM 子用户 a，员工 m 希望使用该子账号能够同时运维管理账号 B 下的安全信息。这时我们可以按照以下步骤执行操作：

操作步骤

1. 在账号 B 下创建安全运维角色 role，并将角色载体指定为主账号 A。
详细操作请参见 创建角色。

2. 在账号 A 下创建权限策略，策略支持通过 AssumeRole 扮演安全运维角色 role。
3. 将策略授权给 CAM 子用户 a。

详细操作请参见 为子账号赋予扮演角色策略。

4. 员工 m 登录 CAM 子用户 a。
5. 员工 m 在腾讯云控制台选择切换角色，使用安全角色 role 登录腾讯云控制台。

详细操作请参见 使用角色登录腾讯云控制台。

6. 执行安全运维相关操作。
7. 如果员工 m 需要同时对多个主账号执行安全运维的相关操作，则可以参照上述步骤为员工 m 授予对应主账号的安全运维权限。

协作者

最近更新时间：2024-01-23 17:59:15

协作者简介

本身拥有主账号身份，被添加作为当前主账号的协作者，则为当前主账号的子账号之一，可以协助管理主账号下的云资源。

操作场景

假设企业在云上有多个账号，如账号 A、账号 B、账号 C 等，希望账号 B 和账号 C 能够具有账号 A 下的资源访问权限。

操作步骤

1. 账号 A 登录 CAM 控制台，将账号 B、账号 C 添加为协作者，并授予权限。
详细操作请参见 新建协作者、协作者权限设置。
2. 账号 B 或者账号 C 以协作者身份登录腾讯云控制台。
详细操作请参见 子账号登录控制台 - 协作者登录。
3. 如果您想切换访问其他账号，则需要退出重新登录。
详细操作请参见 协作者身份切换。

查看员工腾讯云操作记录

最近更新时间：2024-01-23 17:59:15

操作场景

当您为员工创建 CAM 子用户并授权后，员工可以使用 CAM 子用户登录腾讯云控制台，或者使用 CAM 子用户密钥通过云 API 来访问和操作您账号下的资源。当有较多员工需要同时登录腾讯云并访问资源时，您可能需要了解以下信息：

员工访问了哪些资源

员工操作是否遇到问题

某个资源是哪个员工购买的

如何查看资源配置的修改记录

如何跟踪敏感操作

员工是否在您限定的环境内访问腾讯云

这时您可以通过云审计查看和跟踪员工操作记录，云审计支持在线查看90天以内的腾讯云控制台和云 API 操作记录。

前提条件

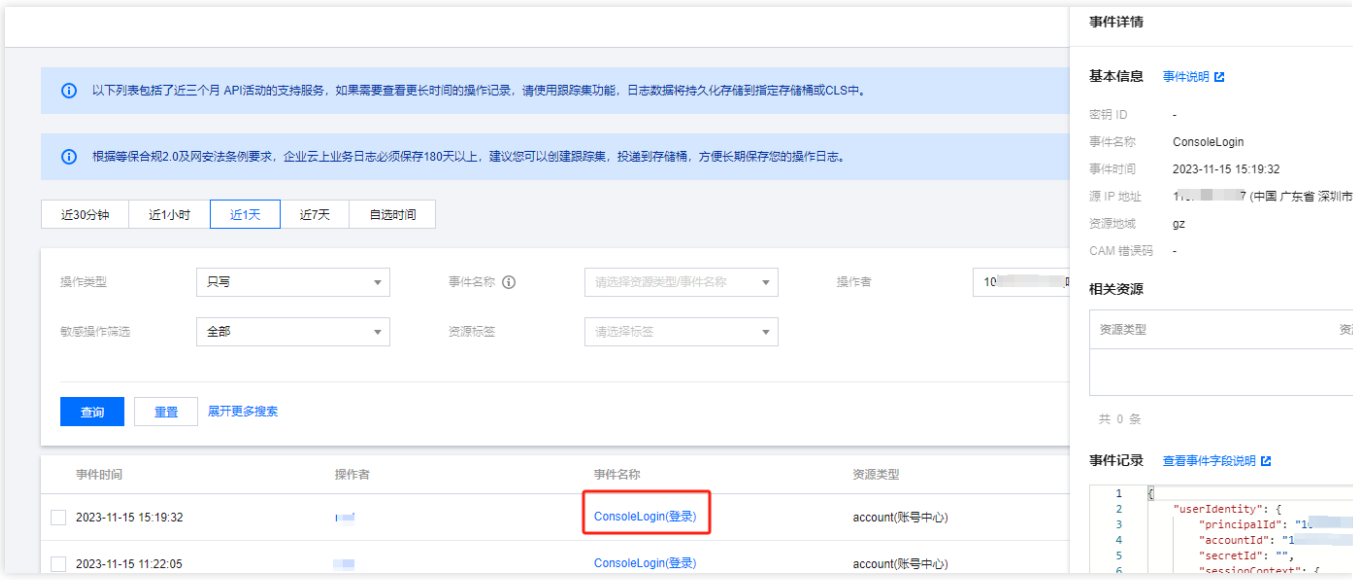
1. 已 新建子用户。
2. 已登录 云审计控制台，进入操作记录页面。

操作步骤

查看操作记录事件详情

您可以通过筛选条件“操作者”按照 CAM 子用户/角色搜索，查看指定员工的操作记录。

您可以通过单击**事件名称**在右侧查看事件详情，在具体的日志摘要中，通过操作者字段来识别实际操作的账号 ID 和名称，通过源 IP 地址查看操作来源。



在具体的日志详情中，您可以通过 principalId 来识别实际操作的账号 ID。

详细操作请参见：查看操作记录事件详情。

使用跟踪集投递日志

如果您需要查看更长时间的员工操作记录，您可以使用云审计的跟踪集功能，将日志投递到 COS 存储桶或者 CLS。在投递到 CLS 时，您可以选择指定产品的具体操作（如敏感操作），并在 CLS 中配置告警策略。
详细操作请参见：使用跟踪集投递日志。

使用 ABAC 管理员工资源访问权限
应用场景

最近更新时间：2024-01-23 17:59:15

操作场景

在腾讯云的实际使用中，通过 ABAC 的授权策略，我们可以使用标签来定义权限。将标签绑定到 CAM 子用户、角色以及具体的云资源，之后可以定义权限策略，这些策略使用标签条件键来根据请求身份的标签向其授予权限。当您使用标签控制对腾讯云资源的访问时，可通过对授权策略进行较少更改来实现团队和资源的变更，操作更加灵活。本章节将详细说明如何为员工在 CAM 中创建一个带有标签的 CAM 角色，以及支持通过带入角色的属性拥有访问与其标签匹配的资源的权限策略。当员工通过该角色向腾讯云发出请求时，将根据带入的角色标签和资源标签是否匹配来授予权限，实现仅允许员工查看或操作其工作需要的资源。

使用示例

假设在游戏公司 A 中，有两个项目 webpage 和 app，其中员工 m 为 webpage 的开发员工，员工 n 为 app 的开发员工，在创建授权策略时，需要保证不同团队内的员工能够访问其工作所需的资源，同时随着公司发展要考虑后续的扩展性。

可以通过使用资源标签和 CAM 角色标签来为支持 ABAC 策略的产品创建授权策略。当您的员工希望通过联合身份访问到腾讯云中时，其属性将应用到腾讯云中的角色标签中。然后，您可以使用 ABAC 来允许或拒绝基于这些属性的访问。

说明

通过 支持标签的产品，了解哪些产品支持基于标签的授权。
通过 生效条件概述，了解授权策略中支持哪些标记条件键。
我们根据上述项目和团队，做以下标签定义：
game-project = web（对应 web 项目）
game-project = app（对应 app 项目）
web = dev（对应 web 项目开发人员）
app = dev（对应 app 的开发人员）
game=dev（对应 web/app 项目开发人员）

实现原理

1. 员工使用 CAM 用户凭证进行登录，然后扮演其团队和项目的 CAM 角色。
2. 将向相同岗位的角色附加同一策略，根据标签来实现允许或拒绝操作。

验证场景

假设有两台云服务器 ins-78qewdr8（标签 game-project:app）和 ins-7txjj4a6（标签 game-project:web），分别属于 app 和 webpage 项目。
验证点1：不同项目的员工使用不同的 CAM 子用户登录后，如何实现不同员工只能访问到其所属项目下的云服务器。
验证点2：假设员工岗位变更，员工 n 也需要项目 webpage 的权限，如何快速调整权限。
验证点3：假设公司新增加一个 H5 类的项目，如何快速为员工授予新项目的权限。

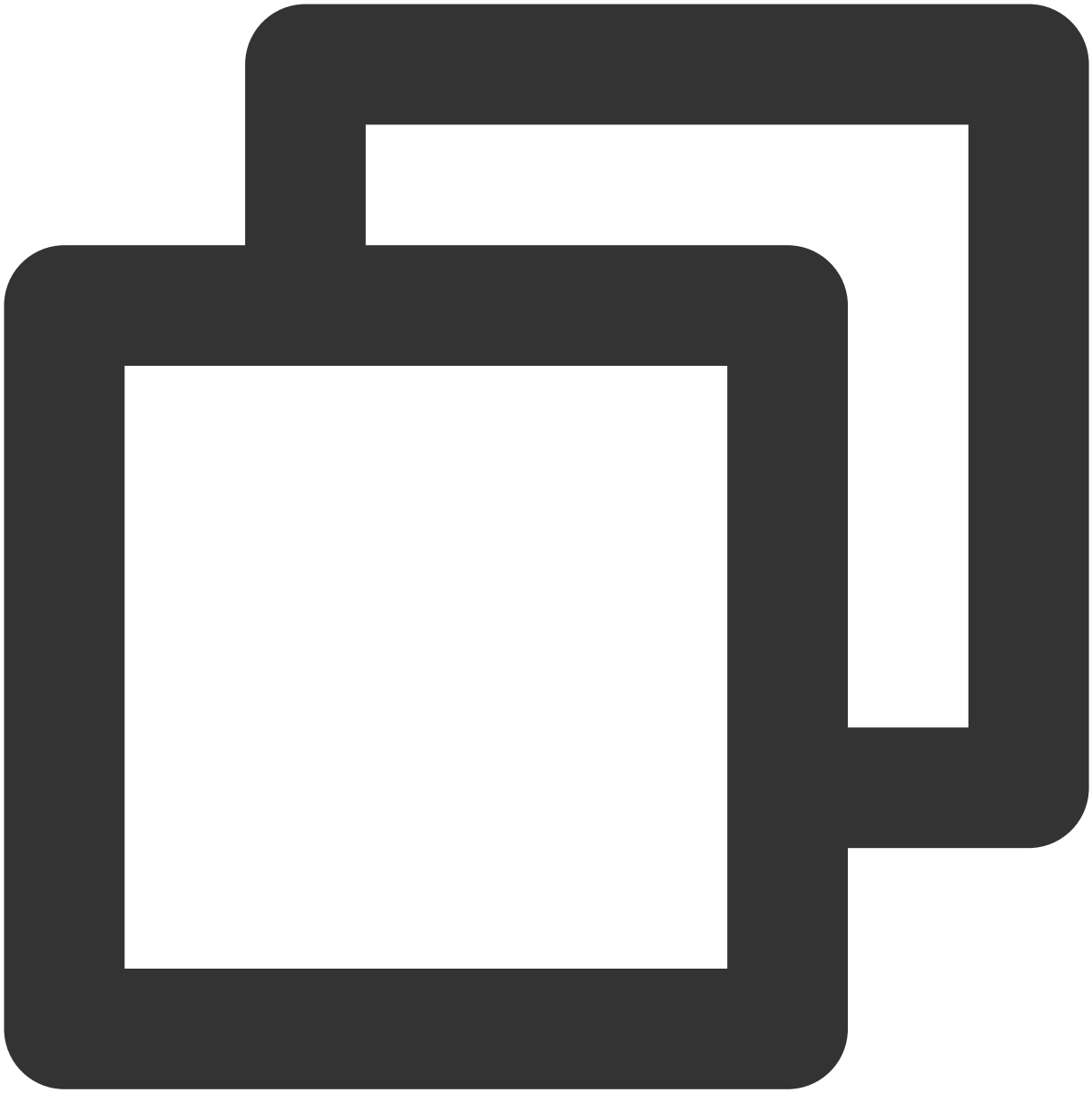
操作步骤

步骤1：创建测试 CAM 子用户

1. 创建名为 access-assume-role 的自定义策略，策略内容为“当带入身份的标签与角色标签匹配时，允许带入 ABAC 角色”。

说明

创建 CAM 策略的详细操作，请参见 创建角色。



```
{
 "version": "2.0",
 "statement": [
     {
         "effect": "allow",
         "action": [
             "sts:AssumeRole"
         ],
         "resource": "*",
         "condition": {
             "for_any_value:string_equal": {
```

```
                "qcs:resource_tag": [
                    "game&${qcs:principal_tag_value}"
                ]
            }
        }
    },
    {
        "effect": "allow",
        "action": [
            "cam:ListUserTags",
            "cam:ListLoginRoles"
        ],
        "resource": [
            "*"
        ]
    }
 ]
}
```

2. 创建 CAM 子用户 m-developer 和 n-developer，并为子用户绑定 access-assume-role 的授权策略，并为子用户绑定下述标签。

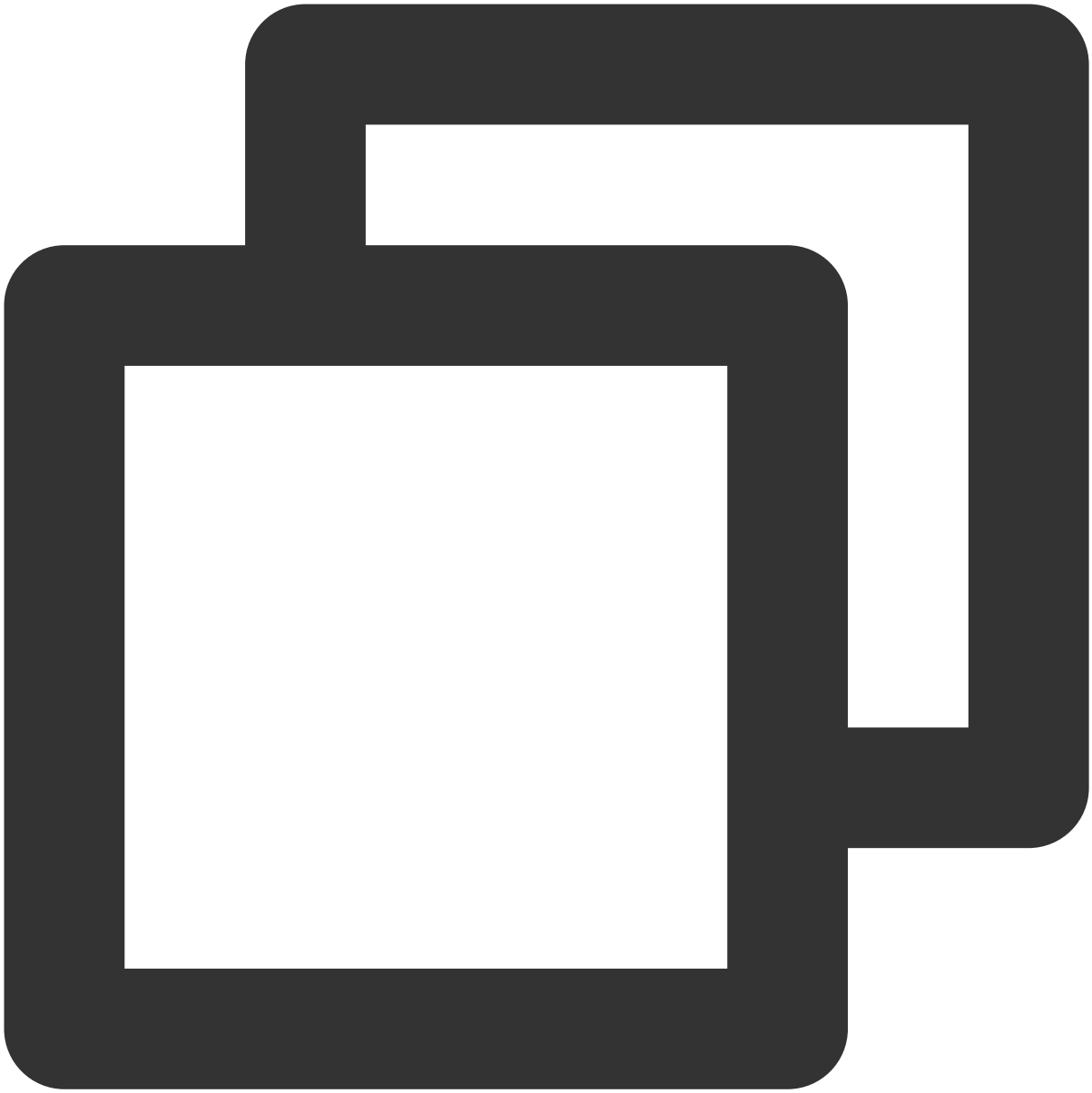
说明

创建 CAM 子用户的详细操作，请参见 新建子用户。

子用户名称	关联标签
m-developer	web=dev
n-developer	app=dev

步骤2：创建 ABAC 策略

1. 创建名为 access-resource-project（以 cvm 产品为例子）的自定义策略，策略内容如下：



```
{
 "version": "2.0",
 "statement": [
     {
         "effect": "allow",
         "action": "cvm:*",
         "resource": "*",
         "condition": {
             "for_any_value:string_equal": {
                 "qcs:request_tag": [
                    "game-project&${qcs:principal_tag_key}"
```

```
                ]
            }
        }
    },
    {
        "effect": "allow",
        "action": "cvm:*",
        "resource": "*",
        "condition": {
            "for_any_value:string_equal": {
                "qcs:resource_tag": [
                    "game-project&${qcs:principal_tag_key}"
                ]
            }
        }
    },
     {
        "effect": "allow",
        "action": [
            "vpc:DescribeVpcEx",
            "vpc:DescribeSubnetEx",
            "vpc:DescribeNetworkInterfaces",
            "cvm:DescribeDiskSecurityConfigurations",
            "cvm:DescribeCbsStorages",
            "tag:DescribeTagKeys",
            "tag:DescribeTagValues"
        ],
        "resource": [
            "*"
        ]
    }

 ]
}
```

game-project 与 ${qcs:principal_tag_key} 标签绑定的 key 和 value 值关联并确定项目与特定标签键相关联的数值。

2. 创建角色 access-developer-role，关联上述策略，并绑定如下标签。

说明

创建 CAM 策略的详细操作，请参见 创建角色。

CAM 角色名称	关联标签
access-developer-role	game=dev

步骤3：场景验证

验证点1：使用不同的子用户登录后，只能访问到对应项目下的云服务器

1. 使用子用户 m-developer 登录 腾讯云控制台，在控制台右上角，单击账号下的**切换角色**。

2. 在切换角色页面，应用选择 web（子用户 m-developer 的标签 value），角色选择 access-developer-role，单击**切换角色**。

3. 以角色身份登录腾讯云控制台，进入 CVM 实例 页面。

在 CVM 产品控制台，若仅可以查看到 ins-7txjj4a6（标签 game-project:web），则符合预期。

4. 切换身份，使用子用户 n-developer 登录 腾讯云控制台，登录后切换角色，应用选择 app，角色选择 access-developer-role，显示名称为 n-developer-app，单击**切换角色**。

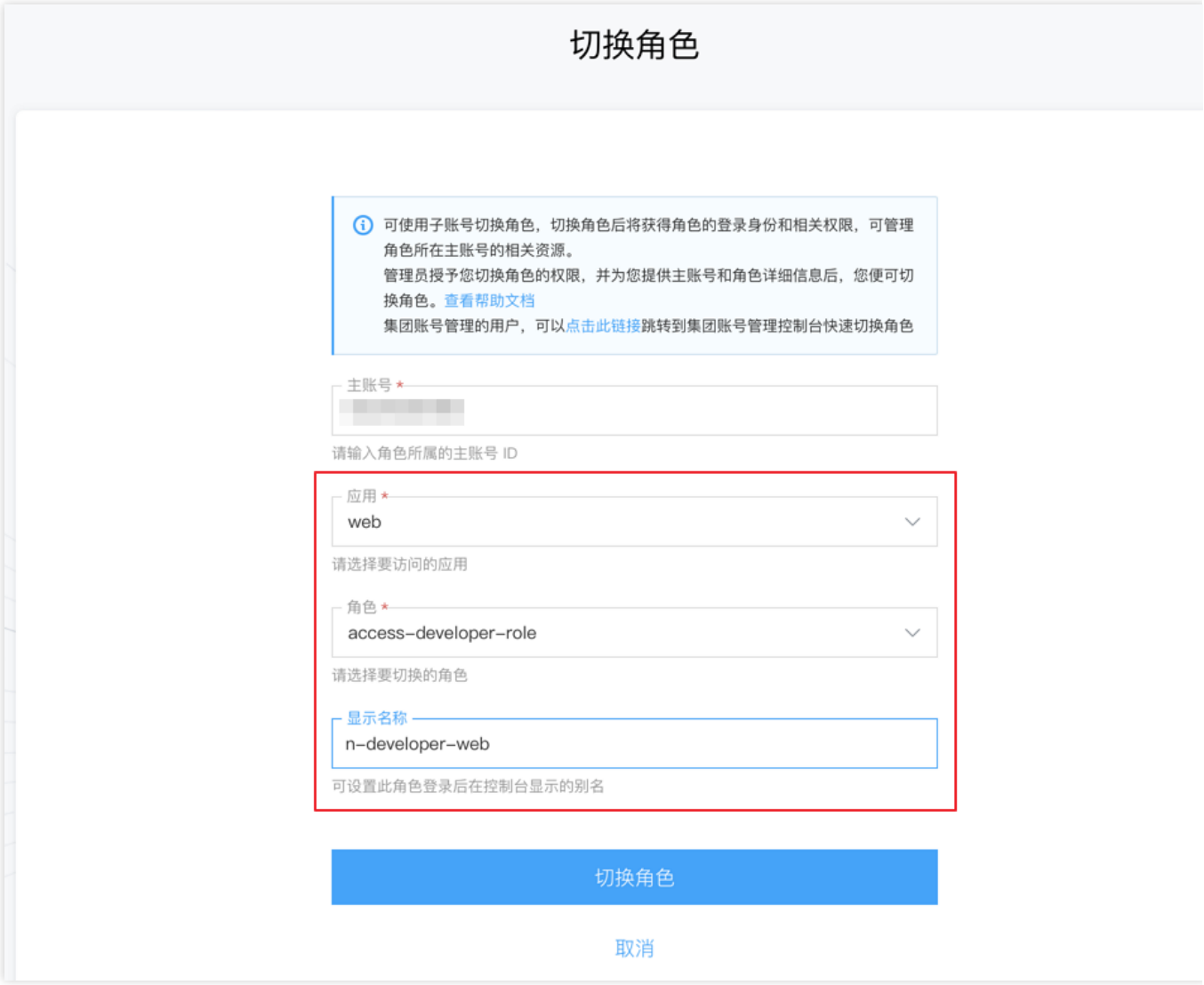
5. 以角色身份进入腾讯云控制台，进入 CVM 实例 页面。

在 CVM 产品控制台，若仅能查看云服务器 ins-78qewdr8（标签 game-project:app），则符合预期。

验证点2：假设岗位变更，员工 n 也需要项目 webpage 的权限，该如何设置

当前场景下，我们仅需要在 访问管理控制台 的用户详情中，为员工 n 对应的 CAM 子用户 n-developer 增加标签 app:web 即可。

1. 使用子用户 n-developer 登录 腾讯云控制台，在控制台右上角，单击账号下的**切换角色**。
2. 在切换角色页面，应用选择 web，角色选择access-developer-role，别名为 n-developer-web，单击**切换角色**。



3. 以角色身份登录腾讯云控制台，进入 CVM 实例 页面。

在 CVM 产品控制台，若仅能查看云服务器 ins-7txjj4a6（标签 game-project:web），则符合预期。

验证点3：假设公司新增加一个 H5 类的项目，该如何调整权限策略适配

公司新增 H5 项目后，如果我们需要增加 H5 项目的开发权限，则无需对策略本身进行变更，仅需要：

1. 为 H5 项目的开发同事创建新的子用户。
2. 为子用户绑定 H5 项目对应的标签，关联 access-assume-role 策略即可。

按标签鉴权时支持仅匹配标签键

最近更新时间：2024-01-23 17:59:15

本文档介绍如何为您的子账号授予某个标签下所有资源的权限以及如何授予子账号只能绑定某个标签键的权限。

说明：

resource_tag 授予某个标签下所有资源的权限，request_tag 授予子账号只能绑定某个标签键的权限，对于控制台列表及相关 API 不生效。

授予关联某个标签键下所有资源的权限（resource_tag）

操作场景

若您的公司购买了多种腾讯云资源，资源均通过标签分组管理，希望能够授予关联某个标签键下所有资源的权限（resource_tag）。

假设存在以下条件：

企业账号 CompanyExample 下有个子账号 Operator。

企业账号 CompanyExample 下有个为**运营**的标签键。

企业账号 CompanyExample 希望给子账号 Operator 授予标签键**运营**下的所有资源。

操作步骤

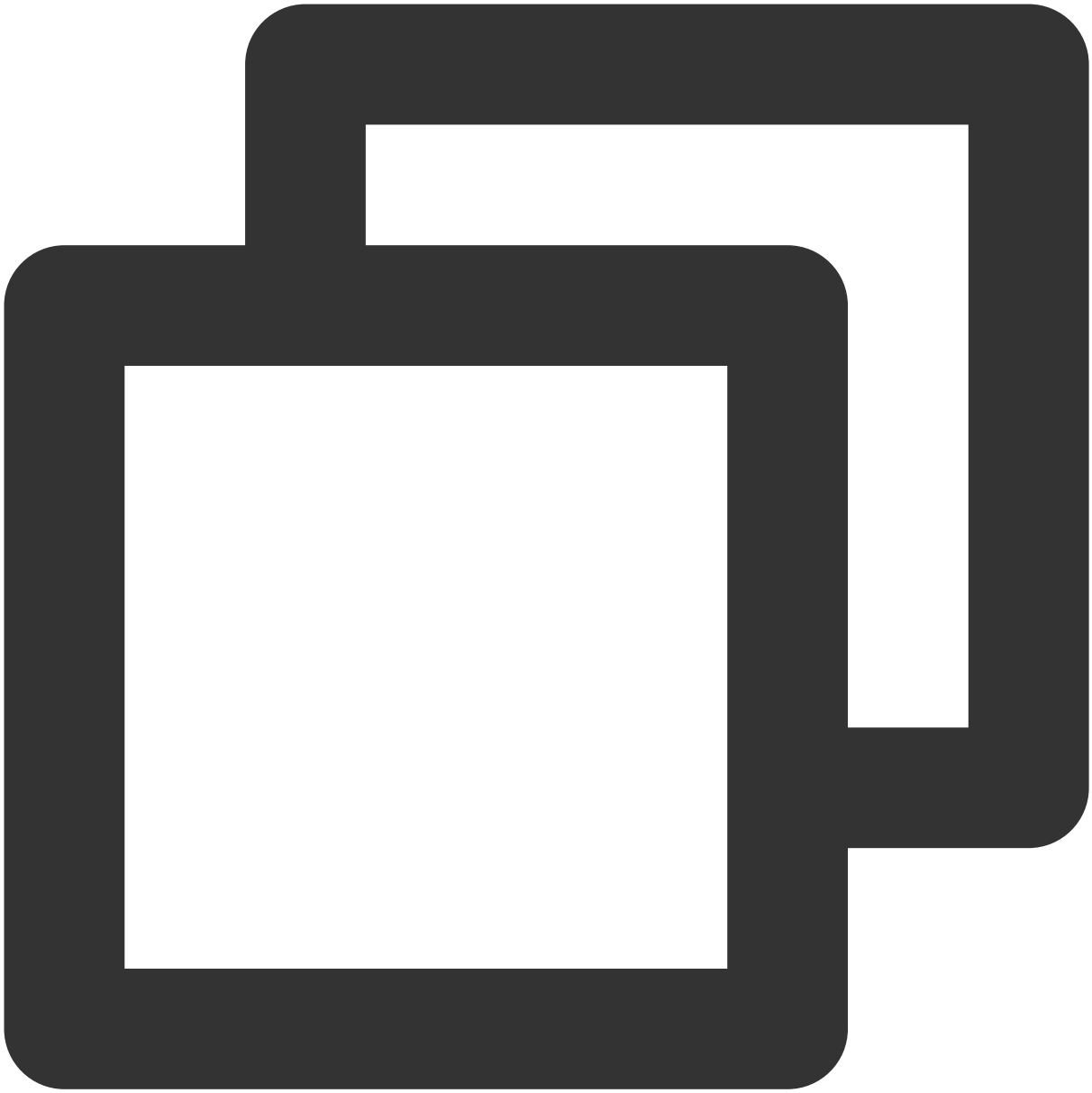
1. 使用企业账号 CompanyExample 登录 访问管理控制台。
2. 在**策略**页面，单击**新建自定义策略** > 按策略语法创建。
3. 在选择模板类型下选择空白模板，单击**下一步**，进入编辑策略页面。

4. 进入编辑策略页面，填写如下表单：

策略名称：默认为 `policygen-当前日期` ，推荐您自行定义一个不重复且有意义的策略名称，例如 Operator-resource_tag 。

描述：可选，自行编写。

策略内容：复制以下内容并填写。其中，运营 为标签键名称，可为中文和英文， `false` 为固定的标签值。



```
{
"version": "2.0",
 "statement": [
   {
        "effect": "allow",
        "action": "*",
        "resource": "*",
        "condition": {
            "null_equal": {
                "qcs:resource_tag/运营": "false"
            }
```

```
            }
        }
    ]
}
```

5. 单击**完成**，完成策略的创建。新建的策略将显示在策略列表页。
6. 在 策略列表 中搜索找到刚才已创建的策略，单击右侧操作列下的**关联用户/组/角色**。

7. 在弹出的**关联用户/用户组/角色**窗口中，搜索勾选子账号 Operator，单击**确定**完成授权操作。

子账号 Operator 将拥有标签**运营**下所有资源的权限。

授予子账号只能绑定某个标签键的权限（request_tag）

操作场景

若您的公司购买了多种腾讯云资源，资源均通过标签分组管理，希望能够授予子账号只能绑定某个标签键的权限（request_tag）。

假设存在以下条件：

企业账号 CompanyExample 下有个子账号 Developer。

企业账号 CompanyExample 下有个为**开发**的标签键。

企业账号 CompanyExample 希望给子账号 Developer 授予只能绑定**开发**标签键的权限（request_tag）。

操作步骤

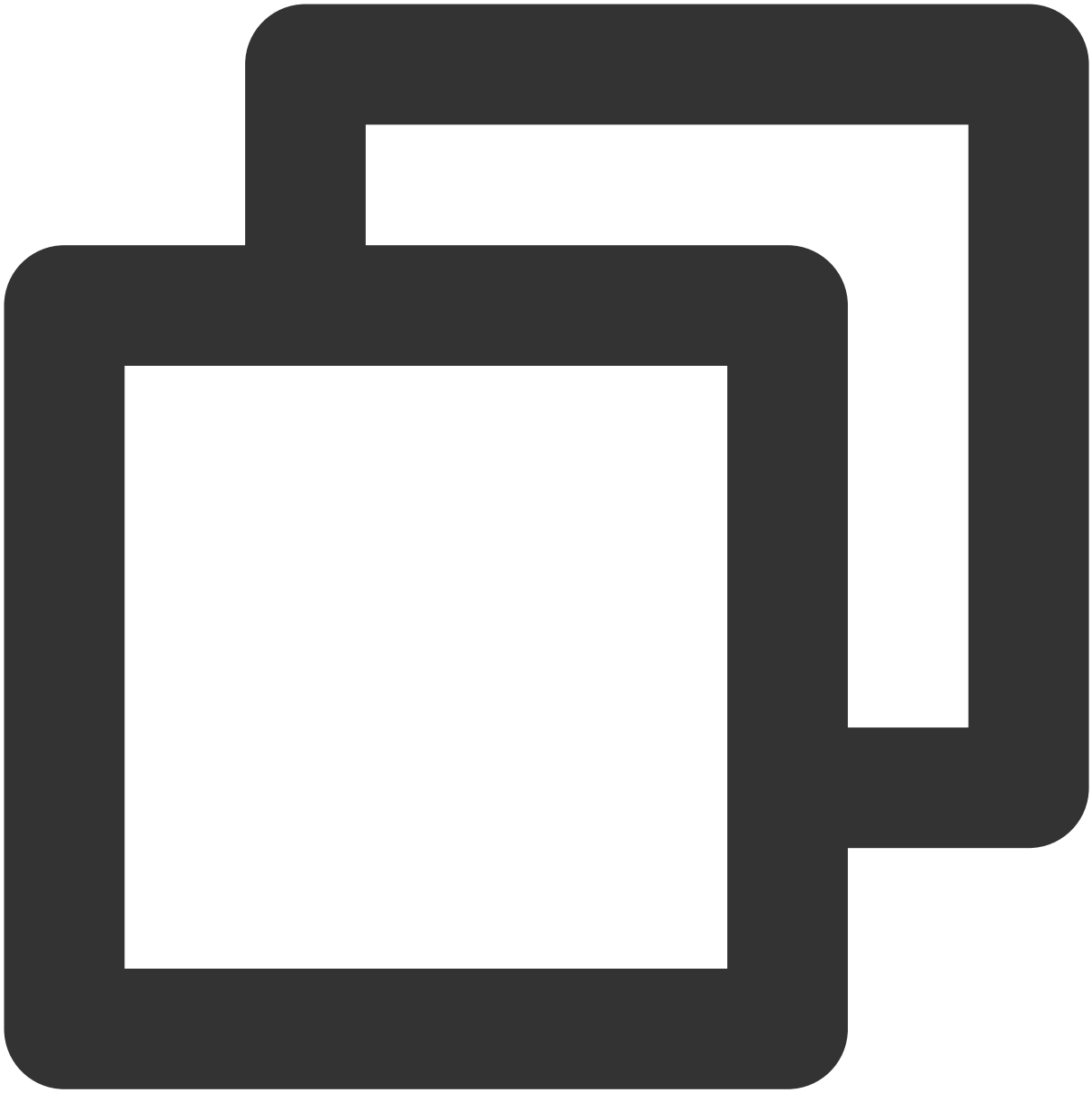
1. 使用企业账号 CompanyExample 登录 访问管理控制台。
2. 在**策略**页面，单击**新建自定义策略** > 按策略语法创建。
3. 在选择模板类型下选择空白模板，单击**下一步**，进入编辑策略页面。

4. 进入编辑策略页面，填写如下表单：

策略名称：默认为 `policygen-当前日期` ，推荐您自行定义一个不重复且有意义的策略名称，例如 Developer-request_tag。

描述：可选，自行编写。

策略内容：复制以下内容并填写。其中，开发 为标签键名称，可为中文和英文， `false` 为固定的标签值。



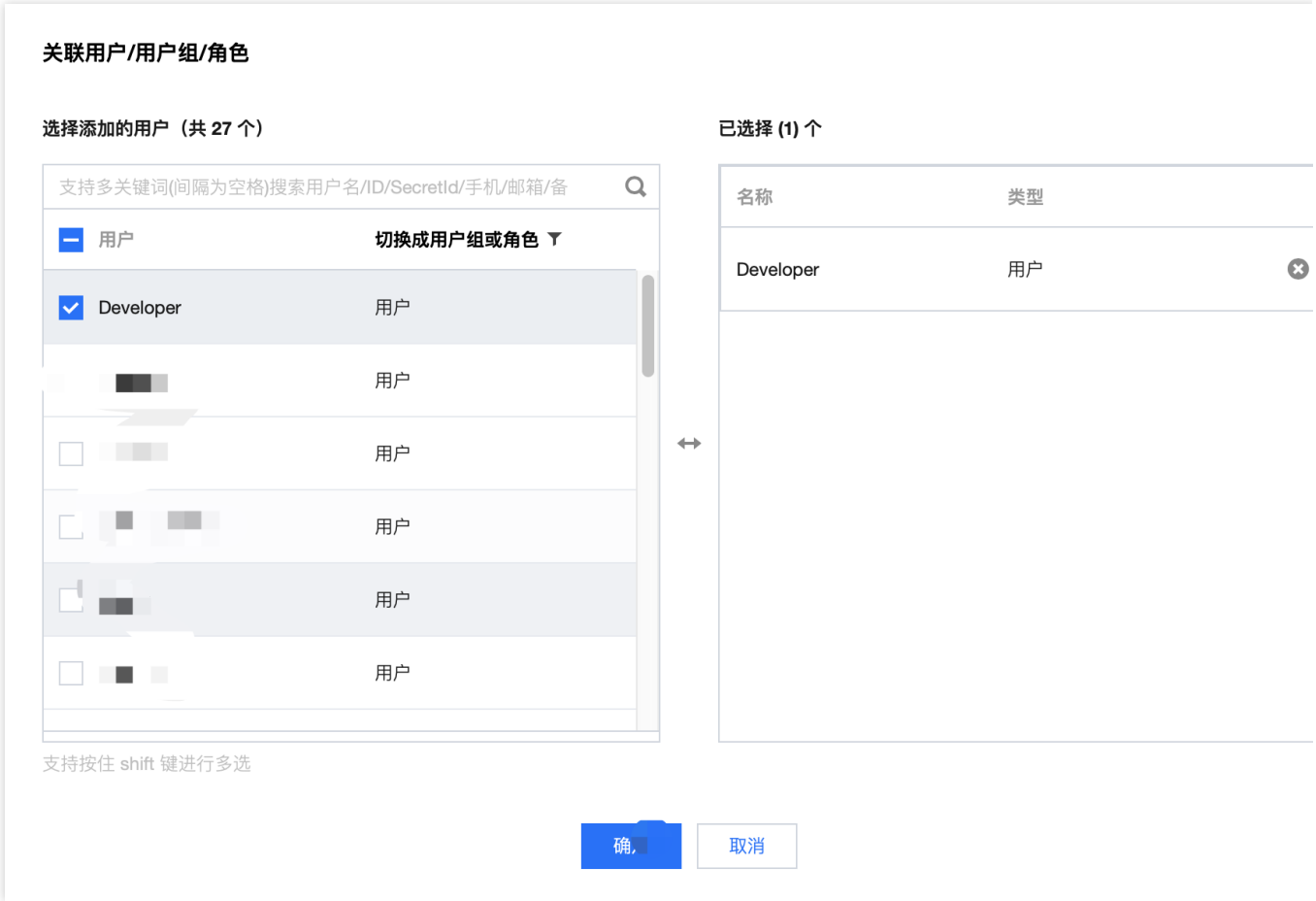
```
{
"version": "2.0",
 "statement": [
   {
        "effect": "allow",
        "action": "*",
        "resource": "*",
        "condition": {
            "null_equal": {
                "qcs:request_tag/开发": "false"
            }
```

```
            }
        }
    ]
}
```

5. 单击**完成**，完成策略的创建。新建的策略将显示在策略列表页。
6. 在 策略列表 中搜索找到刚才已创建的策略，单击右侧操作列下的**关联用户/组/角色**。

7. 在弹出的**关联用户/用户组/角色**窗口中，搜索勾选子账号 Developer，单击**确定**完成授权操作。

子账号 Developer 将拥有只能绑定**开发**标签键的权限。



关联文档

如果您想了解如何将资源和标签建立关联关系，请参见 管理标签。