容器服务

TKE 注册集群指南

产品文档

腾讯云

文档目录

TKE 注册集群指南
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。
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

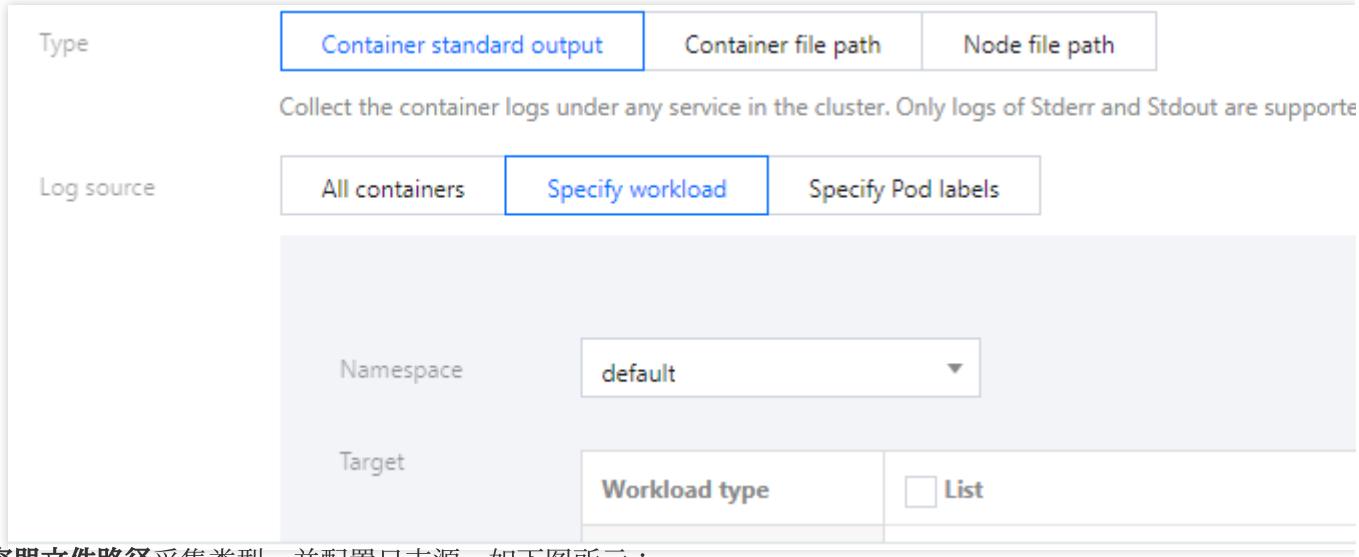
1. 登录 容器服务控制台，选择左侧导航栏中的**运维功能管理**。
2. 在**功能管理**页面上方选择地域和**注册集群**，单击需要开启日志采集的集群右侧的**设置**。
3. 在“设置功能”页面，单击日志采集**编辑**，开启日志采集，选择**投递方式**后单击**确定**。

配置日志规则

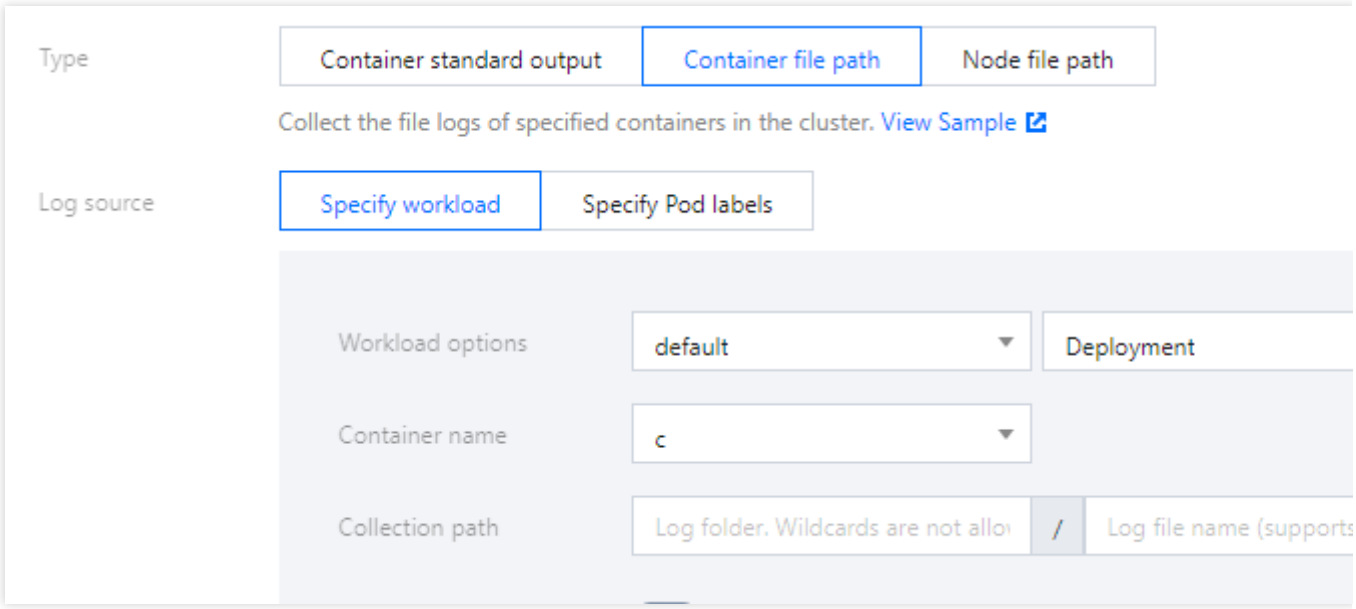
1. 登录 容器服务控制台，选择左侧导航栏中的**日志管理 > 日志规则**。
2. 在**功能管理**页面上方选择地域和**注册集群**，筛选需要配置日志采集规则的集群，单击**新建**。
3. 在**新建日志采集规则**页面，选择采集类型，并配置日志源。目前采集类型支持**容器标准输出**、**容器文件路径**和**节点文件路径**。

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`。

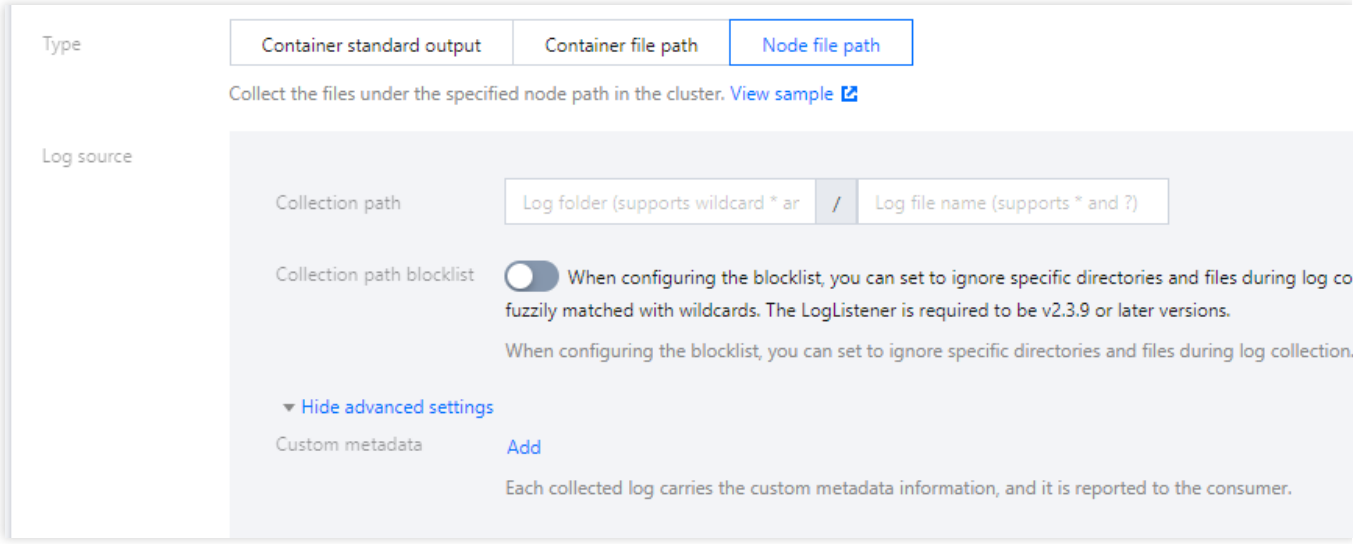
注意：

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`。

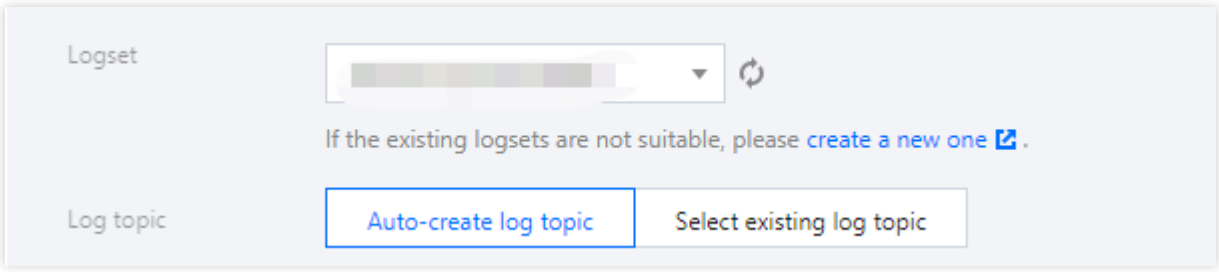
说明：

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：

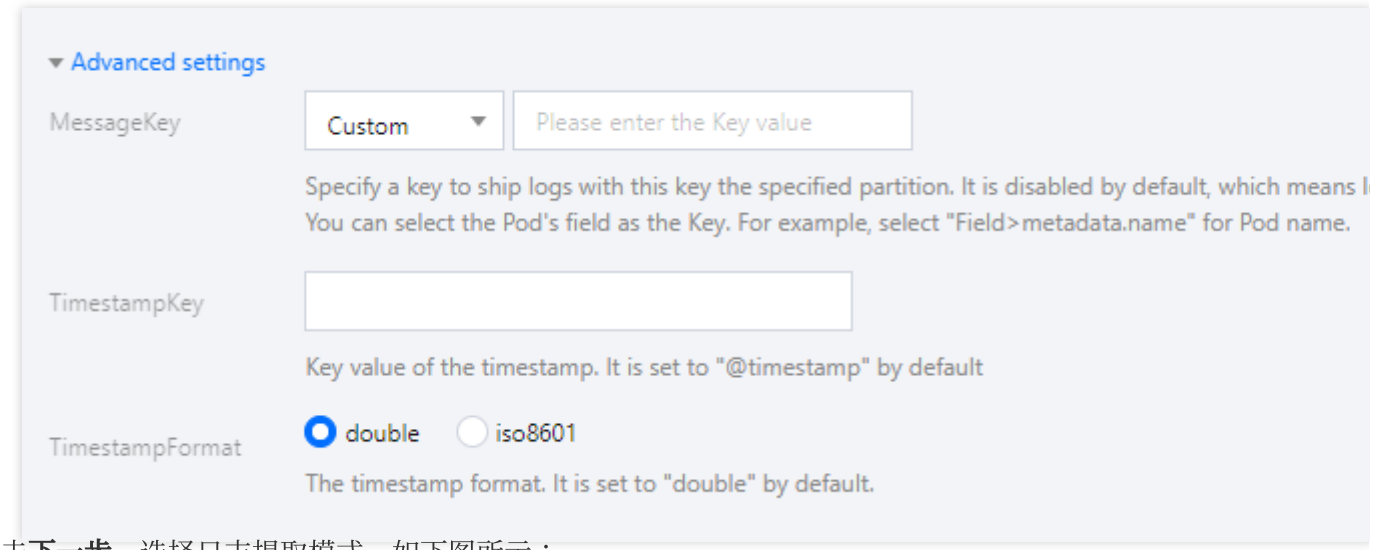


注意

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。

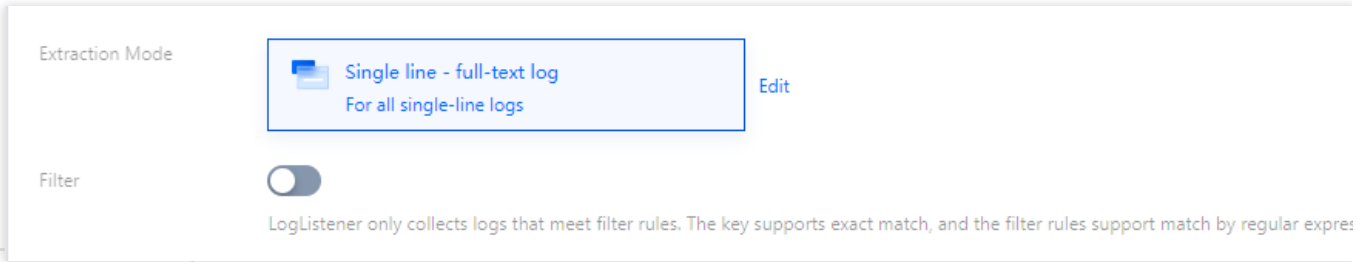
5. 支持在高级设置内通过指定 Key 值将日志投递到指定分区，该功能默认不开启，日志随机投放，当开启后，带有同样 Key 值的日志，将投递到相同的分区。支持输入 TimestampKey（默认@timestamp）和指定时间戳格式。如下图所示：



6. 单击**下一步**，选择日志提取模式。如下图所示：

注意

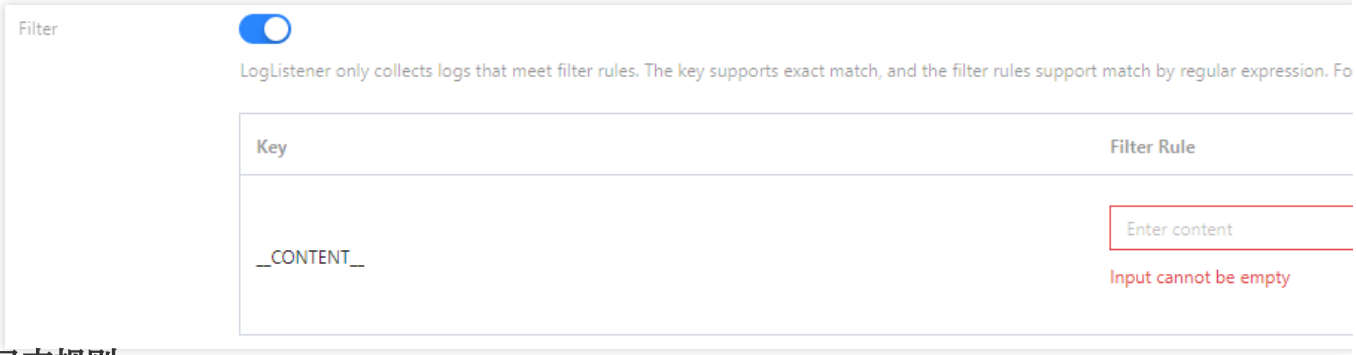
当前仅投递到 CLS 支持配置日志解析方式。



解析模式	说明
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。
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

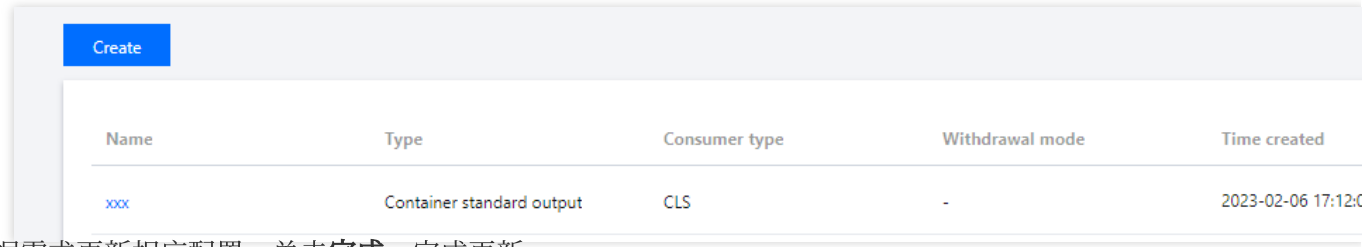
	的开头，而下一个行首出现作为该条日志的结束标识符，也会设置一个默认的键值 CONTEN 支持自动生成正则表达式。
单行 - 完全正则	指将一条完整日志按正则方式提取多个 key-value 的日志解析模式，您需先输入日志样例，其 将根据正则表达式里的捕获组提取对应的 key-value。支持自动生成正则表达式。
多行 - 完全正则	适用于日志文本中一条完整的日志数据跨占多行（例如 Java 程序日志），可按正则表达式提 解析模式，您需先输入日志样例，其次输入自定义正则表达式，系统将根据正则表达式里的捕 持自动生成正则表达式。
JSON	JSON 格式日志会自动提取首层的 key 作为对应字段名，首层的 value 作为对应的字段值，以 处理，每条完整的日志以换行符 \\n 为结束标识符。
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 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 均为空。

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"]
```

```
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：

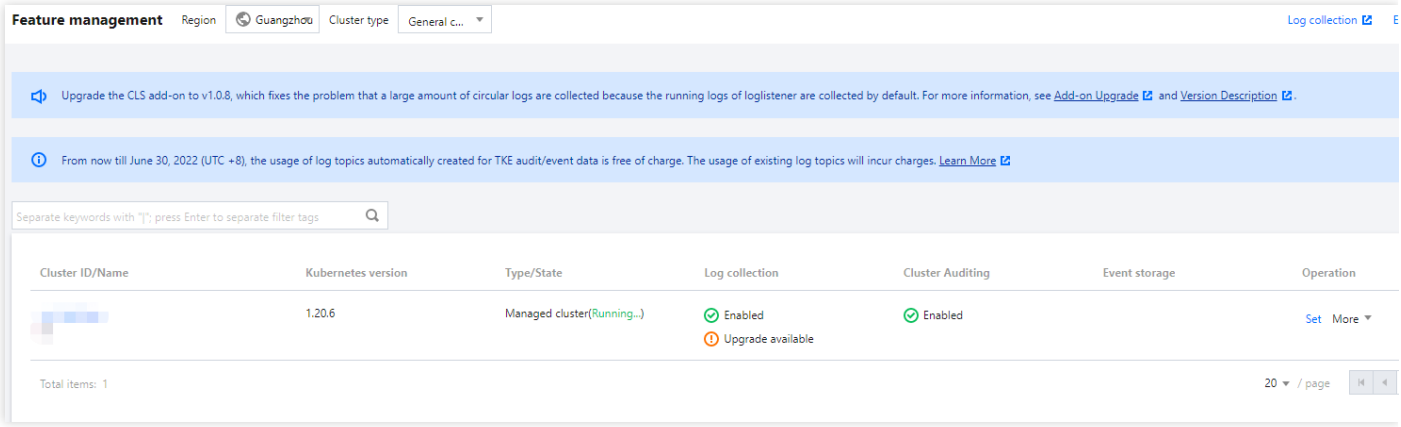
```
spec:
containers:
- command:
- kube-apiserver
- --audit-log-maxbackup=10
- --audit-log-maxsize=100
- --audit-log-path=/var/log/kubernetes/kubernetes.audit
- --audit-log-maxage=30
- --audit-policy-file=/etc/kubernetes/audit-policy.yaml
```

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：

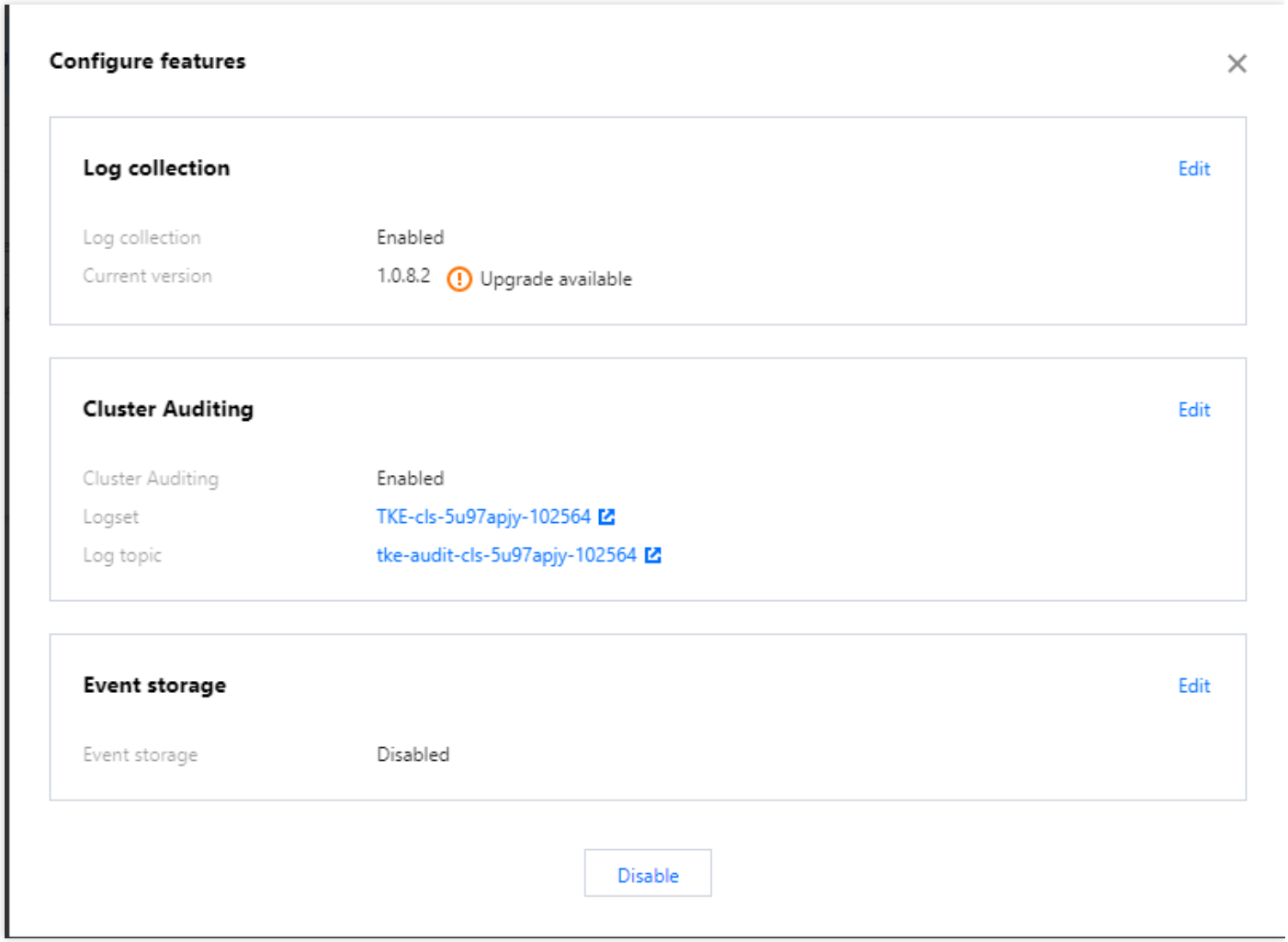
```
spec:
containers:
- command:
- kube-apiserver
- --audit-log-maxbackup=10
- --audit-log-maxsize=100
- --audit-log-path=/var/log/kubernetes/kubernetes.audit
- --audit-log-maxage=30
- --audit-policy-file=/etc/kubernetes/audit-policy.yaml
...
...
volumeMounts:
- mountPath: /var/log/kubernetes
name: k8s-audit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

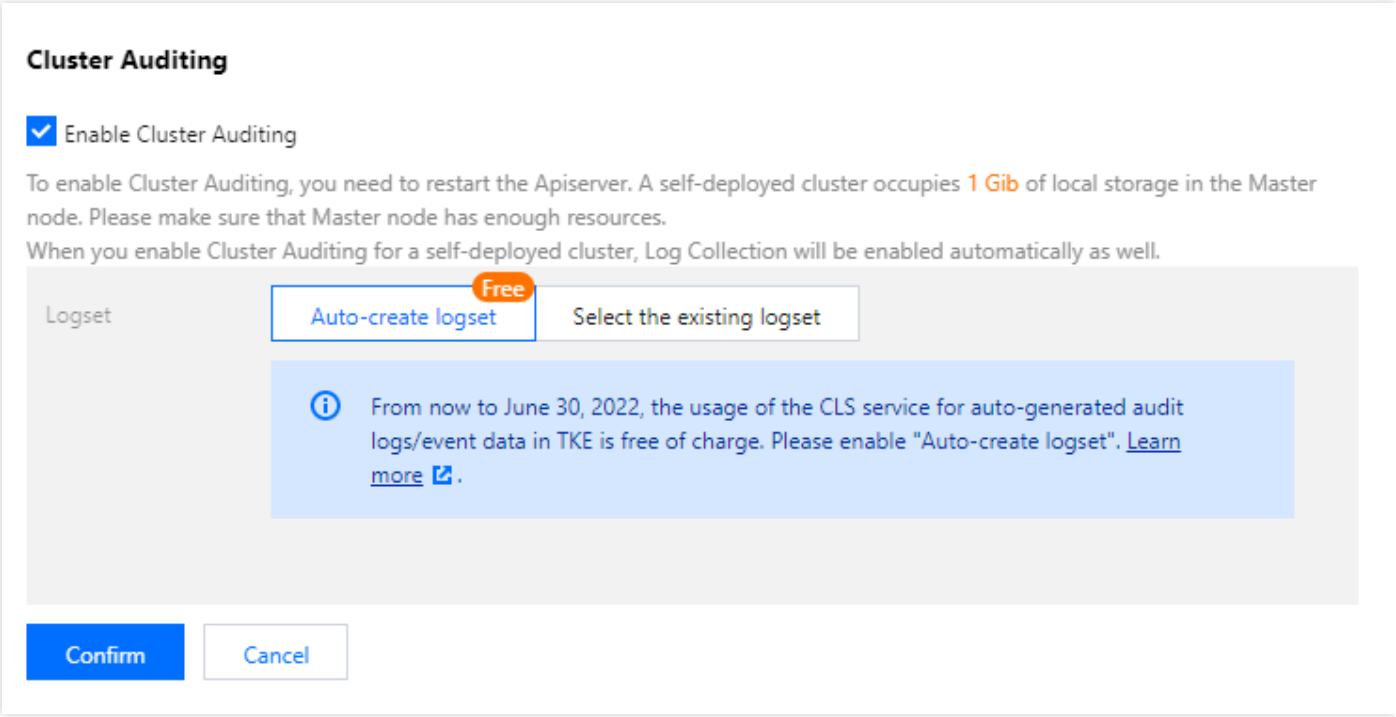
1. 登录 腾讯云容器服务控制台，选择左侧导航中的**运维功能管理**。
2. 在“功能管理”页面上方选择地域和注册集群，单击希望开启集群审计的集群右侧的**设置**。如下图所示：



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。