云日志服务

用户指南

文档版本 01

发布日期 2024-04-29

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 产品介绍 1
1.1 什么是云日志服务 1
1.2 产品功能 2
1.3 应用场景 2
1.4 使用限制 3
1.4.1 基础资源 3
1.4.2 日志读写 3
1.4.3 ICAgent 5
1.4.4 搜索与分析 9
1.4.5 日志转储 10
1.4.6 操作系统 11
1.5 权限管理 11
1.6 术语 16
2 快速入门 18
2.1 入门概览 18
2.2 步骤 1：创建日志组和日志流 19
2.3 步骤 2：安装 ICAgent 20
2.4 步骤 3：接入日志 21
2.5 步骤 4：查看实时日志 22
3 日志管理 24
3.1 控制台首页 24
3.2 资源统计 25
3.3 日志组 26
3.4 日志流 27
3.5 标签管理 29
4 日志接入 31
4.1 云服务接入 31
4.1.1 ECS 接入 31
5 主机管理 37
5.1 主机组 37
5.2 主机 40
5.2.1 安装 ICAgent 40

5.2.2 升级 ICAgent....43
5.2.3 卸载 ICAgent....43
5.2.4 Agent 状态....45
6 日志搜索与分析....47
6.1 日志搜索....47
6.2 内置保留字段....50
6.3 索引配置....54
6.4 云端结构化解析....58
6.4.1 日志结构化配置....58
6.4.2 结构化方式....60
6.4.3 结构化模板....64
6.4.4 结构化配置字段....64
6.5 搜索语法与功能....66
6.5.1 搜索语法....66
6.5.2 短语搜索....72
6.5.3 实时查看日志....74
6.5.4 快速分析....74
6.5.5 快速查询....75
7 日志告警....77
7.1 过滤器....77
7.1.1 通过自定义指标查询日志....77
7.1.2 禁用过滤器....78
7.1.3 删除过滤器....79
8 日志转储....80
8.1 概述....80
8.2 转储至 OBS....80
9 配置中心....84
9.1 日志采集....84
10 常见问题....85
10.1 日志采集....85
10.1.1 使用 ICAgent 过程中，CPU 占用较高怎么处理？....85
10.1.2 云日志服务可以采集哪类日志？支持采集哪些文件类型？....85
10.2 日志搜索与查看....85
10.2.1 实时查看最新日志，每一次加载数据时延是多久？....85
10.2.2 在云日志服务控制台查看不到原始日志怎么办？....86
10.2.3 如何手动删除日志？....86
10.2.4 日志搜索相关问题....86
10.3 日志转储....87
10.3.1 日志转储后，LTS 会删除转储的内容吗？....87
10.3.2 日志转储页面，转储状态异常是什么原因？....87

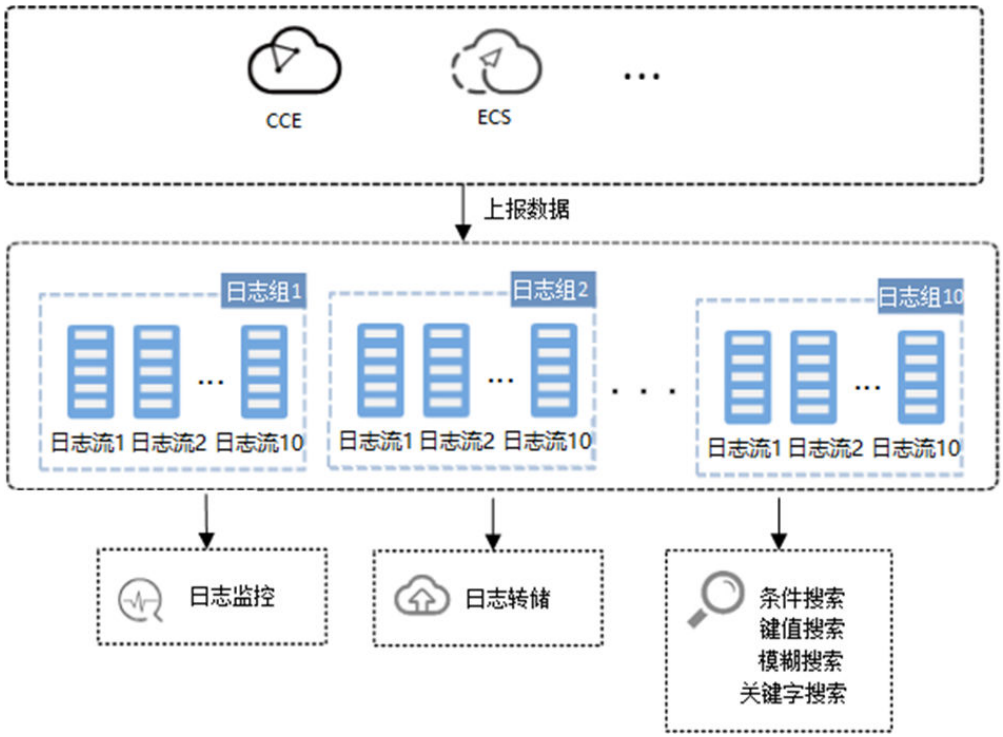
10.3.3 如何转储云审计服务 CTS 的日志? 88
10.4 其他问题 88
10.4.1 如何获取 AK/SK? 88
A 修订记录 89

1 产品介绍

1.1 什么是云日志服务

云日志服务（Log Tank Service，简称LTS），用于收集来自主机和云服务的日志数据，通过海量日志数据的分析与处理，可以将云服务和应用程序的可用性和性能最大化，为您提供实时、高效、安全的日志处理能力，帮助您快速高效地进行实时决策分析、设备运维管理、用户业务趋势分析等。

图 1-1 云日志服务示意图



日志采集与分析

云日志服务可以采集主机和云服务的日志数据，采集日志后，日志数据可以在云日志控制台以简单有序的方式展示、方便快捷的方式进行查询，并且可以长期存储。对采

集的日志数据，可以通过关键字查询、模糊查询等方式简单快速地进行查询，适用于日志实时数据分析、安全诊断与分析、运营与客服系统等，例如云服务的访问量、点击量等，通过日志数据分析，可以输出详细的运营数据。

图 1-2 日志采集与分析示意图

1.2 产品功能

实时采集日志

云日志服务提供实时日志采集功能，采集到的日志数据可以在云日志控制台以简单有序的方式展示、方便快捷的方式进行查询，并且可以长期存储。

采集到日志数据按照结构化和非结构化进行分析。结构化日志是通过规则将日志流中的日志进行处理，提取出来有固定格式或者相似度高的日志内容做结构化的分类。这样就可以采用SQL的语法进行日志的查询。

日志查询与实时分析

对采集的日志数据，可以通过关键字查询、模糊查询等方式简单快速地进行查询，适用于日志实时数据分析、安全诊断与分析、运营与客服系统等，例如云服务的访问量、点击量等，通过日志数据分析，可以输出详细的运营数据。

日志转储

主机和云服务的日志数据上报至云日志服务后，支持自定义存储时间。超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），云日志服务提供转储功能，可以将日志转储至对象存储服务（OBS）中长期保存。日志转储基于复制的转储机制，在LTS设置的存储时间内转储至OBS的日志，不会在LTS被删除。

1.3 应用场景

日志采集与分析

主机和云服务的日志数据，不方便查阅并且会定期清空。云日志服务采集日志后，日志数据可以在云日志控制台以简单有序的方式展示、方便快捷的方式进行查询，并且可以长期存储。对采集的日志数据，可以通过关键字查询、模糊查询等方式简单快速地进行查询，适用于日志实时数据分析、安全诊断与分析、运营与客服系统等，例如云服务的访问量、点击量等，通过日志数据分析，可以输出详细的运营数据。

合理优化业务性能

网站服务（数据库、网络等）的性能和服务质量是衡量用户满意度的关键指标，通过用户的拥塞记录日志发现站点的性能瓶颈，以提示站点管理者改进网站缓存策略、网络传输策略等，合理优化业务性能。例如：

- 分析历史网站数据，构建业务网络基准。
- 及时发现业务性能瓶颈，合理扩容或流量降级。
- 分析网络流量，优化网络安全策略。

快速定位网络故障

网络质量是业务稳定的基石，将日志上报至云日志服务，确保问题发生时能及时查看、定位问题，助力您快速定位网络故障，进行网络回溯取证。例如：

- 快速定位问题根源的云服务器，例如带宽过度使用的云服务器。
- 通过分析访问日志，判断业务是否遭到了攻击、非法盗链和不良请求等，及时定位并解决问题。

1.4 使用限制

1.4.1 基础资源

本文介绍云日志服务基础资源的使用限制。

表 1-1 基础资源使用限制表

限制项	说明	备注
日志组数量	您在1个账号下最多可创建100个日志组。	不涉及。
日志流数量	您在1个日志组中最多可创建100个日志流。 **说明** 日志流名称不能重复。	不涉及。
日志保存时间	日志默认保存7天，可以在1~7天之间进行设置。	不涉及。
主机组	您在1个账号下最多可创建200个主机组。	不涉及。
快速查询	您在1个日志流中最多可创建10个快速查询。	不涉及。
LogItem (单行日志)	通过API上报：单个LogItem最大为1MB。	不涉及。
	通过API上报：单个LogItem中Labels的数量最多为100个。	不涉及。
	通过ICAgent采集：单个LogItem最大为500 KB。	不涉及。

1.4.2 日志读写

本文介绍云日志服务日志读写的限制。

表 1-2 日志读写限制表

类别	限制项	说明	备注
一套云日志服务（LTS）	每日新增日志量	您在一套云日志服务（LTS）下，每日新增日志量受您购买的应用运维管理（Application Operations Management，简称AOM）VCPU数量和日志扩容包限制： ● 每购买100VCPU，包含50GB/天每日新增日志量。 ● 单独购买多套日志扩容包。 当前最大规格支持80TB/天每日新增日志量。	例如： 某客户购买了1000VCPU和2个100GB/天日志扩容包，那么该客户的LTS使用限制如下： ● 每日新增日志量：1000VCPU含500GB/天+2*100GB/天日志扩容包=700GB/天 ● 日志稳态速率：700GB/天*1024 / 24小时 / 3600秒 = 8.3 MB/秒 ● 日志峰值速率：8.3*2=16.6 MB/秒 当用户的使用量超过License限制时，LTS会发出告警信息，可能会限流，如果您需要更大规格的日志，请购买日志扩容包和升级。
	日志稳态速率	日志稳态速率=每日新增日志量/24小时/3600秒。 当前最大规格支持1000MB/秒稳态速率。	
	日志峰值速率	日志峰值速率=2*日志稳态速率。 当前最大规格支持2000MB/秒峰值速率。	
	日志写入次数	您在一套云日志服务（LTS）下，写入次数小于Max(1000,每日新增日志量/1TB*1000)。 当前最大规格支持10000次/秒。	不涉及。
	日志查询流量	您在一套云日志服务（LTS）下，通过API查询日志，单次返回日志最大为10MB。	不涉及。
	日志读取次数	您在一套云日志服务（LTS）下，读取次数最大为600次/min。	不涉及。
日志组	每日新增日志量	所有日志组之和不超过一套云日志服务（LTS）的限制。	不涉及。

类别	限制项	说明	备注
	日志稳态速率	所有日志组之和不超过一套云日志服务（LTS）的限制。	不涉及。
	日志峰值速率	所有日志组之和不超过一套云日志服务（LTS）的限制。	不涉及。
	日志读取次数	您在1个日志组下，读取次数最大为500次/min。 不涉及。	不涉及。
	日志写入次数	所有日志组之和不超过一套云日志服务（LTS）的限制。	不涉及。
	日志查询流量	您在1个日志组下，通过API查询日志，单次返回日志最大为10MB。	不涉及。
	日志读取次数	所有日志组之和不超过一套云日志服务（LTS）的限制。	不涉及。
日志流	每日新增日志量	所有日志流之和不超过一套云日志服务（LTS）的限制。	不涉及。
	日志稳态速率	所有日志流之和不超过一套云日志服务（LTS）的限制。	不涉及。
	日志峰值速率	所有日志流之和不超过一套云日志服务（LTS）的限制。	不涉及。
	日志写入次数	所有日志流之和不超过一套云日志服务（LTS）的限制。	不涉及。
	日志查询流量	您在1个日志流下，通过API查询日志，单次返回日志最大为10MB。	不涉及。
	日志读取次数	所有日志流之和不超过一套云日志服务（LTS）的限制。	不涉及。
	日志时间	日志时间不超过48小时。从当前时间往前推48小时或往后推48小时，超过该时间的日志将无法进行采集。 例如： • 当前时间为2022年1月7日11:00，那么1月5日11:00前的日志无法进行采集。 • 当前时间为2022年1月7日11:00，那么1月9日11:00后的日志无法进行采集。	不涉及。

1.4.3 ICAgent

本文介绍日志采集器ICAgent的限制。

表 1-3 ICAgent 文件采集限制

限制项	说明	备注
文件编码	支持UTF8，其他编码可能会产生乱码。 可通过开关配置是否支持采集含有二进制内容的日志文件，二进制字符可能会展示为乱码。	不涉及。
主机类型	仅支持采集Linux云主机的日志。	不涉及。
日志文件大小	无限制。	不涉及。
日志文件轮转	ICAgent目前支持配置固定日志文件名或者模糊匹配文件名，用户需要自己处理日志文件轮转。	不涉及。
日志采集路径	**Linux**： ● 采集路径支持递归路径，**表示递归5层目录。示例：/var/logs/**/a.log。 ● 采集路径支持模糊匹配，匹配目录或文件名中的任何字符。示例：/var/logs/*/a.log、/var/logs/service/a*.log。 ● 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。 ● 采集路径不能重复配置，即同一主机下的同一路径，即使跨日志组和日志流，也只能配置一次。	不涉及。
软链接	不支持软链接。	不涉及。
单条日志大小	可通过开关配置是否支持日志拆分，单条日志大小限制不超过500KB，超过限制部分会被截断丢弃。 启用日志拆分，单条日志超过500KB会被拆分为多条采集。例如日志大小为600KB，被拆分为2条日志采集，第一条500KB，第二条100KB。仅支持linux主机，不支持windows主机；仅支持单行日志，不支持多行日志。	不涉及。
正则表达式	正则表达式类型支持Perl兼容正则表达式。	不涉及。

限制项	说明	备注
同一文件对应多个采集配置	同一个文件只能上报到一个日志组、日志流。如果配置一个文件采集到多个日志流，只会有一个配置生效。	不涉及。
文件打开行为	读取时打开，读取完后关闭。	不涉及。
首次日志采集行为	全量采集，从头开始。	不涉及。

表 1-4 ICAgent 性能规格

限制项	说明	备注
日志采集速率	原始日志单节点最大采集速率50MB/S。	超过限制尽可能提供服务，不保证服务质量。
监控目录数	目录递归深度最多5层，最大不超过1000个文件。	不涉及。
监控文件数	容器场景下： ● 每个通过卷挂载日志的路径下，ICAgent最多采集20个日志文件。 ● 每个ICAgent最多采集1000个容器标准输出日志文件，容器标准输出日志只支持json-file类型。 虚机场景下： ● 最大1000个文件。	不涉及。
默认资源限制	CPU：对CPU资源的消耗最大不超过2核。 内存：对内存的消耗不超过min{4G，节点物理内存/2}，超过时将启动重启保护（ min{4G，节点物理内存/2}表示取“节点物理内存的一半”和“4G”中的较小值 ）。	不涉及。
资源超限处理策略	强制重启，若期间日志轮转，可能会丢失或重复。	不涉及。
Agent安装、升级或卸载	无限制。	不涉及。

表 1-5 ICAgent 其他限制

限制项	说明	备注
配置更新	配置更新生效的延时约1-3分钟。	不涉及。
配置动态加载	支持console的配置动态下发，且其中某一配置更新不影响其他采集。	不涉及。
配置数	无限制。	不涉及。
多租户隔离	默认隔离。	不涉及。
日志采集延迟	正常情况下从日志写入磁盘到采集日志延迟<2秒（阻塞状态下除外）。	不涉及。
日志上传策略	检测到文件变更，会立即读取上传，单次可以上报1条或者多条日志。	不涉及。
网络错误处理	在出现网络异常时会主动重试，间隔5秒。	不涉及。
资源配额超限处理	当日志量太大，分配给ICAgent的资源无法满足日志上报的要求时，ICAgent尽量上报，失败会重试，持续资源不足日志采集会积压。	不涉及。
超时最大尝试时间	周期性重试。	不涉及。
状态自检	通过心跳检测采集器状态是否正常。	不涉及。
Checkpoint超时时间	12小时无更新，则自动删除Checkpoint。	不涉及。
Checkpoint保存策略	上报成功则更新checkpoint的内容。	不涉及。
Checkpoint保存位置	默认保存路径为 */var/share/oss/manager/ICProbeAgent/internal/TRACE*	不涉及。

限制项	说明	备注
日志丢失 日志重复	采集器使用多种机制保证日志采集的可靠性，尽可能保证数据不丢失，但在如下场景可能导致日志丢失。 ● 日志文件轮转速度过快，如1秒轮转一次。 ● 系统安全设置或syslog自身原因导致无法转发日志。 ● 容器运行时间过短，例如小于30s。 ● 单节点总日志产生速度过快，超过了单节点网络发送带宽或日志采集速度，建议单节点总日志产生速度<50MB/s。 当采集器被重启后，重启时间点附近可能会产生一定的数据重复。	不涉及。

1.4.4 搜索与分析

本文介绍云日志服务查询与分析的限制。

搜索

表 1-6 日志搜索限制

限制项	说明	备注
日志采集到搜索时延	从日志产生到日志在控制台能被搜索到的时间间隔小于2分钟（非阻塞情况下）。	不涉及。
关键词个数	关键词，即单次查询时布尔逻辑符外的条件个数。每次查询最多30个。	不涉及。
操作并发数	您在1个账号下支持的最大查询操作并发数为600次/min。	不涉及。
返回结果	通过控制台查询：默认最多返回250条查询结果。	不涉及。

限制项	说明	备注
	通过API查询：默认最多返回5000条查询结果。	不涉及。
字段值大小	单个字段值最大为2KB，超出部分不参与快速分析，但是可以通过关键词查询。	不涉及。
查询结果排序	默认按照秒级时间从最新开始展示。	不涉及。
模糊查询	• 在查询语句单个词长度小于255字符 • 星号（*）或问号（?）不能用在词的开头。 • long数据类型和double数据类型不支持使用星号（*）或问号（?）进行模糊查询	不涉及
搜索时间范围	默认不超过30天。	不涉及。

1.4.5 日志转储

本文介绍云日志服务转储的限制。

表 1-7

类别	限制项	说明	备注
转储OBS	单个日志流转储任务数量	1 个日志流只能配置一个转储OBS任务。	不涉及。
	转储周期	2分钟、5分钟、30分钟、1小时、3小时、6小时、12小时。	不涉及。
	每次转储数据大小	0MB-2GB。	不涉及。
	转储速率阈值	转储速率<Min（日志量每日新增速率，您购买的OBS速率限制），超过限制时，可能会转储失败。	不涉及。
	转储条件已触发，待转储成功时会有时间延迟。	延迟10Min。 例如：转储周期30分钟，8:30开始转储，最晚8:40可见转储文件。	不涉及。
	转储目标桶	仅支持标准桶，不支持并行文件系统。	不涉及。

1.4.6 操作系统

LTS日志采集支持多个操作系统，在购买主机时您需选择LTS支持的操作系统，否则无法使用LTS对主机日志进行采集。

表 1-8 LTS 支持的操作系统及版本（Linux）

操作系统	版本					
SUSE	SUSE Enterprise 11 SP4 64bit	SUSE Enterprise 12 SP1 64bit	SUSE Enterprise 12 SP2 64bit	SUSE Enterprise 12 SP3 64bit		
openSUSE	13.2 64bit	42.2 64bit	15.0 64bit（该版本暂不支持syslog日志采集）			
EulerOS	2.2 64bit	2.3 64bit				
CentOS	6.3 64bit	6.5 64bit	6.8 64bit	6.9 64bit	6.10 64bit	
	7.1 64bit	7.2 64bit	7.3 64bit	7.4 64bit	7.5 64bit	7.6 64bit
	7.7 64bit	7.8 64bit	7.9 64bit	8.0 64bit	8.1 64bit	8.2 64bit
Ubuntu	14.04 server 64bit	16.04 server 64bit	18.04 server 64bit			
Fedora	24 64bit	25 64bit	29 64bit			
Debian	7.5.0 32bit	7.5.0 64bit	8.2.0 64bit	8.8.0 64bit	9.0.0 64bit	
Kylin	Kylin V10 SP1 64bit					

说明

- 对于Linux ARM服务器，CentOS操作系统仅支持7.4 及其以上版本，上表所列的其他操作系统对应版本均支持。

1.5 权限管理

权限说明

如果您需要对LTS资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用IAM进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制LTS资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并使用策略来控制其对LTS资源的访问范围。例如您的员工中有负责软件开发的人员，您希望员工拥有LTS的使用权限，但是不希望员工拥有删除服务发现规则等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用服务发现规则，但是不允许删除服务发现规则的权限策略，控制其对服务发现规则资源的使用范围。

如果账号已经能满足您的使用需求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用LTS的其它功能。

IAM是提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见“统一身份认证服务 用户指南的产品简介章节”。

LTS 权限

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对LTS进行操作。

LTS部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问LTS时，需要先切换至授权区域。

策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对ECS服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分。

如表1-9所示，包括了LTS的所有系统权限。

表 1-9 LTS 系统权限

策略名称	描述	策略类别	依赖关系
LTS FullAccess	云日志服务的所有权限，拥有该权限的用户可以操作并使用LTS。	系统策略	OBS Administrator、AOM FullAccess
LTS ReadOnlyAccess	云日志服务的只读权限，拥有该权限的用户仅能查看LTS数据。	系统策略	OBS Administrator、AOM FullAccess
LTS Administrator	云日志服务的管理员权限。	系统策略	Tenant Guest、Tenant Administrator
LTS Admin	云日志服务的管理员权限。	系统角色	Tenant Guest、Tenant Administrator

表1-10列出了LTS常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 1-10 常用操作与系统权限

操作	LTS FullAccess	LTS ReadOnlyAccess	LTS Administrator
查询日志组	√	√	√
创建日志组	√	×	√
修改日志组	√	×	√

操作	LTS FullAccess	LTS ReadOnlyAccess	LTS Administrator
删除日志组	√	×	√
查询日志流	√	√	√
创建日志流	√	×	√
修改日志流	√	×	√
删除日志流	√	×	√
配置主机日志接入	√	×	√
查询结构化配置	√	√	√
配置结构化	√	×	√
开启快速分析	√	×	√
关闭快速分析	√	×	√
查询过滤器	√	√	√
禁用过滤器	√	×	√
启用过滤器	√	×	√
删除过滤器	√	×	√
查看日志转储	√	√	√
添加日志转储	√	×	√
修改日志转储	√	×	√
删除日志转储	√	×	√
开启周期性转储	√	×	√
暂停周期性转储	√	×	√
安装ICAgent	√	×	√
升级ICAgent	√	×	√
卸载ICAgent	√	×	√

使用自定义细粒度策略，请使用管理员用户进入统一身份认证（IAM）服务，按需选择云日志服务的细粒度权限进行授权操作。

云日志服务细粒度权限依赖说明请参见**表1-11**。

表 1-11 云日志服务细粒度权限依赖说明

权限名称	权限描述	权限依赖
lts:agents:list	查询Agent列表	无
lts:buckets:get	查询指定桶	无
lts:groups:put	修改指定日志组	无
lts:transfers:create	创建日志转储	obs:bucket:PutBucketAcl obs:bucket:GetBucketAcl obs:bucket:GetEncryptionConfiguration obs:bucket:HeadBucket dis:streams:list dis:streamPolicies:list
lts:groups:get	查询指定日志组	无
lts:transfers:put	修改日志转储	obs:bucket:PutBucketAcl obs:bucket:GetBucketAcl obs:bucket:GetEncryptionConfiguration obs:bucket:HeadBucket dis:streams:list dis:streamPolicies:list
lts:resourceTags:delete	删除资源标签	无
lts:ecsOsLogPaths:list	查询指定镜像的系统日志路径	无
lts:structConfig:create	创建LTS结构化配置	无
lts:agentsConf:get	查询指定Agent配置	无
lts:logIndex:list	查询日志索引列表	无
lts:transfers:delete	删除日志转储	无
lts:regex:create	提取结构化字段	无
lts:subscriptions:delete	删除指定订阅	无
lts:overviewLogsLast:list	查询用户的最近日志	无
lts:logIndex:get	查询指定日志索引	无
lts:sqlalarmrules:create	添加告警相关	无
lts:agentsConf:create	创建Agent配置	无
lts:sqlalarmrules:get	查询告警相关	无

权限名称	权限描述	权限依赖
lts:datasources:batchdelete	批量删除datasource	无
lts:structConfig:put	修改LTS结构化配置	无
lts:groups:list	查询日志组列表	无
lts:sqlalarmrules:delete	删除告警相关	无
lts:transfers:action	启停日志转储	无
lts:datasources:post	创建datasource	无
lts:topics:create	创建日志主题	无
lts:resourceTags:get	查询资源标签	无
lts:filters:put	修改日志过滤器	无
lts:logs:list	查询日志列表	无
lts:subscriptions:create	创建订阅	无
lts:filtersAction:put	启停日志过滤器	无
lts:overviewLogsTopTopic:get	查询日志量最大的主题的数据指标	无
lts:datasources:put	修改datasource	无
lts:structConfig:delete	删除LTS结构化配置	无
lts:logIndex:delete	删除指定日志索引	无
lts:filters:get	查询指定日志过滤器	无
lts:topics:delete	删除指定日志主题	无
lts:agentSupportedOsLogPaths:list	查询Agent支持的操作系统日志的路径	无
lts:topics:put	修改指定日志主题	无
lts:agentHeartbeat:post	上传agent心跳	无
lts:logsByName:upload	根据日志组和日志主题的名字上传日志	无
lts:buckets:list	查询桶列表	无
lts:logIndex:post	创建日志索引	无
lts:logContext:list	查询日志上下文	无
lts:groups:delete	删除指定日志组	无
lts:filters:delete	删除日志过滤器	无
lts:resourceTags:put	更新资源标签	无

权限名称	权限描述	权限依赖
lts:structConfig:get	查询LTS结构化配置	无
lts:overviewLogTotal:get	查询当前用户的日志总量	无
lts:subscriptions:put	修改指定订阅	无
lts:subscriptions:list	查询订阅器列表	无
lts:datasources:delete	删除指定datasource	无
lts:transfersStatus:get	查询日志转储状态	无
lts:logIndex:put	修改指定日志索引	无
lts:sqlalarmrules:put	修改告警相关	无
lts:logs:upload	上传日志	无
lts:agentDetails:list	查询agent诊断日志	无
lts:agentsConf:put	修改Agent配置	无
lts:logstreams:list	筛选日志流资源	无
lts:subscriptions:get	查询指定订阅	无
lts:disStreams:list	查询DIS通道	无
lts:groupTopics:put	创建日志组和日志主题	无
lts:resourceInstance:list	查询资源实例	无
lts:transfers:list	查询日志转储列表	无
lts:topics:get	查询指定日志主题	无
lts:agentsConf:delete	删除指定Agent配置	无
lts:agentEcs:list	查询ECS列表	无
lts:indiceLogs:list	搜索日志	无
lts:topics:list	查询日志主题列表	无

1.6 术语

本章节主要介绍在使用云日志服务时的一些常用术语，帮助用户更好的理解和使用云日志服务。

表 1-12 术语

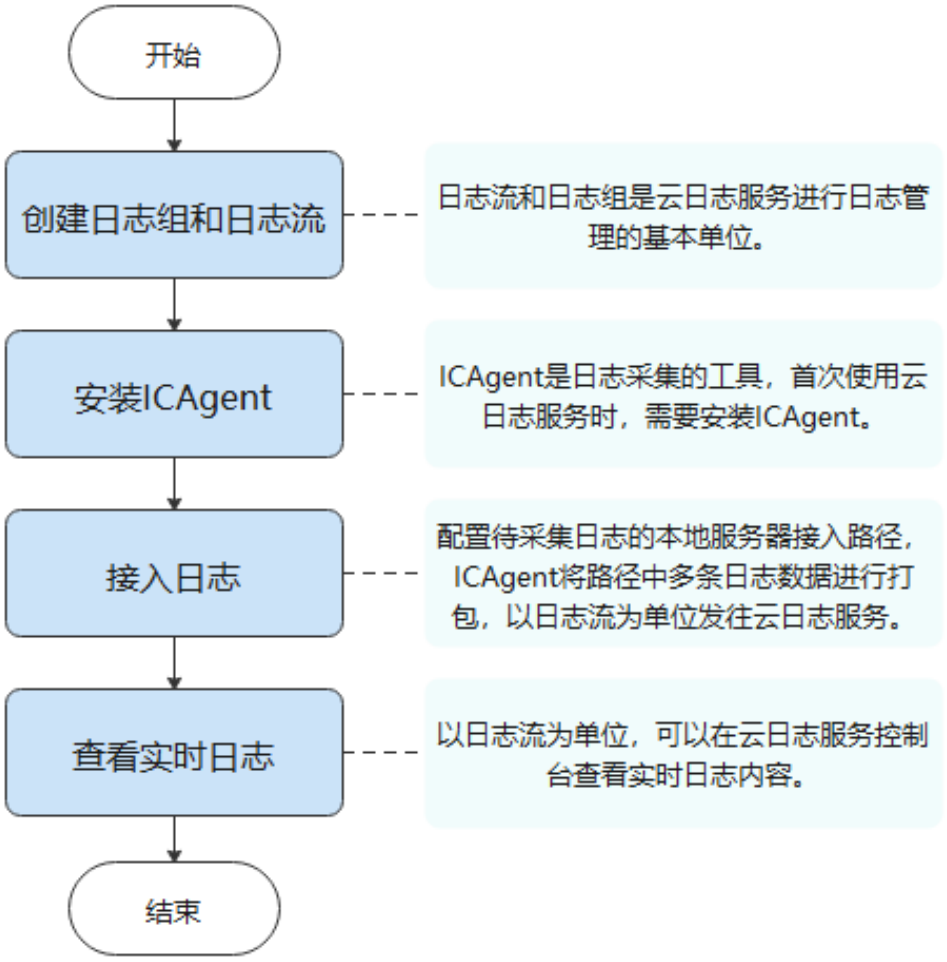
缩写	英文全称	定义
LTS	Log Tank Service	云日志服务可以提供日志收集、分析、存储等服务。用户可以通过云日志服务快速高效地进行设备运维管理、用户业务趋势分析、安全监控审计等操作。
-	Log Group	日志组是一组日志的集合，是日志管理的基本单位，用于查询和转储日志。
-	Log Stream	日志流是日志读写的基本单位，日志组中可以创建日志流，将不同类型的日志分类存储，方便对日志进一步分类管理。
-	ICAgent	ICAgent是云日志服务的日志采集工具，运行在需要采集日志的主机中。首次使用云日志服务采集日志时，需要安装ICAgent，如果需要采集多台主机的日志，还支持批量安装ICAgent，在云日志服务控制台可以实时查看ICAgent的运行状态。

2 快速入门

2.1 入门概览

本文以Linux主机接入云日志为例，并且首次进行安装ICAgent，帮助您快速上手云日志服务。

图 2-1 流程图



2.2 步骤 1：创建日志组和日志流

日志组和日志流是云日志服务进行日志管理的基本单位，在使用云日志服务时，您首先需要创建一个日志组和日志流。

前提条件

已获取控制台的登录账号与密码。

创建日志组

1. 在云日志服务管理控制台，“日志管理”页面中，单击“创建日志组”。
2. 在“创建日志组”页面中，输入日志组名称。

说明

日志采集后，将发送到对应日志组中的日志流中，如果日志较多，需要分门别类，建议您给日志组和日志流做好命名，方便后续快速查找日志。

日志组名称需要满足如下要求：

- 只支持输入英文、数字、中文、中划线、下划线及小数点，且不能以小数点、下划线开头或以小数点结尾。
- 长度为1-64个字符。

3. 输入“日志存储时间”，可以在1~7天之间进行设置，如果不设置，系统默认存储时间为7天。
4. 单击“确定”，完成日志组的创建。

创建日志流

1. 单击日志组名称对应的 按钮。
2. 单击“创建日志流”。
3. 在“创建日志流”页面中，输入日志流名称。
4. 单击“确定”，完成日志流的创建。

2.3 步骤 2：安装 ICAgent

ICAgent是云日志服务的日志采集工具，运行在需要采集日志的云主机中。首次使用云日志服务采集主机的日志时，需要安装ICAgent。

如果在使用其他云服务时已经安装了ICAgent，不再需要重复安装ICAgent，请跳过该步骤。

前提条件

安装ICAgent前，请确保本地浏览器的时间、时区与主机的时间、时区一致。

安装 ICAgent

步骤1 在云日志服务管理控制台，单击“主机管理”。

步骤2 在主机管理页面，单击右上角“安装ICAgent”。

步骤3 “安装系统”选择“Linux”。

步骤4 “安装方式”选择“获取AK/SK凭证”。

说明

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。

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。

AK/SK（Access Key ID/Secret Access Key）即访问密钥，在“我的凭证”控制台获取，步骤如下：

1. 单击页面右上角的用户名，选择“我的凭证”。
2. 在“我的凭证”页面中选择“访问密钥”。
3. 单击“新增访问密钥”，输入访问密钥信息。

   说明

   每个用户最多可创建2个访问密钥，访问密钥仅能在创建时下载一次。如果界面“新增访问密钥”灰化，请删除一个访问密钥并重新创建。
4. 单击“确定”，创建成功后请立即下载访问密钥，并妥善保管。

步骤5 单击“复制命令”，复制ICAgent安装命令。

步骤6 使用PuTTY等远程登录工具，以**root**用户登录待安装ICAgent的服务器，执行ICAgent安装命令进行安装，并根据提示输入已获取到的AK/SK。

当显示“ICAgent install success”时，表示安装成功，ICAgent已安装在了/opt/oss/servicemgr/目录。安装成功后，在云日志服务左侧导航栏中选择“主机管理 > 主机”，查看该服务器ICAgent的状态。

----结束

2.4 步骤 3：接入日志

以主机接入为例完成日志接入。

ICAgent安装完成后，需要将主机待采集日志的路径配置到日志流中，ICAgent将多条日志进行打包，以日志流为单位发往云日志服务。

前提条件

- 已创建日志组和日志流。
- 已完成ICAgent安装。

操作步骤

步骤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。

步骤2 选择“云主机 ECS - 文本日志”，进行接入日志配置。

步骤3 选择日志流。

1. 单击“所属日志组”后的目标框，在下拉列表中选择具体的日志组，若没有所需的日志组，单击“所属日志组”目标框后的“新建”，在弹出的创建日志组页面创建新的日志组。
2. 单击“所属日志流”后的目标框，在下拉列表中选择具体的日志流，若没有所需的日志流，单击“所属日志流”目标框后的“新建”，在弹出的创建日志流页面创建新的日志流。
3. 单击“下一步：选择主机组”。

步骤4 选择主机组。

1. 在主机组列表中选择一个或多个需要采集日志的主机组，若没有所需的主机组，单击列表左上方“新建”，在弹出的新建主机组页面创建新的主机组，具体可参考创建主机组（IP地址）。

说明

主机组可以为空，可以在接入配置设置完成后对主机组进行设置。

- 在“主机管理 > 主机组”页面对主机组和接入配置进行关联。
- 在接入配置详情中对主机组和接入配置进行关联。

2. 单击“下一步：采集配置”。

步骤5 采集配置。

1. 对主机日志采集设置具体的采集规则，具体可参考采集配置。
2. 设置完成后单击“提交”。

步骤6 结构化配置（可选项）。

步骤7 索引配置（可选项）。

步骤8 完成。

接入成功，可以单击“返回接入配置列表”查看日志接入，也可单击“查看日志流”查看该日志流下的采集日志。

----结束

2.5 步骤 4：查看实时日志

完成日志接入配置后，可以在云日志控制台实时查看上报的日志。

前提条件

- 已创建日志组和日志流。
- 已完成ICAgent安装。
- 已接入日志。

查看实时日志

1. 在云日志服务管理控制台，单击“日志管理”。
2. 在日志组列表中，单击已创建的日志组名称，进入日志流详情页面。
3. 或者在日志流列表中，单击已创建的日志流名称，进入日志流详情页面。
4. 在日志流详情页面，单击“实时日志”，查看实时日志。

   日志大约每隔5秒钟上报一次，在日志消息区域，您最多需要等待5秒钟左右，即可查看实时上报的日志。

   同时，您还可以通过页面右上方的“清屏”、“暂停”对日志消息区域进行操作。

   - 清屏：清除日志消息区域已经显示出来的日志。
   - 暂停：暂停日志消息的实时显示，页面定格在当前已显示的日志。

     暂停后，“暂停”会变成“继续”，再次单击“继续”，日志消息继续实时显示。

说明

如果您正在使用实时查看功能，请停留在实时查看页面，请勿切换页面。如果您离开实时查看页面，实时查看功能将会被关闭。

3 日志管理

3.1 控制台首页

云日志服务控制台首页提供资源统计、我的收藏/我的收藏（本地缓存）、最近访问和FAQ等信息。

资源统计

资源统计展示账号下所有日志前一天的读写流量、索引流量、存储量和原始日志流量，以及这些指标的日环比数据。

如需查看资源明细，您可以单击**相关明细**。

详细信息，请参见**资源统计**。

我的收藏/我的收藏（本地缓存）

我的收藏展示您收藏的日志流，有两种收藏方式：我的收藏和我的收藏（本地缓存）。

- **我的收藏**：将日志流保存至数据库中，默认为关闭状态。当您的账号开通写权限时，可显示该功能和我的收藏（本地缓存）。
- **我的收藏（本地缓存）**：将日志流保存至浏览器本地缓存，默认为关闭状态。所有账号均显示我的收藏（本地缓存）。

  说明

  当您的账号开通写权限时，**我的收藏/我的收藏（本地缓存）**至少有一个是开启状态，否则无法收藏日志流。

您可以通过云日志服务提供的收藏功能个性化定制属于自己的收藏日志流列表，方便您直接、快速的定位到常用的日志流。

以日志组lts-test为例，收藏日志组lts-test下某个日志流的操作步骤如下：

步骤1 登录云服务日志控制台

步骤2 在日志组列表区域，单击日志组lts-test对应的 按钮，选择待收藏的日志流。

步骤3 单击日志流右侧  图标，编辑收藏，选择收藏方式，单击“确定”，即可收藏日志流。

说明

编辑收藏取消已收藏的日志流，推荐如下两种方式：

- 在日志流列表中，单击待取消收藏的日志流对应的  ，即可取消收藏。
- 在我的收藏中，鼠标悬浮待取消收藏的日志流，单击  ，即可取消收藏。

----结束

最近访问

最近访问展示最近访问的日志流。

说明

最近访问最多可显示3条日志流访问记录。

FAQ

FAQ（常见问题）展示经常被询问的问题。

如需查看更多FAQ，您可以单击**更多**。

3.2 资源统计

日志资源统计是对日志进行分类统计及日志数据的可视化展示，主要分类有读写流量、索引流量、存储量和原始日志流量。统计日志资源的数据量仅供参考。

- 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。
- 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。
- 存储量：日志存储量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。
- 原始日志流量：原始日志数据的大小。

资源统计

资源统计主要展示日志资源数据，默认展示时间为1周（相对）的日志资源数据，您可以根据自己的实际需求选择时间范围。

- 统计选择时间范围内的读写流量、索引流量、存储量和原始日志流量。
- 显示选择时间范围内的环比值，查看变化趋势。
- 按照选择时间范围显示流量（或存储量）数据趋势图。趋势图中每个点表示某时间内的数据统计，单位为KB、MB和GB，根据实际情况进行统计。

资源详情

资源详情按照读写流量、索引流量和最新存储量三种方式，分别展示其Top100的日志组/日志流，默认按照最新存储量的Top100显示，单位为GB。您可根据自己的实际情况，选择读写流量、索引流量或最新存储量任一方式，进行Top100的日志组/日志流资源统计。

- 新创建的日志组/日志流，需间隔至少1小时才能进行资源统计。
- 单击Top100中的日志组名称，可查询该日志组下的日志流资源统计。
- 单击  按钮，可下载日志组资源统计和日志流资源统计。

  说明

  下载的日志组资源统计和日志流资源统计文件为.CSV格式。
- 资源详情可选择时间范围统计。

  时间范围有三种方式，分别是相对时间、整点时间和自定义时间。您可以根据自己的实际需求，选择时间范围。

  说明

  - 相对时间：表示查询距离当前时间1分钟、5分钟、15分钟等时间区间的日志数据。例如当前时间为19:20:31，设置相对时间1小时，表示查询18:20:31~19:20:31的日志数据。
  - 整点时间：表示查询最近整点1分钟、15分钟等时间区间的日志数据。例如当前时间为19:20:31，设置整点时间1小时，表示查询18:00:00~19:00:00的日志数据。
  - 自定义时间：表示查询指定时间范围的日志数据。
- 根据选择的时间范围，展示每日存储量（GB）、每日索引流量（GB）和每日读写流量（GB）的数据。

  有两种展示方式：

  – 表格
  – 柱状图

3.3 日志组

日志组（LogGroup）是云日志服务进行日志管理的基本单位，可以创建日志流，每个账号下可以创建100个日志组。

前提条件

已获取控制台的登录账号与密码。

创建日志组

日志组的创建类型分为用户创建（主动）和云服务创建（被动），云服务创建指其他云服务与云日志服务进行系统对接后，系统自动在云日志服务控制台创建的日志组，本操作中日志组的创建类型为用户创建（主动）。

1. 在云日志服务管理控制台，单击页面右上角的“创建日志组”。
2. 在“创建日志组”页面中，输入日志组名称。

说明

- 日志采集后，将发送到对应的日志组中的日志流，如果日志较多，需要分门别类，建议您给日志组做好命名，方便后续快速查找日志。日志组创建后，名称不支持修改。
- 日志名称只支持英文、数字、中文、中划线、下划线及小数点，且不能以小数点、下划线开头或小数点结尾。长度为1-64个字符。

3. 输入“日志存储时间”，可以在1~7天之间进行设置，如果不设置，系统默认存储时间为7天。
4. 单击“确定”，完成日志组的创建。
   - 在日志组列表中，可以查看日志组名称、日志存储时间（天）、创建类型、创建时间、日志流数量。
   - 单击日志组名称，可跳转到日志流详情页面。
   - 并发创建时，可能会偶现创建个数超过限制。

删除日志组

如果日志组不再需要使用，可以删除日志组。日志组删除后，日志组中的日志流、日志数据将被同时删除。**日志组删除后无法恢复，请谨慎操作。**

说明

如果日志组绑定了日志转储任务，删除日志组之前，需要先删除该日志组关联的日志转储任务。

1. 在日志组列表中，单击待删除日志组操作列下的“删除”。
2. 在弹出框中输入“DELETE”后，单击“确定”，完成日志组删除。

搜索日志组/日志流

在日志组列表中，单击搜索框，通过如下筛选条件进行搜索：

- 日志组/日志流
- 日志组名称/ID
- 日志流名称/ID
- 日志组标签

3.4 日志流

日志流（LogStream）是日志读写的基本单位，日志组中可以创建日志流，将不同类型的日志分类存储，方便对日志进一步分类管理。例如，您可以将不同的日志（操作日志、访问日志等）写入不同的日志流，查询日志时可以进入对应的日志流快速查看日志。

1个日志组中最多可以创建100个日志流，不支持扩大配额。如果您的配额已满，无法创建日志流，建议删除不再需要使用的日志流后重试，或者在新的日志组中创建日志流。

前提条件

已创建日志组。

创建日志流

日志流的创建类型分为用户创建（主动）和云服务创建（被动），云服务创建指其他云服务与云日志服务进行系统对接后，系统自动在云日志服务控制台创建的日志流，本操作中日志流的创建类型为用户创建（主动）。

1. 在云日志服务管理控制台，单击日志组名称对应的 按钮。
2. 单击展开页面左上角的“创建日志流”，输入日志流名称，名称需要满足如下要求：
   - 只支持输入英文、数字、中文、中划线、下划线及小数点，且不能以小数点、下划线开头或以小数点结尾。
   - 长度为1-64个字符。

   说明

   日志采集后，以日志流为单位，将多条日志数据发往云日志服务。如果日志较多，需要分门别类，建议您创建多个日志流，并给日志流做好命名，方便后续快速查找日志。日志流创建后，名称不支持修改。
3. 单击“确定”，完成日志流的创建。在日志流列表中，可以查看日志流名称、操作等信息。

删除日志流

如果日志流不再需要使用，可以删除日志流，日志流删除后，日志流中的日志数据将被同时删除。**日志流删除后无法恢复，请谨慎操作。**

说明

- 删除日志流前请确认该日志流下没有配置日志采集任务，否则删除后可能影响正常的日志上报。
- 如果日志流绑定了日志转储任务，删除日志流之前，需要先删除该日志流关联的日志转储任务。

1. 在日志流列表中，单击待删除日志流所在行的 。
2. 在弹出框中输入“DELETE”后，单击“确定”，完成日志流删除。

其他操作

- **收藏日志流**

  单击日志流中操作列下的 ，收藏日志流，在控制台首页里我的收藏/我的收藏（本地缓存）中展示已收藏的日志流。
- **指标过滤**

  单击日志流中操作列下的 ，在弹出的自定义指标过滤配置页面，进行指标过滤配置。

  说明

  云日志服务从日志中提取您指定的关键词，便于在应用运维管理服务对日志中的关键指标进行监控及告警。
- **详情**

单击日志流中操作列下的 ，可查看日志流详情。包括日志流名称、日志流ID、日志存储时间（天）、创建类型、创建时间等信息。

3.5 标签管理

LTS支持对日志组和日志流进行标签管理，按照业务需求对不同的日志组、日志流、主机组及日志接入的配置添加对应的标签。标签分为系统标签和普通标签，系统标签包括原有的日志清洗标签，用户不可更改；普通标签每个资源最多可添加20个。

日志组

用户可以在日志组界面对标签进行增删改查，操作日志组标签会将标签同步至该日志组下所有日志流。

1. 在云日志服务管理控制台，选择左侧的“日志管理”。
2. 在日志管理页面，日志组列表中，将鼠标悬浮在“标签”列单击 。
3. 在弹出标签管理页面填写标签键和标签值后单击“添加”，会将填写的键值按照“标签键=标签值”的形式显示在页面下方显示框中，如下图所示。

   说明

   - 如需添加多个标签可重复该步骤。
   - 如需删除标签可单击标签管理界面显示框中待删除标签后的 。
   - 标签键长度不能超过128个字符；标签值长度不能超过255个字符。
   - 标签键名称不可重复。
4. 单击“确定”，完成对该日志组的标签管理。

   在日志管理页面，日志组列表的“标签”列可以查看日志组已添加的普通标签。

日志流

用户可以在日志流界面对标签进行增删改查，操作日志流标签仅对当前流有效。

1. 在云日志服务管理控制台，选择左侧的“日志管理”。
2. 在日志管理页面，单击日志组列表下日志组名称对应的 按钮。
3. 在日志流列表中，将鼠标悬浮在日志流的“标签”列单击 。
4. 在弹出标签管理页面填写标签键和标签值后单击“添加”，会将填写的键值按照“标签键=标签值”的形式显示在页面下方显示框中，如下图所示。

   说明

   - 如需添加多个标签可重复该步骤。
   - 如需删除标签可单击标签管理界面显示框中待删除标签后的 。
   - 标签键长度不能超过128个字符；标签值长度不能超过255个字符。
   - 标签键名称不可重复。
5. 单击“确定”，完成对该日志流的标签管理。

   在日志流列表的“标签”列可以查看该日志流下的系统标签和已添加的普通标签。

主机组

用户可以在主机组界面对标签进行增删改查，操作主机组标签仅对当前主机组有效。

1. 在云日志服务管理控制台，选择左侧的“主机管理”。
2. 在主机管理页面，单击主机组所在行“操作”列的 。
3. 在弹出标签管理页面填写标签键和标签值后单击“添加”，会将填写的键值按照“标签键=标签值”的形式显示在页面下方显示框中，如下图所示。

   说明

   - 如需添加多个标签可重复该步骤。
   - 如需删除标签可单击标签管理界面显示框中待删除标签后的 。
   - 标签键长度不能超过128个字符；标签值长度不能超过255个字符。
   - 标签键名称不可重复。
4. 单击“确定”，完成对该主机组的标签管理。

   在主机管理页面，主机组列表的“标签”列可以查看主机组已添加的普通标签。

日志接入

用户可以在日志接入界面对标签进行增删改查，操作日志接入标签仅对当前日志接入有效。

1. 在云日志服务管理控制台，选择左侧的“日志接入”。
2. 在日志接入页面，单击接入配置名称所在行“操作”列的 。
3. 在弹出标签管理页面填写标签键和标签值后单击“添加”，会将填写的键值按照“标签键=标签值”的形式显示在页面下方显示框中，如下图所示。

   说明

   - 如需添加多个标签可重复该步骤。
   - 如需删除标签可单击标签管理界面显示框中待删除标签后的 。
   - 标签键长度不能超过128个字符；标签值长度不能超过255个字符。
   - 标签键名称不可重复。
4. 单击“确定”，完成对该日志接入的标签管理。

   在日志接入页面，日志接入列表的“标签”列可以查看日志接入已添加的普通标签。

4 日志接入

4.1 云服务接入

4.1.1 ECS 接入

当您选择了ECS接入方式时，云日志服务可以将ECS待采集日志的路径配置到日志流中，ICAgent将按照日志采集规则采集日志，并将多条日志进行打包，以日志流为单位发往云日志服务，您可以在云日志服务控制台实时查看日志。

前提条件

已**安装ICAgent**并**添加至主机组**。

操作步骤

云日志服务接入方式选择**云主机 ECS-文本日志**时，按照如下操作完成接入配置。

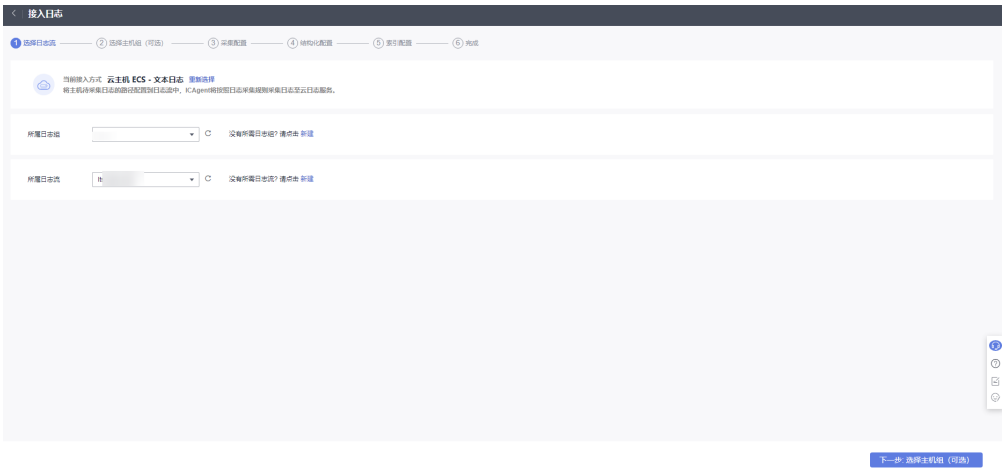
步骤1 登录云日志服务控制台。

步骤2 在左侧导航栏中，选择“日志接入”，单击“云主机 ECS-文本日志”进行主机接入配置。

步骤3 选择日志组。

1. 单击“所属日志组”后的目标框，在下拉列表中选择具体的日志组，若没有所需的日志组，单击“所属日志组”目标框后的“新建”，在弹出的创建日志组页面创建新的日志组。
2. 单击“所属日志流”后的目标框，在下拉列表中选择具体的日志流，若没有所需的日志流，单击“所属日志流”目标框后的“新建”，在弹出的创建日志流页面创建新的日志流。
3. 单击“下一步：选择主机组（可选）”。

图 4-1 选择日志组



步骤4 选择主机组。

1. 在主机组列表中选择一个或多个需要采集日志的主机组，若没有所需的主机组，单击列表左上方“新建”，在弹出的新建主机组页面创建新的主机组，具体可参考**创建主机组（IP地址）**。

   说明

   主机组可以为空，但是会导致采集配置不生效，建议第一次接入时选择主机组。若不选择，可以在接入配置设置完成后对主机组进行设置。

   - 在“主机管理 > 主机组”页面对主机组和接入配置进行关联。
   - 在接入配置详情中对主机组和接入配置进行关联。

2. 单击“下一步：采集配置”。

步骤5 采集配置。

对主机日志采集设置具体的采集规则，具体请参考**采集配置**。

步骤6 结构化配置（可选项）。

结构化配置，具体请参考结构化配置。

说明

当所选日志流已配置结构化时，请谨慎执行删除操作。

步骤7 索引配置（可选项）。

索引配置，具体请参考索引配置。

步骤8 完成。

接入成功，可以单击“返回接入配置列表”**查看日志接入**，也可单击“查看日志流”查看该日志流下的采集日志。

----结束

采集配置

在使用主机接入完成日志接入时，采集配置的具体配置如下：

图 4-2 采集配置

1. 采集配置名称：自定义采集配置名称，长度范围为1到64个字符，只支持输入英文、数字、中文、中划线、下划线以及小数点，且不能以小数点、下划线开头或以小数点结尾。

   说明

   导入旧版配置：将旧版主机接入配置导入到新版日志接入中。

   - 若是新安装云日志服务的场景，页面没有显示“导入旧版配置”，则表示不需要导入旧版配置，直接新建配置即可。
   - 若是升级云日志服务的场景，页面显示“导入旧版配置”，若需要旧版配置里的主机日志路径，可以选择导入旧版配置，或者直接新建配置。

2. 路径配置：添加您需要收集的日志路径，LTS将按照配置的路径进行日志采集。
   - **采集路径支持递归路径，**表示递归5层目录。**

     示例：采集路径配置为 /var/logs/**/a.log，日志匹配如下：

     ```
     /var/logs/1/a.log
     /var/logs/1/2/a.log
     /var/logs/1/2/3/a.log
     /var/logs/1/2/3/4/a.log
     /var/logs/1/2/3/4/5/a.log
     ```

     说明

     - 以上示例中的/1/2/3/4/5/，表示/var/logs目录中，往里递归的5个目录层级，在这5个目录层级中只要存在a.log，都能进行日志匹配。
     - 采集路径中只能出现一次**，不能出现两个及以上。正确示例：/var/logs/**/a.log；错误示例：/opt/test/**/log/**。
     - 采集路径中第一个层级不允许为**（避免误采集系统文件），错误示例：/**/test。
   - **采集路径支持模糊匹配，匹配目录或文件名中的任何字符。**

     说明

     如果配置了C:\windows\system32类似的日志采集路径，但无法采集日志，请尝试打开WAF物理防火墙后重新配置。

     - 示例1：采集路径配置为 /var/logs/*/a.log，表示/var/logs/目录下，任何一个目录中存在a.log，都能进行日志匹配，例如：

       /var/logs/1/a.log

/var/logs/2/a.log

- 示例2：采集路径配置为 /var/logs/service-*/a.log，日志匹配示例：
  /var/logs/service-1/a.log
  /var/logs/service-2/a.log
- 示例3：采集路径配置为 /var/logs/service/a*.log，日志匹配示例：
  /var/logs/service/a1.log
  /var/logs/service/a2.log

– **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，只支持内容是文本格式的文件。可以通过*file -i 文件名*命令，查询文件格式。

说明

- 请注意您的敏感信息是否在收集范围内。
- 目前只支持采集安装在ECS（主机）实例的日志。
- **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。
- 相同主机的同一个日志采集路径，如果在AOM进行了配置，则不能在LTS重复配置。
- 配置采集的文件最后修改时间和当前时间差如果已超过12小时，则不会采集。

3. 设置采集黑名单：LTS支持对日志进行过滤采集，即通过设置黑名单，在采集时过滤指定的目录或文件。指定按目录过滤，可过滤掉该目录下的所有文件。

   目录和文件名支持完全匹配，也支持模糊匹配，具体可参考**路径配置内容**进行设置。

   说明

   当设置的黑名单与配置的采集路径重复或者有重合时，优先过滤掉黑名单设置的文件。

4. 日志格式、日志时间具体说明如下：

表 4-1 日志采集信息

名称	说明
日志格式	• 单行日志：采集的日志文件中，如果您希望每一行日志在LTS界面中都显示为一条单独的日志数据，则选择单行日志。 • 多行日志：采集的日志中包含像java异常的日志，如果您希望多行异常的日志显示为一条日志，正常的日志则每一行都显示为一条单独的日志数据，则选择多行日志，方便您查看日志并且定位问题。
日志时间	系统时间：表示系统当前时间，默认为日志采集时间，每条日志的行首显示日志的采集时间。 **说明** • 日志采集时间：ICAgent采集日志，并且发送到云日志服务的时间。 • 日志打印时间：系统产生并打印日志的时间。ICAgent采集日志并发送日志到云日志平台的频率为1秒钟。 • 采集日志时间限制：系统时间的前后24小时内。

名称	说明
	时间通配符：用日志打印时间来标识一条日志数据，通过时间通配符来匹配日志，每条日志的行首显示日志的打印时间。 ● 如果日志中的时间格式为：2019-01-01 23:59:59.011，时间通配符应该填写为：YYYY-MM-DD hh:mm:ss.SSS。 ● 如果日志中的时间格式为：19-1-1 23:59:59.011，时间通配符应该填写为：YY-M-D hh:mm:ss.SSS。 **说明** 如果日志中不存在年份信息，则云日志会自动补齐年份数据为当前年份数据。 填写示例： YY - year (19) YYYY - year (2019) M - month (1) MM - month (01) D - day (1) DD - day (01) hh - hours (23) mm - minutes (59) ss - seconds (59) SSS - millisecond (999) hpm - hours (03PM) h:mmpm - hours:minutes (03:04PM) h:mm:sspm - hours:minutes:seconds (03:04:05PM) hh:mm:ss ZZZZ (16:05:06 +0100) hh:mm:ss ZZZ (16:05:06 CET) hh:mm:ss ZZ (16:05:06 +01:00)
分行模式	日志格式选择多行日志时，需要选择分行模式，分行模式选择“日志时间”时，是以时间通配符来划分多行日志；当选择“正则模式”时，则以正则表达式划分多行日志。
正则表达式	此配置是用来标识一条日志数据的正则表达式。日志格式选择“多行日志”格式后且“分行模式”已选择“正则模式”后需要设置。
日志拆分	云日志服务支持对日志进行拆分，默认为关闭状态。 当日志大小超过500KB时，开启日志拆分按钮，则单行日志会被拆分为多行采集。例如：日志大小为600KB，被拆分为2行日志采集，第一行500KB，第二行100KB。 当日志大小超过500KB时，未开启日志拆分按钮，则单条日志大小限制不超过500KB，超过限制部分会被截断丢弃。
采集二进制文件	云日志服务支持采集二进制文件，默认为关闭状态。 您可以通过命令（*file -i 文件名*）查看文件类型，如果包含charset=binary，那么该日志文件就是二进制文件。 当日志的文件类型为二进制时，开启采集二进制文件按钮，则对接入的二进制文件日志进行采集，但仅支持UTF8编码的字符串，非UFT8编码的字符在LTS控制台页面会显示乱码。 当日志的文件类型为二进制时，未开启采集二进制文件按钮，则对接入的二进制文件日志停止采集，开启后即可进行采集。

说明

时间通配和正则表达式均是从每行日志的开头进行严格匹配，如果匹配不上，则会默认使用系统时间上报，这样可能会和文件内容中的时间不一致。**如果没有特殊需求，建议使用单行日志-系统时间模式即可**。

查看日志接入

返回云日志服务管理控制台，单击“日志接入”，或在完成主机接入成功后单击“返回接入配置列表”，进入日志接入页面。

- 在接入配置列表中显示已配置完成的接入配置，单击接入配置名称可进入详情页面，查看该接入配置详细信息。
- 单击所属日志组或所属日志流，可以进入对应日志组列表或日志流页面查看详细信息。
- 编辑日志接入：单击需修改接入配置所在行操作列的  ，参考日志接入的**操作步骤**进行修改。
- 删除日志接入：单击需删除接入配置所在行操作列的  。
- 标签管理：单击需添加接入配置所在行操作列的  ，添加标签。

5 主机管理

5.1 主机组

主机组是为了便于分类管理、提升配置多个主机日志采集的效率，对主机进行虚拟分组的单位。云日志服务支持通过一个接入配置来采集多台主机上的日志，您可以将这些主机加入到同一个主机组，并将该主机组关联至对应的接入配置中，方便您对多台主机日志进行采集。

- 当用户扩容主机时，只需在主机组中添加主机，该主机会自动继承关联的日志路径，无需为每台主机重复配置路径。
- 当用户修改多个主机采集路径时，只需修改对应的主机组关联的路径，无需为每台主机重复配置路径。

创建主机组（IP 地址）

1. 登录云日志服务管理控制台，单击“主机管理”，进入主机管理页面，单击右上角“新建主机组”。
2. 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”。
3. 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。
   - 可以通过主机名称或主机IP对列表进行过滤，也可以单击 批量搜索主机IP ，并在弹出的搜索框中输入多个主机IP，进行批量搜索。
   - 当列表中没有所需主机时，单击“安装ICAgent”，在弹出的页面安装指引完成主机安装，具体操作可参见**安装ICAgent**。

创建主机组（自定义标识）

1. 在主机管理页面，单击右上角“新建主机组”。
2. 在弹出的新建主机组页面，输入“主机组名称”，选择主机组类型“自定义标识”。
3. 单击 添加标识 ，添加自定义标识。

说明

最多可添加10个自定义标识。

4. 完成后，单击“确定”。
5. 执行以下操作创建custom_tag文件。
   a. 执行“cd /opt/cloud”命令，在cloud目录下，执行mkdir lts 创建lts目录。
   b. 继续执行“chmod 750 lts”，修改lts目录权限。
   c. 在lts目录下执行“touch custom_tag”，创建custom_tag文件 。
   d. 继续执行“chmod 640 custom_tag;vi custom_tag”命令，修改custom_tag权限并打开该文件。
   e. 按i进入insert模式，键入自定义标识后，按ESC键，“:wq!”保存退出即可。

说明

执行5之后，支持以下两种方式将主机加入到自定义标识主机组：

第一种（推荐使用）：

Linux主机

在主机里***/opt/cloud/lts***目录下的**custom_tag**文件中，查看该主机的标识，然后将该主机的标识，添加为主机组自定义标识，就可以将主机加入到该主机组下。例如：在主机里***/opt/cloud/lts***目录下的**custom_tag**文件中，查看该主机的标识为test1，创建主机组的自定义标识为test1，即将该主机加入到主机组下。

第二种：

Linux主机

- 在主机里***/opt/cloud/lts***目录下的**custom_tag**文件中，添加主机组自定义标识，可以将主机加入到该主机组下。例如：主机组的自定义标识为test，则在**custom_tag**文件中填写test，就可以将将主机加入到该主机组下。
- 当添加了多个自定义标识时，在主机里***/opt/cloud/lts***目录下的**custom_tag**文件中，任意填写一个自定义标识，就可以将主机加入到该主机组下。

修改主机组

对于已创建的主机组可以对其名称进行修改，也可以对主机组进行添加主机、移除主机或者关联接入配置，具体操作如下：

表 5-1 操作列表

操作	具体步骤
修改主机组名称	1. 在主机管理页面，默认显示主机组页签。 2. 在主机组列表中，单击待修改的主机组所在行的操作列 。 3. 在弹出的修改主机组页面，修改主机组名称、自定义标识。 4. 单击“确定”，完成主机名称修改。

操作	具体步骤
添加主机	**方式一：** 1. 在主机组列表，单击待修改的主机组所在行前的 。 2. 在主机页签，单击“添加主机”。 3. 在弹出的添加主机页面，主机列表中显示该主机组所选主机类型下所有未选主机，选择需要加入该主机组的主机。 ● 可以通过主机名称或主机IP对列表进行过滤，也可以单击 批量搜索主机IP ，并在弹出的搜索框中输入多个主机IP，进行批量搜索。 ● 当列表中没有所需主机时，单击“安装ICAgent”，在弹出的页面安装指引完成主机安装，具体操作可参见**安装ICAgent**。 4. 单击“确定”。 **方式二：** 1. 在主机管理页面，单击“主机”，切换至主机页签。 2. 在主机列表中勾选需要添加的主机，单击“添加到主机组”。 3. 在弹出的添加到主机组页面，勾选目标主机组。 4. 单击“确定”，完成主机的添加。
移除主机	1. 在主机组列表，单击待修改的主机组所在行前的 。 2. 在主机页签，单击待移除主机所在行操作列的“移除”。 3. 在弹出的移除主机页面，单击“确定”，将该主机移除。 **说明** 自定义标识主机组下的主机不支持该操作。
取消部署	1. 在主机组列表，单击待修改的主机组所在行前的 。 2. 在主机页签，单击待移除主机所在行操作列的“取消部署”。 3. 在弹出的取消部署页面，单击“确定”，将该主机卸载并移除。 **说明** ● 自定义标识主机组下的主机不支持该操作。 ● 主机取消部署后，其他主机组下的该主机也会被移除。
批量移除	1. 在主机组列表，单击待修改的主机组所在行前的 。 2. 在主机页签，勾选待删除的主机，单击“批量移除”。 3. 单击“确定”。
新增关联配置	1. 在主机组列表，单击待修改的主机组所在行前的 。 2. 默认显示主机页签，单击“相关接入配置”，切换至相关接入配置页签。 3. 单击“新增关联配置”。 4. 在弹出的新增关联配置页面，勾选需要关联的接入配置。 5. 单击“确定”，配置完成后会将所选的接入配置显示在列表中。

操作	具体步骤
解除关联	1. 在相关接入配置页签，单击待解除配置所在行操作列的“解除关联”。 2. 单击“确定”，解除该主机组与该接入配置的关联。
批量解除关联	1. 在相关接入配置页签，勾选待解除的配置，单击“批量解除关联”。 2. 单击“确定”，解除该主机组与所勾选的接入配置的关联。

删除主机组

删除主机组

1. 在主机管理页面，默认显示主机组页签。
2. 在主机组列表中，单击待删除的主机组所在行的操作列删除图标。
3. 在弹出的删除主机组页面，单击“确定”，删除该主机组。

批量删除主机组

1. 在主机组列表，勾选待删除的主机组，单击列表左上方“批量删除”。
2. 在弹出的删除主机组页面，单击“确定”，删除所勾选的主机组。

5.2 主机

5.2.1 安装 ICAgent

ICAgent是云日志服务进行日志采集的工具，运行在需要采集日志的主机中。使用云日志服务在主机采集日志时，需要安装ICAgent。您可以通过以下操作指导在主机中安装ICAgent。

前提条件

安装ICAgent前，请确保本地浏览器的时间、时区与主机的时间、时区一致。如果不一致，可能会导致日志上报出错。

安装方式说明

ICAgent有两种安装方式，请按照您的场景进行选择。

表 5-2 安装方式

方式	适用场景
首次安装	该服务器上未安装过ICAgent。
继承安装（Linux环境支持）	您有多个服务器需要安装ICAgent，其中一个服务器已经通过首次安装方式装好了ICAgent，对于没有安装ICAgent的其他多个服务器，您可以采用该安装方式。

首次安装（Linux 环境）

步骤1 在云日志服务管理控制台，单击“主机管理”。

步骤2 在主机管理页面，单击右上角“安装ICAgent”。

步骤3 “安装系统”选择“Linux”。

步骤4 选择“安装方式”。

- 获取AK/SK，方法请参考：**如何获取AK/SK**。
  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。

  须知

  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。

步骤5 单击“复制命令”，复制ICAgent安装命令。

步骤6 使用PuTTY等远程登录工具，以**root**用户登录所在region待安装ICAgent的服务器，执行ICAgent安装命令进行安装，当选择安装方式为“获取AK/SK”时需根据提示输入已获取到的AK/SK。

说明

- 当显示“ICAgent install success”时，表示安装成功，ICAgent已安装在了/opt/oss/servicemgr/目录。安装成功后，在云日志服务左侧导航栏中选择“主机管理 > 主机”，查看该服务器中ICAgent的状态。
- 如果安装失败，请卸载ICAgent后重新安装，如果还未安装成功，请联系技术支持。

----结束

继承安装（Linux 环境）

您有多个服务器需要安装ICAgent，其中一个服务器已经通过首次安装方式装好了ICAgent，且该服务器“/opt/ICAgent/”路径下存在ICAgent的安装包**ICProbeAgent.tar.gz**，对于没有安装ICAgent的服务器，可以通过该方式对服务器进行一键式继承安装。

1. 在已安装ICAgent的服务器上执行如下命令，其中*x.x.x.x*表示待安装ICAgent服务器的IP地址。

   bash /opt/oss/servicemgr/ICAgent/bin/remoteInstall/remote_install.sh -ip x.x.x.x
2. 根据提示输入待安装ICAgent的服务器root用户密码。

说明

- 如果已安装ICAgent的服务器安装过expect工具，执行上述命令后，即可完成安装。如果已安装ICAgent的服务器未安装expect工具，请根据提示输入密码，进行安装。
- 请确保已安装ICAgent的服务器可以使用root用户执行SSH、SCP命令，来与待安装ICAgent的服务器进行远端通信。
- 当显示“ICAgent install success”时，表示安装成功，ICAgent已安装在了/opt/oss/servicemgr/目录。安装成功后，在云日志服务左侧导航栏中选择主机管理 > 主机”，查看该服务器ICAgent的状态。
- 如果安装失败，请卸载ICAgent后重新安装，如果还未安装成功，请联系技术支持。

继承批量安装（Linux 环境）

您有多个服务器需要安装ICAgent，其中一个服务器已经通过首次安装方式装好了ICAgent，且该服务器“/opt/ICAgent/”路径下存在ICAgent的安装包**ICProbeAgent.tar.gz**，对于没有安装ICAgent的服务器，可以通过该方式对服务器进行一键式继承批量安装。

须知

- 批量安装的服务器需同属一个VPC下，并在同一个网段中。
- **批量安装功能依赖python3.*版本，如果安装时提示找不到python请安装python版本后重试。**

前提条件

已收集需要安装Agent的所有服务器的IP地址、密码，按照iplist.cfg格式整理好，并上传到已安装过ICAgent机器的/opt/ICAgent/目录下。iplist.cfg格式示例如下所示，IP地址与密码之间用空格隔开：

192.168.0.109 密码（请根据实际填写）

192.168.0.39 密码（请根据实际填写）

说明

- iplist.cfg中包含您的敏感信息，建议您使用完之后进行清理。
- 如果所有服务器的密码一致，iplist.cfg中只需列出IP，无需填写密码，在执行时输入此密码即可；如果某个IP密码与其他不一致，则需在此IP后填写其密码。

操作步骤

1. 在已安装ICAgent的服务器上执行如下命令。

   bash /opt/oss/servicemgr/ICAgent/bin/remoteInstall/remote_install.sh -batchModeConfig /opt/ICAgent/iplist.cfg

   根据脚本提示输入待安装机器的root用户默认密码，如果所有IP的密码在iplist.cfg中已有配置，则直接输入回车键跳过即可，否则请输入默认密码。

   ```
   batch install begin
   Please input default passwd:
   send cmd to 192.168.0.109
   send cmd to 192.168.0.39
   2 tasks running, please wait...
   2 tasks running, please wait...
   2 tasks running, please wait...
   ```



```
End of install agent: 192.168.0.39
End of install agent: 192.168.0.109
All hosts install icagent finish.
```

请耐心等待，当提示All hosts install icagent finish.时，则表示配置文件中的所有主机安装操作已完成。

2. 安装完成后，在云日志服务左侧导航栏中选择“主机管理 > 主机”，查看服务器的**Agent状态**。

5.2.2 升级 ICAgent

为了更好的采集体验，LTS会不断更新ICAgent版本。当系统提示您有新的ICAgent版本时，您可以按照如下操作步骤进行升级。

说明

云日志服务主机管理界面仅支持升级安装在Linux环境中ICAgent，不支持升级Windows环境中的ICAgent。

操作步骤

1. 在云日志服务管理控制台，单击“主机管理”。
2. 在主机管理页面，选择“主机”页签。
3. 选择“普通主机”，在主机列表中选中一个或多个待升级ICAgent前的复选框，单击“升级ICAgent”。
4. 在“升级ICAgent”对话框中单击“确定”。

   ICAgent开始升级，升级ICAgent预计需要1分钟左右，请耐心等待。待ICAgent的状态由“升级中”变为“运行”时，表示升级成功。

   说明

   如果升级后，界面显示ICAgent状态异常或者其它升级失败场景，请直接登录节点使用安装命令重新安装ICAgent即可（覆盖式安装，无需卸载操作）。

5.2.3 卸载 ICAgent

服务器上的ICAgent被卸载后，会影响该服务器的日志采集能力，请谨慎操作！

说明

卸载ICAgent不会删除对应的安装文件，请您根据实际情况自行删除。

卸载方式，您可以按照需要进行选择：

- **通过界面卸载**：此操作适用于正常安装ICAgent后需卸载的场景。
- **登录服务器卸载**：此操作适用于未成功安装ICAgent需卸载重装的场景。
- **远程卸载**：此操作适用于正常安装ICAgent后需远程卸载的场景。
- **批量卸载**：此操作适用于正常安装ICAgent后需批量卸载的场景。

通过界面卸载

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“主机”切换至主机页签。

3. 勾选一个或多个待卸载ICAgent的服务器的复选框，单击“卸载ICAgent”。
4. 在“卸载ICAgent”对话框中单击“确定”。
   ICAgent开始卸载，卸载ICAgent预计需要1分钟左右，请耐心等待。
   卸载完成后主机列表中将不会显示该主机。

   说明

   通过界面卸载ICAgent后如果需要再次安装，请等待5分钟后执行安装操作，否则可能出现被再次自动卸载的情况。

登录服务器卸载

1. 以**root**用户登录需卸载ICAgent的服务器。
2. 执行如下命令卸载ICAgent。
   bash /opt/oss/servicemgr/ICAgent/bin/manual/uninstall.sh;
   当显示“ICAgent uninstall success”时，表示卸载成功。

远程卸载

除了上述登录服务器上执行uninstall.sh命令卸载ICAgent的方式，还可以对服务器进行远程卸载。

1. 在已安装ICAgent的服务器上执行如下命令，其中*x.x.x.x*表示待卸载ICAgent的服务器的IP地址。
   bash /opt/oss/servicemgr/ICAgent/bin/remoteUninstall/remote_uninstall.sh -ip x.x.x.x
2. 根据提示输入待卸载ICAgent的服务器root用户密码。

   说明

   - 如果已安装ICAgent的服务器安装过expect工具，执行上述命令后，即可完成卸载。如果已安装ICAgent的服务器未安装expect工具，请根据提示输入密码，进行卸载。
   - 请确保已安装ICAgent的服务器可以使用root用户执行SSH、SCP命令，来与待卸载ICAgent的服务器进行远端通信。
   - 当显示“ICAgent uninstall success”时，表示卸载成功。

批量卸载

当您已有服务器安装过ICAgent，且该服务器“/opt/ICAgent/”路径下存在ICAgent安装包**ICProbeAgent.tar.gz**，通过该方式可对多个服务器进行一键式继承批量卸载。

须知

批量卸载的服务器需同属一个VPC下，并在同一个网段中。

前提条件

已收集需要卸载Agent的所有服务器的IP地址、密码，按照iplist.cfg格式整理好，并上传到已安装过ICAgent机器的/opt/ICAgent/目录下。iplist.cfg格式示例如下所示，IP地址与密码之间用空格隔开：

192.168.0.109 密码（请根据实际填写）

192.168.0.39 密码（请根据实际填写）

说明

- iplist.cfg中包含您的敏感信息，建议您使用完之后进行清理。
- 如果所有服务器的密码一致，iplist.cfg中只需列出IP地址，无需填写密码，在执行时输入此密码即可；如果某个IP密码与其他不一致，则需在此IP地址后填写其密码。

操作步骤

1. 在已安装ICAgent的服务器上执行如下命令。

   bash /opt/oss/servicemgr/ICAgent/bin/remoteUninstall/remote_uninstall.sh -batchModeConfig /opt/ICAgent/iplist.cfg

   根据脚本提示输入待卸载机器的root用户默认密码，如果所有IP地址的密码在iplist.cfg中已有配置，则直接输入回车键跳过即可，否则请输入默认密码。

   ```
   batch uninstall begin
   Please input default passwd:
   send cmd to 192.168.0.109
   send cmd to 192.168.0.39
   2 tasks running, please wait...
   End of uninstall agent: 192.168.0.109
   End of uninstall agent: 192.168.0.39
   All hosts uninstall icagent finish.
   ```

   请耐心等待，当提示All hosts uninstall icagent finish.时，则表示配置文件中所有服务器的卸载操作已完成。

2. 卸载完成后，在云日志服务左侧导航栏中选择“主机管理 > 主机”，查看该服务器的ICAgent状态。

5.2.4 Agent 状态

ICAgent状态说明详见下表。

表 5-3 ICAgent 状态

状态	说明
运行	该服务器的ICAgent运行正常。
未安装	该服务器未安装ICAgent。
安装中	正在为该主机安装ICAgent。安装ICAgent预计需要1分钟左右，请耐心等待。
安装失败	该主机的ICAgent安装失败。
升级中	正在升级该服务器的ICAgent。升级ICAgent预计需要1分钟左右，请耐心等待。
升级失败	该服务器的ICAgent升级失败。
离线	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。
异常	该主机ICAgent功能异常，请联系技术支持。
卸载中	正在卸载该主机。卸载ICAgent预计需要1分钟左右，请耐心等待。

状态	说明
鉴权错误	安装该主机时配置的参数问题导致无法正常鉴权。
受限	LTS服务的License受限，需要用户查看License使用情况，并及时更新。

6 日志搜索与分析

6.1 日志搜索

您可以通过本操作设置关键字和时间范围进行日志搜索。

1. 在云日志服务管理控制台，单击“日志管理”。
2. 在日志组列表中，单击日志组名称前对应的 按钮。
3. 在日志流列表中，单击日志流名称，进入日志详情页面。
4. 在右上角选择时间范围。

   时间范围有三种方式，分别是相对时间、整点时间和自定义时间。您可以根据自己的实际需求，选择时间范围。

   说明

   - 相对时间：表示查询距离当前时间1分钟、5分钟、15分钟等时间区间的日志数据。例如当前时间为19:20:31，设置相对时间1小时，表示查询18:20:31~19:20:31的日志数据。
   - 整点时间：表示查询最近整点1分钟、15分钟等时间区间的日志数据。例如当前时间为19:20:31，设置整点时间1小时，表示查询18:00:00~19:00:00的日志数据。
   - 自定义时间：表示查询指定时间范围的日志数据。
5. 在日志详情页面，有以下搜索方式：

   a. 在页面搜索区域中，鼠标单击搜索框，下拉框中显示如下：

      - 结构化配置字段或索引配置字段。内置字段不展示在该下拉提示框中，但输入内置字段时，下拉提示框会自动关联匹配。
      - 关键词：有“NOT”、“AND”、“OR”、“:”和“:*”五种，除“NOT”外的其他关键词需要输入关键词后，才会展示在下拉提示框里。

        说明

        - 当输入关键字时，可使用Tab键自动补全下拉提示框中显示的第一个关键词。
        - 关键词不区分大小写。

- 历史记录：可以记录20条，但搜索提示框仅展示最新3条记录。
- 快速查询：展示已创建的快速查询字段。
- 搜索语法说明：常用的搜索语法。

输入待搜索的关键字，或在弹出的下拉框中选择待搜索的字段和关键词，单击“查询”，开始搜索。

显示包含搜索关键字的日志。

说明

- 内置字段有appName、category、clusterId、clusterName、collectTime、containerName、hostIP、hostIPv6、hostId、hostName、nameSpace、pathFile、podName、serviceID，默认简化显示，并且hostIP、hostName、pathFile默认显示在最前面。
- 结构化配置的字段按照key:value显示。

b. 在原始日志页面中，鼠标悬浮指向**日志内容**中的字段，单击蓝色字体的日志内容，支持复制、添加到查询、从查询中排除的方式搜索日志。

c. 对已创建快速分析的字段，单击选择字段可直接将其添加到页面搜索框中，进行搜索。

说明

通过单击字段添加到搜索框中，如果是同一字段，则将直接替换该方式添加的字段，不会进行AND搜索；如果是不同字段，则对不同字段进行AND搜索。

d. 在页面搜索区域，使用键盘的"↑""↓"箭头，选择待搜索的关键字或搜索语法，单击Tab键或Enter键选中后，单击“查询”，开始搜索。

日志搜索的常用操作

日志搜索的常用操作有分享日志、刷新等操作，具体参考如下图所示：

表 6-1 常用操作

操作	说明
创建快速查询	单击 按钮，创建快速查询。
分享日志	单击 复制当前日志搜索页面的链接，用于分享搜索日志。
刷新日志	单击 对日志进行刷新，有两种方式刷新方式：手动刷新和自动刷新。 ● 手动刷新：单击“手动刷新”可直接对日志进行刷新。 ● 自动刷新：选择自动刷新的间隔时间，将对日志进行自动刷新。间隔时间范围为15秒、30秒、1分钟和5分钟。
复制	单击 复制日志内容。
查看上下文	单击 查看日志上下文。

操作	说明
简化字段详情	单击 ··· 查看简化字段详情。
换行/取消换行	单击  按钮，搜索的日志内容将换行显示。若不需要换行，单击  按钮，取消换行。 **说明** 默认开启换行按钮。
下载日志	单击  按钮，在弹出的下载日志页面中单击“本地下载”和“前往创建转储”。 本地下载：将日志文件直接下载到本地，单次下载支持最大5,000条日志。 在下拉框中选择“.csv”或“.txt”，单击“开始下载日志”，可将日志导出至本地。 **说明** ● 选择以CSV格式导出日志后，本地以表格形式保存日志的具体标签信息。 ● 选择导出TXT格式日志后，本地会以.txt格式保存日志的日志内容。
全部折叠/全部展开	单击  设置日志内容展示的行数。若不需要展示日志内容，再单击一次  按钮即可关闭展示的日志内容。 **说明** 默认不折叠。折叠后，默认显示2行，最多支持展示6行。
版面设置	鼠标悬浮在  按钮上，单击“版面设置”，在弹出的版面设置页面中，设置字段是否简化显示和可见性。 ● 是否简化显示：开启该按钮，日志的字段内容将简化显示。 ● 可见性：当关闭字段的可见性时，日志内容中将不显示。
JSON设置	鼠标悬浮在  按钮上，单击“JSON设置”，在弹出的JSON设置页面中，设置格式化显示。 **说明** 默认开启格式化，JSON默认展开层级为2层。 ● 开启格式化按钮：设置JSON默认展开层级，最大设置为10层。 ● 关闭格式化按钮：对于JSON格式的日志，将不会格式化层级显示。

操作	说明
不可见字段列表	该列表展示版面设置中配置的不可见性字段。 • 当日志流未配置版面设置时，将不显示 按钮。 • 当日志内容为“CONFIG_FILE”且未配置版面设置时，不可见字段默认有appName、clusterId、clusterName、containerName、hostIPv6、NameSpace、podName和serviceID。

6.2 内置保留字段

在采集日志时，日志服务会将采集时间、日志类型、主机IP等信息以Key-Value对的形式添加到日志中，这些字段是云日志服务的内置字段。

说明

- 使用API写入日志数据或添加ICAgent配置时，请不要将字段名称设置为内置保留字段，否则可能会造成字段名称重复、查询不精确等问题。
- 用户自定义日志字段名称中不能使用双下划线__，否则无法配置索引。

日志示例

如下是一条日志示例，content字段值是日志原文，其他字段是常见的一些内置保留字段。

```
{    "hostName":"epstest-xx518",
     "hostIP":"192.168.0.31",
     "clusterId":"c7f3f4a5-xxxx-11ed-a4ec-0255ac100b07",
     "pathFile":"stdout.log",
     "content":"level=error ts=2023-04-19T09:21:21.333895559Z",
     "podIp":"10.0.0.145",
     "containerName":"config-reloader",
     "clusterName":"epstest",
     "nameSpace":"monitoring",
     "hostIPv6":"",
     "collectTime":"1681896081334",
     "appName":"alertmanager-alertmanager",
     "hostId":"318c02fe-xxxx-4c91-b5bb-6923513b6c34",
     "lineNum":"1681896081333991900",
     "podName":"alertmanager-alertmanager-54d7xxxx-wnfsh",
     "__time__":"1681896081334",
     "serviceID":"cf5b453xxxad61d4c483b50da3fad5ad",
     "category":"LTS"
 }
```

内置保留字段说明

内置保留字段	数据格式	索引与统计设置	说明
collectTime	整型，Unix时间戳（毫秒）	索引设置：开启索引后，日志服务默认为collectTime创建字段索引，索引数据类型为long类型。 查询时输入 collectTime : xxx。	采集时间，指日志被采集器ICAgent采集时的时间。 示例中的"collectTime":"1681896081334"，转换成标准时间是2023-04-19 17:21:21
__time__	整型，Unix时间戳（毫秒）	索引设置：开启索引后，日志服务默认为time创建字段索引，索引数据类型为long类型。该字段不支持查询。	日志时间，指的是日志在控制台页面展示的日志时间。 例如示例中的"__time__":"1681896081334"，转换成标准时间是2023-04-19 17:21:21 日志时间默认使用采集时间，也支持自定义日志时间。
lineNum	整型	索引设置：开启索引后，日志服务默认为lineNum创建字段索引，索引数据类型为long类型。	行号（偏移量），用来排序日志。 非高精度日志会根据collectTime生成，默认是collectTime * 1000000 + 1，高精度日志就是用户上报的纳秒值。 例如示例中的"lineNum":"1681896081333991900"。
category	字符串	索引设置：开启索引后，日志服务默认为category创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入 category: xxx。	日志类型，表示该日志的来源。 例如ICAgent采集的日志该字段为LTS，某云服务例如VPC上报的日志该字段为VPC。
clusterName	字符串	索引设置：开启索引后，日志服务默认为clusterName创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入 clusterName: xxx。	集群名称，k8s场景下集群名称。 例如示例中的"clusterName":"epstest"。

内置保留字段	数据格式	索引与统计设置	说明
clusterId	字符串	索引设置：开启索引后，日志服务默认为clusterId创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入clusterId: xxx。	集群ID，k8s场景下集群ID。 例如示例中的"clusterId":"c7f3f4a5-xxxx-11ed-a4ec-0255ac100b07"。
nameSpace	字符串	索引设置：开启索引后，日志服务默认为nameSpace创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入nameSpace: xxx。	命名空间，k8s场景下命名空间。 例如示例中的"nameSpace":"monitoring"。
appName	字符串	索引设置：开启索引后，日志服务默认为appName创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入appName: xxx。	组件名称，k8s场景下工作负载的名称。 例如示例中的"appName":"alertmanager-alertmanager"。
serviceID	字符串	索引设置：开启索引后，日志服务默认为serviceID创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入serviceID: xxx。	工作负载ID，k8s场景下工作负载ID。 例如示例中的"serviceID":"cf5b453xxxad61d4c483b50da3fad5ad"。
podName	字符串	索引设置：开启索引后，日志服务默认为podName创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入podName: xxx。	POD名称，k8s场景下POD名称。 例如示例中的"podName":"alertmanager-alertmanager-0"。
podIp	字符串	索引设置：开启索引后，日志服务默认为podIp创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入podIp: xxx。	pod的ip，k8s场景下pod的IP地址。 例如示例中的"podIp":"10.0.0.145"。

内置保留字段	数据格式	索引与统计设置	说明
containerName	字符串	索引设置：开启索引后，日志服务默认为containerName创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入containerName: xxx。	容器名称，k8s场景下容器名称。 例如示例中的"containerName":"config-reloader"。
hostName	字符串	索引设置：开启索引后，日志服务默认为hostName创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入hostName: xxx。	主机名称，ICAgent所在主机的名称。 例如示例中的"hostName":"epstest-xx518"。
hostId	字符串	索引设置：开启索引后，日志服务默认为hostId创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入hostId: xxx。	主机ID，ICAgent所在主机的id，该id由ICAgent生成。 例如示例中的"hostId":"318c02fe-xxxx-4c91-b5bb-6923513b6c34"。
hostIP	字符串	索引设置：开启索引后，日志服务默认为hostIP创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入hostIP: xxx。	主机IP，日志采集器所在主机的ip（适用于ipv4场景） 例如示例中的"hostIP":"192.168.0.31"。
hostIPv6	字符串	索引设置：开启索引后，日志服务默认为hostIPv6创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入hostIPv6: xxx。	主机IP，日志采集器所在主机的ip（适用于ipv6场景） 例如示例中的"hostIPv6":""。
pathFile	字符串	索引设置：开启索引后，日志服务默认为pathFile创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入pathFile: xxx。	文件路径，采集的日志文件的路径。 例如示例中的"pathFile":"stdout.log"。

内置保留字段	数据格式	索引与统计设置	说明
content	字符串	索引设置：开启全文索引后，会使用全文索引定义的分词符对content字段的value进行分词；不支持将content字段配置到字段索引中。	日志原文 例如示例中的"content":"level=error ts=2023-04-19T09:21:21.333895559Z"
logContent	字符串	不支持将logContent字段配置到字段索引中。	不涉及
logContentSize	整型	不支持将logContentSize字段配置到字段索引中。	不涉及
logIndexSize	整型	不支持将logIndexSize字段配置到字段索引中。	不涉及
groupName	字符串	不支持将groupName字段配置到字段索引中。	不涉及
logStream	字符串	不支持将logStream字段配置到字段索引中。	不涉及

6.3 索引配置

索引是一种存储结构，用于对日志数据进行查询。通过配置索引后，可对日志进行查询和分析操作。不同的索引配置，则会产生不同的查询和分析结果，请根据您的需要，合理配置索引。

日志示例

以下是一条典型日志，content字段值是日志原文，使用分隔符逗号将原始日志解析成3个字段level、status、message；

示例日志中的hostName、hostIP、pathFile是常见的内置保留字段，详细内置字段请参考**内置保留字段**。

```
{ "hostName":"epstest-xx518",
    "hostIP":"192.168.0.31",
    "pathFile":"stdout.log",
    "content":"error,400,I Know XX",
    "level":"error",
    "status":400,
    "message":"I Know XX"
 }
```

下图是日志示例的一种典型索引配置：

索引类型

云日志服务的索引类型如下：

表 6-2 索引类型表

索引类型	说明
全文索引	开启全文索引后，日志服务根据您设置的分词符将整条日志所有字段值拆分成多个词并构建索引。 **说明** • 用户上传的自定义标签（label）字段，不包含全文索引中，如果您需要搜索自定义标签字段，请添加对应的字段索引。 • LTS内置保留字段，不包含全文索引中，您需要通过字段索引Key:Value的方式进行搜索，请参考**内置保留字段**。
字段索引	配置字段索引后，您可以指定字段名称和字段值（Key:Value）进行查询，缩小查询范围。 **说明** • 日志服务默认为部分内置保留字段创建字段索引，请参考**内置保留字段**。 • 如果您的某个字段单独配置了字段索引，那么该字段值的分词符以字段索引配置为准。 • 结构化配置中的的快速分析列已被移除，如果您要使用**快速分析功能**，则必须配置字段索引且开启对应字段的快速分析按钮。 关于日志示例有两种情况： • 在日志示例中，配置了level和status两个字段索引，其中level是string类型，字段值是error，单独配置了分词符，status是long类型，不需要配置分词符；您可以使用level：error的方式精确搜索level字段值为error的所有日志。 • 在日志示例中，云日志服务LTS会默认为hostName、hostIP、pathFile这些内置保留字段创建字段索引。

注意事项

- 全文索引属性和字段索引属性必须至少启用一种。
- 索引配置（新增、编辑、删除字段，修改配置项等操作）只对新写入的日志生效，历史日志不会生效。当前不支持对历史日志重建索引。
- 关闭索引后，历史索引的存储空间将在当前日志流的数据保存时间到期后，自动被清除。
- 日志服务默认已为部分内置保留字段创建字段索引，请参见**内置保留字段**。
- 不同的索引配置，会产生不同的查询和分析结果，请根据您的需求，合理创建索引。全文索引和字段索引互不影响。

配置全文索引

步骤1 登录云服务日志控制台，单击“日志管理”。

步骤2 在日志组列表中，单击日志组名称左侧的 ，选择日志流，进入日志流管理界面。

步骤3 在日志流详情页面，单击右上角 ，进入索引配置页面。

步骤4 在索引配置页面中，默认开启“全文索引”按钮。

说明

- 在索引配置页面选择自动配置时，默认获取最近15分钟的原始日志和内置字段的交集，LTS自动将原始日志和内置字段的交集、当前结构化字段、tag字段一起组成字段索引下方的表格数据。
- 若15分钟内没有原始日志，则获取hostIP、hostName、pathFile、结构化字段、tag字段结合共同组成字段索引下方的表格数据。
- ECS接入选择结构化配置时，进入索引配置页面，则会自动加上如下字段：category、hostName、hostId、 hostIP、 hostIPv6、 pathFile，添加字段时，若某个字段已存在于索引配置，则不会重复添加。

步骤5 请参考表6-3配置参数信息。

表 6-3 自定义全文索引配置参数

参数	说明
全文索引	打开全文索引开关，表示创建全文索引。
大小写敏感	查询时是否区分英文字母的大小写。 • 打开大小写敏感开关，则查询时区分大小写。例如示例日志含有Know，那么您只能使用**Know**才能查询到该日志。 • 关闭大小写敏感开关，则查询时不区分大小写。例如示例日志含有Know，那么您使用关键字**KNOW**和**know**都能查到该日志。
包含中文	查询时是否区分中英文。 • 打开包含中文开关后，如果日志中包含中文，默认按照一元分词法拆分中文内容，按照分词符的设置拆分英文内容。 **说明** 一元分词是指将中文字符串拆分为一个个独立的中文字。 使用一元分词符的优点是对海量日志分词效率高，其他中文分词方法对写入速度影响大。 • 关闭包含中文开关后，按照分词符的设置拆分所有内容。 例如示例日志内容为： **error,400,I Know 今天是星期一**。 • 关闭包含中文开关后，按照分词符的设置拆分英文内容，日志会被拆分为**error**、**400**、**I**、**Know**、**今天是星期一**，您可以通过**error**或**今天是星期一**查找该日志。 • 打开包含中文开关后，日志服务后台分词器将日志拆分为**error**、**400**、**I**、**Know**、**今**、**天**、**是**、**星**、**期**、**一**，您通过**error**或**今天**等词都可以查找到该日志。

参数	说明
分词符	根据指定分词符，将日志内容拆分成多个词。日志服务的默认分词符为, '";=()[]{}@&<>/:\n\t\r。当默认设置不能满足您的需求时，您可以自定义设置分词符。所有的ASCII码包括中文都可被定义为分词符。 如果设置分词符为空，则字段值将被当成一个整体，您只能通过完整字符串或模糊查询查找对应的日志。 例如示例日志内容为： **error,400,I Know 今天是星期一**。 • 如果不设置任何分词符，整条日志被作为一个词**error,400,I Know 今天是星期一**，您只能通过完整字符串**error,400,I Know 今天是星期一**或模糊查询**error,400,I K***查找该日志。 • 如果设置分词符为逗号（,），则原始日志被拆分为**error**、**400**、**I Know 今天是星期一**3个词，您通过任意一个词或词的模糊查询都可以找到该日志，例如**error**、**400**、**Kn***、**今天是***。 • 如果设置分词符为逗号（,）和空格，则原始日志被拆分为**error**、**400**、**I**、**Know**、**今天是星期一**5个词，您通过任意一个词或词的模糊查询都可以找到该日志，例如**Know**、**今天是***。

步骤6 完成后，单击确定。

----结束

配置字段索引

创建字段索引时，最多支持添加500个字段。其中JSON类型字段，最多支持添加100个子字段。

步骤1 登录云服务日志控制台，单击“日志管理”。

步骤2 在日志组列表中，单击日志组名称左侧的 ，选择日志流，进入日志流管理界面。

步骤3 在日志流详情页面，单击右上角 ，进入索引配置页面。单击添加字段，输入字段名称。

步骤4 参考表6-4配置字段索引。

说明

- 字段索引的参数配置仅对该字段生效。
- 当添加的字段在日志内容中不存在时，则配置的该索引字段无效。

表 6-4 自定义字段索引配置参数

参数	说明
字段名称	日志字段名称，例如示例日志中的level。 字段名称只能包括字母、数字或下划线（ _ ），且只能以字母或下划线（ _ ）开头，字段名称中不能含有双下划线。 **说明** • 双下划线（ __ ）在LTS不对用户呈现的内置保留字段中使用，用户自定义日志字段名中不能使用双下划线__，否则无法配置字段索引名称。 • 日志服务默认会对部分内置保留字段开启字段索引，请参见**内置保留字段**。
类型	• 日志字段值（ Value ）的数据类型，可选值为string、long、float。 • long类型和float类型不支持设置大小写敏感、包含中文和分词符。
快速分析	默认为开启状态，开启后，可以对字段值做采样统计，请参见**11.6.4-快速分析**。 **说明** • 快速分析的原理是对搜索命中的日志采样10万条进行数据统计，不是全量统计。 • 快速分析的字段长度最大为2000字节。 • 快速分析字段展示前100条数据。
操作	单击“删除”，删除添加的自定义字段。

步骤5 完成后，单击“确定”。

----结束

自动配置字段索引

在创建字段索引时，您可以单击自动配置，日志服务会自动添加一些字段索引，您可以根据自己的需要增加或者删除字段：

- 日志服务会根据采集时预览数据中的第一条内容，自动生成字段索引。
- 日志服务会选取几个最常见的内置保留字段添加到字段索引中（例如hostIP、hostName、pathFile）。

6.4 云端结构化解析

6.4.1 日志结构化配置

日志数据可分为结构化数据和非结构化数据。结构化数据指能够用数字或统一的数据模型加以描述的数据，具有严格的长度和格式。非结构化数据指不便于用数据库二维逻辑表来表现的数据，数据结构不规则或不完整，没有预定义的数据模型。

日志结构化是以日志流为单位，通过不同的日志提取方式将日志流中的日志进行结构化，提取出有固定格式或者相似程度较高的日志，过滤掉不相关的日志。

注意事项

- 日志结构化是以日志流为单位，请先创建一个日志流。
- 日志流中的大部分日志需有一定的规则，否则结构化是无意义的。

创建结构化配置

通过对日志流添加提取规则将日志流中的原始日志按一定的规律进行提取，并将提取后的日志整合到一起。

下面详细介绍原始日志结构化的操作步骤：

步骤1 登录LTS控制台，在左侧导航栏中选择“日志管理”。

步骤2 结构化日志以日志流为单位，请在“日志管理”页面选择目标日志组和日志流。

步骤3 在日志流详情页面，单击右上角  ，在弹出页面中，选择“结构化配置”，进入日志结构化配置页面，选择对应的日志提取方法进行配置。

- **正则分析**
- **JSON**
- **分隔符**
- **Nginx**
- **结构化模板**

说明

- 如果结构化后的字段长度超过20k字节时，仅会保留前20k字节长度。
- 结构化不支持的系统字段包括：groupName、logStream、lineNum、content、logContent、logContentSize、collectTime、category、clusterId、clusterName、containerName、hostIP、hostId、hostName、nameSpace、pathFile、podName。

步骤4 完成后，单击“保存”。

----结束

修改结构化配置

结构化配置创建完成后，如果您需要修改结构化配置时，操作步骤如下：

步骤1 在结构化配置页面中，单击  ，可修改结构化配置。

说明

修改结构化配置支持修改结构化方式、日志提取字段和tag字段等。

步骤2 完成后，单击“保存”。

----结束

删除结构化配置

如果日志结构化配置不再使用，可以删除结构化配置，操作步骤如下：

步骤1 在结构化配置页面中，单击 ，可删除结构化配置。

步骤2 在弹出对话框中，单击“确定”。

说明

删除结构化配置后，无法恢复，请谨慎操作。

----结束

6.4.2 结构化方式

云日志服务（LTS）目前支持5种日志结构化方式，分别是正则分析、JSON、分隔符、Nginx和结构化模板。您可以根据日志内容的实际场景进行选择。

正则分析

正则分析是使用正则表达式提取字段。

步骤1 选择示例日志：应选择一条比较典型的日志作为示例日志。

- **从已有日志中选择**：单击“从已有日志中选择”，在弹出框中根据业务需求选择待操作的日志，单击“确定”。通过选择不同时间段筛选日志。
- **从剪切板中粘贴**：单击“从剪切板中粘贴”，可直接自动将您剪切的日志内容复制到示例日志框中。

说明

时间范围有三种方式，分别是相对时间、整点时间和自定义时间。您可以根据自己的实际需求，选择时间范围。

- 相对时间：表示查询距离当前时间1分钟、5分钟、15分钟等时间区间的日志数据。例如当前时间为19:20:31，设置相对时间1小时，表示查询18:20:31~19:20:31的日志数据。
- 整点时间：表示查询最近整点1分钟、15分钟等时间区间的日志数据。例如当前时间为19:20:31，设置整点时间1小时，表示查询18:00:00~19:00:00的日志数据。
- 自定义时间：表示查询指定时间范围的日志数据

步骤2 字段提取。包括自动生成和手动输入两种方式，可将选择的日志提取为以一个示例字段对应一个字段名称的格式的日志解析结果。

- 自动生成：当用户选择自动生成时，可以用鼠标选中示例日志中待结构化的日志内容，在弹出的对话框中为选中内容设置一个名称，名称必须以字母开始，且仅包含字母和数字。单击“添加”，如下图所示。
- 手动输入：当用户选择手动输入时，可以在输入框中输入正则表达式，单击“生成字段”来进行字段提取。正则表达式通过分组来捕获字段，分组指用圆括号"()"括起来的正则表达式，匹配出的内容就表示一个分组，分组包含如下三种形式：
  - (exp)：把括号内的正则作为一个分组，系统自动分配组号，规则为从正则表达式的左边开始，第一个左括号”(”对应第一个分组，第二个”(”对应第二个分组，依次类推，组号从1开始，从左向右，依次累加。
  - (?<name>exp)：表示命名分组，分组的正则表达式为exp，分组名为name。分组名必须以字母开始，且仅包含字母和数字，可以通过分组名或分组号引用该分组。

- (?:exp)：表示不捕获分组，该分组只在当前位置匹配文本，在该分组之后，无法引用该分组，因为该分组没有分组名，没有分组号，也不会占用分组编号。

说明

- 在手工输入方式中，正则表达式的长度不能超过5000个字符，不强制要求用户在输入正则表达式时对分组进行命名，单击“生成字段”会以命名分组中的分组名作为字段名称，对于非命名分组会提取出对应的字段，并给字段名称默认命名field1、field2、field3……。

步骤3 单击“保存”，完成日志结构化配置，初次设置完成后将不能对字段类型编辑修改。

----结束

JSON

JSON是通过提取JSON字段将其拆分为键值对。

步骤1 选择示例日志：应选择一条比较典型的日志作为示例日志。在“步骤1 选择示例日志”中，可单击“从已有日志中选择”，在弹出框中根据业务需求选择待操作的日志，也可以直接在输入框中输入待操作的日志，单击“确定”。通过选择不同时间段筛选日志。

说明

时间范围有三种方式，分别是相对时间、整点时间和自定义时间。您可以根据自己的实际需求，选择时间范围。

- 相对时间：表示查询距离当前时间1分钟、5分钟、15分钟等时间区间的日志数据。例如当前时间为19:20:31，设置相对时间1小时，表示查询18:20:31~19:20:31的日志数据。
- 整点时间：表示查询最近整点1分钟、15分钟等时间区间的日志数据。例如当前时间为19:20:31，设置整点时间1小时，表示查询18:00:00~19:00:00的日志数据。
- 自定义时间：表示查询指定时间范围的日志数据

步骤2 字段提取。可将输入或选择的日志自动提取为以一个示例字段对应一个字段名称的格式的日志解析结果。

在“步骤2 字段提取”下单击“智能提取”。以如下原始日志为例进行分析：

将以下原始日志输入待操作框中。

```
{"a1": "a1", "b1": "b1", "c1": "c1", "d1": "d1"}
```

通过智能提取结果如下图。

说明

- 当日志提取字段的类型为float时，精确度为7位有效数字。
- 如果超过7位有效数字的话，则会导致提取字段内容不准确，从而影响可视化查看和快速分析，因此建议将字段类型修改为String。

在字段提取完成后，可对日志模板进行设置。结构化字段设置规则请参考**设置结构化字段**。

步骤3 单击“保存”，完成日志结构化配置，初次设置完成后将不能对字段类型编辑修改。

----结束

分隔符

分隔符是使用分隔符（例如：逗号、空格或字符）提取字段。

步骤1 选择示例日志：应选择一条比较典型的日志作为示例日志。在“步骤1 选择示例日志”中，可单击“从已有日志中选择”，在弹出框中根据业务需求选择待操作的日志，也可以直接在输入框中输入待操作的日志，单击“确定”。通过选择不同时间段筛选日志。

说明

时间范围有三种方式，分别是相对时间、整点时间和自定义时间。您可以根据自己的实际需求，选择时间范围。

- 相对时间：表示查询距离当前时间1分钟、5分钟、15分钟等时间区间的日志数据。例如当前时间为19:20:31，设置相对时间1小时，表示查询18:20:31~19:20:31的日志数据。
- 整点时间：表示查询最近整点1分钟、15分钟等时间区间的日志数据。例如当前时间为19:20:31，设置整点时间1小时，表示查询18:00:00~19:00:00的日志数据。
- 自定义时间：表示查询指定时间范围的日志数据

步骤2 在“步骤2 指定分隔符”需要根据原始日志内容选择分隔符，或自定义其他需要的特殊字符作为分隔符。

说明

- 不可见字符需要输入0x开头的16进制字符，长度为0-4个字符，总共32个不可见字符。
- 自定义字符支持输入1-10个字符，每个字符都作为独立的分隔符。
- 自定义字符串支持输入1-30个字符，字符串整体作为一个分隔符。

步骤3 字段提取。可将输入或选择的日志自动提取为以一个示例字段对应一个字段名称的格式的日志解析结果。

在“步骤3字段提取”下单击“智能提取”。以如下原始日志为例进行分析：

将以下原始日志输入待操作框中。

```
1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd 192.168.0.154 192.168.3.25 38929 53 17 1 96 1548752136 1548752736 ACCEPT OK
```

配置通过智能提取结果如下图。

说明

当日志提取字段的类型为float时，精确度为7位有效数字。

如果超过7位有效数字的话，则会导致提取字段内容不准确，从而影响可视化查看和快速分析，因此建议将字段类型修改为String。

在字段提取完成后，可对日志模板进行设置。结构化字段设置规则请参考**设置结构化字段**。

步骤4 单击“保存”，完成日志结构化配置，初次设置完成后将不能对字段类型编辑修改。

----结束

Nginx

Nginx是通过log_format指令来自定义访问日志的格式。

步骤1 选择示例日志：应选择一条比较典型的日志作为示例日志。在“步骤1 选择示例日志”中，可单击“从已有日志中选择”，在弹出框中根据业务需求选择待操作的日

志，也可以直接在输入框中输入待操作的日志，单击“确定”。通过选择不同时间段筛选日志。

说明

时间范围有三种方式，分别是相对时间、整点时间和自定义时间。您可以根据自己的实际需求，选择时间范围。

- 相对时间：表示查询距离当前时间1分钟、5分钟、15分钟等时间区间的日志数据。例如当前时间为19:20:31，设置相对时间1小时，表示查询18:20:31~19:20:31的日志数据。
- 整点时间：表示查询最近整点1分钟、15分钟等时间区间的日志数据。例如当前时间为19:20:31，设置整点时间1小时，表示查询18:00:00~19:00:00的日志数据。
- 自定义时间：表示查询指定时间范围的日志数据

步骤2 在“步骤2 输入Nginx日志配置”中需要输入Nginx日志配置，根据输入或选择的日志进行配置。其中有默认配置可使用，单击“默认Nginx配置”即可。

说明

标准Nginx配置文件中，日志配置的部分通常以log_format开头。

日志格式

- 默认配置如下所示。

```
log_format  main   '$remote_addr - $remote_user [$time_local] "$request" '
                   '$status $body_bytes_sent "$http_referer" '
                   '"$http_user_agent" "$http_x_forwarded_for"';
```

- 用户也可进行自定义配置，具体配置格式要求如下所示。
  - 使用Nginx配置，不可为空
  - 以log_format开头，并且包含（'）和字段名称
  - 长度最大限制为5000
  - 需要与示例日志内容匹配
  - log_format字段之间的间隔，除大小字母、数字、下划线及中划线外，可使用其他任意字符
  - 以（'）或者（';）结尾

步骤3 字段提取。可将输入或选择的日志自动提取为以一个示例字段对应一个字段名称的格式的日志解析结果。

在“步骤3 字段提取”下单击“智能提取”。以如下原始日志为例进行分析：

将以下原始日志输入待操作框中。

```
39.149.31.187 - - [12/Mar/2020:12:24:02 +0800] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36" "-"
```

并使用如下Nginx日志配置。

```
log_format  main   '$remote_addr - $remote_user [$time_local] "$request" '
                   '$status $body_bytes_sent "$http_referer" '
                   '"$http_user_agent" "$http_x_forwarded_for"';
```

通过智能提取结果如下图。

说明

- 当日志提取字段的类型为float时，精确度为7位有效数字。
- 如果超过7位有效数字的话，则会导致提取字段内容不准确，从而影响可视化查看和快速分析，因此建议将字段类型修改为String。

在字段提取完成后，可对日志模板进行设置。结构化字段设置规则请参考**设置结构化字段**。

步骤4 单击“保存”，完成日志结构化配置，初次设置完成后将不能对字段类型编辑修改。

----结束

结构化模板

结构化模板是通过自定义模板或系统内置模板提取字段。

详情请参考**结构化模板**。

6.4.3 结构化模板

云日志服务（LTS）目前支持的结构化模板有两种：系统模板和自定义模板。

系统模板

系统模板有VPC、TOMCAT、NGINX。

步骤1 在“选择模板”下，选择“系统模板”，选择对应的系统模板，模板日志从对应的云服务接入，可以直接应用模板的数据模型作为示例日志。

步骤2 选择模板后“模板详情”中会自动显示对应的日志解析结果。单击“保存”完成结构化配置

说明

结构化配置时，如果使用系统模板，则系统模板中的时间为自定义日志时间。

----结束

自定义模板

在“选择模板”下，选择“自定义模板”，选择已有的结构化模板。模板来源有以下两种方式：

- 在配置正则分析、JSON、分隔符或Nginx方式时单击左下角的“另存为模板”，系统会弹出“另存模板”页面，输入模板名称，单击“确定”，完成自定义模板的保存，会在“自定义模板”下的模板列表看到该模板。
- 新增结构化模板，具体操作如下：

  在“选择模板”下，选择“自定义模板”，单击“新增结构化模板”，在“新增结构化模板”界面选择正则分析、JSON、分隔符或Nginx方式，进行配置，配置完成后输入模板名称，单击“确定”。完成自定义模板的保存，会在“自定义模板”下的模板列表看到该模板。

6.4.4 结构化配置字段

设置结构化字段

在进行结构化配置字段提取之后，可对结构化字段进行设置，具体设置规则如下表。

表 6-5 结构化字段设置规则

日志提取方式	字段名称	字段类型是否可修改	字段是否可删除
正则分析（自动生成）	用户自定义。 名称必须以字母开始，且仅包含字母和数字。	是	是
正则分析（手动输入）	• 支持在输入正则表达式时进行命名。 • 支持使用系统默认命名field1、field2、field3……，或对其修改后的名称。	是	是
JSON格式	智能提取字段名称，可定义别名。	是	是
分隔符	默认名称field1、field2、field3……，可进行修改。	是	是
Nginx	根据Nginx配置生成，可定义别名。	是	是
VPC模板	根据VPC资料中提供的日志字段被定义。	否	否
自定义模板	用户自定义。	是	是

说明

正则分析（手动输入）、JSON格式、分隔符、Nginx和自定义模板的字段名称需要满足如下要求：

- 只支持输入英文、数字、中划线、下划线及小数点。
- 不能以小数点、下划线开头或以小数点结尾。
- 长度为1-64个字符。

设置 tag 字段

设置结构化配置时，可以对日志维度信息进行tag字段设置，设置完成后可以在可视化界面对设置字段进行SQL查询。

步骤1 在字段提取步骤中选择“tag字段”页签。

步骤2 单击“添加字段”。

步骤3 在tag字段列表中“字段名称”，输入需要设置 tag字段名称，例如hostIP。

说明

tag字段功能上线前设置的结构化配置，在修改结构化配置进行tag字段设置时，系统tag不会带出示例字段。

步骤4 如需添加多个字段可单击“添加字段”，继续添加。

步骤5 设置完成后单击“保存”。

说明

- tag支持的系统字段包括：category、clusterId、clusterName、containerName、hostIP、hostId、hostName、nameSpace、pathFile、podName。
- tag不支持的系统字段包括：groupName、logStream、lineNum、content、logContent、logContentSize、collectTime。
- 日志提取字段和tag字段可以同时设置。

----结束

6.5 搜索语法与功能

6.5.1 搜索语法

云日志服务LTS提供一套搜索语法用于设置搜索条件，帮助您更有效地搜索日志。

说明

- 使用搜索语法前，请您在索引配置处设置对应分词符，如无特殊需要，可直接使用默认的分词符，**'";=()[]{}@&<>/:\n\t\r。**
- 搜索语法不支持对分词符进行搜索。

  搜索语句不支持区分分词符，例如搜索语句**var/log**，其中/为分词符，搜索语句等同于**var log**，搜索的是同时包含**var**和**log**的所有日志。同理，搜索语句**"var:log"**、**var;log**等搜索的也是同时包含**var**和**log**的所有日志。

搜索方式

搜索语句用来指定日志搜索时的过滤规则，返回符合条件的日志。

根据索引配置方式可分为全文搜索和字段搜索，根据搜索精确程度可分为精确搜索和模糊搜索。其他类型的搜索方式包括范围搜索、短语搜索等。

表 6-6 搜索方式说明

搜索方式	说明	示例
全文搜索	配置全文索引后，日志服务根据您设置的分词符将整条日志拆分成多个关键词。 **说明** • content为日志原文对应的内置字段，搜索语句GET等同于content:GET，默认匹配日志原文的内容。 • 多个关键词默认通过AND连接，搜索语句GET POST等同于GET and POST。	• GET POST • GET and POST • content:GET and content:POST 上述三个搜索语句功能相同，均表示搜索同时包含关键词GET和POST的日志。

搜索方式	说明	示例
字段搜索	配置字段索引后，您可以指定字段名称和字段值（key:value）进行搜索。根据字段索引中设置的数据类型，您可以进行多种类型的基础搜索和组合搜索。 **说明** • value参数不可为空。 • 字段搜索和 not 运算符配合使用时，还会匹配到不包含该字段的日志。	• request_time>60 and request_method:po*表示搜索request_time字段值大于60且request_method字段值以po开头的日志。 • not request_method:GET表示搜索不包含request_method字段和request_method字段值不为GET的日志。
精确搜索	使用精确的词进行搜索。 日志服务搜索采用的是分词法，搜索时不会保证关键词出现的顺序。 **说明** 搜索语句为abc def，会匹配所有同时包含abc和def的日志，日志abc def或者def abc都会命中，如果需要确保关键词出现的顺序，请您采用**#"abc def"**。	• GET POST表示搜索同时包含关键词GET和POST的日志。 • request_method:GET表示搜索request_method字段值包含GET的日志。 • #"/var/log"表示搜索包含短语/var/log的日志。
模糊搜索	在搜索语句中指定一个词，在词的中间或者末尾加上模糊搜索关键字，即星号（*）或问号（?），日志服务会在所有日志中搜索到符合条件的词，返回包含这些词并满足搜索条件的所有日志。 **说明** • 星号（*）代表匹配多个字符，问号（?）代表匹配1个字符。 • 星号（*）或问号（?）不能用在词的开头。 • long数据类型和float数据类型不支持使用星号（*）或问号（?）进行模糊搜索。	• GE*表示在所有日志中查找以GE开头的词，并返回包含这些词的日志。 • request_method:GE*表示在所有日志中查找request_method字段值以GE开头的词，并返回包含这些词的日志。
范围搜索	long数据类型和float数据类型支持范围搜索。 • 方式1：通过 =（等于）>（大于）<（小于） 运算符搜索日志。 • 方式2：通过 in 运算符搜索日志，支持修改开闭区间。 **说明** string类型的字段不支持范围查询。	• request_time>=60表示在所有日志中查找request_time字段值大于等于60的日志。 • request_time in (60 120]表示在所有日志中查找request_time字段值大于60且小于等于120的日志。

搜索方式	说明	示例
短语搜索	短语搜索用于完全匹配日志中的目标短语，可以确保关键词出现的顺序。 **说明** 短语搜索不支持模糊搜索。	**#"abc def"**表示在所有日志中查找包含目标短语 abc def 的日志。

- 分词符

  云日志服务LTS会根据分词符，将日志内容拆分成多个词。日志服务默认配置的分词符为 **, '";=()[]{}@&<>/:\n\t\r**。

  例如日志**2023-01-01 09:30:00**，默认分词符会将其分为四部分：**2023-01-01**、**09**、**30**、**00**。

  此时搜索语句**2023**无法匹配到该条日志，可以通过**2023-01***或**2023-01-01**搜索到该条日志。

  如果设置分词符为空，则字段值将被当成一个整体，您只能通过完整日志内容或模糊搜索查找对应的日志。

- 关键词顺序

  只有短语搜索**#"abc def"**才能保证关键词出现的顺序，其他搜索方式多个关键词默认AND连接。

  例如**request_method:GET POST**查询的是同时包含GET和POST的日志，不会保证GET和POST的顺序。

- 语法关键词

  日志搜索语句的语法关键词包括：&& || AND OR and or NOT not in : > < = ( ) [ ] 中文冒号 中文双引号

  其中 **and AND or OR NOT not in** 作为语法关键词使用时，前后需要使用空格分隔；

  如果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，否则可能会导致语法错误或搜索到错误的结果。

  例如搜索语句**content:and**, 包含语法关键词 **and** ,需要修改为**content:"and"**。

运算符

搜索语句支持如下运算符。

说明

- 除in运算符外，其他运算符不区分大小写。
- 运算符的优先级由高到低排序如下所示：
  1. 冒号 (:)
  2. 双引号 ("")
  3. 圆括号( )
  4. and、not
  5. or

表 6-7 运算符说明

运算符	说明
and	与运算符，如果多个关键词之间没有语法关键词，默认为and关系，例如**GET 200**等同于**GET and 200**。 **说明** and作为运算符使用时前后需要使用空格分隔。例如 **1 and 2** 代表搜索同时包含**1** 和**2**的日志；**1and2**代表搜索包含词语**1and2**的日志。
AND	与运算符，等同于and。
&&	与运算符。 **说明** &&作为运算符使用时不需要使用空格分隔。例如 **1 && 2** 等同于**1&&2**，代表搜索同时包含**1** 和**2**的日志。
or	or运算符，例如**request_method:GET or status:200**。 **说明** or 作为运算符使用时前后需要使用空格分隔。
OR	或运算符，等同于or。
||	或运算符。|| 作为运算符使用时不需要使用空格分隔。
not	非运算符。例如**request_method:GET not status:200**、**not status:200**。 **说明** ● not 作为运算符使用时需要使用空格分隔。 ● not 运算符和字段搜索配合使用时还会匹配到不包含对应字段的日志。
( )	用于提高括号内搜索条件的优先级。例如**(request_method:GET or request_method:POST) and status:200**。
:	用于字段搜索（key:value），例如**request_method:GET**。 **说明** 如果字段名称或者字段值内有空格、冒号（:）等保留字符，请使用双引号（""）包裹字段名称或者字段值。例如**"request method":GET**、**message:"This is a log"**。
""	使用双引号（""）包裹一个语法关键词，可以将该语法关键词转换成普通字符，例如"and"表示搜索包含and的日志，此处的and不代表运算符。
\	转义符号，用于转义双引号（""），转义后的引号表示符号本身。例如日志内容为instance_id:nginx"01"，您可以使用instance_id:nginx\"01\"进行查询。
*	通配符搜索，匹配零个、单个、多个字符。例如**request_method:P*T**。 **说明** 不支持放在关键词开头，推荐放在关键词的中间部分或者结尾。
?	通配符搜索，匹配单个字符。例如**request_method:P?T**，可以匹配到PUT，无法匹配到POST。 **说明** 不支持放在关键词开头，推荐放在关键词的中间部分或者结尾。

运算符	说明
>	搜索某字段值大于某数值的日志。例如**request_time>100**。
>=	搜索某字段值大于或等于某数值的日志。例如**request_time>=100**。
<	搜索某字段值小于某数值的日志。例如**request_time<100**。
<=	搜索某字段值小于或等于某数值的日志。例如**request_time<=100**。
=	搜索某字段值等于某数值的日志，仅适用于float、long类型的字段。对于该类型的字段，等号（=）和冒号（:）作用相同。例如**request_time=100**等同于**request_time:100**。
in	搜索某字段值处于某数值范围内的日志，中括号表示闭区间，小括号表示开区间，两个数字之间使用空格分隔。例如**request_time in [100 200]**或**request_time in (100 200]**。 **说明** in只能为小写字母，且作为运算符使用时前后需要使用空格分隔。
#""	用于搜索包含目标短语的日志，可以保证关键词出现的顺序。 **说明** 短语搜索中的星号（*）和问号（?）会被视为普通字符，因此短语搜索不支持模糊搜索，可以用来搜索日志中的星号（*）和问号（?）。

搜索语句示例

同一条搜索语句，针对不同的日志内容和索引配置时，会有不同的搜索结果。本文基于如下日志样例和索引介绍搜索语句示例。

表 6-8 普通搜索示例

搜索需求	搜索语句
搜索POST请求且状态码为200的日志。	request_method:POST and status=200
搜索GET请求或POST请求成功（状态码为200~299）的日志。	(request_method:POST or request_method:GET) and status in [200 299]
搜索GET请求或POST请求失败的日志。	(request_method:POST or request_method:GET) not status in [200 299]
搜索非GET请求的日志。	not request_method:GET
搜索GET请求成功且请求时间小于60秒的日志。	request_method:GET and status in [200 299] not request_time>=60
搜索请求时间为60秒的日志。	• request_time:60 • request_time=60

搜索需求	搜索语句
搜索请求时间大于等于60秒，并且小于200秒的日志。	• request_time>=60 and request_time<200 • request_time in [60 200)
搜索包含and的日志。	content:"and" **说明** 此处使用双引号将and包裹，and为普通字符串，不代表运算符。
搜索不存在user字段的日志。	not user:*
搜索星期字段值不为星期一的日志。	not week:星期一
搜索sec-ch-ua-mobile字段值为?0的日志。	sec-ch-ua-mobile:#"?0" **说明** 日志内容中包含*或?且需要搜索时，需要采用短语查询。

下面介绍进阶搜索示例。

表 6-9 模糊搜索

搜索需求	搜索语句
搜索包含以GE开头的词的日志。	GE*
搜索包含以GE开头，结尾只有一个字符的词的日志。	GE?
搜索request_method字段值包含以G开头的词的日志。	request_method:G*
搜索request_method字段值包含以P开头，以T结尾，中间还有单个字符的词的日志。	request_method:P?T
搜索request_method字段值包含以P开头，以T结尾，中间包含零个、单个或多个字符的词的日志。	request_method:P*T

基于分词符的搜索，例如User-Agent字段值为**Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36**。

- 设置分词符为空时，该字段值将被当成一个整体，则您使用**User-Agent:Chrome**搜索语句进行搜索时，无法搜索到日志。
- 设置分词符为**, '";=()[]{}?@&<>/:\n\t\r**后，该字段值会被拆分为**Mozilla**、**5.0**、**Windows**、**NT**、**10.0**、**Win64**、**x64**、**AppleWebKit**、**537.36**、**KHTML**、**like**、**Gecko**、**Chrome**、**113.0.0.0**、**Safari**、**537.36**。

  此时可以使用**User-Agent:Chrome**等搜索语句进行搜索。

表 6-10 基于分词符的搜索

搜索需求	搜索语句
搜索User-Agent字段值中包含Chrome的日志。	User-Agent:Chrome
搜索User-Agent字段值中包含以Win开头的词的日志。	User-Agent:Win*
搜索User-Agent字段值中包含Chrome和Linux的日志。	User-Agent:"Chrome Linux"
搜索User-Agent字段值中包含Firefox或Chrome的日志。	User-Agent:Chrome OR User-Agent:Linux
搜索User-Agent字段值包含Chrome，但不包含Linux的日志。	User-Agent:Chrome NOT User-Agent:Linux

6.5.2 短语搜索

短语搜索用于准确匹配目标短语，例如搜索语句**abc def**，不区分先后顺序，将匹配所有同时包含**abc**和**def**的日志。短语搜索和关键词搜索的区别请参考**表6-11**。

- 短语搜索：在关键词搜索语法的基础上实现，短语搜索能够区分关键词的顺序，用于精准匹配目标短语，搜索结果更加精确。短语搜索适用于英文短语、中文短语的搜索，不支持模糊搜索。
- 关键词搜索：关键词搜索是基于分词实现，通过分词符先将搜索内容拆分为多个关键词，然后匹配日志。关键词搜索不会区分多个关键词在日志中出现的顺序，因此只要日志中按照搜索的与或非逻辑能命中关键词，该日志就会被搜索到。

表 6-11 搜索区别

搜索方式	短语搜索	关键词搜索
搜索区别	区分关键词的顺序，用于精准匹配目标短语，搜索结果更加精确。	不区分关键词的顺序，按照搜索逻辑命中关键词即可。
举例说明	假设您的日志流中存在2条原始日志，如下： • 原始日志1：this service is lts • 原始日志2：lts is service	
	短语搜索：#"is lts"，会命中1条日志。	关键词搜索：is lts，会命中2条日志。
	短语搜索：#"lts is"，会命中1条日志。	关键词搜索：lts is，会命中2条日志。

搜索语法

表 6-12 搜索方式

搜索方式	说明
全文搜索	• #"abc def" • content:#"abc def" **说明** content为日志原文对应的内置字段，**#"abc def"**等同于**content:#"abc def"**，默认匹配日志原文的内容。
字段搜索	key:#"abc def" **说明** • value参数不可为空。 • 字段搜索和not运算符配合使用时，还会匹配到不包含该字段的日志。

使用限制

- 短语搜索不支持搭配模糊搜索。

  短语搜索中的星号（*）和问号（?）会被视为普通字符，因此短语搜索不支持搭配模糊搜索，可以用来搜索日志中的星号（*）和问号（?）。

- 短语搜索不支持对分词符进行搜索。

  例如搜索语句**#"var/log"**，其中 / 为分词符，搜索语句等同于**#"var log"**，会搜索包含目标短语**var log**的日志。同理，搜索语句**#"var:log"**、**#"var;log"**等搜索的也是包含目标短语**var log**的日志。

- 中文搜索推荐采用短语搜索。

  由于中文默认采用的是一元分词，每个汉字单独分词，搜索时会匹配同时包含搜索语句中每一个汉字的日志，本身便具有模糊搜索的特性，当需要更加精确的结果时，推荐采用短语搜索。

示例说明

表 6-13 搜索说明

搜索需求	搜索语句
搜索User-Agent字段值包含短语Mon, 17 Apr 2023的日志。	User-Agent:#"Mon, 17 Apr 2023"
搜索User-Agent字段值包含短语Mozilla/5.0的日志。	User-Agent:#"Mozilla/5.0"
搜索week字段值包含短语星期一的日志。	week:#"星期一"

6.5.3 实时查看日志

您可以在云日志服务管理控制台实时查看上报的日志。

前提条件

- 已创建日志组和日志流。
- 已完成**ICAgent安装**。
- 已配置日志采集规则。

操作步骤

1. 在云日志服务管理控制台，单击“日志管理”。
2. 在日志组列表中，单击日志组名称前对应的 按钮。
3. 在日志流列表中，单击日志流名称，进入日志详情页面。
4. 在“实时日志”页签，查看实时日志。

日志每隔大约1分钟上报一次，在日志消息区域，您最多需要等待1分钟左右，即可查看实时上报的日志。

同时，还可以通过页面右上方的“清屏”、“暂停”对日志消息区域进行操作。

- 清屏：清除日志消息区域已经显示出来的日志。
- 暂停：暂停日志消息的实时显示，页面定格在当前已显示的日志。
  暂停后，“暂停”会变成“继续”，再次单击“继续”，日志消息继续实时显示。

说明

如果您正在使用实时查看功能，请停留在实时查看页面，请勿切换页面。如果离开实时查看页面，实时查看功能将会停止，重新开启后上一次查看的实时日志将不会显示。

6.5.4 快速分析

日志包含了系统性能及业务等信息，例如关键词ERROR的多少反应了系统的健康度，关键词BUY的多少反应了业务的成交量等，当您需要了解这些信息时，可以通过快速分析功能，指定查询日志关键词，LTS能够针对您配置的关键词进行统计，并生成指标数据，以便您实时了解系统性能及业务等信息。

前提条件

快速分析的对象为结构化日志中提取的关键字段，创建快速分析前请先对原始日志进行结构化配置。

创建快速分析

可通过日志结构化打开“快速分析”按钮进行创建。也可通过如下步骤进行创建。

步骤1 登录云日志服务控制台，在左侧导航栏中选择“日志管理”。

步骤2 快速分析以日志流为单位，请在“日志管理”页面选择目标日志组和日志流。

步骤3 支持两种方式创建快速分析：

1. 单击 进入设置详情页面，在索引配置页签的字段索引下方，添加字段时开启快速分析。
2. 在结构化配置页签，开启自动配置索引和快速分析，默认是开启状态。开启后将使用结构化字段配置字段索引并打开快速分析。

步骤4 单击“创建快速分析”，跳转到索引配置页面添加需要快速分析的字段。

步骤5 单击“确定”，快速分析创建完成。

说明

- 快速分析的字段长度最大为2000字节。
- 快速分析字段展示前100条数据。

----结束

6.5.5 快速查询

当您需要重复使用某一关键字搜索日志时，可以将其设置为快速查询语句。

操作步骤

1. 在云日志服务控制台，单击“日志管理”。
2. 在日志组列表中，单击日志组名称前对应的 按钮。
3. 在日志流列表中，单击日志流名称，进入日志详情页面。
4. 在日志流详情页面，单击 ，输入“快速查询名称”和“快速查询语句”。
   - 快速查询名称，用于区分多个快速查询语句。名称自定义，需要满足如下要求：
     - 只支持输入英文、数字、中文、中划线、下划线及小数点。
     - 不能以小数点、下划线开头或以小数点结尾。
     - 长度为1-64个字符。
   - 快速查询语句，搜索日志时需要重复使用的关键字，例如“error*”。
5. 单击“确定”，完成快速查询条件的创建。
   单击快速查询语句的名称，查看日志详情。

查看上下文

您可以通过本操作查看指定日志生成时间点前后的日志，用于在运维过程中快速定位问题。

1. 在日志详情页面的原始日志页签，单击可以查看上下文。
   在查看上下文结果中，可以查看该日志的前后若干条日志详细信息。
2. 在弹出的查看上下文页面中，查看日志上下文。

表 6-14 查看上下文日志功能介绍

功能	说明
查询行数	查询日志的行数，有三种选择：100、200和500。
高亮显示	输入需要高亮的字符串，回车确认，在日志内容中高亮显示。
过滤日志	输入需要过滤的字符串，回车确认，在日志内容中高亮显示。当高亮显示和过滤日志同时设置时，均可高亮显示。
显示字段	查看上下文，默认字段为content，单击“显示字段”选择查看其他字段的上下文。
更早	从当前位置往前查看设置**查询行数**的二分之一。例如：当查询行数设置为100时，单击“更早”则从当前位置朝前显示50行，此时行号为-50；再次单击“更早”，依次叠加分别为-100、-150、-200.....
当前位置	当前日志位置。当设置了更早或更新时，单击“当前位置”可回到查看上下文开始的位置，即行数为0时。
更新	从当前位置往后查看设置**查询行数**的二分之一。例如：当查询行数设置为100时，单击“更新”则从当前位置朝后显示50行，此时行号为50；再次单击“更新”，依次叠加分别为100、150、200.....

7 日志告警

7.1 过滤器

7.1.1 通过自定义指标查询日志

每个日志流允许创建5个过滤器。本操作指导用户按需配置需要过滤的关键指标，并且通过应用运维管理服务对过滤的指标进行监控及告警。

1. 登录控制台。
2. 选择“服务列表 ☰ >管理与部署 > 云日志服务 LTS”。
   进入云日志服务界面，默认进入日志管理页面。
3. 在日志组列表中单击需要查看的日志所在的日志组名称。
   进入该日志组下的日志流列表页面。
4. 单击“指标过滤”，进行配置。
5. 参考**表7-1**，过滤指标参数配置完成后，单击“确定”，完成过滤器的创建。

表 7-1 指标过滤参数解释

名称	说明
过滤器名称	过滤器名称帮助您区分同一日志流下的不同过滤器，过滤器名称只支持输入英文、数字、中文、中划线、下划线以及小数点，且不能以小数点、下划线开头或以小数点结尾。
过滤关键词	过滤器将会按照您输入的过滤关键词在该日志流下执行过滤和累加关键词的动作。 仅支持过滤单个字词，例如Error、Warning或者Fail to root等，不支持过滤组合后的字词，日志服务的过滤方式是精确匹配，且区分大小写，数字及特殊符号需用双引号包含起来。

名称	说明
日志样例	日志样例用于测试配置的“过滤关键词”是否能匹配到相关日志，如果无法匹配到相关日志，可以在日志列表中寻找符合条件的日志粘贴到测试框中验证过滤关键词是否生效，也可以调整过滤关键词。
指标名称	指标名称是指“过滤关键词”对应的指标名称，类似key-value中的key值，以便日志服务帮助您做指标统计，并且将指标统计值发布到应用运维管理服务便于您在对日志中的关键指标进行监控及告警。指标名称可以由1~64位的大小写字母、数字和下划线组成，并且必须以大小写字母作为开头。请注意同一日志流下的指标名称不能重复，否则可能会造成数据不准的情况出现。

7.1.2 禁用过滤器

操作场景

对于已经配置过滤器的日志流可能出现日志格式或日志内容变化导致当前过滤关键词失效，该章节用于指导用户禁用已经失效或者不需要再进行监控及告警的过滤器。

前提条件

- 已获取控制台的登录账号与密码。
- 已创建日志组。
- 已创建日志流。
- 已完成日志采集。
- 已完成自定义指标过滤器的配置。

操作步骤

1. 登录控制台。
2. 选择“ ☰ >管理与部署 > 云日志服务 LTS”。
   进入云日志服务界面，默认进入日志管理页面。
3. 在日志组列表中选择需要禁用的过滤器所在的日志组名称。
   进入该日志组下的日志流列表页面。
4. 在日志流列表，找到目标日志流所在行。
5. 单击“指标数”下的数字或横线，进入该日志流下的“自定义指标过滤器”列表。
6. 对于需要禁用的过滤器，单击其所在行的禁用按钮。

   说明

   过滤器禁用后，您将无法在应用运维管理服务中再针对这项指标进行监控。

7.1.3 删除过滤器

操作场景

由于一个日志流下只能配置5个关键指标过滤器，所以如果您增加过滤器配置请您先删除不需要使用的过滤器后再试，本章节指导用户在日志列表中删除不需要使用的过滤器。

前提条件

- 已获取控制台的登录账号与密码。
- 已创建日志组。
- 已创建日志流。
- 已完成日志采集。
- 已完成自定义指标过滤器的配置。

操作步骤

1. 登录控制台。
2. 选择“ ☰ >管理与部署 > 云日志服务 LTS”。
   进入云日志服务界面，默认进入日志管理页面。
3. 在日志组列表中选择需要删除的过滤器所在的日志组名称。
   进入该日志组下的日志流列表页面。
4. 在日志流列表，找到目标日志流所在行。
5. 单击“指标数”下的数字或横线，进入该日志流下的“自定义指标过滤器”列表。
6. 对于需要删除的过滤器，单击其所在行的删除按钮。

   说明

   删除过滤器后，您将无法在应用运维管理服务中再针对这项指标进行监控，之前配置的告警规则可能会因为数据不足而触发告警。

8 日志转储

8.1 概述

主机和云服务的日志数据上报至云日志服务后，默认存储时间为7天不支持修改。超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），云日志服务提供转储功能，可以将日志转储至对象存储服务（OBS）中或自定义Kafka中长期保存。

说明

日志转储功能只能拷贝已有日志，不会删除日志。根据配置的存储时间可定时清理日志文件，不会影响转储后的日志。

8.2 转储至 OBS

对象存储服务 OBS提供日志存储功能；您可以将日志转储至OBS，并在OBS控制台下载日志文件。

说明

创建日志转储时，除需拥有LTS使用权限外，还需要拥有OBS Administrator权限。

前提条件

- 日志已接入LTS。
- 已创建OBS。

创建日志转储

1. 在云日志服务控制台，左侧导航栏中，单击“日志转储”。
2. 在“日志转储”页面右上角，单击“配置转储”。
3. 在“配置转储”页面，设置转储日志相关参数。

   说明

   转储任务创建成功后，日志组名称日志流名称和转储对象不支持修改，其他参数支持修改。

表 8-1 配置转储参数说明

参数名称	说明	样例
是否开启转储	默认开启转储。	开启
转储对象	选择转储的云服务。	OBS
日志组名称	选择已创建的日志组。	-
日志流名称	选择已创建的日志流。	-
OBS桶	● 选择已创建的OBS桶。 – 如果没有可选择的OBS桶，单击“查看OBS”，进入对象存储服务管理控制台，创建OBS桶。 ● LTS目前仅支持存储类别为“标准存储”的OBS桶。	-
自定义转储路径	● 开启：将日志转储至自定义路径中，用于区分不同日志流之间的转储日志文件。格式为：/LogTanks/RegionName/*自定义转储路径*。自定义转储路径默认为lts/%Y/%m/%d，其中%Y代表年，%m代表月，%d代表日，格式需要符合如下规范： – “/LogTanks/RegionName”为系统默认路径，不可以修改。 – 名称只能由英文字母、数字及特殊字符“&”“$”“@”“;”“:”“,”“=”“+”“?”“-”“.”“_”“/”和“%”组成，且“%”后只可跟Y（年）、m（月）、d（日）、H（时）、M（分），在%Y、%m、%d、%H和%M前后可以添加任意长度字符，并且可对其先后顺序进行调换。 – 自定义转储路径名称不允许为空，长度限制为1~128个字符。 示例： 1. 输入LTS-test/%Y/%m/%done/%H/%m，则日志转储路径为：*LogTanks/RegionName/LTS-test/Y/m/done/H/m/日志文件名称*。 2. 输入LTS-test/%d/%H/%m/%Y，则日志转储路径为：*LogTanks/RegionName/LTS-test/d/H/m/Y/日志文件名称*。 ● 不开启：将日志转储至系统默认路径中。系统默认路径为：LogTanks/RegionName/*2019/01/01/日志组/日志流/日志文件名称*。	LTS-test/%Y/%m/%done/%H/%m

参数名称	说明	样例
日志文件前缀	转储至OBS桶中的日志文件前缀。 日志文件前缀需符合如下规范： ● 名称长度限制为0~64个字符。 ● 名称只能由英文大小写字母、数字、中划线“-”、下划线“_”和小数点“.”组成。 示例：输入LTS-log，则日志文件名称为：LTS-log_日志文件名称。	LTS-log

转储格式	用于配置日志的转储格式，可选择“原始日志格式”、“Json格式”。
	● 原始日志格式示例：
	云日志服务控制台展示的日志内容的格式为原始日志格式。
	`Sep 30 07:30:01 ecs-bd70 CRON[3459]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1)`
	● JSON格式示例：
	`{"host_name":"ecs-bd70","ip":"192.168.0.54","line_no":249,"message":"Sep 30 14:40:01 ecs-bd70 CRON[4363]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1)\n","path":"/var/log/syslog","time":1569825602303}`
		Json

转储周期	日志自动转储至OBS桶的时间间隔，支持2分钟、5分钟、30分钟、1小时、3小时、6小时、12小时。	3小时
文件名时区	日志自动转储至OBS桶时，按照UTC时间生成转储目录及文件名称。	(UTC)协调世界时间
是否投递tag	如主机日志，转储时会增加采集器收集的tag字段。 ● 不开启：不会投递tag。 ● 开启：默认的投递tag有：主机信息（hostIP、hostId、hostName、pathFile、collectTime）；kubernetes信息（clusterName、clusterId、nameSpace、podName、appName、containerName）。可选择公共tag有：regionName、projectId、logStreamName、logGroupName。 **说明** 当开启投递tag后，转储格式必须是JSON格式。 ● 转储标签：开启后，会将日志流标签添加至转储内容。	开启

4. 单击“确定”，完成配置。当转储任务状态为“正常”时，表示转储任务创建成功。
5. 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。

   转储到OBS后的日志，支持从OBS下载到本地进行查看。

   说明

   转储至OBS的日志支持下载的格式：原始日志、JSON格式。

修改日志转储

1. 在日志转储列表中，单击待修改配置转储任务所在行的“修改”，弹出“修改转储”对话框，进行修改。
2. 修改完成后，单击“确定”。

查看转储详情

1. 在日志转储列表中，单击待查看配置转储任务所在行的“详情”。
2. 在弹出的“转储详情”页面中，可查看日志转储详情。

删除转储任务

如果日志不再需要转储，可以删除转储任务。

说明

- 转储任务一旦删除将不再对日志进行转储，请谨慎操作。
- 删除转储任务后，之前已经转储日志将会继续保存在OBS。
- 创建转储任务时，选中的OBS桶会将读写策略授权给云日志服务。当多个转储任务使用同一OBS桶时，如您需要删除转储任务，请按如下操作：
  - 如果仅使用该OBS桶创建了一个转储任务，删除该转储任务时，请在对象存储服务（Object Storage Service，OBS）中，**“访问权限控制”>“桶ACLs”**里删除特定用户的桶访问权限。
  - 如果使用该OBS桶创建了多个转储任务，请勿删除桶访问权限，否则会导致转储失败。

1. 在日志转储列表中，单击待删除的日志组所在行的“删除”，弹出“删除”对话框。
2. 单击“确认”，删除转储任务。

查看转储状态

日志转储任务的转储状态共分为正常、异常、关闭三种状态。

- 正常：日志转储任务正常进行。
- 异常：日志转储任务异常，可能是如下原因导致：
  - OBS桶被删除，请您重新指定已创建的OBS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。
  - OBS加密桶的密钥被删除或被取消授权，请您确保授权密钥的合法性。
- 关闭：日志转储任务停止。

9 配置中心

9.1 日志采集

为了减少内存、数据库和磁盘空间占用，您可以按需进行日志采集设置。日志采集开关用来控制是否对日志数据进行采集。

步骤1 在云日志服务管理控制台，单击“配置中心”，选择“日志采集开关”。

步骤2 单击开启或关闭“日志采集开关”。

说明

采集开关默认打开，当您不需要采集日志时，可通过关闭采集开关来停止日志采集，以减少资源占用。

----结束

10 常见问题

10.1 日志采集

10.1.1 使用 ICAgent 过程中，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。

10.1.2 云日志服务可以采集哪类日志？支持采集哪些文件类型?

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，需要到对应的云服务上启用日志上报。

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。

10.2 日志搜索与查看

10.2.1 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。

10.2.2 在云日志服务控制台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
- 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。
- 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。
- 更换Google Chrome 或Firefox浏览器查询日志。

10.2.3 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（默认7天）自动清理过期的日志数据。

10.2.4 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，详细请参考索引配置。
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，详细请参考索引配置。
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。
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"**。

10.3 日志转储

10.3.1 日志转储后，LTS 会删除转储的内容吗?

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。

10.3.2 日志转储页面，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。

10.3.3 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. 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”。
4. 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。

10.4 其他问题

10.4.1 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。

说明

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。

操作步骤

1. 登录控制台，将鼠标移动到右上方的用户名称，并在下拉列表中选择“我的凭证”。
2. 在“我的凭证”页面中选择“访问密钥”。
3. 在列表上方单击“新增访问密钥”，输入访问密钥信息。
4. 单击“确定”，创建成功后请立即下载密钥信息（AK/SK）。

   说明

   为防止AK/SK泄露，建议您将其保存到安全的位置。

A 修订记录

版本日期	变更说明
2024-04-14	第一次正式发布。