日志服务

常见问题

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

常见问题
健康监测问题解释
索引配置相关
日志上传相关
采集相关
机器组状态异常问题
LogListener 常见问题
LogListener 安装异常问题
容器日志采集常见问题
自建 K8S 日志采集排查指南
检索分析相关
检索不到日志
检索分析报错
其他问题

常见问题
健康监测问题解释
索引配置相关

最近更新时间：2024-01-20 17:11:56

如何开启索引配置？

索引配置 是使用日志服务（Cloud Log Service，CLS）进行检索分析的必要条件，未开启索引将无法对日志进行检索分析。 强烈建议开启。

操作步骤

1. 登录 日志服务控制台。
2. 在左侧导航栏中，单击**日志主题**，进入日志主题列表页面。
3. 单击需要配置索引的日志主题 ID/名称，进入日志主题管理页面。
4. 选择**索引配置**页签， 单击**编辑**，进入编辑索引配置页面。
5. 单击索引状态开关， 开启索引。
6. 开启索引后， 您可进一步配置全文索引或键值。

全文索引：支持对日志进行全文检索。

键值索引：支持基于日志内容中的指定字段进行检索。该配置的前提是日志采集配置中的提取模式为结构化提取模式（即将日志解析为键值对）。

如何开启键值索引配置？

键值索引指的是在全文索引的基础上，进一步将原始日志按字段（即 key:value）分别切分为多个分词进行索引构建，检索时基于键值方式进行检索（即键值检索）。强烈建议开启，以最大化提升日志检索的效率。

注意：

开启键值索引的前提条件是日志采集配置中的提取模式为结构化提取模式（即将日志解析为键值对）。

操作步骤

1. 登录 日志服务控制台。
2. 在左侧导航栏中，单击**日志主题**，进入日志主题列表页面。
3. 单击需要配置索引的日志主题 ID/名称，进入日志主题管理页面。
4. 选择**索引配置**页签， 单击**编辑**，进入编辑索引配置页面。
5. 单击键值索引开关， 开启键值索引。
6. 开启键值索引后， 您还可以单击自动配置，系统将自动获取采集到的最近1条日志作为样例，并将其中的字段解析为键值索引。您可以在自动配置的基础上进行微调，快速获取最终的索引配置信息。

版权所有：腾讯云计算（北京）有限责任公司

日志上传相关

最近更新时间：2024-01-20 17:11:57

如何应对提示参数错误？

该错误说明通过 API 或 SDK 上传日志时，请求输入参数 填写错误，请确保参数填写正确。

哪些原因可能会导致鉴权失败？

该错误说明上传日志时出现鉴权错误。 该类问题的出现通常可能由以下几种原因导致：

错误原因	解决方法
密钥不存在	请在控制台检查密钥是否已被删除或者禁用。 如状态正常，请检查密钥是否填写正确，注意前后不得有空格。您可单击 此处 查看您的密钥信息。
签名错误	签名计算错误，请对照调用方式中的 签名方法 检查签名计算过程。
签名过期	请对照调用方式中的签名方法文档重新计算签名。
请求未授权	无上传日志权限。请前往 CAM 控制台，为您的账号添加 CLS 上传日志的权限。
密钥非法	密钥格式不正确。您可单击 此处 查看您的密钥信息。
其他	若以上原因均已排除，且错误持续存在， 请联系 在线客服 提交工单反馈。

如何应对上传日志大小超限？

单条日志上传请求中的日志大小存在超限， 请根据以下规格限制调整日志上传大小：

限制项	说明
上传日志	一个 pb 包里 logGroup 不能超过10个。
	一个 pb 包里 logGroup 包含日志条数最多为10000条，至少包含1条。
	log 中单个 value 最大为1MB。
	一个 pb 包里 logGroup 部分所有 Value 大小最大总和为5MB。
	单次上传请求的包体压缩前不能超过6MB。

为什么会出现触发流控或频控？

该错误说明存在以下规格超限的情况：

限制项	说明

写频控	单个日志主题分区写请求限制：500QPS。
写流控	单个日志主题分区写流量限制：5MB/s。

建议减少日志上传的频次与流量。 若不希望改变日志上传的频次或流量，建议为日志主题 开启自动分裂。

如何应对上传请求错误？

该错误说明存在其他上传错误，请联系 在线客服 提交工单反馈。

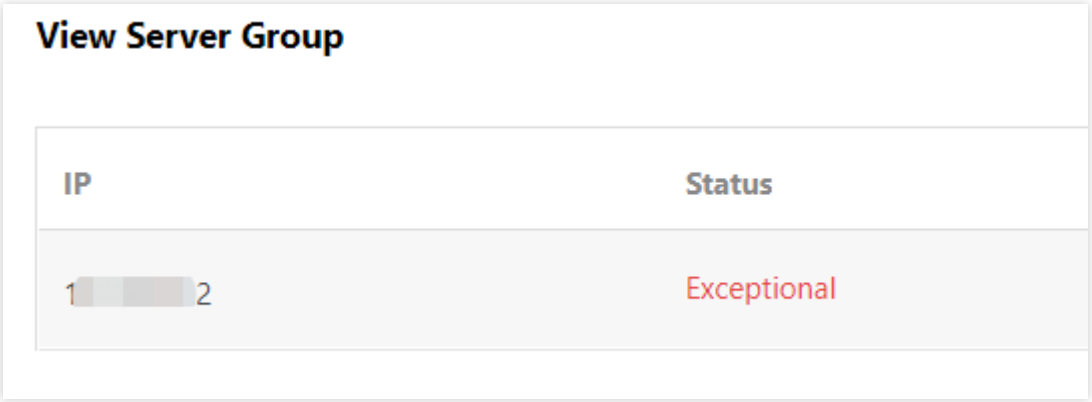
版权所有：腾讯云计算（北京）有限责任公司

采集相关
机器组状态异常问题

最近更新时间：2024-01-20 17:11:57

现象描述

配置机器组时，可能会出现所安装的 LogListener 状态异常。一旦状态异常，则 LogListener 与日志服务后端连接中断，会导致 LogListener 无法正常上传日志，异常状态如图：



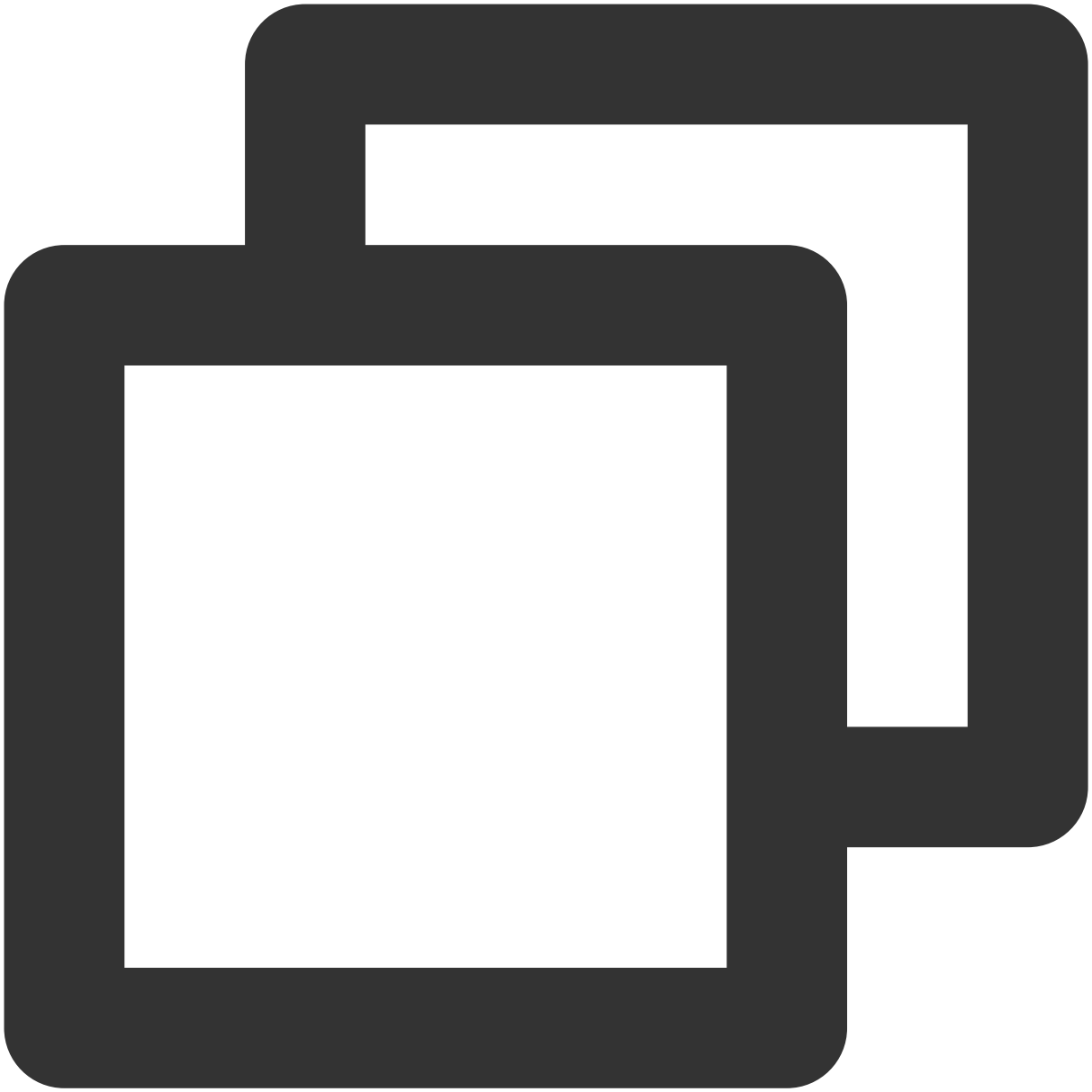
排查步骤

说明：

本篇文档所述排查步骤仅适合于 LogListener 2.2.4 及以上版本，其他请参考 低版本 LogListener 异常状态排查。

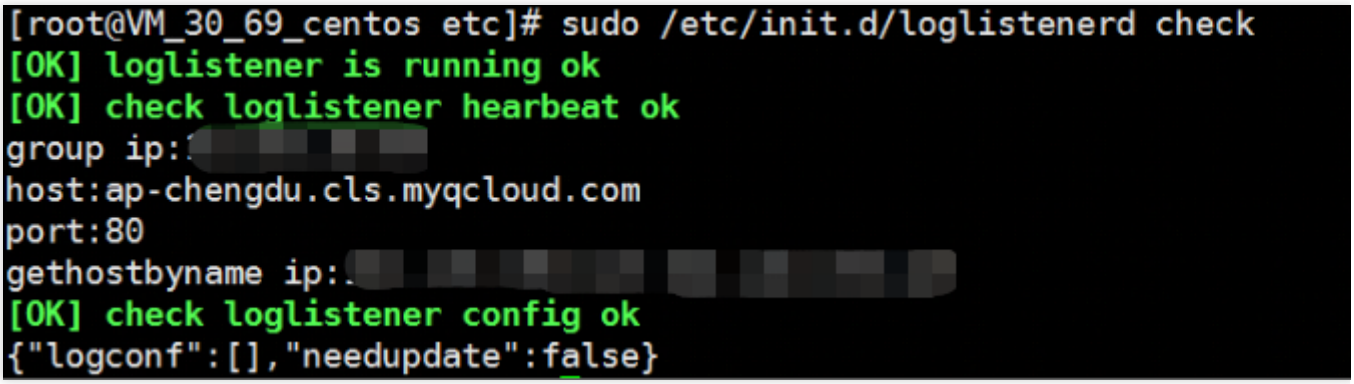
1. 使用 LogListener 快速诊断工具

LogListener 快速诊断工具可以快速诊断 LogListener 是否启动、心跳是否正常、配置拉取是否正常。
在命令行下执行如下指令：



```
/etc/init.d/loglistenerd check
```

若 LogListener 运行正常，诊断工具返回的结果如图所示：



LogListener 进程异常

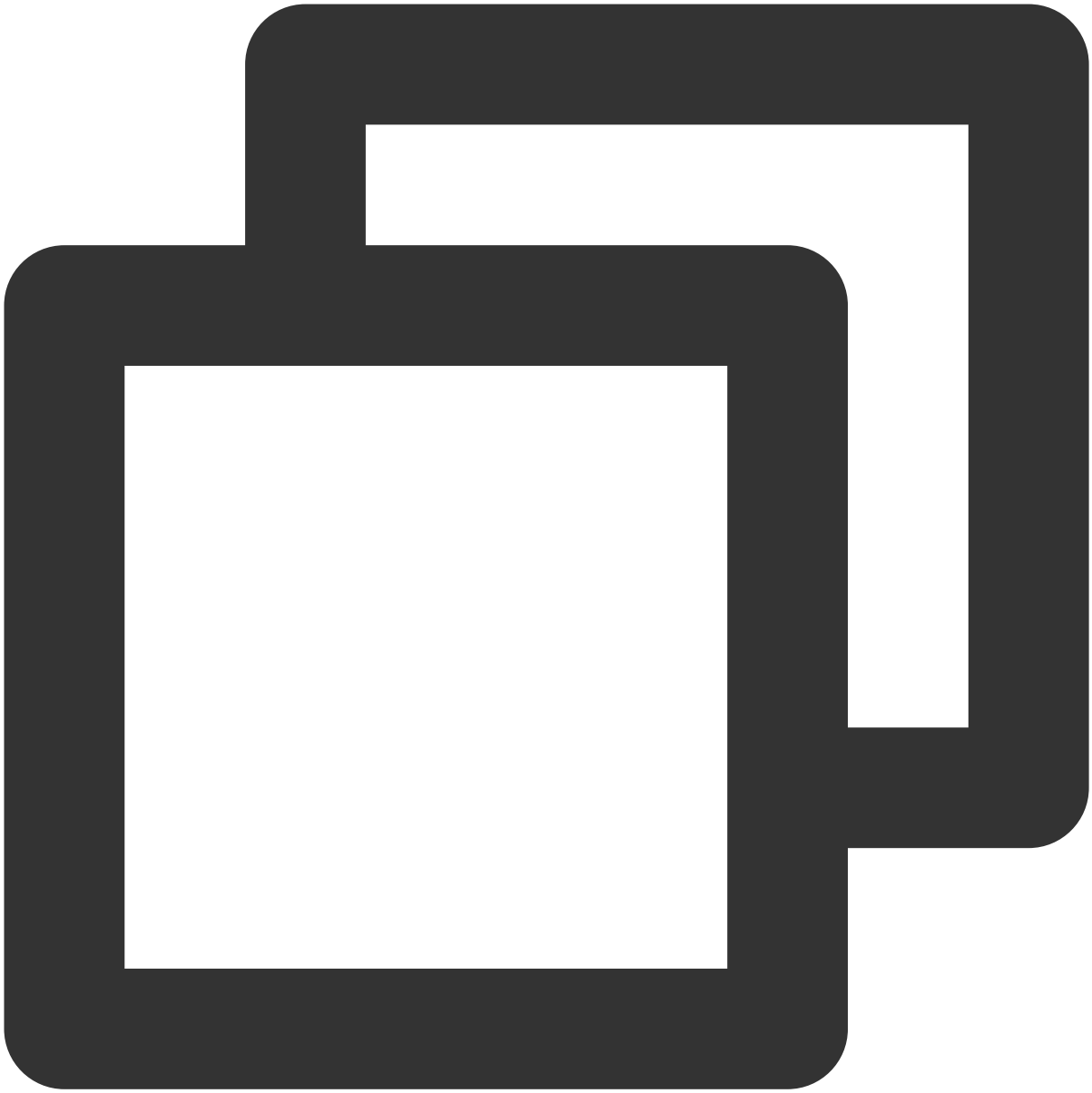
如果出现如下图所示 “[ERROR] loglistener is not running” 字样，表示 LogListener 没有启动。 执行 `/etc/init.d/loglistenerd start` 启动，更多操作指令参考 LogListener 常用操作指令。

LogListener 心跳异常

如果出现 “[ERROR] check loglistener heareat fail” 字样，表示 LogListener 心跳异常。

引起 LogListener 心跳异常的原因有很多，最常见的情况有：

网络异常



```
telnet <cls domain name> 80
```

检查网络环境是否连通，CLS 服务域名请参见 可用地域 文档。

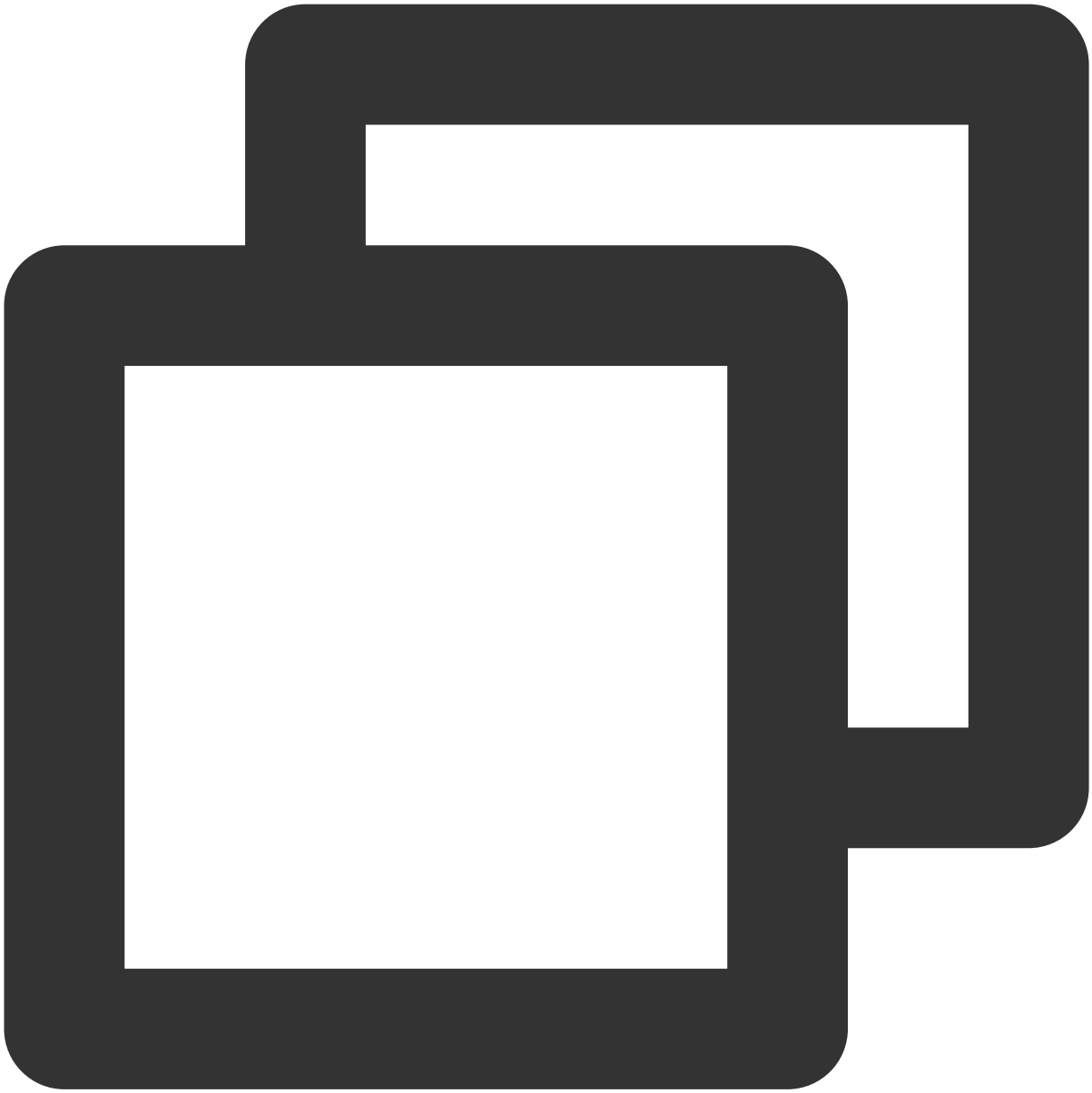
密钥信息错误

检查 LogListener 密钥信息是否正确，进入到 LogListener 安装目录执行如下命令。

```
grep secret etc/loglistener.conf
```

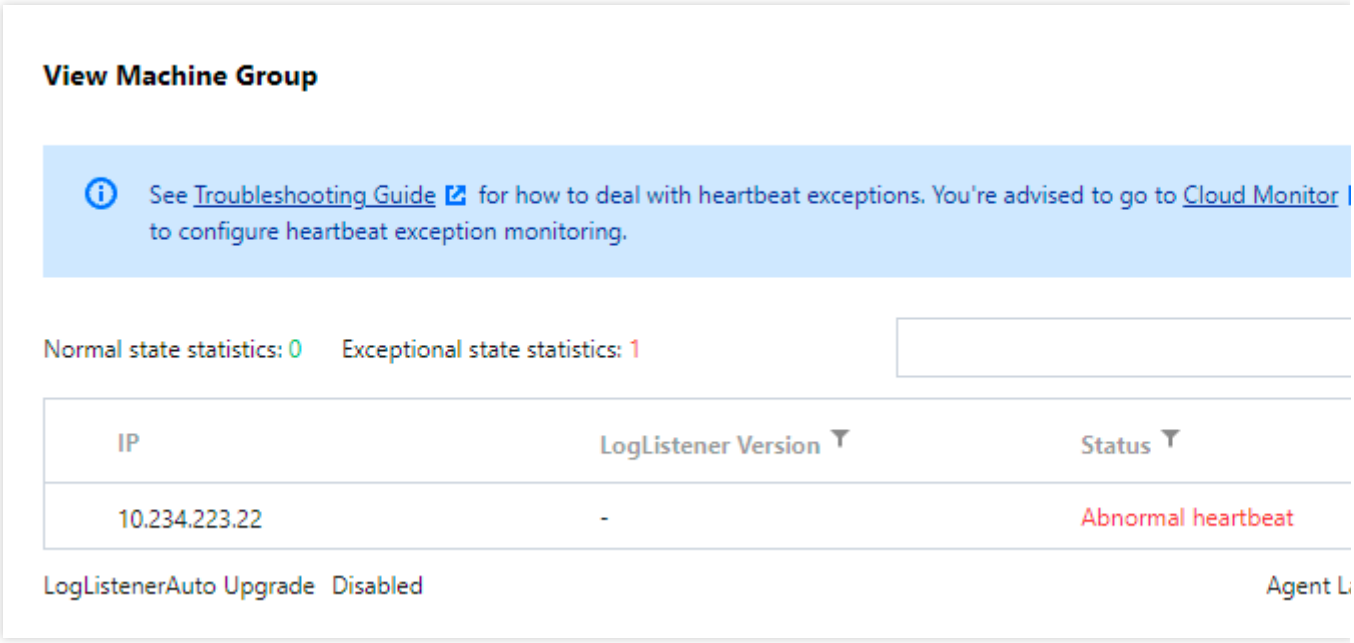
2. 检查机器组 IP 配置

检查机器组所添加的 IP 地址是否为 LogListener 安装过程中获取的 IP 地址。检查 LogListener 配置的 IP 地址：



```
grep group_ip etc/loglistener.conf
```

登录 日志服务控制台，单击**机器组管理**，查看机器组配置的 IP 地址，机器组所配置的 IP 地址必须与 LogListener 获取的 IP 地址完全一致。



LogListener 常见问题

最近更新时间：2024-01-20 17:11:57

为何单个文件不支持上报至多个 topic？

LogListener 采集程序的策略是，单个文件，只能上传至一个 topic。
例如，您有 topicA 和 topicB 两个文件，并对这两个文件进行如下设置。
设置 topicA 的采集路径为：/data/log/**/*.log
设置 topicB 的采集路径为：/data/log/test/**/*.log、/data/log/**/test*.log、/data/log/**/*.log，或者其他与 topicA 采集路径类似的路径。
此场景的配置，虽对应到两条采集路径交集的文件，但只会将数据上传至其中一个 topic 中。因此，我们建议针对不同的日志主题，应承载不同业务类型的日志，并在设置采集配置路径时，尽量精确配置信息。如果仍需要将某一个文件上传至不同的 topic，可使用软链接实现。对同一个采集目标创建不同的软链接，不同的 topic 分别采集不同的软链接路径/文件。

如何进行采集路径的设置？

目前采集路径的配置为：路径前缀+ “/**/”+通配文件名的形式。例如：/data/log + /**/ + *.log ==> /data/log/**/*.log。
由于设置通配采集路径时，需要将采集路径（前缀部分）设置的尽量准确，从而使采集器能够更有效率的提供服务。如果采集路径前缀部分设置不准确，可能会导致采集路径匹配到的路径数量巨大，从而造成采集器进入异常转台，无法工作。
例如，采集路径设置为：//**/*.log，其前缀部分为"/"，这种情况下采集程序会扫描整个根目录，导致采集程序无法工作。

推荐的日志轮转方案是什么？

对于日志的轮转，推荐方式为轮转后的文件名，不要被采集通配路径覆盖到。
例如，配置的采集路径是 /var/log/xxxx/**/*.log，需要采集的日志是 test.log。当 test.log 轮转成 test.2021-07-13.4.log 时，LogListener 能够识别 test.2021-07-13.4.log 是 test.log 的轮转文件，对它仍按照 test.log 来标记。因此，LogListener 保存的位点文件中，没有 test.2021-07-13.4.log 这个文件的采集记录。
而当 LogListener 重启后，LogListener 会按照 /var/log/xxxx/**/*.log 去扫描文件，并发现 test.2021-07-13.4.log 文件符合匹配规则，且没有采集记录，是一个新文件，然后重新采集。
所以建议，采集通配路径不要匹配到轮转文件，避免造成重启后重新采集轮转文件。
我们推荐的日志轮转方案是，如果您需要采集 test.log，建议将轮转后的文件名命名为 test.log.2021-07-13.xxx，可以有效不被 *.log 覆盖到。

LogListener 升级说明？

在 LogListener 迭代过程中，采集路径的接口参数做过变更，比较老的版本（ver< 2.2.8）设置的采集路径，在新版本中不再被支持。

版权所有：腾讯云计算（北京）有限责任公司

因此，如需对存量老版本（ver < 2.2.8）进行升级，在采集程序升级之后，需要在控制台重新以通配路径的方式，再次设置采集路径。

LogListener 采集配置如何使用正则采集模式？

在控制台设置采集配置时，如果选择正则相关的采集模式，控制台虽提供正则 kv 提取小工具，但此工具暂不提供对中文内容的正则自动生成功能。如需对中文文本进行正则提取，可以自行编写正则表达式，在控制台进行验证，或者使用其他第三方工具进行验证。

初次使用 LogListener 采集器接入时，发现无日志上传，怎么办？

可能是采集器配置不正确导致，常见情况如下：
配置的服务端域名不匹配，采集器拉取不到当前地域的采集配置，无采集业务进行。
采集器加入了 IP 机器组，但是采集器中又配置了标签 label 信息，导致在当前地域拉取不到采集配置，无采集业务进行。
采集器中配置的 secret ID/KEY 不正确，或者权限不足，导致无法上传日志。
环境问题（如 VPC 子网内，外网未开启），如果配置了跨地域上传，是不生效的，采集器实际上还是与本地域服务端进行通信。
通常这种情况下，可以登录采集器所在机器，进入采集器安装目录，并执行 `./bin/check` 命令，检查如下内容：
域名是否正确。
心跳上报是否正常。
采集配置是否正确拉取。

机器组使用混用，导致采集不采集，怎么办？

目前机器组分为两类，其使用方法相互独立：
IP 机器组，机器 IP 需要在控制台上手动加入机器组，对应机器上 loglistener.conf的group_label 需为空。
标签机器组，控制台设置机器组标签，对应机器上 loglistener.conf的group_label 需要设置为相同的标签。
如上两种用法不兼容，如果混合使用，采集机器将拉取不到正确的采集配置，造成不采集的现象。

LogListener 的采集策略是什么？

一堆文件排队进行 LogListener 采集时，队首文件先采集，且要求其在某个时刻读取到文件尾才会让出队首位置。
即：不是每个文件在单位时间内，都能均等的享受采集资源。
当单个文件始终写入大于采集速度，且采集速度慢导致始终消费不到文件最新位置时，会出现某个文件长时间或一直霸占采集资源，从而导致其他的文件无法进入采集流程。

Topic 采集阻塞严重怎么办？

在某段时间内，如果单个文件的产生速度大于采集速度，LogListener 会持续一直在采集这一个文件，陷入了对其他文件的采集阻塞场景。

过滤器的规则是什么？

过滤器的规则是匹配后采集，而不是匹配后丢弃。对于未能匹配的日志，LogListener 将不会进行采集。

如何使用非 root 权限启动 LogListener？

建议用户使用 root 权限安装启动。如需在非 root 权限下使用 LogListener，可以参考设置非 root 权限启动 LogListener。

如何对 LogListener 的进程进行绑核？

使用 taskset 工具进行绑核，`taskset -cp ${cpu number} ${pid>}` 。

如何处理 LogListener 占用内存过高，控制资源的使用？

建议升级到最新 LogListener 版本，并设置 `memory_tight_mode = true` 。
使用 CGroup 限制 CPU 和内存使用。

LogListener 是否支持软链接方式采集？

LogListener 低于2.3.0版本不支持监听软连接方式的日志文件和 NFS、CIFS 等共享文件目录上的日志文件，以上版本均可支持。

LogListener 可以向多个日志主题上传数据吗？

LogListener 可以为同地域的多个日志主题采集数据，但不支持为异地多个日志主题采集。
同一个日志文件只支持采集到一个主题。

LogListener 初始化的时候是否可以自动加入机器组？

标识机器组机支持, 参考文档 管理机器组。

LogListener 日志上传策略是什么？

缓存的日志量超过4M。
缓存的日志条数超过10000条。
读到文件末尾。

LogListener 支持的最大性能是多少？

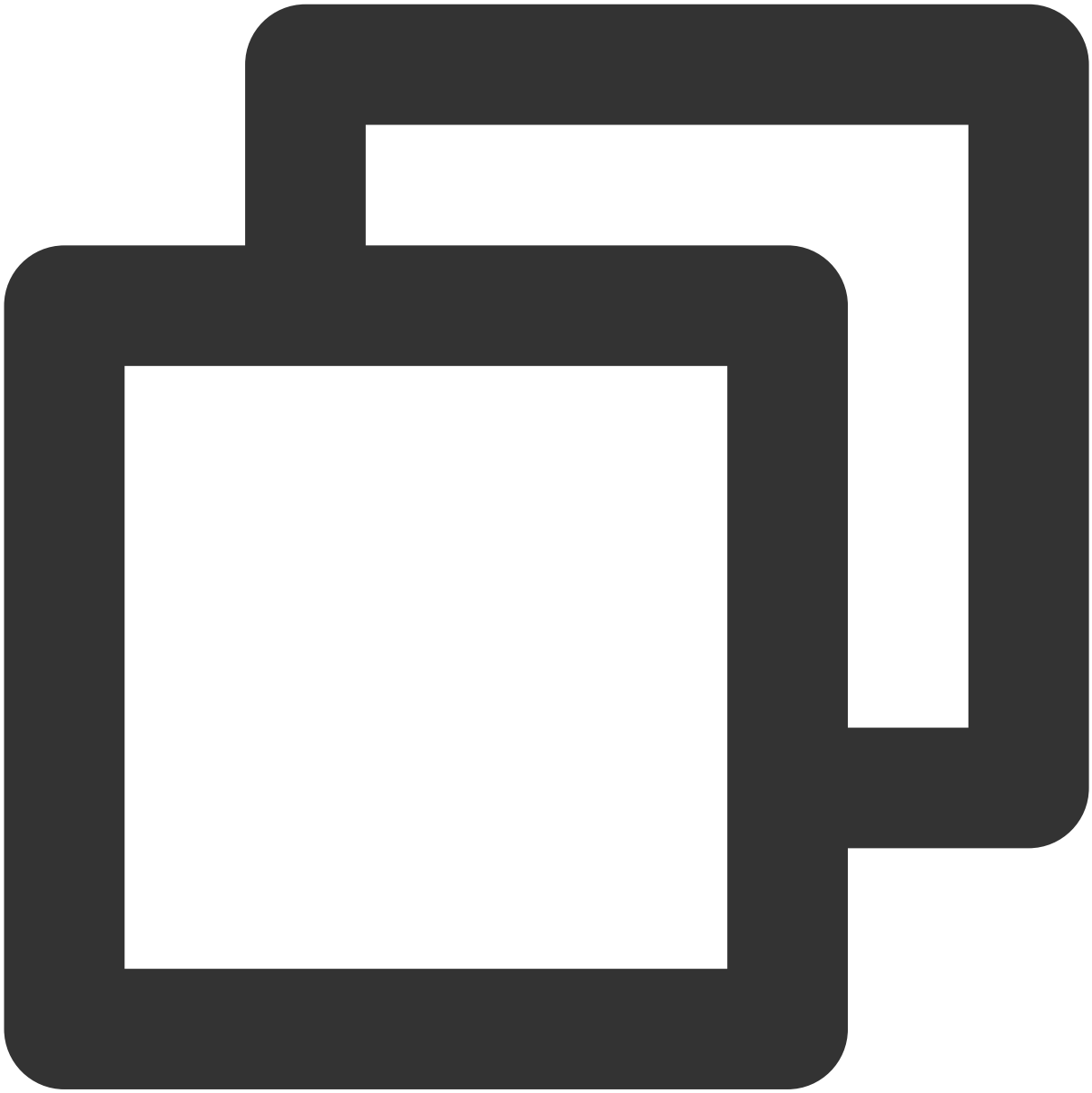
单行全文日志最大处理能力为115MB/s。
多行全文日志最大处理能力为40MB/s。
JSON 格式日志最大处理能力为25MB/s。
CSV 格式日志采最大处理能力为50MB/s。
完全正则格式日志最大处理能力为18MB/s (和正则的复杂度有关)。

服务器更换 IP 地址后，LogListener 应该如何适配？

若服务器通过机器标识绑定机器组，用户无需变更 LogListener 配置。若服务器 IP 需要频繁变更，建议用户使用 机器标识 配置机器组。

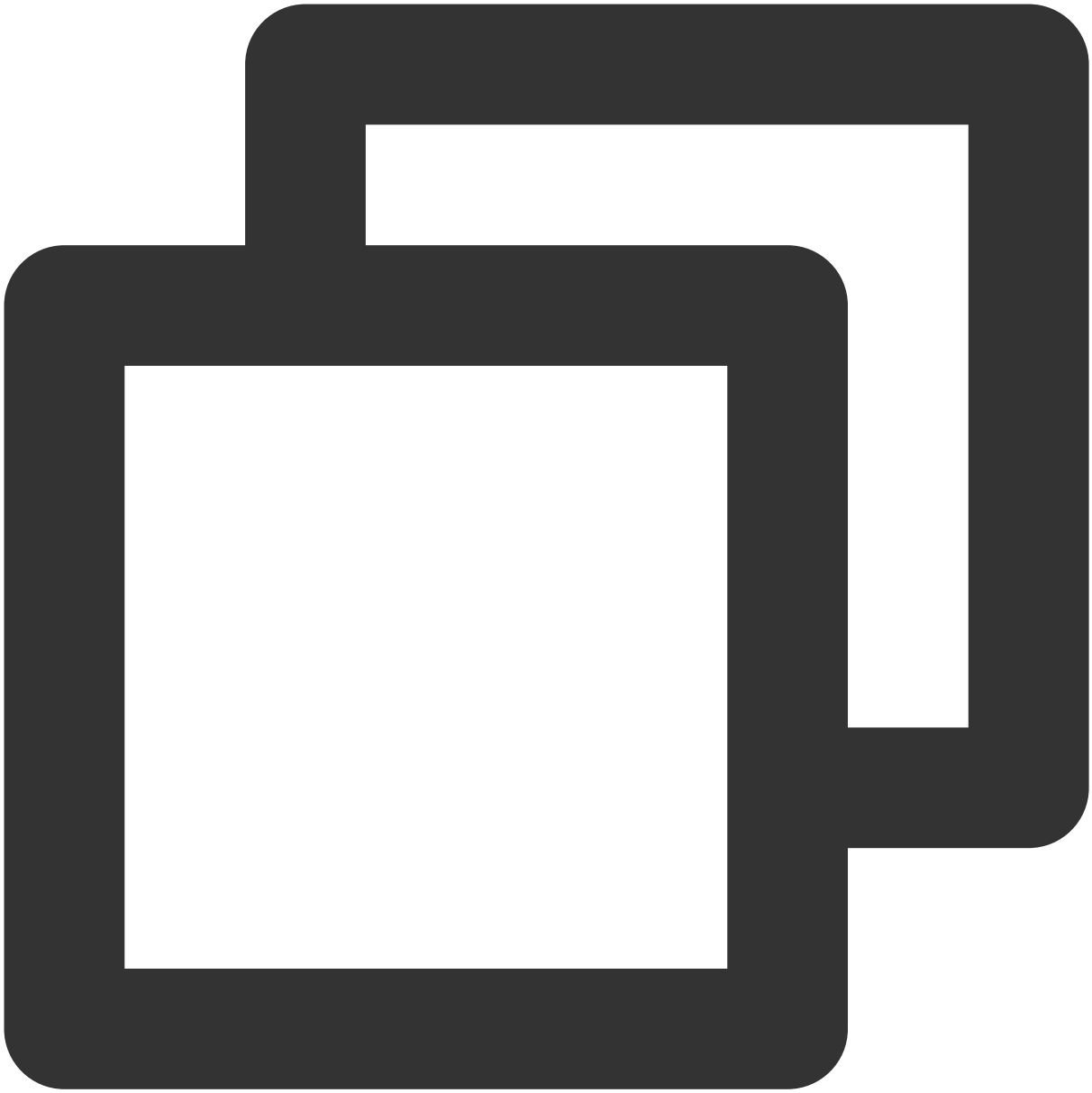
若服务器通过 IP 地址绑定机器组，用户需要完成以下配置变更：

a. 修改配置文件中 group_ip 选项，填入变更后的 IP 地址，例如：



```
sed -i '' "s/group_ip *=.*/group_ip = ${group_ip}/" etc/loglistener.conf
```

b. 重启 LogListener。



```
/etc/init.d/loglistenerd restart
```

c. 如果使用的是 IP 机器组，登录 日志服务控制台，在左侧导航栏中，单击**机器组管理**，修改该服务器绑定的机器组配置，使用新 IP 替换原机器 IP 地址并确定。

LogListener 安装异常问题

最近更新时间：2024-01-20 17:11:57

如何安装及使用日志服务 Loglistener，请参见 LogListener 安装指南 文档。

可能原因

以下原因可能会导致无法正确安装 Loglistener：

1. 内核版本仅支持64位。
2. 安装方式出错。
3. 最新特性功能依赖较高版本 Loglistener。

处理步骤

1. 确认内核版本。

Loglistener 安装目录下的 bin 目录中的可执行文件只支持 Linux 64位内核，执行命令 **uname -a**， 确认内核版本是否为 x86_64。

2. 确认安装执行命令是否正确。

具体请参见 LogListener 安装指南 文档进行操作。

3. 确认 Loglistener 版本。

日志服务最新特性可能依赖新版 Loglistener，若确认是使用新特性异常，请下载 Loglistener 最新版本。LogListener 下载及详细安装步骤请参见 LogListener 安装指南。

4. 验证 LogListener 成功安装。

参考如何使用 LogListener 快速诊断工具 检查 LogListener 进程、心跳和拉配置是否正常。

版权所有：腾讯云计算（北京）有限责任公司

容器日志采集常见问题

最近更新时间：2024-01-20 17:11:57

安装与升级相关

如何在 TKE 集群中部署日志采集组件？

1. 登录 容器服务控制台。
2. 在左侧导航栏中，单击**运维功能管理**，进入功能管理页面。
3. 找到待操作的集群，单击**设置**。
4. 在弹出的窗口中，单击**日志采集**栏的**编辑**。
5. 勾选**开启日志采集**，单击**确定**。
6. 单击**关闭**。

如何在 TKE 集群中升级日志采集组件？

1. 登录 容器服务控制台。
2. 在左侧导航栏中，单击**运维功能管理**，进入功能管理页面。
3. 找到可升级组件的集群，单击**设置**。
4. 在弹出的窗口中，单击**日志采集**栏的**编辑**。
5. 单击**升级组件**。

网络与权限相关

云 API 域名不通，怎么办？

容器服务（Tencent Kubernetes Engine，TKE）日志采集组件和日志服务（Cloud Log Service，CLS）通信的组件 cls-provisioner 使用腾讯云 API 域名，需要保证域名的可连通性。如果存在组件部署失败等问题，并在日志中看到有如下图所示报错，即表示网络域名不通。

如上图所示，cls-provisioner 启动异常。通过查看日志发现，cls.internal.tencentcloudapi.com 域名不通。
在腾讯云上的机器，默认腾讯云的内外网域名都是联通的。通常导致此类问题的原因是 TKE 节点的 DNS 配置被修改过，您可通过如下两种方法进行修复：

TKE 节点机器的 DNS 配置添加腾讯云默认 DNS。

如果宿主机上的 DNS 是服务器是 core-dns，在 coredns 上添加腾讯云 DNS 解析即可。

说明：

建议在 TKE 集群中遇到域名不通的问题优先检查 TKE 节点 DNS 配置。

CLS 日志上传域名不通，怎么办？

日志上传的域名和云 API 域名不同，日志上传的域名为 `<region>.cls.tencentcs.com`（外网）和 `<region>.cls.tencentyun.com`（内网），更多详情请参考 域名 文档。

修复方案：

在集群节点机器打通域名的访问。

在 cls-provisioner 和 CLS 的通信中提示未授权，怎么办？

在 cls-provisioner 和 CLS 的通信中，一般会有类似如下的报错：

修复方案：

在创建 TKE 集群的账号下，预设策略。即在 TKE_QCSRole 角色中关联 QcloudAccessForTKERoleInOpsManagement 策略。

采集相关

采集到 CLS 的日志被截断了，怎么办？

在某些情况下，用户日志的输出类型是标准输出，但采集到 CLS 的日志发现被截断了。因为 Docker 的默认日志存储 json-tool，对单行日志大小有限制，所以超过16K的日志会进行截断。

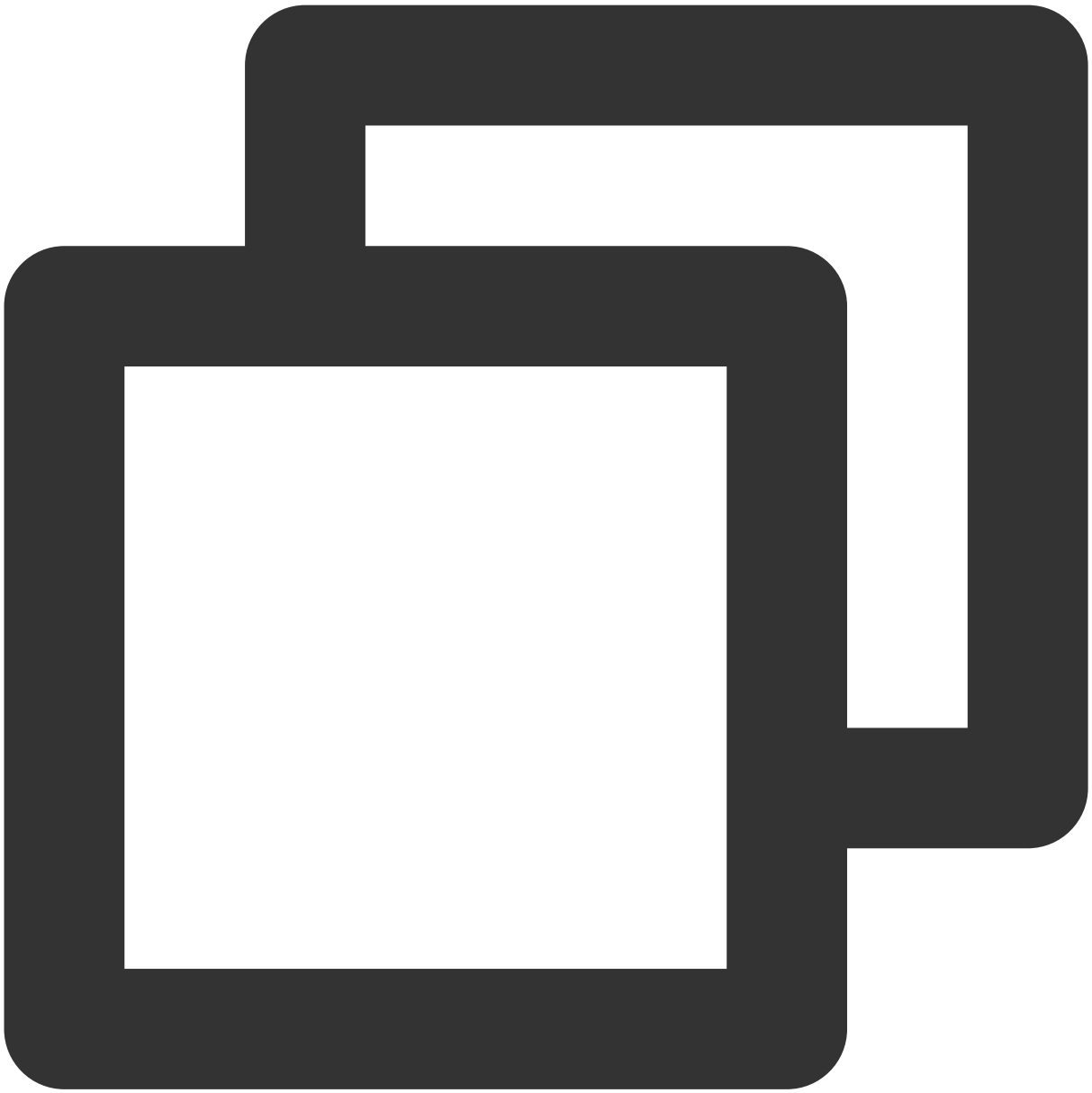
修复方案：

修改日志输出，单行日志打印不要超过16K。

日志重复采集，怎么办？

用户通过 CLS 控制台检索，发现有些日志出现了重复采集。此时，可以优先检查日志输出的路径，确认日志是否输出到 PV/PVC 创建的持久化存储上。

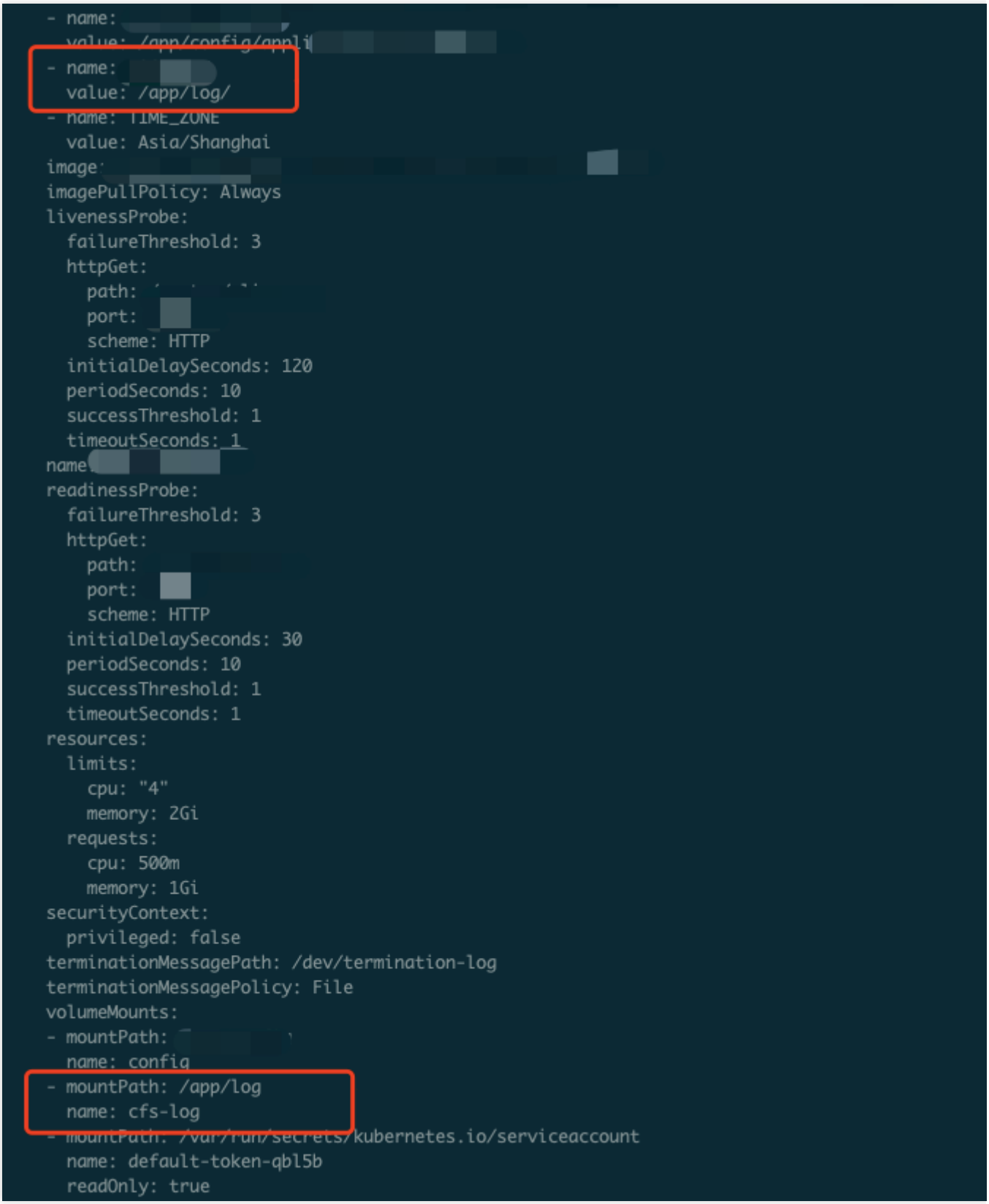
如果日志输出到持久化存储上，当业务 Pod 重建时，会导致日志会被重新采集。可以使用如下命令，查看 Pod 的 yaml 定义：



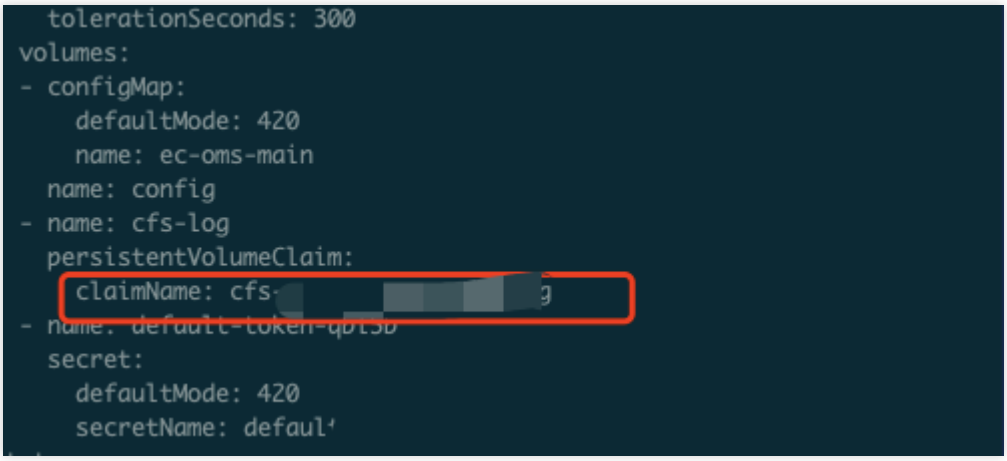
```
kubectl get pods <pod_name> -n <namespace> -o yaml | less
```

返回类似如下信息即表示日志输出到持久化存储上。

业务使用了 CFS，且 CFS 挂载到容器上。


- name:
value: /app/config/appli
- name:
value: /app/log/
- name: TIME_ZONE
value: Asia/Shanghai
image:
imagePullPolicy: Always
livenessProbe:
failureThreshold: 3
httpGet:
path:
port:
scheme: HTTP
initialDelaySeconds: 120
periodSeconds: 10
successThreshold: 1
timeoutSeconds: 1
name:
readinessProbe:
failureThreshold: 3
httpGet:
path:
port:
scheme: HTTP
initialDelaySeconds: 30
periodSeconds: 10
successThreshold: 1
timeoutSeconds: 1
resources:
limits:
cpu: "4"
memory: 2Gi
requests:
cpu: 500m
memory: 1Gi
securityContext:
privileged: false
terminationMessagePath: /dev/termination-log
terminationMessagePolicy: File
volumeMounts:
- mountPath:
name: config
- mountPath: /app/log
name: cfs-log
- mountPath: /var/run/secrets/kubernetes.io/serviceaccount
name: default-token-qbl5b
readOnly: true

使用了 CFS 声明



修复方案：

如果日志不需要保存在持久化存储上，可以在容器集群中开启日志采集，即可将日志采集到 CLS 内。

如果需要将日志文件保存在持久化存储上，可以在 CLS 控制台中配置 LogListener 采集规则时，将采集策略修改为**增量**采集，但是增量采集不保证会采集到全部日志。

日志漏采集，怎么办？

Loglistener 当前不支持保存在 NFS 上的日志。Loglistener 获取文件的更新信息是通过订阅 Linux 内核事件来的，并不是主动去扫描目标文件。

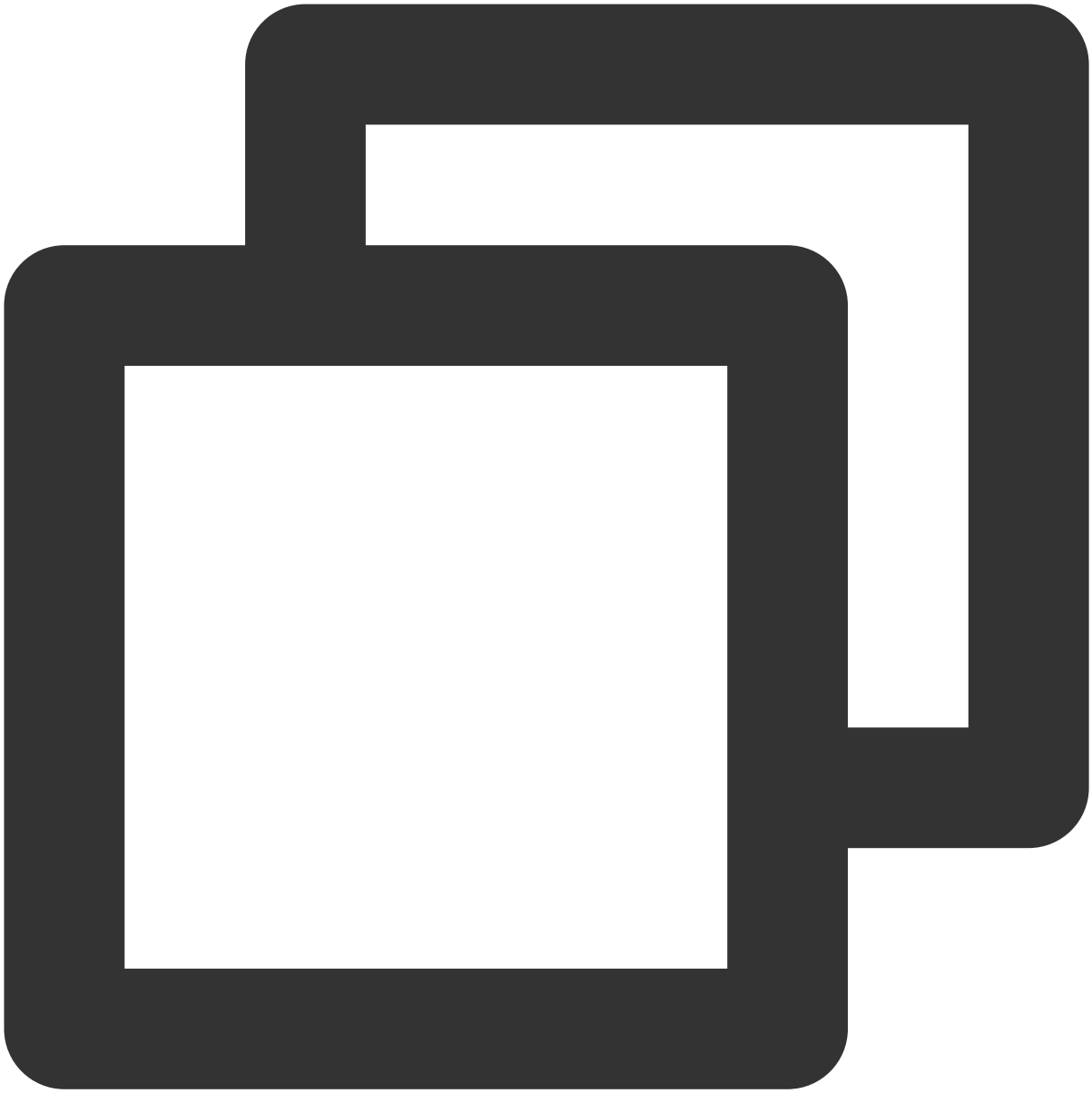
NFS 文件更新信息是在 NFS 服务端完成，无法在 client 本地的内核产生事件，因此无法被感知，所以 NFS 文件无法实时采集，会存在漏采集。

采集配置与 Pod 不匹配，怎么办？

您可以通过如下操作进行排查：

1. 使用如下命令，确认 Pod 的 label 是否与采集配置匹配。

版权所有：腾讯云计算（北京）有限责任公司

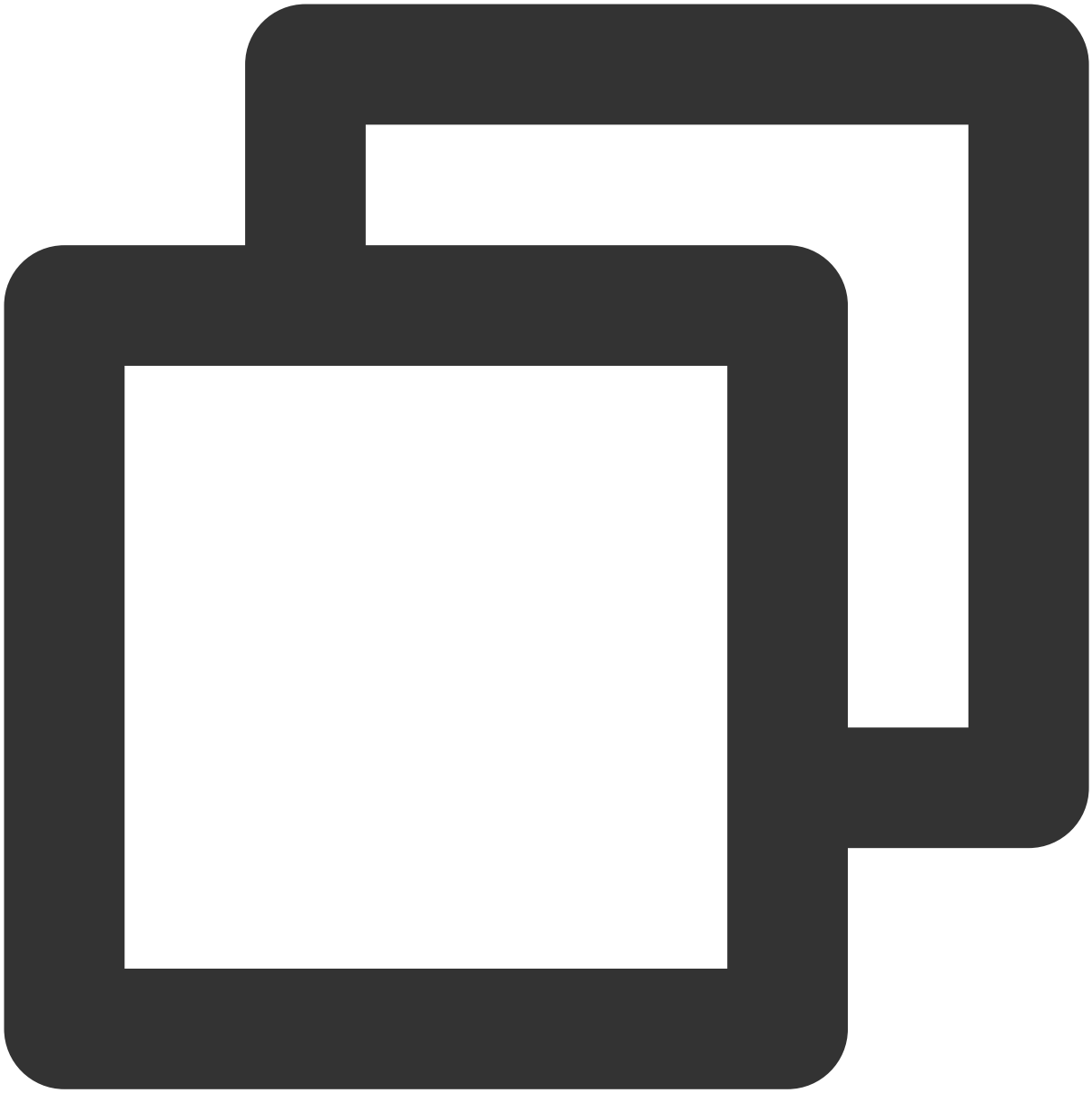


```
kubectl get pods <pod_name> -n <namespace> --show-labels
```

匹配，请执行下一步。

不匹配，请对照正确内容修改采集配置。

2. 检查 Pod 的 workload（Deployment 或者 statefulsets 等）是否和采集配置匹配。

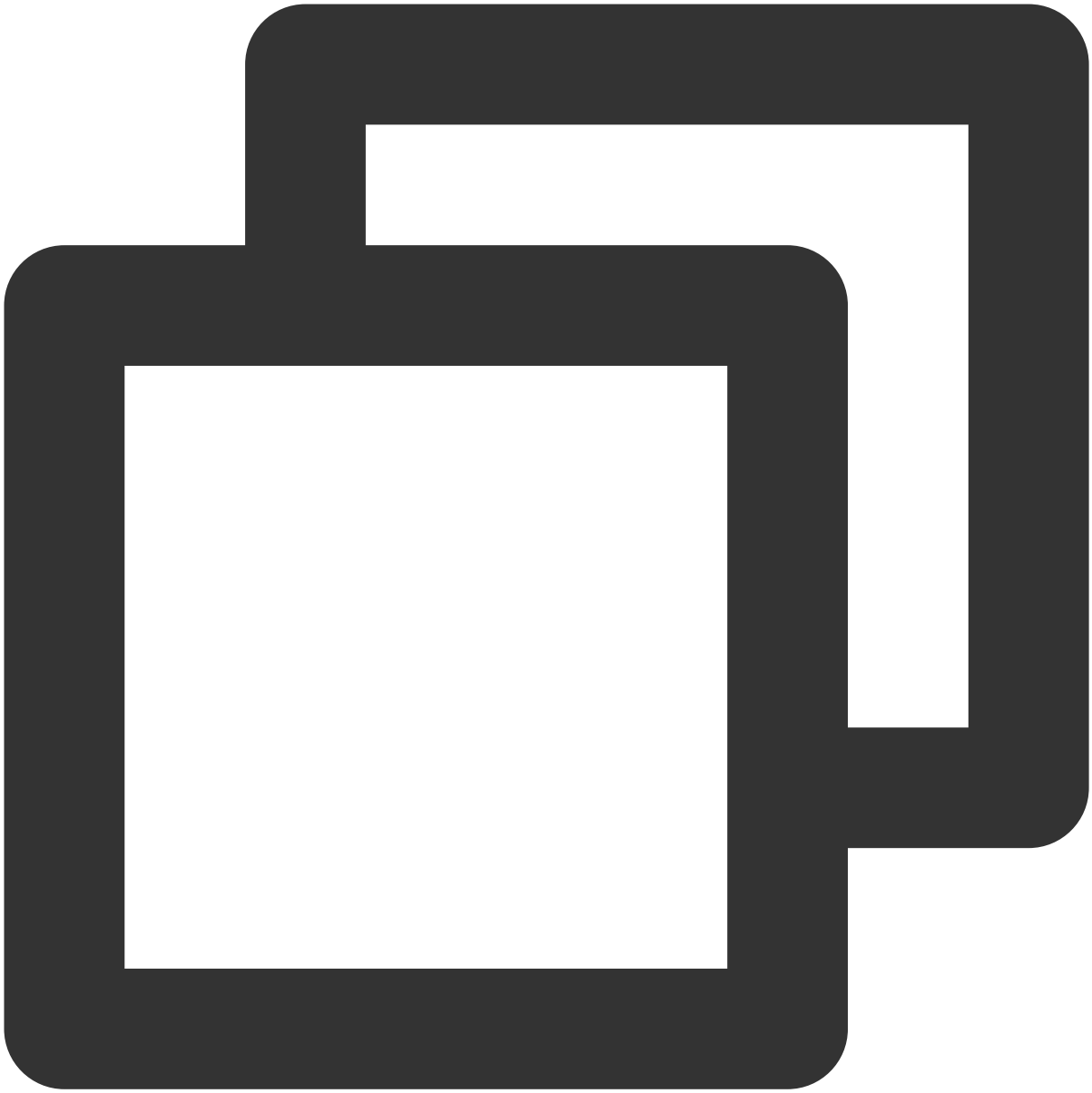


```
kubectl get pods -n <namespace> |grep testa
```

匹配，请执行下一步。

不匹配，请对照正确内容修改采集配置。

3. 使用如下命名，查看 Pod 的 yaml 定义，确认 container 的名字和采集配置中指定的容器名是否匹配。



```
kubectl get pods <pod_name> -n <namespace> -o yaml
```

匹配，任务完成。

不匹配，请对照正确内容修改采集配置。

采集路径不正确怎么办？

在采集容器文件或者采集宿主机文件的场景下，确认采集的目录路径正确，并且有符合采集规则的日志。

日志文件可以使用软连接吗？

容器文件的采集场景下，不支持匹配到的日志文件存在软连接的场景。

Kubernetes 场景下，**CLS 的实现是解析容器文件在宿主机的位置。由于容器中的软连接目标指向的是容器内的路径，如果匹配到的采集文件存在软连接，将不能正确可达。**

修复方案：

修改采集规则的路径和匹配文件，即采集日志文件实际所在路径和文件，避免匹配到软连接。

触发采集规格限制是什么？

由于 Loglistener 采集在容器场景下，资源收到限制，所以对监听的目录和文件有个数限制：

监控目录数：5000

监控文件数：10000

在采集容器文件或者采集宿主机文件场景下，可能会遇到此类问题。通常情况下，由于用户没有清理过期的日志文件，在查看 Loglistener 日志时，日志中有类似如下图信息：

对于超过最大限制的文件和目录，Loglistener 将不会纳入监听，导致有些用户预期内的日志文件没有采集。

更多详情请参考 资源与性能限制 文档。

修复方案：

在日志目录下，使用 `tree` 命令，查看整个目录下当前的目录数量和文件数量是否达到 Loglistener 限制。

如果没有达到限制，在业务容器所在宿主机的 /var/log/tke-log-agent 下执行 `tree -L 5`，检查整体机器粒度是否达到限制。

因为 Loglistener 的限制是机器粒度的，如果某一个容器文件数量没有达到阈值，但是可能整体机器粒度所有的容器文件达到限制。

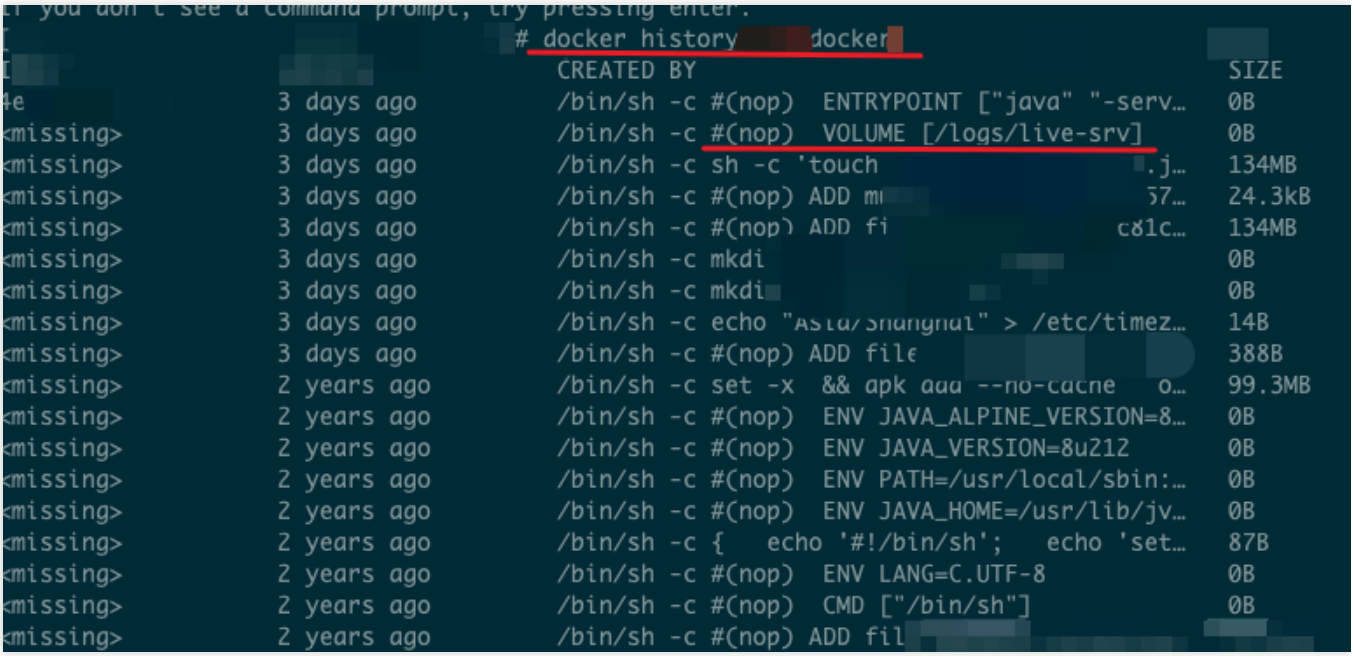
如果达到限制，请将过期日志及时归档，减少 Loglistener 监控的目录和文件所消耗的资源。

在 Dockerfile 定义了 volume，怎么办？

Docker 场景：使用 `docker history $image` 命令，查看镜像在构建信息。

Containerd 场景：使用 `crictl inspecti $image` 命令，查看镜像在构建信息。

返回如下信息，可以看出，在 Dockerfile 中，用户自定义了一个 volume /logs/live-srv，刚好是日志所在目录。该操作会干扰日志采集组件找到正确的日志文件。



修复方案：

修改 Dockerfile，去掉 volume，然后重新构建镜像，重新部署服务。

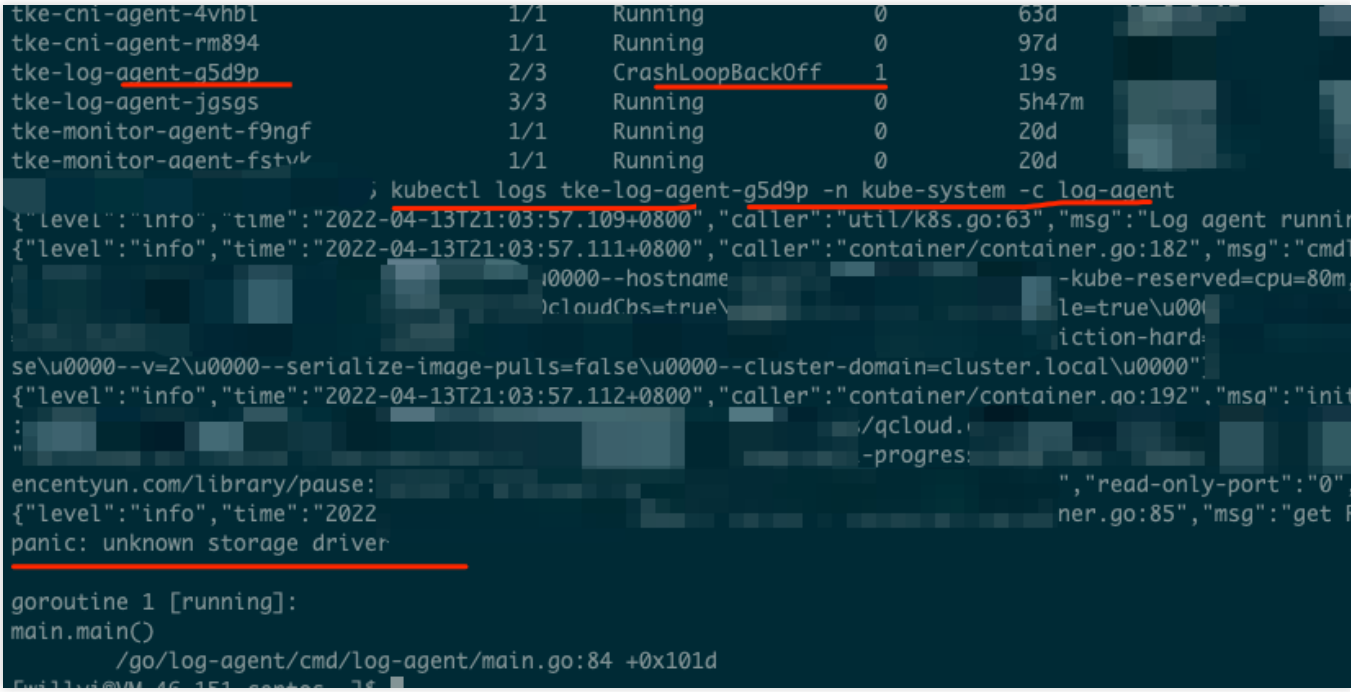
修改服务日志写入目录，不要写入 Dockerfile 中定义的 volume 路径中。

其他问题

容器引擎类型识别错误，怎么办？

在 Docker 场景下，一些场景会触发老版本的一些 bug，导致日志采集组件不能正常启动，出现 panic 日志。

其主要原因是由于用户自定义了 TKE 集群节点的 Docker 配置，从而导致出现如下图所示的错误：



修复方案：

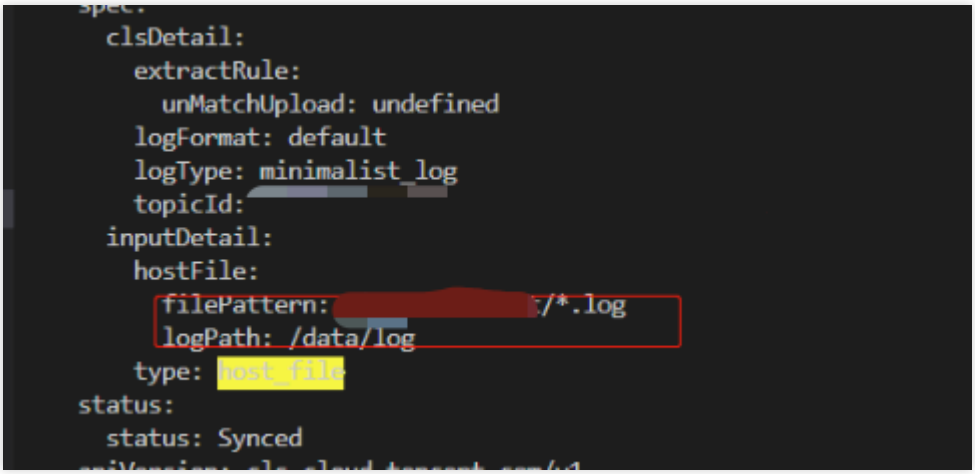
在 /etc/docker/daemon.json 配置中，添加 `"storage-driver": "overlay2"` 。如下图所示：

```
[root@VM-0-5-centos ~]# cat /etc/docker/daemon.json
{
  "bridge": "none",
  "debug": false,
  "default-runtime": "runc",
  "exec-opts": [],
  "exec-root": "",
  "graph": "/var/lib/docker",
  "group": "",
  "insecure-registries": [],
  "ip-forward": true,
  "ip-masq": false,
  "iptables": false,
  "ipv6": false,
  "labels": [],
  "live-restore": true,
  "log-driver": "json-file",
  "log-level": "warn",
  "log-opts": {
    "max-file": "10",
    "max-size": "100m"
  },
  "max-concurrent-downloads": 10,
  "registry-mirrors": [
    "https://mirror.ccs.tencentyun.com"
  ],
  "runtimes": {},
  "selinux-enabled": false,
  "storage-driver": "overlay2",
  "storage-opts": [
    "overlay2.override_kernel_check=true"
  ]
}
[root@VM-0-5-centos ~]#
```

在 TKE 控制台升级日志采集组件版本。因为新版本采集组件已经修复此问题，无需修改 Docker 配置。

filePattern 设置了子目录，怎么办？

如下图所示，用户在 filePattern 字段参数中设置了子目录。此操作会导致日志不能正常采集。



修复方案：

在 logPath 参数中设置日志文件目录，filePattern 中只设置文件类型参数，不设置子目录。

自建 K8S 日志采集排查指南

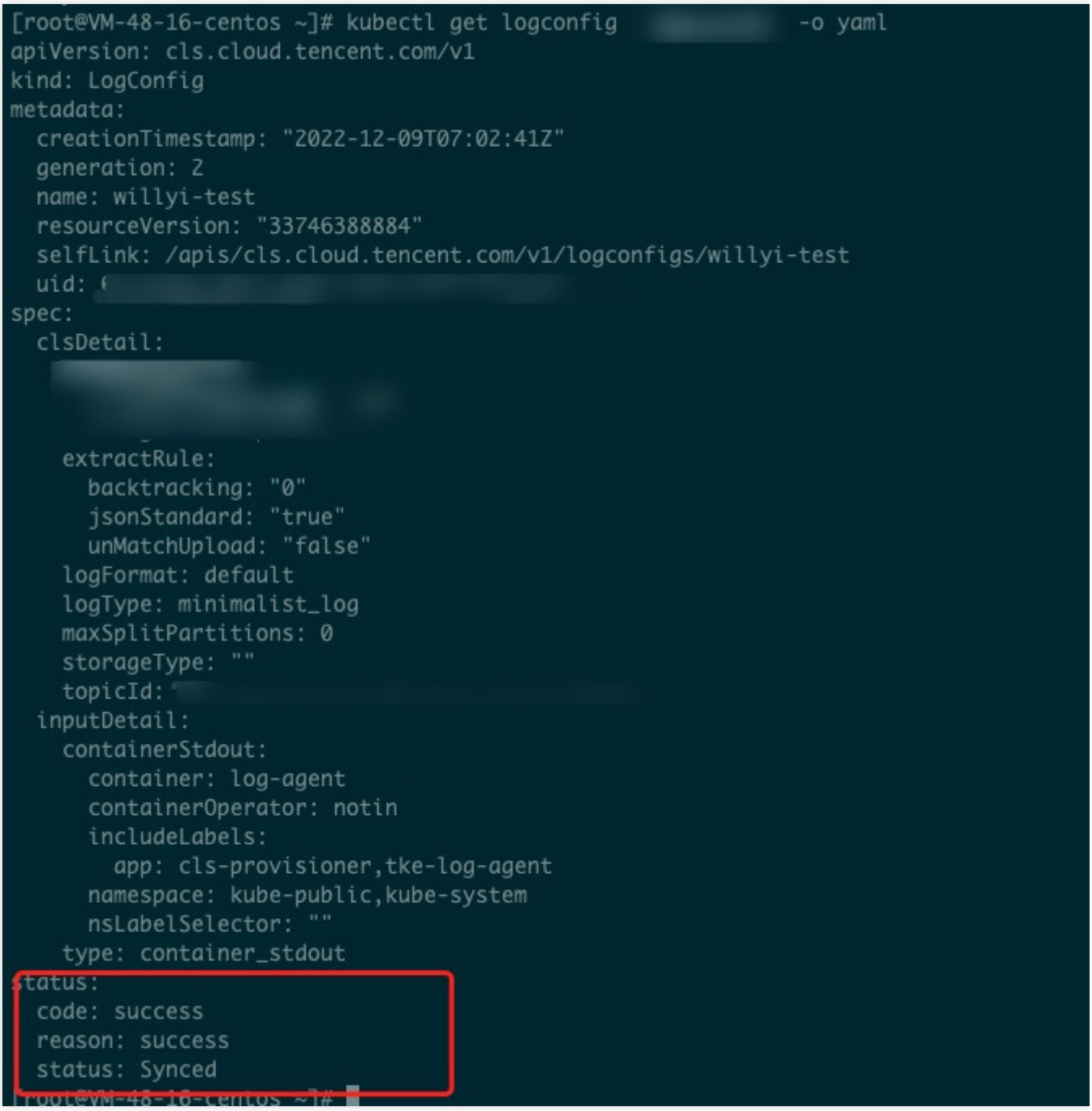
最近更新时间：2024-01-20 17:11:57

按照自建 K8S 集群安装 LogListener 部署完成后，就可以通过创建 LogConfig 或者通过控制台去设置采集配置，开始日志采集了
如果出现日志采集异常，首先按照下面的流程自查一下。

1. 确认 logconfig 状态

查看集群所有的采集配置：kubectl get logconfig
查看具体某一个采集配置： kubectl get logconfig xxx -o yaml
查看 logconfig 同步的状态，status 非 Synced 状态都是异常的，异常信息会在 reason 里面，正常都是 success 的状态。
如上 logconfig 的状态同步是成功的，那么采集异常的原因就是其他方面的。如下图所示:

版权所有：腾讯云计算（北京）有限责任公司



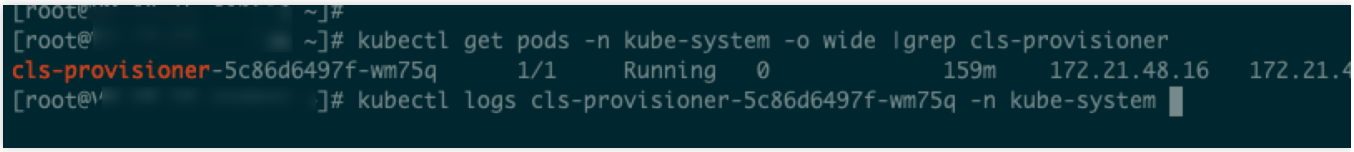
想要进一步了解同步错误的原因，可以看下 cls-provisioner 的日志。

2. 查看 cls-provisioner 日志

确定 cls-provisioner 的 Pod: kubectl get pods -n kube-system -o wide |grep cls-provisioner

查看日志: kubectl logs cls-provisioner-xxx -n kube-system

如下图所示：



查看 cls-provisioner 的日志，来看同步错误的具体原因。

注意：

cls-provisioner 组件的作用是和 CLS 服务端通信，将 logconfig 采集配置经过转换，同步到 CLS 服务端，这样采集器才能从服务端获取到采集配置，进而进行正常日志采集。

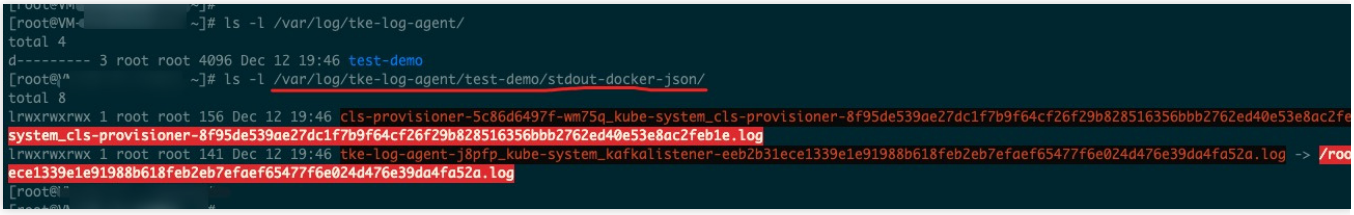
3. 查看采集端日志

如果采集配置同步正常，但是日志还是采集有异常，可以具体看下采集端的相关日志。

查看软连是否建立成功。

我们以采集标准输出为例：

会在 /var/log/tke-log-agent/<采集配置名称(logconfig 名称)>/stdout-docker-json 下创建需要采集的 Pod 的标准输出日志的软连，创建好之后才能正常采集。

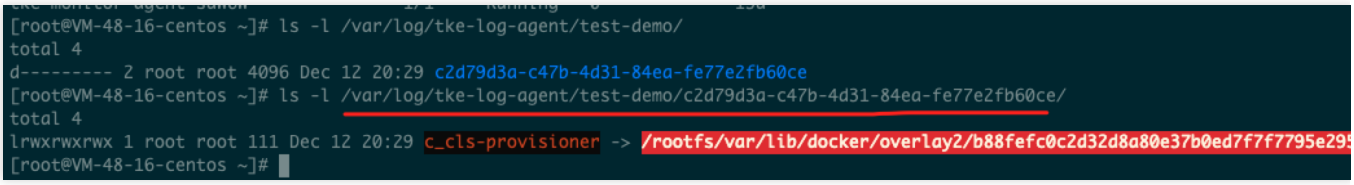


我们是以 Docker 为例的，如果 runtime 是 containerd，那么路径是/var/log/tke-log-agent/<采集配置名称(logconfig 名称)>/stdout-containerd。

采集 container file 的软连建立方式如下：

/var/log/tke-log-agent/<采集配置名称(logconfig 名称)>/

如下图：



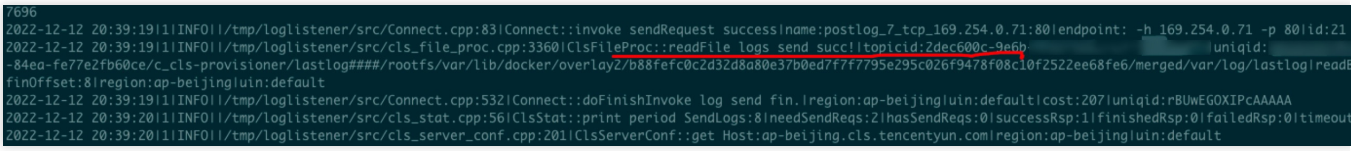
确认按照上面示例的软连是否建立 OK，如果未建立，则是有异常的。如果建立成功，则要继续看下采集器 loglistener 的日志。

查看采集器 loglistener 日志。

kubectl get pods -n kube-system -o wide |grep tke-log-agent

首先找到日志采集异常 Pod 对应宿主机上的 tke-log-agent 的 Pod，然后查看 loglistener 日志

kubectl logs tke-log-agent-xxx -n kube-system -c loglistener



确定是否有如上图所示类似 **readFile logs send succ!|topicid** 的字样，如果有，则表示日志成功采集到对应的 topic 了；如果没有如上的字样，那说明采集有问题，可以联系相关研发人员。

如果已经采集到了 topic，但是检索不到，可以先看下是否打开 topic 的全文索引。

版权所有：腾讯云计算（北京）有限责任公司

检索分析相关
检索不到日志

最近更新时间：2024-01-20 17:11:57

检索日志时，可能会出现检索不到日志的状态异常。出现该状态异常时，可通过以下几种方式排查问题。

确认检索条件

检索不到日志，很多情况下是检索时间范围不正确或检索语句有问题导致。用户先选择较大时间范围（如最近30分钟），检索条件为空，确定是否有日志。
如果检索数据成功，则可能是检索语句或者时间范围有误导致，建议用户查看 检索语法 或修改检索时间范围。

检查索引配置

索引配置是使用日志服务进行检索分析的必要条件，单击检索页右上方**索引配置**入口，查看索引配置是否开启。索引配置区分全文索引和键值索引，详情可参见 索引介绍 文档。
注意：
索引配置仅对新写入数据生效，每次更改索引配置，约有1分钟生效延时。

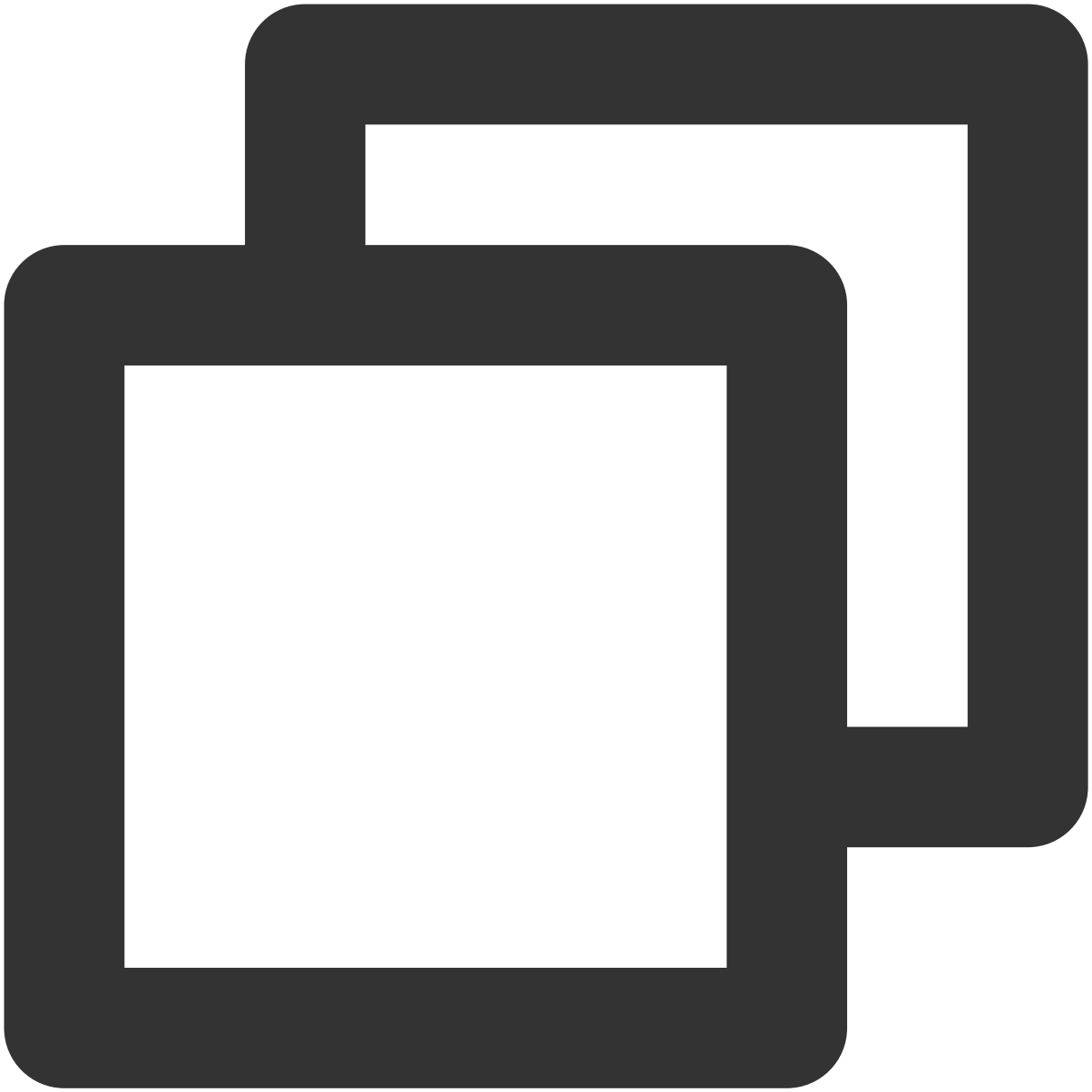
确认日志采集是否成功

云产品日志采集

若您的日志是其他云产品日志，如容器 TKE，负载均衡 CLB 等，可参见 云产品日志采集指引 确认是否配置成功，如有问题，请联系 在线客服。

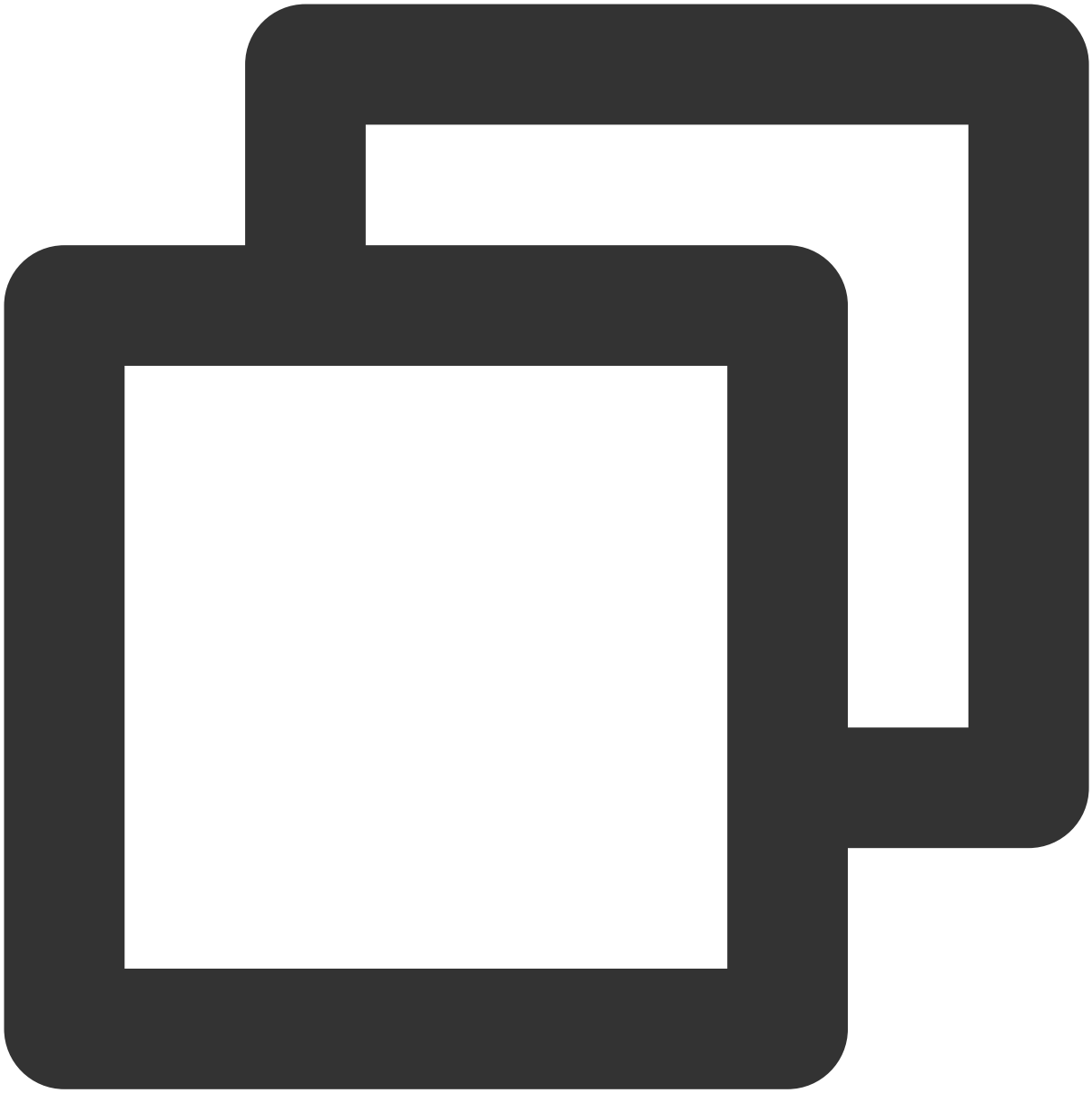
使用 LogListener 客户端采集日志

若您是通过 CLS 提供的日志采集客户端 LogListener 采集日志，可按以下步骤排查：
1. 检查机器组状态。
单击检索页右上角**LogListener 采集配置**，确认待采集机器状态是否正常。
注意：
若待采集日志的机器状态异常，请参见 机器组异常排查 文档。
2. 检查 LogListener 是否成功拉取采集配置
在命令行下执行如下命令：



```
/etc/init.d/loglistenerd check
```

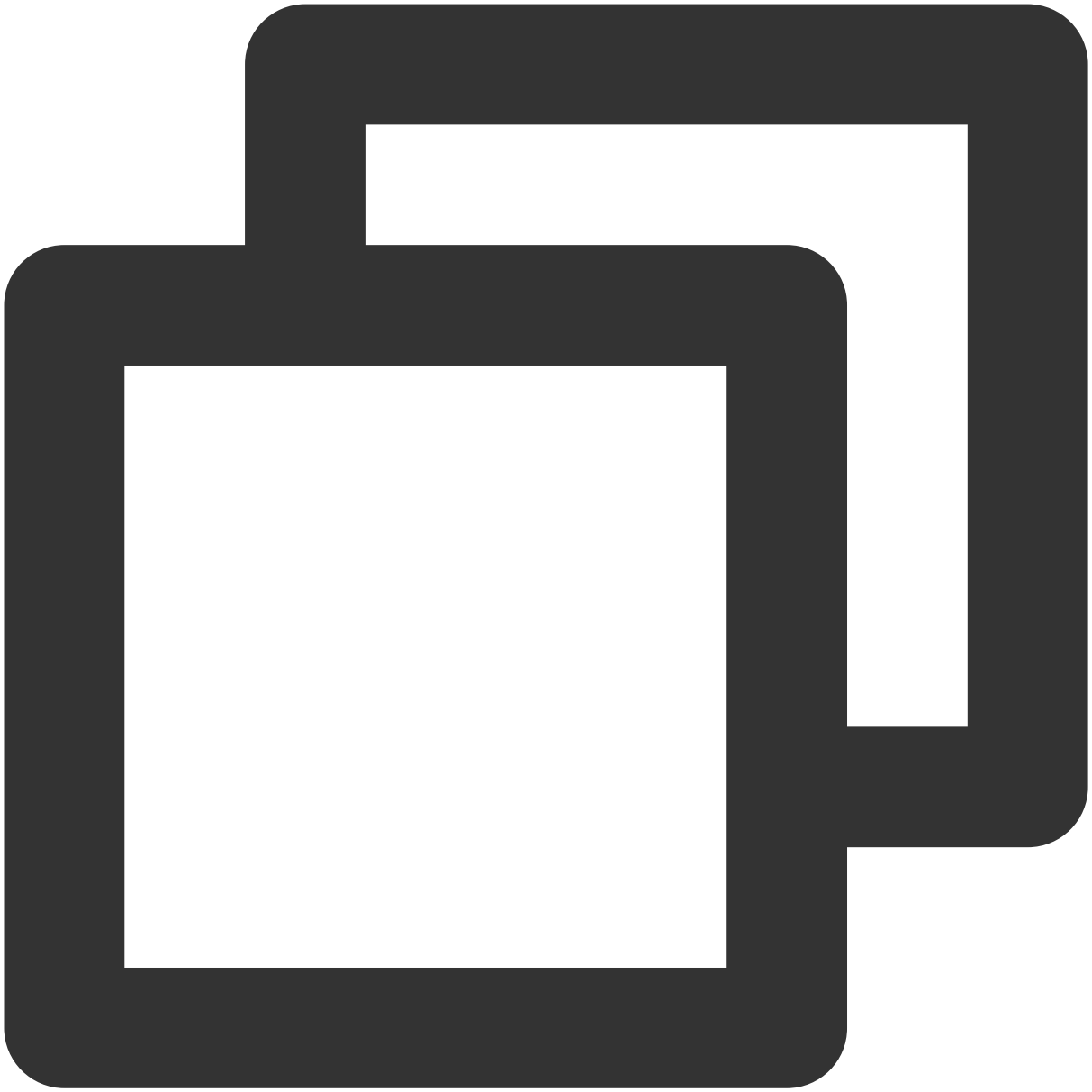
版权所有：腾讯云计算（北京）有限责任公司



如果出现如下图所示“[OK] check loglistener config ok”表示调用拉取配置接口成功。

返回结果中的 `logconf` 字段为采集配置，如果为空表示没有拉取到对应的采集配置，参考 [LogListener

3. 尽可能确保是最新版本的 LogListener。
执行以下命令，查看版本号。当前最新版本可查看 LogListener安装 文档。



```
/etc/init.d/loglistenerd -v
```

注意：

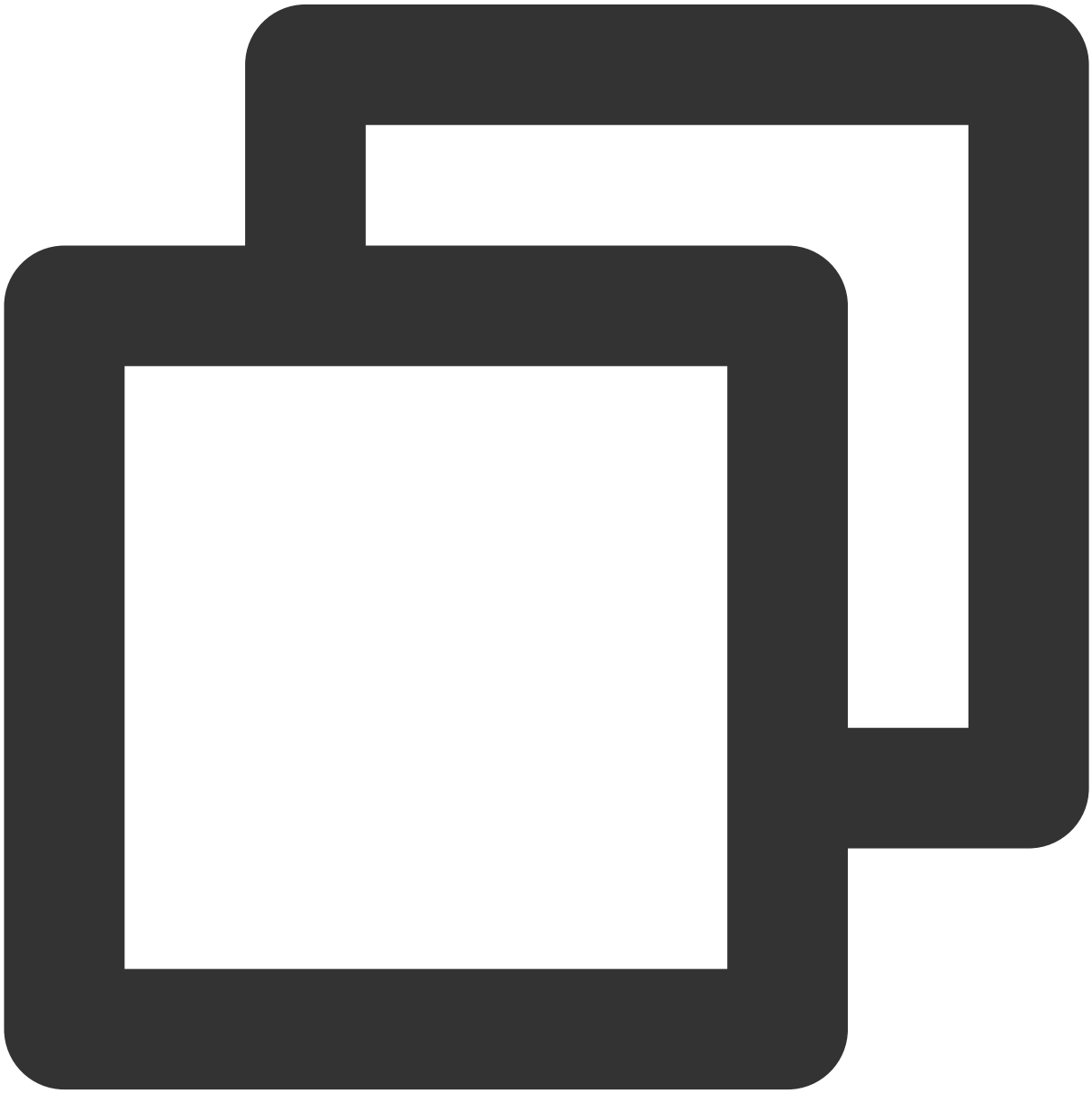
LogListener 低于2.3.0版本，不能监听软连接方式的日志文件。

4. 确认日志上报成功。

4.1 打开 LogListener Debug 日志， 在 LogListener 安装目录下编辑 `etc/loglistener.conf` 配置文件，将 **level** 设置为 DEBUG，并重启 LogListener。

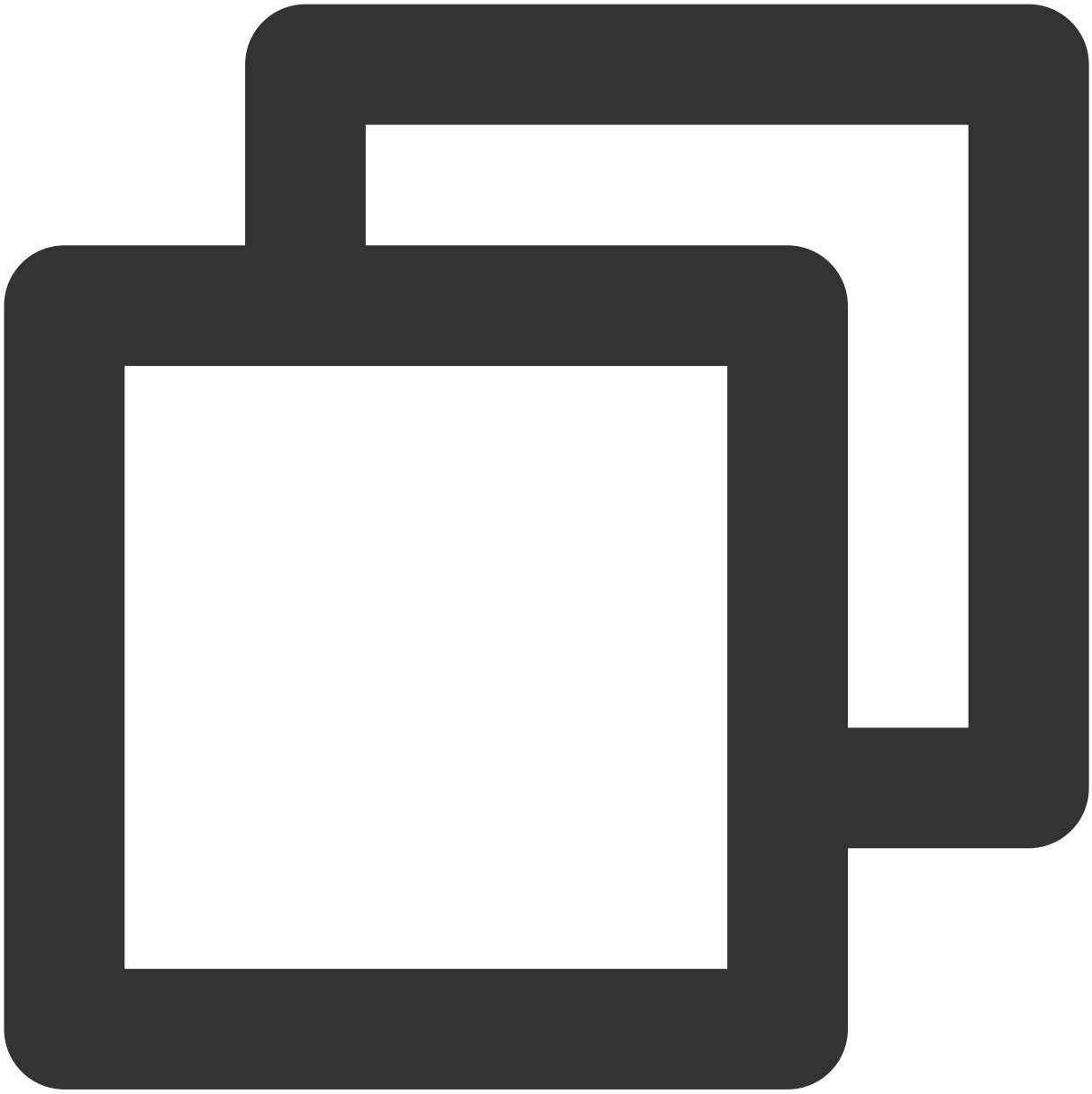
```
<log>
    level   = DEBUG
    path    = log/
    name    = loglistener
    size    = 10000000
    num     = 10
</log>
```

4.2 执行如下命令，重启 LogListener。



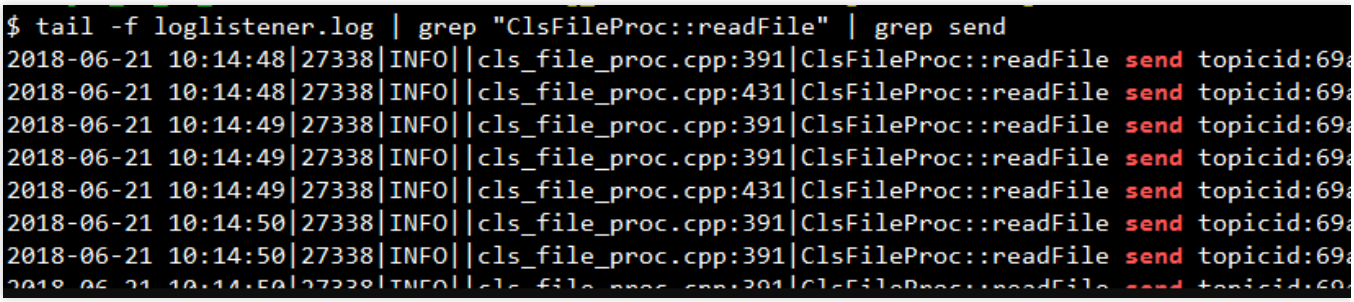
```
/etc/init.d/loglistenerd restart
```

4.3 执行以下命令，查看日志是否成功上报：



```
tail -f log/loglistener.log | grep "ClsFileProc::readFile" | grep send
```

如果日志成功上报到服务后台，则会出现类似下图所示的日志：

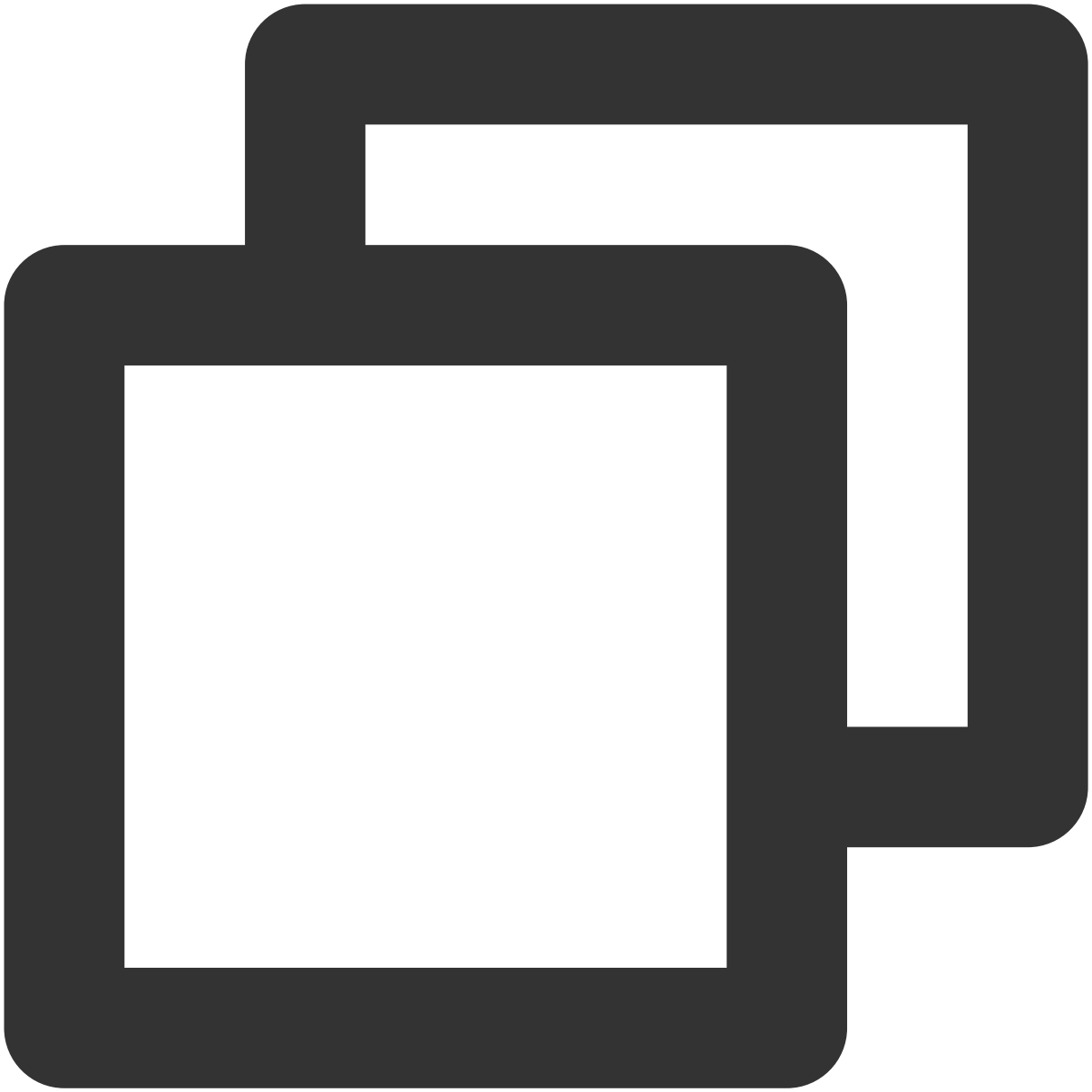


注意：

如果日志通过 HTTP 方式上报，可以通过抓包查看80端口，判断日志是否上报成功。

日志未上报，请按以下步骤排查：

a. 在安装目录下执行以下命令，检查 LogListener 采集配置是否正确。



```
tail -f log/loglistener.log | grep "ClsServerConf::load"
```

如果已配置下发，日志则如下所示：

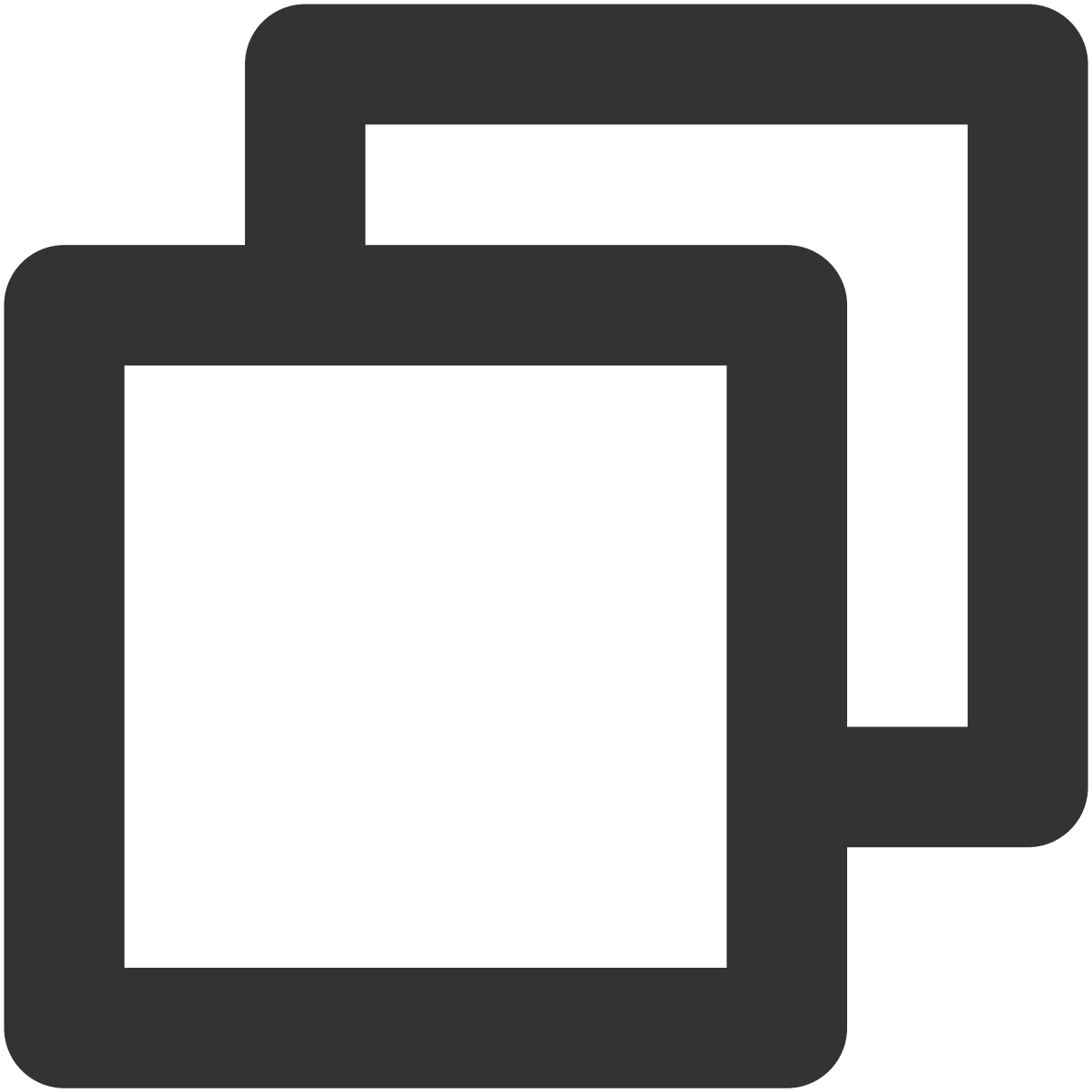
```
$ tail -f log/loglistener.log | grep "ClsServerConf::load"
2018-06-21 10:01:49|20706|DEBUG||cls_server_conf.cp:24|ClsServerConf::loa
"path":"/log","topicid":"56ed3e87-c895-49ba-a1cc-2f2c30e57a35"},{"extract_
a0207f-f3ec-4beb-a50f-9572546c1e8c"}],"needupdate":false}
```

下发配置需要检查 log_type、path 信息是否正确。

log_type 表示配置的日志解析类型（单行全文：minimalist_log，分隔符：delimiter_log，json日志：json_log，多行全文：regex_log）。

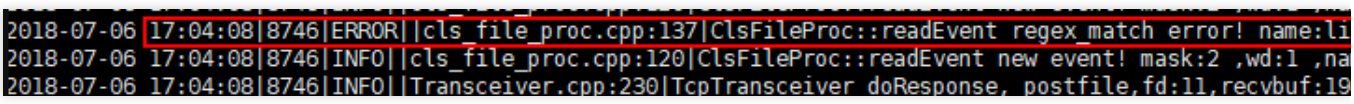
path 表示日志采集目录。

b. 在安装目录下执行以下命令，检查文件是否被正常监听。



```
grep [上报日志文件的文件名] log/loglistener.log
```

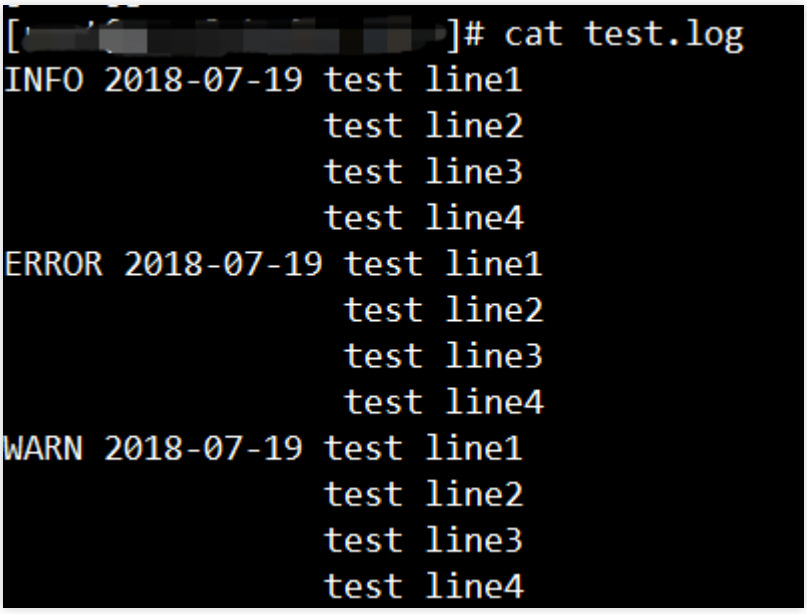
如果 grep 失败，使用 `grep regex_match log/loglistener.log` 搜索，检查控制台的正则表达式是否配置合理。如果出现下图所示的内容，表示文件名匹配正则失败，请登录控制台更改表达式。



c. 检查日志正则解析是否正确。

对于完全正则和多行全文提取模式，需要指定正则表达式。多行全文中，首行正则表达式匹配的是整个首行的内容，而非首行开头的部分内容。

例如，下图所示的日志样例。 INFO、ERROR、WARN 为日志首行，除了匹配（INFO|ERROR|WARN）外，还需将 INFO、ERROR、WARN 后面的字符匹配上。



错误配置方法： `^(INFO|ERROR|WARN)`

正确配置方法： `^(INFO|ERROR|WARN).*`

5. 确认一个文件被一个日志主题采集、单行日志最大不超过1M。

未按上述要求可能导致采集缺失。

检索分析报错

最近更新时间：2024-01-20 17:11:57

常见报错信息、原因及解决方案如下：

报错信息	报错原因	解决方案
QueryError [illegal_argument_exception.Cannot search on field [xxx] since it is not indexed.]	查询字段xxx未开启键值索引	为该字段开启键值索引，详情请参见 键值索引
QueryError [illegal_argument_exception.Cannot search on Full-Text since it is not indexed.]	未开启全文索引	开启全文检索，详情请参见 全文索引
QueryError [illegal_argument_exception.syntax error on field [and|or|not], or full text search is closed]	检索条件不支持小写逻辑操作符，小写逻辑操作符会按照普通字段进行全文检索	使用大写逻辑操作符 AND|OR|NOT，如您并不需要逻辑操作，而是全文检索包含 and|or|not 的日志，请开启全文索引
QueryError [number_format_exception.For input string: ">"]	数值比较语句语法错误	检查数值比较符号周围是否存在空格等特殊符号，正确格式参考 status:>400
QueryError [circuit_breaking_exception. Analysis data is too large,please reduce the scope of data query]	查询数据量过大	适当缩减查询时间范围，精确检索条件。如果仍旧报错，请联系 技术支持
QueryError [parse_exception.parse_exception: Cannot parse 'xxx': '*' or '?' not allowed as first character in WildcardQuery	不允许使用前缀模糊查询，例如 content:*example	建议使用分词符将字段拆分为多个词，详情请参见 配置索引
QueryError [sql_illegal_argument_exception.cannot cast [13/Jul/2021:17:04:34] to [datetime]: failed to parse date field [13/Jul/2021:17:04:34] with format [date_optional_time]]	cast 不能转换 13/Jul/2021:17:04:34 格式的日期，仅支持 ISO 标准的时间格式和毫秒级 Unix 时间戳，例如 yyyy-MM-dd'T'HH:mm:ss.SSSZ 或者 yyyy-MM-dd	修改时间字段的格式，或者使用__TIMESTAMP__ 内置字段
QueryError [verification_exception.Cannot order by	查询字段xxx未开启统计，不能用来排序	为该字段开启统计，详情请参见 分析简介

non-grouped column [xxx], expected [xxx] or an aggregate function		
QueryError [verification_exception.Cannot use non-grouped column [xxx], expected [xxx]]	查询字段xxx未开启统计	为该字段开启统计，详情请参见 分析简介
QueryError [verification_exception.Field [xxx] of data type [text] cannot be used for grouping]	查询字段xxx未开启统计，不能用来 group	为该字段开启统计，详情请参见 分析简介
QueryError [verification_exception.Unknown column [xxx]]	查询字段xxx不存在	检查该字段名称是否正确
QueryError [verification_exception.Unknown function [xxxxxx]]	不存在函数xxxxxx	检查函数名称是否正确。此外，部分函数与 Histogram 函数同时使用时也会出现该错误，此时可使用 时间补全函数 替代 Histogram 函数
QueryError [verification_exception.argument of [FUNCNAME(xxx)] must be [numeric], found value [xxx] type [text]]	传入 FUNCNAME 函数的参数类型不正确，例如 SUM(level)，level 字段为 text 类型时会报错	检查字段类型是否满足函数要求
QueryError [parse_exception.Failed to parse query [xxx]]	查询语句语法错误	检查报错信息中指出的错误位置
QueryError [line X:X: XXX]	查询语句语法错误	检查报错信息中指出的错误位置及错误原因
Internal error. Please try again later RequestId:[7be994d4-xxxx-xxxxx-xxxx-9c38xxxx65de]	CLS 内部错误	请联系 技术支持，并提供报错信息中的 RequestId
SyntaxError[xxx]	SQL 语句部分存在语法错误	参考报错信息中的详细提示修正语法错误，其中 line x,column x 不包含检索条件部分（即"|"及其前面的部分）
SearchTimeout	查询超时	适当缩小数据查询范围及 SQL 复杂度，或稍后再试
LimitExceeded.LogSearch	搜索并发超过限制	降低查询频率（包括 API），稍后再试。如当前查询频率

		并不高，仍旧报错，请联系技术支持

其他问题

最近更新时间：2024-01-20 17:11:57

日志服务 CLS 是什么？

日志服务（Cloud Log Service，CLS）提供一站式的日志数据解决方案。您无需关注扩缩容等资源问题，五分钟快速便捷接入，即可享受日志的采集、存储、加工、检索分析、消费投递、生成仪表盘、告警等全方位稳定可靠服务。全面提升问题定位、指标监控的效率，极大降低日志运维门槛。

日志服务主要提供以下功能：

日志采集：便捷实时采集跨地域、多渠道、多平台、不同数据源的日志数据，轻松采集多种其他腾讯云产品日志。

日志存储：提供两种存储类型：实时存储和低频存储。

日志检索分析：使用关键词检索日志，帮助用户快速定位异常日志，同时支持使用 SQL 对日志进行统计分析，获取日志条数随时间变化趋势、错误日志比例等统计指标。

日志数据加工：日志过滤、清洗、脱敏、富化、分发、结构化。

日志投递与消费：投递到腾讯云存储、中间件，消费到流计算。

仪表盘：将检索分析结果快速生成自定义 Dashborad。

告警：异常日志秒级告警，支持通过电话、短信、邮件和自定义接口回调等方式通知用户。

日志服务如何定义一条日志？

日志（Log）是应用系统运行过程中产生的记录数据，如用户操作日志、接口访问日志、系统错误日志等。日志通常以文本的形式存储在应用系统所在的机器上，一条系统运行记录对应的日志可能为一行文本（单行日志），也可能为多行文本（多行日志）。

更多说明及示例可查看 日志与日志组 文档。

日志可以保存多长时间？

日志服务提供日志生命周期管理，在创建日志主题时可以指定日志的有效保存周期，支持保存1 - 3600天或永久保存，逾期后数据将会被清理且不会再产生存储费用。

日志集和日志主题的区别是什么？

日志主题（Topic）是日志数据在日志服务（Cloud Log Service，CLS）平台进行采集、存储、检索和分析的基本单元，采集到的海量日志以日志主题为单元进行管理，包括采集规则配置、保存时间配置、日志检索分析以及日志下载/消费/投递等。

日志集（Logset）是对日志主题的分类，一个日志集可包含多个日志主题。日志集本身不存储任何日志数据，仅方便用户管理日志主题。

更多说明及示例可查看 日志主题与日志集 文档。

单个日志主题最多可采集多少日志？

为应对海量日志采集需求，单个日志主题包含多个主题分区，每个主题分区写请求最大为500QPS，写流量最大为5MB/s。采集日志量较大时，建议开启 主题分区自动分裂 功能（默认开启），单个日志主题最大可拥有50个分区，此时单个日志主题的写请求最大为50 * 500 = 25000QPS，写流量最大为50 * 5 = 250MB/s。
此处的写请求及写流量并不能简单的等于日志条数及日志量，日志上传时会将多条日志打包为一个 日志组 并进行压缩，实际支持的日志条数及日志量将远大于上述限制。使用 Loglistener 时将自动进行日志打包及压缩，您无需关注具体的打包策略。

什么是索引和分词？

索引配置是使用日志服务（Cloud Log Service，CLS）进行检索分析的必要条件，只有开启索引才能对日志进行检索分析。创建索引实际上是将原始日志按指定的符号切分为多个片段（即分词），并对分词进行 倒排索引 的过程。
更多说明及示例可查看 分词与索引 文档。

全文索引和键值索引有什么区别？

全文索引：全文索引将原始日志整体切分为多个分词进行索引构建，检索时直接通过关键词进行检索（即全文检索）。例如输入 `error` 表示检索包含 `error` 关键词的日志。
键值索引：键值索引将原始日志按字段（即 key:value）分别切分为多个分词进行索引构建，检索时基于键值方式进行检索（即键值检索）。例如输入 `level:error` 表示检索 `level` 字段中包含 `error` 的日志。
更多说明及示例可查看 配置索引 文档。

检索和分析有什么区别？

检索：根据指定的条件查找匹配的原始日志，例如使用 `status:404` 检索响应状态码为404的应用请求日志。
分析：针对符合检索条件的日志使用 SQL 进行统计分析，例如使用 `status:404 | select count(*) as logCounts` 统计响应状态码为404的应用请求日志数量。
更多说明及示例可查看 检索分析概述及语法规则 文档。

日志检索分析性能如何？

检索性能：百亿级别日志，秒级返回结果。
分析性能：亿级别日志，秒级返回结果；百亿级别日志，1分钟内返回结果。该性能与分析使用的 SQL 复杂度有很大的关系，SQL 非常复杂时可能低于该性能指标。

从日志生成到可以检索到需要多久？

使用 Loglistener 采集日志时，延迟不超过1分钟。使用 API 及 SDK 采集日志时，从发起 API 调用到可以检索到日志不超过1分钟。

服务不在腾讯云上，可以使用日志服务吗？

可以使用。日志服务对日志源没有限制要求，只要日志源与日志服务的服务端之间网络可达，就可以将日志采集到日志服务中来。日志服务支持的地域及对应的域名详见 可用地域。

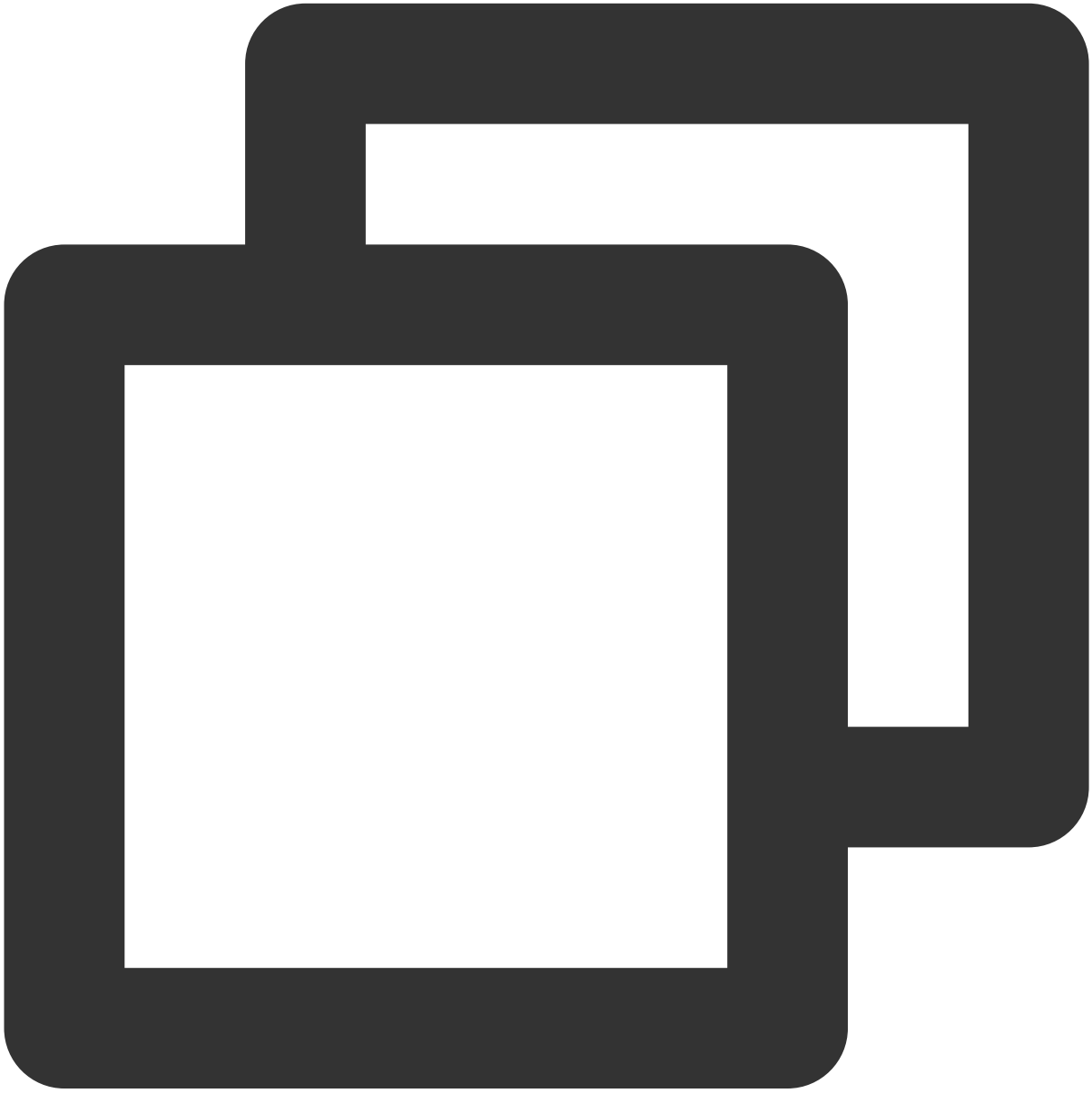
版权所有：腾讯云计算（北京）有限责任公司

服务器更换 IP 地址后，Loglistener 应该如何适配？

若服务器通过机器标识绑定机器组，用户无需变更 Loglistener 配置。若服务器 IP 需要频繁变更，建议用户使用机器标识配置机器组。单击 了解详情。

若服务器通过 IP 地址绑定机器组，用户需要完成以下配置变更：

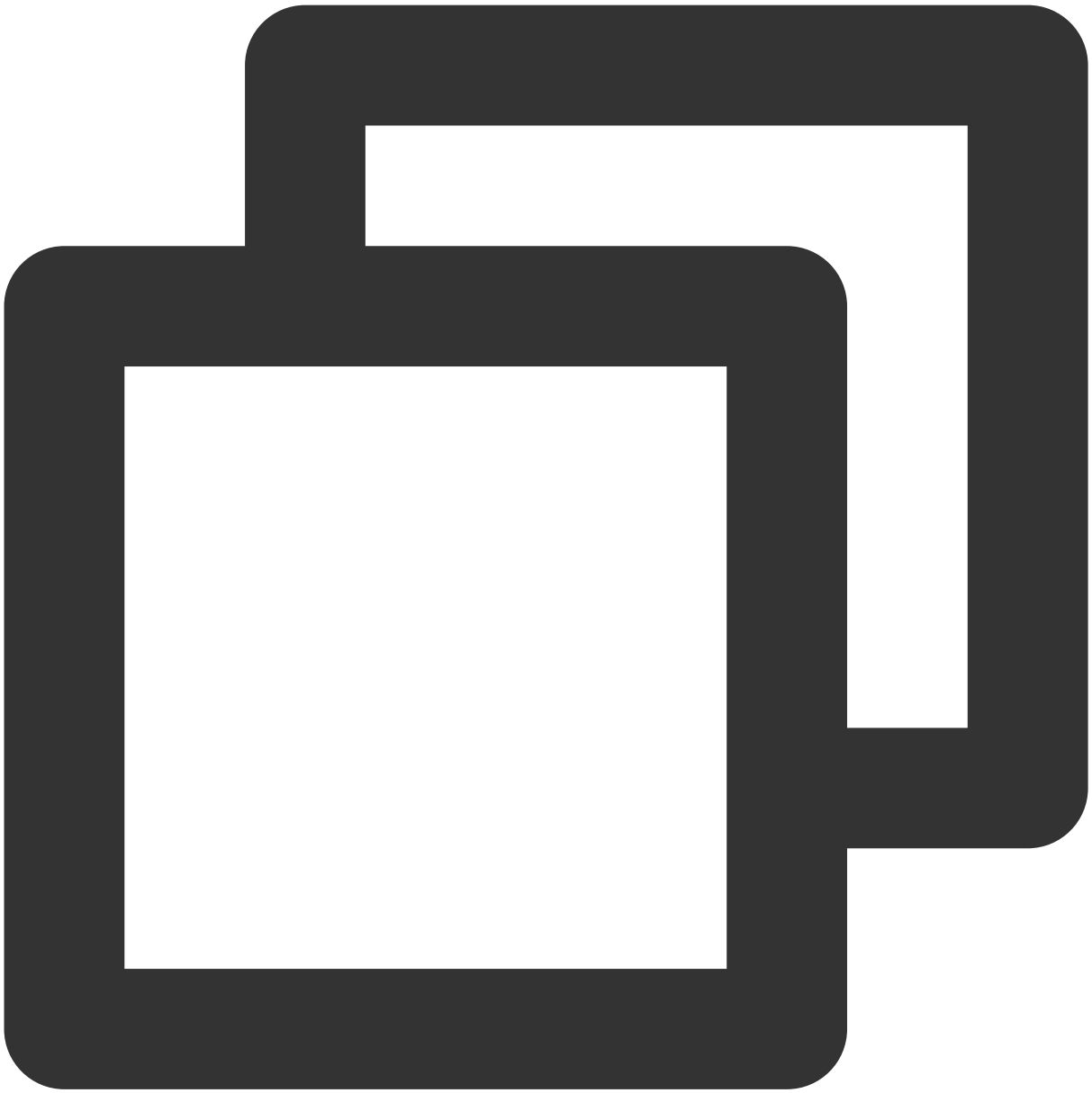
1. 修改 Loglistener 安装目录下的 /etc/loglistener.conf 文件。此处安装目录以 /user/local 为例：



```
vi /usr/local/loglistener-2.3.0/etc/loglistener.conf
```

2. 键盘按 **i** 键，进入编辑模式。
3. 修改配置文件中 group_ip 部分，填入变更后的 IP 地址。

4. 保存设置并退出编辑器，具体操作步骤：按 **Esc** 键，输入 **:wq**，按 **Enter** 键。
5. 执行如下命令，重启 Loglistener。



```
/etc/init.d/loglistenerd restart
```

6. 登录 日志服务控制台，在左侧导航栏中，单击**机器组管理**，修改该服务器绑定的机器组配置，使用新 IP 替换原机器 IP 地址，单机**确定**。

如何排查测试告警通知渠道报错或未收到测试消息？

情况1：页面显示“发送失败”

鼠标在“发送失败”上悬停可查看错误码及详细的失败原因，常见的错误码如下：

错误码	含义	排查方式
-1004	该通知渠道消息发送失败	一般是由于接受对象中的用户或用户组未配置或验证手机、邮箱导致，可在用户列表 中查看并配置。
-1005	该通知渠道部分消息发送失败，例如部分用户未成功发送，或部分渠道未成功发送	一般是由于接受对象中的部分用户或用户组未配置或验证手机、邮箱导致，可在 用户列表 中查看并配置。
-1006	自定义接口回调报错	根据详细的失败原因进一步排查，常见的错误包括： invalid URI for request：不是一个合法的 URL 地址。 i/o timeout：接口访问超时，请检查接口地址及能否通过公网直接访问。 callback custom error with status:xxx：接口响应报错，请检查接口地址及后端服务是否正常。 ssrf attack：回调接口地址需为公网可直接访问的地址，接口地址为腾讯云内网时可能出现该错误。

情况2：页面显示“已发送”，但实际未收到测试消息

根据接收渠道，常见原因如下：

接收渠道	原因
邮件、短信、电话	为避免重复通知干扰用户，一天内仅允许向同一用户使用同一渠道发送一次测试消息。
自定义接口回调（钉钉及飞书机器人地址）	测试消息不符合钉钉及飞书 API 接口要求，消息被忽略，此时测试通知渠道功能无实际意义，您可直接在告警策略中按钉钉及飞书 API 要求配置合适的请求头和请求内容来发送告警。
自定义接口回调（其它地址）	CLS 以 HTTP 响应状态码来判断消息发送是否成功，请检查自定义接口是否存在 HTTP 响应状态码正常，但仍存在其他业务逻辑限制的情况。

版权所有：腾讯云计算（北京）有限责任公司