容器服务

集群安全配置

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

集群安全配置
身份验证和授权
权限管理
概述

最近更新时间：2023-05-17 15:40:18

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 TKE 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 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：2025-09-23 11:10:01

在使用腾讯云容器服务（Tencent 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。

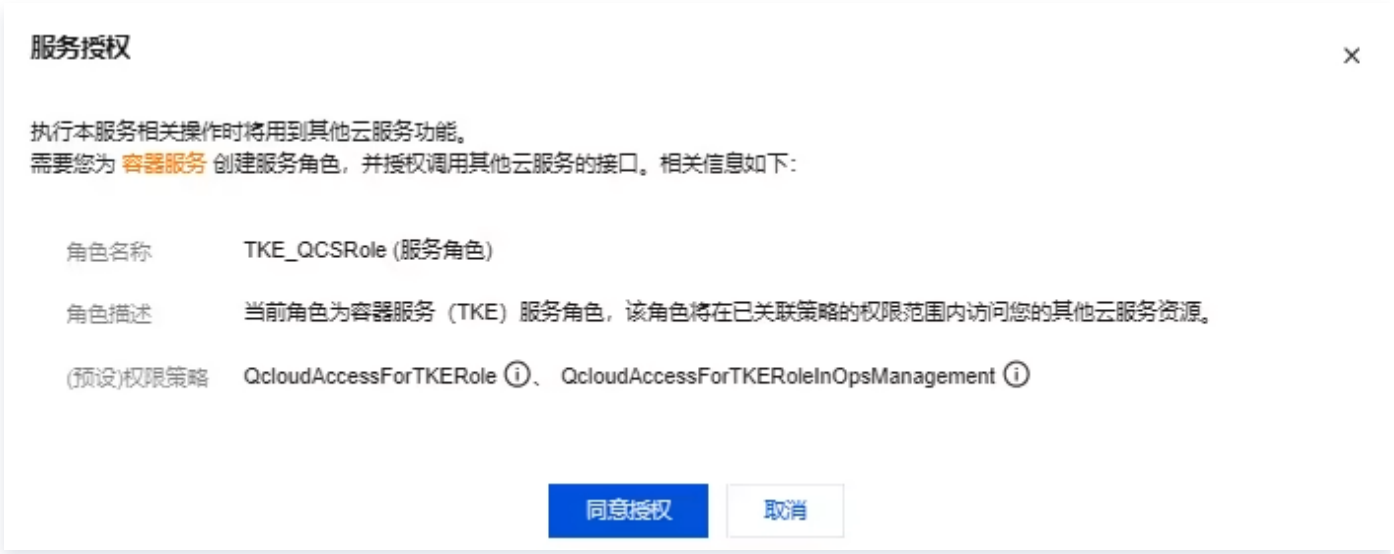
预设策略 QcloudAccessForTKERole

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**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

可前往访问管理平台查看预设策略 QcloudAccessForTKERole 授权访问周边云服务的权限内容。

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

可前往访问管理平台查看预设策略 QcloudAccessForTKERoleInOpsManagement 授权访问 CLS 日志服务的权限内容。

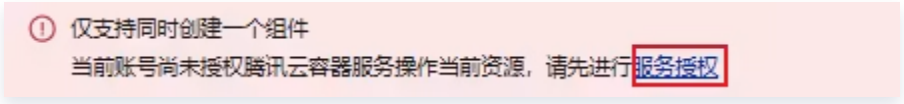
预设策略 QcloudAccessForTKERoleInCreatingCFSStorageclass

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，选择地域及集群后，进入集群详情页。
3. 选择左侧导航中的**组件管理**，在组件管理页面单击**新建**。
4. 在新建组件管理中，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. 在服务授权中，单击**同意授权**并完成身份验证即可成功授权。

权限内容

可前往访问管理平台查看预设策略 QcloudAccessForTKERoleInCreatingCFSStorageclass 授权访问 CFS 文件存储服务的权限内容。

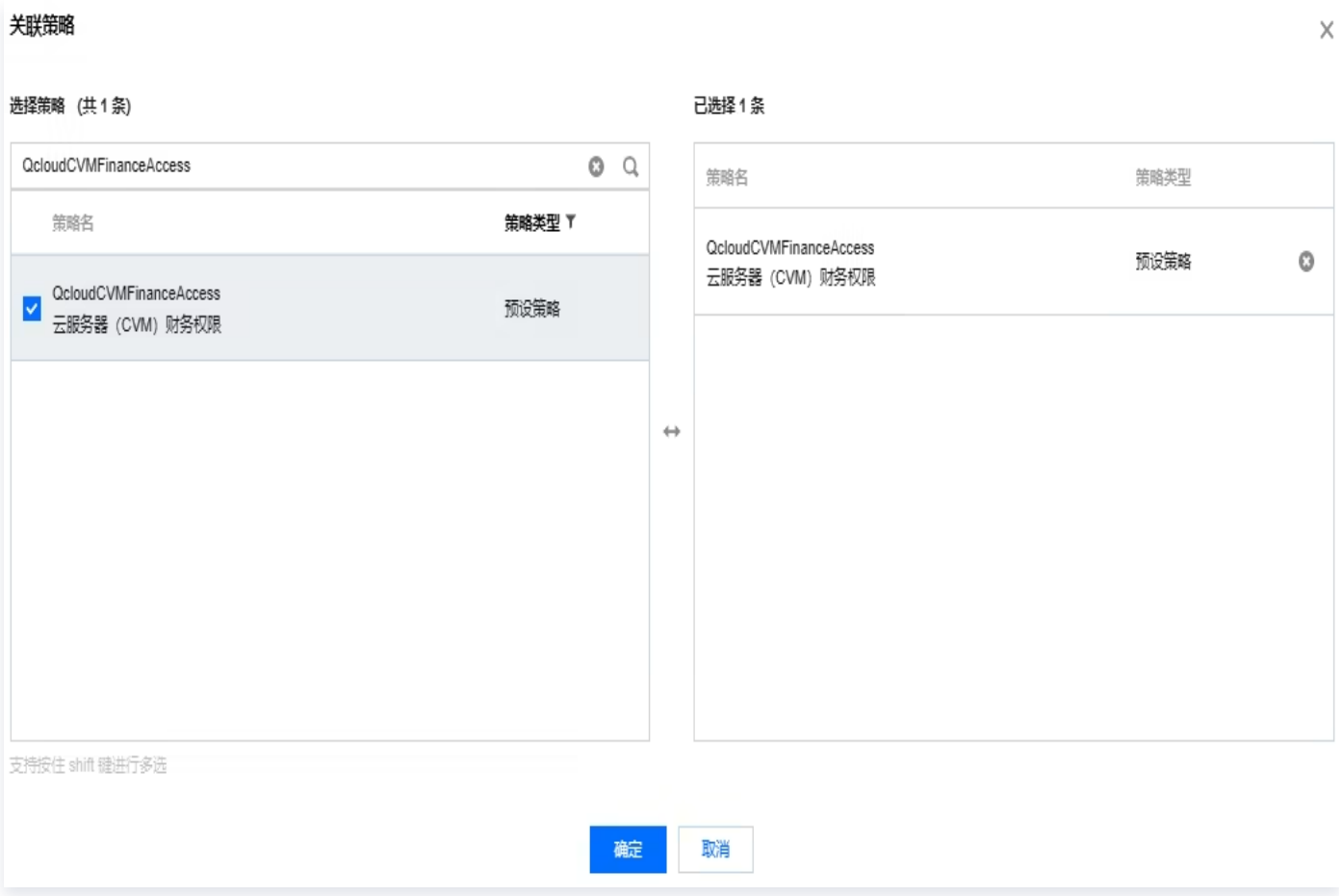
预设策略 QcloudCVMFinanceAccess

授权场景

当您需要购买包年包月云硬盘时，需要为角色 `TKE_QCSRole` 添加该策略以配置支付权限，否则可能会因为没有支付权限导致创建基于包年包月 StorageClass 的 PVC 失败。

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。
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. 在关联策略中，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

可前往访问管理平台查看预设策略 QcloudCVMFinanceAccess 授权访问云服务器财务权限的权限内容。

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. 单击集群列表上方的**新建**。
3. 在创建集群页面，找到**网络配置** > **容器网络插件**，选择 VPC-CNI 时，单击**服务授权**。
4. 在服务授权中，单击**同意授权**并完成身份验证即可成功授权。

权限内容

可前往访问管理平台查看预设策略 QcloudAccessForIPAMDofTKERole 授权访问周边云服务的权限内容。

TCR 镜像仓库资源级权限设置

最近更新时间：2023-12-19 10:53:31

TKE 内置支持使用容器镜像服务 TCR 内镜像，并同时支持个人版及企业版。在使用镜像仓库时，可以按照命名空间、仓库颗粒度配置访问权限，方便企业灵活、精细管理权限。

具体设置请参考：

- 企业版：TCR 企业版权限管理指南
- 个人版：TCR 个人版权限管理指南

TKE 集群级权限控制
使用 TKE 预设策略授权

最近更新时间：2025-05-26 17:00:01

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
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。

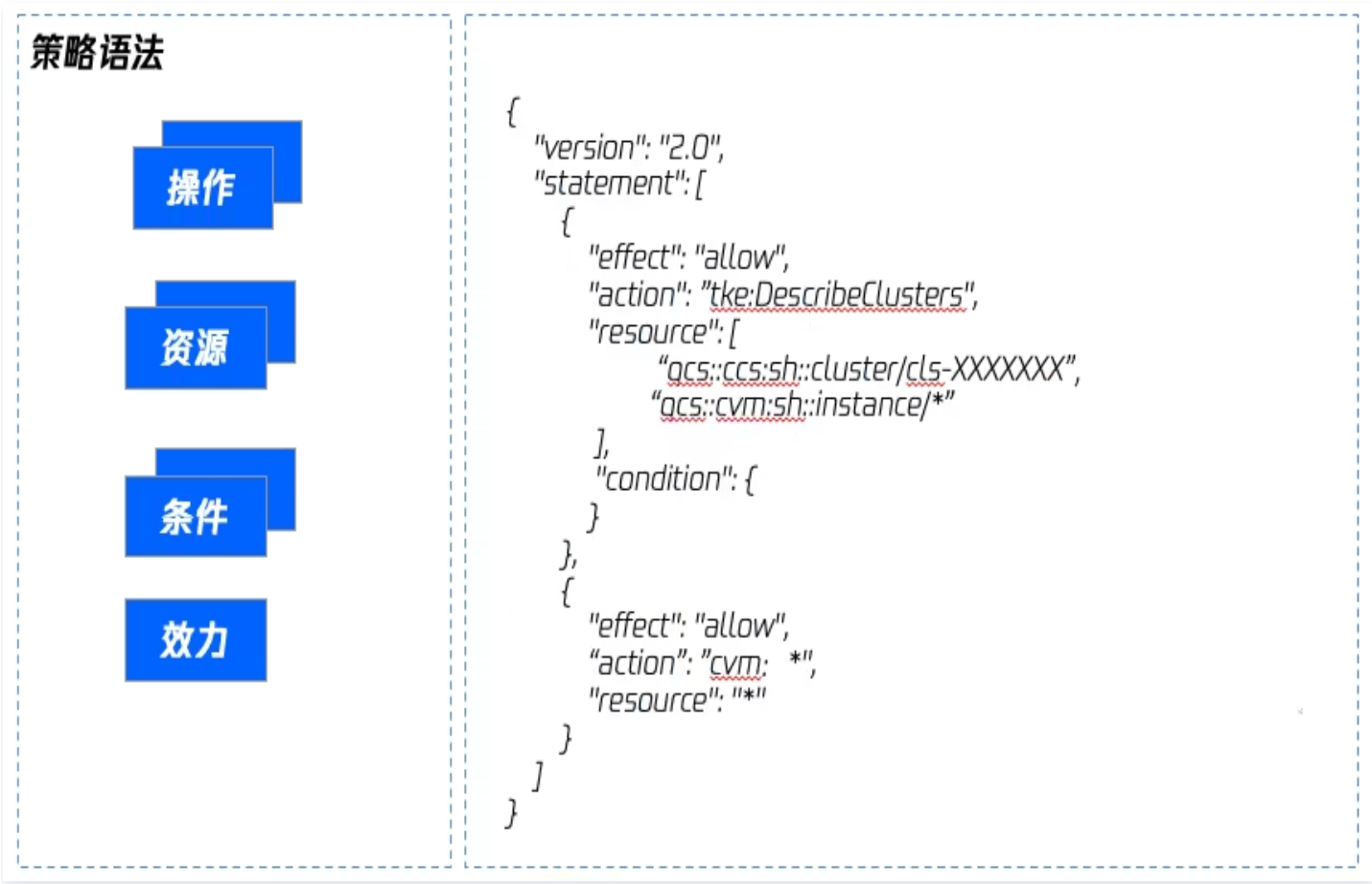
使用自定义策略授权

最近更新时间：2024-08-29 16:14:01

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需求进行配置。

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

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	权限控制资源级别	Action 字段
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 vpc:DescribeVpcEx cvm:DescribeImages	• 创建集群是接口级别权限控制 • 获取 VPC 列表，需要 VPC 的资源权限	"tke:CreateCluster", "cam:GetRole", "tag:GetTagKeys", "vpc:DescribeVpcEx", "cvm:DescribeImages"
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	• 创建集群是接口级别权限控制 • 获取 CVM 列表，需要 CVM 的资源权限	"tke:CreateCluster", "cvm:DescribeInstances", "vpc:DescribeSubnetEx", "cvm:DescribeSecurityGroups", "vpc:DescribeVpcEx", "cvm:DescribeImages", "cvm:ResetInstance", "cvm:Desc

					ribeKeyPairs"
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	• 创建集群是接口级别权限控制 • 获取 VPC 列表，需要 VPC 的资源权限 • 获取 CVM 列表，需要 CVM 的资源权限	"tke:CreateCluster", "cvm:DescribeInstances", "vpc:DescribeSubnetEx", "cvm:DescribeSecurityGroups", "vpc:DescribeVpcEx", "cvm:DescribeImages", "cvm:ResetInstance", "cvm:DescribeKeyPairs"
自动新建 CVM 创建托管集群	• 创建空集群包含功能 • 购买 CVM 作为 node • 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	• 创建集群是接口级别权限控制 • 获取 VPC 列表，需要 VPC 的资源权限	"cvm:DescribeSecurityGroups", "cvm:DescribeKeyPairs", "cvm:RunInstances", "vpc:DescribeSubnetEx", "vpc:DescribeVpcEx", "cvm:DescribeImages", "tke:CreateCluster"
自动新建 CVM 创建独	• 创建空集群包含功		cvm:DescribeSecurity	• 创建集群是接口级	"cvm:DescribeSecurit

立集群	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		Groups cvm:DescribeKeyPairs cvm:RunInstancesvpc:DescribeSubnetExvpc:DescribeVpcExcvm:DescribeImages	别权限控制 • 获取 VPC 列表，需要 VPC 的资源权限	yGroups", "cvm:DescribeKeyPairs", "cvm:RunInstances", "vpc:DescribeSubnetEx", "vpc:DescribeVpcEx", "cvm:DescribeImages", "tke:CreateCluster"
查询集群列表	-	tke:DescribeClusters	-	获取集群列表，需要集群的资源权限	"tke:DescribeClusters"
显示集群凭证	-	tke:DescribeClusterSecurity	-	显示集群凭证，需要集群的资源权限	"tke:DescribeClusterSecurity"
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:Delete	-	开启关闭集群访问，需要集群资源的权限	-

		ClusterEndpoint			
删除集群	–	tke:DeleteCluster	tke:DescribeClusterInstances tke:DescribeInstancesVersion tke:DescribeClusterStatus	删除集群，需要集群的资源权限	"tke:DescribeClusterInstances", "tke:DescribeInstancesVersion", "tke:DescribeClusterStatus", "tke:DeleteCluster"

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	Action 字段
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	"cvm:DescribeInstances", "vpc:DescribeSubnetEx", "cvm:DescribeSecurityGroups", "vpc:DescribeVpcEx", "cvm:DescribeImages", "cvm:ResetInstance", "cvm:DescribeKeyPairs", "tke:DescribeClusters", "tke:AddEx

					istedInstances"
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	"cvm:DescribeSecurityGroups", "cvm:DescribeKeyPairs", "cvm:RunInstances", "vpc:DescribeSubnetEx", "vpc:DescribeVpcEx", "cvm:DescribeImages", "tke:DescribeClusters"
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	"cvm:DescribeInstances", "tke:DescribeClusters", "tke:DescribeClusterInstances"
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	"cvm:TerminateInstances", "tke:DescribeClusters", "tke:DeleteClusterInstances"

				• 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：2023-05-17 15:40:19

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. 在访问管理控制台的 策略 页面，单击左上角的**新建自定义策略**。
2. 在弹出的选择创建方式窗口中，单击**按标签授权**，进入按标签授权页面。
3. 在“可视化策略生成器”中添加服务与操作栏，补充以下信息，编辑一个授权声明。
   - 服务（必选）：选择容器服务 (tke)。
   - 操作（必选）：选择您要授权的操作。
4. 在选择标签栏，选择需要授权的标签信息，可添加多个标签。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**，进入关联用户/用户组/角色页面。在关联用户/用户组/角色页面补充策略名称和描述信息。策略名称由控制台自动生成，默认为 "policygen" ，后缀数字根据创建日期生成。您可进行自定义。
6. 对关联用户/用户组/角色快速授权。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。
   - **将此权限授权给用户**：按需勾选需授权的子账号。
   - **将此权限授权给用户组**：按需勾选需授权的子账号所在的用户组。
   - **将此权限授权给角色**：按需勾选需授权的子账号所在的角色。
7. 单击**完成**。

配置子账号对单个 TKE 集群的管理权限

最近更新时间：2025-09-08 18:09:42

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 访问管理控制台，在左侧导航栏中选择 策略。
2. 在策略页面，单击**新建自定义策略**，选择 “按策略语法创建” 方式。
3. 选择 “空白模板” 类型，单击**下一步**。
4. 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"
        }
    ]
}
```

5. 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。
   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。

6. 单击**完成**，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 访问管理控制台，在左侧导航栏中选择 策略。
2. 在策略页面，单击**新建自定义策略**，选择 “按策略语法创建” 方式。
3. 选择 “空白模板” 类型，单击**下一步**。
4. 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": "*"
        }
    ]
}
```

5. 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。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` 。
6. 单击**完成**，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：2024-10-25 17:53:41

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

3. 在“关联用户/用户组/角色”弹窗中，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**页面，单击 **QcloudCCRFullAccess** 策略行的**关联用户/用户组/角色**。
5. 在“关联用户/用户组/角色”弹窗中，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。

配置只读权限

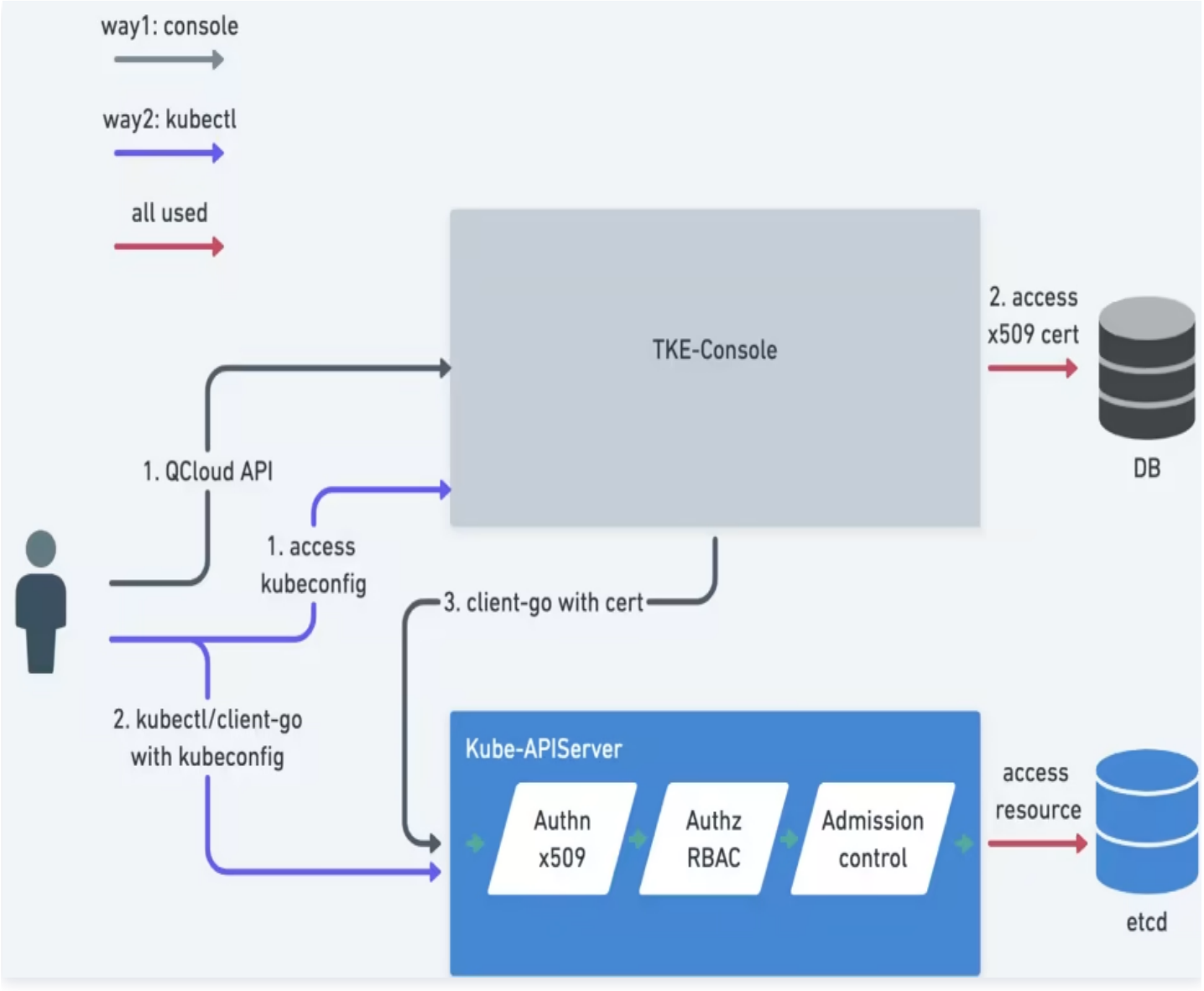
1. 登录访问管理控制台，选择左侧导航栏中的 策略 。
2. 在**策略**页面，选择 **QcloudTKEReadOnlyAccess** 策略行的**关联用户/用户组/角色**。
3. 在“关联用户/用户组/角色”弹窗中，勾选需对 TKE 服务拥有只读权限的账号，并单击**确定**，即可完成子账号对 TKE 服务只读权限的配置。
4. 在**策略**页面，单击 **QcloudCCRReadOnlyAccess** 策略行的**关联用户/用户组/角色**。
5. 在“关联用户/用户组/角色”弹窗中，勾选需对镜像仓库拥有只读权限的账号，并单击**确定**，即可完成子账号对镜像仓库只读权限的配置。

TKE Kubernetes 对象级权限控制

概述

最近更新时间：2023-08-29 16:34:01

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 bearer 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验，并且需要与原生 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：2025-09-09 17:58:11

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

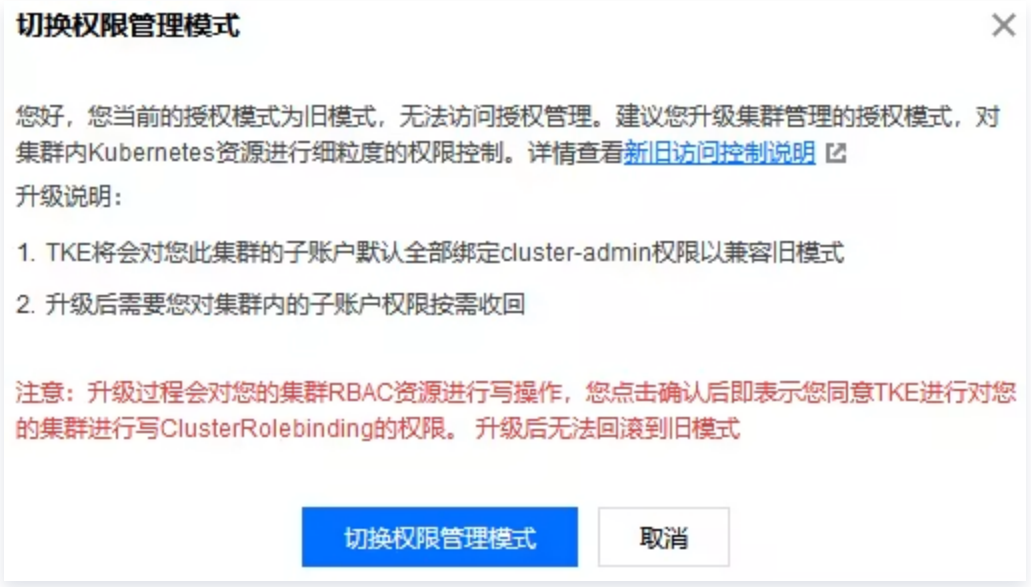
对比项	旧模式	新模式
Kubeconfig	admin token	子账号独立的 x509 证书
控制台访问集群资源	无细粒度权限，子账号具备全读写权限	对接 Kubernetes RBAC 资源控制

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. 在集群页面，选择需升级的集群 ID，进入集群基本信息页。
3. 选择左侧**授权管理**，在 **ClusterRole** 中，单击 **RBAC 策略生成器**。
4. 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。如下图所示：



为确保新旧模式的兼容性，升级过程中会进行如下操作：

4.1 创建默认预设管理员 ClusterRole：`tke:admin` 。

4.2 拉取子账号列表。

4.3 为每个子账号生成可用于 Kubernetes APIServer 认证的 x509 客户端证书。

4.4 为每个子账号都绑定 `tke:admin` 角色（确保和存量功能兼容）。

4.5 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“选择账号”步骤中，勾选需回收权限的子账号并单击**下一步**。
3. 在“集群 RBAC设置” 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”。
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?

不会自动回收，您可进入控制台“授权管理”页面，单击 ClusterRoleBinding，点击右上角“清理失效账户”进行权限回收。

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

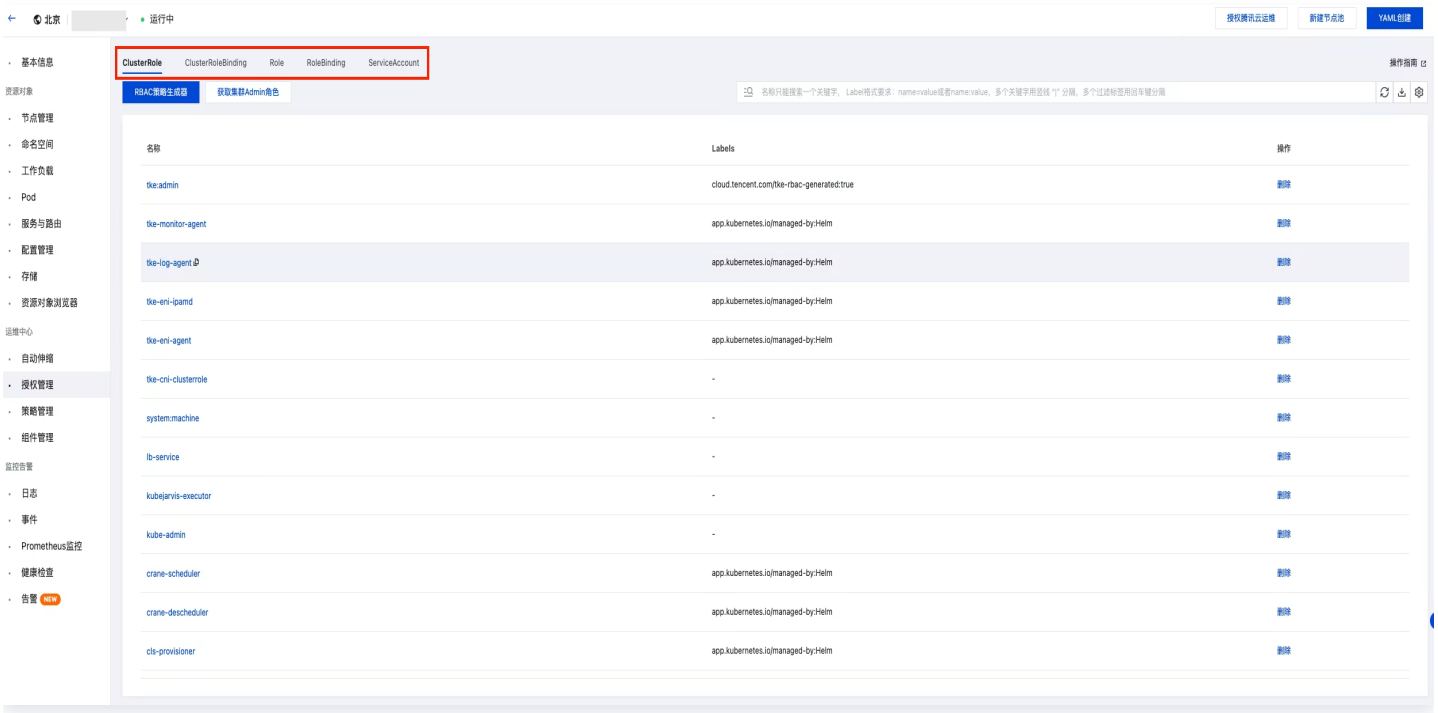
最近更新时间：2025-09-09 17:58:11

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。
  - **只读用户（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。
- 自定义：用户自定义命名空间。

- 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，选择集群 ID，进入集群的基本信息页面。
3. 在**集群 APIServer 信息**模块中查看并下载 Kubeconfig 文件。

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，选择集群 ID，进入集群的基本信息页面。
2. 选择左侧**授权管理** > **ClusterRoleBinding**。
3. 在 **ClusterRoleBinding** 页面，单击 **RBAC 策略生成器**。
4. 在**新建 ClusterRoleBinding** 页面，勾选需授权的子账号，单击**下一步**。
5. 在**集群 RBAC 设置**步骤中，按照以下指引进行权限设置：
   - **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：2025-09-09 17:58:11

本文介绍如何通过编写 Kubernetes 的 ClusterRole 和 Role，授予子账号特定权限，您可根据业务实际需求自定义授权策略。

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: test-role
  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: test-clusterrole
rules:
- apiGroups:
```

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

操作步骤

> **说明：**
> 此处以为子账号绑定自定义 ClusterRole 为例，与绑定 Role 的操作基本一致，请按实际需求进行操作。

1. 登录容器服务控制台，选择左侧导航栏中的 集群 。
2. 在集群列表中，单击目标集群 ID，进入集群详情页。
3. 选择左侧菜单栏中的**授权管理**，在 **ClusterRole** 页面，单击右上角的 **YAML 创建**。
4. 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。
5. 该步骤以 ClusterRole（集群维度）YAML 为例，创建完成后，可在 **ClusterRole** 页面中查看自定义权限“test-clusterrole”。
6. 在 **ClusterRoleBinding** 页面，单击 **RBAC 策略生成器**。
7. 在**新建授权管理**页面勾选需授权的子账号，单击**下一步**。
8. 进入**集群 RBAC** 页面，按照以下指引进行权限设置。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 “test-clusterrole” 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：2025-09-09 17:58:11

访问凭证功能

腾讯云容器服务 TKE 基于 x509 证书认证，实现如下功能：

- 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，将获得子账号独有的 x509 客户端证书，该证书由每个集群的自签名 CA 签发。
- 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. 在集群列表中，选择目标集群 ID。
3. 在集群**基本信息**页面，选择 **API Server 信息**页签，找到 Kubeconfig 权限管理，单击**配置**。
4. 在 **Kubeconfig 权限管理**中，按需勾选认证账号并单击**更新**即可。

控制平面安全
使用腾讯云密钥管理系统 KMS 进行 ETCD 数据加密

最近更新时间：2024-12-02 09:56:22

操作场景

在腾讯云 TKE 独立集群和托管集群中，使用密钥管理系统（Key Management Service，KMS）实现 Kubernetes 数据源加密，并提供丰富的密钥管理功能，针对 Kubernetes 集群中 Secret 提供强大的加密/解密能力。本文主要介绍如何通过 KMS 对 Kubernetes 集群进行数据加密。

基本概念

密钥管理系统 KMS

密钥管理系统（Key Management Service，KMS）是一款安全管理类服务，它使用经过第三方认证的硬件安全模块 HSM（Hardware Security Module）来生成和保护密钥。KMS 可以帮助用户轻松创建和管理密钥，满足用户多应用多业务的密钥管理需求，同时符合监管和合规要求。

数据加密

在 Kubernetes 中，可以使用 Secrets 对象来存储集群内部使用的各类敏感数据，例如数据库用户名、密码、证书、OAuth Token、SSH KEY 等，从而使得敏感信息和普通配置文件有效解耦。默认情况下，Secrets 存储在 etcd 中。
在腾讯云 TKE 标准集群的独立集群和托管集群中，您可以使用在 KMS 中创建的密钥来加密 Kubernetes Secrets 数据。KMS 加密过程基于 Kubernetes 提供的 KMS Encryption Provider 机制，使用信封加密的方式对存储在 etcd 中的 Kubernetes Secrets 数据进行自动加密和解密。Kubernetes Secrets 密钥加密和解密的过程如下：

- 当一个业务密钥需要通过 Kubernetes Secrets API 存储时，数据会首先被 API Server 生成的一个随机的数据加密密钥加密。然后，该数据密钥会被指定的 KMS 密钥加密为一个密文密钥，并存储在 etcd 中。
- 解密 Kubernetes Secrets 密钥时，系统会首先调用 KMS 的解密 OpenAPI 进行密文密钥的解密。然后，使用解密后的明文密钥对 Secrets 数据进行解密，并最终返回给用户。

前提条件

在使用腾讯云 KMS 加密 Kubernetes Secret 之前，请确保您已创建符合以下条件的容器服务独立集群或托管集群：

- Kubernetes 版本为1.18.0及以上。
- Etcd 版本为3.0及以上。

> **说明：**
> - Kubernetes 版本，您可以前往容器服务控制台 集群管理 页面，选择集群并查看**集群基本信息**。
> - Etcd 版本，需通过 Kubectl 连接 Kubernetes 集群进行查看。

使用限制及注意事项

- 使用腾讯云 KMS 加密 Kubernetes Secret 会产生计费。KMS 对 API 调用（以万次调用为单位）和用户上传密钥的托管会收取一定费用，关于 KMS 服务计费的详细说明，请参见 KMS 计费说明 。
- 开启数据加密功能后，请勿通过 KMS 的 OpenAPI 或控制台禁用、删除或计划删除集群数据加解密时选择的密钥，否则会使集群 API Server 不可用，导致 Secret 和 ServiceAccount 等对象无法正常获取，影响业务应用的正常运行。

操作步骤

创建集群时开启数据加密

1. 登录 容器服务控制台 ，单击左侧导航栏中的**集群**。
2. 在**集群管理**页面，单击集群列表上方的**新建**。
3. 选择**标准集群**，单击**创建**。
4. 在**创建集群**页面，单击展开**高级设置**，单击 开启**数据加密**。
5. 开启**数据加密**后，选择地域和 KMS 密钥。如下图所示：

   如果您尚未创建 KMS 密钥，请单击**新建 KMS 密钥**，前往 密钥管理系统（合规） 控制台创建密钥。具体操作请参见 创建密钥 。
6. 创建集群的其他配置项详情请参见 通过控制台创建集群 。配置结束后，单击**完成**。
7. 创建完成的集群将出现在 集群列表 中。您可单击集群 ID 进入集群详情页面，在集群**基本信息**中查看数据加密功能开启状态。

在已创建集群中开启数据加密

> **说明：**
> 如果您需要开启数据加密功能，请确保您当前登录的账号具有 CAM 权限，并且在该集群中具有 RBAC 的管理员或运维人员权限。更多信息请参见 TKE Kubernetes 对象级权限控制 。
> 如果您需要授权 TKE_QCSRole 角色，请确保您使用的是腾讯云账号（主账号）或拥有 CAM 管理权限的用户或角色。有关服务授权相关角色权限的说明，请参见 服务授权相关角色权限说明 。

1. 登录 容器服务控制台 ，单击左侧导航栏中的**集群**。
2. 在**集群**页面，选择需开启数据加密的集群 ID，进入集群详情页。
3. 在集群**基本信息**中，单击**数据加密**右侧的，开启数据加密。如下图所示：

4. 在 **ETCD 数据加密**中，选择地域和已有的 KMS 密钥，单击**提交**。如下图所示：

关闭数据加密

如果您不再需要使用数据加密功能，可在容器服务控制台关闭该功能。

1. 登录 容器服务控制台 ，单击左侧导航栏中的**集群**。
2. 在**集群管理**页面，选择需关闭数据加密的集群 ID，进入集群详情页。

3. 在集群**基本信息**中，单击**数据加密**右侧的，关闭数据加密。

4. 在 ETCD 数据加密确认窗口中，确认是否关闭，单击**提交**。如下图所示：

应用安全
策略管理

最近更新时间：2025-09-28 10:02:12

简介

原生 Kubernetes 存在级联删除机制，删除一个资源时会自动删除与之相关的其他资源，例如删除 Namespace 时会自动删除 Namespace 下所有的 Pod、Service、ConfigMap 等关联资源，可能导致业务故障。
K8S 自身的脆弱性会导致在生产环境存在稳定性和安全的风险，例如用户配置的镜像拉取来源没有限制，可能导致镜像被篡改；缺少容器级别的安全隔离策略，可能导致容器发生越权等行为。
容器服务（Tencent Kubernetes Engine，TKE）提供策略管理能力，通过系统预置策略或者用户自主开启策略的方式，防止误删除引起业务故障，支持通过对计算资源、网络资源进行策略的加固，提升 TKE 集群的稳定性和安全性。

策略说明

策略分类

- **删除防护**：包含集群删除保护和集群内资源删除保护。在删除 TKE 集群内的各类资源时，如果资源正在使用中，或者存在和其他资源之间的引用关系，则不允许删除。
- **策略管控**：用于约束和规范 K8S 集群内的资源配置。例如：要求 Pod 具有 Readiness 或 Liveness Probe；限制容器镜像来源必须在指定的列表内等。
- **安全加固**：包含 PSP（PodSecurityPolicy）相关策略。TKE 提供基于 gatekeeper 的安全防护能力。例如，禁止创建特权容器，约束 PodSecurityPolicy 中的 hostPath、hostPID 和 hostIPC 字段等。

支持边界

支持1.16及以上 K8S 版本的 TKE 标准集群和 TKE Serverless 集群，暂不支持注册集群和边缘集群。

策略类型

- **基线策略**：TKE 内置的策略，包含保护集群基础设施资源不被误删除等策略。
- **优选策略**：TKE 最佳实践形成的标准和规范，对用户的各项配置进行校验，使得用户请求符合约束。用户可根据实际情况开启策略，并设置策略运行模式。
- **可选策略**：官方 OPA gatekeeper 策略库支持的策略，包含替代 PSP 能力的策略和通用策略。用户可以根据实际情况，自行创建策略实例，具体创建流程请参见 新建策略实例 。

运行模式

- dryrun：不会实际拦截业务请求，请求命中策略后会生成记录，在策略管理页面不展示拦截记录。
- deny：请求命中策略后会被拦截，同时在策略管理页面可以拦截记录的总次数。

策略库

> **说明：**
> 为最大程度防范集群资源误删现象，TKE 策略管理系统计划于2025年6月5日后新建集群针对“存在 pod 的命名空间不允许删除”、“存在 cr 的 crd 不允许删除”、“非封锁状态的 Node 不允许删除”、“CoreDNS 组件删除保护”、“PV 处于绑定状态则不允许删除”开启默认 deny 策略，您可前往**集群详情-策略管理**模块进行查看和修改。

基线策略

策略分类	策略名称	策略描述	拦截对象	运行模式
删除保护	存在节点的集群不允许删除	集群中存在任意节点（普通节点、原生节点、注册节点），需先下线节点后方可删除。	集群	默认 deny

优选策略

策略分类	策略名称	策略描述	拦截对象	运行模式
删除保护	存在 pod 的命名空间不允许删除	命名空间内如果存在 pod，需先清除 pod 后方可删除 namespace。	Namespace	默认 dryrun
删除保护	存在 cr 的 crd 不允许删除	crd 定义的 apiversion 下如果有创建 cr 资源，则清空 cr 后方可删除 crd。	CRD	默认 dryrun
删除保护	非封锁状态的 Node 不允许删除	ready 状态的节点处于非封锁状态时不允许直接删除。	Node	默认不创建策略实例
删除保护	CoreDNS 组件删除保护	禁止删除 CoreDNS 组件的 Service、ConfigMap 和 Deployment。	Deployment、Service、ConfigMap	默认不创建策略实例

删除保护	资源删除保护	存在指定 Label 的资源（Service、Ingress、Deployment、StatefulSet）不允许被删除。	Service、Ingress、Deployment、StatefulSet	默认不创建策略实例
删除保护	PV 处于绑定状态则不允许删除	PersistentVolume 如果处于 Bound 状态，则不允许被删除。	PV	默认不创建策略实例
策略管控	禁止挂载指定的 volume 类型	将可挂载的 volume 类型限制为用户指定的类型。	Pod	默认不创建策略实例
策略管控	禁止镜像拉取策略使用 Always	禁止容器使用 Always 镜像拉取策略，减少对镜像仓库的访问。	Pod	默认不创建策略实例
策略管控	容器镜像来源限制	只允许从指定的镜像仓库拉取镜像。	Pod	默认不创建策略实例
策略管控	禁止未知的 DaemonSet 部署	只允许部署指定的 DaemonSet。	DaemonSet	默认不创建策略实例
策略管控	工作负载镜像版本升级策略管控	限制 Deployment 和 DaemonSet 只能在配置的镜像列表中升级。	Deployment、DaemonSet	默认不创建策略实例
策略管控	ServiceAccount 权限管控	禁止 ServiceAccount 绑定较大权限的 Role 和 ClusterRole，提升集群安全性。	ServiceAccount	默认不创建策略实例
策略管控	不允许 Service 为 ClusterIP 类型	禁止创建 ClusterIP 类型的 Service 或将 Service 由其他类型更新为 ClusterIP 类型。	Service	默认不创建策略实例
策略管控	禁止公网访问	禁止通过创建公网类型的 Service 或 Ingress 的方式将后端服务暴露到公网。	Service、Ingress	默认不创建策略实例

策略管控	弹性网卡资源配置限制	限制跨租户弹性网卡必须配置 Request 资源。	Pod	默认不创建策略实例

可选策略

策略分类	策略名称	策略描述	拦截对象
策略管控	tkeblockvolumemountpath	禁止容器挂载指定的目录。	pods
策略管控	k8sallowedrepos	容器镜像必须以指定字符串列表中的字符串开头。	pods
策略管控	k8spspautomountserviceaccounttokenpod	约束容器不能设置 automountServiceAccountToken 为 true。	pods
策略管控	k8sblockendpointeditdefaultrole	默认情况下，许多 Kubernetes 都预定义了一个名为 system:aggregate-to-edit 的 ClusterRole，k8sblockendpointeditdefaultrole 策略定义禁止该 ClusterRole 对 Endpoints 进行 create、patch 和 update 操作。	clusterroles
策略管控	k8sblockloadbalancer	不允许 Service 为 LoadBalancer 类型。	services
策略管控	k8sblocknodeport	不允许 Service 为 NodePort 类型。	services
策略管控	k8sblockwildcardingress	禁止 Ingress 配置空白或通配符类型的 hostname。	ingresses
策略管控	k8scontainerlimits	限制容器必须设置 CPU 和内存 Limit，并且小于设定的最大值。	pods
策略管控	k8scontainerrequests	限制 CPU 和内存的 Request 必须设置且小于配置的最大值。	pods
策略管控	k8scontainerratios	限制 CPU 和内存的 Request 与 Limit 的最大比率。	pods
策略管控	k8srequiredresources	必须配置内存的 Limit，CPU 和内存的 Request。	pods

策略管控	k8sdisallowanonymous	不允许将白名单以外的 ClusterRole 和 Role 关联到 system:anonymous User 和 system:unauthenticated Group。	rolebindings clusterrolebindings
策略管控	k8sdisallowedtags	约束容器镜像 tag。	pods
策略管控	k8sexternalips	限制服务 externalIP 仅为允许的 IP 地址列表。	services
策略管控	k8simagedigests	容器镜像必须包含 digest。	pods
策略管控	noupdateserviceaccount	拒绝白名单外的资源更新 ServiceAccount。	replicationcontrollers replicasets deployments statefulsets daemonsets cronjobs
策略管控	k8sreplicalimits	要求具有 “spec.replicas” 字段的对象（Deployments、ReplicaSets等）在定义的范围内。	deployments
策略管控	k8srequiredannotations	要求资源包含指定的 annotations，其值与提供的正则表达式匹配。	services
策略管控	k8srequiredlabels	要求资源包含指定的标签，其值与提供的正则表达式匹配。	namespaces
策略管控	k8srequiredprobes	要求 Pod 具有 Readiness 或 Liveness Probe。	pods
安全加固	k8spspallowprivilegeescalationcontainer	约束 PodSecurityPolicy 中的 “allowPrivilegeEscalation” 字段为 false。	pods

安全加固	k8spspapparmor	约束 AppArmor 字段列表。	pods
安全加固	k8spspcapabilities	限制 PodSecurityPolicy 中的“allowedCapabilities”和“requiredDropCapabilities”字段。	pods
安全加固	k8spspflexvolumes	约束 PodSecurityPolicy 中的 allowedFlexVolumes 字段类型。	pods
安全加固	k8spspforbiddensysctls	约束 PodSecurityPolicy 中的“sysctls”字段不能使用的 name。	pods
安全加固	k8spspfsgroup	控制 PodSecurityPolicy 中的“fsGroup”字段在限制范围内。	pods
安全加固	k8spsphostfilesystem	约束 PodSecurityPolicy 中的“hostPath”字段的参数。	pods
安全加固	k8spsphostnamespace	限制 PodSecurityPolicy 中的“hostPID”和“hostIPC”字段。	pods
安全加固	k8spsphostnetworkingports	约束 PodSecurityPolicy 中的“hostNetwork”和“hostPorts”字段。	pods
安全加固	k8spspprivilegedcontainer	禁止 PodSecurityPolicy 中的“privileged”字段为 true。	pods
安全加固	k8spspprocmount	约束 PodSecurityPolicy 中的“allowedProcMountTypes”字段。	pods
安全加固	k8spspreadonlyrootfilesystem	约束 PodSecurityPolicy 中的“readOnlyRootFilesystem”字段。	pods
安全加固	k8spspseccomp	约束 PodSecurityPolicy 上的“seccomp.security.alpha.kubernetes.io/allowedProfileNames”注解。	pods
安全加固	k8spspselinuxv2	约束 Pod 定义 SELinux 配置的允许列表。	pods
安全加固	k8spspallowedusers	约束 PodSecurityPolicy 中的 runAsUser、runAsGroup、supplementalGroups 和 fsGroup 字段。	pods
安全加	k8spspvolumetypes	约束 PodSecurityPolicy 中的	pods

固		“volumes” 字段类型。	

操作说明

开启/关闭策略

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，选择目标集群 ID，进入集群的基本信息页面。
3. 在左侧导航中选择**策略管理**，进入策略管理页面选择策略，单击**开启/关闭**。关闭策略需要二次确认，开启则不需要。

验证策略效果

以集群删除策略为例，创建 TKE 标准集群，验证集群在存在节点情况下删除请求是否会被拦截。

1. 创建有节点的 TKE 标准集群，详细步骤请参见 创建集群 。
2. 发起删除集群请求。

通过控制台删除

1. 删除集群，详细步骤请参见 删除集群 。
2. 窗口提示需要先清空节点后，方可继续删除集群。如下图所示：

调用云 API 删除

1. 调用云 API 删除，调用方式请参见 API 文档 删除集群 。
2. 删除集群接口调用失败，错误信息返回中包含集群中存在的节点清单。如下图所示：

```
{
  "Response": {
    "Error": {
      "Code": "FailedOperation.ClusterForbiddenToDelete",
      "Message": "cluster cls- still has nodes, please delete the node and try again, regularNodeNames:
[ins- ], nativeNodeNames: [], superNodeNames: [], externalNodeNames: [], otherNodeNames: []"
    },
    "RequestId": "f1d1cc40- -84d5684688ab"
  }
}
```


3. 在**策略管理**页面，单击关联事件的数字，查看拦截事件信息。如下图所示：

新建策略实例

以禁止创建特权容器为例，演示如何新建策略实例。

- 策略名称：k8spspprivilegedcontainer
- 策略类型：K8sPSPPrivilegedContainer
- 策略描述：禁止 Pod securityContext 中的 privileged 字段为 true。
- 生效资源类型：Pod

需要修改的参数如下：

- namespaces 可选参数：表示策略作用生效的命名空间。
  - 不填该字段或者字段取值为空时，表示所有命名空间都生效。
  - 支持前缀匹配，例如 namespaces: ["kube-*"] 匹配 "kube-system" 和 "kube-public"。
- excludedNamespaces 可选参数：表示策略豁免生效的命名空间，在该列表中的命名空间不会生效此条策略。
  - 不填该字段或者字段取值为空时，表示没有豁免的命名空间。
  - 支持前缀匹配，例如 excludedNamespaces: ["kube-*"] 匹配 "kube-system" 和 "kube-public"。
- exemptInitContainers 自定义参数：布尔值。含义：是否允许 initContainer 使用特权容器。

- 部分业务的 initContainer 以特权容器的方式运行，执行类似 iptables 规则下发等操作。
- 创建策略实例时，默认会允许 initContainer 使用特权容器。

策略实例 YAML：

```
apiVersion: constraints.gatekeeper.sh/v1beta1
kind: K8sPSPPrivilegedContainer
metadata:
  name: psp-privileged-container
spec:
  match:
    kinds:
      - apiGroups: [""]
        kinds: ["Pod"]
    namespaces: []
    excludedNamespaces: ["kube-system"]
  parameters:
    exemptInitContainers: true
```

创建命令：

```
kubectl apply -f K8sPSPPrivilegedContainer.yaml
```

测试策略是否生效的 Pod YAML 如下。直接执行 `kubectl apply -f pod.yaml` ，若被策略拦截则说明已生效。

```
apiVersion: v1
kind: Pod
metadata:
  name: privileged-pod
spec:
  containers:
  - name: privileged-container
    image: nginx
    securityContext:
      privileged: true
  initContainers:
  - name: privileged-init-container
    image: busybox
    command: ['sh', '-c', 'echo Hello, Kubernetes!']
    securityContext:
```

```
      privileged: true
```

创建一个特权容器的 Pod，预期输出示例：

```
Error from server (Forbidden): error when creating "pod.yaml": admission
webhook "validation.gatekeeper.sh" denied the request: [psp-privileged-
container] Privileged container is not allowed: privileged-container,
securityContext: {"privileged": true}, Pod name: privileged-pod
```

备份中心

概述

最近更新时间：2024-06-27 14:09:11

腾讯云容器服务 TKE 备份中心为容器化应用的备份、恢复与迁移提供了一体化解决方案，目前已支持 TKE 标准集群资源对象的备份与恢复。本文主要介绍备份中心的使用场景及核心组件。

使用场景

- **备份恢复**：当集群或命名空间下的所有资源被误删除时，可以通过备份数据快速恢复业务。
- **业务合规**：配合安全部门定期拉取备份数据进行业务审计。

核心组件

组件名称	描述
tke-backup	备份组件，部署在用户集群中，基于开源工具 Velero 支持通过 CRD 方式定时备份和还原 Kubernetes 集群资源。

说明：

1. 跨集群备份恢复能力要求组件版本在 1.1.0及以上，建议您及时更新。
2. 当前仅支持 kubernetes 资源对象的恢复，不支持云硬盘 CBS、负载均衡 CLB 等云资源的恢复。

部署在集群内的 Kubernetes 对象

kubernetes 对象名称	类型	资源量	Namespaces
tke-backup	Deployment	至少需要0.1核 CPU 和256MB内存	tke-backup
tke-backup	Service	-	tke-backup
tke-backup	backupstoragelocation	-	-
tke-backup	backup	-	-
tke-backup	restores	-	-

资源类型

TKE 自定义的备份相关 CRD 资源，描述如下：

资源名称	描述
Backup	指定资源对象的备份策略。创建 Backup 资源会启动备份过程，删除 Backup 资源不会关联删除已存储在备份仓库 COS 的底层数据。
BackupSchedule	指定资源对象在特定时间点的备份策略，负责定时产生 Backup 资源对象。
Restore	将备份信息恢复至 TKE 目标集群中。创建 Restore 资源会启动恢复过程。删除 Restore 资源不会产生其他影响，只会从恢复列表中移除恢复操作的记录。

操作步骤

1. 登录 容器服务控制台，创建备份仓库，详情请参见 创建备份仓库。
2. 为目标集群创建备份或定时备份策略，详情请参见 备份管理。
3. 根据备份数据恢复集群中的指定资源对象，详情请参见 恢复管理。

备份仓库

最近更新时间：2024-06-27 14:09:11

操作场景

腾讯云容器服务 TKE 备份中心为业务应用的备份和恢复提供了产品化解决方案，本文介绍如何创建备份仓库来存储备份数据。

前提条件

1. 登录 对象存储控制台 新建 COS 存储桶作为备份仓库的底层存储。容器服务角色采用最小化授权方式访问您的 COS 存储，存储桶的命名必须以 “**tke-backup**” 开头。具体操作步骤请参见 创建存储桶 。
2. 完成对 COS 对象读写操作的授权。在使用备份仓库之前，在控制台根据提示将策略 QcloudAccessForTKERoleInCOSObject 授权给角色 TKE_QCSRole。

> **说明：**
> 对象存储 COS 计费方式详情请参见 对象存储计费概述 。

操作步骤

1. 登录 容器服务控制台 ，在左侧导航栏中选择**运维中心 > 备份中心**。
2. 进入备份仓库页面，单击**创建**。
3. 在创建备份仓库页面，填写仓库基本信息，如下图所示：

- **仓库名称**：自定义备份仓库的名称
- **COS 地域**：选择对象存储所在地域
- **存储桶列表**：存储桶命名需要以 “tke-backup” 开头， 如当前 COS 存储桶不适合，可前往 对象存储控制台 新建。

4. 单击**确定**完成创建。

说明：

- 不同地域的 TKE 集群可使用相同的备份仓库存储数据，但国内和国外地域之间的数据不可同时存储在一个仓库中。
- 删除仓库时，关联了本仓库的备份对象将无法正常执行恢复操作，请谨慎处理。
- 删除仓库时，底层存储资源不会被删除，您可前往 对象存储控制台 进一步操作。

备份管理

最近更新时间：2025-04-17 17:36:02

操作场景

腾讯云容器服务 TKE 备份中心为业务应用的备份和恢复提供了产品化解决方案，本文介绍如何针对目标集群创建备份任务和定时备份策略。

前提条件

> **说明：**
> 若您之前在集群中已安装社区开源备份组件如 velero，需要提前卸载，否则会影响 TKE 备份组件的正常安装。

在目标集群中安装 **tke-backup** 备份组件。您可以前往集群中的**组件管理**模块进行操作，具体操作步骤请参见 组件安装 。

操作步骤

创建备份

1. 登录 容器服务控制台 。
2. 在左侧导航中选择**运维中心 > 备份中心**，在**备份管理**中单击**创建备份**。
3. 在**创建备份任务**页面，依次填写备份信息，如下图所示：

相关字段介绍如下：

- 备份名称：请遵循控制台的提示校验规则填写备份任务的名称。
- 备份类型：
  - 立即备份：根据您筛选的业务即时创建 Backup 备份任务并执行备份操作。

- 定时备份：创建资源对象 BackupSchedule，该对象会根据您设置的规则定时创建 Backup 备份任务。
- 备份仓库：选择已经创建好的备份仓库。
- 命名空间：选择需要备份的命名空间，代表备份您选择的命名空间下的所有应用。
- 备份有效期：备份数据的保留时长，过期后数据将被删除且无法恢复。
- 高级设置：
  - 排除命名空间：若您在**命名空间**选项处勾选了“全选”，可通过该字段快速过滤不需要备份的命名空间。
  - 备份对象：仅备份您指定的 Kubernetes 资源对象，“全选”则代表备份筛选命名空间下的所有资源对象。
  - 排除备份对象：若您在**备份对象**选项处勾选了“全选”，可通过该字段快速过滤不需要备份的资源对象。
  - 指定标签：根据您指定的标签进一步筛选资源对象，仅备份目标命名空间下带有该标签的应用。

4. 单击**确定**完成创建。

> **说明：**
> 目前支持的 Kubernetes 资源对象的备份范围包括 Deployment、StatefulSet、DaemonSet、Job、CronJob、ConfigMap 和 Secret 等。

查看备份

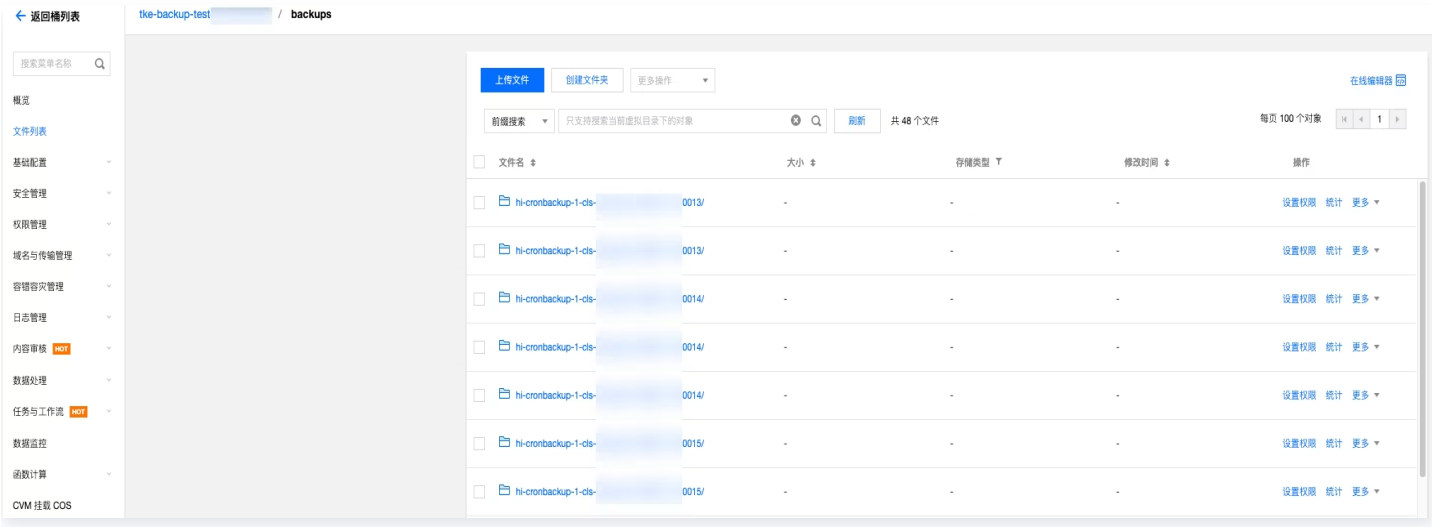
您可在**备份管理**页面查看**备份列表**和**定时备份**列表。

检查备份状态

状态	描述
初始化中	创建 Backup 资源对象。
执行中	执行备份任务。
完成	备份操作已完成。
部分失败	备份出现部分资源对象成功、部分失败情况，可在控制台通过查看 YAML 中的 status 字段获取成功的对象数量，失败的原因等。
失败	备份执行失败，可在控制台或通过 YAML 的 status 字段查看失败原因。

查看备份内容

您可前往 对象存储控制台 查看存储的备份数据，每个备份任务对应在 COS 的命名方式为 “备份名称-集群名称-年月日时分秒”。



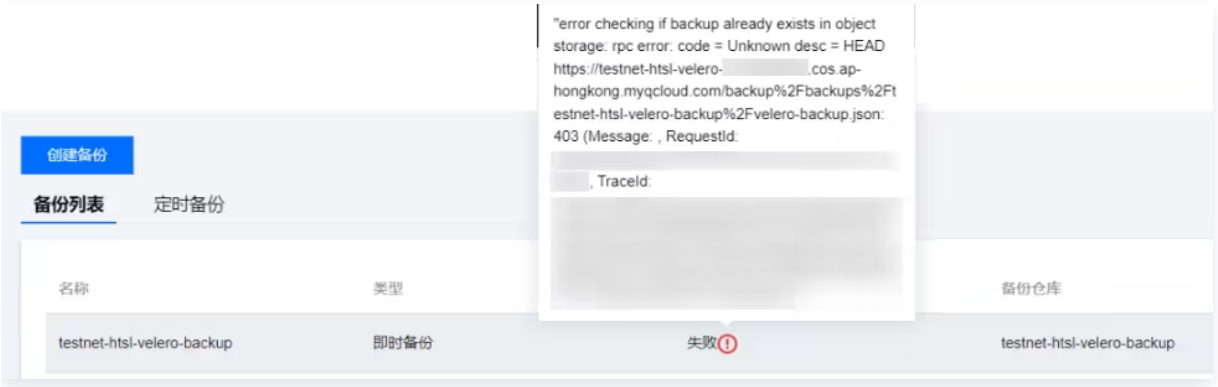
常见问题

删除备份资源时，对象存储中的数据是否会一起删除?

不会，删除备份资源时您存储在 COS 的数据会被保留。如果需要删除这些数据，您需要前往对象存储控制台进行手动操作。

创建“立即备份”任务失败，提示 “error checking if backup already exists in object storage: xxx”？

这可能是因为在历史上，您创建过一个同名的备份任务，但该任务删除后，存储在 COS 的数据还在，导致备份失败。您可以尝试修改备份名称或删除同名的备份数据来解决这个问题。



恢复管理

最近更新时间：2025-04-11 09:18:22

操作场景

腾讯云容器服务 TKE 备份中心为业务应用的备份和恢复提供了产品化解决方案，本文介绍如何针对已经创建了备份任务的目标集群进行恢复操作。

前提条件

源集群中已经创建了备份任务。

> **说明：**
> 假设您计划将A集群备份的业务恢复至B集群，为方便理解，此时A集群称为源集群，B集群称为恢复集群。

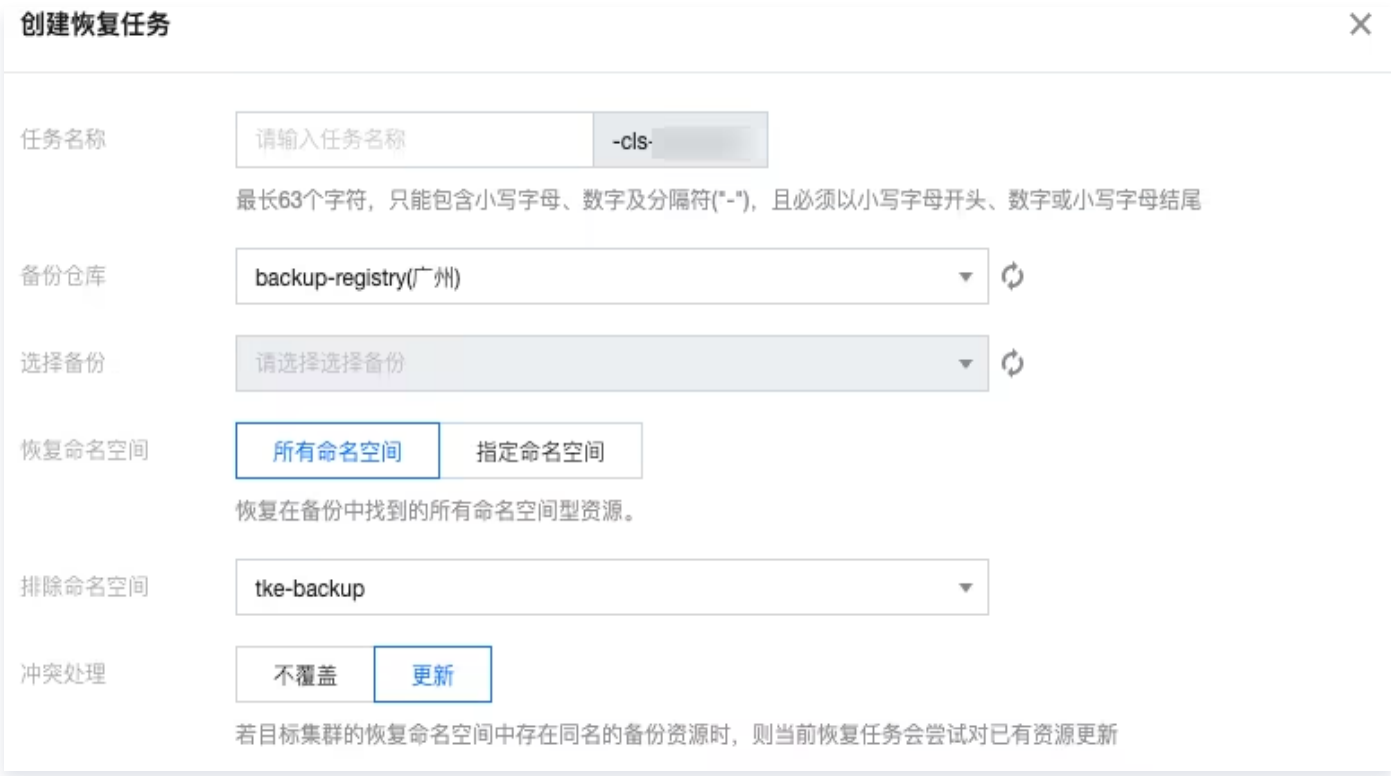
操作限制

1. 跨集群备份恢复能力要求目标集群中安装的组件版本在 1.1.0及以上，建议您及时更新。
2. 当前仅支持 kubernetes 资源对象的恢复，不支持云硬盘 CBS、负载均衡 CLB 等云资源的恢复。

操作步骤

创建恢复任务

1. 登录 容器服务控制台 。
2. 在左侧导航中选择**运维中心 > 备份中心**，在**恢复管理**中单击**创建恢复任务**。
3. 在**创建恢复任务**页面，依次填写恢复信息，如下图所示：



相关字段介绍如下：

- 任务名称：请遵循控制台的提示校验规则填写恢复任务的名称。
- 备份仓库：选择已经创建好的备份仓库，需要根据仓库过滤出源集群的备份数据。
- 选择备份：选择待恢复的备份数据，**支持选择当前或其他集群（即源集群）创建的备份任务**作为恢复依据。
- 恢复命名空间：用来恢复在源集群备份数据命名空间下找到的相关应用。
  - 所有命名空间：恢复在备份数据中找到的所有命名空间下的资源对象，您可通过“排除”选项快速过滤。
  - 指定命名空间：从备份数据中选择特定命名空间恢复资源。
- 冲突处理：
  - 不覆盖（推荐）：若恢复集群的命名空间中存在同名的备份资源时，则当前恢复任务不会覆盖已有资源。
  - 更新：若恢复集群的命名空间中存在同名的备份资源时，则当前恢复任务会尝试对已有资源更新覆盖。

4. 单击**确定**，创建恢复任务资源 Restore 并执行恢复操作。

> **说明：**
> - 恢复任务无法保证100%成功。
> - 删除备份任务不会产生其他影响，也不会删除 COS 中存储的备份数据，只会从恢复列表中移除恢复操作的记录。

查看恢复状态

状态	描述
初始化中	创建 Restore 资源对象。
执行中	执行恢复任务。
完成	恢复操作已完成。
部分失败	恢复出现部分资源对象成功、部分失败情况，可在控制台通过查看 YAML 中的 status 字段获取成功的对象数量，失败的原因等。
失败	恢复执行失败，可在控制台或通过 YAML 的 status 字段查看失败原因。

跨集群备份恢复说明

1. 恢复操作时，源集群和恢复集群的网络模式（如 VPC-CNI、GR）需保持一致。
2. 暂不支持恢复集群中的云存储资源，如 CBS/CFS/COS，涉及存储相关的 Pod 可能会由于找不到存储资源而 Pending。
3. 如果将业务从独立集群恢复至托管集群，可能会由于部分系统组件部署模式的差异而造成恢复任务失败。为提高恢复成功率，建议您在恢复时优先选择“指定命名空间”进行少量多次操作。
4. kubernetes 不同版本之间会存在不兼容的变更（如参数废弃、apiserver 版本变更），为提高恢复成功率，恢复集群的 Kubernetes 版本与源集群尽量保持相同或相邻大版本，如源集群1.18可恢复至目标集群1.18/1.20。
5. 建议在执行恢复动作前预先检查恢复集群的资源情况，资源不足时可能会造成 Pod Pending。
6. 源集群和目标集群不在相同地域下需确保网络联通性，否则会造成镜像拉取失败造成 Pod Pending。
7. 若您的 Service 资源绑定的 CLB 开启了删除保护（即 CLB 没有随 Service 资源一同被删除），在 Service 资源恢复时可复用原有的 CLB 实现业务恢复。

备份恢复实践

最近更新时间：2025-09-22 17:46:53

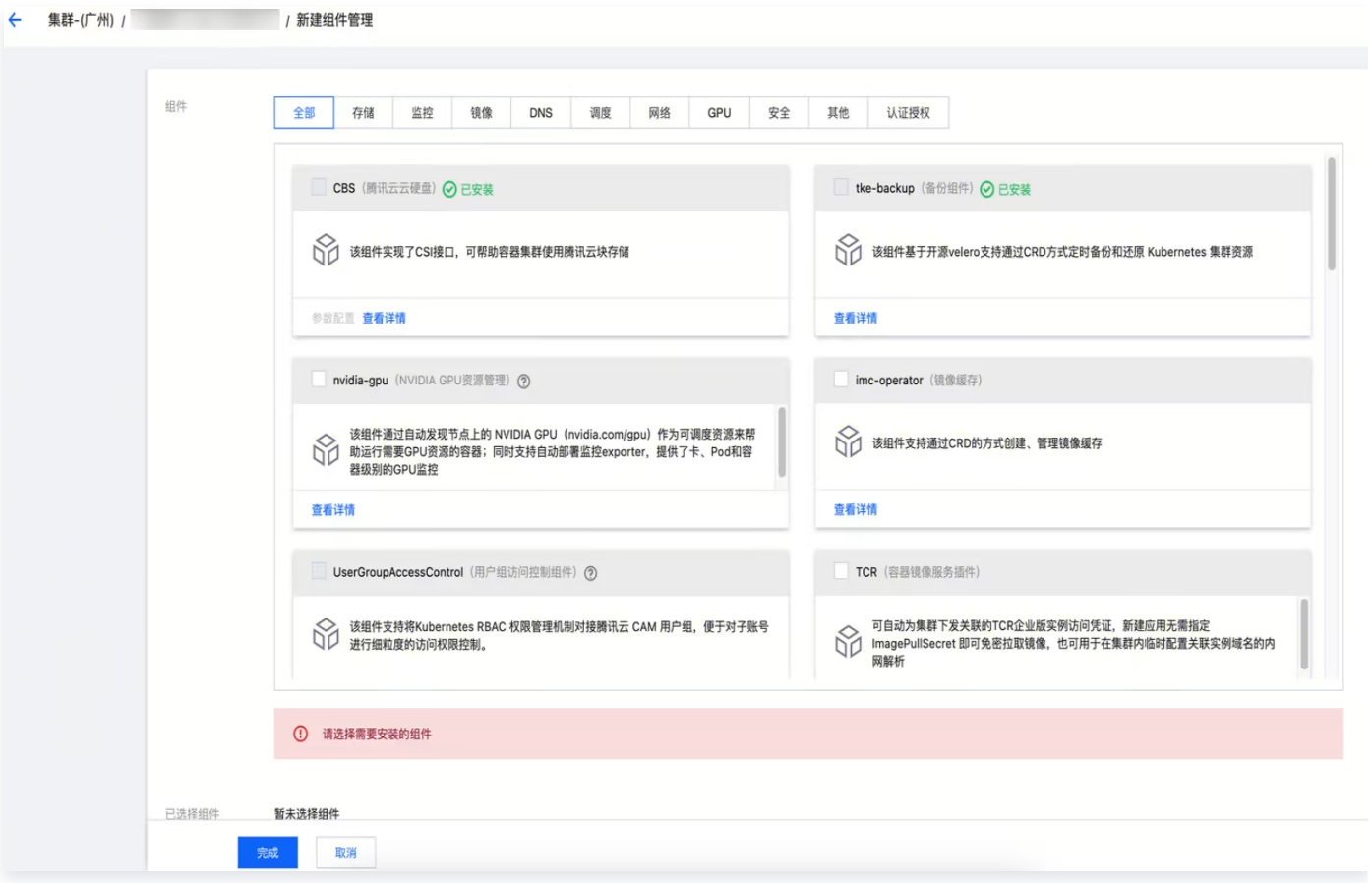
操作场景

本文档以误删除集群中的 “service-controller” 资源为例，介绍备份与恢复操作流程。

操作步骤

1. 开启周期性备份

1. 登录 容器服务控制台 ，在左侧导航栏中选择**集群**。
2. 在集群组件管理中安装 “tke-backup” 组件，并确保组件状态显示为“成功”。组件安装步骤详情请参见 通过组件管理页安装组件 。



3. 在**备份中心**页面，单击**创建**，新建并完成仓库配置，操作详情请参见 创建备份仓库 。
4. 在**备份管理**页面，为集群创建周期性备份，操作详情请参见 创建备份 。
5. 在定时备份中确认备份情况。
6. 在备份列表中确认状态是否正常。

2. 模拟误删除

模拟误删集群 kube-system 命名空间下的 service-controller 资源对象，此时集群中新增 service 对象出现异常。

```
[          @VM-46-151-centos ~]$ k delete deploy -n kube-system   service-controller
deployment.apps "service-controller" deleted
[          @VM-46-151-centos ~]$
```

3. 完成恢复流程

1. 在**备份中心 > 恢复管理**页面，选择集群并在当前集群下创建恢复任务，操作详情请参见 创建恢复任务 。
   - 由于 service-controller 部署在 kube-system 命名空间下，我们选择了对应的命名空间进行恢复。
   - 在冲突处理中，我们选择“不覆盖”，这意味着除 service-controller 之外，其他在 kube-system 命名空间下运行的同名资源对象在本次恢复中不会被备份数据所更新。
2. 在**备份中心 > 恢复管理**页面，确认恢复任务的执行状态。
3. 后台查看 service-controller 对应 Pod 的执行情况是否运转正常，业务是否已经恢复。

```
[          @VM-46-151-centos ~]$ k get po -n kube-system | grep service-controller
service-controller-                    1/1     Running     0          12d
```