云日志服务

常见问题

文档版本 01

发布日期 2024-04-25

华为云计算技术有限公司

商标声明

HUAWEI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。

日志管理

- 云日志服务使用建议有哪些?
- 云日志服务LTS对比自建ELK，应该如何选择?

主机管理

- ICAgent安装失败怎么办?
- 界面上单击升级ICAgent操作失败怎么办?
- 在原始日志页面无法查询新产生的日志
- ICAgent上报指标断点或无指标
- 安装ICAgent完成后反复重启如何解决?
- 安装ICAgent完成后显示离线如何解决?
- 安装ICAgent完成后不显示如何解决?

日志接入

- 使用agent过程中，CPU占用较高怎么处理?
- 云日志服务可以采集哪类日志？支持采集哪些文件类型?
- 在AOM（应用运维管理）中关闭日志采集开关，会影响LTS（云日志服务）收集日志吗?
- 主机接入配置完成后未采集到日志怎么办?
- 如何升级使用新版日志接入?
- CCE标准输出日志默认采集到AOM，应该如何关闭?
- 使用ICAgent采集日志时，推荐的日志轮转方案是什么?

日志搜索与分析

- 实时查看最新日志，每一次加载数据时延是多久?
- 在云日志服务控制台查看不到原始日志怎么办?

- 如何手动删除日志?
- 日志搜索相关问题

日志转储

- 日志转储后，LTS会删除转储的内容么?
- 日志转储页面，转储状态异常是什么原因?
- 如何转储云审计服务CTS的日志?
- 如何配置CTS审计日志存储180天?
- 配置OBS转储后，OBS桶无法查看历史数据?

其他问题

- 快速问答列表
- 如何获取AK/SK?
- 如何从第三方云厂商将日志搬迁到华为云
- 存储在LTS的日志是否可以用于安全合规审计?
- LTS配置日志接入后多久有日志?

2 日志管理

2.1 云日志服务使用建议有哪些?

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。
- 日志组规划建议：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。

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。

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，你可以添加多个图表，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。
- 日志加工：有些时候想要分析的业务日志混在运行日志中，或者业务日志中有些敏感数据需要删除，或者有些数据缺少维度数据，这个时候可以使用DSL加工（23年930开始邀测）功能对日志进行规整、富化、流转、脱敏、过滤等操作。

2.2 云日志服务 LTS 对比自建 ELK，应该如何选择?

本文将华为云日志服务（LTS）与自建ELK进行全面对比，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。

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。

特性	子特性	LTS	ELK	描述
	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。
	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。

特性	子特性	LTS	ELK	描述
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。
	告警通知渠道（邮件、短信、HTTPS等）	☆☆☆☆☆	☆	ELK：无法将告警方便的以钉钉、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

特性	子特性	LTS	ELK	描述
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） = 13200 GB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

大类	小类	月成本	费用占比
搭建ES	3 * ECS（C6 16U64G）	3*1999=5997	47.6%
	云硬盘EVS（高IO 15TB）	0.35*15*1024=5376	42.7%
搭建KAFKA	3 * ECS（2U4G）	3*208=624	4.9%
	云硬盘EVS（超高IO 3*200GB）	600	4.7%
-	-	**自建ELK，合计：12597**	-

LTS使用**价格计算器**，计算出来月成本约为**2102元**，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

大类	小类	月成本	费用占比
搭建ES	3 * ECS（C6 16U64G）	3*1999=5997	31.7%
	云硬盘EVS（高IO 31TB）	0.35*31*1024=11110	58.7%
搭建KAFKA	3 * ECS（2U4G）	3*208=624	3.3%
	云硬盘EVS（超高IO 3*400GB）	1200	6.3%
-	-	**自建ELK，合计：18931**	-

LTS使用价格计算器，计算出来月成本约为**13408元**，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

大类	小类	月成本	费用占比
搭建ES	66 * ECS（C6 16U64G）	66*1999=131934	35.3%
	云硬盘EVS（高IO 660TB）	0.35*660*1024=236544	63.2%
搭建KAFKA	3 * ECS（2U4G）	3*208=624	0.2%
	云硬盘EVS（超高IO 3*1700GB）	5100	1.4%
-	-	**自建ELK，合计：374202**	-

LTS使用**价格计算器**，计算出来月成本约为**107655元**，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 主机管理

3.1 安装 ICAgent 失败怎么办?

Windows 环境下安装 ICAgent 失败，并提示 SERVICE STOP

现象：在Windows环境下安装ICAgent失败，提示SERVICE STOP。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。命令行下执行sc query icagent提示未找到。

原因：一般为360安全卫士等杀毒软件拦截了icagent服务注册。

解决方法：

1. 检查360安全卫士等杀毒软件是否正在运行。
2. 关闭360安全卫士后再进行icagent安装。

说明

Windows下ICAgent采集文件类型需要手动配置采集路径*.log、 *.trace、 *.out等文本文件，不支持二进制文件。

3.2 升级 ICAgent 操作失败怎么办?

当在控制台升级ICAgent失败时，您可以登录到vm节点上，直接执行安装命令再次进行安装即可。ICAgent的安装是覆盖式安装，无需先卸载，直接安装即可。

3.3 在原始日志页面无法查询新产生的日志

问题现象

在原始日志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. 日志采集开关未开启。
2. 日志是否发送失败。
3. LTS下发的采集配置异常，覆盖了正确的采集配置。

排查方法

步骤1 确认日志采集开关是否开启。

1. 登录云日志服务LTS控制台，选择“配置中心”。
2. 在“日志采集开关”页签，确认日志采集开关是否开启，若没有开启，需要开启日志采集开关。

步骤2 检查最近一次下发的日志采集开关配置。

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。

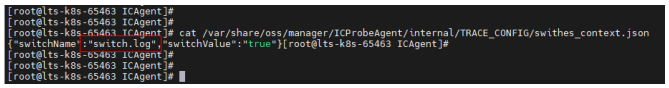
```
zgrep switchList *.zip    //查询已转储日志压缩包
cat oss.icAgent.trace | grep switchList  //查询当前日志文件
```

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（代表开启日志采集开关）。

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

1. 登录ICAgent所在的主机。
2. 查询日志采集开关文件。

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



日志采集开关文件的内容switch.log为true。

步骤4 确认是否日志发送失败。

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 确认LTS下发配置。

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下发的日志采集配置。

```
cat oss.icAgent.trace | grep 'als event' | grep -v grep | tail -n 1
```

```
[root@icagent-66081 ICAgent]#
[root@icagent-66081 ICAgent]# cat oss.icAgent.trace | grep 'als event' | grep -v grep | tail -n 1
2023/05/22 10:21:04.470  [W]   als_cfg_event.go:50 debug, als event: [map[binary_collect:%!s(bool=false) black_paths:[] containerNameRegex: customHostTag:[k8s-log-1c0cca03-e
d8d-11ed-84a4-0255ac1001b3] excludeEnvs:map[] excludeLabels:map[] format:map[multi:map[mode:time value:YYYY-MM-DD hh:mm:ss]] includeEnvs:map[] includeLabels:map[] logEnvs:ma
p[] logGroup:90182541-e17a-41fa-a4ff-01e70bb362cd logLabels:map[] logStream:35599b7d-fc74-4b06-b914-0c70400d02ef log_split:%!s(bool=false) namespaceRegex: pathType:container
_stdout paths:[] podNameRegex:multi stderr:%!s(bool=false) stdout:%!s(bool=true)] map[agentId:f13c7821-3dd0-4953-90ef-5bcbcd79b7f8 binary_collect:%!s(bool=false) format:map[
single:map[mode:system value:1683855629972]] logGroup:13dbe3af-0c24-46ca-b3c5-b1c170f47047 logStream:a6150105-a944-4480-a168-8c7957912558 log_split:%!s(bool=false) pathType:
host_file paths:[/root/test.log] stderr:%!s(bool=false) stdout:%!s(bool=false)] map[agentId:2cba224c-a088-407a-8bb1-4455d629d3d0 binary_collect:%!s(bool=false) format:map[si
ngle:map[mode:system value:1683855629972]] logGroup:13dbe3af-0c24-46ca-b3c5-b1c170f47047 logStream:a6150105-a944-4480-a168-8c7957912558 log_split:%!s(bool=false) pathType:ho
st_file paths:[/root/test.log] stderr:%!s(bool=false) stdout:%!s(bool=false)] map[binary_collect:%!s(bool=false) black_paths:[] containerNameRegex: customHostTag:[k8s-log-ea
51c969-efd4-11ed-85b0-0255ac100b0e] excludeEnvs:map[] excludeK8sLabels:map[] excludeLabels:map[] format:map[single:map[mode:system value:1684200152057]] includeEnvs:map[] in
cludeK8sLabels:map[] includeLabels:map[] logEnvs:map[] logGroup:95c72c1c-e859-4929-b18c-25977a1fc4b8 logK8s:map[] logLabels:map[] logStream:68d15d63-be15-4806-9b64-d61774b93
2d4 log_split:%!s(bool=false) namespaceRegex: pathType:container_stdout paths:[] podNameRegex: stderr:%!s(bool=false) stdout:%!s(bool=true)] map[agentId:aff59e31-7692-4e39-b
```

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，则确保已下发采集配置。

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
```

```
[root@icagent-66081 ICAgent]#
[root@icagent-66081 ICAgent]# zgrep 'als event' *.zip | grep -v grep | tail -n 1
oss.icAgent.trace.20230522101402360.zip:2023/05/22 10:10:04.487  [W]   als_cfg_event.go:50 debug, als event: [map[binary_collect:%!s(bool=false) black_paths:[] containerName
Regex: customHostTag:[k8s-log-1c0cca03-ed8d-11ed-84a4-0255ac1001b3] excludeEnvs:map[] excludeLabels:map[] format:map[multi:map[mode:time value:YYYY-MM-DD hh:mm:ss]] includeE
nvs:map[] includeLabels:map[] logEnvs:map[] logGroup:90182541-e17a-41fa-a4ff-01e70bb362cd logLabels:map[] logStream:35599b7d-fc74-4b06-b914-0c70400d02ef log_split:%!s(bool=f
alse) namespaceRegex: pathType:container_stdout paths:[] podNameRegex:multi stderr:%!s(bool=false) stdout:%!s(bool=true)] map[agentId:f13c7821-3dd0-4953-90ef-5bcbcd79b7f8 bi
nary_collect:%!s(bool=false) format:map[single:map[mode:system value:1683855629972]] logGroup:13dbe3af-0c24-46ca-b3c5-b1c170f47047 logStream:a6150105-a944-4480-a168-8c795791
2558 log_split:%!s(bool=false) pathType:host_file paths:[/root/test.log] stderr:%!s(bool=false) stdout:%!s(bool=false)] map[agentId:2cba224c-a088-407a-8bb1-4455d629d3d0 binar
y_collect:%!s(bool=false) format:map[single:map[mode:system value:1683855629972]] logGroup:13dbe3af-0c24-46ca-b3c5-b1c170f47047 logStream:a6150105-a944-4480-a168-8c795791255
8 log_split:%!s(bool=false) pathType:host_file paths:[/root/test.log] stderr:%!s(bool=false) stdout:%!s(bool=false)] map[binary_collect:%!s(bool=false) black_paths:[] conta
inerNameRegex: customHostTag:[k8s-log-ea51c969-efd4-11ed-85b0-0255ac100b0e] excludeEnvs:map[] excludeK8sLabels:map[] excludeLabels:map[] format:map[single:map[mode:system va
lue:1684200152057]] includeEnvs:map[] includeK8sLabels:map[] includeLabels:map[] logEnvs:map[] logGroup:95c72c1c-e859-4929-b18c-25977a1fc4b8 logK8s:map[] logLabels:map[] log
```

5. 登录云日志服务LTS控制台，确认是否正确下发了采集配置。

----结束

3.4 ICAgent 上报指标断点或无指标

问题现象

ICAgent上报指标断点或无指标。

对系统的影响

影响用户查看指标监控。

可能原因

1. 指标采集开关被关闭。
2. 发送指标失败。

排查方法

步骤1 检查指标采集开关是否关闭。

1. 登录应用运维管理AOM控制台，选择“配置管理 > 指标配置”。

2. 确认指标采集开关是否开启，若没有开启，需要开启指标采集开关。

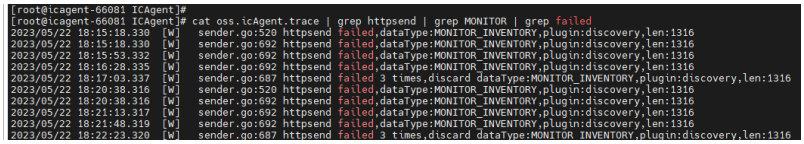
步骤2 后台查找指标采集开关配置。

1. 登录ICAgent所在ecs主机。
2. 执行“cd /var/ICAgent”进入ICAgent日志目录。
3. 查找指标采集开关配置。
   cat oss.icAgent.trace| grep 'switchL'

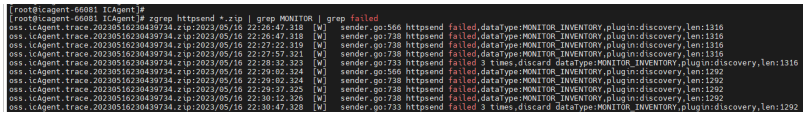
4. 如果查询不到，则过滤日志压缩包
   zgrep switchL *.zip

步骤3 指标是否发送失败

1. 登录ICAgent所在ecs的主机。
2. 执行“cd /var/ICAgent”进入ICAgent日志目录。
3. 查询指标发送失败日志
   cat oss.icAgent.trace | grep httpsend | grep MONITOR | grep failed



4. 如果日志文件查询不到，则查找日志压缩包。
   zgrep httpsend *.zip| grep MONITOR | grep failed



----结束

3.5 安装 ICAgent 完成后反复重启如何解决?

问题现象

安装ICAgent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

1. 资源占用超过限制。
2. 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 过滤日志文件，排查资源占用是否超过限制。

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

```
[root@icagent-66081 ICAgent]#
[root@icagent-66081 ICAgent]#
[root@icagent-66081 ICAgent]# cat oss.icAgent.trace| grep 'icagent exit'
[root@icagent-66081 ICAgent]#
[root@icagent-66081 ICAgent]#
```

步骤4 过滤日志压缩包，排查资源占用是否超过限制。

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

```
[root@icagent-66081 ICAgent]#
[root@icagent-66081 ICAgent]#
[root@icagent-66081 ICAgent]# zgrep 'icagent exit' *.zip
[root@icagent-66081 ICAgent]#
[root@icagent-66081 ICAgent]#
```

步骤5 过滤日志文件，ICAgent是否异常。

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

```
[root@icagent-66081 ICAgent]#
[root@icagent-66081 ICAgent]#
[root@icagent-66081 ICAgent]# cat oss.script.trace | grep runtime
[root@icagent-66081 ICAgent]#
[root@icagent-66081 ICAgent]#
```

步骤6 过滤日志压缩包，ICAgent是否异常。

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

```
[root@icagent-66081 ICAgent]#
[root@icagent-66081 ICAgent]# zgrep runtime oss.script.*.zip
gzip: oss.script.*.zip.gz: No such file or directory
[root@icagent-66081 ICAgent]#
[root@icagent-66081 ICAgent]#
```

----结束

3.6 安装 ICAgent 完成后显示离线如何解决?

安装ICAgent完成后显示离线，可能原因是输入的AK/SK错误导致该主机的ICAgent功能异常。请获取正确的AK/SK后重新安装，详细操作请参考**如何获取访问密钥（AK/SK）?**

3.7 安装 ICAgent 完成后不显示如何解决?

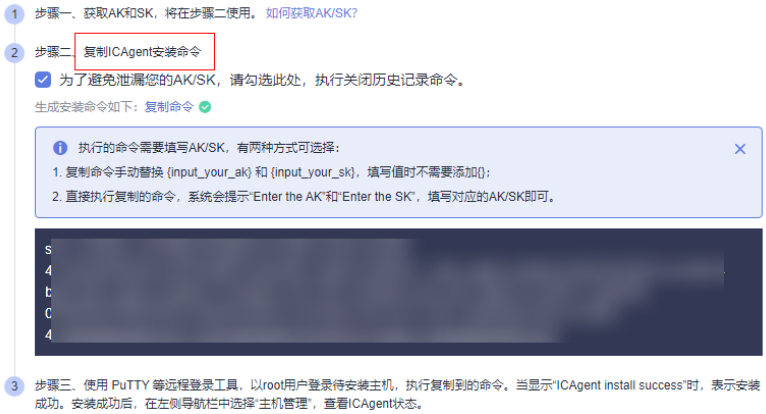
安装ICAgent完成后，在云日志服务控制台主机管理页面的主机页签，不显示主机如何解决？请参考如下步骤排查。

前提条件

已登录云日志服务控制台。

操作步骤

1. 若是ECS接入时，安装ICAgent完成后在主机页面不显示。
   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”命令查看主机网络是否正常。
2. 若是CCE接入时，安装ICAgent完成后在主机页面不显示。

   确保CCE集群已安装ICAgent并且已创建相关节点自定义标识的主机组，若没有安装ICAgent，请到主机管理页面进行升级。详细操作请参考**升级ICAgent**。

3. 在Windows环境安装ICAgent失败。
   a. 确保使用administrator账户安装。
   b. 检查已获取的AK/SK是否正确，且AK/SK没有被删除。

4 日志接入

4.1 使用 ICAgent 时 CPU 占用较高怎么处理?

如果在使用ICAgent过程中遇到CPU占用较高的情况，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。

4.2 支持采集哪些日志类型和文件类型?

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。
- 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（东八区 UTC/GMT+08:00）必须是最近7天以内的。

4.3 在 AOM 关闭超额继续采集日志开关，会影响 LTS 收集日志吗?

会。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。

4.4 主机接入完成后无法采集到日志?

1. 若刚完成配置则需要等待片刻，日志才会开始上报。

2. 排查主机配置的采集路径是否重复，即有可能主机的路径配置了多次，这样则需要修改配置，同一个主机的路径只允许存在一种配置。
3. 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。
4. 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。
5. 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。

4.5 如何升级使用新版日志接入?

随着用户创建的日志流越来越多，单个日志流下的主机采集配置也越来越多，用户维护的难度也随之增大，所以云日志服务引入了主机组的概念来方便用户管理主机。配置日志接入可以通过将主机与配置解耦，直接配置在主机组上，实现批量设置，使用户未来在管理配置日志接入时更加方便快捷。

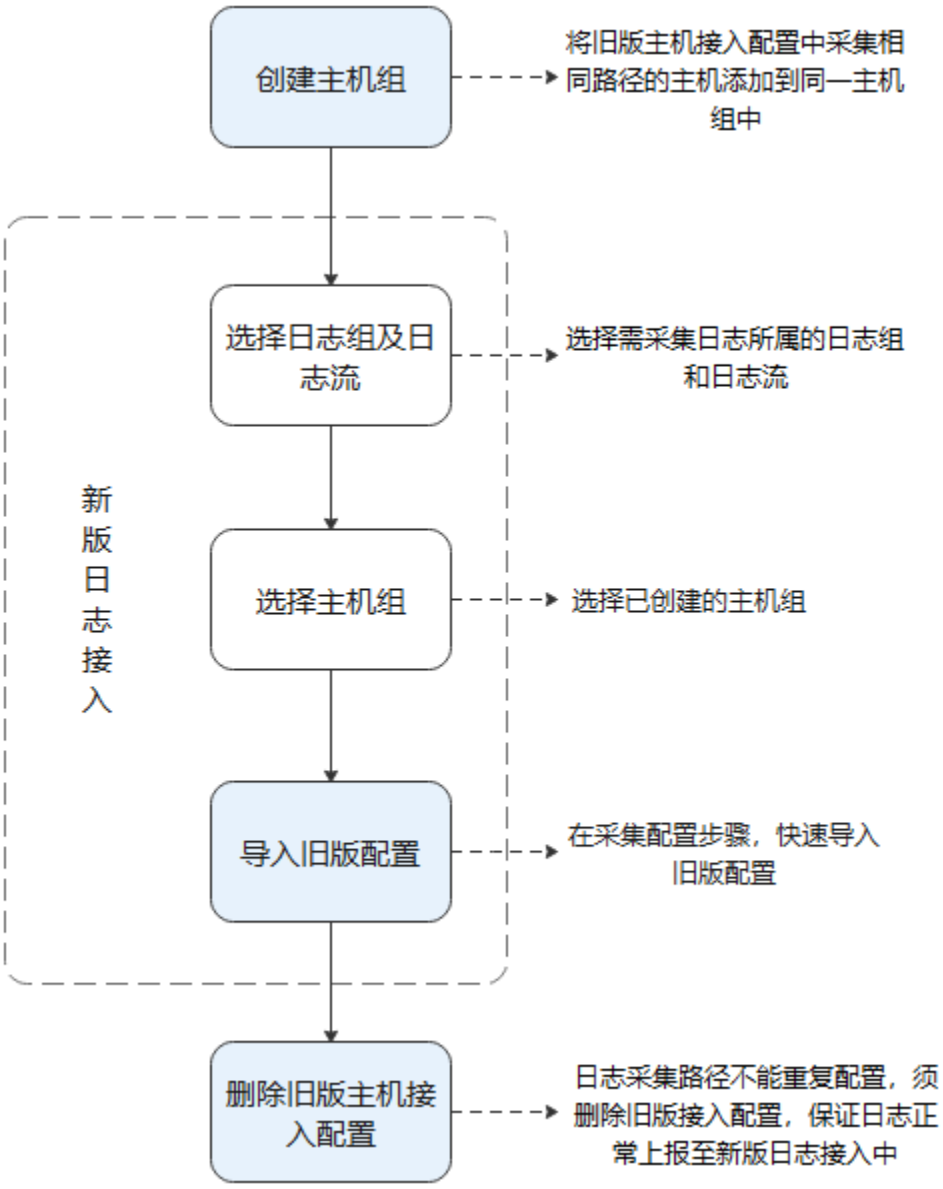
说明

因为主机组是新引入的概念，有很强的用户自定义属性，LTS无法感知不同用户需求的情况下，无法替用户创建主机组，需要您配合将主机按照自己的个人需求来进行归类，放入不同的主机组中，而后配置是与主机组相关联。

操作指导

升级使用新版日志接入流程及操作步骤如下所示。

图 4-1 升级使用新版日志接入流程图



步骤1 创建主机组。

1. 在云日志服务管理控制台，单击“主机管理”，进入主机管理页面。
2. 单击右上角“新建主机组”。
3. 在弹出的新建主机组页面，输入“主机组名称”，选择主机类型“Linux主机”或“Windows主机”。
4. 在列表中选择需要加入该主机组的主机，单击“确定”，完成主机组的创建。

步骤2 选择日志组及日志流。

1. 在云日志服务管理控制台，单击“日志接入”，进入日志接入页面。
2. 单击“云主机 ECS-文本日志”进行主机接入配置。
3. 在选择日志流步骤中，选择需采集日志所属的日志组和日志流，单击“下一步：选择主机组”。

步骤3 选择主机组。

选择已创建的主机组，单击“下一步：采集配置”。

步骤4 导入旧版配置。

在采集配置步骤，自定义采集配置名称，并单击输入框后的“导入旧版配置”，在弹出的“导入旧版配置”页面选择需要导入的旧配置，单击“确定”，导入后单击“提交”。

步骤5 删除旧版主机接入配置。

在日志流详情界面，“日志接入 > 主机接入”页面删除步骤4中已选择导入的旧版接入配置。

说明

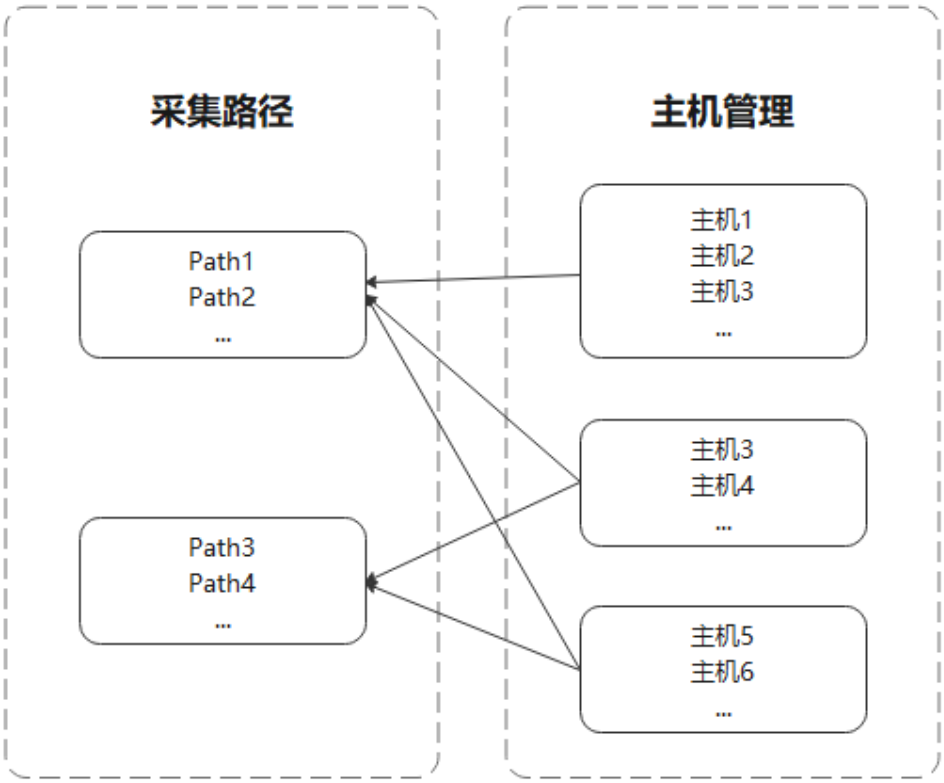
日志采集路径不能重复配置，即相同主机的同一个日志采集路径不能重复配置，否则可能会导致日志采集异常。必须**删除旧版接入配置**，保证日志正常上报至新版日志接入中。

----结束

分组原则

用户将多个主机添加入主机组中，此主机组若关联接入配置，将在此主机组下的每一个主机上生效。所以用户在使用主机组管理主机时，要根据主机的配置来划分。

图 4-2 分组原则



4.6 如何关闭 CCE 标准输出日志默认采集到 AOM?

问题描述

随着产品的不断发展，CCE标准输出日志默认采集到应用运维管理（AOM）已不推荐使用，但为了兼容老用户使用习惯，该默认配置未修改。如果该默认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。

说明

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。

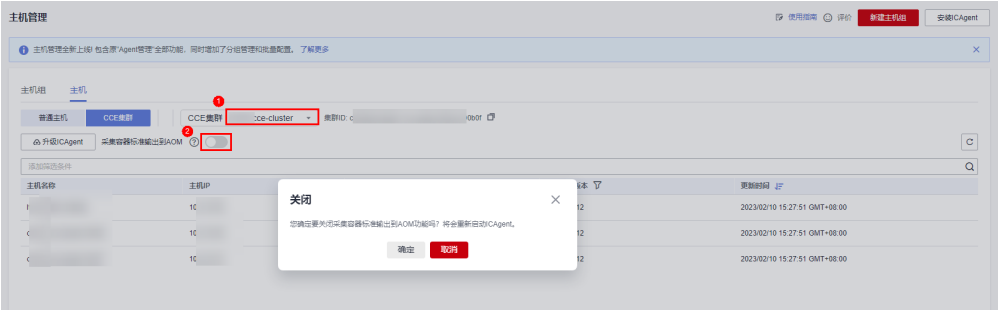
解决办法

步骤1 在云日志服务（LTS）控制台，单击左侧导航栏“主机管理”。

步骤2 选择“主机”页签，单击“CCE集群”。

步骤3 在CCE集群中，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。

图 4-3 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

4.7 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 日志搜索与分析

5.1 实时查看最新日志，每一次加载数据时延是多久？

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。

5.2 查看不到原始日志怎么办？

问题描述

云日志服务控制台原始日志页签下无内容。

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 > 日志采集开关”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

- 安装ICAgent，方法请参见：**安装ICAgent**。
- 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**。
- 登录LTS控制台，在“配置中心 > 日志采集开关”页签，将采集开关置于“开启”状态。

- 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。
- 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。
- 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。

5.3 如何手动删除日志?

不可以手动删除。系统会根据设置的日志存储时间自动清理过期的日志数据。

5.4 日志搜索相关问题

本文介绍查询日志使用搜索语法的常见问题和相关报错的处理方法。

常见问题及解决方法

1. 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。
2. 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。请参考短语搜索。
3. 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1：不支持搜索分词符。
   - 可能原因2：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。

报错提示及解决方法

1. 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**。

   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。
2. 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**。

   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。
3. 查询日志时报错提示：**星号（*）或问号（?）不支持使用在词的开头**。

   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。

4. 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**。

   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。

5. 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**。

   解决方法：

   - 修改查询语句，使用星号（*）或问号（?）进行模糊查询。
   - 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。

6. 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，详细请参见搜索语法。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"**。

6 日志转储

6.1 日志转储后，LTS 会删除转储的内容吗?

不会删除。在云日志服务控制台，日志转储是把日志“另存”一份至OBS，转储后，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。

6.2 日志转储状态异常是什么原因?

- OBS桶被删除，请您重新指定已创建的存储桶。
- OBS桶策略异常，请您在对象存储服务中设置访问控制策略。
- Kafka集群被删除，请您重新创建Kafka转储配置。
- Kafka的topic被删除，请您重新创建或指定Kafka的topic。

6.3 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的日志组和日志流，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。

6.4 如何配置 CTS 审计日志存储 180 天?

问题描述

搜索回溯一些问题，需要审计日志存储180天，如何配置审计日志存储时间并进行搜索分析?

操作步骤

- **配置转储**

  开通云审计日志后，系统会自动创建一个名为system的管理事件追踪器，并将当前租户的所有操作记录在该追踪器中。在追踪器中配置CTS转储到LTS，配置完成后会在LTS自动创建日志组日志流，日志流默认存储时间为30天，可以在LTS修改日志流存储时间为180天，即可实现CTS审计日志存储180天。

  a. 登录管理控制台。

     - 如果您是以主账号登录华为云，请直接执行**3**。
     - 如果您是以IAM用户登录华为云，请先联系管理员（主账号、admin用户组中的用户）对IAM用户授予以下权限，授权方法请参见**给IAM用户授权**。
       - CTS FullAccess

  b. 在管理控制台左上角单击 图标，选择区域和项目。

  c. 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务详情页面。

  d. 配置system追踪器，将审计日志接入LTS，单击操作列中的“配置”。

  e. 配置转储时，打开“转储到LTS”开关，系统会自动在LTS创建日志组：CTS，日志流：system-trace。

  图 6-1 转储 LTS

  f. 配置转储到LTS，修改LTS的日志流为180天存储，配置结构化规则为CTS。

     i. 单击左上角 ，选择“管理与监管 > 云日志服务 LTS”，进入云日志服务控制台页面。

     ii. 在日志管理页面，单击**e**中创建的system-trace日志流对应操作列的“编辑”，打开“日志存储时间（天）”开关，修改日志流存储时间为180天。

图 6-2 编辑日志流

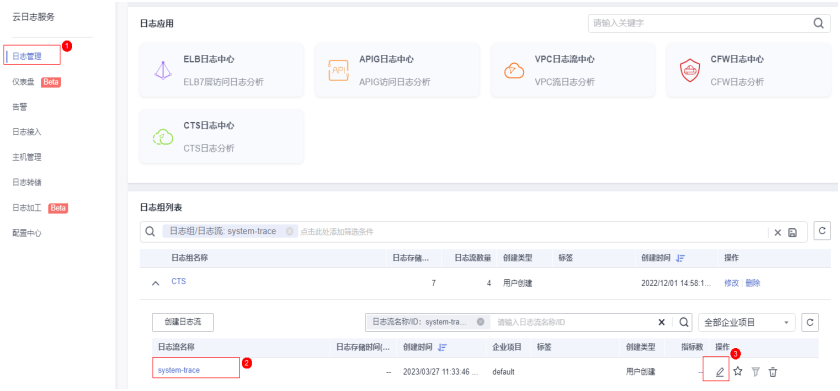


图 6-3 修改存储时间

iii. 在“日志接入 > 云审计 CTS”页面，选择日志组：CTS，日志流：system-trace。

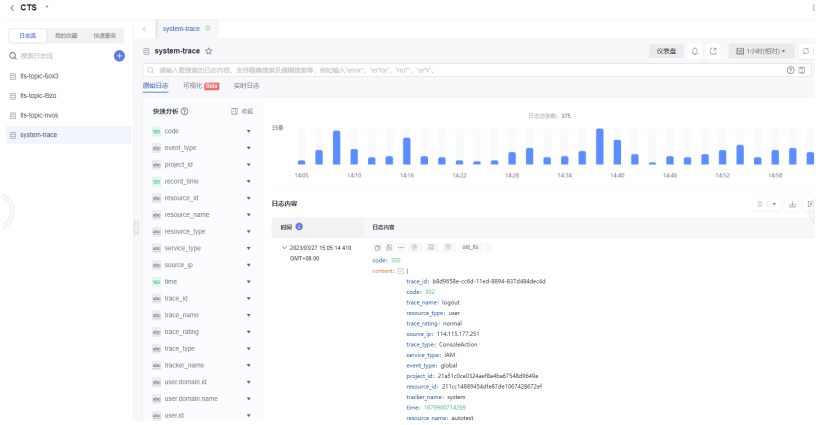
图 6-4 选择日志流

iv. CTS配置已完成，跳到下一步“日志流配置”，完成CTS日志的结构化配置。

v. 单击“提交”，即可完成接入LTS配置。

vi. 单击“查看日志流”，进入日志流详情页面。

图 6-5 日志流详情

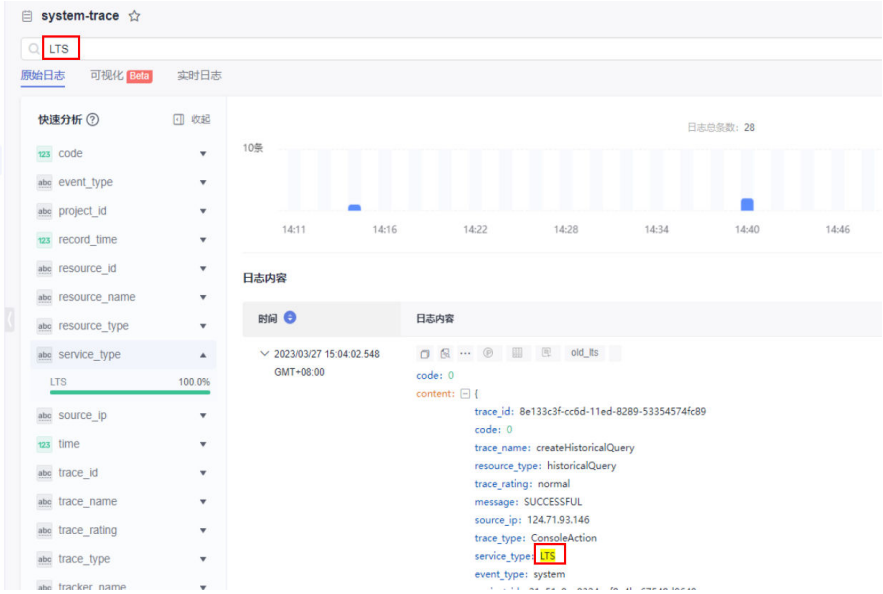


- **日志搜索分析**

  配置转储到LTS完成后，可在LTS进行审计日志的搜索分析。

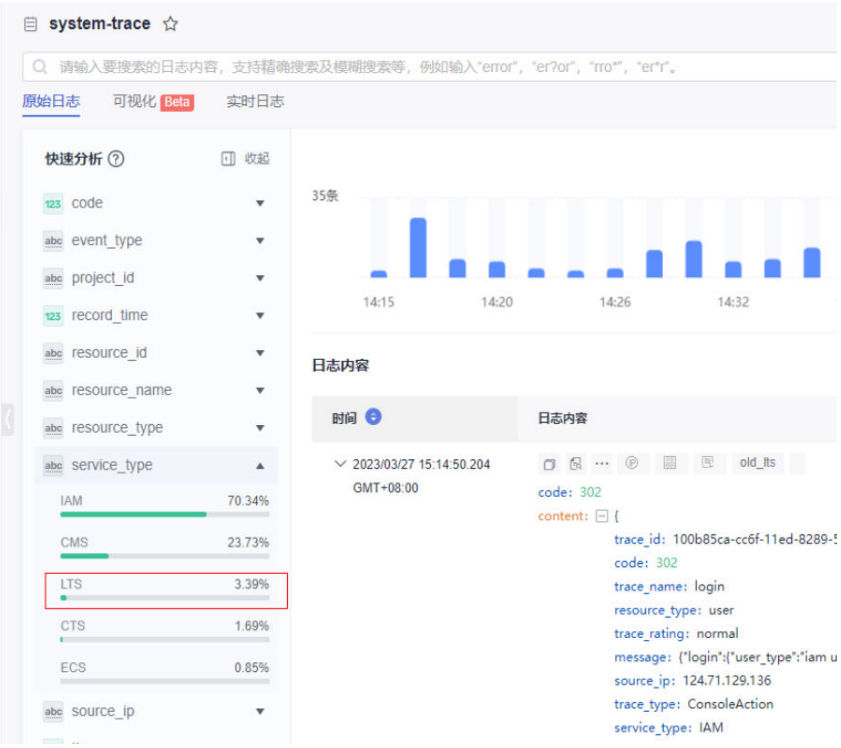
  – 方式一：直接在搜索框中输入“LTS”，搜索日志。

图 6-6 搜索日志



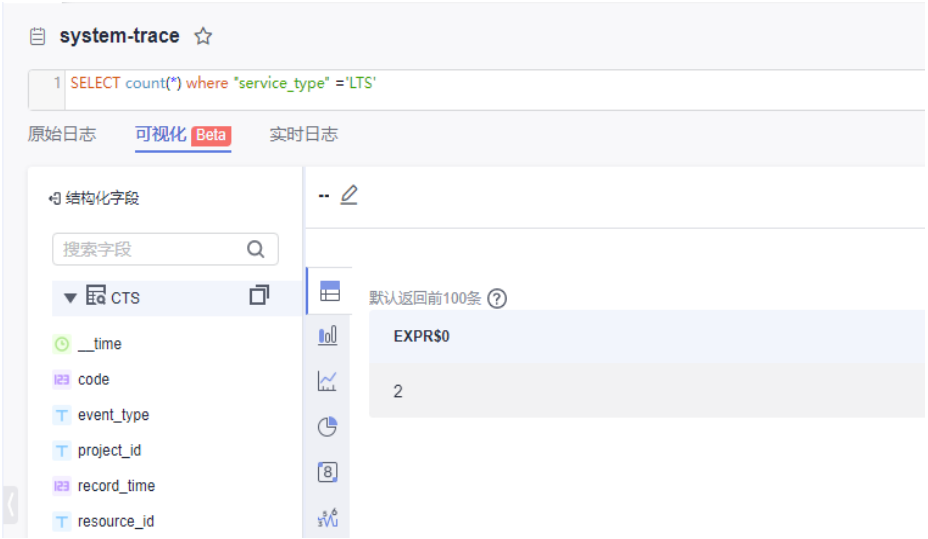
  – 方式二：在“快速分析”中找到“service_type”（审计日志中“service_type”代表云服务类型），选择“LTS”字段，即可快速搜索到日志。

图 6-7 搜索日志



– 方式三：在“可视化”中输入SQL语句，不仅可以过滤审计日志，还可以统计审计日志的总条数。

图 6-8 SQL 语句查询日志



6.5 配置 OBS 转储后，OBS 桶无法查看历史数据?

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。

7 计费

7.1 500M 免费额度怎么算?

云日志服务的计费功能包括：1、日志读写和索引；2、日志存储。每月各赠送500M免费额度，具体说明如下：

- **日志读写、索引**：按流量计费，每月免费赠送您500M额度，超过后按需收费。
- **日志存储**：按存储空间计费，每月免费赠送您500M额度，超过后按需收费。

如果每月免费赠送的额度已经可以满足您的使用需求，超过后希望暂停日志采集，请参见：如何停止日志采集（停止计费）。

7.2 日志如何计费，日志索引流量是什么?

日志包含3个计费量纲：日志读写流量、日志索引流量和日志存储空间，LTS每月各赠送500M免费额度，具体单价请参考官网日志计费说明。

1. 日志读写流量：读写流量根据传输的流量计算，传输流量为压缩后的日志大小，日志一般有5倍压缩率。

   示例：原始日志为10GB，实际压缩大小为 2GB，则以2GB 计费。
2. 日志索引流量：原始日志数据默认都会建立全文索引，创建索引（对日志分词处理）后，才能搜索日志，在写入时一次性收取流量费用。

   示例：原始日志为10GB，需要索引的流量为10GB，产生索引流量费用3.2元。
3. 日志存储空间：日志存储空间为压缩后的日志数据、索引数据、副本数据之和，这些空间约等于原始日志数据大小。

   示例：原始日志为10GB，那么一天存储最大收费为 0.000479*24*10=0.12元（金额如果遇小数点，则保留小数点后两位，第三位四舍五入。如遇四舍五入后不足￥0.01 元，则按￥0.01 元展示）。

7.3 转储日志怎么计费?

云日志服务的**转储功能目前在公测期间，暂不收费**，公测结束后将按流量计费，但是日志转储至OBS、DIS后，储存日志等功能由**OBS和DIS独立计费**，收费详情请参见：华为云定价。

7.4 如何停止日志采集（停止计费）

云日志服务可以采集主机和云服务的日志数据，如需停止计费，请参考如下操作：

- **主机日志**：通过ICAgen进行采集，当日志超过每月免费赠送的额度（500M）时，超过的部分将按需收费，如果每月免费赠送的额度已经可以满足您的使用需求，超过后希望暂停日志收集，可以在**配置中心**进行设置，关闭“**超额继续采集日志**”开关。同时建议将“**日志存储时长**”改为1天（日志组->修改），加速历史日志老化。停止采集后，不会产生读写和索引的费用，但会收取日志存储时长内的费用，如将老化周期修改1天，1天以后将不会产生存储费用。

  云日志服务（LTS）与应用运维管理（AOM）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。同时，您可以在AOM界面的“日志管理>配额设置”查看已采集的日志量。
- **云服务日志**：如需停止云服务的日志上报，请在对应的云服务中关闭上报日志的开关。例如在ELB服务控制台，配置ELB访问日志时关闭日志记录，详细操作请参考**访问日志**。虚拟私有云VPC关闭上报日志请参考**开启/关闭VPC流日志**。

7.5 CCE 用户没有开通日志功能，为什么会开始计费?

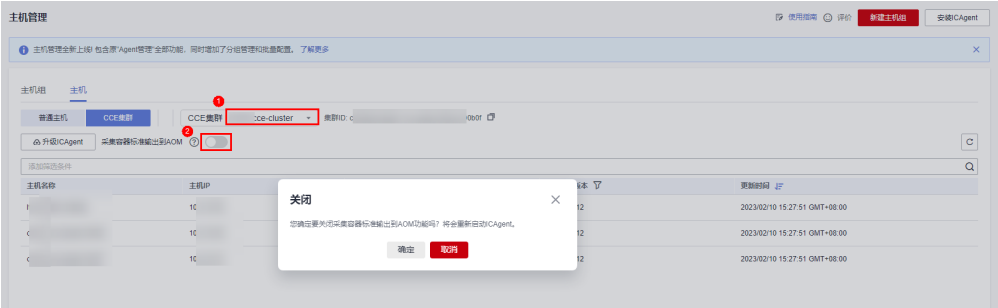
用户在**购买CCE集群**时，系统会默认勾选**自动采集容器标准输出**，会采集日志（如标准输出日志）、指标、K8S事件等运维数据。如果想停止使用日志功能，请参考以下方法：

步骤1 在云日志服务（LTS）控制台，单击左侧导航栏“主机管理”。

步骤2 选择“主机”页签，单击“CCE集群”。

步骤3 在CCE集群中，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。

图 7-1 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

8 其他问题

8.1 快速问答列表

Q：业务/应用产生的日志文件较多，是否可以手动删除日志数据?

A：不可以。系统根据设置的日志存储时间自动清理过期的日志数据。

Q：日志转储后，LTS会删除转储的内容么？转储的日志如何查询?

A：不会删除。日志转储是把日志“另存”一份至OBS，转储后，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。

Q：在应用运维管理（AOM）中关闭日志采集开关，会影响云日志服务收集日志吗?

A：会。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。

8.2 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。

8.3 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。

操作步骤

1. 登录控制台，选择“ > 管理与部署 > 统一身份认证”。

2. 在“统一身份认证”页面中，单击“委托”，进入委托页面。
3. 单击右上角“创建委托”，参考下表设置参数。

表 8-1 创建委托

名称	说明
委托名称	标识该委托代理的名称，示例：lts_ecm_trust。
委托类型	选择“云服务”。
云服务	选择“ECS BMS”。
持续时间	选择“永久”。
描述	可选参数，用于补充说明该委托代理的详细信息。

4. 单击“下一步”，进入授权页面。
5. 作用范围选择“区域级项目”，然后选择项目。在“拥有以下权限”下方搜索“LTS Admin”和“APM Administrator”并选择。
6. 单击“确定”，授权后需等待15-30分钟才可生效。

委托生效

1. 选择“服务列表 > 计算 > 弹性云服务器”，进入“弹性云服务器”页面。
2. 单击ICAgent所在的弹性云服务器名称，进入弹性云服务器参数配置页面。
3. 在“委托”选择已创建的委托名称，确认后即可生效。
4. （可选）如果您新购买的虚拟机需要设置委托，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。

8.4 如何从第三方云厂商将日志搬迁到华为云

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（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。详细请参考开始使用云日志服务。

8.5 存储在 LTS 的日志是否可以用于安全合规审计?

存储在LTS的日志可以用于安全合规审计。日志上报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。

8.6 LTS 配置日志接入后多久有日志?

在云日志服务LTS控制台的“日志接入”页面配置接入后，在“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，若查看到实时

日志即代表日志接入成功。等待1~5分钟，即可在“原始日志”页面查看到上报的原始日志。