容器服务

TKE 注册集群指南

产品文档

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

文档目录

TKE 注册集群指南
注册集群管理
创建注册集群
连接注册集群
解除注册集群
运维指南
日志采集
集群审计

TKE 注册集群指南
注册集群管理
创建注册集群

最近更新时间：2024-05-09 15:46:55

注册集群是腾讯云容器服务一种新的集群类型，可以将用户本地基础设施的 Kubernetes 集群或者其他云厂商的 Kubernetes 集群注册到腾讯云容器服务 TKE 统一管理。本文将介绍如何将第三方的 Kubernetes 集群注册到腾讯云容器服务 TKE。

前提条件

已经开通注册集群的功能。目前注册集群的能力处于免费内测阶段，请 联系我们 进行申请。
支持被注册的 K8s 集群版本范围：1.18.x ~ 1.24.5。超出此范围的 K8s 集群版本未经过验证，不保证支持该版本。

操作步骤

创建 Hub 集群

说明：
注册集群属于 云原生分布式云中心（Tencent Kubernetes Engine Distributed Cloud Center, TDCC） 资源管理能力的重要组成部分，基于开源的 Clusternet 多集群应用治理项目实现。
在进行注册集群操作前，需要先创建 Hub Cluster，后续可通过该托管的 Hub Cluster 集群来管理其他注册进来的 Child Cluster 子集群。
1. 在 腾讯云控制台 中，选择**云产品 > 云原生分布式云中心**，进入云原生分布式云中心控制台，按照界面提示开通云原生分布式云中心服务并为服务授权。（如果您已为该服务授权，请跳过该步骤。）
2. 按照页面提示设置 Hub Cluster 的基本信息：
开通地域：选择 Hub Cluster 的地域，当前仅支持广州、北京和新加坡，未来会支持更多地域。
可用区：选择 Hub Cluster 的可用区。
集群网络：选择一个子网。 访问 Hub Cluster 的 kube-apiserver 需要使用弹性网卡，因此需要您提供 VPC 子网。TKE 会自动在选定的子网内创建代理弹性网卡。
注意：
创建 Hub Cluster 后接入地域及可用区无法更改。

创建注册集群

1. 登录 容器服务控制台，选择左侧导航栏中的**注册集群**。
2. 在注册集群管理的页面中，单击集群列表上方的**注册已有集群**。
3. 设置注册集群的基本信息：

集群名称：创建的注册集群名称，不超过60个字符。

接入地域：选择注册集群的接入地域，目前支持广州、北京和新加坡，未来会支持更多地域。

说明：

接入地域与待注册集群的真实运行地域无关，它的含义是：管理此注册集群的Hub Cluster所在地域。

腾讯云标签：为集群绑定标签后可实现资源的分类管理。详情请参见 通过标签查询资源。

集群描述：填写集群的相关信息，该信息将显示在**集群信息**页面。

4. 单击**完成**，即可创建一个注册集群。您可以在注册集群列表，看到您创建的集群，集群的状态为**等待注册**，如下图：

说明：

您可以在集群列表，**查看注册命令**或者**删除**等待注册的集群。

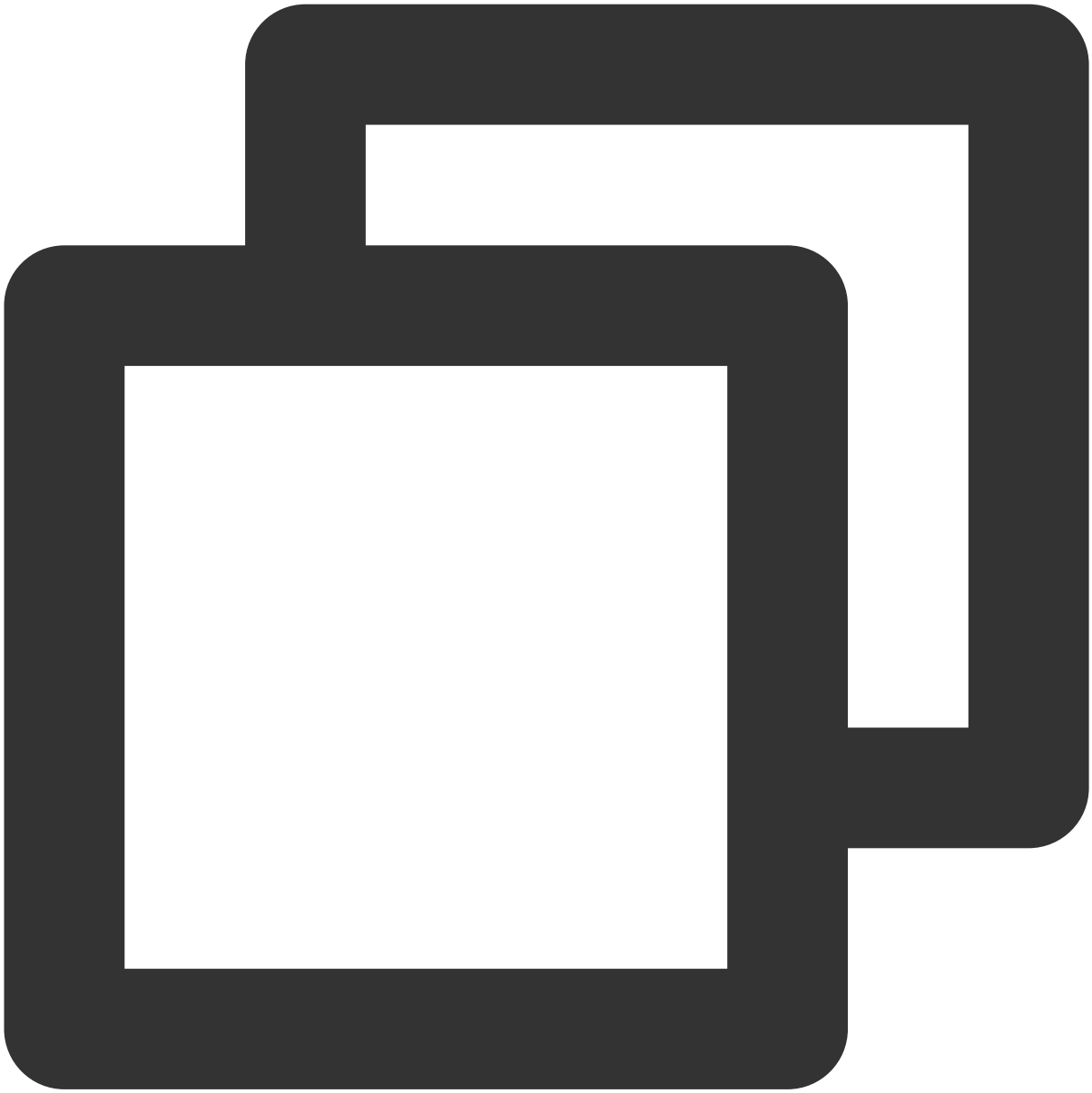
执行注册命令

1. 在集群管理的页面，找到创建的注册集群，选择注册集群所在行右侧的**查看注册命令**，查看对应的注册命令。
2. 用户可以根据需要选择**外网**或者**内网**的方式注册集群，复制或者下载注册的命令，在第三方的集群中执行 kubectl 命令，完成注册的操作。

注意：

注册命令的有效期为24小时，请在有效期内完成注册。如果超过有效期，则需要在页面上重新生成注册命令。

3. 执行以下命令查看代理运行状态，示例如下：



```
# kubectl get pod -n clusternet-system
NAME                                  READY   STATUS    RESTARTS   AGE
clusternet-agent-78444974d7-f6fsc     1/1     Running   0          7m32s
clusternet-agent-78444974d7-qjp2q     1/1     Running   0          7m32s
clusternet-agent-78444974d7-r575w     1/1     Running   0          7m32s
```

注册成功后，注册集群的状态变为**运行中**，即表示集群注册成功。

连接注册集群

最近更新时间：2024-05-09 15:47:22

操作场景

本文档介绍如何通过 Kubernetes 命令行工具 Kubectl 从本地客户端机器连接到注册集群。

前提条件

已安装 curl 软件。

请根据操作系统的类型，选择获取 Kubectl 工具的方式：

注意：

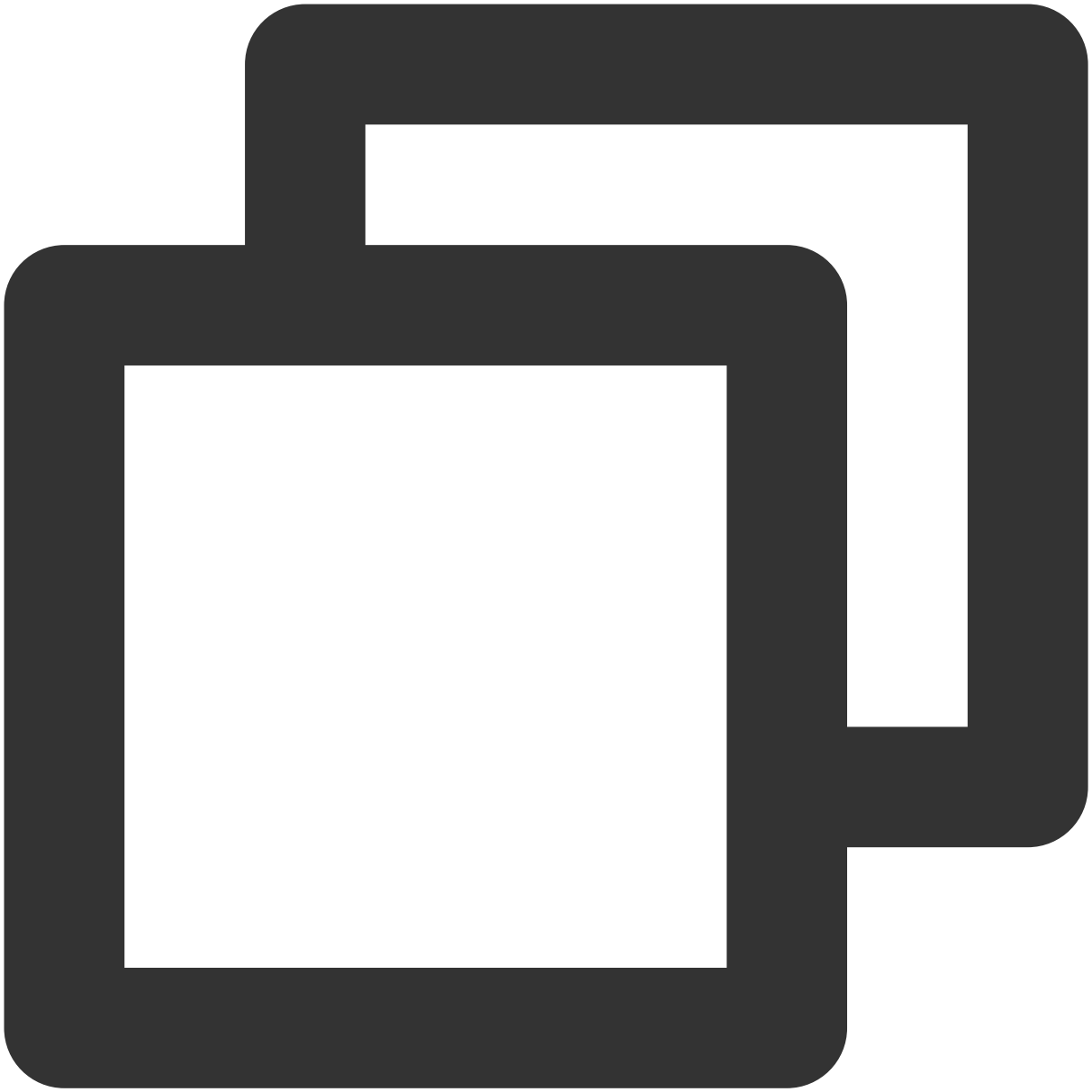
请对应您实际使用版本，将命令行中的 `v1.8.13` 替换成业务所需的 Kubectl 版本。

MacOS 系统

Linux 系统

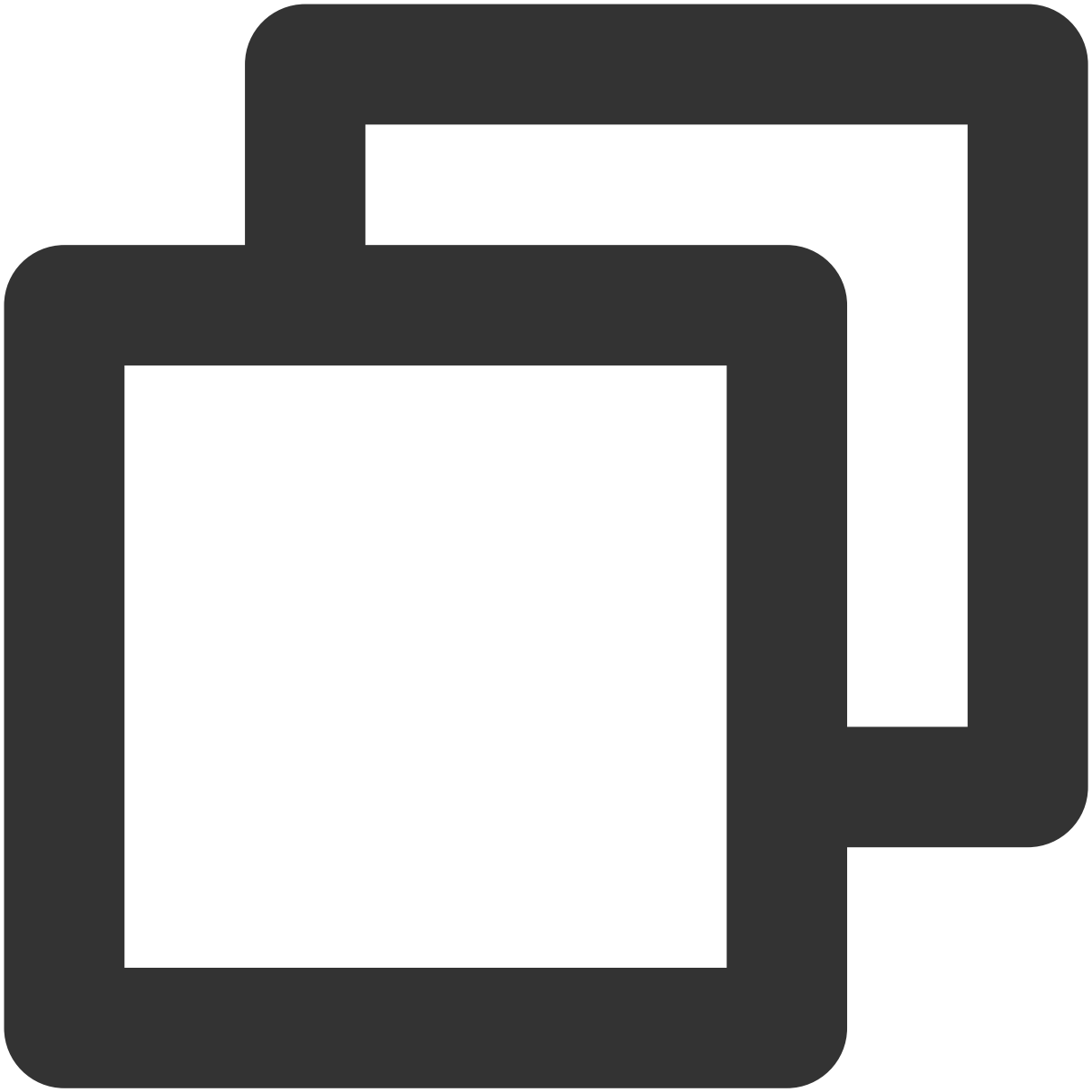
Windows 系统

执行以下命令，获取 Kubectl 工具：



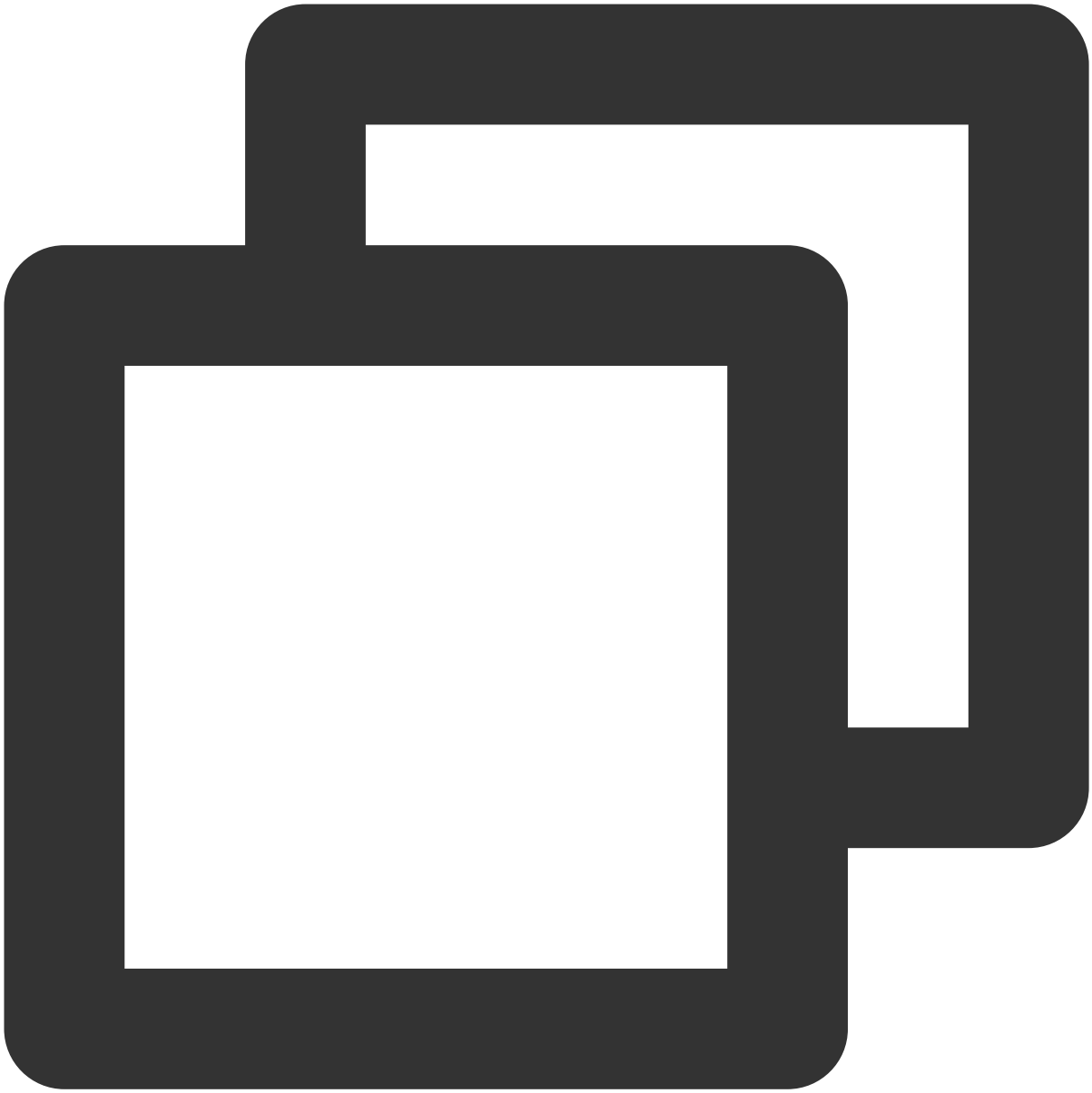
```
curl -LO https://storage.googleapis.com/kubernetes-release/release/v1.8.13/bin/darw
```

执行以下命令，获取 Kubectl 工具：



```
curl -LO https://storage.googleapis.com/kubernetes-release/release/v1.8.13/bin/linu
```

执行以下命令，获取 Kubectl 工具：



```
curl -LO https://storage.googleapis.com/kubernetes-release/release/v1.8.13/bin/wind
```

操作步骤

安装 Kubectl 工具

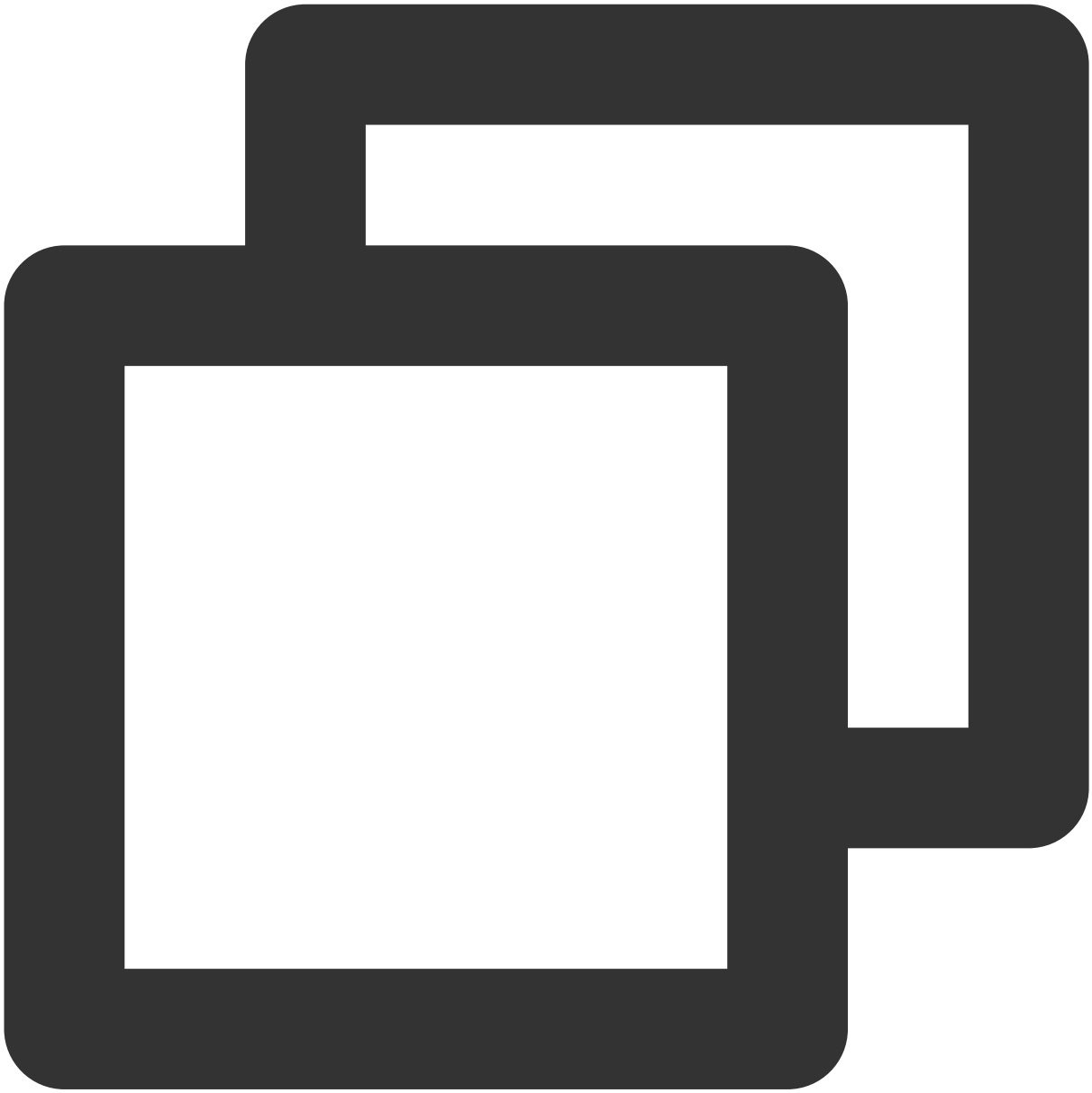
1. 参考 Installing and Setting up kubectl ， 安装 Kubectl 工具。

说明：

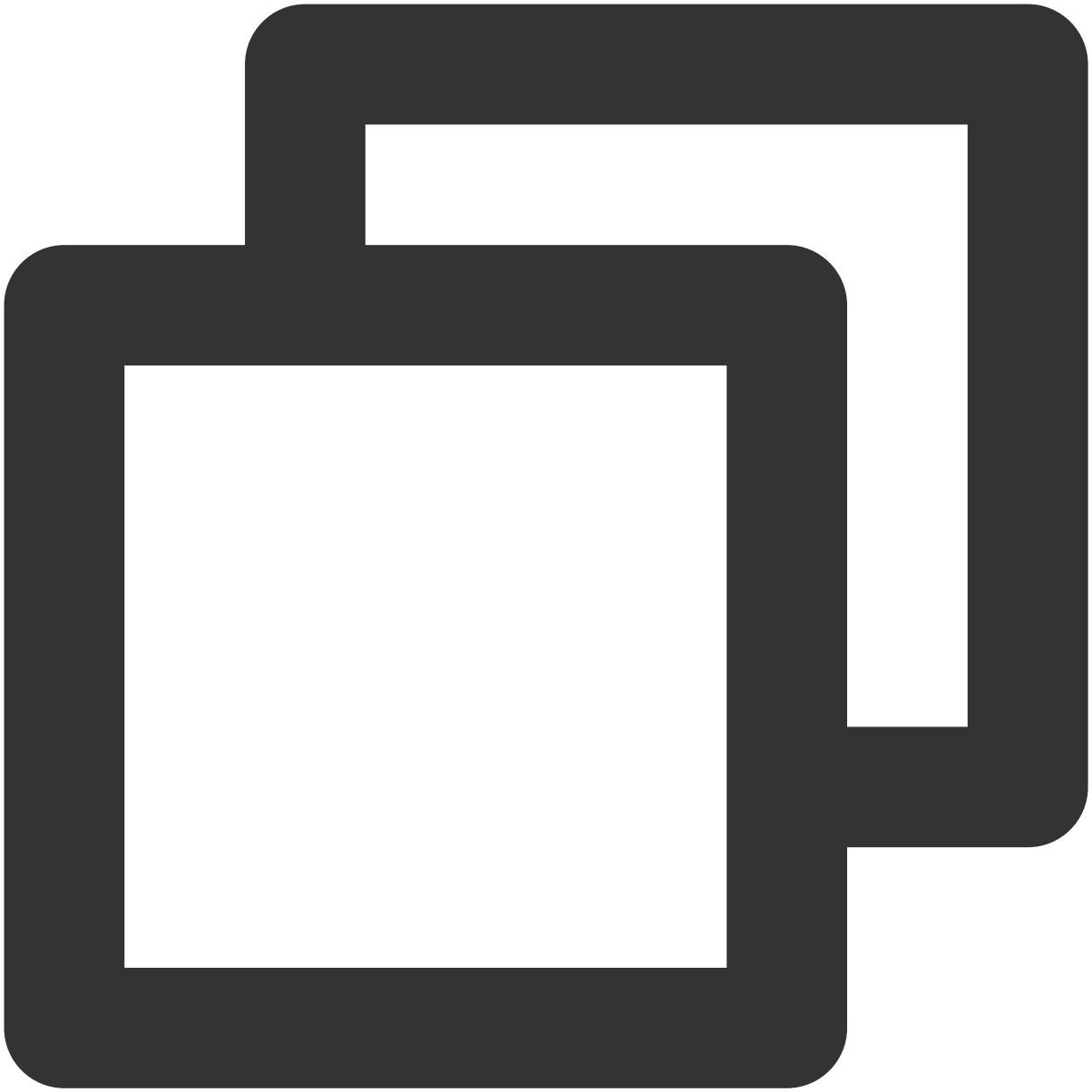
如果您已经安装 Kubectl 工具，请忽略本步骤。

此步骤以 Linux 系统为例。

2. 依次执行以下命令，添加执行权限。

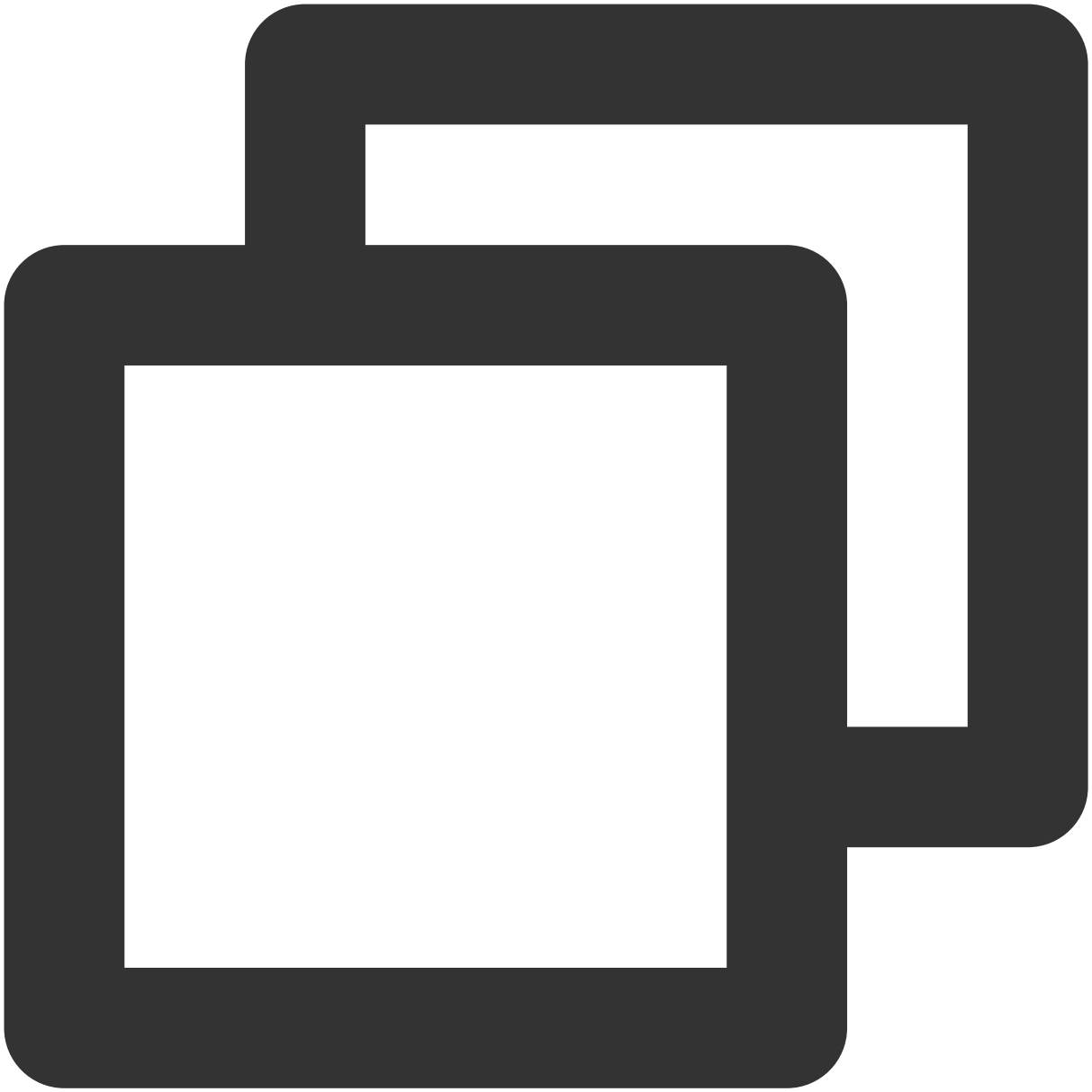


```
chmod +x ./kubectl
```



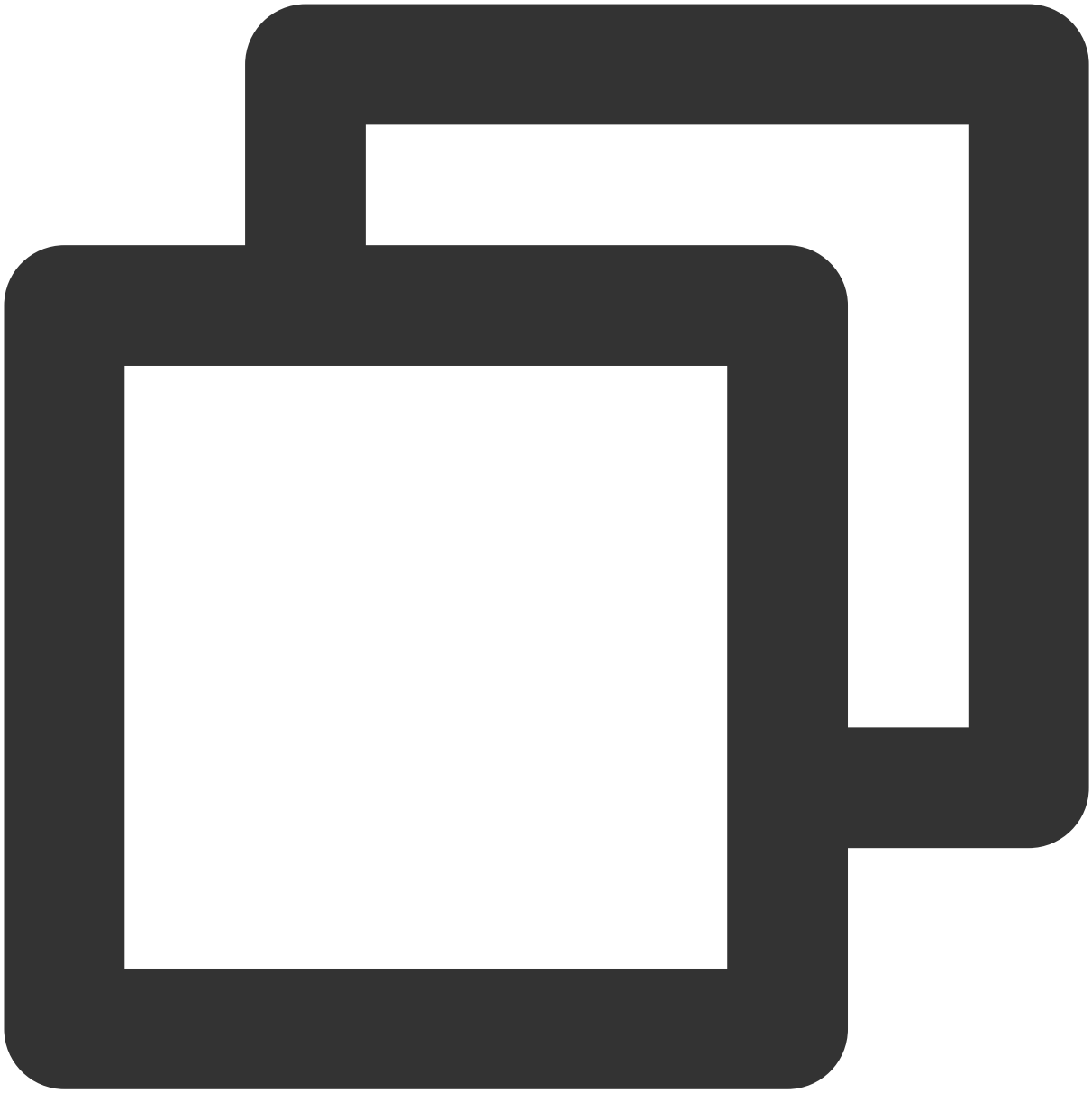
```
sudo mv ./kubectl /usr/local/bin/kubectl
```

3. 执行以下命令，测试安装结果。



```
kubectl version
```

如若输出类似以下版本信息，即表示安装成功。



```
Client Version: version.Info{Major:"1", Minor:"5", GitVersion:"v1.5.2", GitCommit:"
```

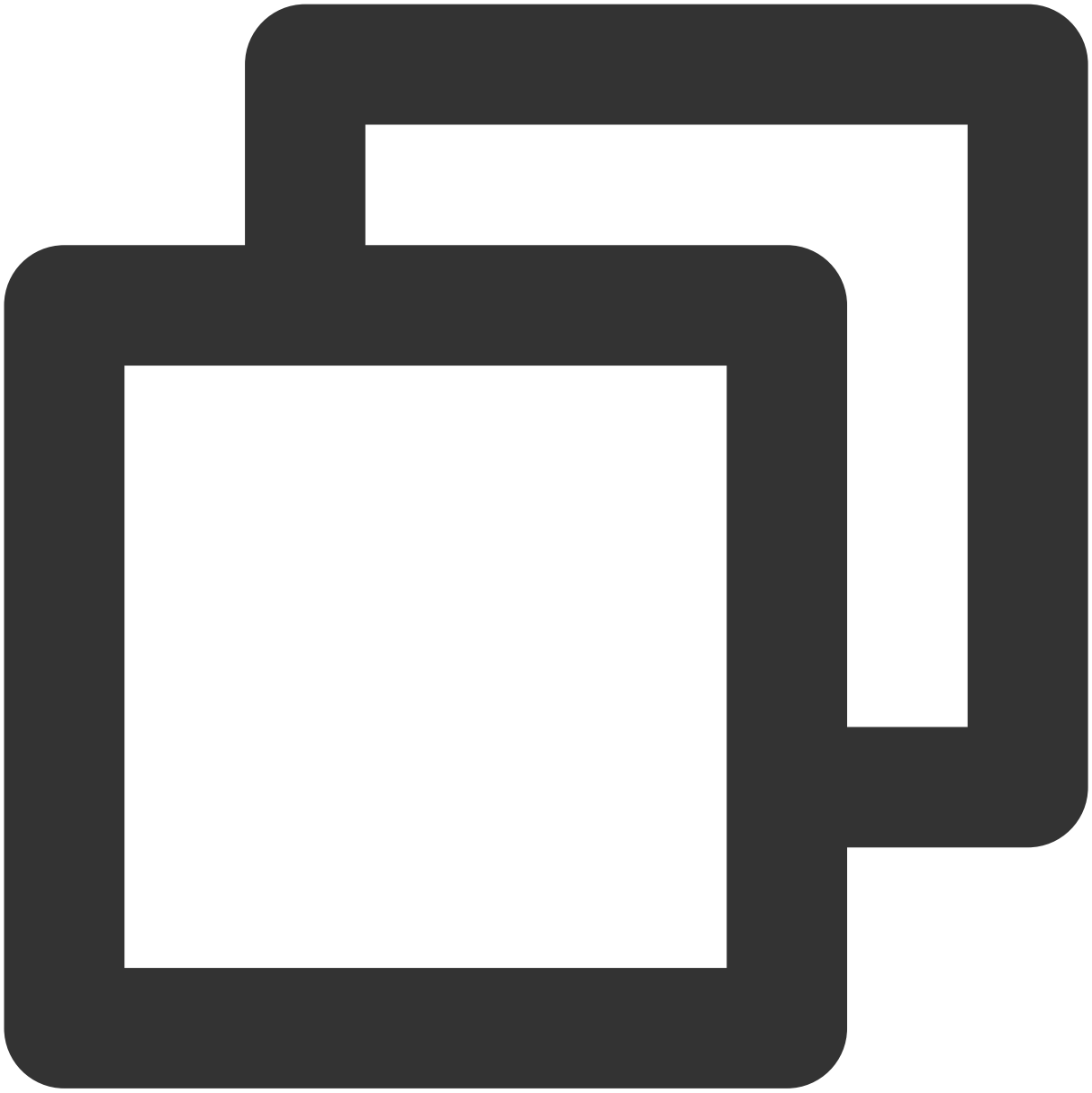
配置 Kubeconfig

1. 登录容器服务控制台，选择左侧导航栏中的 集群。
2. 在集群列表页面，单击需连接的注册集群 ID，进入该集群的管理页面。
3. 选择左侧导航栏中的**基本信息**，进入该集群基础信息页面。
4. 在**集群APIServer信息**中，获取对应的**公网访问**或**内网访问**的 kubeconfig，可以复制或者下载。
5. 根据实际情况进行集群凭据配置。详情可参见控制台内**通过Kubectl连接Kubernetes集群操作说明**。

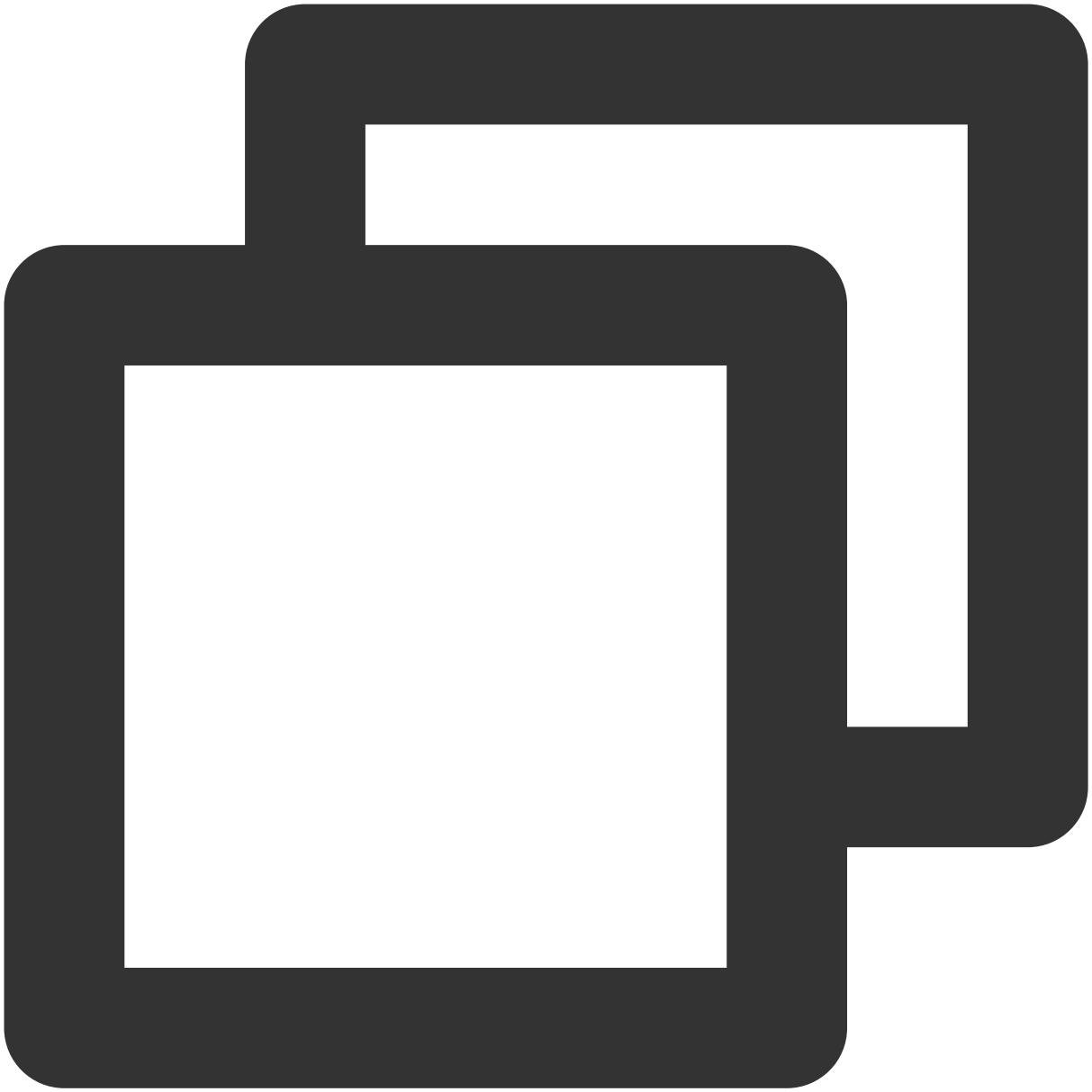
版权所有：腾讯云计算（北京）有限责任公司

访问 Kubernetes 集群

1. 完成 Kubeconfig 配置后，依次执行以下命令查看并切换 context 以访问本集群。

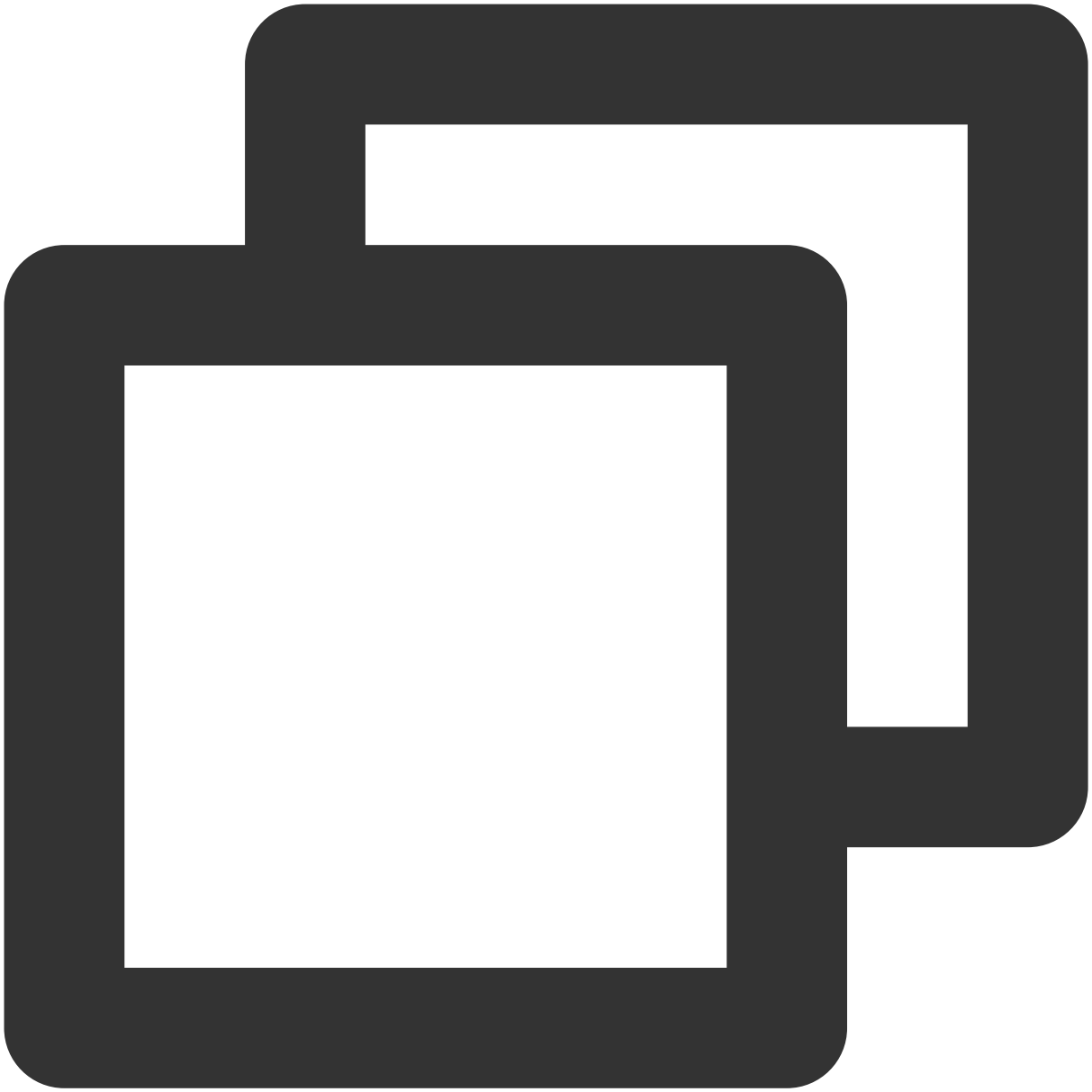


```
kubectl config get-contexts
```



```
kubectl config use-context cls-3jju4zdc-context-default
```

2. 执行以下命令， 测试是否可正常访问集群。



```
kubectl get pod
```

如果无法连接请查看是否已经开启公网访问或内网访问入口，并确保访问客户端在指定的网络环境内。

相关说明

Kubectl 命令行介绍

Kubectl 是一个用于 Kubernetes 集群操作的命令行工具。本文涵盖 Kubectl 语法、常见命令操作并提供常见示例。有关每个命令（包括所有主命令和子命令）的详细信息，请参见 Kubectl 参考文档 或使用 `kubectl help` 命令查看详细帮助，Kubectl 安装说明请参见上文 安装 Kubectl 工具。

版权所有：腾讯云计算（北京）有限责任公司

解除注册集群

最近更新时间：2024-05-09 15:47:33

操作场景

您可以解除已经注册的集群，注册集群一旦被解除，您将无法通过腾讯云容器服务控制台管理此集群。

操作步骤

1. 登录 容器服务控制台。
2. 在集群列表中，单击需要解绑的集群所在行右侧的**解除注册**。
3. 在“解除注册集群”弹窗中，单击**确定**。

注意

解除注册集群后，集群内安装的代理软件会被删除，集群本身以及集群内的其他资源不受影响。

运维指南
日志采集

最近更新时间：2023-06-08 11:16:57

本文主要介绍如何通过控制台的方式将注册集群的日志接入到 腾讯云日志服务 CLS。

操作场景

日志采集功能是容器服务 TKE 为用户提供的集群内日志采集工具，可以将集群内服务或集群节点特定路径文件的日志发送至 腾讯云日志服务 CLS。日志采集功能适用于需要对 Kubernetes 集群内服务日志进行存储和分析的用户。
日志采集功能需要为每个集群手动开启并配置采集规则。日志采集功能开启后，日志采集 Agent 会在集群内以 DaemonSet 的形式运行，并根据用户通过日志采集规则配置的采集源、CLS 日志主题和日志解析方式，从采集源进行日志采集，将日志内容发送到日志消费端。

使用须知

已经创建注册集群，且注册集群的状态为**运行中**。
目前注册集群的日志仅支持投递至 腾讯云日志服务 CLS，暂不支持其他日志消费端。
请在开启前保证集群节点上有足够资源。开启日志采集功能会占用您集群的部分资源。
占用 CPU 资源：0.11 - 1.1 核，日志量过大时可根据情况自行调大。
占用内存资源：24 - 560MB，日志量过大时可根据情况自行调大。
日志长度限制：单条 512K，如超过会截断。
若使用日志采集功能，请确认 Kubernetes 集群内节点能够访问日志消费端。TKE 提供公网和内网两种方式进行日志投递，用户可以根据业务情况自行选择：
公网投递：集群日志将通过公网的方式进行投递至日志服务 CLS ，需要集群中的节点具有访问公网的能力。
内网投递：集群日志将通过内网的方式进行投递至日志服务 CLS ，需要集群内的节点与腾讯云日志服务 CLS 内网互通。选择该选项前，请 联系我们 进行确认。

概念

日志采集 Agent：TKE 用于采集日志信息的 Agent，采用 Loglistener，在集群内以 DaemonSet 的方式运行。
日志规则：用户可以使用日志规则指定日志的采集源、日志主题、日志解析方式和配置过滤器。
日志采集 Agent 会监测日志采集规则的变化，变化的规则会在最多 10s 内生效。
多条日志采集规则不会创建多个 DaemonSet，但过多的日志采集规则会使得日志采集 Agent 占用的资源增加。

版权所有：腾讯云计算（北京）有限责任公司

日志源：包含指定容器标准输出、容器内文件以及节点文件。
在采集容器标准输出日志时，用户可选择所有容器、或指定工作负载和指定 Pod Labels 内的容器服务日志作为日志的采集源。
在采集容器文件路径日志时，用户可指定工作负载或 Pod Labels 内容器的文件路径日志作为采集源。
在采集节点文件路径日志时，用户可设定日志的采集源为节点文件路径日志。
消费端：用户选择日志服务 CLS 的日志集和日志主题作为消费端。
提取模式：日志采集 Agent 支持将采集到的日志以单行文本、JSON、分隔符、多行文本和完全正则的形式发送至用户指定的日志主题。
过滤器：开启过滤器后可以根据用户指定的规则采集部分日志，key 支持完全匹配，过滤规则支持正则匹配，如仅采集 ErrorCode = 404 的日志。

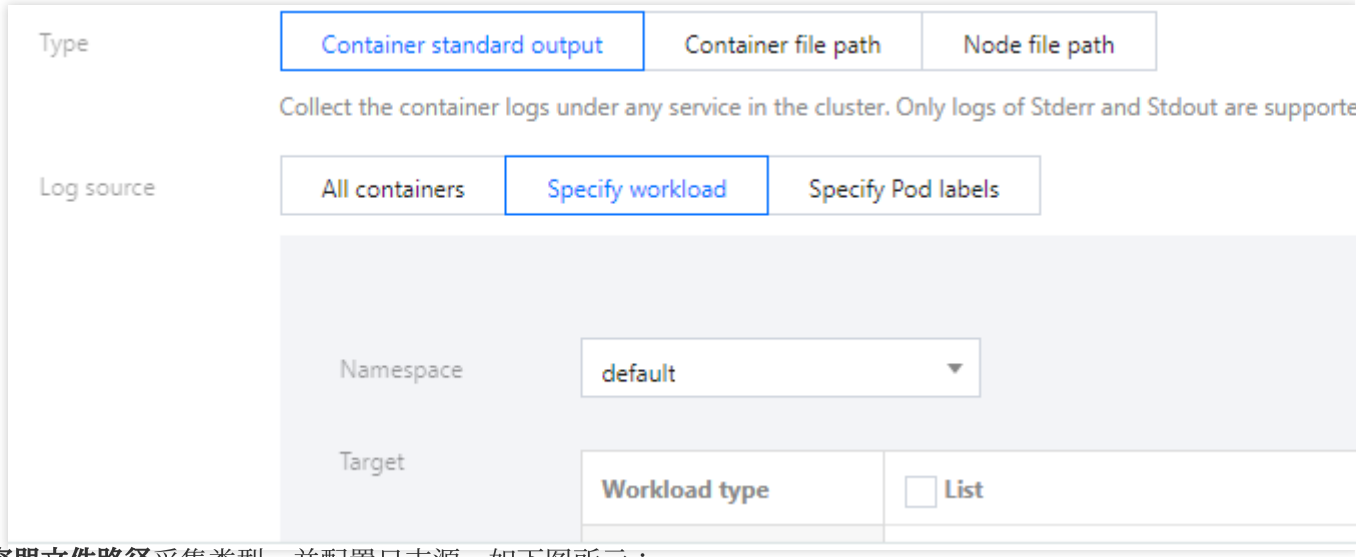
操作步骤

开启日志采集

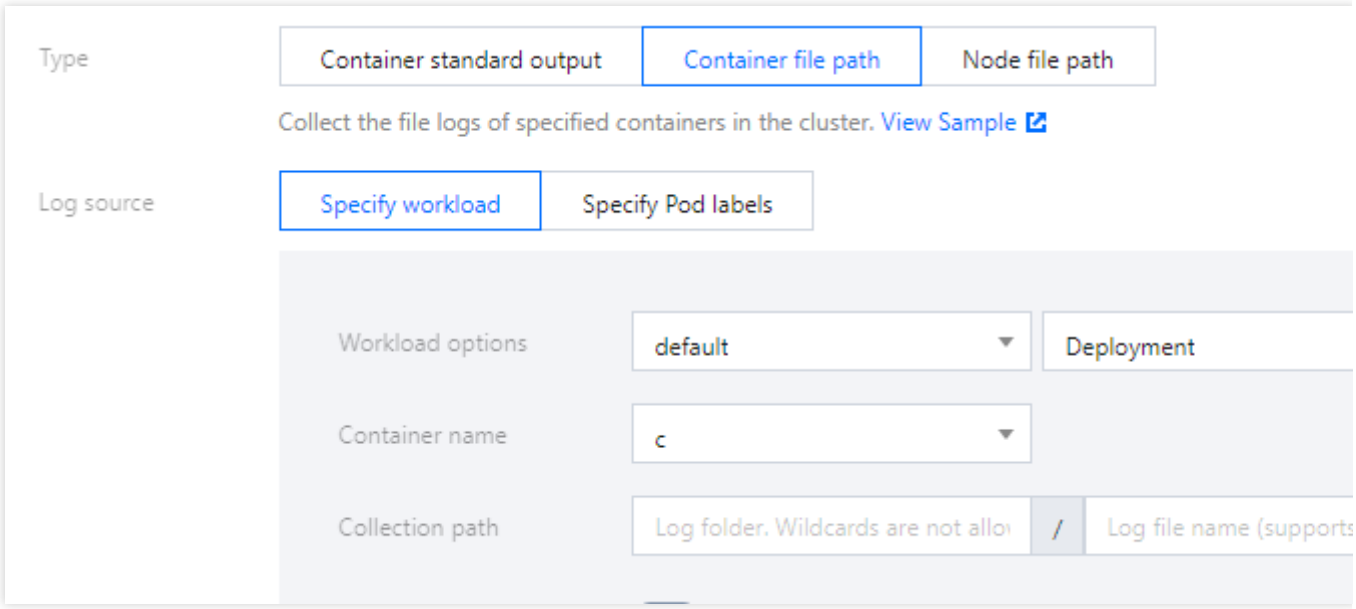
1. 登录 容器服务控制台，选择左侧导航栏中的**运维功能管理**。
2. 在**功能管理**页面上方选择地域和**注册集群**，单击需要开启日志采集的集群右侧的**设置**。
3. 在“设置功能”页面，单击日志采集**编辑**，开启日志采集，选择**投递方式**后单击**确定**。

配置日志规则

1. 登录 容器服务控制台，选择左侧导航栏中的**日志管理 > 日志规则**。
2. 在**功能管理**页面上方选择地域和**注册集群**，筛选需要配置日志采集规则的集群，单击**新建**。
3. 在**新建日志采集规则**页面，选择采集类型，并配置日志源。目前采集类型支持**容器标准输出**、**容器文件路径**和**节点文件路径**。
采集容器标准输出日志
采集容器内文件日志
采集节点文件日志
选择**容器标准输出**采集类型，并根据需求配置日志源。该类型日志源支持一次选择多个 Namespace 的工作负载。如下图所示：



选择**容器文件路径**采集类型，并配置日志源。如下图所示：



采集文件路径支持文件路径和通配规则，例如当容器文件路径为 `/opt/logs/*.log`，可以指定采集路径为 `/opt/logs`，文件名为 `*.log`。

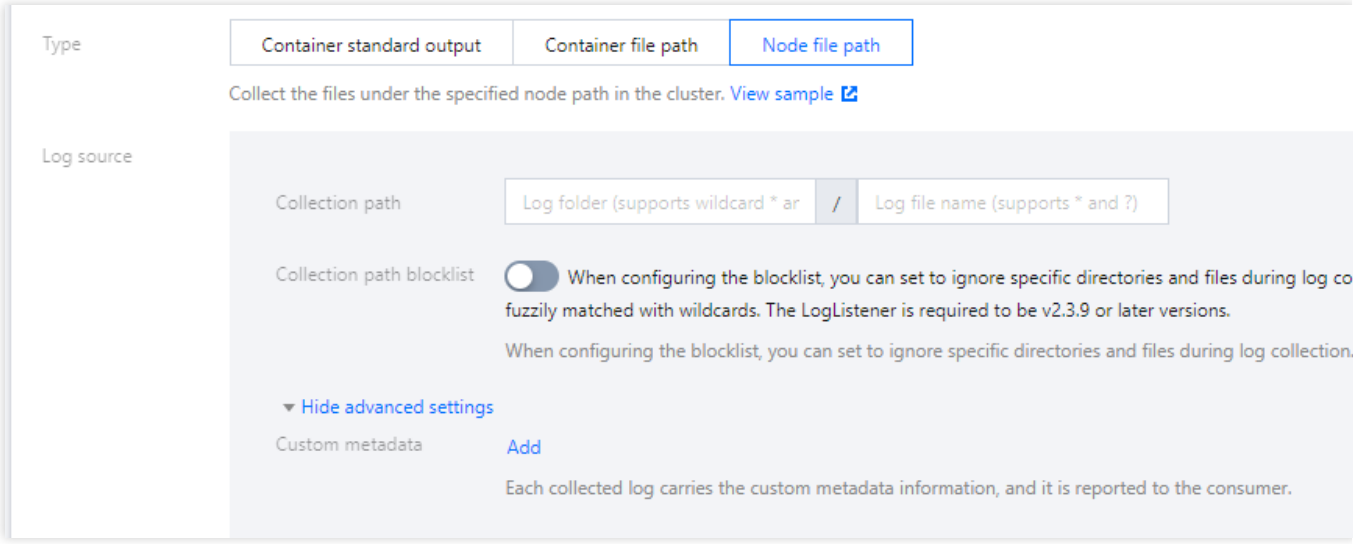
注意：

如果选择采集类型为“容器文件路径”时，对应的“容器文件路径”不能为软链接，否则会导致软链接的实际路径在采集器的容器内不存在，采集日志失败。

选择**节点文件路径**采集类型，用户可根据实际需求进行添加自定义的 “metadata”，将采集到的日志信息附加指定 Key-Value 形式的 “metadata”，附加 metadata 将会添加到日志记录中。如下图所示：

注意

一个节点日志文件只能被一个日志主题采集。



路径支持文件路径和通配规则，例如当需要采集所有文件路径形式为 `/opt/logs/service1/*.log`，`/opt/logs/service2/*.log`，可以指定采集路径的文件夹为 `/opt/logs/service*`，文件名为 `*.log`。

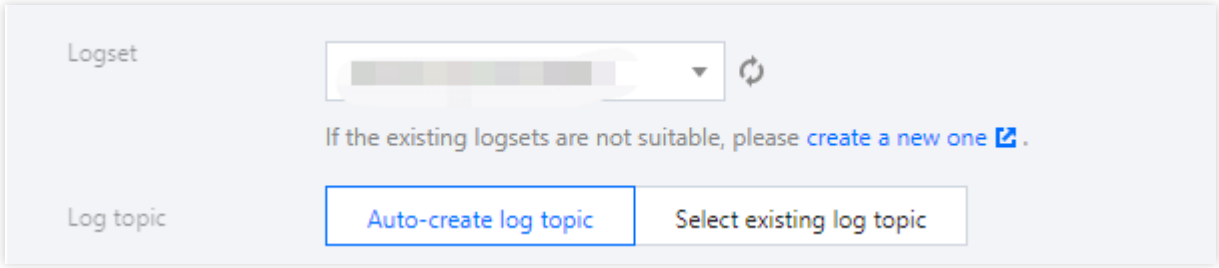
说明：

对于容器的标准输出及容器内文件（非 hostPath 挂载），除了原始的日志内容，还会带上容器或 kubernetes 相关的元数据（例如：产生日志的容器 ID）一起上报到 CLS，方便用户查看日志时追溯来源或根据容器标识、特征（例如：容器名、labels）进行检索。

容器或 kubernetes 相关的元数据请参考下方表格：

字段名	含义
container_id	日志所属的容器 ID。
container_name	日志所属的容器名称。
image_name	日志所属容器的镜像名称 IP。
namespace	日志所属 pod 的 namespace。
pod_uid	日志所属 pod 的 UID。
pod_name	日志所属 pod 的名字。
pod_lable_{label name}	日志所属 pod 的 label（例如一个 pod 带有两个 label：app=nginx，env=prod，则在上传的日志会附带两个 metedata：pod_label_app:nginx，pod_label_env:prod）。

4. 配置日志服务消费端，选择日志集和相应的日志主题，可以选择新建和已有日志主题。如下图所示：

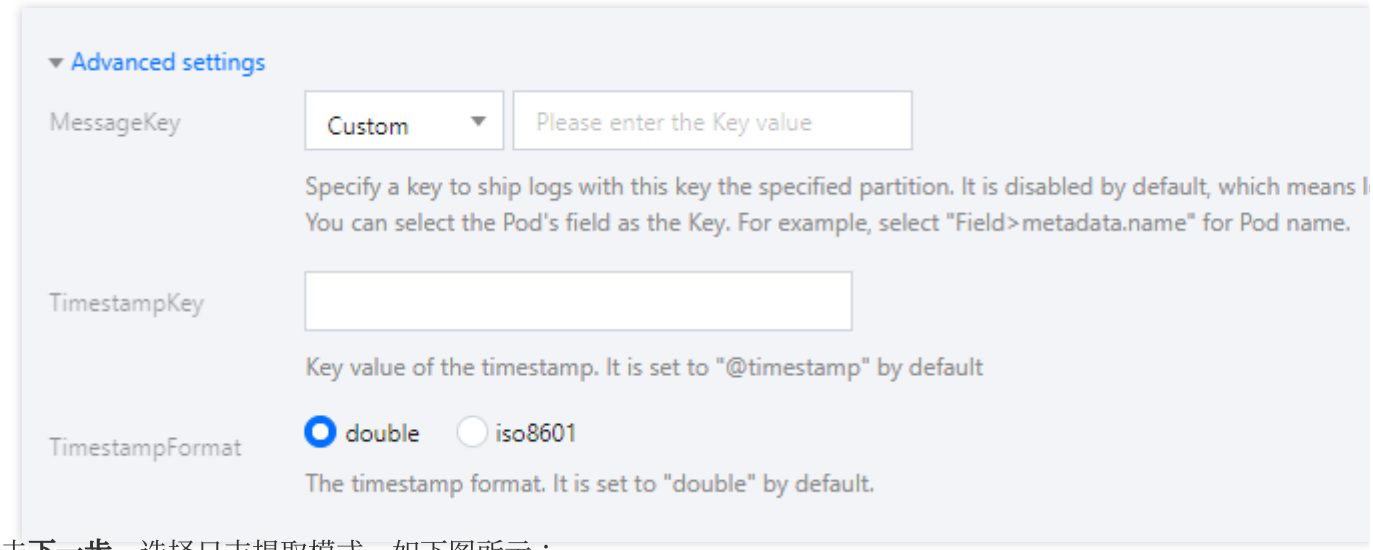


注意

腾讯云日志服务 CLS 目前只能支持同地域的容器集群进行日志采集上报。

若日志集下已存在 500 个日志主题，则不能新建日志主题。

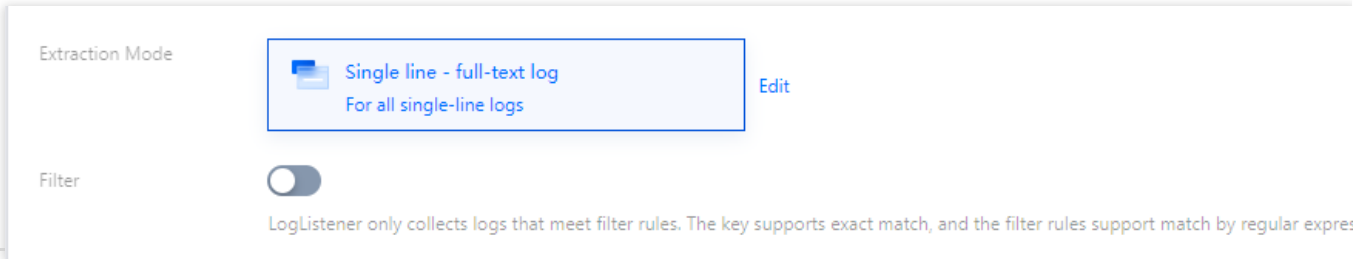
5. 支持在高级设置内通过指定 Key 值将日志投递到指定分区，该功能默认不开启，日志随机投放，当开启后，带有同样 Key 值的日志，将投递到相同的分区。支持输入 TimestampKey（默认@timestamp）和指定时间戳格式。如下图所示：



6. 单击**下一步**，选择日志提取模式。如下图所示：

注意

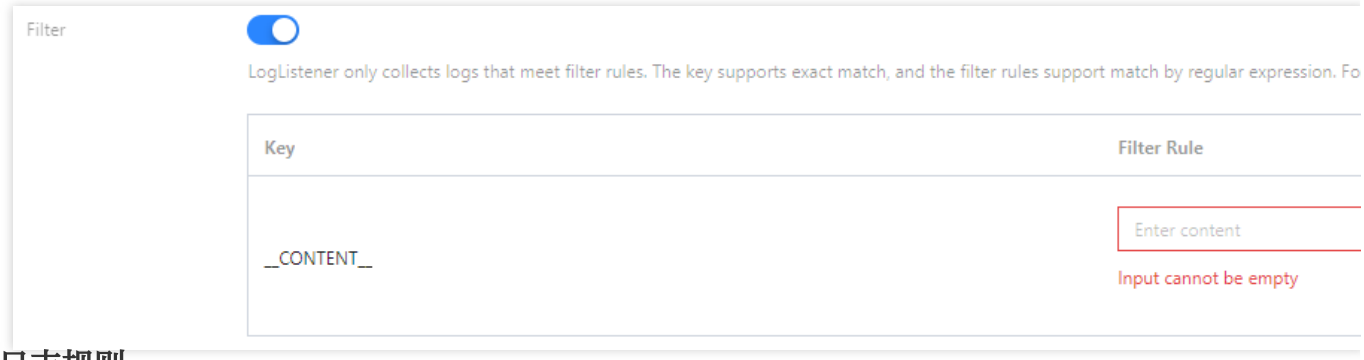
当前仅投递到 CLS 支持配置日志解析方式。



解析模式	说明	相关文档
单行全文	一条日志仅包含一行的内容，以换行符 \\n 作为一条日志的结束标记，每条日志将被解析为键值为 CONTENT 的一行完全字符串，开启索引后可通过全文检索搜索日志内容。日志时间以采集时间为准。	单行全文格式

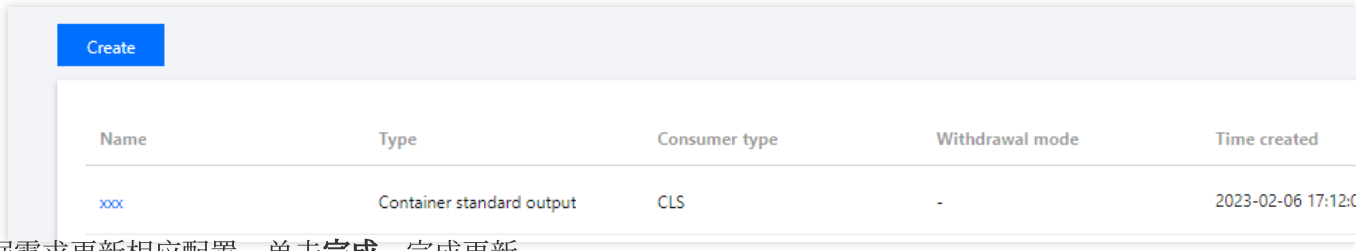
多行全文	指一条完整的日志跨占多行，采用首行正则的方式进行匹配，当某行日志匹配上预先设置的正则表达式，就认为是一条日志的开头，而下一个行首出现作为该条日志的结束标识符，也会设置一个默认的键值 CONTENT，日志时间以采集时间为准。支持自动生成正则表达式。	多行全文格式
单行 - 完全正则	指将一条完整日志按正则方式提取多个 key-value 的日志解析模式，您需先输入日志样例，其次输入自定义正则表达式，系统将根据正则表达式里的捕获组提取对应的 key-value。支持自动生成正则表达式。	单行 - 完全正则格式
多行 - 完全正则	适用于日志文本中一条完整的日志数据跨占多行（例如 Java 程序日志），可按正则表达式提取为多个 key-value 键值的日志解析模式，您需先输入日志样例，其次输入自定义正则表达式，系统将根据正则表达式里的捕获组提取对应的 key-value。支持自动生成正则表达式。	多行-完全正则格式
JSON	JSON 格式日志会自动提取首层的 key 作为对应字段名，首层的 value 作为对应的字段值，以该方式将整条日志进行结构化处理，每条完整的日志以换行符 \\n 为结束标识符。	JSON 格式
分隔符	指一条日志数据可以根据指定的分隔符将整条日志进行结构化处理，每条完整的日志以换行符 \\n 为结束标识符。日志服务在进行分隔符格式日志处理时，您需要为每个分开的字段定义唯一的 key，无效字段即无需采集的字段可填空，不支持所有字段均为空。	分隔符格式

7. 根据需求开启过滤器并配置规则，并单击**完成**，完成创建。如下图所示：



更新日志规则

1. 登录 容器服务控制台，选择左侧导航栏中的**日志管理 > 日志规则**。
2. 在**日志采集**页面上方选择地域和**注册集群**，筛选需要更新日志采集规则的集群，单击右侧的**编辑收集规则**。如下图所示：



3. 根据需求更新相应配置，单击**完成**，完成更新。

注意

日志集和日志主题不可更新。

相关文档

通过 YAML 使用 CRD 配置日志采集

集群审计

最近更新时间：2022-12-23 11:04:28

本文主要介绍如何将注册集群的审计日志接入到 腾讯云日志服务 CLS。

简介

集群审计是基于 Kubernetes Audit 对 kube-apiserver 产生的可配置策略的 JSON 结构日志的记录存储及检索功能。本功能记录了对 kube-apiserver 的访问事件，会按顺序记录每个用户、管理员或系统组件影响集群的活动。

使用须知

- 已经创建注册集群，且注册集群的状态为运行中。
- 目前注册集群的审计日志仅支持投递至 腾讯云日志服务 CLS，暂不支持其他日志消费端。
- 注册集群开启审计功能，需要用户自行登录集群的 Master 节点配置相关审计策略和 API Server 相关参数。
- 开启集群审计功能，默认会同步开启集群日志采集功能。
- 若使用集群审计功能，请确认 Kubernetes 集群内节点能够访问日志消费端。这里我们提供公网和内网两种方式进行日志投递，用户可以根据业务情况自行选择：
  - 公网投递：集群审计日志将通过公网的方式进行投递至日志服务 CLS ，需要集群中的节点具有访问公网的能力。
  - 内网投递：集群审计日志将通过内网的方式进行投递至日志服务 CLS ，需要集群内的节点与腾讯云日志服务 CLS 内网互通。选择该选项前，请 提交工单 进行确认。

使用步骤

在集群 Master 节点上配置审计策略

依次登录集群的所有 Master 节点，配置审计策略文件 `/etc/kubernetes/audit-policy.yaml` 。您可以根据业务的实际情况，按需修改。

```
apiVersion: audit.k8s.io/v1beta1
kind: Policy
omitStages:
- "RequestReceived"
rules:
- level: None
users: ["system:kube-proxy"]
```

版权所有：腾讯云计算（北京）有限责任公司

```
verbs: ["watch"]
resources:
- group: ""
resources: ["endpoints", "services"]
- level: None
users: ["system:unsecured"]
namespaces: ["kube-system"]
verbs: ["get"]
resources:
- group: ""
resources: ["configmaps"]
- level: None
users: ["kubelet"]
verbs: ["get"]
resources:
- group: ""
resources: ["nodes"]
- level: None
userGroups: ["system:nodes"]
verbs: ["get"]
resources:
- group: ""
resources: ["nodes"]
- level: None
users:
- system:kube-controller-manager
- system:kube-scheduler
- system:serviceaccount:kube-system:endpoint-controller
verbs: ["get", "update"]
namespaces: ["kube-system"]
resources:
- group: ""
resources: ["endpoints"]
- level: None
users: ["system:apiserver"]
verbs: ["get"]
resources:
- group: ""
resources: ["namespaces"]
- level: None
nonResourceURLs:
- /healthz*
- /version
- /swagger*
- level: None
resources:
- group: ""
```

```
resources: ["events"]
- level: Metadata
resources:
- group: "" # core
resources: ["secrets", "configmaps"]
- group: authentication.k8s.io
resources: ["tokenreviews"]
- level: Request
verbs: ["get", "list", "watch"]
resources:
- group: ""
- group: "admissionregistration.k8s.io"
- group: "apps"
- group: "authentication.k8s.io"
- group: "authorization.k8s.io"
- group: "autoscaling"
- group: "batch"
- group: "certificates.k8s.io"
- group: "extensions"
- group: "networking.k8s.io"
- group: "policy"
- group: "rbac.authorization.k8s.io"
- group: "settings.k8s.io"
- group: "storage.k8s.io"
- level: RequestResponse
resources:
- group: ""
- group: "admissionregistration.k8s.io"
- group: "apps"
- group: "authentication.k8s.io"
- group: "authorization.k8s.io"
- group: "autoscaling"
- group: "batch"
- group: "certificates.k8s.io"
- group: "extensions"
- group: "networking.k8s.io"
- group: "policy"
- group: "rbac.authorization.k8s.io"
- group: "settings.k8s.io"
- group: "storage.k8s.io"
- level: Metadata
```

在 Master 节点上配置 API Server 参数

依次登录集群所有的 Master 节点，修改 `/etc/kubernetes/manifests/kube-apiserver.yaml` 文件

1. 添加相关 command 参数，内容如下：

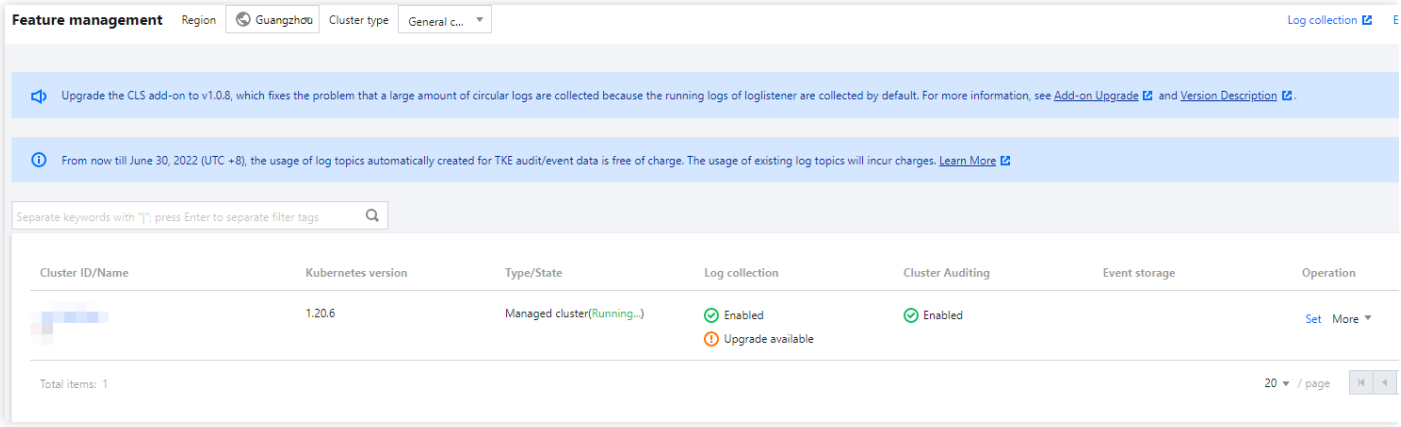
```
spec:
containers:
- command:
- kube-apiserver
- --audit-log-maxbackup=10
- --audit-log-maxsize=100
- --audit-log-path=/var/log/kubernetes/kubernetes.audit
- --audit-log-maxage=30
- --audit-policy-file=/etc/kubernetes/audit-policy.yaml
```

2. 添加相关的 Volume 参数，将 /etc/kubernetes/audit-policy.yaml 挂载到 API Server Pod，内容如下：

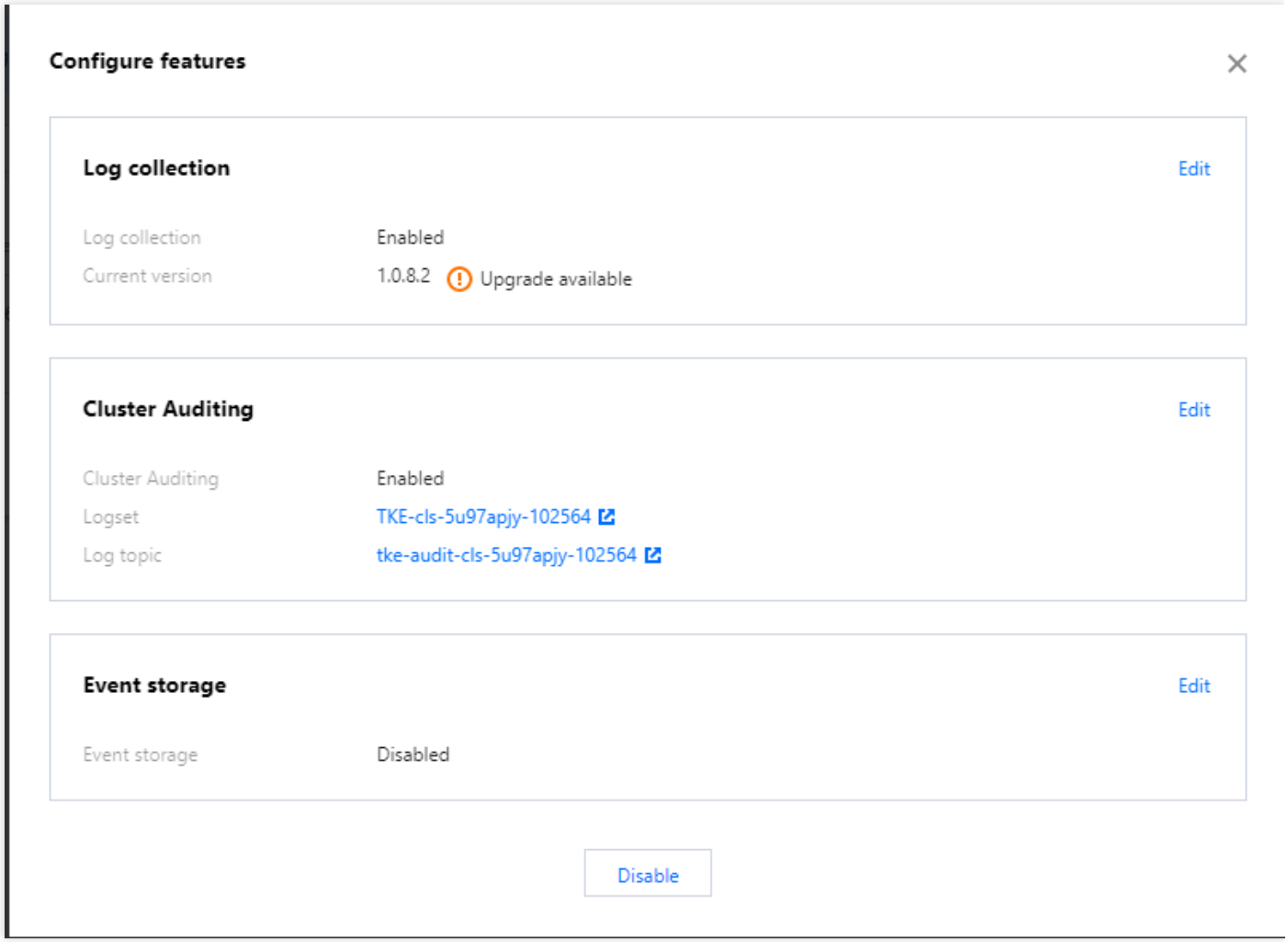
```
spec:
containers:
- command:
- kube-apiserver
- --audit-log-maxbackup=10
- --audit-log-maxsize=100
- --audit-log-path=/var/log/kubernetes/kubernetes.audit
- --audit-log-maxage=30
- --audit-policy-file=/etc/kubernetes/audit-policy.yaml
...
...
volumeMounts:
- mountPath: /var/log/kubernetes
name: k8s-audit
- mountPath: /etc/kubernetes/audit-policy.yaml
name: audit-policy
readOnly: true
...
...
volumes:
- hostPath:
path: /var/log/kubernetes
type: DirectoryOrCreate
name: k8s-audit
- hostPath:
path: /etc/kubernetes/audit-policy.yaml
type: FileOrCreate
name: audit-policy
...
```

开启集群审计

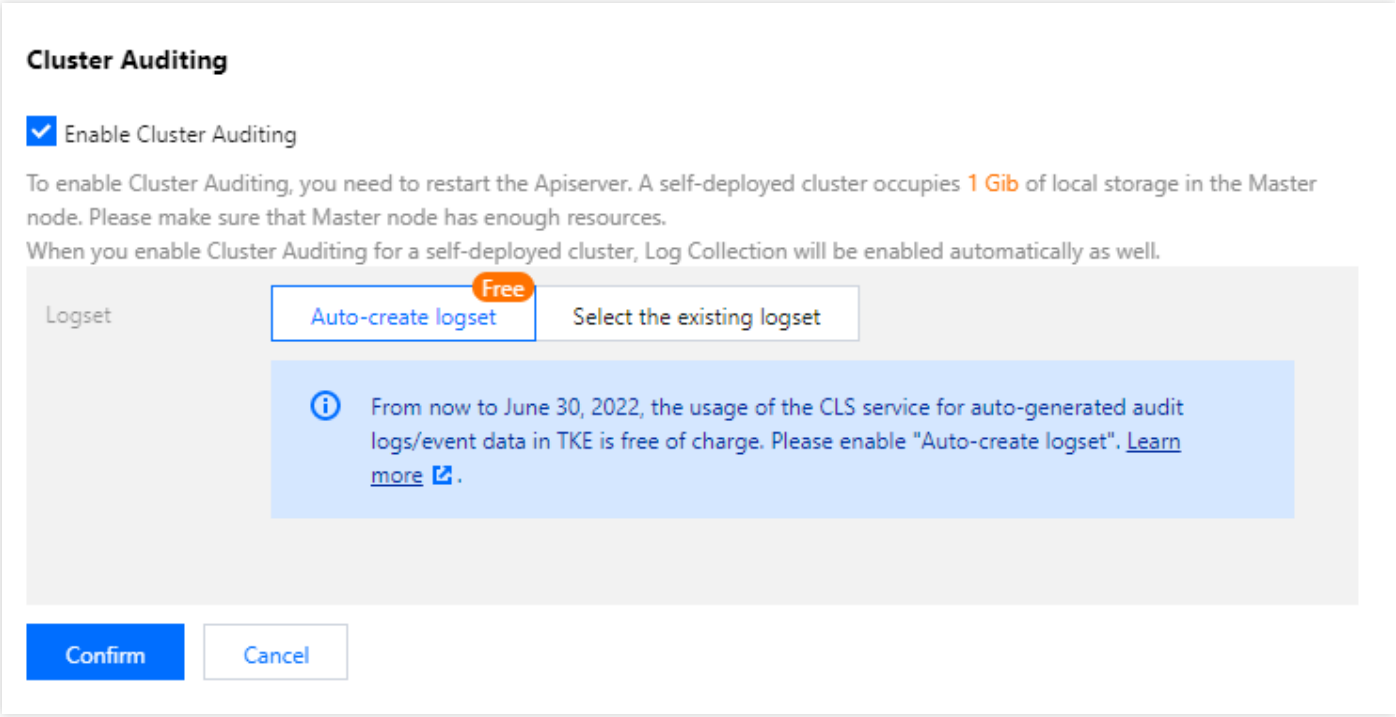
1. 登录 腾讯云容器服务控制台，选择左侧导航中的**运维功能管理**。
2. 在“功能管理”页面上方选择地域和注册集群，单击希望开启集群审计的集群右侧的**设置**。如下图所示：



3. 在弹出的“设置功能”窗口，单击“集群审计”功能右侧的**编辑**。



4. 勾选**开启集群审计**，选择投递方式和存储审计日志的日志集、日志主题，推荐选择**自动创建日志主题**。



5. 单击**确定**即可开启注册集群审计功能。

审计仪表盘

容器服务为用户提供了开箱即用的审计仪表盘。在集群开启集群审计功能后，TKE 将自动为该集群配置审计总览、节点操作总览、K8S 对象操作概览、聚合检索仪表盘。还支持用户自定义配置过滤项，同时内置 CLS 的全局检索，方便用户观测和检索各类集群操作，以便于及时发现和定位问题。更多详细介绍，请参考 审计仪表盘。