容器服务

权限管理

产品文档

腾讯云

文档目录

权限管理

概述

最近更新时间：2022-06-10 16:48:46

如果您在腾讯云中使用到了容器服务（Tencent Kubernetes Engine，TKE），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，您可以通过使用子帐号来实现不同的人管理不同的业务。默认情况下，子帐号没有使用 TKE 的权限，我们需要创建策略来允许子帐号拥用他们所需要的权限。

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 的时候，可以将策略与一个用户或者一组用户关联起来，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，请参照 策略语法。有关 CAM 策略的更多相关使用信息，请参照策略。
如果您不需要对子账户进行 CAM 相关资源的访问管理，您可以跳过此章节。跳过这些部分并不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 TKE 操作或者必须拒绝使用一个或多个 TKE 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的条件。

TKE 部分 API 操作不支持资源级权限，意味着对于该类 API 操作，您不能在使用该类操作的时候指定某个具体的资源来使用，而必须要指定全部资源来使用。

服务授权相关角色权限说明

最近更新时间：2022-05-09 11:40:29

在使用腾讯云容器服务（Tencnet Kubernetes Engines，TKE）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 `TKE_QCSRole` 和 `IPAMDofTKE_QCSRole` 两个角色。本文档接下来将分角色展示各个授权策略的详情、授权场景及授权步骤。

> 说明：
> 本文档示例角色均不包含容器镜像仓库相关授权策略，容器镜像服务权限详情请参见 TKE 镜像仓库资源级权限设置。

TKE_QCSRole 角色

开通容器服务后，腾讯云会授予您的账户 `TKE_QCSRole` 角色的权限。该容器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。 `TKE_QCSRole` 角色关联的预设策略包含如下：

默认关联预设策略

- `QcloudAccessForTKERole` ：容器服务对云资源的访问权限。
- `QcloudAccessForTKERoleInOpsManagement` ：日志服务等运维管理。

其他关联预设策略

- `QcloudAccessForTKERoleInCreatingCFSStorageclass` ：容器服务操作文件存储（CFS）权限，包含增删查文件存储文件系统、查询文件系统挂载点等。
- `QcloudCVMFinanceAccess` ：云服务器财务权限。

预设策略 QcloudAccessForTKERole

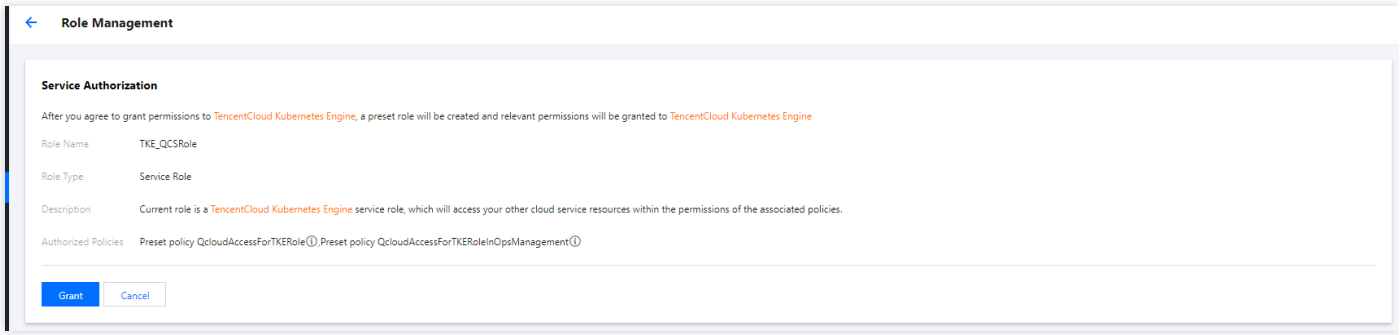
授权场景

当您已注册并登录腾讯云账号后，首次登录 容器服务控制台 时，需前往“访问管理”页面对当前账号授予腾讯云容器服务操作云服务器（CVM）、负载均衡（CLB）、云硬盘（CBS）等云资源的权限。

授权步骤

1. 登录 容器服务控制台，选择左侧导航栏中的**集群**，弹出**服务授权**窗口。
2. 单击**前往访问管理**，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。如下图所示：



权限内容

- 云服务器相关

权限名称	权限说明
`cvm:DescribeInstances`	查询服务器实例列表
`cvm:*Cbs*`	云硬盘相关权限

- 标签相关

权限名称	权限说明
`tag:*`	标签相关所有功能

- 负载均衡相关

权限名称	权限说明
`clb:*`	负载均衡相关所有功能

- 容器服务相关

权限名称	权限说明
`ccs:DescribeCluster`	查询集群列表
`ccs:DescribeClusterInstances`	查询集群节点信息

预设策略 QcloudAccessForTKERoleInOpsManagement

授权场景

该策略默认关联 `TKE_QCSRole` 角色，开通容器服务并完成 `TKE_QCSRole` 角色授权后，即可获得包含日志在内的各种运维相关功能的权限。

授权步骤

该策略与 预设策略 QcloudAccessForTKERole 同时授权，无需额外操作。

权限内容

日志服务相关

权限名称	权限说明
`cls:listTopic`	列出指定日志集下的日志主题列表
`cls:getTopic`	查看日志主题信息
`cls:createTopic`	创建日志主题
`cls:modifyTopic`	修改日志主题
`cls:deleteTopic`	删除日志主题
`cls:listLogset`	列出日志集列表
`cls:getLogset`	查看日志集信息
`cls:createLogset`	创建日志集
`cls:modifyLogset`	修改日志集
`cls:deleteLogset`	删除日志集
`cls:listMachineGroup`	列出机器组列表
`cls:getMachineGroup`	查看机器组信息
`cls:createMachineGroup`	创建机器组
`cls:modifyMachineGroup`	修改机器组
`cls:deleteMachineGroup`	删除机器组
`cls:getMachineStatus`	查看机器组状态
`cls:pushLog`	上传日志
`cls:searchLog`	查询日志

权限名称	权限说明
`cls:downloadLog`	下载日志
`cls:getCursor`	根据时间获取游标
`cls:getIndex`	查看索引
`cls:modifyIndex`	修改索引
`cls:agentHeartBeat`	心跳
`cls:getConfig`	获取推流器配置信息

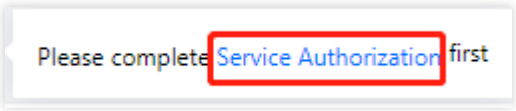
预设策略 QcloudAccessForTKERoleInCreatingCFSStorageclass

授权场景

使用腾讯云文件存储（CFS）扩展组件，能够帮助您在容器集群中使用文件存储。首次使用该插件时，需通过容器服务进行文件存储中文件系统等相关资源的授权操作。

授权步骤

1. 登录 容器服务控制台，单击左侧导航栏中**集群**。
2. 在“集群管理”页面中，选择地域及集群后，进入“集群详情”页。
3. 在“集群详情”页的左侧导航栏中选择**组件管理**，单击**新建**。
4. 在“组件管理”页面中，当扩展组件首次选择为 “CFS 腾讯云文件存储” 时，单击页面下方的**服务授权**。如下图所示：



5. 在弹出的“服务授权”窗口中，单击**访问管理**。
6. 在“角色管理”页面中，单击**同意授权**并完成身份验证即可成功授权。

权限内容

文件存储相关

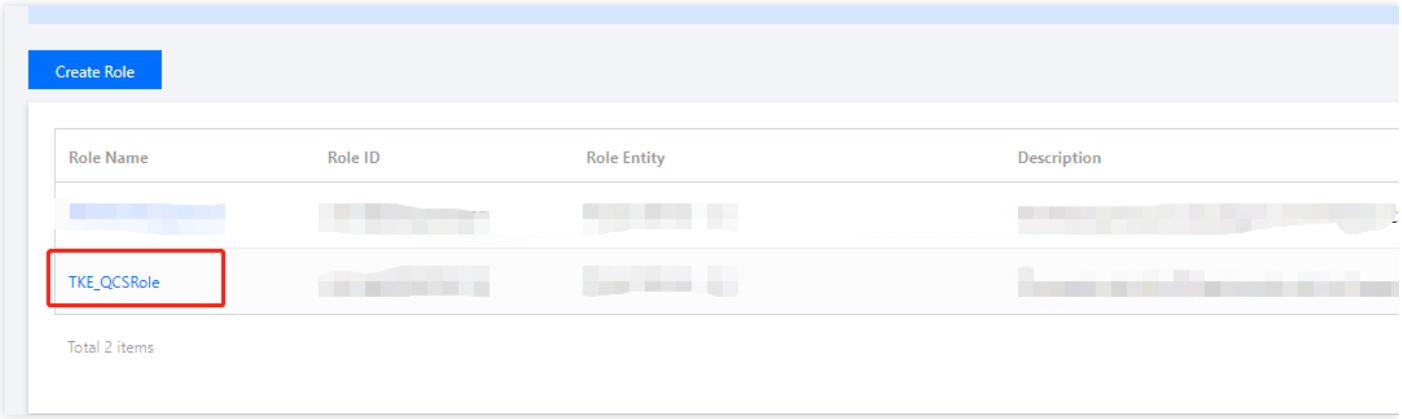
权限名称	权限说明
cfs:CreateCfsFileSystem	创建文件系统
cfs:DescribeCfsFileSystems	查询文件系统

权限名称	权限说明
cfs:DescribeMountTargets	查询文件系统挂载点
cfs:DeleteCfsFileSystem	删除文件系统

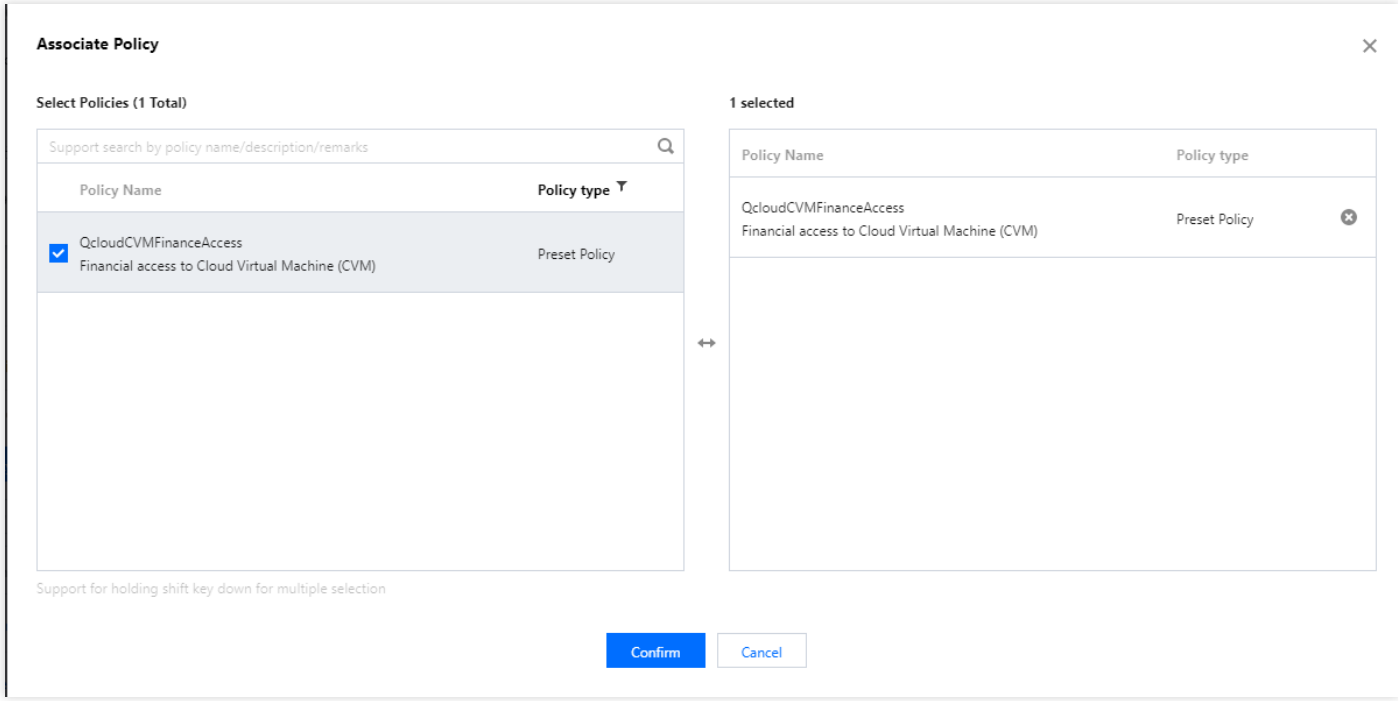
预设策略 QcloudCVMFinanceAccess

授权步骤

1. 登录访问管理控制台，选择左侧导航栏的 **角色**。
2. 在“角色”列表页面中，单击 TKE_QCSRole 进入该角色管理页面。如下图所示：



3. 选择 “TKE_QCSRole” 页面中的**关联策略**，并在弹出的“风险提醒”窗口中进行确认。
4. 在弹出的“关联策略”窗口中，找到 `QcloudCVMFinanceAccess` 策略并勾选。如下图所示：



5. 单击**确定**即可完成授权。

权限内容

权限名称	权限说明
`finance:*`	云服务器财务权限

IPAMDofTKE_QCSRole 角色

`IPAMDofTKE_QCSRole` 角色为容器服务的 IPAMD 支持服务角色。被授予该角色的权限后，在本文描述的授权场景下需进行预设策略关联操作。完成操作后，以下策略会出现在该角色的已授权策略列表中：

`QcloudAccessForIPAMDofTKERole` ：容器服务 IPAMD 支持（TKE IPAMD）对云资源的访问权限。

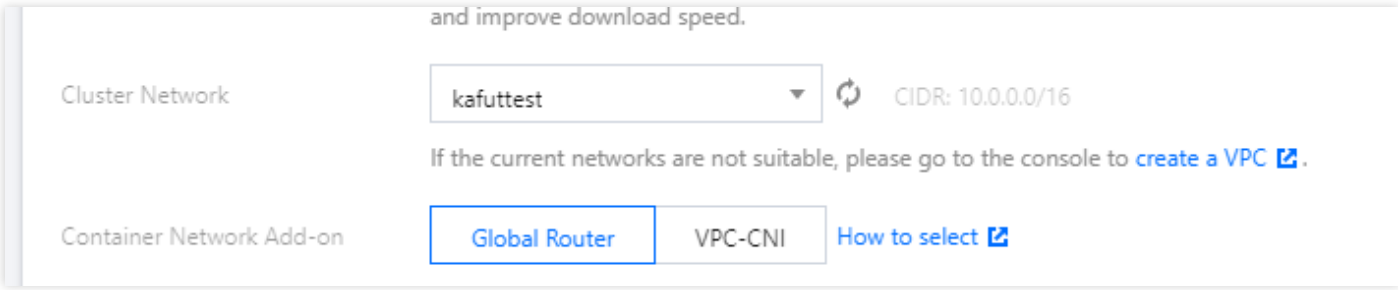
预设策略 QcloudAccessForIPAMDofTKERole

授权场景

在首次使用 VPC-CNI 网络模式创建集群时，需要首先对容器服务 IPAMD 支持（TKE IPAMD）对云资源的访问权限进行授权，以便能够正常使用 VPC-CNI 网络模式。

授权步骤

1. 登录 容器服务控制台，单击左侧导航栏中**集群**。
2. 在“集群管理”页面中，单击集群列表上方的**新建**或**使用模板新建**。
3. 在“创建集群”页面的设置“集群信息”步骤，选择“容器网络插件”中的**VPC-CNI**时，单击**服务授权**。如下图所示：



4. 在弹出的“服务授权”窗口中，单击**前往访问管理**。
5. 在“角色管理”页面中，单击**同意授权**并完成身份验证即可成功授权。

权限内容

- 云服务器相关

权限名称	权限说明

权限名称	权限说明
cvm:DescribeInstances	查看实例列表

- 标签相关

权限名称	权限说明
tag:GetResourcesByTags	通过标签查询资源列表
tag:ModifyResourceTags	批量修改资源关联的标签
tag:GetResourceTagsByResourceIds	查看资源关联的标签

- 私有网络相关

权限名称	权限说明
vpc:DescribeSubnet	查询子网列表
vpc:CreateNetworkInterface	创建弹性网卡
vpc:DescribeNetworkInterfaces	查询弹性网卡列表
vpc:AttachNetworkInterfac e	弹性网卡绑定云服务器
vpc:DetachNetworkInterface	弹性网卡解绑云服务器
vpc:DeleteNetworkInterface	删除弹性网卡
vpc:AssignPrivateIpAddresses	弹性网卡申请内网 IP
vpc:UnassignPrivateIpAddresses	弹性网卡退还内网 IP
vpc:MigratePrivateIpAddress	弹性网卡内网 IP 迁移
vpc:DescribeSubnetEx	查询子网列表
vpc:DescribeVpcEx	查询对等连接
vpc:DescribeNetworkInterfaceLimit	查询弹性网卡配额
vpc:DescribeVpcPrivateIpAddresses	查询 VPC 内网 IP 信息

TKE 镜像仓库资源级权限设置

最近更新时间：2022-05-09 11:40:29

容器镜像服务权限介绍

腾讯云容器镜像的地址格式是：`ccr.ccs.tencentyun.com/${namespace}/${name}:${tag}`。
镜像仓库的权限围绕以下两个字段进行设置：

- `${namespace}`：镜像仓库所属命名空间。
- `${name}`：镜像仓库名称。

> 注意：
> 命名空间 `${namespace}` 及镜像名字 `${name}` 中不能包含斜杠 “/”。
> `${tag}` 字段目前只实现了删除操作鉴权，请参考 镜像 Tag 权限。

通过 `${namespace}`，`${name}` 两个字段，管理者可以为协作者制定详细的权限方案，实现灵活的权限管理。例如：

- 允许协作者 A 拉取镜像
- 禁止协作者 A 删除镜像
- 禁止协作者 B 拉取命名空间 ns1 中的镜像

如果您不需要详细管理镜像仓库权限，可以使用 预设策略授权。
如果您需要细致地管理协作者权限，请使用 自定义策略授权。
容器镜像服务权限基于腾讯云 CAM 进行管理，您可以详细了解 CAM 的使用方法：

- 用户管理
- 策略管理
- 授权管理

预设策略授权

为了简化容器镜像服务权限管理，容器镜像服务内置了两个预设策略：

- 镜像仓库（CCR）全读写访问权限
  该预设策略配置了容器镜像服务所有权限，如果协作者关联该预设策略后，将与管理者拥有相同的镜像仓库权

限。详情请查看 权限列表。

- 镜像仓库（CCR）只读访问权限
  该预设策略包含了容器镜像服务只读操作的权限，如果协作者在容器镜像服务中**只**关联了该预设策略，则以下操作将被禁止：
- `docker push` 推送镜像
- 新建镜像仓库命名空间
- 删除镜像仓库命名空间
- 创建镜像仓库
- 删除镜像仓库
- 删除镜像 Tag

如果您不了解如何为协作者关联预设策略，请参考 CAM 文档：策略、授权管理。

自定义策略授权

通过自定义策略，管理者可以为不同的协作者关联不同的权限。
当您分配权限时，请考虑这些要素：

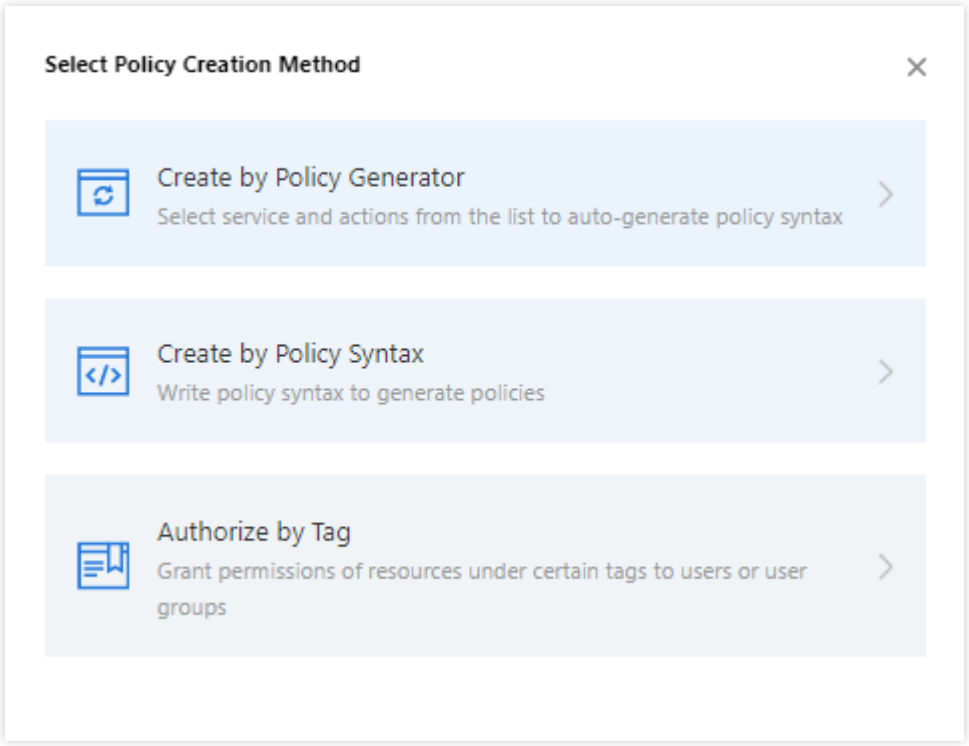
- **资源(resource)**：该权限策略关联哪些镜像仓库，例如所有镜像仓库描述为 `qcs::ccr:::repo/*` ，详见 CAM 资源描述方式。
- **动作(action)**：**该权限策略对**资源(resource)**进行哪些操作，如删除、新建等，通常使用接口进行描述。
- **效力(effect)** ：该权限策略对协作者表现出的效果（允许/拒绝）。

一旦您规划好权限设置，就可以开始进行权限分配。下面我们以“允许协作者创建镜像仓库”为例进行说明：

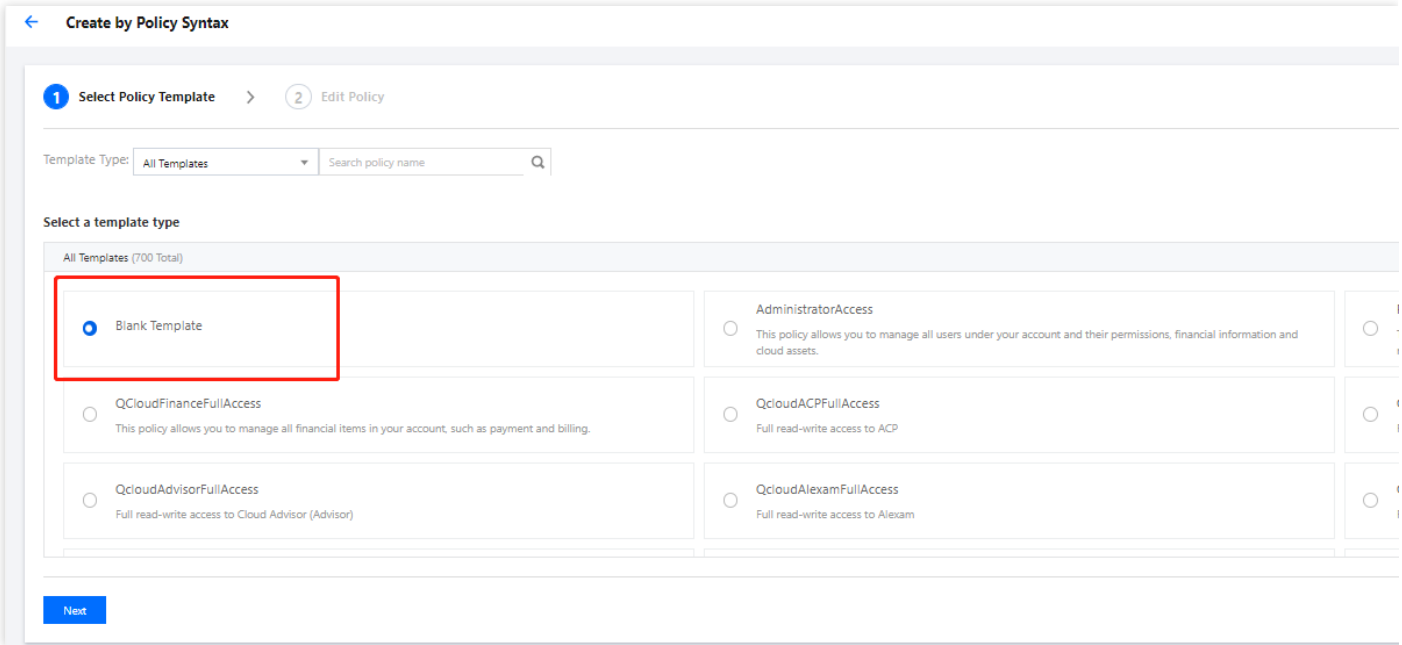
1. 创建自定义 策略。

2. 使用开发商账号登录腾讯云-控制台。

3. 进入 CAM 自定义策略管理页面，单击**新建自定义策略**，打开“选择创建策略方式”对话框。如下图所示：



4. 选择**按策略语法创建** > **空白模板**。

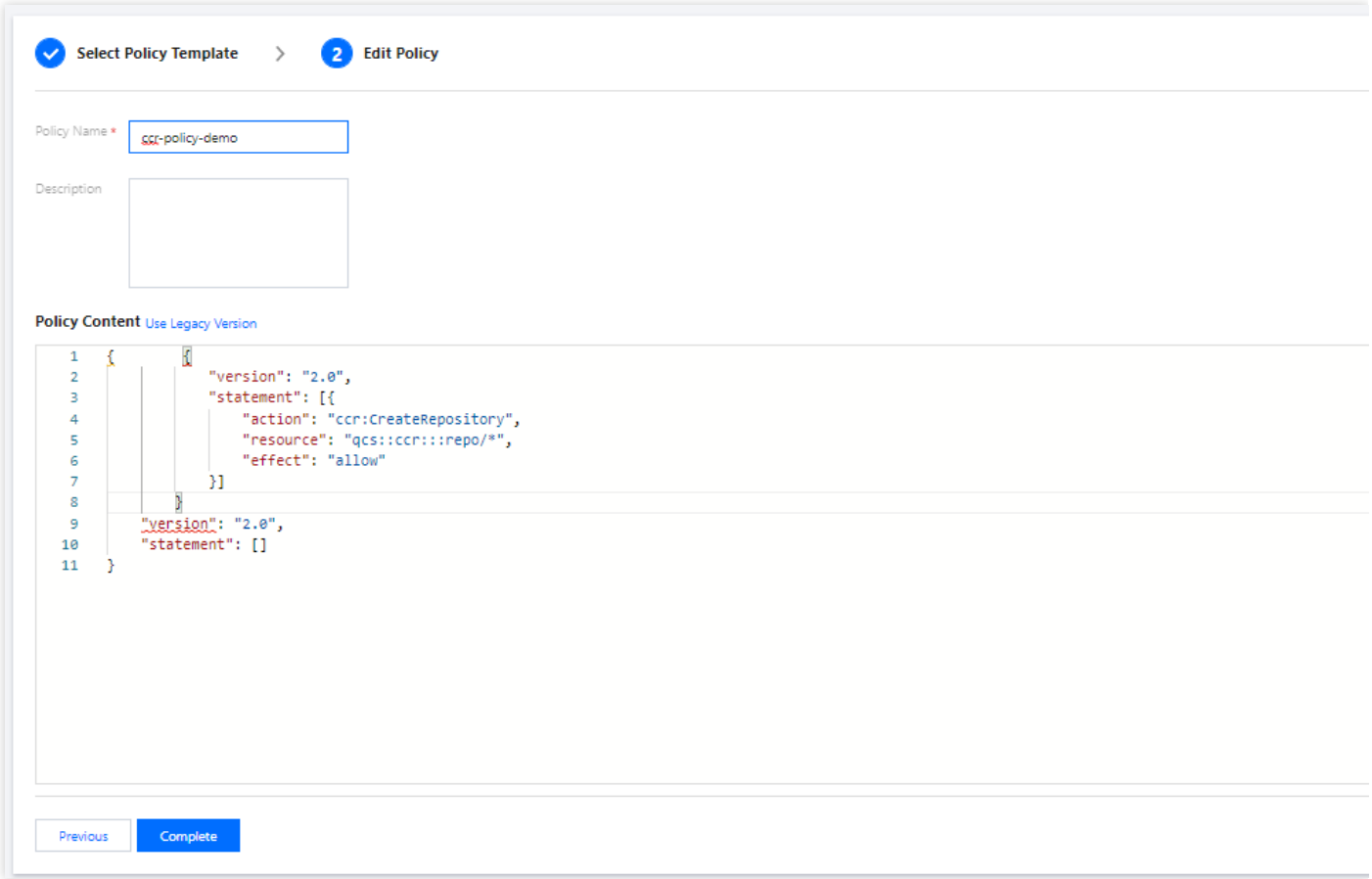


5. 单击**下一步**，进入“编辑策略” 页面。

6. 设置策略名称，并将以下内容填入“编辑策略内容”编辑框中。

```
{
"version": "2.0",
"statement": [{
"action": "ccr:CreateRepository",
"resource": "qcs::ccr:::repo/*",
"effect": "allow"
}]
}
```

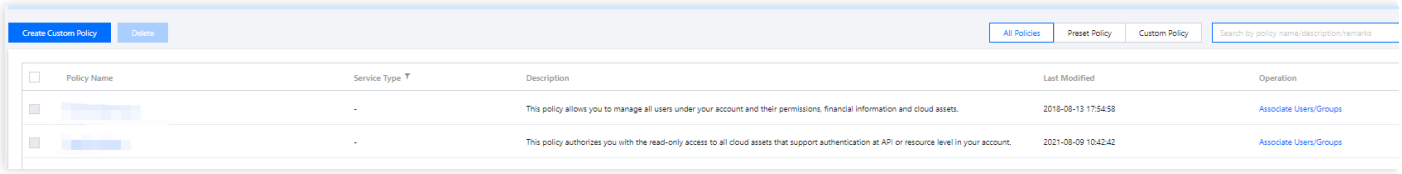
例如，将策略名称设置为 `ccr-policy-demo`，如下图所示：



说明：

resource 末尾使用 * 表示可以在任意命名空间下创建镜像仓库。

6. 单击**创建策略**，结束策略创建过程。



7. 关联自定义策略。步骤1中的策略（ccr-policy-demo）创建完成以后，您可以将其关联到任意协作者，详见 授权管理。策略关联完成后协作者即拥有**在任意命名空间下创建镜像仓库权限**。
   _resource `qcs::ccr:::repo/*` 格式说明：

- `qcs::ccr:::` 为固定格式，表示开发商的腾讯云容器镜像仓库服务。
- `repo` 为固定前缀，代表资源类型，这里是镜像仓库。
- 斜杠(`/`)后面的 `*` 表示匹配所有镜像仓库。

关于 resource 更详细的描述，请参考 CAM 资源描述方式。

按资源进行授权

您可以同时为多个资源进行授权。例如：“允许删除命名空间 foo, bar 中的镜像仓库”，可以创建下面的自定义策略：

```
{
"version": "2.0",
"statement": [{
"action": [
"ccr:BatchDeleteRepository",
"ccr:DeleteRepository"
],
"resource": [
"qcs::ccr:::repo/foo/*",
"qcs::ccr:::repo/bar/*"
],
"effect": "allow"
}]
}
```

注意：

- `qcs::ccr:::repo/foo/*` 中 `foo/*` 表示镜像仓库命名空间 `foo` 下的所有镜像。
- `qcs::ccr:::repo/bar/*` 中 `bar/*` 表示镜像仓库命名空间 `bar` 下的所有镜像。

按动作(接口)进行授权

您可以对一个资源配置多个 `action`，实现资源权限的统一管理。例如："允许创建、删除、push 命名空间 foo 中的镜像仓库"，可以创建下面的自定义策略：

```
{
"version": "2.0",
"statement": [{
"action": [
"ccr:CreateRepository",
"ccr:BatchDeleteRepository",
"ccr:DeleteRepository",
"ccr:push"
],
"resource": "qcs::ccr:::repo/foo/*",
"effect": "allow"
}]
}
```

权限列表

docker client 权限

resource： `qcs::ccr:::repo/${namespace}/${name}`

action：

- `ccr:pull` 使用 docker 命令行 pull 镜像
- `ccr:push` 使用 docker 命令行 push 镜像

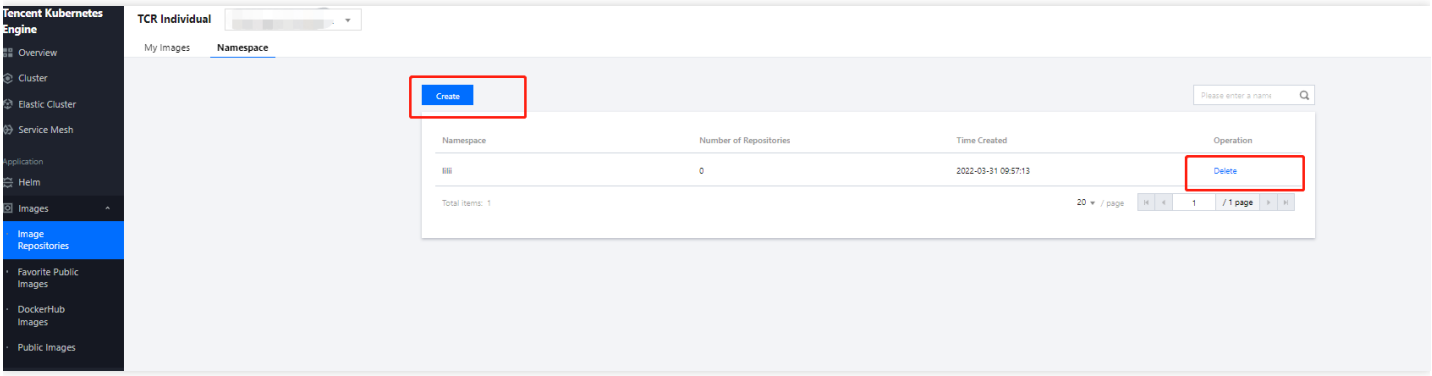
命名空间权限

resource： `qcs::ccr:::repo/${namespace}`

action:

- `ccr:CreateCCRNamespace` 新建镜像仓库命名空间
- `ccr:DeleteUserNamespace` 删除镜像仓库命名空间

功能指引：**容器服务**> 左侧导航栏**镜像仓库** >我的镜像>命名空间。



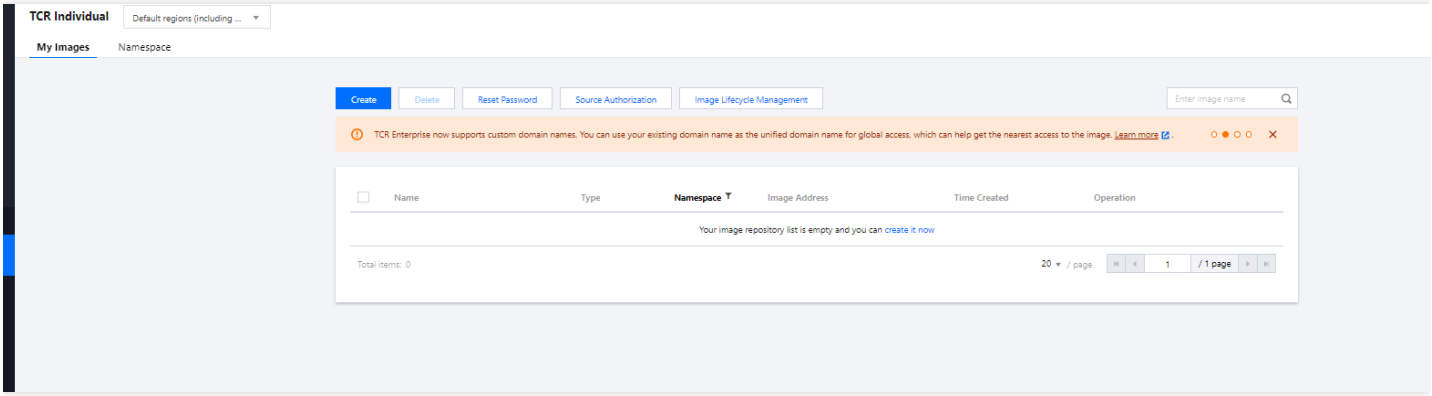
镜像仓库权限

resource： `qcs::ccr:::repo/${namespace}/${name}`

action：

- `ccr:CreateRepository` 创建镜像仓库
- `ccr:DeleteRepository` 删除镜像仓库
- `ccr:BatchDeleteRepository` 批量删除镜像仓库
- `ccr:GetUserRepositoryList` 查看镜像仓库列表

功能指引：**容器服务**> 左侧导航栏**镜像仓库** >我的镜像>我的镜像。



注意：
若要阻止协作者删除某些镜像，请配置多个 action 来实现。

例如，禁止删除任何镜像仓库。

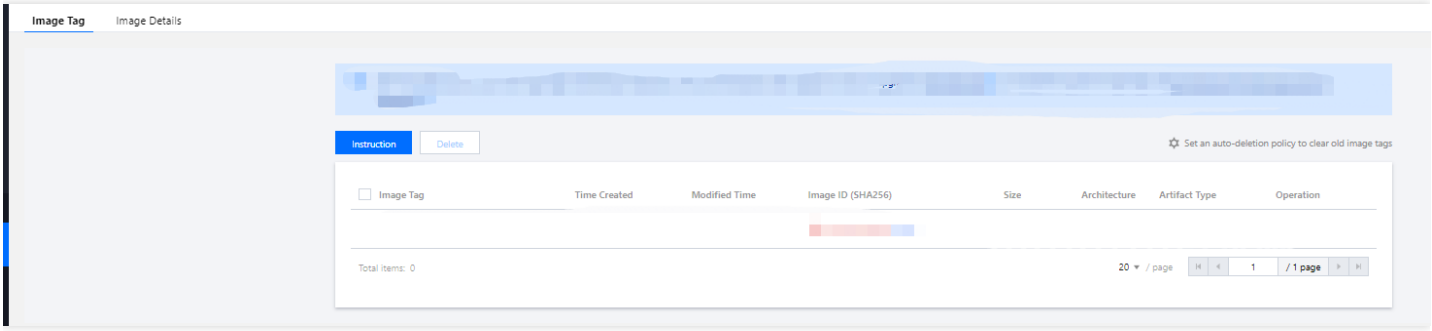
```
{
"version": "2.0",
"statement": [{
"action": [
"ccr:BatchDeleteRepository",
"ccr:DeleteRepository"
],
"resource": "qcs::ccr:::repo/*",
"effect": "deny"
}]
}
```

镜像Tag权限

resource： `qcs::ccr:::repo/${namespace}/${name}:${tag}`

action： `ccr:DeleteTag` 删除镜像 Tag 权限

功能指引：**容器服务**> 左侧导航栏**镜像仓库** >我的镜像>我的镜像> 单击某个镜像名称 > **镜像版本**页面。



TKE 集群级权限控制
使用 TKE 预设策略授权

最近更新时间：2022-03-30 17:57:15

本文介绍腾讯云容器服务 TKE 的预设策略，及如何将子账号关联预设策略，授予子账号特定权限。您可参考文本并根据实际业务诉求进行配置。

TKE 预设策略

您可以使用以下预设策略为您的子账号授予相关权限：

策略	描述
`QcloudTKEFullAccess`	TKE 全读写访问权限，包括 TKE 及相关云服务器、负载均衡、私有网络、监控及用户组权限。
`QcloudTKEInnerFullAccess`	TKE 全部访问权限， TKE 涉及较多产品，建议您配置 `QcloudTKEFullAccess` 权限。
`QcloudTKEReadOnlyAccess`	TKE 只读访问权限。

以下预设策略是在您使用 TKE 服务时，授予 TKE 服务本身的权限。不建议为子账号关联以下预设策略：

策略	描述
`QcloudAccessForCODINGRoleInAccessTKE`	授予 Coding 服务 TKE 相关权限。
`QcloudAccessForIPAMDofTKERole`	授予 TKE 服务弹性网卡相关权限。
`QcloudAccessForIPAMDRoleInQcloudAllocateEIP`	授予 TKE 服务弹性公网 IP 相关权限。
`QcloudAccessForTKERole`	授予 TKE 服务云服务器、标签、负载均衡、日志服务相关权限。
`QcloudAccessForTKERoleInCreatingCFSStorageclass`	授予 TKE 服务文件存储相关权限。
`QcloudAccessForTKERoleInOpsManagement`	该策略关联 TKE 服务角色（TKE_QCSRole），用于 TKE 访问其他云服务资源，包含日志服务等相关操作权限。

子账号关联预设策略

您可在创建子账号的“设置用户权限”步骤中，通过 直接关联 或 随组关联 方式，为该子账户关联预设策略。

直接关联

您可以直接为子账号关联策略以获取策略包含的权限。

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”管理页面，选择需要设置权限的子账号所在行右侧的**授权**。
3. 在弹出的“关联策略”窗口中，勾选需授权的策略。
4. 单击**确定**即可。

随组关联

您可以将子账号添加至用户组，该子账号将自动获取该用户组所关联策略的权限。如需解除随组关联策略，仅需将子账号移出相应用户组即可。

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”管理页面，选择需要设置权限的子账号所在行右侧的**更多操作**>**添加到组**。
3. 在弹出的“添加到组”窗口中，勾选需加入的用户组。
4. 单击**确定**即可。

登录子账号验证

登录 腾讯云容器服务控制台，验证可使用所授权策略对应功能，则表示子账号授权成功。

使用自定义策略授权

最近更新时间：2020-10-10 15:03:43

本文介绍如何自定义配置腾讯云容器服务 TKE 的自定义策略，授予子账号特定权限。您可参考文本并根据实际业务诉求进行配置。

策略语法说明

策略语法结构如下图所示：

- **action**：表示接口。
- **resource**：表示资源。

说明：

您可自行编写策略语法，或通过访问管理 CAM 策略生成器创建自定义策略。可结合以下示例进行自定义策略配置：

- 配置子账号对单个 TKE 集群的管理权限
- 通过标签为子账号配置批量集群的全读写权限限

TKE 接口权限配置

本节提供了集群、节点模块的多个功能所包含的子功能、对应云 API 接口、间接调用接口、权限控制资源级别以及 Action 字段展示相关信息。

集群模块

功能接口对照表如下：

功能	包含子功能	对应云 API 接口	间接调用接口	权限
创建空集群	• Kubernetes 版本选择 • 运行时组件选择 • 选择 VPC 网络 • 设置容器网络 • 自定义镜像选择 • Ipvs 设置	tke:CreateCluster	cam:GetRole account:DescribeUserData account:DescribeWhiteList tag:GetTagKeys cvm:GetVmConfigQuota vpc:DescribeVpcEx cvm:DescribeImages	• 创 口 制 • 获 表 的
使用已有 CVM 创建托管集群	• 创建空集群包含功能 • 将已有 CVM 作为 Node • 挂载安全组 • 挂载数据盘 • 开启自动调节		cvm:DescribeInstances vpc:DescribeSubnetEx cvm:DescribeSecurityGroups vpc:DescribeVpcEx cvm:DescribeImages cvm:ResetInstance cvm:DescribeKeyPairs	• 创 口 制 • 获 表 的
使用已有 CVM 创建独立集群	• 创建空集群包含功能 • 将已有 CVM 作为 Node • 将已有 CVM 作为 Master&ETCD • 挂载安全组 • 挂载数据盘 • 开启自动调节		cvm:DescribeInstances vpc:DescribeSubnetEx cvm:DescribeSecurityGroups vpc:DescribeVpcEx cvm:DescribeImages cvm:ResetInstance cvm:DescribeKeyPairs	• 创 口 制 • 获 表 的 • 获 表 的
自动新建 CVM 创建	• 创建空集群包含功能 • 购买 CVM 作为 node		cvm:DescribeSecurityGroups cvm:DescribeKeyPairs cvm:RunInstances vpc:DescribeSubnetEx	• 创 口 制

托管集群	• 挂载安全组 • 挂载数据盘 • 开启自动调节		vpc:DescribeVpcEx cvm:DescribeImages	• 获表的
自动新建CVM创建独立集群	• 创建空集群包含功能 • 购买 CVM 作为 Node • 购买 CVM 作为 Master&ETCD • 挂载安全组 • 挂载数据盘 • 开启自动调节		cvm:DescribeSecurityGroups cvm:DescribeKeyPairs cvm:RunInstances vpc:DescribeSubnetEx vpc:DescribeVpcEx cvm:DescribeImages	• 创口制 • 获表的
查询集群列表	-	tke:DescribeClusters	-	获取要集
显示集群凭证	-	tke:DescribeClusterSecurity	-	显示要集
开启/关闭集群内/外网访问地址	• 创建托管集群外网访问端口 • 创建集群访问端口 • 修改托管集群外网端口的安全策略 • 查询托管集群开启外网端口流程状态 • 删除托管集群外网访问端口 • 删除集群访问端口	tke:CreateClusterEndpointVip tke:CreateClusterEndpoint tke:ModifyClusterEndpointSP tke:DescribeClusterEndpointVipStatus tke:DescribeClusterEndpointStatus tke:DeleteClusterEndpointVip tke:DeleteClusterEndpoint	-	开启问，的权
删除集群	-	tke:DeleteCluster	tke:DescribeClusterInstances tke:DescribeInstancesVersion tke:DescribeClusterStatus	删除群的

节点模块

功能接口对照表如下：

功能	包含子功能	对应云 API 接口	间接调用接口	权限控制资源级别
添加已有节点	• 将已有节点加入到集群 • 重新设置数据盘 • 设置安全组	tke:AddExistedInstances	cvm:DescribeInstances vpc:DescribeSubnetEx cvm:DescribeSecurityGroups vpc:DescribeVpcEx cvm:DescribeImages cvm:ResetInstance cvm:DescribeKeyPairs cvm:ModifyInstancesAttribute tke:DescribeClusters	• 添加已有节点、需要对应集群的资源权限 • 获取 CVM 列表，需要 CVM 的资源权限
新建节点	• 新建节点加入到集群 • 重新设置数据盘 • 设置安全组	tke:CreateClusterInstances	cvm:DescribeSecurityGroups cvm:DescribeKeyPairs cvm:RunInstances vpc:DescribeSubnetEx vpc:DescribeVpcEx cvm:DescribeImages tke:DescribeClusters	新建节点、需要对应集群的资源权限
节点列表	查看集群节点列表	tke:DescribeClusterInstances	cvm:DescribeInstances tke:DescribeClusters	• 查看节点列表需要对应集群的资源权限 • 获取 CVM 列表，需要 CVM 的资源权限
移出节点	-	tke:DeleteClusterInstances	cvm:TerminateInstances tke:DescribeClusters	• 查看节点列表需要对应集群的资源权限 • 获取 CVM 列表，需要 CVM 的资源权限 • 删除节点，需要对应节点的销毁策略

使用示例
通过标签为子账号配置批量集群的全读写权限

最近更新时间：2022-04-18 16:21:32

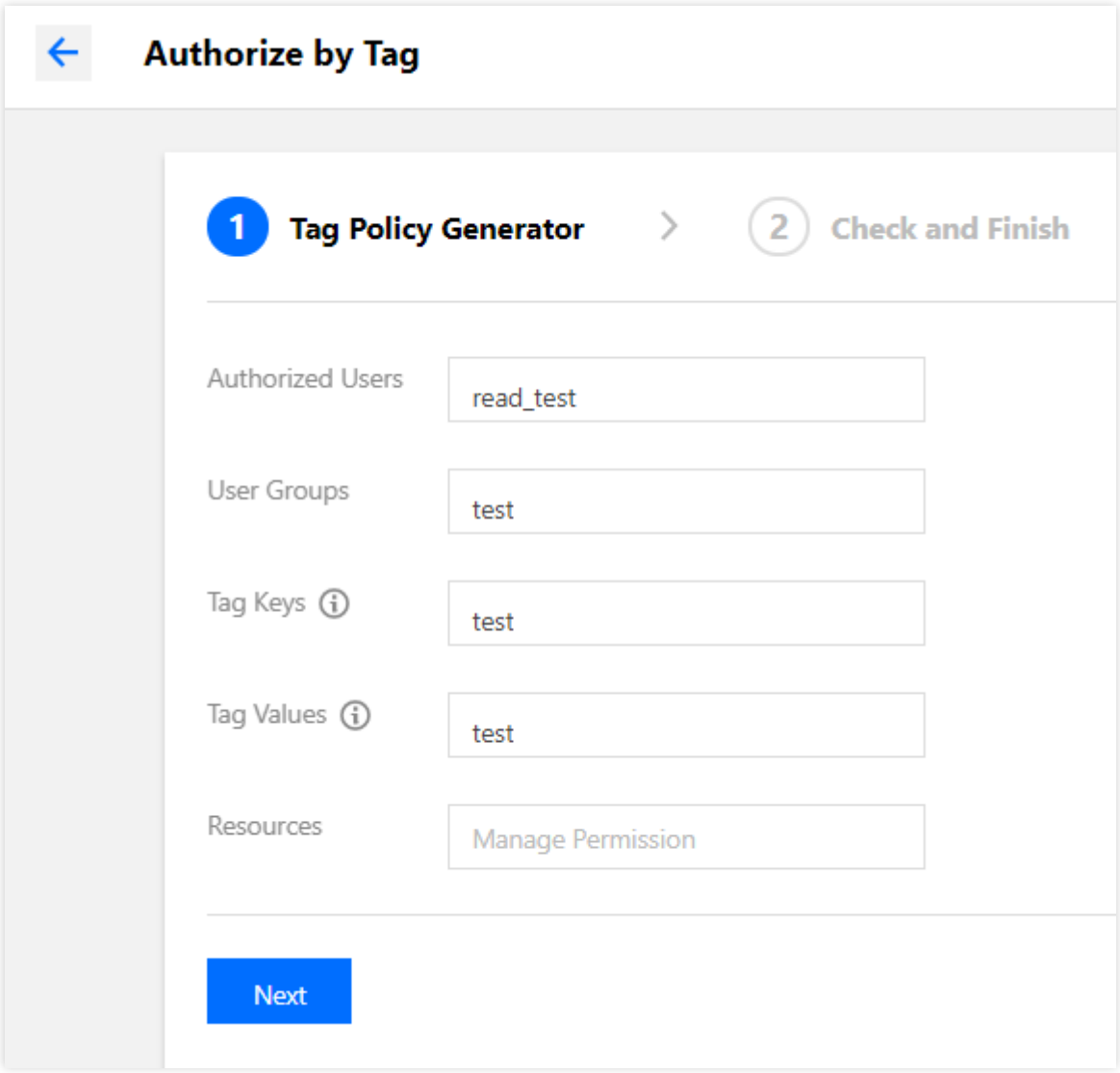
操作场景

您可以通过使用访问管理（Cloud Access Management，CAM）策略让用户拥有在容器服务（Tencent Kubernetes Engine，TKE）控制台中查看和使用特定资源的权限。本文档中的示例介绍如何通过控制台，为子账号授予指定标签集群的权限。

操作步骤

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，单击**新建自定义策略**。
3. 在弹出的“选择创建策略方式”窗口中选择**按标签授权**。

4. 在“按标签授权”页面中，参考以下信息进行配置。如下图所示：



- **赋予用户**：按需勾选需授权的子账号。
- **和用户组**：按需勾选需授权的子账号所在的用户组。
- **在标签键、且具有标签值**：按需选择，授权完成的子账号将对具有该标签键及标签值的资源拥有全读写权限。

5. 单击**下一步**，进入“检查并完成”步骤。
6. 确认策略名及内容无误，单击**完成**即可完成配置。

> 说明：
> 若您未修改由系统自动生成的策略内容，则子账号将被授予指定标签的资源全读写的权限。

配置子账号对单个 TKE 集群的管理权限

最近更新时间：2022-01-25 10:36:21

操作场景

您可以通过使用访问管理（Cloud Access Management，CAM）策略让用户拥有在容器服务（Tencent Kubernetes Engine，TKE）控制台中查看和使用特定资源的权限。本文档中的示例指导您在控制台中配置单个集群的策略。

操作步骤

配置对单个集群全读写权限

1. 登录 CAM 控制台。

2. 在左侧导航栏中，单击 策略，进入策略管理页面。

3. 单击**新建自定义策略**，选择 “按策略语法创建” 方式。

4. 选择 “空白模板” 类型，单击**下一步**。

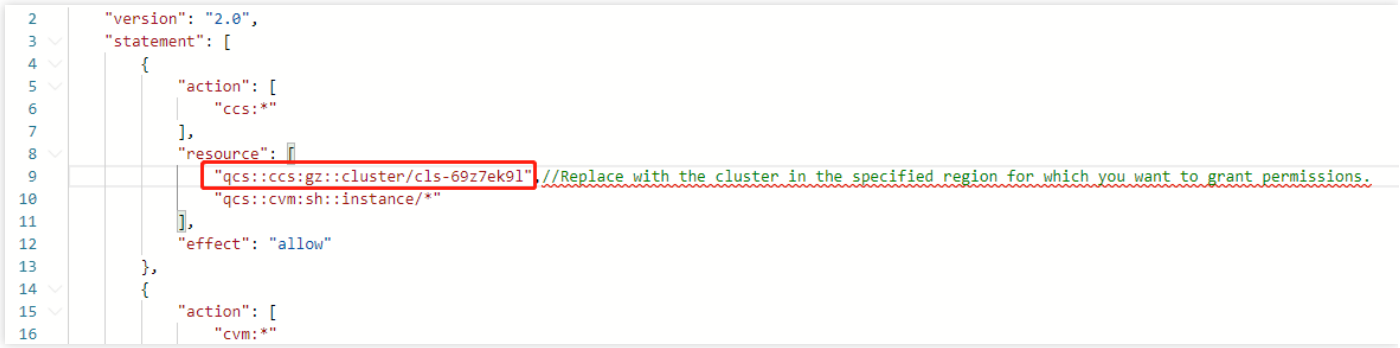
5. 自定义策略名称，将 “编辑策略内容” 替换为以下内容。

```
{
"version": "2.0",
"statement": [
{
"action": [
"tke:*"
],
"resource": [
"qcs::tke:sh::cluster/cls-XXXXXXX",
"qcs::cvm:sh::instance/*"
],
"effect": "allow"
},
{
"action": [
"cvm:*"
],
```

```
"resource": "*",
"effect": "allow"
},
{
"action": [
"vpc:*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"clb:*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"monitor:*",
"cam:ListUsersForGroup",
"cam:ListGroups",
"cam:GetGroup",
"cam:GetRole"
],
"resource": "*",
"effect": "allow"
}
]
}
```

6. 在 “编辑策略内容” 中，将 `qcs::tke:sh::cluster/cls-XXXXXXX` 修改为您想赋予权限的指定地域下的集群。如下图所示：
   例如，您需要为广州地域的 cls-69z7ek9l 集群赋予全读写的权限，将 `qcs::tke:sh::cluster/cls-`

`XXXXXXX` 修改为 `"qcs::tke:gz::cluster/cls-69z7ek9l"`。



> 注意
> 请替换成您想赋予权限的指定地域下的集群 ID。如果您需要允许子账号进行集群的扩缩容，还需要配置子账号用户支付权限。

7. 单击**创建策略**，即可完成对单个集群全读写权限的配置。

配置对单个集群只读权限

1. 登录 CAM 控制台。

2. 在左侧导航栏中，单击 策略，进入策略管理页面。

3. 单击**新建自定义策略**，选择 “按策略语法创建” 方式。

4. 选择 “空白模板” 类型，单击**下一步**。

5. 自定义策略名称，将 “编辑策略内容” 替换为以下内容。

```
{
"version": "2.0",
"statement": [
{
"action": [
"tke:Describe*",
"tke:Check*"
],
"resource": "qcs::tke:gz::cluster/cls-1xxxxxx",
```

```
"effect": "allow"
},
{
"action": [
"cvm:Describe*",
"cvm:Inquiry*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"vpc:Describe*",
"vpc:Inquiry*",
"vpc:Get*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"clb:Describe*"
],
"resource": "*",
"effect": "allow"
},
{
"effect": "allow",
"action": [
"monitor:*",
"cam:ListUsersForGroup",
"cam:ListGroups",
"cam:GetGroup",
"cam:GetRole"
],
"resource": "*"
}
]
}
```

6. 在 “编辑策略内容” 中，将 `qcs::tke:gz::cluster/cls-1xxxxxx` 修改为您想赋予权限的指定地域下的集群。如下图所示：
   例如，您需要为北京地域的 cls-19a7dz9c 集群赋予只读的权限，将 `qcs::tke:gz::cluster/cls-`

`1xxxxxx` 修改为 `qcs::tke:bj::cluster/cls-19a7dz9c` 。

```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "ccs:Describe*",
                "ccs:Check*"
            ],
            "resource": "qcs::ccs:bj::cluster/cls-19a7dz9c",//Replace with the cluster in the specified region for which you want to grant permissions.
            "effect": "allow"
        },
        {
            "action": [
                "cvm:Describe*",
                "cvm:Inquiry*"
            ],
```

7. 单击**创建策略**，即可完成对单个集群只读权限的配置。

配置子账号对 TKE 服务全读写或只读权限

最近更新时间：2022-04-18 15:24:29

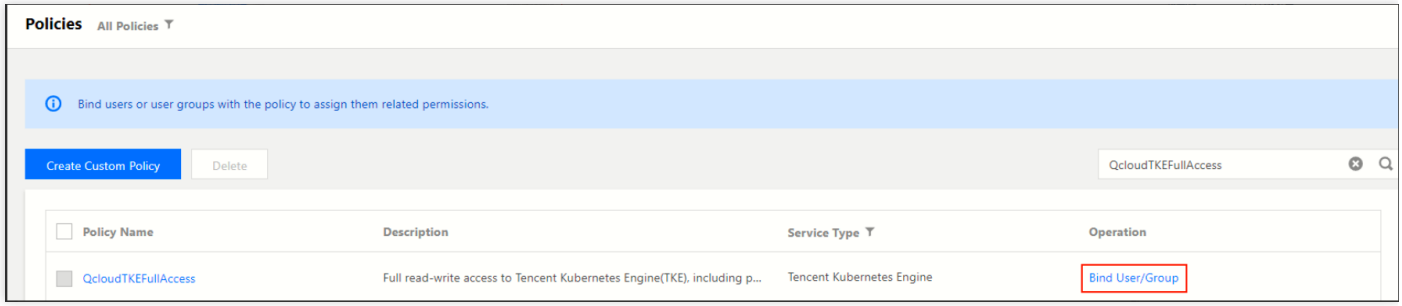
操作场景

您可以通过使用访问管理（Cloud Access Management，CAM）策略让用户拥有在容器服务（Tencent Kubernetes Engine，TKE）控制台中查看和使用特定资源的权限。本文档中的示例指导您在控制台中配置部分权限的策略。

操作步骤

配置全读写权限

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 **QcloudTKEFullAccess** 策略行的**关联用户/组**。如下图所示：



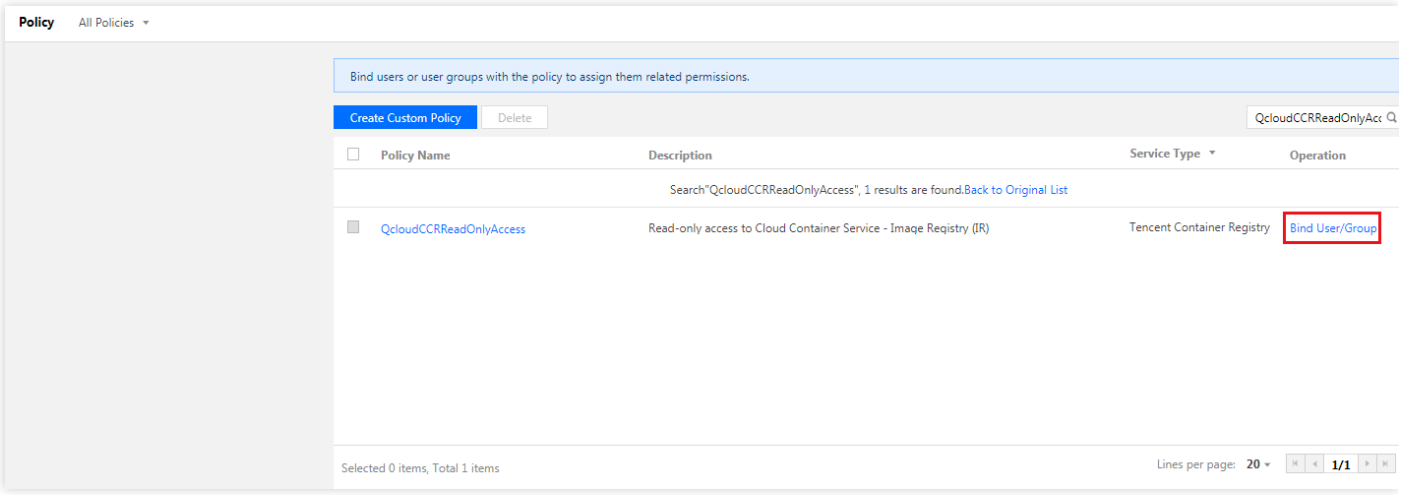
3. 在弹出的“关联用户/用户组”窗口中，勾选需对 TKE 服务拥有全读写权限的账号，单击**确定**，即可完成子账号对 TKE 服务全读写权限的配置。
4. 在策略管理页面中，单击 **QcloudTKEFullAccess** 策略行的**关联用户/组**。
5. 在弹出的“关联用户/用户组”窗口中，勾选需对镜像仓库拥有全读写权限的账号，并单击**确定**，即可完成子账号对镜像仓库全读写权限的配置。

> 说明：
> 如果您需要使用镜像仓库的触发器和自动构建功能，还需额外配置容器服务-持续集成（CCB）的相关权限。

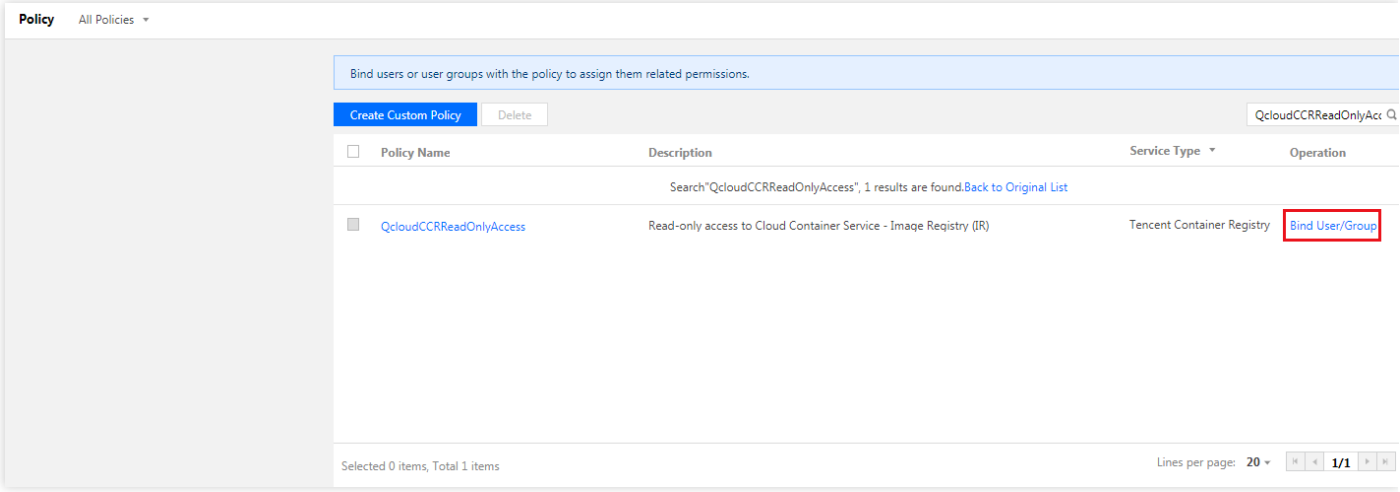
配置只读权限

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 **QcloudTKEReadOnlyAccess** 策略行的**关联用户/组**。如下图所示：



3. 在弹出的“关联用户/用户组”窗口中，勾选需对 TKE 服务拥有只读权限的账号，并单击**确定**，即可完成子账号对 TKE 服务只读权限的配置。
4. 在策略管理页面中，单击 **QcloudCCRReadOnlyAccess** 策略行的**关联用户/组**。如下图所示：



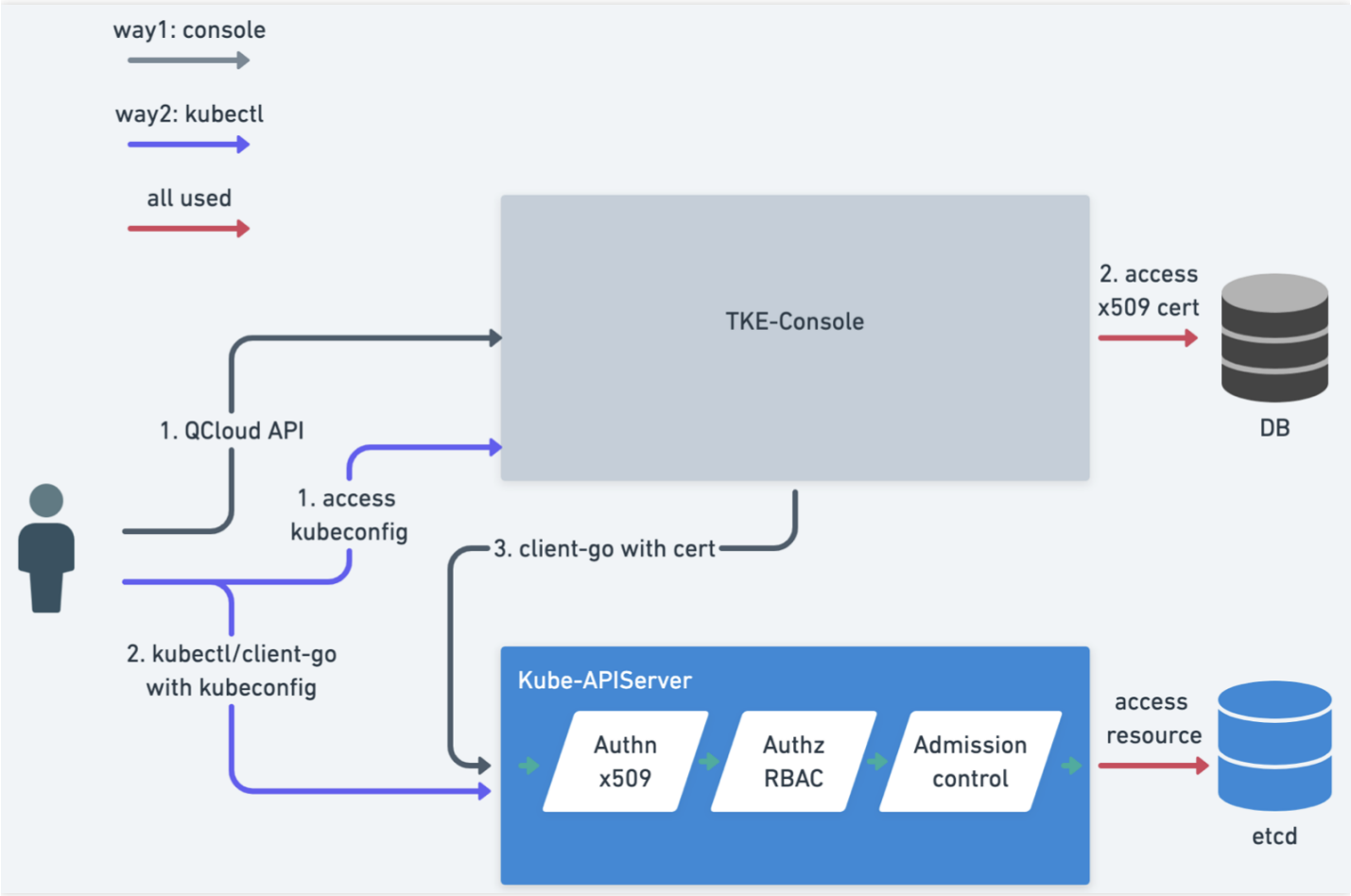
5. 在弹出的“关联用户/用户组”窗口中，勾选需对镜像仓库拥有只读权限的账号，并单击**确定**，即可完成子账号对镜像仓库只读权限的配置。

> 说明：
> 如果您需要使用镜像仓库的触发器和自动构建功能，还需额外配置容器服务-持续集成（CCB）的相关权限。

TKE Kubernetes 对象级权限控制概述

最近更新时间：2020-12-24 10:56:28

TKE 提供了对接 Kubernetes RBAC 的授权模式，便于对子账号进行细粒度的访问权限控制。该授权模式下，可通过容器服务控制台及 kubectl 两种方式进行集群内资源访问。如下图所示：



名词解释

RBAC（Role-Based Access Control）

基于角色的权限控制。通过角色关联用户、角色关联权限的方式间接赋予用户权限。

在 Kubernetes 中，RBAC 是通过 `rbac.authorization.k8s.io` API Group 实现的，即允许集群管理员通过 Kubernetes API 动态配置策略。

Role

用于定义某个命名空间的角色的权限。

ClusterRole

用于定义整个集群的角色的权限。

RoleBinding

将角色中定义的权限赋予一个或者一组用户，针对命名空间执行授权。

ClusterRoleBinding

将角色中定义的权限赋予一个或者一组用户，针对集群范围内的命名空间执行授权。

如需了解更多信息，请前往 Kubernetes 官方说明。

TKE Kubernetes 对象级别权限控制方案

认证方式

Kubernetes APIServer 支持丰富多样的认证策略，例如 x509 证书、bearer token、basic auth。其中，仅 bearer token 单个认证策略支持指定 known-token csv 文件的 beaer token、serviceaccount token、OIDC token、webhook token server 等多种 token 认证方式。

TKE 分析了实现复杂性及多种场景等因素，选择使用 x509 证书认证方式。其优势如下：

- 用户理解成本低。
- 对于存量集群无需进行复杂变更 。
- 按照 User 及 Group 进行划分，后续扩展性好。

TKE 基于 x509 证书认证实现了以下功能：

- 每个子账号单独具备客户端证书，用于访问 Kubernetes APIServer。
- 当子账号在控制台访问 Kubernetes 资源时，后台默认使用该子账号的客户端证书去访问用户 Kubernetes APIServer。
- 支持子账号更新独有的客户端证书，防止凭证泄露。
- 支持主账号或使用集群 `tke:admin` 权限的账号进行查看、更新其他子账号的证书。

授权方式

Kubernetes 包含 RBAC 及 Webhook Server 两种主流授权模式。为给熟悉 Kubernetes 的用户提供一致性体检及需与原生 Kubernetes 结合使用，TKE 选择使用 RBAC 模式。该模式提供了预设 Role 及 ClusterRole，用户只需要在集群内创建相应的 RoleBinding 和 ClusterRoleBinding 即可实现授权变更。其优势如下：

- 亲和有 Kubernetes 基础的用户。

- 复用 Kubernetes RBAC 能力，支持 Namespace 维度、APIGroup 维度及资源维度的多种 Verb 权限控制。
- 支持用户自定义策略。
- 支持管理用户自定义的扩展 API 资源。

TKE Kubernetes 对象级别权限控制功能

通过 TKE 提供的授权管理功能，您可以进行更细粒度的权限控制。例如，仅赋予某个子账号只读权限或仅赋予某个子账号下的某个命名空间读写权限等。可参考以下文档，对子账号进行更细粒度的权限控制：

- 使用预设身份授权
- 自定义策略授权

授权模式对比

最近更新时间：2022-03-30 18:11:44

腾讯云容器服务 TKE 目前存在新旧两种授权模式，旧的授权模式无法进行 Kubernetes 级别的授权管理，建议您升级集群管理的授权模式，以便能够对集群内 Kubernetes 资源进行细粒度的权限控制。

新旧模式对比

对比项	旧模式	新模式
Kubeconfig	admin token	子账号独立的 x509 证书
控制台访问集群资源	无细粒度权限，子账号具备全读写权限	对接 Kubernetes RBAC 资源控制

存量集群授权模式升级操作

升级授权模式

若使用旧授权模式的集群需要升级时，请参考以下操作步骤进行升级：

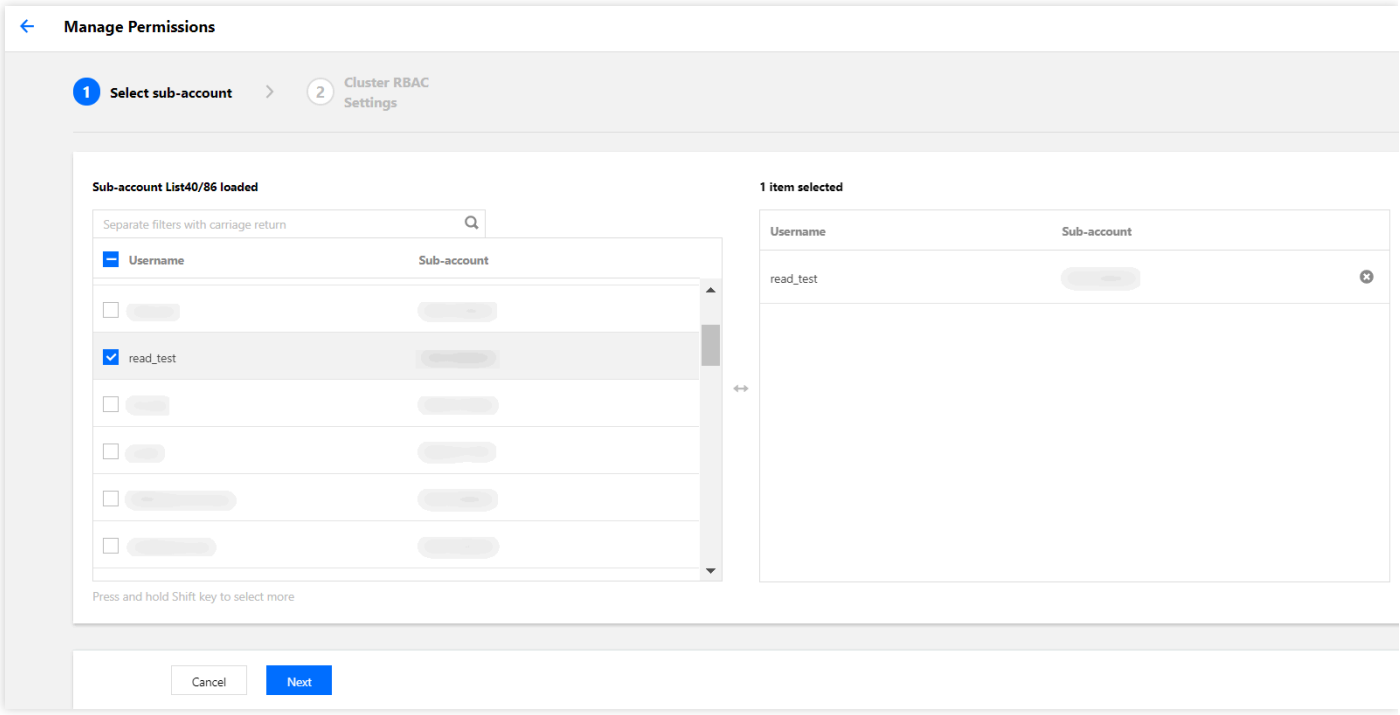
1. 登录容器服务控制台，选择左侧导航栏中的**集群**。
2. 在“集群管理”页面中，选择需升级的集群 ID。
3. 在集群详情页面中，选择左侧**授权管理**>**ClusterRole**。
4. 在 “ClusterRole” 管理页面中，单击**RBAC策略生成器**。
5. 在弹出的“切换权限管理模式”窗口中，单击**切换权限管理模式**即可进行授权模式升级。
   为确保新旧模式的兼容性，升级过程中会进行如下操作：
6. 创建默认预设管理员 ClusterRole：`tke:admin` 。
7. 拉取子账号列表。
8. 为每个子账号生成可用于 Kubernetes APIServer 认证的 x509 客户端证书。
9. 为每个子账号都绑定 `tke:admin` 角色（确保和存量功能兼容）。
0. 升级完毕。

回收子账号权限

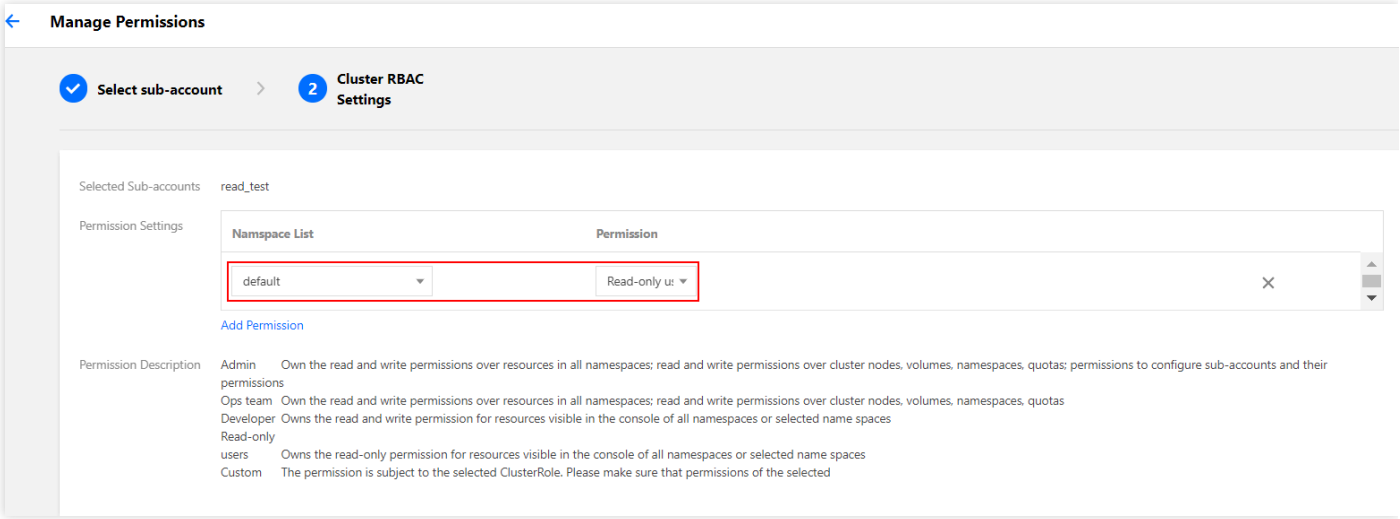
集群授权模式升级完毕后，集群管理员（通常为主账号管理员或创建集群的运维人员）可按需对具有该集群权限的子账号进行权限回收操作，步骤如下：

1. 选择集群**授权管理**下的菜单项，在对应的管理页面中单击**RBAC策略生成器**。

2. 在“管理权限”页面的“选择子账号”步骤中，勾选需回收权限的子账号并单击**下一步**。如下图所示：



3. 在“集群RBAC”步骤中，设置权限。例如，“权限设置”选择为命名空间 “default” 下的“只读用户”。如下图所示：



4. 单击**完成**即可完成回收操作。

确认子账号权限

当完成子账号回收操作后，您可通过以下步骤进行确认：

1. 选择左侧的**授权管理>ClusterRoleBinding**，进入 “ClusterRoleBinding” 管理页面。
2. 选择被回收权限的子账号名称，进入 YAML 文档页面。
   子账号默认为 `tke:admin` 权限，回收对应权限后，可在 YAML 文件中查看变更。如下图所示：

YAML

```yaml
apiVersion: rbac.authorization.k8s.io/v1beta1
kind: ClusterRoleBinding
metadata:
  annotations:
    cloud.tencent.com/tke-account-nickname: bxg
  creationTimestamp: "2020-07-08T12:59:05Z"
  labels:
    cloud.tencent.com/tke-account: "[redacted]"
  name: [redacted]-ClusterRole
  resourceVersion: "5838559579"
  selfLink: /apis/rbac.authorization.k8s.io/v1beta1/clusterrolebindings/[redacted]-ClusterRole
  uid: d43ef4ac-d68a-4e01-[redacted]
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: tke:ro
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: User
  name: [redacted]-1594205611
```

新授权模式相关问题

在新授权模式下创建的集群，谁具备管理员 admin 权限？

集群的创建者及主账号始终具备 `tke:admin` ClusterRole 的权限。

当前使用账号是否可控制自身权限？

目前不支持通过控制台操作当前使用账号权限，如需进行相关操作，可通过 kubectl 完成。

是否可以直接操作 ClusterRoleBinding 及 ClusterRole？

请勿直接对 ClusterRoleBinding 及 ClusterRole 进行修改或删除等操作。

客户端证书是如何创建的？

当您使用子账号通过控制台访问集群资源时，TKE 会获取该子账号的客户端证书。若未获取到证书，则会为该子账号创建客户端证书。

在访问管理 CAM 中删除了子账号，相关权限会自动回收吗？

支持权限自动回收，您无需再进行相关操作。

如何授权其他账户“授权管理”的权限？

可使用默认管理员角色 `tke:admin` 进行“授权管理”的授权操作。

使用预设身份授权

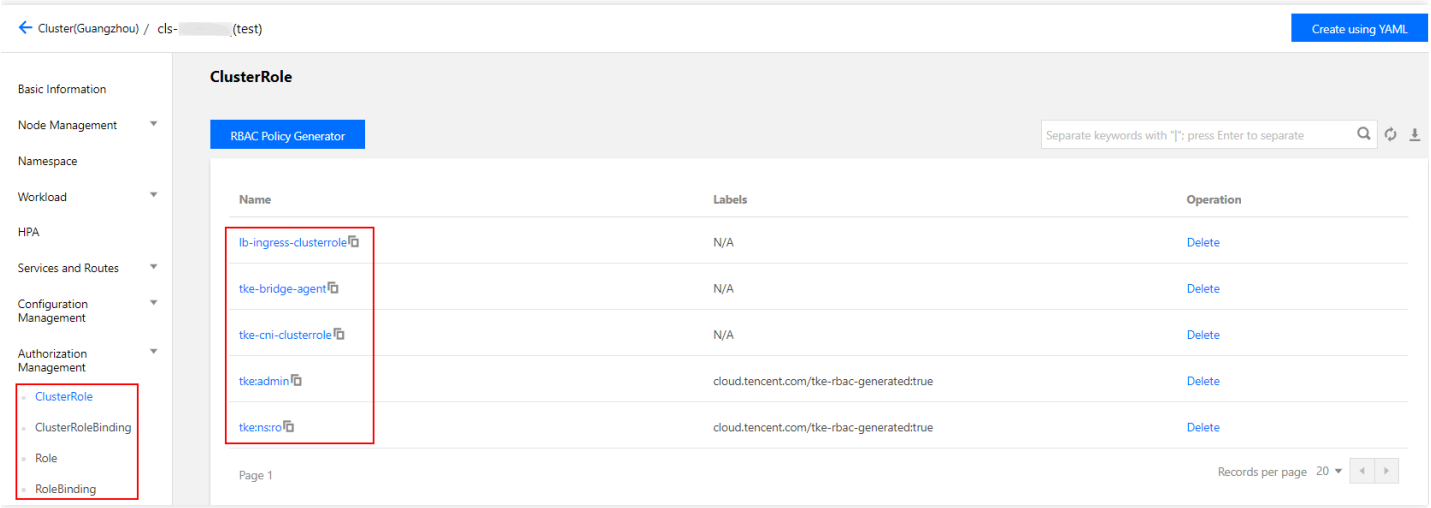
最近更新时间：2022-03-30 17:55:45

预设角色说明

腾讯云容器服务控制台通过 Kubernetes 原生的 RBAC 授权策略，针对子账号提供了细粒度的 Kubernetes 资源权限控制。同时提供了预设角色： Role 及 ClusterRole，详细说明如下：

Role 说明

容器服务控制台提供授权管理页，默认**主账号**及**集群创建者**具备管理员权限。可对其他拥有该集群 DescribeCluster Action 权限的子账号进行权限管理。如下图所示：



ClusterRole 说明

- **所有命名空间维度**：
- **管理员（tke:admin）**：对所有命名空间下资源的读写权限，具备集群节点、存储卷、命名空间、配额的读写权限，可配置子账号的读写权限。
- **运维人员（tke:ops）**：对所有命名空间下控制台可见资源的读写权限，具备集群节点、存储卷、命名空间、配额的读写权限。
- **开发人员（tke:dev）**：对所有命名空间下控制台可见资源的读写权限。
- **受限人员（tke:ro）**：对所有命名空间下控制台可见资源的只读权限。
- **自定义**：用户自定义 ClusterRole。
- **指定命名空间维度**：
  - **开发人员（tke:ns:dev）**：对所选命名空间下控制台可见资源的读写权限，需要选择指定命名空间。
  - **只读用户（tke:ns:ro）**：对所选命名空间下控制台可见资源的只读权限，需要选择指定命名空间。

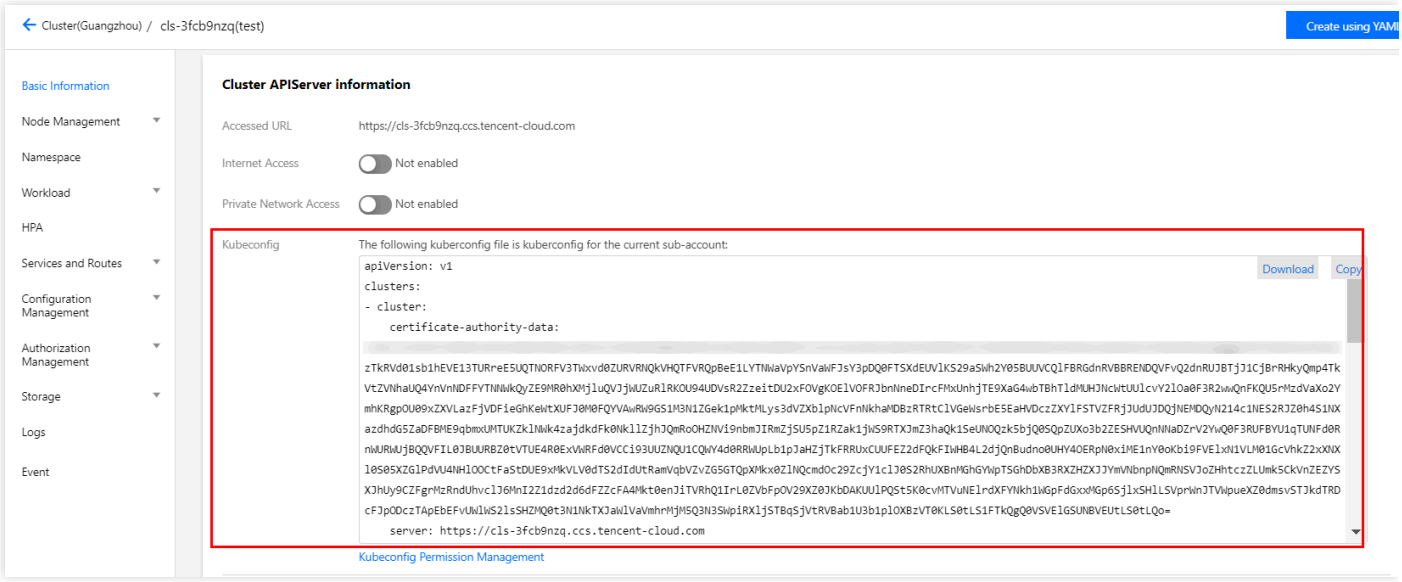
- 所有预设的 ClusterRole 都将带有固定 label： `cloud.tencent.com/tke-rbac-generated: "true"` 。
- 所有预设的 ClusterRoleBinding 都带有固定的 annotations： `cloud.tencent.com/tke-account-nickname: yournickname` 及 label： `cloud.tencent.com/tke-account: "yourUIN"` 。

操作步骤

获取凭证

容器服务默认会为每个子账号创建独立的凭证，用户只需访问集群详情页或调用云 API 接口 DescribeClusterKubeconfig，即可获取当前使用账号的凭证信息 Kubeconfig 文件。通过控制台获取步骤如下：

1. 登录容器服务控制台，选择左侧导航栏中的**集群**。
2. 在“集群管理”页面中，选择需目标集群 ID。
3. 在集群详情页面中，选择左侧的**基本信息**即可在“集群APIServer信息”模块中查看并下载 Kubeconfig 文件。如下图所示：



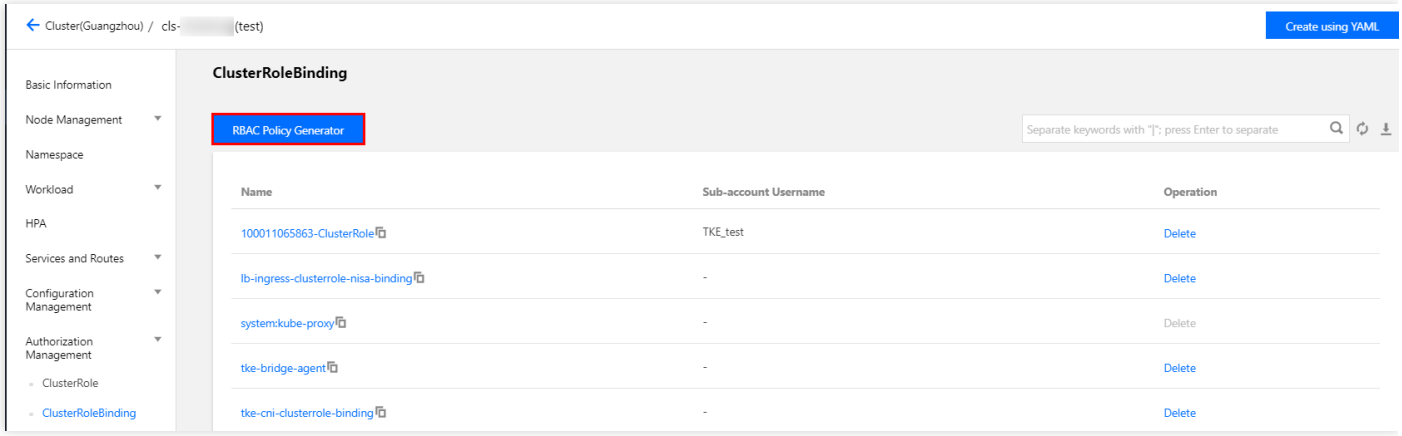
凭证管理

集群管理员可以访问凭证管理页，进行查看并更新所有账号下集群的凭证。详情请参见 更新子账号的 TKE 集群访问凭证。

授权

> 说明：
> 请联系集群管理员（主账号、集群创建者或拥有 admin role 的用户）进行授权。

1. 在“集群管理”页面中，选择目标集群 ID。
2. 在集群详情页面中，选择左侧**授权管理**>**ClusterRoleBinding**。
3. 在 “ClusterRoleBinding” 管理页面中，单击**RBAC策略生成器**。如下图所示：



4. 在“管理权限”页面的“选择子账号”步骤中，勾选需授权的子账号并单击**下一步**。
5. 在“集群RBAC设置”步骤中，按照以下指引进项权限设置：

- **Namespace列表**：按需指定权限生效的 Namespace 范围。
- **权限**：请参考界面中的“权限说明”，按需设置权限。

> 说明：
> 您还可以单击**添加权限**，继续进行权限自定义设置。

鉴权

登录子账号，确认该账号已获得所授权限，则表示授权成功。

自定义策略授权

最近更新时间：2022-04-21 17:47:05

本文介绍如何通过自行编写 Kubernetes 的 ClusterRole 和 Role 以授予子账号特定权限，您可根据业务诉求进行对应操作。

策略语法说明

您可自行编写策略语法，或通过访问管理 CAM 策略生成器创建自定义策略。YAML 示例如下：

Role：命名空间维度

```
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
name: testRole
namespace: default
rules:
- apiGroups:
- ""
resources:
- pods
verbs:
- create
- delete
- deletecollection
- get
- list
- patch
- update
- watch
```

ClusterRole：集群维度

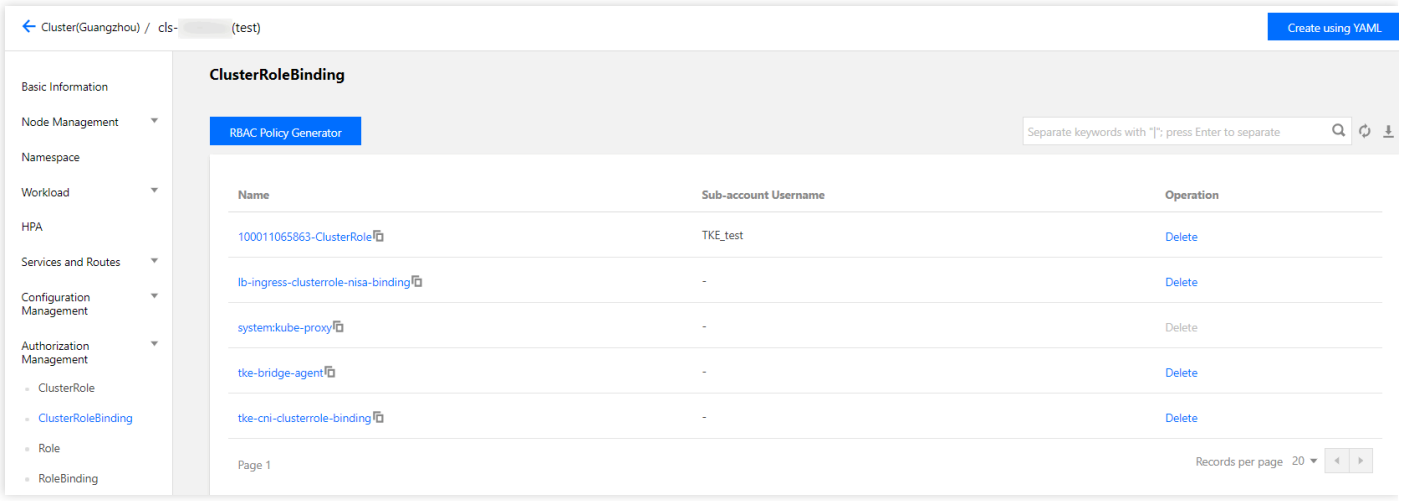
```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
name: testClusterRole
rules:
- apiGroups:
- ""
```

```
resources:
- pods
verbs:
- create
- delete
- deletecollection
- get
- list
- patch
- update
- watch
```

操作步骤

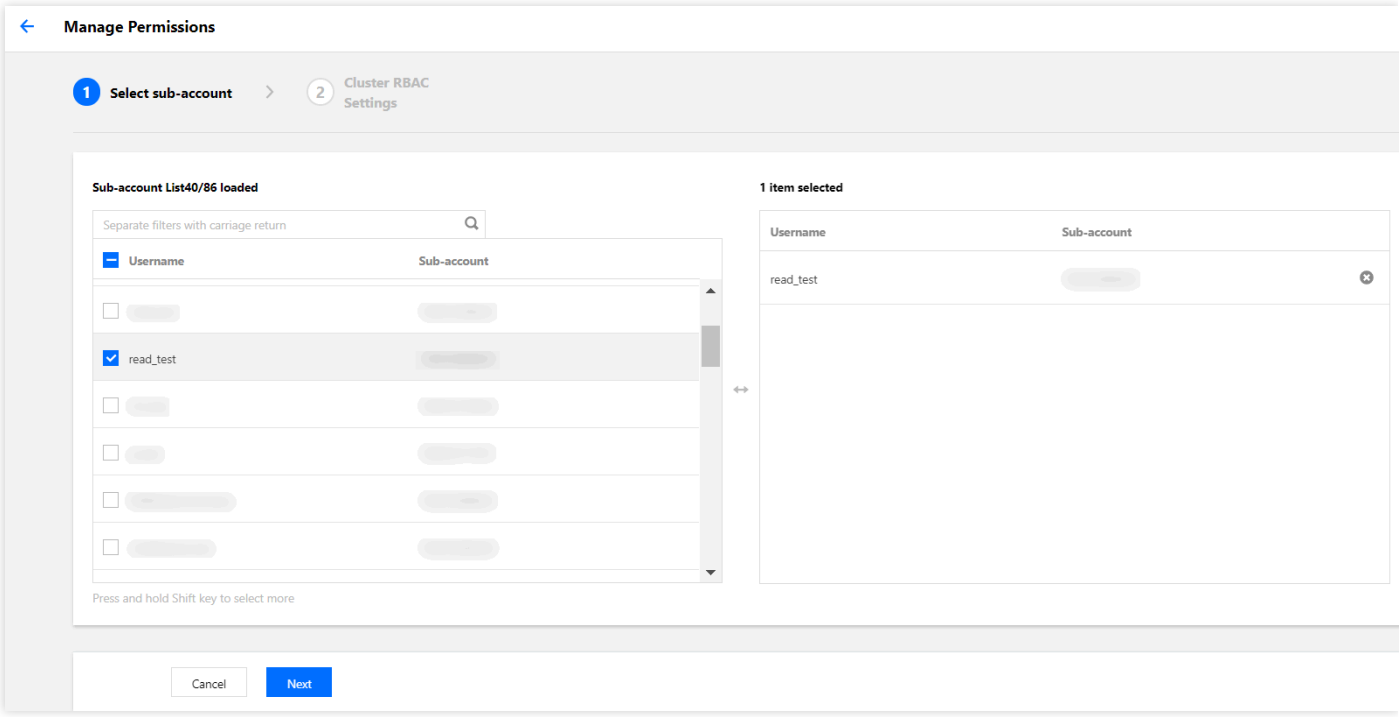
> 说明：
> 该步骤以为子账号绑定自定义 ClusterRole 为例，与绑定 Role 的步骤基本一致，您可结合实际需求进行操作。

1. 登录容器服务控制台，选择左侧导航栏中的**集群**。
2. 在“集群管理”页面中，选择需升级的集群 ID。
3. 在集群详情页面中，选择左侧**授权管理**>**ClusterRole**。如下图所示：

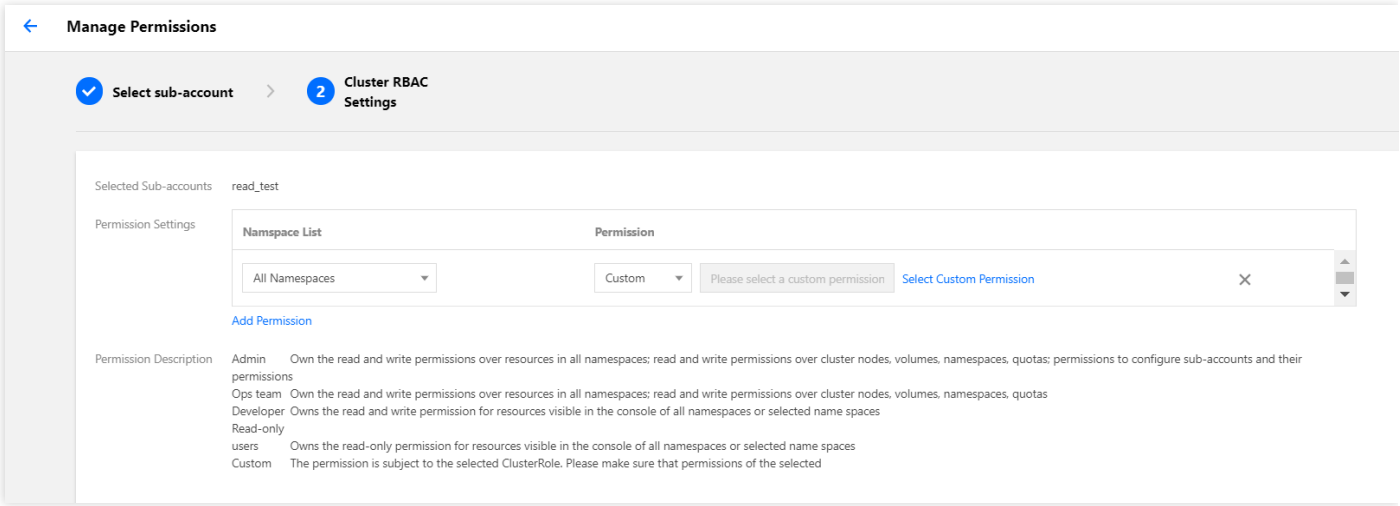


4. 在 “ClusterRole” 管理页面中，选择右上角的**YAML创建资源**。
5. 在编辑界面输入自定义策略的 YAML 内容，单击**完成**即可创建 ClusterRole。
   该步骤以 ClusterRole：集群维度 YAML 为例，创建完成后，可在 “ClusterRole” 管理页面中查看自定义权限 “testClusterRole”。

6. 在 “ClusterRoleBinding” 管理页面中，单击**RBAC策略生成器**。
7. 在“管理权限”页面的“选择子账号”步骤中，勾选需授权的子账号并单击**下一步**。如下图所示：



8. 进入“集群RBAC设置”界面，按照以下指引进项权限设置。如下图所示：



- **Namespace列表**：按需指定权限生效的 Namespace 范围。
- **权限**：选择“自定义”，并单击**选择自定义权限**。按需在自定义权限列表中进行权限选择，本文以选择已创建的自定义权限 “testClusterRole” 为例。

> 说明：
> 您还可以单击**添加权限**，继续进行权限自定义设置。

9. 单击**完成**即可完成授权操作。

参考资料

如需了解更多信息，可参考 Kubernetes 官方文档 ：使用RBAC授权。

更新子账号的 TKE 集群访问凭证

最近更新时间：2022-03-30 18:09:13

访问凭证功能

腾讯云容器服务 TKE 基于 x509 证书认证实现了以下功能：

- 每个子账号均单独具备客户端证书，用于访问 Kubernetes APIServer。
- 在 TKE 新授权模式下，不同子账号在获取集群访问凭证时，即访问集群基本信息页面或调用云 API 接口 DescribeClusterKubeconfig 时，将会获取到子账户独有的 x509 客户端证书，该证书是使用每个集群的自签名 CA 进行签发的。
- 当子账号在控制台访问 Kubernetes 资源时，后台默认使用该子账号的客户端证书去访问用户 Kubernetes APIServer。
- 支持子账号更新独有的客户端证书，防止凭证泄露。
- 支持主账号或使用集群 `tke:admin` 权限的账号进行查看、更新其他子账号的证书。

操作步骤

1. 登录容器服务控制台，选择左侧导航栏中的**集群**。
2. 在“集群管理”页面中，选择需目标集群 ID。
3. 在集群详情页面中，选择左侧的**基本信息**，在“集群APIServer信息”模块中单击**Kubeconfig权限管理**。

4. 在弹出的 “Kubeconfig权限管理” 窗口中，按需勾选认证账号并单击**更新**即可。如下图所示：