云日志服务

常见问题

文档版本 01

发布日期 2025-02-08

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 问题总览

本文汇总云日志服务的常见问题。

产品咨询问题

- 如何从第三方云厂商将日志搬迁到华为云LTS?
- 存储在LTS的日志是否可以用于安全合规审计?
- 云日志服务LTS使用建议有哪些?
- 云日志服务LTS对比自建ELK Stack有什么优势?

日志管理

- 设置多账号日志汇聚后如何只保存一份日志内容?

主机管理

- 在Windows环境下ICAgent安装失败并提示SERVICE STOP怎么办?
- 在LTS页面升级ICAgent失败怎么办?
- 在LTS页面无法查询新产生的日志怎么办?
- ICAgent安装完成后反复重启怎么办?
- 在LTS页面完成ICAgent安装后显示离线怎么办?
- ICAgent安装完成后，在LTS页面不显示怎么办?
- 如何在VPCEP控制台创建终端节点?
- 如何获取AK/SK?
- 如何通过创建委托授权安装ICAgent?

日志接入

- 主机接入LTS后无法采集到日志?
- 在AOM关闭超额继续采集日志开关，会影响LTS收集日志吗?
- 使用ICAgent收集日志时CPU占用较高怎么处理?
- 云日志服务LTS支持采集的日志类型和文件类型有哪些?
- 如何在LTS页面关闭CCE标准输出日志采集到AOM?

- 使用ICAgent采集日志时，推荐的日志轮转方案是什么？
- 是否支持Log4j插件上报日志到LTS？
- LTS配置日志接入后多久有日志？
- 通过ICAgent接入LTS后无法采集到日志？

日志搜索与分析

- 查看LTS实时最新日志，每一次加载数据时延是多久？
- 无法查看上报到LTS的日志怎么办？
- 在LTS控制台如何手动删除日志数据？
- 在LTS页面无法搜索日志时怎么办？

日志转储

- 日志转储后，LTS会删除转储的日志内容吗？
- LTS日志转储状态显示异常是什么原因？
- 如何转储云审计服务CTS的日志？
- 配置LTS日志转储至OBS后，OBS桶无法查看历史数据？
- 日志转储至DLI后，在DLI表中查不到新增分区怎么处理？

2 产品咨询问题

2.1 如何从第三方云厂商将日志搬迁到华为云 LTS?

若用户是在第三方云厂商使用日志服务，有大量数据在第三方云厂商对象存储上，希望将日志搬迁到华为云，对于不同的日志类型，请参考如下方法：

- 热日志（用于搜索分析）：典型保存7-14天，用于应用运维，该日志不需要搬迁到华为云。用户在华为云直接启用云日志服务LTS，运行14天后，第三方云厂商保存的日志自然就老化了。详细请参考**日志管理**。
- 归档日志（用于等保合规）：典型保存180天以上，用于安全合规审计，该日志一般转储存放到对象存储中。使用对象存储的迁移工具，将第三方云厂商保存在对象存储中的文件迁移到华为云对象存储服务OBS即可。详细操作请参考**迁移第三方云厂商数据至OBS**。

2.2 存储在 LTS 的日志是否可以用于安全合规审计?

存储在云日志服务LTS的日志可以用于安全合规审计。日志上报到LTS后，LTS不支持修改日志，防止日志被篡改。因此，用户可以将日志长期存储在LTS，随时查询用于安全合规审计场景。

如果使用日志组的日志存储时间，请参考**管理日志组**修改日志存储时间；如果使用日志流的日志存储时间，请参考**管理日志流**修改日志存储时间。

2.3 云日志服务 LTS 使用建议有哪些?

云主机应用日志场景

场景描述：适用于用户将应用系统部署在云主机上，使用LTS统一采集和搜索日志的场景。用户的应用系统一般由多个组件（也称微服务）组成，每个组件部署在至少2台云主机上。

使用建议：

- 日志采集方式：建议使用采集器ICAgent采集日志，您需要在云主机上安装ICAgent，然后使用**ECS接入**配置日志采集路径。不建议使用SDK、API上报日志。

使用ICAgent的好处是与应用系统完全解耦，无侵入，无需更改代码，使用SDK/API等方式步骤相对复杂，如果代码编写不当容易对应用系统的稳定性造成影响。

- 日志组规划建议：将一个应用系统的日志放在一个日志组中，日志组的名称可以使用应用系统的名称。
- 日志流规划建议：
  - 如果您的日志是没有固定规则的日志，可以将类似组件的日志采集到同一个日志流，例如java组件、php组件、python组件。类似组件的日志采集到一个日志流的好处是日志流的数量不至于太多而难以管理，如果您的组件数量比较少（例如小于20个），您可以将每个组件的日志采集到不同的日志流。
  - 如果您的日志是类似NGINX网关这种可以结构化解析的日志，建议您将有相同格式的日志采集到同一个日志流。因为统一的日志格式才能方便您后续统一使用SQL分析功能，实现可视化图表分析。
- 权限隔离建议：云日志服务的日志流支持企业项目隔离，通过为日志流设定不同的企业项目可以实现不同IAM用户有不同日志流的访问权限。

容器应用日志场景

场景描述：适用于用户将应用系统部署在K8S集群上，使用LTS统一采集和搜索日志的场景。用户的应用系统一般由多个工作负载组成，每个工作负载至少部署2个实例。

使用建议：

- 日志采集方式：
  - 建议使用采集器ICAgent采集日志，您可以使用**CCE接入**配置日志采集路径。不建议使用SDK、API上报日志。使用ICAgent的好处是与应用系统完全解耦，无侵入，无需更改代码，使用SDK/API等方式步骤相对复杂，如果代码编写不当容易对应用系统的稳定性造成影响。
  - 采集容器应用日志的方式有：容器标准输出、容器文件、节点文件、K8S事件，建议优先使用容器文件。对比容器标准输出，容器文件的优点是可以持久化挂载到主机上，且输出的内容用户自主控制性更强。对比节点文件，容器文件的优点是采集的日志有命名空间、工作负载、POD等元数据信息，在搜索日志的时候更加便捷。
- 日志组规划：将一个CCE集群的所有日志放在一个日志组中，日志组的别名（支持修改）可以使用CCE集群的名称，日志组的原始名称（不支持修改）建议使用k8s-log-{集群ID}。
- 日志流规划：
  - 如果您的日志是没有固定规则的日志，可以将类似组件的日志采集到同一个日志流，例如java组件、php组件、python组件。类似组件的日志采集到一个日志流的好处是日志流的数量不至于太多而难以管理，如果您的组件数量比较少（例如小于20个），您可以将每个组件的日志采集到不同的日志流。
  - 如果您的日志是类似NGINX网关这种可以结构化解析的日志，建议您将相同格式的日志采集到同一个日志流。因为统一的日志格式才能方便您后续统一使用SQL分析功能，实现可视化图表分析。
- 权限隔离：云日志服务的日志流支持企业项目隔离，通过为日志流设定不同的企业项目可以实现不同IAM用户有不同日志流的访问权限。

云服务日志分析场景

- 如何采集云服务日志到LTS：LTS支持多种**云服务接入**采集到LTS，您需要在对应云服务的页面打开日志开关，即可以将日志采集到指定的日志组/日志流。
- 如何配置到最佳使用状态：很多云服务的日志都是支持结构化的，您可以在结构化配置页面为您的云服务日志配置对应的结构化解析规则，详细操作请参考**日志结构化配置**。结构化解析之后即可对日志使用SQL进行可视化分析。

应用监控告警场景

场景描述：适用于使用日志来实时监控应用系统是否正常，提前发现系统故障的场景。

SQL告警仅支持全部用户使用的局点有：华南-广州、华北-北京四、华东-上海一、中国-香港、西南-贵阳一、亚太-新加坡、华南-深圳，支持部分白名单用户使用的局点有：亚太-曼谷、华北-北京一、华东-上海二、、亚太-雅加达，其他局点暂不支持该功能。

使用建议：

- 告警统计方式：LTS有两种告警配置方式：**关键词告警**和SQL告警。如果您的日志是无规则的，那么适用关键词告警，例如java程序的运行日志；如果您的日志是有规则的，例如NGINX网关日志，那么适用SQL统计告警，您可以使用SQL语句对结构化的日志做统计分析，获取您想要的指标配置告警。
- 告警规则配置：告警触发一般需要越快越好，您的告警规则统计周期建议使用1分钟。您可以使用LTS提供的默认消息模板来发送告警。如果您有个性化的诉求，您可以在系统提供的默认模板的基础上做一些修改保存为**消息模板**，然后发送告警。
- 配置ELB/APIG等关键云服务日志告警：ELB经常用来作为应用系统的对外的入口，您可以打开ELB日志对接到LTS，然后配置ELB 5XX状态码告警，这样就可以及时发现系统是否有故障。同时您可以借助开箱即用的ELB仪表盘模板，观察应用系统整体的成功率。

业务运营分析场景

场景描述：适用于在应用系统中打印业务日志，例如交易额、客户、产品等信息，然后使用LTS的SQL分析功能，输出可视化图表和仪表盘的场景。

使用建议：

- 日志采集方式：建议使用采集器ICAgent采集日志，将日志打印到单独的日志文件中，不要与应用程序的运行日志混在一起。不建议使用SDK、API上报日志。
- 日志结构化解析方式：建议您打印的业务日志使用空格分割或者JSON格式，这样方便快速配置日志结构化解析规则。
- 日志可视化呈现：

  您可以**创建自定义仪表盘**，使用类SQL语法分析已经结构化处理好的业务日志。自定义的仪表盘中，您可以添加**多个图表**，也可以添加过滤器，使用LTS做业务分析，可以减少采购数据仓库，没有额外成本，上手更简单。

2.4 云日志服务 LTS 对比自建 ELK Stack 有什么优势?

本章节主要介绍华为云日志服务（ LTS ）对比自建ELK，帮助您更好的了解LTS的主要功能和优势。

背景信息

提到日志搜索，很多人都会想到基于ELK Stack（Elasticsearch/Logstash/Kibana）来搭建，开源的ELK方案，在社区中有大量的内容和使用案例供大家参考。

华为云日志服务LTS，聚焦3大场景（应用运维/等保合规/业务运营），为客户提供采、存、查、加工、分析和告警全托管式日志分析平台。更多信息请参考**图解云日志服务**。

功能对比

云日志服务LTS在功能特性的完备度、日志搜索分析性能方面对比ELK有明显的优势，详细对比请见如下表格：

特性	子特性	LTS	ELK	描述
日志采集	云服务日志采集	☆☆☆☆☆	无	ELK：不支持采集云服务日志。 LTS：云服务租户面日志统一采集到LTS。
	虚机和容器日志采集	☆☆☆☆☆	☆☆☆☆	ELK：使用logstash或者filebeat等开源采集器采集日志。 LTS：使用ICAgent采集日志，有提供向导页面，上手难度低。
	多语言SDK日志采集	☆☆☆	无	ELK：不支持。 LTS：提供java SDK直接上报日志到LTS
	主机组管理（主机动态扩缩容）	☆☆☆☆☆	无	ELK：不支持。 LTS：提供主机管理、主机组管理能力，主机组支持自定义标识主机组，可以管理动态扩缩容主机组。
	日志结构化解析	☆☆☆☆	☆☆☆☆☆	ELK：基于采集器实现自定义日志结构化解析。 LTS：提供结构化解析能力，可以正则表达式、JSON、分隔符、自定义模板等方式解析日志。
日志搜索	关键词搜索、模糊搜索、快速分析	☆☆☆☆☆	☆☆☆☆☆	ELK和LTS：提供类似的日志关键词搜索能力。
	实时日志查看	☆☆☆☆☆	无	ELK：未提供实时日志查看页面。 LTS：提供实时日志查看页面。

特性	子特性	LTS	ELK	描述
	百亿日志秒级搜索	☆☆☆☆☆	☆☆	ELK：自建ELK受限于机器资源数量，搜索海量日志时耗时较长。 LTS：利用公有云海量的弹性计算资源，百亿日志可以在3秒内返回搜索结果。
	千亿级日志迭代搜索	☆☆☆☆☆	无	ELK：无法直接搜索千亿条日志，会出现响应超时。 LTS：提供迭代搜索能力，用户可以直接搜索千亿条日志。
	日志管理规模	百PB级	百TB级	ELK：经常要关注机器扩容，费时费力。 LTS：按需付费，LTS自动管理百PB级日志，不用关心底层资源消耗情况。
日志搜索	SQL分析日志	☆☆☆☆☆	☆☆	ELK：SQL性能差，语法上不支持嵌套SQL。 LTS：SQL性能强，支持嵌套SQL。
日志搜索	SQL函数	☆☆☆☆☆	☆☆	ELK：只支持最基础的SQL统计函数。 LTS：在基础SQL函数基础上，提供了大量的扩展函数，例如IP函数、统计函数、环比同比函数、URL函数等，极大扩展了使用场景。
日志搜索	可视化图表	☆☆☆☆	☆☆☆	LTS：提供了表格、折线图、饼图、柱状图等多种可视化图表。
日志搜索	仪表盘	☆☆☆☆☆	☆☆	ELK：没有云服务日志开箱即用仪表盘。 LTS：提供开箱即用的仪表盘，对常见的云服务日志例如ELB/APIG/DDS/DCS/CFW等提供开箱即用的仪表盘。
日志告警	日志关键词告警和SQL告警	☆☆☆☆☆	☆	ELK：没有日志告警功能。 LTS：提供准实时的日志关键词和SQL告警功能。

特性	子特性	LTS	ELK	描述
	告警通知渠道（邮件、短信、HTTPS等）	☆☆☆☆☆	☆	ELK：无法将告警方便地以钉钉、微信、短信等方式通知用户。 LTS：对接华为云消息通知服务，能以邮件、短信、微信、钉钉、飞书、HTTP等多种渠道通知客户。
日志转储	转储到对象存储	☆☆☆☆☆	无	ELK：无法直接转储对象存储。 LTS：页面简单配置可以将日志转储到对象存储。
日志转储	转储到kafka	☆☆☆☆☆	☆☆	ELK：需要自己部署程序将日志转发到KAFKA。 LTS：页面简单配置可以将日志实时转储到KAFKA。
日志转储	转储到数据仓库	☆☆☆☆☆	无	ELK：无法直接将日志转储到数据仓库。 LTS：页面简单配置可以将日志转储到数据仓库。
日志加工	定时SQL作业	☆☆☆☆☆	无	ELK：没有定时SQL作业能力。 LTS：可以配置定时SQL作业，将原始日志加工统计为想要的少量日志结果。
	函数加工	☆☆☆☆☆	无	ELK：没有日志加工功能。 LTS：提供函数触发器，在函数服务中可以配置自定义脚本将日志灵活加工。

成本对比

场景一：

假设客户每天原始日志100GB（日志平均速率1.16MB/s），日志平均存储30天，30天原始日志总量为3000GB，日志存储方式为一主一副本。

根据Elasticsearch官方推荐，在一主一副本存储方式下，原始日志+副本数据+索引数据等合计占用的存储空间约为原始日志大小2.2倍，另外由于ES集群存在写不均匀且磁盘不能被耗尽，因此为了存储3000GB原始日志，至少需要准备3000GB*2.2（存储膨胀）*2（50%磁盘冗余） = 13200GB磁盘。

搭建ES最小典型配置是3台ECS（16U64G5TB），kafka双副本能支持缓存最近12小时的日志。

表 2-1 自建 ELK

大类	小类	月成本（合计：1764USD）	费用占比
搭建ES	3 * ECS（C6 16U64G）	3*1999*0.1401=840USD	47.6%
	云硬盘EVS（高IO 15TB）	0.35*15*1024*0.1401=753USD	42.7%
搭建KAFKA	3 * ECS（2U4G）	3*208*0.1401=87USD	4.9%
	云硬盘EVS（超高IO 3*200GB）	600*0.1401=84USD	4.7%

LTS使用**价格计算器**，计算出来月成本约为539.89USD，使用LTS的成本约为自建ELK成本的**16.7%**，原因是在小日志量场景下，自建ELK起步资源成本很高，相比于按需付费的LTS，有很大劣势。

场景二：

假设客户每天原始日志1TB（日志平均速率11.6MB/s），日志平均存储7天，7天原始日志总量为7TB，日志存储方式为一主一副本。根据Elasticsearch官方推荐，在一主一副本存储方式下，原始日志+副本数据+索引数据等合计占用的存储空间约为原始日志大小2.2倍，另外由于ES集群存在写不均匀且磁盘不能被耗尽，因此为了存储7TB原始日志，至少需要准备7TB*2.2（存储膨胀）*2（50%磁盘冗余） = 31 TB磁盘。

搭建ES最小典型配置是3台ECS（16U64G10TB），kafka双副本能支持缓存最近12小时的日志

表 2-2 自建 ELK

大类	小类	月成本（合计：2652USD）	费用占比
搭建ES	3 * ECS（C6 16U64G）	3*1999*0.1401=840USD	31.7%
	云硬盘EVS（高IO 31TB）	0.35*31*1024*0.1401=1557USD	58.7%
搭建KAFKA	3 * ECS（2U4G）	3*208*0.1401=87USD	3.3%
	云硬盘EVS（超高IO 3*400GB）	1200*0.1401=168USD	6.3%

LTS使用**价格计算器**，计算出来月成本约为3409.92USD，使用LTS的成本约为自建ELK成本的**71%**，原因是LTS的存储收费是按用量付费，自建ELK为了保证集群的正常运行需要留有很多磁盘冗余。

场景三：

假设客户每天原始日志5TB（日志平均速率58MB/s），日志平均存储30天，30天原始日志总量为150TB，日志存储方式为一主一副本。

根据Elasticsearch官方推荐，在一主一副本存储方式下，原始日志+副本数据+索引数据等合计占用的存储空间约为原始日志大小2.2倍，另外由于ES集群存在写不均匀且磁盘不能被耗尽，因此为了存储150TB原始日志，至少需要准备150TB*2.2（存储膨胀）*2（50%磁盘冗余）= 660 TB磁盘。

搭建ES最小典型配置是66台ECS（16U64G10TB），kafka双副本能支持缓存最近12小时的日志

表 2-3 自建 ELK

大类	小类	月成本（合计：52440USD）	费用占比
搭建ES	66 * ECS（C6 16U64G）	66*1999*0.1401=18489USD	35.3%
	云硬盘EVS（高IO 660TB）	0.35*660*1024*0.1401=33149USD	63.2%
搭建KAFKA	3 * ECS（2U4G）	3*208*0.1401=87USD	0.2%
	云硬盘EVS（超高IO 3*1700GB）	5100*0.1401=715USD	1.4%

LTS使用**价格计算器**，计算出来月成本约为27648USD，使用LTS的成本约为自建ELK成本的**28.8%**，原因是LTS的存储收费是按用量付费，自建ELK为了保证集群的正常运行需要留有很多磁盘冗余。

总结

云日志服务LTS在功能、性能、成本方面对比ELK都有明显的优势，推荐您使用全托管式的云日志服务替代自建ELK。

3 日志管理

3.1 设置多账号日志汇聚后如何只保存一份日志内容?

参考**设置多账号日志汇聚**成功后，即源日志组/日志流的日志内容汇聚到目标日志组/日志流，LTS同时保存用户两个账号下的日志内容。用户创建源日志组/日志流和目标日志组/日志流时会设置日志存储时间，LTS按照日志存储时间保存日志内容。如何设置保存一份日志内容，请参考如下操作。

关闭日志存储

步骤1 使用源日志组/日志流所在的账号登录云日志服务LTS控制台。

步骤2 在日志管理页面，找到源日志组/日志流。

步骤3 单击源日志流操作列的  ，在修改日志流页面，关闭日志存储和日志存储时间。

图 3-1 修改日志流

步骤4 单击“确定”。关闭日志存储后，日志不会存储到LTS，可节约**索引流量和存储费用**，只能使用日志生成指标、转储功能，不能使用日志搜索分析、告警、消费加工等其他功能。

----结束

4 主机管理

4.1 在 Windows 环境下 ICAgent 安装失败并提示 SERVICE STOP 怎么办?

问题现象

在Windows环境下ICAgent安装失败，提示“SERVICE STOP”。

安装失败后，可能出现以下情况：

- 任务管理器中不存在ICAgent任务。
- 系统服务列表中不存在ICAgent服务。
- 命令行工具下执行**sc query icagent**提示未找到。

可能原因

一般为杀毒软件，如360安全卫士等，拦截了ICAgent服务注册。

解决方法

1. 检查是否有杀毒软件正在运行，如有，请执行下一步。
2. 关闭杀毒软件后再进行ICAgent安装。详细请参考**安装ICAgent**。

4.2 在 LTS 页面升级 ICAgent 失败怎么办?

因为ICAgent安装是覆盖式安装，无需先卸载，因此在LTS页面升级ICAgent失败时，重新执行安装命令再次进行升级ICAgent即可。

详细请参考**安装ICAgent**。

4.3 在 LTS 页面无法查询新产生的日志怎么办?

问题现象

在LTS页面无法查询新产生的日志。

对系统的影响

导致用户无法查询业务日志。

可能原因

1. LTS控制台上的“ICAgent采集开关”被关闭。
2. ICAgent上报日志到LTS失败。
3. 在LTS控制台设置的采集配置下发到ICAgent有误。

排查方法

请按如下步骤排查。

步骤1 确认ICAgent采集开关是否开启。

1. 登录**云日志服务控制台**。
2. 选择“配置中心”。
3. 在“ICAgent采集开关”页签，确认ICAgent采集开关是否开启。若没有开启，则需要开启ICAgent采集开关。

步骤2 检查最近一次下发的ICAgent采集开关配置。

1. 登录ICAgent所在的ECS主机。
2. 执行**cd /var/ICAgent**进入ICAgent日志目录。
3. 执行如下命令，查询日志采集配置。

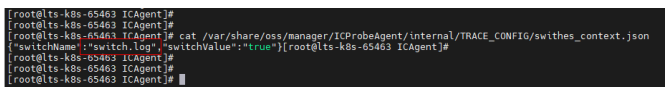
```
zgrep switchList *.zip    //查询已转储日志压缩包
cat oss.icAgent.trace | grep switchList  //查询当前日志文件
```

从过滤结果查找日志时间最新的配置，并查看switch.log是否为true（代表开启ICAgent采集开关）。

步骤3 检查ICAgent采集开关文件的内容switch.log是否为true（代表开启ICAgent采集开关）。

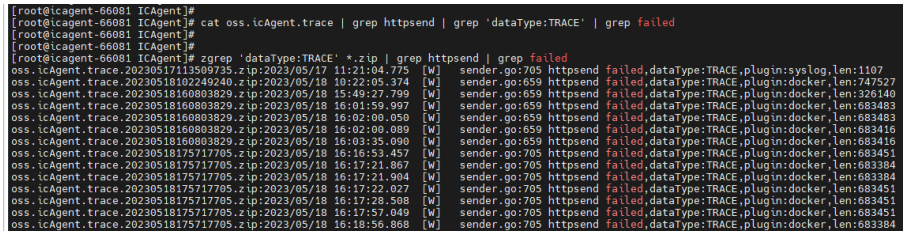
1. 登录ICAgent所在的ECS主机。
2. 查询ICAgent采集开关文件。

```
cat /var/share/oss/manager/ICProbeAgent/internal/TRACE_CONFIG/swithes_context.json
```



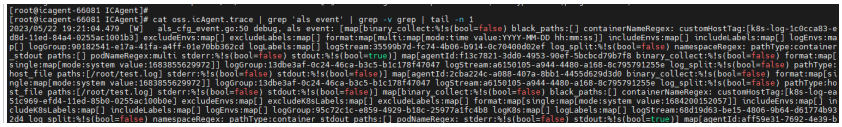
ICAgent采集开关文件的内容switch.log为true。

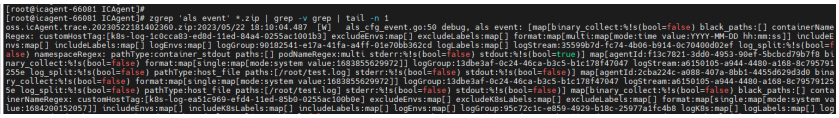
步骤4 确认日志是否发送失败。

1. 登录ICAgent所在ECS主机。
2. 执行**cd /var/ICAgent**进入ICAgent日志目录。
3. 查询发送失败日志。
   ```
   cat oss.icAgent.trace | grep httpsend | grep 'dataType:TRACE' | grep failed
   zgrep 'dataType:TRACE' *.zip | grep httpsend | grep failed
   ```
   
   ```
   [root@icagent-66081 ICAgent]#
   [root@icagent-66081 ICAgent]# cat oss.icAgent.trace | grep httpsend | grep 'dataType:TRACE' | grep failed
   [root@icagent-66081 ICAgent]#
   [root@icagent-66081 ICAgent]#
   [root@icagent-66081 ICAgent]# zgrep 'dataType:TRACE' *.zip | grep httpsend | grep failed
   oss.icAgent.trace.20230517113509735.zip:2023/05/17 11:21:04.775  [W]   sender.go:705 httpsend failed,dataType:TRACE,plugin:syslog,len:1107
   oss.icAgent.trace.20230518102249240.zip:2023/05/18 10:22:05.374  [W]   sender.go:659 httpsend failed,dataType:TRACE,plugin:docker,len:747527
   oss.icAgent.trace.20230518160803829.zip:2023/05/18 15:49:27.799  [W]   sender.go:659 httpsend failed,dataType:TRACE,plugin:docker,len:326140
   oss.icAgent.trace.20230518160803829.zip:2023/05/18 16:01:59.997  [W]   sender.go:659 httpsend failed,dataType:TRACE,plugin:docker,len:683483
   oss.icAgent.trace.20230518160803829.zip:2023/05/18 16:02:00.050  [W]   sender.go:659 httpsend failed,dataType:TRACE,plugin:docker,len:683483
   oss.icAgent.trace.20230518160803829.zip:2023/05/18 16:02:00.089  [W]   sender.go:659 httpsend failed,dataType:TRACE,plugin:docker,len:683416
   oss.icAgent.trace.20230518160803829.zip:2023/05/18 16:03:35.090  [W]   sender.go:659 httpsend failed,dataType:TRACE,plugin:docker,len:683416
   oss.icAgent.trace.20230518175717705.zip:2023/05/18 16:16:53.457  [W]   sender.go:705 httpsend failed,dataType:TRACE,plugin:docker,len:683451
   oss.icAgent.trace.20230518175717705.zip:2023/05/18 16:17:21.867  [W]   sender.go:705 httpsend failed,dataType:TRACE,plugin:docker,len:683384
   oss.icAgent.trace.20230518175717705.zip:2023/05/18 16:17:21.904  [W]   sender.go:705 httpsend failed,dataType:TRACE,plugin:docker,len:683384
   oss.icAgent.trace.20230518175717705.zip:2023/05/18 16:17:22.027  [W]   sender.go:705 httpsend failed,dataType:TRACE,plugin:docker,len:683451
   oss.icAgent.trace.20230518175717705.zip:2023/05/18 16:17:28.508  [W]   sender.go:705 httpsend failed,dataType:TRACE,plugin:docker,len:683451
   oss.icAgent.trace.20230518175717705.zip:2023/05/18 16:17:57.049  [W]   sender.go:705 httpsend failed,dataType:TRACE,plugin:docker,len:683451
   oss.icAgent.trace.20230518175717705.zip:2023/05/18 16:18:56.868  [W]   sender.go:705 httpsend failed,dataType:TRACE,plugin:docker,len:683384
   ```

   若显示failed代表日志发送失败，则需要联系LTS技术支持工程师排查。

步骤5 检查在LTS控制台设置的日志采集配置已下发到ICAgent。

1. 登录ICAgent所在ECS主机。
2. 执行**cd /var/ICAgent**进入ICAgent日志目录。
3. 过滤日志文件查询LTS页面设置的日志采集配置。
   ```
   cat oss.icAgent.trace | grep 'als event' | grep -v grep | tail -n 1
   ```
   

   以上截图仅供参考，请以实际查询结果为准。从过滤结果查找用户实际设置的日志组、日志流以及采集路径，则确保日志采集配置已下发到ICAgent。
4. 如果日志文件查询不到，则查询日志压缩包。
   ```
   zgrep 'als event' *.zip | grep -v grep | tail -n 1
   ```
   

   从日志压缩包查找用户实际设置的日志组、日志流以及采集路径，则确保日志采集配置已下发到ICAgent。
5. 登录云日志服务LTS控制台，在日志接入页面，检查配置接入任务设置的日志采集配置。

----结束

4.4 ICAgent 安装完成后反复重启怎么办?

问题现象

ICAgent安装完成后反复重启。

对系统的影响

影响ICAgent指标/日志采集。

可能原因

- 资源占用超过ICAgent自身的限制。
- ICAgent异常。

排查方法

步骤1 登录ICAgent所在ECS主机。

步骤2 执行**cd /var/ICAgent**进入ICAgent日志目录。

步骤3 查询当前日志文件，检查资源占用是否异常。

```
cat oss.icAgent.trace| grep 'icagent exit'
```

- 若有回显结果，表示资源有异常，请根据实际回显情况排查处理。
- 若没有回显结果，表示资源使用正常。

步骤4 查询历史日志文件，检查资源占用是否异常。

```
zgrep 'icagent exit' *.zip
```

- 若有回显结果，表示资源有异常，请根据实际回显情况排查处理。
- 若没有回显结果，表示资源使用正常。

步骤5 查询ICAgent启动日志文件，检查ICAgent是否异常。

```
cat oss.script.trace | grep runtime
```

- 若有回显结果，表示ICAgent有异常，请根据实际回显情况排查处理。
- 若没有回显结果，表示ICAgent使用正常。

步骤6 查询ICAgent启动历史日志文件，检查ICAgent是否异常。

```
zgrep runtime oss.script.*.zip
```

- 若有回显结果，表示ICAgent有异常，请根据实际回显情况排查处理。
- 若没有回显结果，表示ICAgent使用正常。

----结束

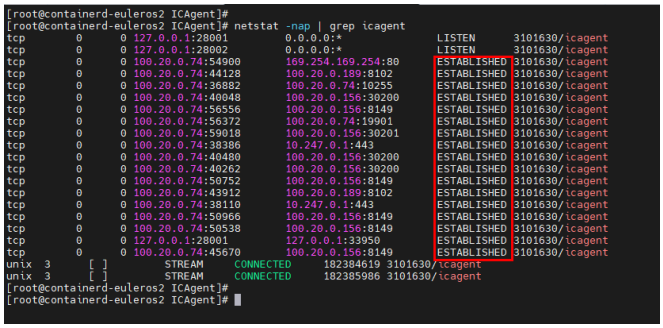
4.5 在 LTS 页面完成 ICAgent 安装后显示离线怎么办?

在LTS页面完成ICAgent安装后显示离线，请按如下步骤检查：

步骤1 检查ICAgent网络连接是否正常。

1. 登录ICAgent所在的主机。
2. 执行**netstat -nap | grep icagent**，检查ICAgent进程网络连接状态为ESTABLISHED，则代表网络连接正常。

   查看服务端30200、30201端口连接状态是否是ESTABLISHED，如果不是ESTABLISHED，则检查安全组是否放通30200、30201端口。



步骤2 检查ICAgent认证是否成功。

1. 执行**cd /var/ICAgent**进入ICAgent日志目录。
2. 执行**zgrep 'msworkflow' * | grep 'retCode\['**查询ICAgent的认证日志。
   - 查看认证返回码是200，则代表认证成功，若认证成功还是显示离线请联系技术支持工程师协助。
   - 查看认证返回码不是200，则检查ICAgent安装输入的AK/SK是否正确。若不正确，请执行下一步。

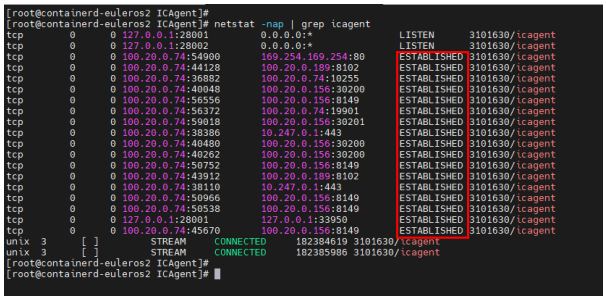
步骤3 请获取正确的AK/SK后重新安装ICAgent。请参考**如何获取AK/SK?** 。

----结束

4.6 ICAgent 安装完成后，在 LTS 页面不显示怎么办?

ICAgent安装完成后，在云日志服务控制台的“主机管理 > 主机”页面不显示对应主机如何解决?

- 若日志接入方式为“ECS接入”时，ICAgent安装完成后在主机页面不显示，请参考如下步骤排查：
  a. 在安装ICAgent页面确认安装命令复制正确，不能使用跨region的安装命令。
  b. 检查已获取的AK/SK是否正确，且AK/SK没有被删除。
  c. 执行**netstat -nap | grep icagent**命令，查看主机网络连接状态为ESTABLISHED代表网络连接正常。



- 若日志接入方式为“CCE接入”时，ICAgent安装完成后在主机页面不显示，请参考如下步骤排查：

  a. 确保CCE集群已安装ICAgent。
  b. 若没有安装ICAgent，在主机页面，选择“CCE集群”，单击“升级ICAgent”。详细操作请参考**升级ICAgent**。
- 若以上解决办法无法解决您的问题，请**提交工单**寻求技术支持工程师的帮助。

4.7 如何在 VPCEP 控制台创建终端节点?

终端节点用于在VPC和终端节点服务之间建立便捷、安全、私密的连接通道。当前支持通过创建终端节点和AOM/LTS服务打通网络，然后进行心跳、指标数据以及日志上报。

如果要通过终端节点的方式打通AOM/LTS的网络，需要为AOM和LTS各自购买1个终端节点。

创建AOM/LTS终端节点的方法：

1. 登录华为云VPC终端节点 VPCEP控制台，进入终端节点页面。
2. 单击“购买终端节点”。
3. 在购买终端节点页面，选择终端节点所在的区域，“服务类别”选择“云服务”，在“选择服务”下方查找并选择AOM的云服务，并且勾选“创建内网域名”，选择终端节点所在的虚拟私有云和子网，其他参数默认设置。更多操作请参考**购买终端节点**。

4. 设置完成后，单击“立即购买”。购买成功后，即可完成AOM终端节点的创建。
5. 重复上面步骤，需要再购买1个终端节点，选择终端节点所在的区域，“服务类别”选择“云服务”，在“选择服务”下方查找并选择LTS的云服务，并且勾选“创建内网域名”，选择终端节点所在的虚拟私有云和子网，其他参数默认设置。
6. 设置完成后，单击“立即购买”。购买成功后，即可完成了LTS终端节点的创建。

4.8 如何获取 AK/SK?

AK/SK（Access Key ID/Secret Access Key）即访问密钥，表示一组密钥对。

- AK：访问密钥ID，是与私有访问密钥关联的唯一标识符。访问密钥ID和私有访问密钥一起使用，对请求进行加密签名。
- SK：与访问密钥ID结合使用的密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。

请获取并使用公共用户账号的AK/SK，请勿使用个人账号的AK/SK。

- 每个用户最多可创建2个AK/SK，且一旦生成永久有效。
- 请确保公共用户账号及其创建的AK/SK不会被删除或禁用。AK/SK被删除，会导致安装的ICAgent无法正常上报数据到LTS。

新增访问密钥

步骤1 登录华为云，在右上角单击“控制台”。

图 4-1 进入控制台

步骤2 在“控制台”页面，鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”。

图 4-2 选择我的凭证

步骤3 在“我的凭证”页面，单击“访问密钥”页签。

步骤4 单击“新增访问密钥”。

图 4-3 新增访问密钥

说明

- 每个用户最多可创建2个访问密钥，**不支持增加配额**。如果您已拥有2个访问密钥，将无法创建访问密钥。
- 如需修改访问密钥，请删除访问密钥后重新创建。
- 为了保证历史兼容性，我们会使用访问密钥创建时间作为最近使用时间的初始值。在您使用该访问密钥时，系统将自动刷新最近使用时间。

步骤5 单击“立即下载”，生成并下载访问密钥。

创建访问密钥成功后，您可以在访问密钥列表中查看访问密钥ID（AK），在下载的.csv文件中查看访问密钥（SK）。

说明

- 请及时下载保存，弹窗关闭后将无法再次获取该密钥信息，但您可重新创建新的密钥。
- 当您下载访问密钥后，可以在浏览器页面左下角打开格式为.csv的访问密钥文件，或在浏览器“下载内容”中打开。
- 为了账号安全性，建议您妥善保管并定期修改访问密钥，修改访问密钥的方法为删除旧访问密钥，然后重新生成。

----结束

4.9 如何通过创建委托授权安装 ICAgent?

安装ICAgent时，可以选择创建IAM委托方式，通过委托授权，ICAgent可以自动获取AK/SK（访问密钥），生成ICAgent的安装命令。

创建委托

1. 登录统一身份认证服务控制台。
2. 在左侧导航栏单击“委托”，进入委托页面。
3. 单击右上角“创建委托”，具体操作请参考**委托其他云服务管理资源**，创建委托时参数设置要求参考如下。
   a. 委托类型：选择“云服务”。
   b. 云服务：选择“弹性云服务器 ECS 裸金属服务器 BMS”。
   c. 持续时间：选择“永久”。
   d. 授权权限：需要同时添加LTS Administrator和APM Administrator，授权后需等待15-30分钟才可生效。
   e. 权限的作用范围：指定区域项目资源。
4. 委托创建成功后，设置委托生效。
   a. 进入弹性云服务器控制台。
   b. 单击需要安装ICAgent的弹性云服务器名称，进入弹性云服务器参数配置页面。
      您可以在购买ECS机器时设置委托，请在“购买弹性云服务器”页面，“高级配置”中选择“现在配置”，在“委托”中选择已创建的委托名称。待剩余参数配置完成后，单击“立刻购买”即可。
   c. 在管理信息下方的“委托”后，单击  ，选择已创建的委托名称，单击  即可生效。更多关于委托的信息，请参见**委托其他账号管理资源**。

5 日志接入

5.1 主机接入 LTS 后无法采集到日志?

如果主机接入LTS后无法采集到日志，请按如下方法进行排查：

- 刚完成接入配置则需要等待1~5分钟，日志才会开始上报。
- 排查相同主机的同一个日志采集路径，是否已在AOM进行了配置。在AOM配置后则不能在LTS重复配置。
- 参考**ECS接入**排查是否存在不规范的配置导致日志采集失败。
- 若以上解决办法无法解决您的问题，请**提交工单**寻求技术支持工程师的帮助。

5.2 在 AOM 关闭超额继续采集日志开关，会影响 LTS 收集日志吗?

在AOM关闭“超额继续采集日志”开关，会影响LTS收集日志。

云日志服务与应用运维服务的日志采集开关为同步状态，即如果您在应用运维管理服务关闭了“超额继续采集日志”开关，则云日志服务的开关也同样关闭，关闭后将停止采集日志。

详细请参考**配置超额采集**。

5.3 使用 ICAgent 收集日志时 CPU 占用较高怎么处理?

如果在使用ICAgent收集日志过程中遇到CPU占用较高（例如运行速度变慢/程序崩溃）的情况，请确认您配置的日志采集路径下是否有大量的日志文件，建议您定时清理，以减少ICAgent在收集日志过程中带来的系统资源占用。若还是无法解决，请联系技术支持协助。

5.4 云日志服务 LTS 支持采集的日志类型和文件类型有哪些?

云日志服务可以采集的日志类型

- 主机日志，通过ICAgent采集器进行采集。当主机选择“Windows主机”时，如需采集系统日志，需要在“配置采集路径”环节，开启“采集Windows事件日志”。
- 云服务日志，如ELB/VPC，需要到对应的云服务上启用日志上报。
- 通过API上报日志。

云日志服务支持采集的文件类型（文件扩展名）

采集路径如果配置的是目录，示例：/var/logs/，则只采集目录下后缀为“.log”、“.trace”和“.out”的文件；如果配置的是文件名，则直接采集对应文件，只支持文本类型的文件，日志的时间（依赖机器的本地时区配置）必须是最近7天以内的。

5.5 如何在 LTS 页面关闭 CCE 标准输出日志采集到 AOM?

问题描述

随着产品的不断发展，CCE标准输出日志采集到应用运维管理（AOM）已不推荐使用。如果该配置不符合您的使用要求，须在云日志服务（LTS）控制台进行关闭。推荐您将CCE标准输出日志直接采集到云日志服务（LTS），由LTS对日志进行统一管理。

关闭CCE标准输出到AOM后，您在云日志服务（LTS）中配置的CCE标准输出采集到LTS才会生效。

解决办法

步骤1 登录**云日志服务控制台**。

步骤2 左侧导航栏选择“主机管理 > 主机”，进入“主机”页面。

步骤3 在“CCE集群”页签，选择您需要关闭标准输出到AOM的CCE集群，关闭**采集容器标准输出到AOM**按钮。建议使用CCE接入LTS，详细操作请参考**云容器引擎CCE应用日志接入LTS**。

图 5-1 关闭采集容器标准输出到 AOM

步骤4 单击“确定”，待ICAgent重启完成后，已关闭CCE标准输出到AOM。

----结束

5.6 使用 ICAgent 采集日志时，推荐的日志轮转方案是什么?

日志轮转也叫日志切割或日志绕接，通俗来讲**是对日志文件的大小进行控制**。 软件系统通常会长时间的不停机运行，这样会产生很多信息记录到不同的日志中。随着时间的推移，日志的容量自然会越来越大，而硬盘的空间是有限的，就需要对日志文件的大小进行控制。

常用的日志轮转方式有两种：按时间轮转和按日志大小轮转。

- **按时间轮转：**在进行轮转日志时，以时间为标准，当日志出现的时间满足设定的时间阈值时，则进行日志轮转。类似的典型用法有：/var/log/messages 日志即按每7天轮转一次的规则进行日志切分。
- **按日志大小轮转：**在进行轮转日志时，以日志大小为标准，当日志的大小满足设定的大小时，则进行日志轮转。一般应用程序的日志多使用日志大小进行轮转。

在使用日志轮转时，有以下建议：

- **如何轮转日志**：

  ICAgent不会对您的日志轮转，建议在应用程序中，使用成熟的软件包自定义日志轮转规则。例如：Java的logback、log4j2、Python的logging、Linux系统的logrotate。典型配置日志文件超过100/50/20MB轮转一次，保存10-20个历史日志文件。

- **轮转后日志文件命名建议**：

  最佳实践建议：假设您的日志文件路径是/your/log/path/**/*.log，建议您轮转后的文件命名为：/your/log/path/**/*.xxx.log。此处的xxx按照用户习惯，一般是指日期，如20240103，但不能含字母。

  自定义轮转规则：如果您的日志文件轮转后命名规则不符合上述的最佳实践建议，可能导致轮转文件被重复采集，您可以通过自定义轮转规则来规避此问题。您可以为每条日志采集路径添加自定义轮转规则，基于正则表达式匹配轮转后的文件名，匹配成功的文件名会被识别为日志轮转文件，不会被重复采集。例如您的日志文件为/your/log/path/**/app1.log，轮转后的文件为/your/log/path/**/app1.20240103.biz.log，那么可以配置自定义轮转规则为{basename}\.[0-9-\.]+\.[0-9]+\.biz\.log。

- **轮转后日志文件不建议压缩**

  如果您的日志打印速率较高，日志文件会快速轮转，此时轮转后的文件末尾可能会有少量日志还未被采集，ICAgent将通过Linux的inode识别采集文件的唯一性，如果您轮转后的日志文件是压缩文件，则inode会发生变化。由于您的日志文件名和inode都发生变化，ICAgent将无法保证一定会采集到该轮转文件末尾未被采集的少量日志。

  例如：假设您轮转后的文件被压缩，文件名为：/your/log/path/**/*.log.xxx.zip，该文件的文件名和inode都发生变化，则ICAgent将无法保证一定会采集到该轮转文件末尾未被采集的少量日志。

5.7 是否支持 Log4j 插件上报日志到 LTS?

LTS不支持log4j插件上报日志到LTS，原因如下：

- 目前Log4j官网已经不再提供Log4j的后期维护，推荐用户使用Log4j2，支持Log4j2插件上报日志到LTS。
- 因为Log4j存在巨大的安全隐患，所以不再提供Log4j的日志采集能力。

5.8 LTS 配置日志接入后多久有日志?

在云日志服务LTS控制台配置日志接入后，选择“日志管理”页面，单击对应日志组进入日志详情页面，查看对应日志流的“实时日志” 页面，如果查看到实时日志即代表日志接入成功。

等待1~5分钟，即可在LTS页面查看到上报的原始日志。

5.9 通过 ICAgent 接入 LTS 后无法采集到日志?

通过ICAgent接入LTS后无法采集到日志，需要等待1~5分钟，日志才会开始上报，如果还是没有查看到日志，请按如下方法进行排查。

操作步骤

步骤1 在云日志服务控制台的“配置中心”页面，检查是否开启“ICAgent采集开关”。若“ICAgent采集开关”关闭后，ICAgent会停止采集日志，因此需要开启“ICAgent采集开关”。

步骤2 在云日志服务控制台的“接入 > 接入管理”页面，检查已创建成功的配置接入任务状态显示“开启”。

步骤3 检查日志采集路径是否重复配置。若有重复配置，配置日志接入时需要开启“允许文件多次采集”。若没有开启“允许文件多次采集”，则需要删除重复的采集路径。

步骤4 检查实时日志是否上报。

1. 登录云日志服务控制台，进入日志管理页面。
2. 单击目标日志流名称，进入日志详情页面。
3. 选择实时日志页面后不需要单击任何按钮。然后尝试触发上报日志，观察实时日志页面是否自动刷新出数据，若有日志，则代表上报成功。若长时间无数据，请按如下步骤排查ICAgent。

步骤5 检查ICAgent状态。

在云日志服务控制台的左侧导航栏选择“主机管理 > 主机”，在主机页面查看主机的“ICAgent状态”显示是否正常。

- “ICAgent状态”显示运行，代表ICAgent运行正常。若有新版本，请升级ICAgent到最新版本。
- “ICAgent状态”显示异常，请联系技术支持工程师处理。

步骤6 在云日志服务控制台的“接入 > 接入管理”页面，单击目标接入配置任务操作列的“更多 > ICAgent采集诊断”，通过查看ICAgent异常监控、ICAgent整体状态和ICAgent采集监控等详情处理问题。

步骤7 若以上解决办法无法解决您的问题，请**提交工单**寻求技术支持工程师的帮助。

----结束

6 日志搜索与分析

6.1 查看 LTS 实时最新日志，每一次加载数据时延是多久？

在LTS控制台查看LTS实时最新日志，正常情况下，每隔5秒加载一次。如果这5秒内没有产生日志，则不显示；5秒后会继续调用接口，刷新出产生的日志数据。即如果每5秒都有日志数据产生，则加载数据时延为5秒。

6.2 无法查看上报到 LTS 的日志怎么办？

问题描述

在云日志服务LTS控制台无法查看上报到LTS的日志。

可能原因

- 未安装ICAgent日志采集工具。
- 采集路径配置错误。
- LTS控制台上的“配置中心 > ICAgent采集开关”未开启。
- “超额继续采集日志”开关未开启。
- 当前账号欠费，故采集器停止采集。
- 日志流写入速率和单行日志长度超出使用限制。
- 日志请求量较大，浏览器处理过慢。

解决办法

- 未安装ICAgent日志采集工具，请先安装ICAgent，方法请参见：**安装ICAgent**。
- 采集路径配置错误的话，修改采集路径。例如采集路径如果配置的是目录，示例：/var/logs/，则只采集目录下后缀为“.log”、“.trace”和“.out”的文件；如果配置的是文件名，则直接采集对应文件，只支持文本类型的文件。更多关于日志采集路径的说明请参见：**配置日志采集规则**。
- LTS控制台上的“配置中心 > ICAgent采集开关”未开启。在“配置中心 > ICAgent采集开关”页签，将采集开关置于“开启”状态。

- “超额继续采集日志”开关未开启。日志的计费依据为日志使用量，包括日志读写、日志索引和日志存储。超过免费额度后，将无法再进行日志读写和索引，同时也不再产生日志读写和索引费用。此时需要打开“超额继续采集日志”开关，详细说明请参见：**配额设置**。
- 当前账号欠费，故采集器停止采集。客户欠费后，为防止相关资源不被停止或者释放，需要客户及时进行充值，详细说明请参见：**欠费还款**。
- 日志流写入速率和单行日志长度超出使用限制、日志请求量较大，浏览器处理过慢。建议更换Google Chrome或Firefox浏览器查询日志。
- 若以上解决办法无法解决您的问题，请**提交工单**寻求工程师的帮助。

6.3 在 LTS 控制台如何手动删除日志数据?

不可以手动删除日志数据。LTS后台会根据设置的日志存储时间自动清理过期的日志数据。

设置日志存储时间请参考**管理日志流**。

6.4 在 LTS 页面无法搜索日志时怎么办?

在LTS页面搜索日志时提示查询结果不精确、查询日志时匹配到的日志结果过多、XXX字段未配置字段索引，不支持查询该字段等报错时，请参考如下方法排查。

查询日志时提示查询结果不精确

- 可能原因：查询时间范围内总日志量过多，当前控制台显示的是查询时间范围内部分日志查询的结果，为不精确结果。
- 解决方法：建议多次单击查询按钮，直至获得精确结果。或者减小查询时间范围后，再进行查询。

查询日志时匹配到的日志结果过多

- 可能原因：只有短语搜索**#"value"**才能保证关键词出现的顺序。例如查询语句**abc def**搜索的是同时包含**abc**和**def**的日志，无法准确匹配包含短语**abc def**的日志。
- 解决方法：推荐采用短语搜索**#"abc def"**，可以准确匹配包含短语**abc def**的日志。详细请参见**搜索语法**。

部分搜索语句查询不到预期的日志，且无报错提示

- 可能原因：不支持搜索分词符。或者短语搜索语句中包含*或?时，视为普通字符，不作为通配符使用。
- 解决方法：请参考搜索语法修改为正确的查询语句。

查询日志时报错提示：XXX 字段未配置字段索引，不支持查询该字段

- 可能原因：用户没有配置字段索引。
- 解决方法：请您在索引配置中创建XXX字段的字段索引，重新执行查询语句。详细请参考**配置索引**。

查询日志时报错提示：未开启全文索引，不支持查询 content 字段和全文查询

- 可能原因：用户没有开启全文索引。
- 解决方法：请您在索引配置中开启全文索引，重新执行查询语句。详细请参考**配置索引**。

查询日志时报错提示：星号（*）或问号（?）不支持使用在词的开头

- 可能原因：用户将星号（*）或问号（?）放在查询语句前面。
- 解决方法：请您修改查询语句或合理的设置分词符，避免此类查询。

查询日志时报错提示：long 和 float 类型的字段不支持使用星号（*）或问号（?）进行模糊查询

- 可能原因：用户使用星号（*）或问号（?）查询long和float类型的字段。
- 解决方法：请您修改查询语句，使用运算符（>=<）或 in 语法进行范围查询。

查询日志时报错提示：string 类型的字段不支持使用运算符（>=<）或 in 语法进行范围查询

- 可能原因：用户使用运算符（>=<）或 in 语法查询string类型的字段。
- 解决方法：
  a. 修改查询语句，使用星号（*）或问号（?）进行模糊查询。
  b. 请您重新配置结构化，将该字段修改为数字类型。更多信息请参考**结构化方式**。

查询日志时报错提示：搜索语法错误，请修改查询语句

- 可能原因：不符合运算符的语法规则。

  解决方法：每种运算符都有其对应的语法规则，请修改搜索语句，例如=运算符，语法规则要求右侧的value参数必须为数字类型。
- 可能原因：搜索语句中包含语法关键词。

  解决方法：当日志中本身包含语法关键词且需要搜索时，搜索语句需要用双引号包裹，使其转变为普通字符。详细请参见**搜索语法**。例如**and**为语法关键词，查询语句**field:and**需要修改为**field:"and"**。

7 日志转储

7.1 日志转储后，LTS 会删除转储的日志内容吗?

日志转储功能只能转发已有日志，不会删除日志内容。云日志服务LTS会根据用户配置的日志存储时间定时清理日志文件，不会影响转储后的日志。

在云日志服务LTS控制台，日志转储是把日志“另存”一份保存至OBS服务，转储成功后，单击“转储对象”列的OBS桶名称，可以跳转至OBS控制台，查看转储的日志文件。

选择转储到DIS服务、DMS服务也是一样的操作。

7.2 LTS 日志转储状态显示异常是什么原因?

在云日志服务LTS控制台的“日志转储”页面，日志转储任务的状态显示异常，有可能是如下原因引起：

- 可能原因：OBS桶策略异常。
  解决方法：请您在对象存储服务中设置访问控制策略。详细请参考**配置桶策略**。
- 可能原因：Kafka集群被删除。
  解决方法：请您重新创建Kafka转储配置，详细请参考**日志转储至DMS**。
- 可能原因：Kafka的topic被删除。
  解决方法：请您重新创建或指定Kafka的topic，详细请参考**日志转储至DMS**。

7.3 如何转储云审计服务 CTS 的日志?

云审计CTS与LTS进行系统对接后，系统自动在云日志服务控制台创建日志组和日志流，如果需要将CTS的日志转储至OBS中，您需要进行以下操作：

1. 在云审计服务管理控制台，单击左侧导航栏中的“追踪器”。
2. 单击追踪器“system”操作列的“配置”。
3. 进入基本信息页面，单击下一步。
4. 在“配置转储”页面，选择转储到OBS的相关信息和开启转储到LTS，单击下一步。

5. 确认信息正确后，单击配置即可完成。
6. 在云日志服务管理控制台，选择左侧导航栏中的“日志转储”，单击“配置转储”，完成将CTS日志转储至OBS的配置。

   其中日志组名称选择“CTS”，日志流名称“system-trace”。
7. 转储成功后在OBS控制台所选OBS桶中可以看到已转储的CTS日志。

7.4 配置 LTS 日志转储至 OBS 后，OBS 桶无法查看历史数据?

在云日志服务LTS控制台，配置OBS转储后，OBS桶无法查看历史数据，是因为云日志服务配置的日志转储是将最新产生的日志转储到OBS桶中，不会对历史日志进行转储。

更多信息请参考**日志转储至OBS**。

7.5 日志转储至 DLI 后，在 DLI 表中查不到新增分区怎么处理?

设置日志转储至DLI后，在DLI表中查不到新增分区，请参考如下方法处理。

方法 1：更新表在元数据库中的分区信息

步骤1 登录DLI控制台。

步骤2 左侧导航栏选择“作业管理-SQL作业”。

步骤3 单击对应队列的操作列“编辑”，进入详情页，在编辑框输入命令“MSCK REPAIR TABLE table_name”，table_name为有分区表的表名称。例如更新表名称为lts_qpg_dli的分区表。

步骤4 单击“执行”，等待更新完成。

关于DLI的更多内容请参见**SQL作业管理**。

----结束

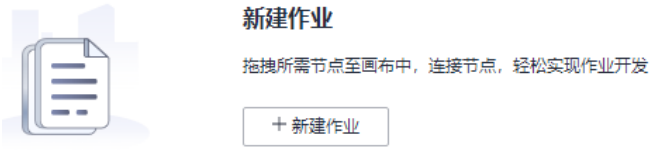
方法 2：配置定时任务

步骤1 登录DataArts Studio服务控制台，确保已创建SQL实例。

步骤2 选择实例，单击进入控制台。

步骤3 在概览页签，单击工作空间下方的数据开发，进入数据开发详情页面。

步骤4 在作业开发页面，单击新建作业，按照提示填写参数后，单击“确定”。详细操作请参考**新建作业**。



步骤5 在已创建成功的作业页面，将DLI SQL拖动到空白区域。

步骤6 在空白区域，单击DLI SQL图标，在DLI SQL页面，填写SQL语句“MSCK REPAIR TABLE table_name”，table_name为有分区表的表名称，数据库名称和队列名称选择用户配置转储DLI创建的数据库和队列。

更多DLI SQL属性信息请参考**开发SQL脚本**。

步骤7 设置完成DLI SQL属性后，单击空白处，单击“调度配置”，设置定时操作时间，详细操作请参考**调度作业**。

步骤8 设置完成后，先单击提交版本，然后单击 执行调度 ，作业执行调度触发成功。

----结束