

日志服务 新手指引 产品文档





【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。



新手指引

最近更新时间: 2024-01-20 16:27:42

本文将为刚入门日志服务(Cloud Log Service, CLS)的用户提供一条学习的路径。

1. 熟悉日志服务的基础知识

日志服务具备哪些功能? 为什么选择腾讯云日志服务? 腾讯云日志服务有哪些可用地域?

2. 日志服务的计费模式

CLS 支持按量计费(后付费)方式,即根据用户的实际使用资源情况进行计量,并按日进行费用扣除。按量计费适用于日志服务所有地域。详情请参见产品定价。

3. 新手入门

步骤1:服务开通

首先,您需要在腾讯云官网申请开通日志服务。

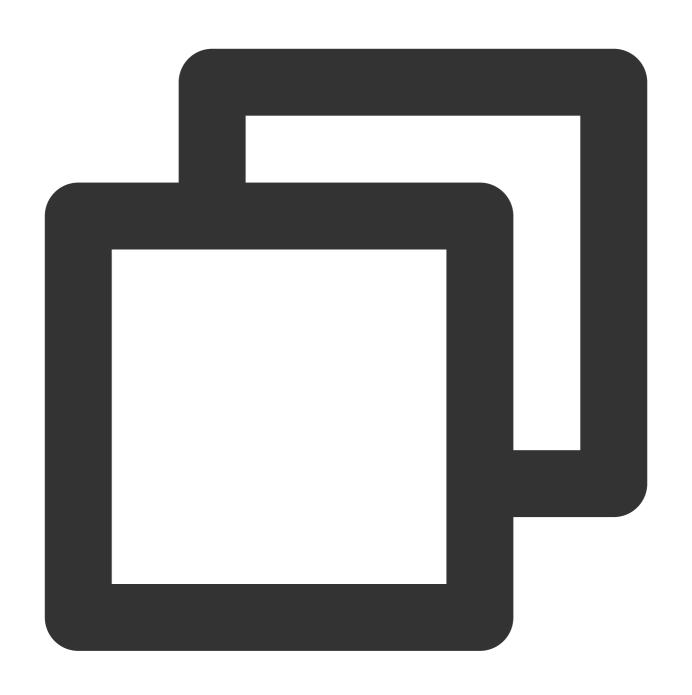
步骤2:下载安装 LogListener

LogListener 是日志服务的采集客户端,通过 LogListener 可实现快速无侵入式的把日志数据采集到日志服务中来, 具体安装步骤如下:

判断网络是否可达

安装 LogListener 要求日志源机器的网络与日志服务的可用地域网络互通(腾讯云服务器默认内网访问日志服务)。 您可以执行以下命令检查网络连通性,其中 <region> 为日志服务所在地域简称,具体地域信息请参阅可用地域 文档。





ping <region 简称>.cls.tencentyun.com

查看 (或创建) 密钥对

登录 访问管理控制台, 查看(或创建)密钥对, 并确认密钥状态为启用。

安装 LogListener

本文演示日志采集的环境搭建在云服务器 CentOS 7.2(64位)环境上。LogListener 下载及详细安装步骤请参见 LogListener 安装指南。



步骤3:创建日志主题

日志服务区分地域,为了降低网络延迟,尽可能选择与服务邻近的服务地域创建日志资源(支持地域详见 地域列表)。日志资源管理主要分为日志集和日志主题,一个日志集表示一个项目,一个日志主题表示一类服务,单个日志集可以包含多个日志主题。

- 1. 登录 日志服务控制台。
- 2. 在左侧导航栏中,单击**日志主题**,进入日志主题管理页面。
- 3. 选择日志主题的地域、单击创建日志主题。
- 4. 在弹出的创建日志主题窗口中, 填写相关信息。

日志主题名称:例如 topic test

日志集操作:默认选择当前地域现有的日志集。如需新建日志集,请选择**创建日志集**,输入日志集名称(例如 cls test)。

5. 单击确定。

创建好的日志主题会出现在日志主题列表中。

新创建的日志集可单击管理日志集、在展开的日志集列表页面进行查看。

步骤4:创建机器组

日志服务使用 机器组 来统一管理一组日志源机器。

登录 日志服务控制台 后,在左侧导航栏单击**机器组管理**,进入到机器组管理页面。在页面顶部选择合适的地域,单击**创建机器组**开始创建,一个机器组可以填入多个机器 IP 地址(每行一个 IP 地址),若是腾讯云服务器 CVM,直接填写内网 IP 地址即可,更多信息请参考 机器组管理。

创建好机器组后,单击机器组列表中的**查看**,检查 LogListener 与服务端的连接状态,若状态正常,则表示客户端 LogListener 已成功连接到日志服务。若显示异常,请参考 机器组异常 文档进行排查。

步骤5:配置 LogListener

- 1. 登录 日志服务控制台。
- 2. 在左侧导航栏单击日志主题,进入到对应的日志主题管理页面。
- 3. 在日志主题管理页面,单击采集配置,为该日志主题指定采集路径、解析模式、绑定机器组。

说明:

此步骤以如何使用 LogListener 采集日志为例,更多信息参考 采集方式。

绑定机器组

选择预先创建好的机器组,将当前日志主题与机器组关联起来后,LogListener 将按照所配置的规则监听采集机器组上的日志文件(一个日志主题可以绑定多个机器组,但一个日志文件只能上报到一个日志主题)。

配置采集路径

采集路径需要匹配机器上日志文件的绝对路径,填写参数有两个:目录前缀和日志文件名,填写格式为**[目录前缀表达式]**/**/**[文件名表达式]**, LogListener 会按照**[目录前缀表达式]** 匹配所有符合规则的公共前缀路径,并监听这些目录(包含子层目录)下所有符合**[文件名表达式]** 规则的日志文件,参数详细说明如下:



字段	说明
目录前缀	日志文件前缀目录结构,仅支持通配符*和?,*表示匹配多个任意字符,?表示匹配单个任意字符
/**/	表示当前目录以及所有子目录
文件名	日志文件名,仅支持通配符*和?,*表示匹配多个任意字符,?表示匹配单个任意字符

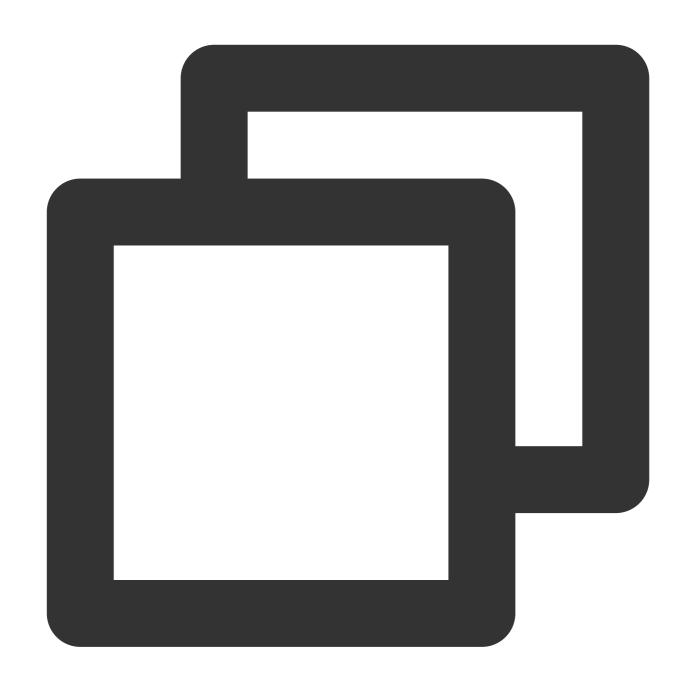
例如待采集文件的绝对路径是 /cls/logs/access.log ,则采集路径填写的目录前缀是 /cls/logs ,日志文件名填写access.log,如下图所示:



配置解析模式

日志服务提供多种日志解析模式(例如单行全文、分隔符、JSON、完全正则等模式),本文以分隔符格式日志为例进行说明(详情参考 分隔符格式),日志样例如下:





Tue Jan 22 14:49:45 2019; download; success; 194; a31f28ad59434528660c9076517dc23b

选择提取模式

本文以分隔符格式日志举例,所以在"键值提取模式"配置项中选择分隔符,并且选择分号作为日志分隔符。 输入日志样例并抽取键值对

在日志样例框中输入一条完整的日志,确认后将自动抽取键值对(key-value),然后为每组键值对定义唯一的键名称(key)。

在本示例中,日志被解析成 Tue Jan 22 14:49:45 2019 , download , success , 194 和 a31f28ad59434528660c9076517dc23b 五个字段,依次为每个字段定义键名称



(key): time , action , status , size , hashcode ,这样 LogListener 将按照所定义的结构化格式进行数据采集。

步骤6:检索日志

配置索引

日志服务的检索分析功能主要基于分词索引,目前提供两种索引类型:全文索引和键值索引,在日志主题的索引配置页进行索引管理(可以同时开启两种索引)。

索引类型	说明
全文索引	将整条日志按分词符拆分成多个分词,然后基于分词进行关键词查询
键值索引	将整条日志按格式拆分成多个键值对(key-value),然后基于键值对进行字段查询

本章节以键值索引为例说明配置方法,在日志主题管理页面,单击**索引配置**进入到索引管理页面,选择编辑键值索引,然后将需要进行检索分析的字段(键名key)配置到键值索引中,并每个字段的键值索引指定数据类型,目前支持 long 、 double 、 text 等数据类型,其中 text 类型可以指定分词符(分词符将字符串切分成多个分词)。在上述例子中,为 time , action , status , size , hashcode 设置键值索引,其中 size 设置为 long 类型。

开启索引后,新写入的数据将会按照所配置规则建立索引,索引会持久化存储一段时间(根据您所配置的存储周期 而定),只有建立索引的部分才能进行日志查询分析。**所以,修改索引规则或关闭索引仅对新写入的数据生效,未过期的历史数据仍可被检索**。

检索日志

- 1. 登录 日志服务控制台。
- 2. 在左侧导航栏单击检索分析,进入到检索分析页。
- 3. 选择目标地域与日志主题,选择时间范围,输入检索分析语句(语法支持关键词检索,后缀模糊检索、范围检索等方式,详情参考语法规则),单击**检索分析**,即可检索日志数据。

示例一:查询失败的日志

检索语句: status:fail

示例二:查询下载文件大小超过300K的日志

检索语句: action:download and size>300

步骤7:投递日志到 COS

日志服务可以将数据投递到对象存储 COS 中,一方面可以实现低成本长时间日志存储,另一方面可以进行离线日志大数据分析。

若要开启日志投递,请进行如下操作:

- 1. 创建 COS 存储桶。
- 2. 进入日志服务控制台。



- 3. 在日志主题管理页面,单击投递配置,进入到投递配置页面。
- 4. 单击添加投递配置,创建投递任务。

日志服务目前支持 CSV 格式、JSON 格式 投递方式,创建好投递任务后,日志服务异步地将数据投递到目标存储桶中,您可以在控制台右侧导航栏的"投递任务管理"中查看数据投递情况。

4. 控制台功能概述

如果您想	您可以阅读
通过控制台进行对应的日志集管理。	
通过控制台进行对应的日志主题管理。	日志主题操作
了解机器组相关内容。	机器组管理
进行索引的相关配置并开启索引。	
根据分析需求选择合适的图表类型展示分析结果。	日志分析
日志服务支持对一个或多个日志主题设置告警策略,当查询分析结果满足触发条件时发送告警通知,方便用户及时发现异常问题。	监控告警
您可以在仪表盘查看多个基于查询与分析结果的统计图表。	仪表盘
对日志进行清洗、分发、结构化,类似于开源 Logstash。	数据加工
定时 SQL 分析是周期性的日志查询分析任务,并将结果保存到新的日志主题。一般可用于聚合日志(可降低存储成本)和报表的场景。	
将日志数据投递到对象存储中,进一步满足日志场景的述求,挖掘日志数据价值。	
通过 Ckafka 实例来消费日志主题的数据。	
了解从不同的操作场景授权配置。	

5. 新手常见问题

LogListener 相关



机器组状态异常问题

LogListener 常见问题

LogListener 安装异常问题

日志检索相关

检索不到日志问题

6. 反馈与建议

使用腾讯云日志服务产品和服务中有任何问题或建议,您可以通过以下渠道反馈,将有专人跟进解决您的问题: 如果发现产品文档的问题,如链接、内容、API 错误等,您可以单击文档页右侧**文档反馈**或选中存在问题的内容进行 反馈。

如果遇到产品相关问题,您可咨询智能客服或 提交工单 寻求帮助。