阿里云
日志服务

产品简介

文档版本：20181009

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 禁止： 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告： 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明： 您也可以通过按**Ctrl** + **A**选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

法律声明.....I
通用约定.....I
1 什么是日志服务.....1
2 产品架构.....3
3 产品优势.....5
4 应用场景.....6
5 限制说明.....10
5.1 基础资源.....10
5.2 数据读写.....11
5.3 查询分析与可视化.....12
5.4 保留字段.....13

1 什么是日志服务

日志服务（Log Service，简称 LOG）是针对日志类数据的一站式服务，在阿里巴巴集团经历大量大数据场景锤炼而成。您无需开发就能快捷完成日志数据采集、消费、投递以及查询分析等功能，提升运维、运营效率，建立 DT 时代海量日志处理能力。

日志服务 学习路径

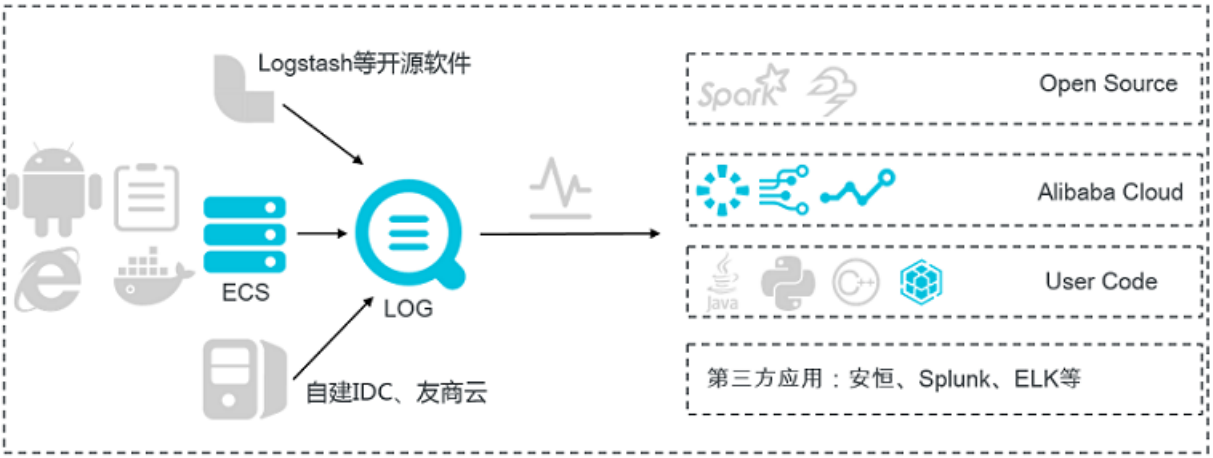
日志服务学习路径图为您推荐热门功能的操作指引文档，帮助您快速了解日志服务产品。视频与文档结合，全方位提升您的产品使用及文档阅读体验。

实时采集与消费（LogHub）

功能：

- 通过ECS、容器、移动端，开源软件，JS等接入实时日志数据（例如Metric、Event、BinLog、TextLog、Click等）
- 提供实时消费接口，与实时计算及服务对接

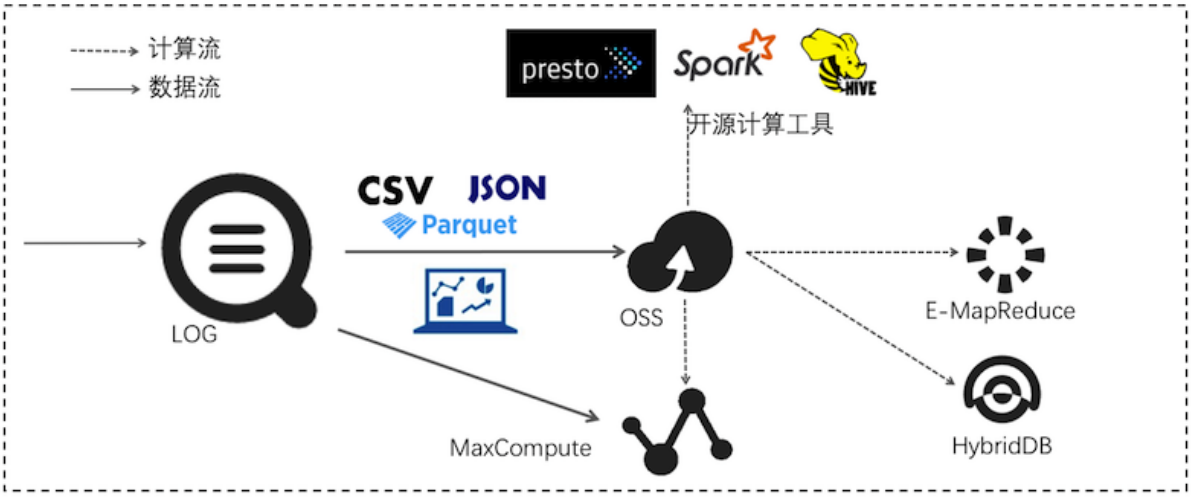
用途：数据清洗（ETL），流计算（Stream Compute），监控与报警， 机器学习与迭代计算。



投递数仓（LogShipper）

稳定可靠的日志投递。将日志中枢数据投递至存储类服务进行存储。支持压缩、自定义Partition、以及行列等各种存储方式。

用途：数据仓库 + 数据分析、审计、推荐系统与用户画像。

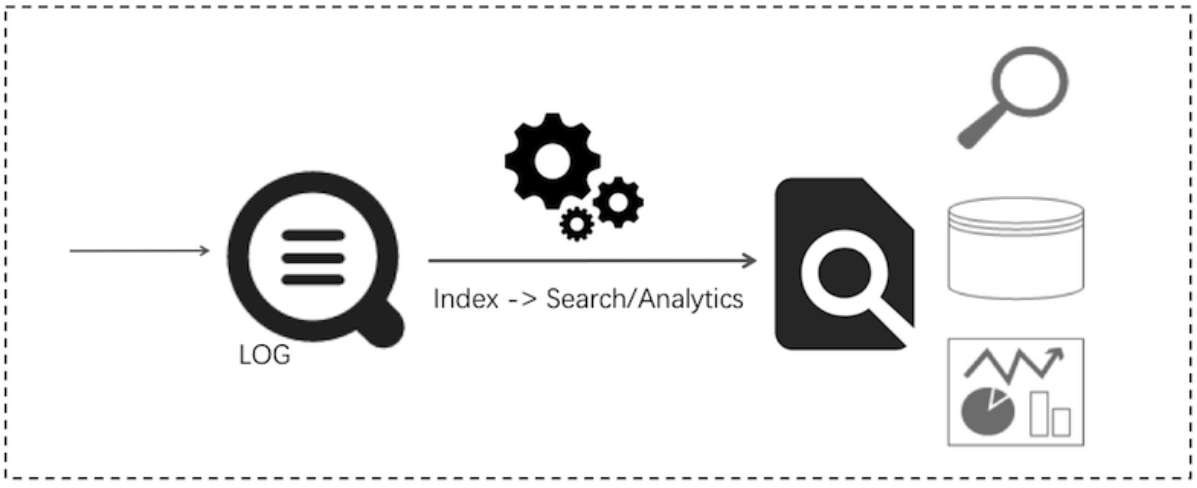


查询与实时分析（Search/Analytics）

实时索引、查询分析数据数据。

- 查询：关键词、模糊、上下文、范围
- 统计：SQL聚合等丰富查询手段
- 可视化：Dashboard + 报表功能
- 对接：Grafana，JDBC/SQL92

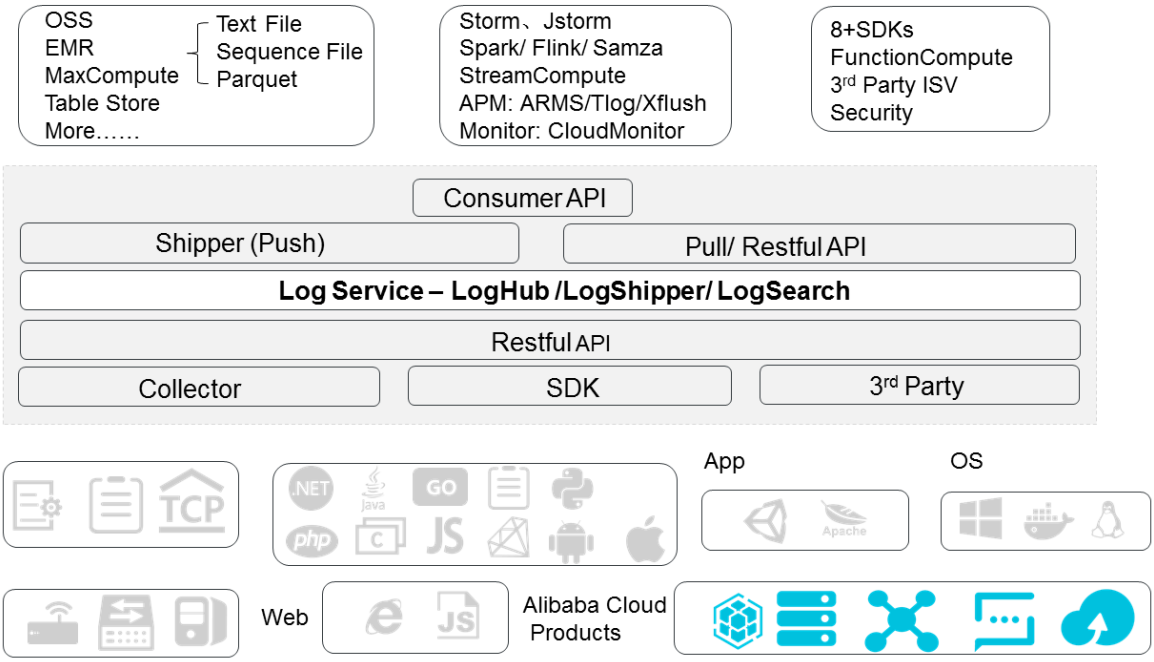
用途：DevOps/线上运维，日志实时数据分析，安全诊断与分析，运营与客服系统。



2 产品架构

日志服务的架构如下图所示。

图 2-1: 产品架构



Logtail

帮助您快速收集日志的Agent。其特点如下所示：

- 基于日志文件、无侵入式的收集日志
  - 只读取文件。
  - 日志文件无侵入。
- 安全、可靠
  - 支持文件轮转不丢失数据。
  - 支持本地缓存。
  - 网络异常重试。
- 方便管理
  - Web端操作。
  - 可视化配置。
- 完善的自我保护

- 实时监控进程CPU、内存消耗。
- 限制使用上限。

前端服务器

采用LVS + Nginx构建的前端机器。其特点如下所示：

- HTTP、REST协议
- 水平扩展
  - 流量上涨时可快速提高处理能力。
  - 支持增加前端机。
- 高吞吐、低延时
  - 纯异步处理，单个请求异常不会影响其他请求。
  - 内部采用专门针对日志的Lz4压缩，提高单机处理能力，降低网络带宽。

后端服务器

后端是分布式的进程，部署在多个机器上，完成实时对Logstore数据的持久化、索引、查询以及投递至MaxCompute。整体后端服务的特点如下所示：

- 数据高安全性：
  - 您写入的每条日志，都会被保存3份。
  - 任意磁盘损坏、机器宕机情况下，数据自动复制修复。
- 稳定服务：
  - 进程崩溃和机器宕机时，Logstore会自动迁移。
  - 自动负载均衡，确保无单机热点。
  - 严格的Quota限制，防止单个用户行为异常对其他用户产生影响。
- 水平扩展：
  - 以分区（Shard）为单位进行水平扩展。
  - 用户可以按需动态增加分区来增加吞吐量。

3 产品优势

全托管服务

- 应用性强，5分钟即可接入服务进行使用，Agent支持任意网络下数据采集。
- LogHub覆盖Kafka 100%功能，提供完整监控、报警等功能数据，并支持弹性伸缩（可支持PB/Day规模），使用成本为自建50%以下。
- LogSearch/Analytics 提供快速查询、仪表盘和报警功能，使用成本为自建 20%以下。
- 0+接入方式，与云产品（OSS/E-MapReduce/MaxCompute/Table Store/MNS/CDN/ARMS等）、开源软件（Storm、Spark）无缝对接。

生态丰富

- LogHub 支持30+采集端，包括Logstash、Fluent等，无论是嵌入式设备，网页，服务器，程序等都能轻松接入。在消费端，支持与Storm、Spark Streaming、云监控等对接。
- LogShipper 支持丰富数据格式（TextFile、SequenceFile、Parquet等），支持自定义Partition，数据可以直接被Presto、Hive、Spark、Hadoop、E-MapReduce、MaxCompute、HybridDB等处理。
- LogSearch/Analytics 查询分析语法完整、兼容SQL92、支持JDBC协议与Grafana对接。

实时性强

- LogHub：写入即可消费；Logtail（采集Agent）实时采集传输，1秒内到服务端（99.9%情况）。
- LogSearch/Analytics：写入即可查询分析，在多个查询条件下1秒可查询10亿级数据，多个聚合条件下1秒可分析1亿级数据。

完整**API/SDK**

- 轻松支持自定义管理及二次开发。
- 所有功能均可通过API/SDK实现，提供多种语言SDK，可轻松管理服务和百万级设备。
- 查询分析语法简单便捷，兼容SQL92；接口友好、适合与生态软件对接，提供Grafana对接方案。

4 应用场景

日志服务的典型应用场景包括：数据采集、实时计算、数仓与离线分析、产品运营与分析、运维与管理等场合。典型应用场景如下。

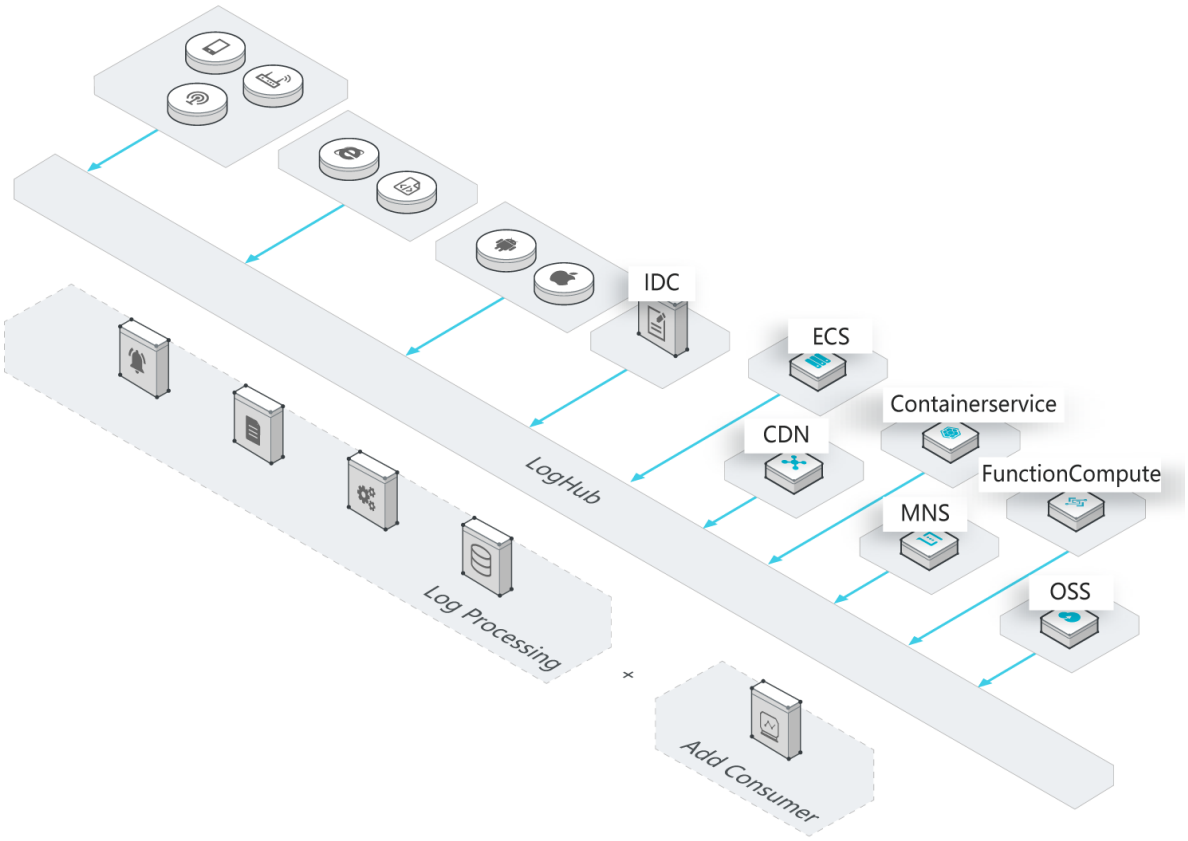
数据采集与消费

通过日志服务LogHub功能，可以大规模低成本接入各种实时日志数据（包括Metric、Event、BinLog、TextLog、Click等）。

方案优势：

- 使用便捷：提供30+实时数据采集方式，让您快速搭建平台；强大配置管理能力，减轻运维负担。
- 弹性伸缩：无论是流量高峰还是业务增长都能轻松应对。

图 4-1: 数据采集与消费

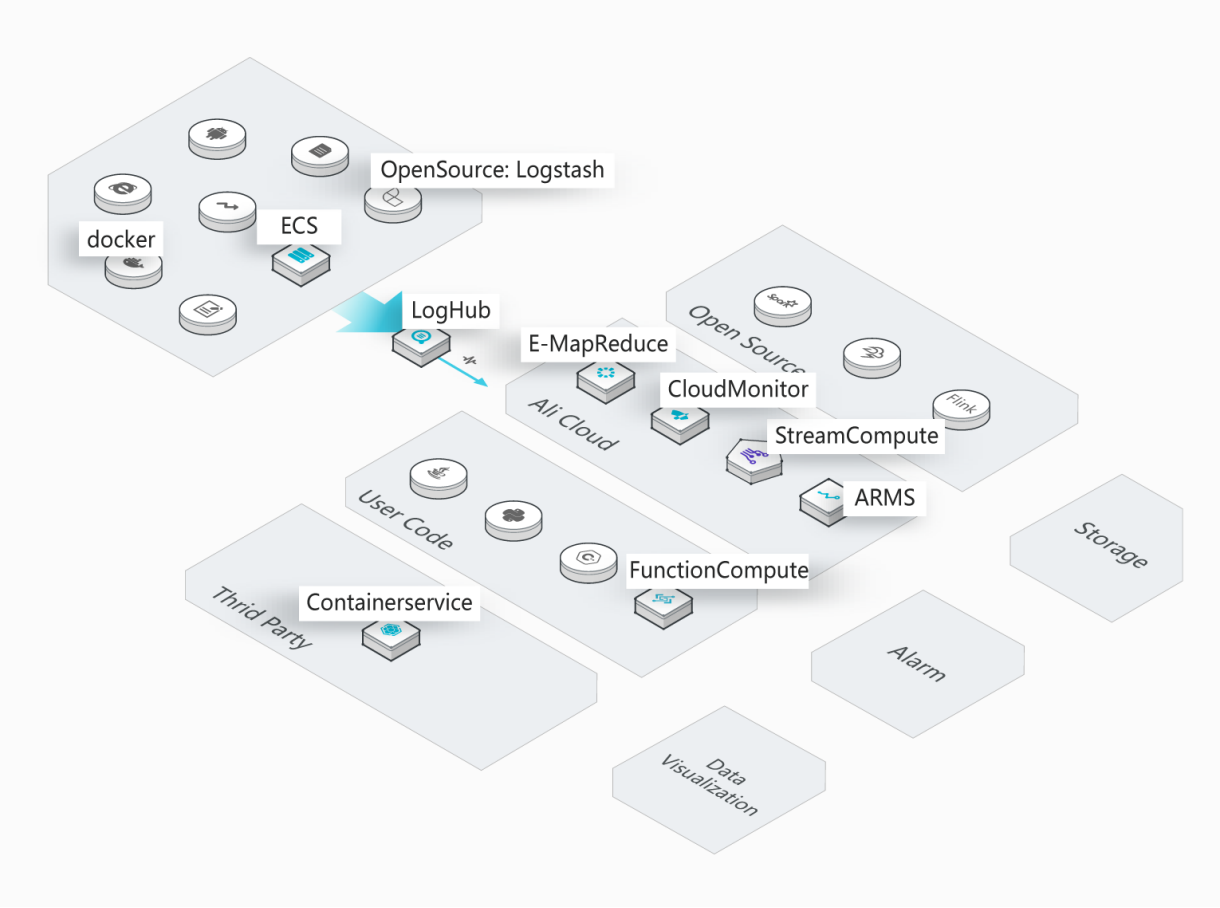


数据清洗与流计算 (ETL/Stream Processing)

日志中枢（LogHub）支持与各种实时计算及服务对接，并提供完整的进度监控，报警等功能，并可以根据SDK/API实现自定义消费。

- 操作便捷：提供丰富SDK以及编程框架，与各流计算引擎无缝对接。
- 功能完善：提供丰富监控数据，以及延迟报警机制。
- 弹性伸缩：PB级弹性能力，0延迟。

图 **4-2:** 数据清洗与流计算

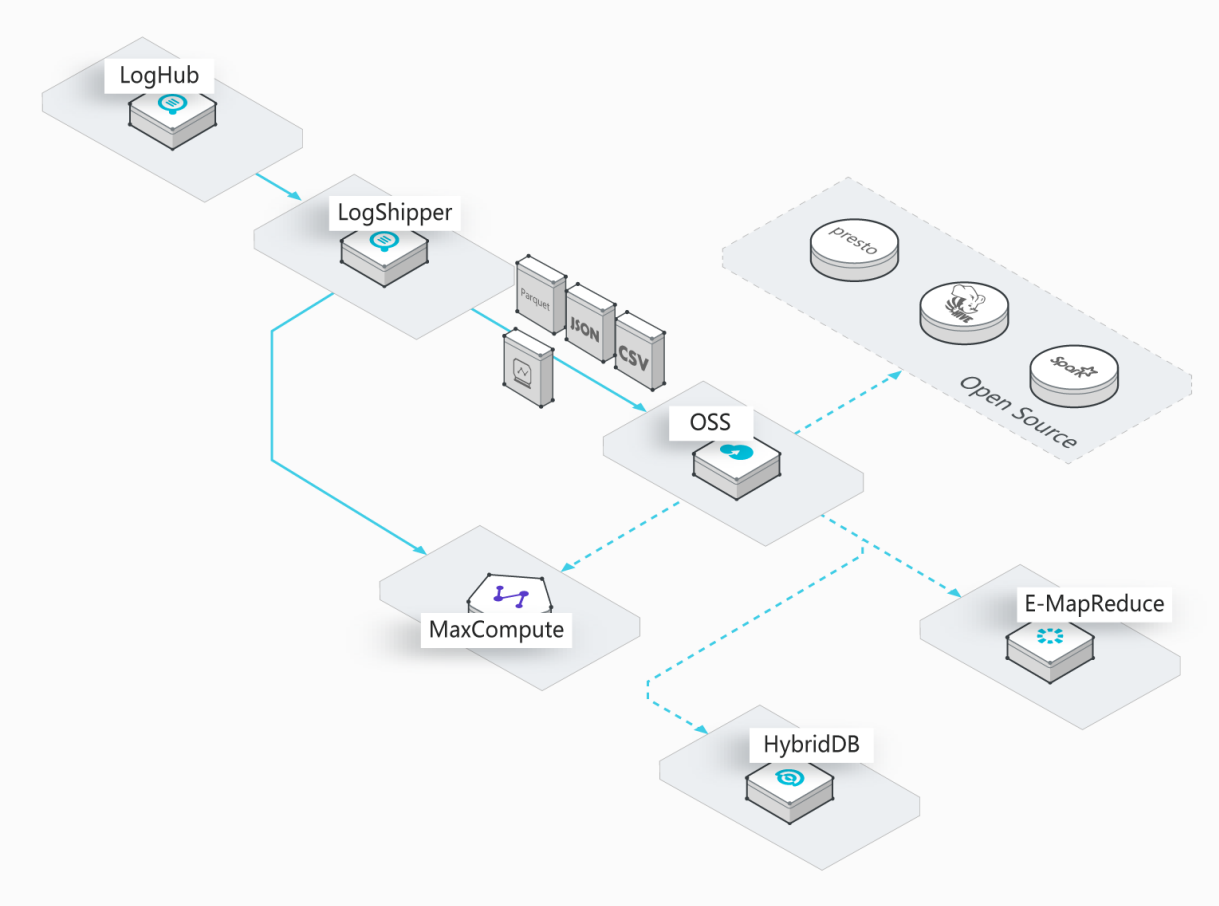


数据仓库对接(Data Warehouse)

日志投递（LogShipper）功能可以将日志中枢（LogHub）中数据投递至存储类服务，过程支持压缩、自定义Partition、以及行列等各种存储格式。

- 海量数据：对数据量不设上限。
- 种类丰富：支持行、列、TextFile等各种存储格式。
- 配置灵活：支持用户自定义Partition等配置。

图 **4-3:** 数据仓库对接

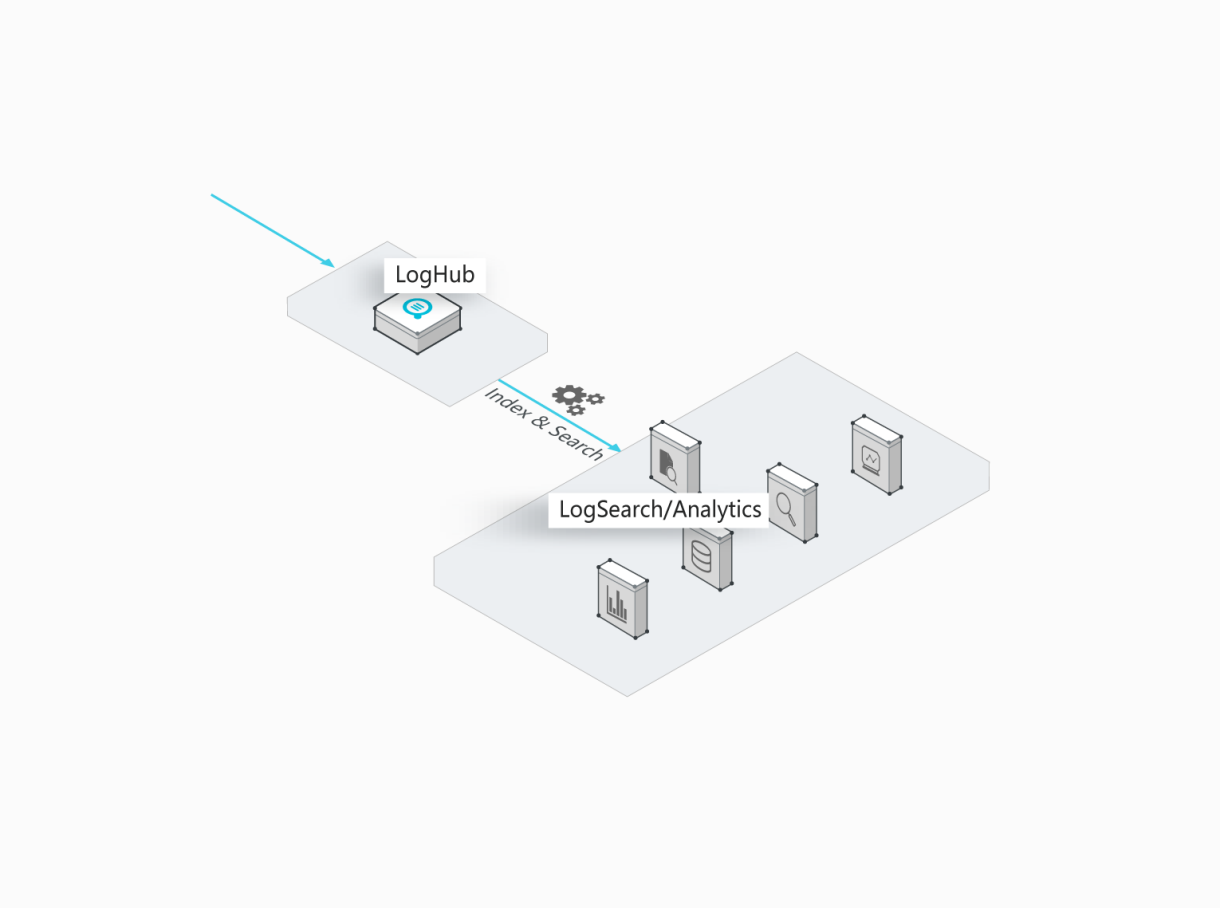


日志实时查询与分析

实时查询分析（LogAnalytics）可以实时索引LogHub中数据，提供关键词、模糊、上下文、范围、SQL聚合等丰富查询手段。

- 实时性强：写入后即可查询。
- 海量低成本：支持PB/Day索引能力，成本为自建方案15%。
- 分析能力强：支持多种查询手段，及SQL进行聚合分析，并提供可视化及报警功能。

图 4-4: 日志实时查询与分析



5 限制说明

5.1 基础资源

分类	限制说明	备注
Project	每个账号下最多可创建50个Project。	如您有更大的使用需求，请提工单申请。
Logstore	一个Project中最多可创建200个Logstore。	如您有更大的使用需求，请提工单申请。
Shard	• 一个Project中最多可创建200个Shard。 • 一个Logstore最多可创建10个Shard。但可以通过分裂操作来增加Shard。	如您有更大的使用需求，请提工单申请。
Logtail配置（LogtailConfig）	每个Project最多可创建100个Logtail配置。	如您有更大的使用需求，请提工单申请。
日志保存时间	支持永久保存。 您也可以自定义日志保存时间，取值范围为1~3000。	-
机器组（MachineGroup）	每个Project最多可创建100个机器组。	如您有更大的使用需求，请提工单申请。
协同消费组（ConsumerGroup）	每个Logstore最多可创建10个协同消费组。	可以删除不使用消费组。
快速查询（SavedSearch）	每个Project最多可创建100个快速查询。	-
仪表盘（Dashboard）	• 每个Project最多可创建50个仪表盘。 • 每个仪表盘最多可包含50张分析图表。	-
LogItem	长度最大为1 MB。	以上为API限制参数，如通过Logtail采集日志，单个LogItem最大为 512KB。
LogItem（Key）	长度最大为128 Bytes。	-

分类	限制说明	备注
LogItem（Value）	长度最大为1 MB。	-
日志组（LogGroup）	每个日志组中最多包含4096条日志，且最大长度为10 MB。	-

说明：

通过日志服务命令行工具CLI可以查看当前的Logstore、Shard、仪表盘等基础资源使用情况，详细说明请查看使用*CLI*查看基础资源使用状况。

5.2 数据读写

分类	限制项	限制说明	备注
Project	写入流量保护	写入流量最大为30 GB/min。	如超过限制，状态码会返回403，提示Inflow Quota Exceed。如您有更大的使用需求，请提工单申请。
	写入次数保护	写入次数最大为600000 次/min。	如超过限制，状态码会返回403，提示Write QPS Exceed。如您有更大的使用需求，请提工单申请。
	读取次数保护	读取次数最大为600000 次/min。	如超过限制，状态码会返回403，提示Read QPS Exceed。如您有更大的使用需求，请提工单申请。
Shard	写入流量	写入流量最大为5 MB/s。	非硬性限制，超过时系统会尽可能服务，但不保证服务质量。
	写入次数	写入次数最大为500 次/s。	非硬性限制，超过时系统会尽可能服务，但不保证服务质量。
	读取流量	读取流量最大为10 MB/s。	非硬性限制，超过时系统会尽可能服务，但不保证服务质量。

分类	限制项	限制说明	备注
	读取次数	读取次数最大为100 次/s。	非硬性限制，超过时系统会尽可能服务，但不保证服务质量。

5.3 查询分析与可视化

分类	分类	限制说明	备注
查询（Search）	关键词个数	关键词，即单词查询时布尔逻辑符外的条件个数。每次查询最多30个。	例如"a and b or c and d..."。
	单个字段长度	单个字段（Value）长度最大为10 KB，超出部分不参与查询。	如果单个字段长度大于10 KB，有一定几率无法通过关键词查询到日志，但数据仍然是完整的。
	单个Project并发	单个Project并发最大为100个。	-
	返回的查询结果条数	每次查询时，默认最多返回100条查询结果。	可以通过翻页读取完整的查询结果。
	单条日志内容显示	由于网页浏览器性能原因，对于超过1w个字符的日志，日志服务只会对前10,000个字符进行DOM切词处理。	-
SQL分析（Analytics）	单个字段（Value）最大长度	单个字段（Value）最大长度为2 KB，超出部分不参与查询。	超出限制时查询结果可能不精确，但数据仍然是完整的。
	单个Project并发	单个Project并发不超过30个。	-
	每次分析的结果条数	每次分析返回结果最大100 MB或100000条。	-

5.4 保留字段

日志服务中有部分字段为保留字段，使用API写入数据，或添加Logtail采集配置时，请不要将字段名称设置为日志服务的保留字段。

在采集日志或投递数据到其他云产品时，日志服务可以将日志来源、时间戳等信息以Key-Value对的形式添加到日志中，其中字段名称为__source__等固定名称，这些字段是日志服务的保留字段。使用API写入日志数据或添加Logtail配置时，请不要将Key即字段名称设置为这些保留字段，否则可能会造成字段名称重复、查询不精确等问题。

目前，日志服务的保留字段包括：

表 5-1: 日志服务保留字段

保留字段名称	数据格式	索引与统计设置	说明
__time__	整型，Unix标准时间格式。	• 索引设置：__time__通过API中的参数from和to选择，无需添加该字段的索引。 • 统计设置：当用户为任何一列开启统计后，默认为__time__开启统计。	使用API/SDK写入日志数据时指定的日志时间，该字段可用于日志投递、查询、分析。
__source__	字符串格式。	• 索引设置：开启索引后，日志服务默认为__source__创建索引，索引数据类型为text类型，分词字符为空。查询时输入 source:127.0.0.1 或者 __source__:127.0.0.1 。 • 统计设置：当用户为任何一列开启统计后，默认为__source__开启统计。	日志来源设备。该字段可用于日志投递、查询、分析、自定义消费。
__topic__	字符串格式。	• 索引设置：开启索引后，日志服务默认为__topic__创建索引，索引数据类型为text类型，分词字符为	日志主题（Topic）。如果您设置了日志主题，日志服务会自动为您的日志添加日志主题字段，Key为__topic__，Value为您的主题内容。该字

保留字段名称	数据格式	索引与统计设置	说明
		空。查询时输入__topic__:XXX。 • 统计设置：当用户为任何一列开启统计后，默认为__topic__开启统计。	段可用于日志投递、查询、分析、自定义消费。
__partition_time__	字符串格式。	日志内容中不存在该字段，无需设置索引。	投递MaxCompute的日志分区时间列。由__time__计算得到，用于日志投递MaxCompute时设置日期格式分区列，详细说明请参考投递日志到*MaxCompute*。
__extract_others__	字符串，可反序列化成JSON Map。	日志内容中不存在该字段，无需设置索引。	日志中投递MaxCompute的未配置字段组装为一个JSON Map。用于日志投递MaxCompute时打包其它未单独配置的字段，详细说明请参考投递日志到*MaxCompute*。
_extract_others_	字符串，可反序列化成JSON Map。	日志内容中不存在该字段，无需设置索引。	与__extract_others__相同，建议使用__extract_others__。
__tag__:__client_ip__	字符串格式。	• 索引设置：开启索引后，日志服务默认为所有标签*#Tag#*字段创建索引，索引数据类型为text类型，分词字符为空，在查询时要完全命中，或采用模糊查询。 • 统计设置：默认没有为该列开启统计。如需开启统计，请手动添加__tag__:__client_ip__的索引，并开启统计功能。	日志来源设备的公网IP，该字段为系统标签（Tag）。开启记录外网*IP*功能后，服务端接收日志时为原始日志追加该字段。可用于日志投递、查询、分析、自定义消费。
__tag__:__receive_time__	字符串，可转换为整型的Unix标准时间格式。	• 索引设置：开启索引后，日志服务默认为所有标签*#Tag#*创建索引，索引数据类型为text类型，分词字	日志到达服务端的时间，该字段为系统标签*#Tag#*。开启记录外网*IP*功能后，服务端接收日志时为原始日志追加该字段。

保留字段名称	数据格式	索引与统计设置	说明
		符为空，在查询时要完全命中，或采用模糊查询。 • 统计设置：默认没有为该列开启统计。如需开启统计，请手动添加`__tag__:__receive_time__`的索引，并开启统计功能。	可用于日志投递、查询、分析、自定义消费。
`__raw_log__`	字符串格式。	请手动添加并设置该字段的索引，索引数据类型为text，并根据需求选择是否开启统计。	解析失败的原始日志。关闭丢弃解析失败日志功能后，Logtail在解析日志失败时上传原始日志。其中Key为`__raw_log__`、Value为日志内容。
`__raw__`	字符串格式。	请手动添加并设置该字段的索引，索引数据类型为text，并根据需求选择是否开启统计。	解析成功的原始日志。开启上传原始日志功能后，Logtail会将原始日志作为`__raw__`字段，和解析后的日志一并上传。一般用于审计、合规审查等场景。