

日志服务 快速入门



腾讯云

【 版权声明 】

©2013–2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 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。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。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。

【 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

快速入门

入门指南

快速体验 CLS

快速入门

入门指南

最近更新时间：2025-03-27 11:23:47

概述

日志服务（Cloud Log Service，CLS）提供一站式的日志数据解决方案，支持日志的采集、存储、加工、检索分析、消费投递、仪表盘、告警等功能。CLS 提供稳定可靠的服务，您可无需关注扩缩容等资源问题，同时降低了日志运维门槛，帮助您提高问题定位和指标监控的效率。

为了帮助您快速入门日志服务，本文将演示如何使用日志服务的基本功能：

- 使用 LogListener 采集服务器中的日志文件。
- 检索分析日志。

如果您没有合适的资源来采集日志，可 [使用 Demo 日志快速体验 CLS](#)，无需采集日志即可体验日志检索分析、仪表盘和告警功能，且不产生任何费用。

步骤1：开通服务

登录 [腾讯云日志服务控制台](#)。若您的账户此前未开通日志服务，该页面将提示您开通，单击**开通**即可。

步骤2：安装 LogListener

LogListener 是日志服务的采集客户端，通过 LogListener 可将日志文件采集至日志服务。下文将演示如何在腾讯云 CVM/Lighthouse 中安装 LogListener。

此外，LogListener 也可部署在 [非腾讯云服务器](#)、[容器服务 TKE](#) 和 [自建 K8s 集群](#)。

步骤2.1：获取密钥

登录 [访问管理控制台](#)，查看（或创建）并记录密钥，并确认密钥状态为启用。

使用提示

- 云API密钥是构建腾讯云 API 请求的重要凭证。用于您调用[腾讯云API](#) 时生成签名，查看[生成签名算法](#)。
- 最近访问时间指最近一次使用密钥调用云 API_v3.0 接口的时间。此时间仅供判断密钥近期是否活跃，以此决定是否禁用或删除密钥。
- 为降低密钥泄露的风险，自2023年11月30日起，对所有主账号、子账号的密钥，关闭查询SecretKey的功能，仅支持在创建时查看，请及时保存SecretKey。

新建密钥

APPID	密钥	备注	创建时间	最近访问时间 ^①	状态	操作
	SecretId: A	-	2024-06-12 11:23:34	2024-06-18 06:54:30	已启用	禁用 更多访问记录
125f	SecretId:	-	2024-07-29 17:59:08	2025-03-21 00:56:01	已启用	禁用 更多访问记录

步骤2.2: 安装 LogListener

1. 前往 [机器组管理](#)，在页面左上角将地域切换为需要安装 LogListener 的 CVM/Lighthouse 所属的地域，单击 [云服务器实例批量部署](#)。

⚠ 注意:

请确保目标 CVM/Lighthouse 已安装 [腾讯云自动化助手 \(TAT\)](#)。



机器组管理 广州

新建机器组 **云服务器实例批量部署** 服务日志 更多操作

机器组名称/ID	系统环境	机器组类型	LogListener服
<input type="checkbox"/> cls-k8 0ef2c	Linux	机器标识	<input type="checkbox"/>
<input type="checkbox"/>	Linux	机器标识	<input checked="" type="checkbox"/>

2. 勾选需要安装 LogListener 的机器实例，在输入 **SecretId** 信息中填写 [步骤2.1](#) 中的 **SecretId** 及 **SecretKey**，并填写 **机器标识**（例如 test，相当于对机器实例的分类，便于后续按照该标识批量采集多台机器的日志）。

实例批量部署

- 1 选择实例 > 2 安装实例 > 3 加入机器组

地域 成都

请选择实例 已选择0台CVM实例, 0台Lighthouse实例

云服务器 CVM 轻量级应用服务器 Lighthouse

多个关键字用竖线 "|" 分隔, 多个过滤标签用回车键分隔

ID/名称	LogListener安装状	实例状态	可用区	实例类型	实例配置	主IPv4地址	实例计费模式	标签
[模糊]		运行中	成都二区	标准型S3	4核 16GB 0Mbps 系统盘: SSD云硬盘 网络: [模糊]	[模糊]	按量计费 2022-06-24 12:43:53创建	[模糊]
[模糊]		运行中	成都二区	标准型S3	2核 4GB 0Mbps 系统盘: SSD云硬盘 网络: [模糊]	[模糊]	按量计费 2022-06-24 12:43:50创建	[模糊]
[模糊]		运行中	成都二区	标准型S3	2核 4GB 0Mbps 系统盘: SSD云硬盘 网络: [模糊]	[模糊]	按量计费 2022-06-24 12:43:54创建	[模糊]

10 条 / 页

输入SecretId信息 安装LogListener需要提供SecretId和SecretKey, 密钥信息用于上传日志。查看获取方式

SecretId SecretKey

高级配置项

机器标识

3. 等待安装完成后, 单击下一步。

实例批量部署

- 1 选择实例 > 2 安装实例 > 3 加入机器组

共选择1台实例 运行中: 1 成功: 0 失败: 0

重装所有失败实例

ID/名称	执行状态	开始时间	结束时间
ins- klat	进行中	2025-03-21 01:05:44	-

共 1 条

下一步

4. 将安装好 LogListener 的机器实例加入至新的机器组中 (机器组是一组需要采集日志的机器实例列表, 可针对同一机器组内的多个实例批量采集相同路径下的日志文件), 填写机器组名称, 单击加入。

选择实例 > 安装实例 > 3 加入机器组

加入方式 选择现有机器组 创建机器组

机器组名称 *
字符长度为1至255个字符

地域 广州

系统环境 * Linux ▾

机器组类型 机器标识 机器组IP地址

IP地址
每行填写一个 IP 地址
注意：请填写Linux机器IP地址，不支持同时关联Linux机器与Windows机器

LogListener 自动升级 01:06 ~ 03:06 ⌚
建议业务低峰期升级LogListener

LogListener 离线剔除策略 LogListener离线超过 30天 ▾ 后，将自动剔除相应机器

LogListener 服务日志 LogListener运行状态、采集状况等重要日志记录

标签 ⓘ ▾ ▾ ×
+ 添加 ⓘ 键值粘贴板

机器组元数据 + 添加

暂不加入 加入

步骤3：创建日志主题

日志主题是日志数据采集、存储、检索和分析的基本单元，一个日志主题通常对应某一个应用/服务（具备类似的日志结构）。还可以使用日志集对日志主题进行分组，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。

1. 前往 [日志主题](#) 管理页面，在页面左上角将地域切换为 [步骤2.2](#) 的地域，单击**创建日志主题**。

日志主题 广州 555

创建日志主题 编辑标签 管理日志集 多个关键字用竖线“|”分隔，：

<input type="checkbox"/> 日志主题名称/ID	检索	监控(昨天)	日志集名称/ID	存储类型	日志保留时间	描述
<input type="checkbox"/> ian-1 5191c			(写:0MB 存:0MB) 12 1a8a5efd-2c58-48f8-987c-271c5ca...	标准存储	标准: 30天	-
<input type="checkbox"/> aud-tes 6c			(写:258.26MB 存:2.22GB) vod_cdn_logset_cn 3572e05b-19aa-46b4-8d46-df78e...	标准存储	标准: 11天	-

2. 在弹出的创建日志主题窗口中，填写相关信息，单击**确定**。

创建日志主题 ×

日志主题名称 *

日志主题ID * 自动生成

日志保存策略 *

日志接入 * 标准存储 低频存储

标准存储的数据可使用所有能力；低频存储费用较低，但无法使用SQL、图表分析、告警功能。详情请参考[存储类型概述](#)

存储选项 日志永久存储 [日志沉降](#)

存储时间 * 日志接入 - 30 + 天后过期

日志集操作 * 选择现有日志集 创建日志集

日志集名称 *

日志集ID * 自动生成

日志集标签 ⓘ ×

+ 添加

日志主题标签 ⓘ ×

+ 添加

▶ 高级设置

费用预估

流量费用 存储费用 主题分区费用

以上费用仅包含主要计费项，实际消费以使用情况为准，此数据仅供参考，计费项详细说明参见[计费概述](#)，已购买资源包时会优先扣除资源包

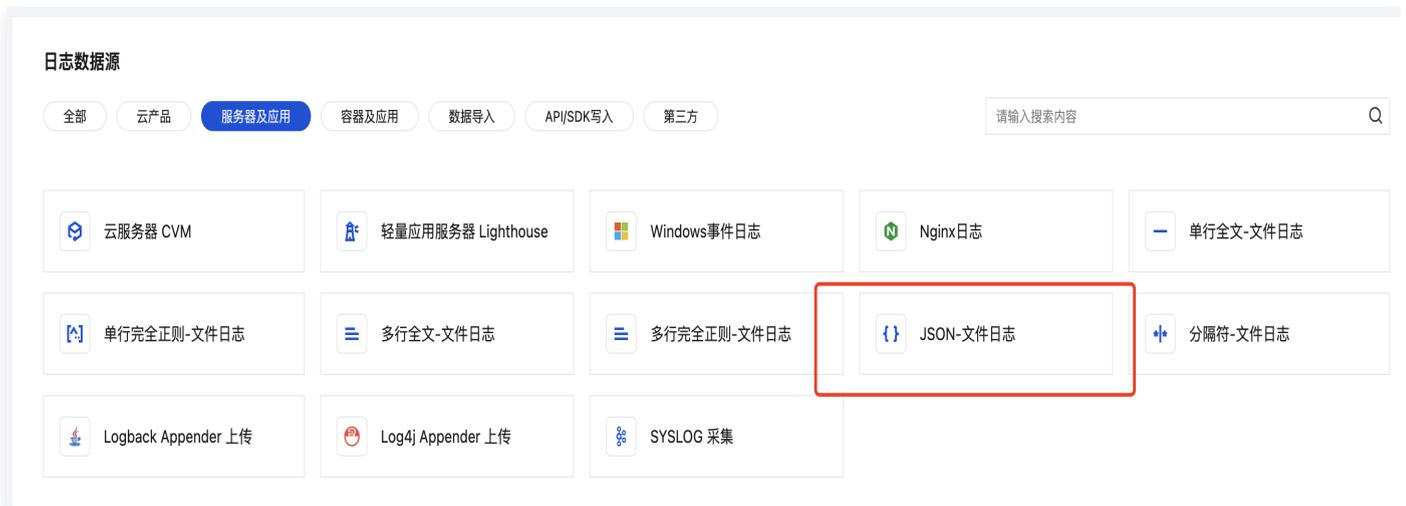
- 日志主题名称：例如 test
- 存储类型：标准存储
- 日志集操作：创建日志集
- 日志集名称：例如 test

步骤4：配置采集规则及索引配置

1. 前往 [日志主题](#) 管理页面，单击步骤3创建的日志主题名称/ID，进入该日志主题管理页面。
2. 选择采集配置页签，在 LogListener 采集配置中单击新增。



3. 在日志数据源页面，选择 JSON-文件日志。



说明:

- **JSON** 是结构化数据类型，日志采集到 CLS 之后，可直接使用日志检索和分析功能（按特定字段检索日志或使用 SQL 进行统计分析）。
- 如果您日志为非结构化的文本，可选择**单行全文日志**。文本日志可以按照关键字检索内容，但必须结构化之后方可使用 SQL 进行统计分析，请参见 [单行-正则提取日志](#) 对日志字段进行分割和提取。

4. 选择 [步骤2.2](#) 创建的机器组，单击下一步。

- 1 创建日志主题 >
 2 机器组管理 >
 3 采集配置 >
 4 索引配置

① 如需在CVM中批量安装LogListener，请点击[这里](#)。**Windows系统的腾讯云服务器暂不支持批量部署。**

● 安装LogListener

LogListener是腾讯云日志服务CLS所提供的专用日志采集器，将它安装部署到服务器上，可以快速采集日志到日志服务。

[Linux安装指南](#)

[Windows安装指南](#)

● 选择机器组

机器组是腾讯云日志服务中LogListener所采集日志服务的对象。没有机器组，[点击新建机器组](#)

系统环境 Linux Windows

搜索机器组名称、ID

机器组名称	操作
<input checked="" type="checkbox"/> kh1-	查看
<input type="checkbox"/> E	查看
<input type="checkbox"/>	查看
<input type="checkbox"/>	查看
<input type="checkbox"/>	查看
<input type="checkbox"/> te d	查看

已选择 (1)

机器组名称
kh1-

支持按住 shift 键进行多选

5. 填写采集规则名称及采集路径（即需要采集的日志文件路径），单击下一步。

例如，待采集文件的绝对路径是 `/root/test.log`，则采集路径填写的目录前缀是 `/root`，日志文件名填写 `test.log`。

创建日志主题 > 机器组管理 > **3 采集配置** > 4 索引配置

导入配置规则

采集规则名称

采集路径

添加

担心路径填写不正确? [使用路径验证](#)

日志目录前缀以/开头, 文件名以非/开头。/**代表LogListener将监听所填前缀目录下的所有层级匹配上的日志文件。多文件路径之间为或关系。
目录前缀和文件名支持?和*通配符, 不支持逗号。

采集路径黑名单 黑名单配置可在采集时忽略指定的目录和文件, 目录和文件名可以是完整匹配, 也支持通配符模式匹配, 需要LogListener-2.3.9 及以上版本

采集策略 全量 增量

回溯采集 从最新的位置, 往前采集 字节 (Byte) 的日志

编码模式 UTF-8 GBK

提取模式 [修改](#)
适用JSON 格式日志

标准JSON
开启标准JSON后, 采集器会优化处理日志原文内的转义符号后再上报保证可读性, 需要 LogListener 2.8.0 及以上版本。[预览效果](#)

自定义元数据

日志时间戳来源 指定日志字段 日志采集时间 [配置时间格式](#)
将使用日志被采集时间作为日志的时间戳

过滤器
仅采集符合过滤规则的日志。例如, 您希望原始日志内容中 response_code 为400或500的所有日志数据被采集, 那么 key 处配置 response_code, 过滤规则选择等于, Value处配置正则表达式 400|500。

上传解析失败日志
开启后, LogListener会上传解析失败的日志; 关闭会丢弃失败的日志。

解析失败日志的键名称 (Key)
所有解析失败的日志, 均以LogParseFailure作为键名称 (Key), 原始日志内容作为值 (Value) 进行上传

高级配置 超时属性 最大目录深度

[上一步](#) [数据加工](#) [下一步](#)

6. 填写索引配置, 开启全文索引、键值索引, 填写相关信息后, 单击提交。

[创建日志主题](#) > [机器组管理](#) > [采集配置](#) > **4 索引配置**

导入配置规则

索引状态

开启后可对日志进行检索分析，将产生索引流量、索引存储及相应费用。[费用详情](#)

全文索引

开启后支持使用关键词检索日志全文，例如输入 error 检索包含 error 关键词的日志。

全文分词符 []{}|\\|"/>

将日志全文按照分词符拆分成若干个分词用于检索。

大小写敏感

包含中文

日志中包含中文且需对中文进行检索时可开启该功能，将每一个汉字拆分为独立的分词用于检索。

键值索引

开启后支持使用键值检索日志，例如添加名称为level的字段，输入level:error即可检索level为error的日志。已开启全文索引时，键值索引不产生任何额外索引流量/存储费用。

大小写敏感

自动配置

[批量添加字段](#) 根据采集配置自动添加字段 显示内置保留字段

字段名称	字段别名 ^①	字段类型 ^①	分词符 ^①	包含中文 ^①	开启统计 ^①
LogParseFailure	采集配置 <input type="text" value="请输入字段别名"/>	text	@&?#()=\":;<>[]{} \\	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[+ 添加字段](#)

[高级设置](#)

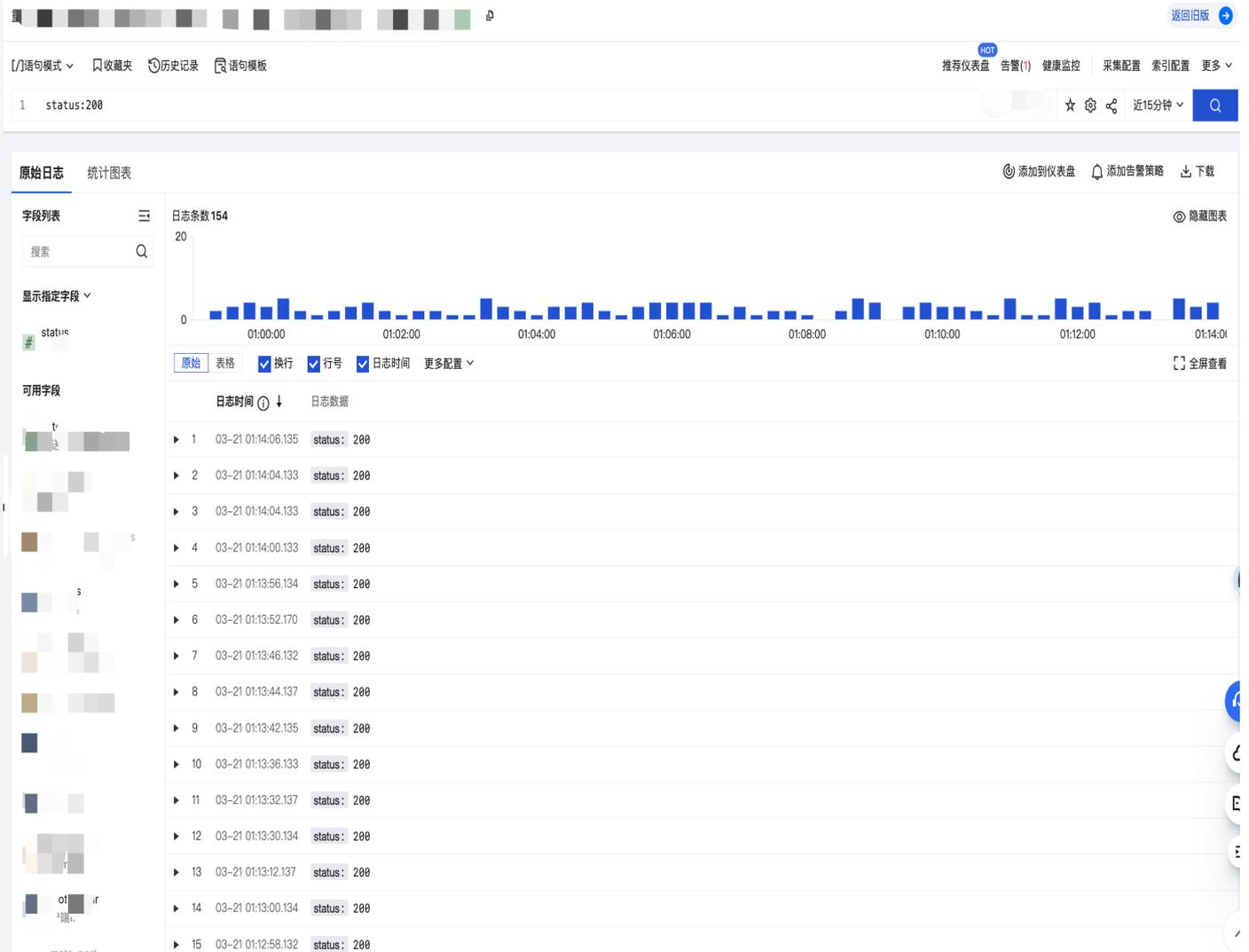
[上一步](#) [提交](#)

说明：

- 修改索引配置仅对新写入的日志生效，已有数据不会更新。
- 索引配置中的各个配置项说明请参见 [索引配置](#) 文档。

步骤5：检索分析日志

1. 前往 [检索分析](#)，即可检索符合检索条件的日志。例如，下图中为检索包含 status 为200的日志。



2. 基于检索到的原始数据，使用管道符和 SQL 进行统计分析。例如，统计 status 为200的日志条数。

原始日志 统计图表

```
1 status:200 | select count(*) as "日志条数" limit 10000
```

日志条数

151

总计 1 条数据 1000 条 / 页 1 / 1 页

数据转换支持对查询分析结果进行二次处理后再进行图表绘制。例如合并多个查询分析语句的结果、变更结果字段类型等。 [帮助文档](#)

- 转换字段类型** Beta: 修改字段类型, 如将 string 类型转换为 time 类型。
- 分组聚合(Group By)**: 根据指定的字段对查询分析结果进行分组合并, 并对各组进行计算。
- 列计算** Beta: 使用列值计算一个新字段。
- 组织字段**: 支持字段显示/隐藏, 字段排序。

说明:
更多检索及分析语法说明请参见 [语法规则](#) 文档。

扩展阅读

- **基本概念**: 通过该文档, 您可以系统了解 CLS 基本产品概念, 包括日志主题、日志集、索引和分词等。
- **采集检索 Nginx 访问日志**: 通过该文档, 您可以了解如何采集 nginx 日志并使用正则表达式对日志内的字段进行分割和提取。
- **将通过 grep 命令查找的本地日志迁移至 CLS**: 通过该文档, 您可以将习惯使用的 grep 命令转换为 CLS 检索语法, 更快地掌握 CLS 语法规则。
- **云产品日志接入**: CLS 已集成了部分常见云产品日志, 可轻松采集这些云产品的日志。
- **数据加工任务**: 可通过数据加工对原始日志进行过滤、清洗、脱敏、富化和分发。
- **监报告警概述**: 可针对日志设置告警策略, 例如1分钟内 ERROR 日志大于10条即触发告警。

快速体验 CLS

最近更新时间：2024-05-16 17:45:51

简介

当您想要快速了解日志服务（Cloud Log Service，CLS）的各项功能，但自己没有资源进行操作时，可通过 CLS 提供的 Demo 日志进行体验。

说明：

Demo 日志免收流量费用与存储费用，请放心体验。

Demo 日志	说明	可用预置仪表盘
负载均衡 CLB	包含 CLB 访问日志，提供检索、仪表盘、告警模板	CLB 访问日志仪表盘
Nginx 日志	包含 Nginx ingress 访问日志，提供检索、仪表盘、告警模板	<ul style="list-style-type: none">Nginx 访问大盘Nginx 监控大盘
容器服务 TKE	包含 TKE 审计日志、TKE 事件日志，提供检索、仪表盘、告警模板	<ul style="list-style-type: none">TKE 审计日志_总览仪表盘TKE 审计日志_节点操作概览仪表盘TKE 审计日志_K8S对象操作概览仪表盘TKE 审计日志_聚合检索仪表盘TKE 事件日志_总览仪表盘TKE 事件日志_异常事件聚合检索仪表盘
内容分发网络 CDN	包含 CDN 访问日志，提供检索、仪表盘、告警模板	<ul style="list-style-type: none">CDN 访问日志_质量监控分析仪表盘CDN 访问日志_用户行为分析仪表盘
网络流日志 Flowlogs	包含 弹性网卡 ENI 网络流日志，云联网 CCN 网络流日志，提供检索、仪表盘、告警模板	<ul style="list-style-type: none">ENI 流日志_高级分析仪表盘CCN 流日志_高级分析仪表盘
对象存储 COS	包含 COS 访问日志，提供检索、仪表盘、告警模板	COS 访问日志分析仪表盘

Web 应用防火墙 WAF	包含 WAF 访问日志，提供检索、仪表盘、告警模板	WAF 访问日志_访问流量分析仪表盘
操作审计 CloudAudit	包含操作审计日志，提供检索、仪表盘、告警模板	CloudAudit 审计日志_事件分析仪表盘
API 网关 API Gateway	包含 API 网关访问日志，提供检索、仪表盘、告警模板	API Gateway 访问日志_接口质量分析仪表盘

使用 Demo 日志

开启 Demo 日志

1. 登录 [日志服务控制台](#)。
2. 在概览页面的 **Demo 日志中心**中，找到想要体验的 Demo 日志，并单击**开启 Demo**。
3. 在弹出的提示框中，单击**确认**。资源初始化过程需约等待2分钟。
4. 初始化完成后，可以执行如下操作：
 - 单击 **Demo 内容 > 进入检索分析页**，查看检索分析详情。
 - 单击 **Demo 内容 > 查看仪表盘**，查看预置仪表盘。
 - 单击 **Demo 内容 > 查看告警**，查看监控告警详情。
 - 单击 **Demo 内容 > 查看日志主题**，查看日志主题详情。

重置 Demo 日志

1. 登录 [日志服务控制台](#)。
2. 在概览页面的 **Demo 日志中心**中，找到对应 Demo，并单击 **Demo 内容 > 重置资源**。当 Demo 日志过期时，可以通过重置再次启用。

删除 Demo 日志

1. 登录 [日志服务控制台](#)。
2. 在概览页面的 **Demo 日志中心**中，找到对应 Demo，并单击 **Demo 内容 > 删除资源**。
3. 在弹出的提示框中，单击**确认**，Demo 日志停止写入，且删除 Demo 资源。