ALIBABA CLOUD

阿里云

日志服务

日志服务公共云合集

文档版本：20220712

阿里云

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
危险	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。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会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，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	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。	单击**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。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 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。	`switch {active|stand}`

目录

1.快速入门

本文介绍如何通过Logtail完整正则模式采集ECS日志，并对日志进行查询与分析。

前提条件

- 已有可用的ECS。更多信息，请参见云服务器ECS快速入门。
- ECS服务器上已有待采集的日志。

背景信息

本示例中待采集的日志路径为*/var/log/nginx/access.log*，日志样例为 `127.0.0.1 - - [10/Jun/2022:12:36:49 +0800] "GET /index.html HTTP/1.1" 200 612 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36"` 。针对该日志样例，本文介绍通过完整正则模式采集的操作步骤。

操作视频

本视频指导您快速使用日志服务。

步骤一：开通日志服务

1. 登录日志服务控制台。
2. 根据页面提示，开通日志服务。

   日志服务的计费说明，请参见计费概述。

步骤二：创建Project和Logstore

1. 创建Project。
   i. 在Project列表区域，单击**创建Project**。
   ii. 在**创建Project**面板中，按照如下说明配置参数，其他参数均可保持默认配置。更多信息，请参见创建Project。

参数	描述
Project名称	Project的名称，全局唯一。创建Project成功后，无法更改其名称。
所属地域	Project的数据中心。建议选择与ECS相同的地域，即可使用阿里云内网采集日志，加快采集速度。 创建Project后，无法修改其所属地域，且日志服务不支持跨地域迁移Project。

   iii. 单击**确定**。
2. 创建Logstore。

   创建Project完成后，系统会提示您创建一个Logstore。

   在**创建Logstore**面板中，按照如下说明配置参数，其他参数均可保持默认配置。更多信息，请参见创建Logstore。

参数	描述

参数	描述
Logstore名称	Logstore的名称，在其所属Project内必须唯一。创建Logstore成功后，无法更改其名称。
Shard数目	日志服务使用Shard读写数据。 一个Shard提供的写入能力为5 MB/s、500次/s，读取能力为10 MB/s、100次/s。如果一个Shard就能满足您的业务需求，您可配置**Shard数目**为1。
自动分裂Shard	开启自动分裂功能后，如果您写入的数据量超过已有Shard服务能力，日志服务会自动根据数据量增加Shard数量。 如果您确保配置的Shard数量已满足业务需求，可关闭**自动分裂Shard**开关。

步骤三：采集日志

创建Logstore成功后，系统将提示您接入数据。

1. 在**创建成功**对话框中，单击**确定**。
2. 在**快速数据接入**对话框的**自建开源/商业软件**页签下，单击**正则-文本日志**。
3. 安装Logtail。
   i. 在**ECS机器**页签中，选中目标ECS实例，单击**立即执行**。
   ii. 确认**执行状态**为**成功**后，单击**确认安装完毕**。
4. 创建IP地址类型的机器组，单击**下一步**。

   按照如下说明配置参数，其他参数均可保持默认配置。更多信息，请参见创建IP地址机器组。

参数	说明
名称	机器组的名称，在其所属Project内必须唯一。创建机器组成功后，无法更改其名称。
IP地址	ECS服务器IP地址。多个IP地址之间请用换行符分隔。 **注意** 请勿将Windows机器和Linux机器添加到同一机器组中。

5. 选中目标机器组，将该机器组从**源机器组**移动到**应用机器组**，单击**下一步**。

   注意 如果创建机器组后立刻应用，可能因为连接未生效，导致心跳为FAIL，您可单击**自动重试**。如果还未解决，请参见Logtail机器组无心跳进行排查。

6. 创建Logtail采集配置，单击**下一步**。

   按照如下说明配置参数，其他参数均可保持默认配置。更多信息，请参见使用完整正则模式采集日志。

参数	描述

参数	描述
配置名称	Logtail采集配置的名称，在其所属Project内必须唯一。创建Logtail采集配置成功后，无法修改其名称。
日志路径	待采集的日志的目录和文件名。 日志的目录和文件名支持完整名称和通配符两种模式，文件名规则请参见Wildcard matching。日志文件查找模式为多层目录匹配，即指定目录（包含所有层级的目录）下所有符合条件的文件都会被查找到。例如： ○ */apsara/nuwa/**/*.log*表示*/apsara/nuwa*目录（包含该目录的递归子目录）中后缀名为*.log*的文件。 ○ */var/logs/app_*/*.log*表示*/var/logs*目录下所有符合*app_**模式的目录（包含该目录的递归子目录）中包含*.log*的文件。 **说明** ○ 默认情况下，一个文件只能匹配一个Logtail配置。如果文件中的日志需要被采集多份，请参见如何实现文件中的日志被采集多份。 ○ 目录通配符只支持星号（*）和半角问号（?）。
日志样例	根据实际场景输入一条日志样例。例如： `127.0.0.1 - - [10/Jun/2022:12:36:49 +0800] "GET /index.html HTTP/1.1" 200 612 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36"`
提取字段	打开**提取字段**开关后，可通过正则表达式将日志内容提取为键值对。
正则	打开**提取字段**开关后，需要配置。 ○ 自动生成正则表达式 在**日志样例**文本框中，选中需要提取的日志内容，单击**生成正则**，自动生成正则表达式。例如 `(\S+)\s-\s(\S+)\s\[([^]]+)]\s"(\w+)([^"]+)"\s(\d+)\s(\d+)[^-]+([^"]+)"\s"([^"]+).*` 。 ○ 手动输入正则表达式 单击**手动输入正则表达式**，手动配置正则表达式。配置完成后，单击**验证**即可验证您输入的正则表达式是否可以解析、提取日志样例。更多信息，请参见如何调试正则表达式。
日志抽取内容	打开**提取字段**开关后，需要配置。 通过正则表达式将日志内容提取为Value后，您需要为每个Value设置对应的Key。

单击**下一步**即表示创建Logtail采集配置完成，日志服务开始采集日志。

> **说明**
> - Logtail采集配置生效时间最长需要3分钟，请耐心等待。
> - 如果遇到Logtail采集报错，请参见如何查看Logtail采集错误信息。

7. 预览数据及设置索引，单击**下一步**。

   日志服务默认开启全文索引。您也可以根据采集到的日志，手动或者自动设置字段索引。更多信息，请参见配置索引。

   > **说明** 如果您要查询分析日志，那么全文索引和字段索引属性必须至少启用一种。同时启用时，以字段索引为准。

步骤四：查询与分析日志

配置索引后，您可以查询与分析日志。

1. 在配置向导的**结束**步骤中，单击**查询日志**。
2. 在目标Logstore的查询与分析页面，输入查询与分析语句，选择时间范围，单击**查询/分析**。

   例如：执行如下查询与分析语句统计各个状态码对应的请求数量，并通过表格展示查询与分析结果。

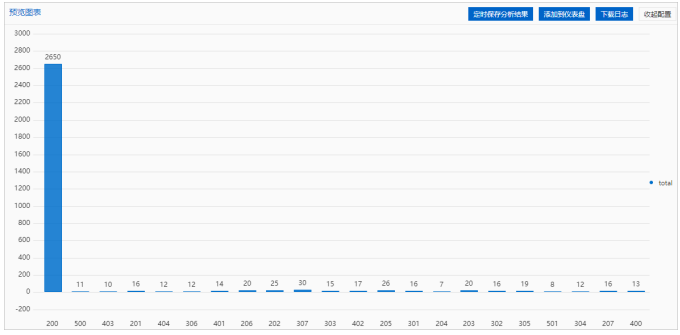
   - 查询与分析语句

     ```
     * | SELECT status, COUNT(status) AS total GROUP BY status
     ```

     关于查询与分析语句的更多信息，请参见查询概述和分析简介。

   - 查询与分析结果

     日志服务支持通过统计图表展示查询与分析结果。更多信息，请参见可视化概述。

常见问题

- 仅创建Project和Logstore，会产生费用吗？

  当您在创建Logstore时，日志服务默认预留Shard资源，因此可能产生活跃Shard租用费用。更多信息，请参见为什么会产生活跃Shard租用费用。

- 采集日志失败，如何排查？

  使用Logtail采集日志失败，可能是因为Logtail心跳异常、采集错误、Logtail采集配置错误等原因。如何排查，请参见Logtail采集日志失败的排查思路。

- 在Logstore查询与分析页面，可以查询日志但无法分析日志，如何解决？

  如果您要分析日志，需要为日志字段配置字段索引并开启统计功能。更多信息，请参见配置索引。

2.最佳实践

本文罗列了日志服务相关的最佳实践。

数据采集

- IoT/嵌入式日志
- 通过WebTracking采集日志
- 搭建移动端日志直传服务
- 采集公网数据
- 多渠道数据
- 采集Zabbix数据
- 跨阿里云账号采集日志
- 跨阿里云账号采集容器日志

时序存储

使用Prometheus采集Kubernetes监控数据

查询与分析

- 查询和分析网站日志
- 查询和分析JSON日志
- Data Explorer案例
- 关联Logstore与MySQL数据库进行查询分析
- 关联Logstore与OSS外表进行查询和分析
- 查询MNS日志
- 采集及分析Nginx监控日志
- 分析Nginx访问日志
- 分析Apache日志
- 分析IIS日志
- 分析Log4j日志
- 分析网站日志
- 查询分析程序日志
- 分析负载均衡7层访问日志
- 分页显示查询分析结果
- 分析行车轨迹日志
- 分析销售系统日志

数据加工

- 调用函数清洗数据
- 事件判断
- 处理日期时间
- 数据脱敏

- 解析Syslog标准格式数据
- 解析Nginx日志
- 解析Java报错日志
- 提取字符串动态键值对
- 特定格式文本数据加工
- 解析CSV格式日志
- 复杂JSON数据加工
- 转换Log为Metric
- 从其他Logstore获取数据进行数据富化
- 从OSS获取IPIP库进行IP地址数据富化
- 从OSS获取IP2Location库进行IP地址数据富化
- 从OSS获取CSV文件进行数据富化
- 从RDS MySQL数据库获取数据进行数据富化
- 使用RDS内网地址访问RDS MySQL数据库
- 使用资源函数增量获取数据
- 使用e_dict_map、e_search_dict_map函数进行数据富化
- 从Hologres数据库获取数据进行富化
- 构建字典与表格做数据富化
- 使用e_table_map函数对HTTP请求返回码进行富化
- 复制Logstore数据
- 跨地域传输数据
- 多目标Logstore数据分发
- 多源Logstore数据汇总
- 复制和分发数据

告警

- 基于日志关键字设置告警
- 迁移Prometheus告警到日志服务
- 自定义分析告警日志

可视化

- 添加变量类型的过滤器
- 添加过滤器类型的过滤器
- 添加多Y轴线图

消费与投递

- 对接数据仓库
- 搭建监控系统
- 计量计费日志
- 通过Consumer Library实现高可靠消费

日志应用

通用数据库审计

Kubernetes中的通用数据库审计部署方案

Trace服务

- 导出Trace数据到Grafana
- 接入Apache SkyWalking Trace数据到日志服务
- 在K8s环境下接入Apache SkyWalking Trace数据到日志服务
- 接入Kubernetes Ingress链路数据

智能异常分析

- 多维指标智能巡检
- 日志聚合多维指标智能巡检
- 对云监控指标进行智能巡检

开发指南

监控日志服务

监控日志服务

其他

- SLS多云日志采集、处理及分析
- 微服务架构日志采集运维管理

3.常见问题

本文汇总日志服务的常见问题。

售前常见问题

- 什么是日志服务？
- 日志服务可以做什么？
- 日志服务能为用户带来哪些价值？
- 日志服务支持采集哪些数据？
- 日志服务支持哪些数据接入方式？
- 阿里云会使用我在日志服务上存储的数据吗？
- 阿里云是否会将自己的数据存储在日志服务上？
- 如果数据量突然激增，日志服务如何保证服务不受影响？
- 日志服务中的数据如何实现低成本存储？
- 日志服务中的数据可以保存多久？
- 如何开始使用日志服务？
- 如果有需求，如何联系？

产品计费常见问题

- 日志服务如何停止计费？
- 为什么购买了资源包仍会欠费？
- 如何选择资源包规格？
- 为什么索引流量费用是读写流量费用的几倍？
- 为什么会产生活跃Shard租用费用？
- 为什么只创建Project和Logstore会产生费用？
- 为什么删除Project和Logstore后仍产生费用？
- 在控制台上查询和分析日志是否会产生外网读取流量？
- 如何降低索引流量费用？

数据采集常见问题

数据存储常见问题

- 日志服务如何存储、管理用户的日志？
- 删除日志库，日志数据是否丢失？

- 日志服务日志保存多长时间？可否修改这个保存时限？
- 希望把日志最终存储到OSS，怎样节省在日志服务上的花费？
- 如何调整日志服务的数据保存时间
- 删除Project提示“操作拒绝，权限不足”错误

查询与分析常见问题

- 日志查询常见问题
- 查询不到日志的排查思路
- 查询与分析日志的常见报错
- 日志消费与查询区别
- 模糊查询
- 如何精确查询日志？
- 查询不精确有哪些原因？
- 如何设置字段索引？
- 如何修改SQL查询语句输出结果的行数？
- 如何查询日志的来源机器和日志条目？
- 如何精确地按照时间排序查询日志？
- 如何将日志下载到本地？

数据加工常见问题

- 错误排查概述
- 加工引擎启动错误
- 源Logstore读取错误
- 加工规则错误
- 资源加载错误
- 目标Logstore输出错误
- 获取Logstore数据（维表）错误
- 从OSS获取数据出错
- 获取RDS MySQL数据语法错误
- 如何动态构建字段？
- 如何将一条日志输出到不同目标？
- 目标Logstore无数据怎么处理？
- 目标Logstore有多余数据怎么处理？
- 如何处理数据加工延迟？

消费与投递常见问题

- 为什么实时消费的速率未达到Shard的读写阈值上限？
- 日志投递到MaxCompute后，如何检查数据完整性？
- 投递日志到OSS失败

告警常见问题

- 告警配置案例

开发常见问题

- 日志服务错误代码汇总
- CLI参考常见问题